# *Made in Surveillance:* A regulação da importação e do uso de tecnologias de vigilância estrangeiras e a relativização dos direitos fundamentais e da soberania estatal

MARIANA CANTO[1]

**Resumo**

Na posição de anfitrião de grandes eventos mundiais, o Brasil se tornou um dos principais laboratórios a céu aberto para as tecnologias de vigilância estrangeiras. No entanto, informações a respeito da origem e do tipo de tecnologia adquirida são escassas e dependem principalmente de declarações de agentes públicos, empresas privadas, e, quando deferidos, pedidos possíveis graças à Lei de Acesso à Informação (LAI).
Além da distopia *orwelliana* brasileira acontecer no plano real por meio de importações de dispositivos estrangeiros, o fornecimento, por exemplo, de um banco de dados com informações de pessoas procuradas a empresas internacionais e a opacidade em relação à falta de dados oficiais acerca da eficácia das novas medidas são só algumas das diversas problemáticas constatadas.
Este ano, a utilização da tecnologia de reconhecimento facial durante o Carnaval brasileiro e as prisões efetuadas em decorrência do seu uso chamou a atenção de grande parte da sociedade. Entretanto, desde 2014 cidades brasileiras firmam projetos de parceria com empresas estrangeiras provedoras de equipamentos de vigilância e monitoramento para fins de segurança pública.
Desse modo, o presente artigo realizará, inicialmente, uma apresentação de casos emblemáticos no ecossistema brasileiro e, em seguida, do arcabouço legal pátrio relacionado à regulação da importação e do uso de tecnologias de vigilância estrangeira. Por fim, busca-se a realização de uma análise acerca da existência de medidas e narrativas adotadas pelo setor privado a fim de garantir o uso ético das tecnologias exportadas. Espera-se que o trabalho incite reflexões e discussões multidisciplinares e multissetoriais a partir dos resultados apresentados.

Palavras-chave: tecnologia; vigilância; privacidade; soberania; direitos humanos.

## Introdução

Durante os últimos anos, devido a sua posição de anfitrião de grandes eventos mundiais, o Brasil chamou a atenção não só das delegações e turistas ao redor do mundo, mas também de diversas empresas e multinacionais estrangeiras. Como afirma Stephen Graham, professor de Arquitetura e Planejamento da Universidade de Newcastle, a organização dos chamados megaeventos mundiais funciona, muitas vezes, como vitrines para novas tecnologias de vigilância e segurança.

Um outro atrativo próprio de situações em que grandes aglomerados de pessoas são previstos é a relativização de direitos fundamentais e a flexibilização de leis que limitam a vigilância devido a magnitude dos acontecimentos (GRAHAM, 2016:16-17). Dessa maneira, como sede de eventos de grande visibilidade internacional como Carnavais anuais, a conferência Rio+20 em 2012, a Copa do Mundo masculina de futebol de 2014, os Jogos Olímpicos e Paraolímpicos de 2016 e a Copa América

[1] Mariana Canto é pesquisadora do Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.rec) e graduada em Direito pela Universidade Federal de Pernambuco (UFPE). E-mail: sobralcantomariana@gmail.com.

masculina de futebol de 2019, o Brasil se tornou um dos principais e mais atraentes laboratórios a céu aberto para as tecnologias de vigilância estrangeiras durante a última década.

Entretanto, apesar de bastante conveniente, os grandes eventos com milhares de participantes e as ofertas de empresas estrangeiras não são o único fator determinante para a aplicação das tecnologias de vigilância nos centros urbanos brasileiros. Assim como explana o professor Marcelo Lopes de Souza, da UFRJ, no Brasil, o endurecimento penal e a militarização de assuntos de natureza policial são a causa principal do incentivo ao uso, cada vez maior, de aparatos e tecnologias distópicos e invasivos, típicos de zonas de combate (SOUZA, 2015: 38). Mesmo após uma série de mudanças ocorridas no Brasil desde a promulgação da Constituição de 1988, as instituições de segurança pública não foram significativamente modificadas. Assim, a cultura da guerra ao "inimigo interno", por exemplo, permanece tão presente como nos tempos da ditadura militar (CARVALHO, 2019).

Além dos aspectos sociais, a escassez e a falta de acesso a documentos e a informações claras e públicas se fazem presente. Muitas vezes, o acesso a informações relacionadas ao funcionamento das tecnologias adquiridas pelo ente público dependem principalmente de declarações de agentes públicos, empresas privadas, e, quando deferidos, pedidos de acesso a informações públicas que se tornam possíveis graças à Lei de Acesso à Informação (LAI).

## 1. Grandes eventos e suas grandes portas de entrada

### 1.1. Copa do Mundo de futebol masculino 2014: o início do fim da privacidade

Considerado por muitos um dos eventos mundiais mais importantes do globo, a Copa do Mundo de futebol masculino de 2014 representou o palco ideal para que as novas tecnologias de vigilância estatal fossem não só aplicadas com justificativas plausíveis para muitos mas também divulgadas em uma grande vitrine internacional.

