DOI: 10.5212/PublicatioCi.Soc.v.28.2020.14435

VIGILÂNCIA DIGITAL COMO INSTRUMENTO DE PROMOÇÃO DA SEGURANÇA PÚBLICA

DIGITAL SURVEILLANCE AS A PUBLIC SECURITY PROMOTION INSTRUMENT

Camila Berlim Schneider*
Pedro Fauth Manhães Miranda**

RESUMO

Em um misto de sensacionalismo midiático e realidade factual, especialmente se tomados os números acerca das minorias, surge o consenso de que os tempos atuais são de insegurança e violência. Diante disso, torna-se necessária a busca por alternativas que transformem a hodierna realidade social. Em uma sociedade totalmente informatizada, marcada pelo estabelecimento de novas tecnologias, as formas de controle social também passam a ser digitais. Assim, através de uma pesquisa exploratória, concretizada via revisão bibliográfica com método dedutivo, o presente trabalho objetiva demonstrar como os novos mecanismos digitais de vigilância estão sendo aplicados às políticas governamentais de segurança pública. Neste contexto, faz-se oportuno refletir sobre a necessidade de uma utilização mais transparente e prudente destes instrumentos, a fim de viabilizar um maior sentimento de segurança na sociedade, evitando estigmatizações e violações de direitos fundamentais.

Palavras-chave: insegurança; violência; novas tecnologias; políticas governamentais.

ABSTRACT

In a mix of media sensationalism and factual reality, especially if one takes numbers about minorities, a consensus emerges that the present times are one of insecurity and violence. Given this, it is necessary to search for alternatives that transform the current social reality. In a fully computerized society, marked by the establishment of new technologies, the forms of social control also become digital. Thus, through an exploratory research, accomplished through bibliographical review with deductive method, the present work aims to demonstrate how the new digital surveillance mechanisms are being applied to government public security policies. In this context, it is appropriate to reflect on the need for a more transparent and prudent use of these instruments, in order to enable a greater sense of security in society, avoiding stigmatizations and violations of fundamental rights.

Keywords: insecurity; violence; new technologies; government policies.

* Mestre em Engenharia e Ciência dos Materiais pela Universidade Federal do Paraná.
** Doutorando em Direito pela Pontifícia Universidade Católica do Paraná.

INTRODUÇÃO

O Brasil e o mundo vivem tempos de violência e medo, constituindo uma realidade cuja insegurança é ainda mais insuflada pelo sensacionalismo midiático. Os altos índices de crimes constituem evidente problema público, especialmente se consideradas as minorias, e, apesar dos discursos dos governantes, a questão nunca foi enfrentada de forma consistente.

Trata-se de um problema histórico e de difícil solução. De forma paliativa, a população acaba adotando medidas que englobam a construção de muros altos, cercas eletrônicas e circuitos integrados de câmeras, tornando-se ela própria prisioneira e cada vez mais longe de um saudável convívio social. As instituições responsáveis pela manutenção da ordem persistem na abordagem punitiva, atingindo preferencialmente aqueles que não possuem meios de defesa (por não serem capazes de arcar com os "custos do medo") e que já foram desguarnecidos de seus direitos, inclusive do direito a tê-los.

Com o avanço tecnológico, surgem algumas alternativas. O advento da internet, como fonte primordial de informação, possibilita o controle de populações inteiras. É verdade que, por meio dos bancos de dados e sistemas de reconhecimento facial, rompemos barreiras de tempo e espaço. A vigilância digital ganha forma, tornando-se a "última novidade" em termos de políticas de segurança pública, implementada tanto nas praças chinesas, como no carnaval carioca.

Mas persistem algumas dúvidas: Até que ponto estas medidas são efetivas no combate à violência? Elas são enviesadas por nossas tendências preconceituosas, ou sua suposta imparcialidade limita tais reflexos indesejáveis? Sem anseio algum de trazer soluções definitivas, e por meio de uma pesquisa exploratória, com revisão bibliográfica e método dedutivo, o presente trabalho constitui uma reflexão sobre a questão da insegurança e a viabilidade dos mecanismos adotados pelo Estado.

Para isto, o texto compõe-se de três seções. A primeira relaciona o conceito de segurança com a caracterização daqueles que são considerados "perigosos", a partir dos ensinamentos de alguns pesquisadores. Na sequência, são expostos os novos modelos de vigilância digital e a sua principal motivação: a segurança. A última seção aborda a implementação destas tecnologias no carnaval do Rio de Janeiro, expondo os aspectos que ainda precisam ser trabalhados e repensados.

(IN)SEGURANÇA BRASILEIRA E A "CLASSE PERIGOSA"

Há algum tempo, Bauman (2009, p.2) já afirmava: "A insegurança e a ideia de que o perigo está em toda parte são inerentes a essa sociedade". É cediço que o Brasil nunca foi uma sociedade imune à violência, mas a percepção negativa da população quanto à segurança aumentou significativamente nos últimos anos. Segundo a pesquisa de opinião "2018 *Global Law and Order*" do Instituto Gallup[1], em 2015 o Brasil sequer aparecia na lista dos dez países com a pior sensação de segurança. Em 2016, apareceu como o sétimo pior. E em 2017, muito mais próximo do cenário atual, já figurava entre os quatro países com maior sensação de insegurança.