Vistas inicialmente como ferramentas de aplicação temporária, as centenas de câmeras de vigilância instaladas em sedes do torneio são parte de um projeto de vigilância denominado Sistema Integrado de Comando e Controle (SICC), que toma corpo por meio de centros de controle espalhados ao redor do país. Criado pela Secretaria de Segurança para Grandes Eventos (SESGE), a pedra angular do sistema são os chamados Centros Integrados de Comando e Controle, também conhecidos por CICCs, localizados em cada uma das cidades que foram palco de partidas do torneio, que são caracterizados como "órgão de gestão integrada de operações e resposta a incidentes de segurança pública, dotado de equipes de alto desempenho, modelo lógico, ferramentas de inteligência e sistemas tecnológicos de última geração capazes de prover uma imagem fiel e em tempo real do panorama global, eventos

associados e recursos envolvidos." (BRASIL, 2013). Além da construção de CICCs, o Brasil também investiu na compra de tecnologias estrangeiras de modo a assegurar a execução da Copa do Mundo masculina da FIFA. Assim, a Força Aérea Brasileira realizou até mesmo a compra de um drone da empresa israelense Elbit System no valor de 8 milhões de dólares. O veículo não tripulado tinha como finalidade a vigilância de zonas de grande acumulação de pessoas durante os jogos da Copa do Mundo (FOLHA DE SÃO PAULO, 2014).

### 1.2. Jogos Olímpicos e Paraolímpicos de 2016: o agravamento do *panopticon* carioca

Orçada em um pouco mais de 100 milhões de reais e inaugurada em 2013, como um dos casos de maior consolidação do modelo CICC, a unidade localizada na cidade do Rio de Janeiro possui quatro pavimentos equipados com tecnologia de vigilância e monitoramento avançada, tendo sido administrada, até janeiro de 2019, pela Secretaria de Segurança do Estado, extinta pelo governador Wilson Witzel. Hoje, o centro de vigilância encontra-se dividido entre as secretarias de polícia militar e civil. Com acesso a pelo menos 3.200 câmeras de vigilância, o "*panopticon* carioca", une-se ao Centro de Operações (COR), um centro municipal, em grande parte equipado pela empresa norte-americana IBM, possibilitando o acesso aos dados de mais 560 câmeras à polícia. Assim, o Rio ganha destaque dentre os demais centros por representar um contorno bem mais visível e distópico a respeito do uso de novas tecnologias com finalidades de vigilância. Durante a realização dos Jogos Olímpicos e Paraolímpicos do Rio de Janeiro, CICCs "setoriais" também foram construídos próximos às arenas olímpicas. Todo CICC oferece transmissões de várias camadas de informações, incluindo atividades em redes sociais, sensores de tráfego entre outras.

Além da construção de CICCs setoriais, a importação de dispositivos de tecnologias de vigilância e controle social também foi constatada por veículos de mídia brasileiros. Em julho de 2016, o jornalista João Paulo Vicente investigou a importação e o uso de simuladores de IMSI fornecidos pela empresa estado-unidense Harris Corporation a órgãos de segurança brasileiros. Entretanto, problemas relacionados ao quesito transparência foram encontrados, assim como a escassez de informações relacionadas à contratação e compra dos produtos (VINCENTE, 2016). Além da empresa americana vender os equipamentos de vigilância por intermédio de empresas parceiras brasileiras, de acordo com o jornalista, o repasse, muitas vezes, é feito no meio de contratos a respeito de outros produtos. Além disso, de acordo com Dia Kayyali, jornalista e ativista estado-unidense, os contratos de venda de dispositivos como StingRays e similares, por parte da Harris Corporation, envolvem também, em muitos casos, cláusulas de confidencialidade.

**1.3.Carnaval 2019: quando máscaras protegem direitos**

Já no ano de 2019, a utilização da tecnologia de reconhecimento facial durante o Carnaval brasileiro e as prisões efetuadas em decorrência do seu uso chamaram a atenção de grande parte da sociedade. Durante o feriado, quatro pessoas foram presas no estado do Rio de Janeiro enquanto em Salvador um caso de prisão foi computado. Mesmo com a questão tendo a sua relevância aumentada devido às prisões, desde 2018 cidades brasileiras firmaram projetos de parceria com a chinesa Huawei visando à instalação de sistemas de reconhecimento facial. Apesar de preocupações a respeito da privacidade e proteção de dados dos cidadãos por parte da sociedade civil, o uso de softwares de reconhecimento facial na segurança pública foi fortemente defendido pelo presidente Jair Bolsonaro (PSL) durante a sua campanha eleitoral e pelos governadores do Rio, Wilson Witzel (PSC), e da Bahia, Rui Costa (PT) como uma grande inovação no combate ao crime.

No Rio de Janeiro, por exemplo, desde janeiro de 2019 uma parceria entre a Polícia Militar, a Polícia Civil e a empresa de telefonia Oi tem acontecido com o intuito de tornar a tecnologia cada vez mais presente nas ruas cariocas. Apesar do projeto-piloto durante o Carnaval ter sido formado por 28 câmeras instaladas na orla de Copacabana, a Oi, parceira da Huawei e responsável pela implementação da tecnologia, não responde aos questionamentos da imprensa a respeito do local de armazenamento ou processamento dos dados coletados, apenas que a operação da plataforma era feita de forma exclusiva pela Secretaria de Segurança Pública do Rio de Janeiro (AGÊNCIA DATA LABE, 2019).

**1.4. Copa América 2019: hermanos pero no mucho**

O dito sucesso das ferramentas de reconhecimento facial nos últimos grandes eventos brasileiros tem incentivado a sua adoção em outros espaços. De acordo com a Secretaria de Segurança Pública (SSP) do Rio Grande do Sul, por exemplo, um banco de dados com cerca de 8 milhões de cidadãos cadastrados será utilizado durante a Copa América 2019 para fins de reconhecimento facial. Um ponto importante a ser frisado é o conteúdo do banco de dados. Diferentemente de sistemas anteriormente implementados, o sistema contará não apenas com dados de pessoas foragidas, mas também com informações de todos os cidadãos cadastrados no banco de dados do estado. De acordo com a Secretaria de Segurança Pública do estado, o objetivo deste convênio é “aprimorar a integração do Estado e criar uma alternativa permanente para o uso do reconhecimento facial”. (SECRETARIA DE SEGURANÇA PÚBLICA DO RIO GRANDE DO SUL, 2019)

Em maio de 2019, o Escritório da Copa América em Porto Alegre recebeu uma lista com cerca de 2 mil torcedores argentinos com histórico de violência, conhecidos como “barra bravas”. Atualmente, a

lista formada pela SSP conta com mais de 4 mil estrangeiros com esse perfil. Os dados foram enviados pelo Ministério das Relações Exteriores e estão com o Departamento de Inteligência da Segurança Pública (Disp).

De acordo com o gerente de Segurança do Comitê Organizador Local da Conmebol, Hilário Medeiros, o projeto, que foi organizado por meio de parcerias entre órgãos de segurança pública e a Interpol, contará com um banco de dados com informações de todo o mundo. De acordo com o gerente "o Brasil organizou uma série de eventos recentemente, como a Copa do Mundo e os Jogos Olímpicos e Paralímpicos, e nada, do ponto de vista da segurança, manchou qualquer um desses eventos". De acordo com portais de notícias, a operação conta com a participação de agentes da Secretaria de Operações Especiais, do Ministério da Justiça, membros da Polícia Federal, da Polícia Rodoviária Federal, da Agência Brasileira de Inteligência (Abin), do Ministério das Relações Exteriores e representantes dos cinco estados onde haverá jogos: São Paulo, Rio de Janeiro, Bahia, Minas Gerais e Rio Grande do Sul.

## 2. O descobrimento da ciberespionagem

### 2.1.A ciberespionagem no Brasil

A atual posição de dependência brasileira de produtos tecnológicos estrangeiros não é um fato desvinculado a acontecimentos ligados às relações de política externa e interna do país. Durante a década de 1980, o modelo econômico instalado pela política das grandes potências, como é o caso dos Estados Unidos, resultou em disputas junto ao governo norte-americano relacionadas ao setor de informática. Como fator agravante, a privatização das telecomunicações em 1990 acabaram por enfraquecer não só um setor estratégico do país mas a indústria nacional de produtos de comunicação e informática, facilitando a entrada de agentes estrangeiros nos meios de comunicação brasileiros, assim como o acesso a dados pessoais dos cidadãos.

A união desses fatores fez com que o país recuasse no setor industrial de informática e com que o cenário de pesquisa e produção tecnológica nacional na referida área fosse dificultado. Apesar de leis que visavam incentivos fiscais para empresas desenvolvedoras de tecnologias, como é o caso da Lei de Informática (8.248/91, 10.176/01, 11.077/04 e 13.023/14), as limitações ainda existentes deixaram o Brasil à mercê da tecnologia produzida pelos grandes centros do mundo. Tecnologias estas que, muitas vezes, são representadas por dispositivos e equipamentos com mecanismos de *backdoor* integrados, o que pode possibilitar, por exemplo, a espionagem internacional, como ficou claro por

meio das informações altamente confidenciais da Agência de Segurança Nacional (NSA) vazadas em 2013 por Edward Snowden (GREENWALD, 2014).

Como afirma o professor de Relações Internacionais da London School of Economics, Barry Buzan, a "dupla utilização" da tecnologia e a influência de forças motrizes como a ação humana dos seus desenvolvedores, faz com que a tecnologia não precise necessariamente de uma natureza militar para que tenha o poder de impactar em questões de segurança e defesa de um Estado soberano (Buzan, 2009). Além da facilitação do acesso a dados em sistemas, o desenvolvimento da espionagem virtual, também chamada de ciberespionagem, possibilitou uma maior segurança ao agente infiltrado, que teve as suas chances de captura drasticamente reduzidas.

Com a relativização da necessidade de uma atuação 'in loco' do espião, um novo perfil de agente foi instaurado. Apesar do treinamento em técnicas de espionagem convencionais ainda existir, o perfil extremamente rígido, de formação ideológica típico do período da Guerra Fria é abandonado para que agentes como jovens com bagagem em áreas de conhecimentos cibernéticos e experiências não institucionalizadas tomem o seu lugar, como foi o caso do ex-agente Edward Snowden.

Em 9 de junho de 2013, o mundo ouviu pela primeira vez um nome que ficaria gravado na história internacional. Edward Snowden. Responsável pelo vazamento de uma série de documentos e arquivos que revelavam um esquema de vigilância e espionagem internacional esquematizado pela Agência de Segurança Nacional Norte-Americana, a NSA, o analista, por meio de entrevistas publicadas no *The Guardian* e no *Washington Post* foi autor de uma das maiores revelações que abalaram as políticas internacionais e intergovernamentais nas últimas décadas. Por meio da análise dos documentos divulgados, mostrou-se comprovada a capacidade das agências americanas, muitas vezes por meio de colaborações com o setor privado, de acessar informações, por exemplo, armazenadas em bancos de dados de empresas americanas.

As respostas e reações ao redor do mundo em relação ao caso Snowden foram as mais diversas. Entretanto, uma das mais marcantes e relevantes para o cenário internacional foi a reação do governo Brasileiro, mais especificamente a da presidenta Dilma Rousseff, que por meio das revelações tomou conhecimento de que não só a sua conta de e-mail pessoal estava sendo vigiada como também toda a rede de computadores da empresa Petrobras.

Como primeira medida tomada pela chefe do Estado brasileiro, a presidenta cancelou a sua visita presidencial aos Estados Unidos assim como se utilizou do discurso de abertura da Assembleia Geral das Nações Unidas de 2013 para condenar, de maneira pública, o uso da espionagem por parte do governo norte-americano, considerando o ato como uma violação aos direitos humanos, liberdades

civis assim como um desrespeito à soberania nacional. Rousseff também enfatizou a necessidade do Brasil intensificar os seus esforços para a construção e adoção de legislações, tecnologias e mecanismos que protegessem o país de interceptações ilegais em seus meios de comunicação e bancos de dados. Dessa maneira, o caso Snowden serviu não só para uma mudança de estratégias e infraestrutura do ciberespaço brasileiro, mas também como um catalisador da elaboração e aprovação do Marco Civil da Internet.

Os documentos de Snowden revelaram não só a espionagem da população brasileira mas também de dezenas de países, até mesmo daqueles considerados como aliados dos norte-americanos. De acordo com os documentos publicizados na obra de Glenn Greenwald, grande parte dos documentos possuía o acrônimo da aliança dos Cinco Olhos (Five Eyes) e revelavam o aparato técnico utilizado para a interceptação de comunicações, entre eles servidores de internet, satélites, cabos de fibra ótica submarinos, sistemas de telefonia nacionais e estrangeiros e computadores pessoais. O Brasil, visto aparentemente como uma incógnita aos olhos norte-americanos, catalogado como “amigo, inimigo ou problema?” em um documento secreto, foi alvo do programa americano BOUNDLESS INFORMANT, e do programa canadense OLYMPIA, que tinha como objetivo o monitoramento do Ministério das Minas e Energia brasileiro. O programa de espionagem BLARNEY, por sua vez, foi possível a partir do acesso a determinadas empresas de telecomunicações por meio de contratos firmados com companhias estrangeiras para criação, suporte e melhoria de suas redes. De modo semelhante, o programa OAKSTAR, utilizava-se do acesso de um dos ‘parceiros’ corporativos da NSA de modo a obter informações acerca de sistemas de telecomunicações estrangeiros. Já o programa BLACKPEARL foi responsável por interceptar conversas e e-mails da Petrobras por meio de cracks da sua rede virtual privada, programas de escuta e interceptações de e-mails da presidenta Dilma Rousseff, e, por fim, por meio de obtenção de várias formas de acesso às embaixadas e consulados, especialmente em Washington, D.C e Nova York, sobretudo por via do programa SIGAD US-3136.

**2.2. A resposta do Brasil no cenário do direito internacional**

Além das repercussões em solo brasileiro, no cenário internacional as respostas às revelações do Caso Snowden também se mostraram impactantes. A presidenta Dilma Rousseff e a chanceler alemã Angela Merkel em 2013 apresentaram perante a Assembleia Geral da ONU de 2013 a Resolução 68/167 [*The right to privacy in the digital age]* na qual a privacidade na internet seria um direito humano fundamental e busca as mesmas condições conferidas à “privacidade offline” ao ambiente online. A Resolução buscou demonstrar a gravidade do fato e o nível de preocupação internacional acerca da descoberta:

Deeply concerned at the negative impact that surveillance and/or interception of communications, including extraterritorial surveillance and/or interception of communications, as well as the collection of personal data, in particular when carried out on a mass scale, may have on the exercise and enjoyment of human rights.

Como também convidou a comunidade internacional a unir esforços em prol da proteção do direito à privacidade e violações aos direitos humanos no ambiente digital por meio das seguintes disposições:

**4. Calls upon all States:**

(a) To respect and protect the right to privacy, including in the context of digital communication;

(b) To take measures to put an end to violations of those rights and to create the conditions to prevent such violations, including by ensuring that relevant national legislation complies with their obligations under international human rights law;

(c) To review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law;

(d) To establish or maintain existing independent, effective domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data.

Em seu discurso, a presidenta Dilma Rousseff afirmou que a rede mundial de espionagem dos Estados Unidos causava repulsa em toda a comunidade internacional uma vez que a invasão caracterizava não apenas uma afronta às relações internacionais mas também violação ao direito internacional. A aprovação unânime da Resolução por parte das nações presentes foi vista como um recado ao governo norte-americano onde a mensagem era clara: era preciso por um fim na vigilância generalizada da NSA.

Rousseff também aproveitou a abertura da Assembleia Geral da ONU em 2013, para anunciar a organização do evento NETmundial, um Encontro Multissetorial Global Sobre o Futuro da Governança da Internet, que aconteceria nos dias 23 e 24 de abril de 2014 em São Paulo. O principal foco do evento foi a elaboração de princípios de governança da Internet e a proposta de um roteiro para a

evolução futura desse ecossistema, que era alvo de diversas críticas devido ao grande poder de influência dos Estados Unidos à época.

No ano seguinte, em dezembro de 2014, após a realização do evento NETMundial em Abril de 2014, a Assembleia Geral, reunida mais uma vez, adotou a Resolução 69/166 [*The right to privacy in the digital age*] que fez referência ao evento e adicionou ao documento de 2013 outras recomendações, como por exemplo o reconhecimento da necessidade de se discutir e analisar, com base na legislação internacional de direitos humanos, questões relacionadas com a promoção e proteção do direito à privacidade na era digital, salvaguardas processuais e a proporcionalidade em relação às práticas de vigilância ao redor do globo. Adicionando entendimentos, por exemplo, a respeito dos riscos relacionados à coleta metadados: *"Noting that while metadata can provide benefits, certain types of metadata, when aggregated, can reveal personal information and can give an insight into an individual's behaviour, social relationships, private preferences and identity."* (ONU, 2014)

Também foi acrescentado à chamada aos Estados de 2013 um dispositivo que determina a provisão de remédios que possibilitem reparações em casos de violação à privacidade de indivíduos ou condutas de vigilância arbitrária: "*(e) To provide individuals whose right to privacy has been violated by unlawful or arbitrary surveillance with access to an effective remedy, consistent with international human rights obligation.*" (ONU, 2014)

## 3. O futuro da vigilância importada

### 3.1. O Brasil escancara as suas portas

Apesar dos esforços dos governos anteriores por meio, por exemplo, da constante renovação dos benefícios trazidos pela Lei da Informática, como anteriormente mencionado, em junho de 2019, o presidente Jair Bolsonaro afirmou considerar uma possível redução de impostos sobre importação de produtos de tecnologia, objetivando a diminuição dos tributos de 16% para 4%, com o intuito de "fomentar a competitividade e a inovação". Além de especialistas, como o professor José Luis Oreiro, do departamento de Economia da Universidade de Brasília (UNB), alertarem para o provável impacto negativo da medida para a indústria nacional, a Associação Brasileira da Indústria Elétrica e Eletrônica (Abinee) observa ainda que a medida gera "insegurança jurídica para o setor" e "prejudica os investimentos no país". Para a Abinee a indústria de informação e comunicação deve ser protegida uma vez que é "imprescindível e estratégica para o Brasil diante da economia digital." (FOLHA DE SÃO PAULO, 2019).

Além da referida medida, observa-se uma maior aproximação do Estado brasileiro em relação a países fornecedores de tecnologia militar, como é o caso de Israel. Em março de 2019, após a visita presidencial ao país, o Ministério das Relações Exteriores divulgou uma Declaração Conjunta entre os Estados, um instrumento bilateral de cooperação em diversos campos, dentre eles os campos da ciência e tecnologia, defesa, segurança pública e segurança cibernética (BRASIL, 2019). Por meio da nota, também é publicizado o lançamento da primeira edição do programa "Scaleup in Brazil"[2] que busca promover e facilitar a instalação de startups israelenses em território brasileiro. Dentre as candidatas selecionadas para o projeto estão empresas, muitas vezes fundadas por veteranos das forças de segurança israelense, especializadas em reconhecimento facial, localização *indoor*, análise preditiva, multibiometria, pesquisa comportamental, comunicação de dados, cibersegurança, genealogia, entre outros.

### 3.2. Parte do mundo fecha as suas portas

Uma vez que o segredo norte-americano foi revelado, a fragilidade dos países espionados também foi publicizada. A falta de conhecimento a respeito da coleta de dados sigilosos representou a violação do conceito de soberania, um conceito sócio-jurídico-político para muitos. Assim, a intervenção clandestina de um Estado em outro poderia contribuir para a desestabilização e violação da autonomia estatal uma vez que, no caso de espionagem, informações fundamentais podem ser obtidas e empregadas de maneira pelo Estado invasor, de modo a reduzir a capacidade de ação e reação do Estado alvo da invasão.

Assim, além da aprovação da Resolução no escritório das Nações Unidas, em 2013, o Parlamento Europeu votou a favor de um "inquérito aprofundado" acerca das revelações do Caso Snowden, em particular, sobre o esquema de vigilância da Internet organizado por meio do sistema PRISM. De acordo com uma declaração oficial publicada no site do Parlamento Europeu, os deputados expressaram uma séria preocupação com o funcionamento do programa de vigilância norte-americano mas também manifestaram um certo receio em relação a alegações de que programas de vigilância semelhantes estavam sendo implementados por estados-membros da União Europeia, como era o caso do Reino Unido, Suécia, Holanda e Alemanha.

Em prol da cibersoberania, diversos países desenvolveram legislações apelidadas de *data localization laws* ou *data residency laws*, isto é, um mecanismo que obrigaria o armazenamento de dados em servidores localizados em território nacional. Casos recentes como as supostas acusações de

2 Mais detalhes em: https://www.scaleupinbrazil.com/

espionagem internacional que envolvem a empresa chinesa Huawei contribuem para o aumento do "nacionalismo de dados" e da desconfiança internacional. Assim, com o objetivo de dificultar o acesso aos dados nacionais armazenados em servidores de empresas estrangeiras, países buscaram desenvolver uma regulação acerca do local de guarda dos dados dos seus cidadãos. Entretanto, sabe-se hoje os riscos da adoção de tal prática são elevados. Países com vieses autoritários que adotam essa prática, como é o exemplo da Rússia e da Turquia, já aplicam um maior controle estatal sobre os servidores e por consequência na internet nacional, o que possibilita uma vigilância estatal mais efetiva assim como o combate e perseguição a dissidentes (Chander & Le, 2015). Muitos, como o CEO (diretor) do Google Eric Schimidt, acreditam que o Caso Snowden seria o estopim da 'balcanização' da internet, já que o que era para ser uma ferramenta universal está sob ameaça de se tornar algo fragmentado e específico de cada país.

### 3.3. Proteção à privacidade e o regulamento brasileiro

Em relação ao fornecimento de dados de nacionais a empresas estrangerias de modo a possibilitar o uso de ferramentas de vigilância pelo Estado brasileiro para fins de segurança pública, é importante lembrar que a recém-aprovada Lei Geral de Proteção de Dados (LGPD) não se aplica à coleta e ao processamento de dados para fins de segurança pública, uma vez que o artigo 4º, III, § 1º, LGPD determina que "*será regido por legislação específica, que deverá providenciar medidas proporcionais e estritamente necessárias a fim de servir ao interesse público*" (BRASIL, 2018), porém, a lei específica não existe até o momento.

De acordo com o advogado Rafael Zanatta, a batalha cívica no Brasil no momento atual será a definição coletiva do que são "medidas proporcionais" e o que é "interesse público". A proposta de alguns pesquisadores e ativistas é a proteção trazida pelos princípios constitucionais gerais, tais como a presunção de inocência, e os princípios gerais da própria LGPD, que lutam contra o uso abusivo da coleta de dados. No entanto, acredita-se que um tremendo esforço interpretativo será necessário para consolidar uma jurisprudência onde esses princípios sejam aplicados em caso de vigilância do Estado. Ainda assim, outras normas presentes no ordenamento jurídico pátrio visam proteger a privacidade do cidadão brasileiro frente a vigilância estrangeira como é o caso do Marco Civil da Internet.

Graças à divulgação dos documentos que denunciavam o alto nível de espionagem internacional executada pelo governo norte-americano, a presidenta Dilma Rousseff transformou a pauta da segurança das comunicações brasileiras em prioridade, organizando o Encontro Multissetorial Global

sobre o Futuro da Governança da Internet (NETMundial) em São Paulo. Durante o evento, o Marco Civil da Internet foi sancionado, tornando-se não só a Constituição Digital brasileira mas ganhando também grande visibilidade e status de referência por diversos países. O diploma legal dispõe em seu art. 7º e 8º a respeito da proteção à privacidade dos usuários da Internet:

Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:

I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;

II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;

[...]

Art. 8º A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet.

Parágrafo único. São nulas de pleno direito as cláusulas contratuais que violem o disposto no caput**,** tais como aquelas que:

I - impliquem ofensa à inviolabilidade e ao sigilo das comunicações privadas, pela internet; ou

II - em contrato de adesão, não ofereçam como alternativa ao contratante a adoção do foro brasileiro para solução de controvérsias decorrentes de serviços prestados no Brasil.

### 3.4. Ethics is the new oil

Nos últimos anos, diante de tantos escândalos envolvendo vazamento de dados e usos abusivos de tecnologias que ameaçam não só democracias mas direitos humanos ao redor do globo, uma nova narrativa vem sendo construída em especial pelas gigantes da tecnologia, também conhecidas como GAFAM (Google, Amazon, Facebook, Apple e Microsoft): A narrativa ética.

Um dos exemplos mais claros – e práticos – dessa narrativa foi o impedimento da comercialização de produtos por parte da Google devido ao alto número de falsos positivos identificados. Já a Microsoft, de Bradford L. Smith, afirma que decidiu não vender a sua tecnologia de vigilância para um determinado departamento de polícia que pretendia usá-la de forma indiscriminada. Entretanto, apesar de defender a criação de princípios éticos para o uso de reconhecimento facial para fins de

monitoração, a Microsoft continua trabalhando junto ao setor militar em diversos países ao redor do globo.

O lançamento de princípios éticos por parte de empresas como a Microsoft e o Google vem chamando a atenção de diversas ONGs assim como grupos e instituições formados pela sociedade civil organizada. Ambos demonstram preocupações e chamam a atenção em relação à apropriação de uma narrativa "ética" por determinadas empresas que visa o afastamento de regulações estatais mais incisivas e duras. No caso da Google, a formação de um controverso Comitê de Ética para assuntos de inteligência artificial foi um dos assuntos mais comentados no primeiro semestre de 2019. O comitê, que possuía na sua composição alguns membros com visões extremamente conservadoras, recebeu duras críticas e devido a sua grande repercussão negativa foi dissolvido pela empresa em menos de uma semana.

Além das "narrativas éticas", algumas gigantes optam por seguir uma abordagem mais retórica, que, para muitos, beira o cinismo. Oferecendo os serviços do seu software de reconhecimento facial, *Rekognition,* para o *Immigration and Customs Enforcement* (ICE), o controverso departamento de controle de imigração norte-americano, recentemente, a Amazon foi alvo de uma série de críticas. Em um comunicado oficial, a empresa disse que oferece diretrizes claras sobre o uso do *Rekognition* para segurança pública – incluindo uma recomendação de que as agências de segurança pública revisem as possíveis combinações faciais sugeridas pelo sistema. A empresa também afirma que seus clientes usaram o *Rekognition* para fins benéficos, incluindo a identificação de mais de 3.000 vítimas de tráfico humano. Da mesma forma, a Huawei, ao ser questionada[3] em audiência pública pela Casa dos Comuns do Reino Unido a respeito do uso da sua tecnologia para fins de perseguição política da minoria muçulmana Uighurs na província de Xinjiang, busca estabelecer que os seus princípios estão em consonância com a regulação local de cada país, não cabendo à empresa qualquer juízo de valor acerca do uso da sua tecnologia por governos ao redor do globo (HOUSE OF COMMONS, 2019).

3 Em um trecho da transcrição disponibilizada pela *House of Commons* do Reino Unido, quando perguntado a respeito de um possível uso da tecnologia desenvolvida pela empresa Huawei para fins que vão na contramão de direitos humanos como a perseguição da minoria muçulmana Uighurs na província de Xinjiang na China, John Suffolk, *Global Cyber Security and Privacy Officer* da Huawei responde: "Eu diria que, em essência, entendemos a lei. É o papel do governo definir a lei, seja no Oriente ou no Ocidente, e é nosso trabalho como fornecedor trabalhar dentro dessa lei. Não importa para nós qual é o nome do país; mas sim, se é legal."(tradução livre). Em seguida, ao ser questionado a respeito da diferenciação entre lei e ética, Suffolk rebate: "Nosso ponto de partida é sempre, em essência, que a lei define a ética uma vez que os governos devem definir o que é certo e errado, assim como o Reino Unido define o que é certo e errado ou o que ele irá ou não permitir. Isso está consagrado na lei. Esse é o nosso ponto de partida." (tradução livre). Documento disponível na íntegra em: <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/uk-telecommunications-infrastructure/oral/102931.pdf>

**Conclusão**

A reintrodução no cenário da geopolítica dos debates acerca da espionagem internacional por meio das polêmicas geradas pelo caso Snowden e, mais recentemente, pelas acusações enfrentadas pela Huawei, representa uma alteração de paradigmas no sistema internacional que vem acontecendo desde o atentado do 11 de setembro de 2001 às Torres Gêmeas. A securitização do 'terrorismo' por parte do governo norte-americano, por exemplo traz consigo, por meio de uma narrativa que procura oferecer uma justificativa ao combate a um inimigo "sem face", um mecanismo de vigilância global em que estratégias verdadeiramente necessárias à segurança nacional são confundidas, ou, até mesmo substituídas, por planos que visam o reestabelecimento de um certo controle do Norte sobre o Sul Global, além de vantagens de cunho econômico que ameaçam a soberania dos países vigiados.

Em relação ao assunto tratado neste trabalho, da utilização de tecnologias de vigilância estrangeiras em território brasileiro, é possível perceber no cenário nacional, mesmo com a existente deficiência da produção local de tecnologias de ponta, um aumento exponencial da adoção de mecanismos de controle social e da informação. Isso se dá em grande parte ao atual *lobbying* da indústria da securitização e militarização, o que resulta, muitas vezes, no domínio por Estados economicamente e militarmente mais avantajados que, às custas dos países periféricos e por meio da sua superioridade econômica, controla infraestruturas, monitorando e vigiando a todos.

**Referências**

AGÊNCIA DATA LABE. (2019). **Scanner facial abre alas e ninguém mais se perde no Carnaval (e fora dele)** https://tab.uol.com.br/noticias/redacao/2019/03/11/carnaval-abre-alas-para-o-escaner-facial-reconhece-milhoes-e-prende-seis.htm

ASSEMBLEIA GERAL DA ONU. (2013) **Resolution adopted by the General Assembly on 18 December 2013. The right to privacy in the digital age**. https://undocs.org/A/RES/68/167

_____. (2014) **Resolution adopted by the General Assembly on 18 December 2014 – 69/166. The right to privacy in the digital age**. https://undocs.org/en/A/RES/69/166

BLOOMBERG. (2019) **Surveillance Startup Wins Microsoft Backing as a 'Tool for Good'** https://www.bloomberg.com/news/articles/2019-06-18/surveillance-startup-wins-microsoft-backing-as-a-tool-for-good

BRASIL. (2013) Portaria nº 112, de 8 de maio de 2013. **Institui O Sistema Integrado de Comando e Controle de Segurança Pública Para Grandes Eventos - SICC**. Brasília, DF, 2013.

_____. (2014) Lei no. 12.965, de 23 de abril de 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil**. Brasília, DF, 2014.

_____. (2018) Lei no. 13.709, de 14 de agosto de 2018. **Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014**. Brasília, DF, 2018.

_____. (2019) Nota 81: **Declaração Conjunta por ocasião da Visita Oficial a Israel de Sua Excelência o Presidente da República Federativa do Brasil, Jair Bolsonaro**, 31 de março de 2019.

Brasília, DF, 2019. http://www.itamaraty.gov.br/pt-BR/notas-a-imprensa/20235-visita-oficial-a-israel-de-sua-excelencia-o-presidente-da-republica-federativa-do-brasil-jair-bolsonaro

BUZAN, B e HANSEN, L. (2009). **The Evolution of International Security Studies**. Cambridge, Reino Unido: Cambridge University Press

CARVALHO, M. A. R. (2019) **Militarização no Brasil: a perpetuação da guerra ao inimigo interno**. http://www.ihu.unisinos.br/159-noticias/entrevistas/586763-militarizacao-no-brasil-a-perpetuacao-da-guerra-ao-inimigo-interno-entrevista-especial-com-maria-alice-rezende-de-carvalho

CHANDER, A. & LE, U.P. (2015) **Data Nationalism**. Emory Law Journal, Vol. 64, No. 3, 2015

FOLHA DE SÃO PAULO. (2014) **Brasil reforça segurança da Copa com drone israelense de R$ 18 milhões.** https://www1.folha.uol.com.br/esporte/folhanacopa/2014/03/1432291-brasil-reforca-seguranca-da-copa-com-drone-israelense-de-r-18-milhoes.shtml

_____. (2019) **Governo estuda reduzir impostos para produtos de tecnologia, diz Bolsonaro** https://www1.folha.uol.com.br/mercado/2019/06/governo-estudar-reduzir-impostos-para-produtos-de-tecnologia-diz-bolsonaro.shtml

GRAHAM, S. (2016) **Cidades sitiadas: o novo urbanismo militar**. São Paulo, SP: Boitempo Editorial

GREENWALD, G. (2014) **Sem lugar para se esconder**. Rio de Janeiro, RJ: Editora Primeira Pessoa

HOUSE OF COMMONS. (2019) **Science and Technology Committee: Oral evidence: UK telecommunications infrastructure**, *HC 2200*. 10 June 2019 *http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/uk-telecommunications-infrastructure/oral/102931.pdf*

RODRIGUES, T. (2017) **Rio de Janeiro sitiada?** *https://diplomatique.org.br/rio-de-janeiro-sitiada/*

SECRETARIA DA SEGURANÇA PÚBLICA - RS. (2019) **SSP finaliza ajustes para utilização de reconhecimento facial durante a Copa América.** https://ssp.rs.gov.br/ssp-finaliza-ajustes-para-utilizacao-de-reconhecimento-facial-durante-a-copa-america

SIRIUS, R. U. (2013) **Cypherpunk rising: WikiLeaks, encryption, and the coming surveillance dystopia.** https://www.theverge.com/2013/3/7/4036040/cypherpunks-julian-assange-wikileaks-encryption-surveillance-dystopia

SOUZA, M. (2008) **Fobópole**. Rio de Janeiro, RJ: Bertrand Brasil

_____. (2015) **Dos espaços de conrole territorios dissidentes**. Rio de Janeiro, RJ: Consequência Editora

VINCENTE, J.P. (2016) **Como as Olimpíadas ajudaram o Brasil a aumentar seu aparato de vigilância social** https://www.vice.com/pt_br/article/3dp8wy/como-o-brasil-aprimorou-seu-aparato-de-vigilancia-social-para-as-olimpiadas