As justificativas para estes índices elevados são inúmeras, mas algumas merecem destaque. Castel (2005, p.6) afirma que a insegurança na sociedade moderna "não seria a falta de proteção, mas antes seu inverso, sua sombra projetada num universo social que se organizou em torno de uma busca sem fim de proteções, ou de uma busca tresloucada de segurança". Já para Bauman (2009, p.2)

[1] O Instituto Gallup apresenta relatórios sobre o sentimento da população com relação à segurança pessoal, bem como suas experiências com o crime e a aplicação da lei. Mais informações podem ser encontradas em relatório publicado pela própria instituição (GALLUP, 2018).

"(...) a insegurança moderna, em suas várias manifestações, é caracterizada pelo medo dos crimes e dos criminosos".

Relacionando ambas as suposições, verificamos a concretização deste excesso de proteção da sociedade, distanciando-a cada vez mais desta suposta "classe perigosa". Destarte, objeto de diversos estudos é exatamente esta "classe perigosa", seja para buscar compreendê-la ou mesmo afastar-se dela, recebendo inúmeras e indesejáveis caracterizações ao longo da história. Não é importante, para os propósitos deste artigo, diferenciá-las, mas antes reconhecer a ocorrência da identificação de indivíduos socialmente dissonantes.

No século XIX, por exemplo, Cesare Lombroso (2010), amparado pela sua "Teoria do Criminoso Nato", sustentava que o criminoso possuía características natas e imutáveis que o identificariam como tal (nariz adunco, caninos bem desenvolvidos, cabelos e olhos escuros etc.). Tendo isto em vista, o indivíduo deveria ser afastado da sociedade, mesmo antes do cometimento de qualquer delito, como forma de defesa social. Esta teoria vigorou por muito tempo, mas foi amplamente rebatida e acabou caindo em desuso, por ser considerada tendenciosa – para não mencionar preconceituosa. Não obstante, poder-se-ia argumentar que ela parece ainda ser aplicada no Brasil, haja vista permanecermos em um país estruturalmente racista, que prejulga com base na cor da pele.

Identificando os preconceitos embutidos nestas análises, os sociólogos passaram a examinar como, na verdade, as razões de segregação não são biológicas, mas sociais. Becker (2008) segue a classificação dos sujeitos desviantes, assim caracterizados por não respeitarem as normas sociais e as regras determinadas por uma coletividade, mesmo porque dela não fazem parte ativamente. Neste sentido, segundo Coimbra (2001, p.163), a classe de criminosos é caracterizada, preferencialmente, por "homem pobre, preto ou pardo, entre 18 e 24 anos, morados de periferia, que não chegou a terminar o primário e é morto em logradouro público". Entretanto, seja qual for a definição adotada, é patente que esta discussão guarda uma relação direta com a criminalidade e a pobreza.

Para Bauman (2009, p.15), a diferenciação entre a classe dos que não conseguem se adaptar à sociedade capitalista (a exemplo dos desempregados) e daqueles rotulados como criminosos é tênue:

> Hoje, apenas uma linha sutil separa os desempregados, especialmente os crônicos, do precipício, do buraco negro da *underclass* (subclasse): gente que não se soma a qualquer categoria social legítima, indivíduos que ficaram fora das classes, que não desempenham alguma das funções reconhecidas, aprovadas, úteis, ou melhor, indispensáveis, em geral realizadas pelos membros "normais" da sociedade; gente que não contribui para a vida social. [...] Assim como aqueles que são excluídos do trabalho, os criminosos (ou seja, os que estão destinados à prisão, já estão presos, vigiados pela polícia ou simplesmente fichados) deixaram de ser vistos como excluídos provisoriamente da normalidade da vida social. Não são mais encarados como pessoas que seriam "reeducadas", "reabilitadas" e "restituídas à comunidade" na primeira ocasião, mas veem-se definitivamente afastadas para as margens, inaptas para serem "socialmente recicladas": indivíduos que precisam ser impedidos de criar problemas e mantidos a distância da comunidade respeitosa das leis.

O perfil do encarcerado brasileiro é sintomático da evidente segregação social. Um levantamento realizado pelo Infopen (2019, p. 33), compilado de informações estatísticas do sistema penitenciário brasileiro, mostra que, em São Paulo, 56,42% da população prisional é composta por pessoas negras e pardas. No Rio de Janeiro a taxa é ainda maior, representando 73,26% da população encarcerada. Ainda, consoante esta mesma verificação (INFOPEN, 2019, p. 21), observa-se que o Brasil conta com 1.507 unidades prisionais ativas, perfazendo um total de 423.242 vagas, para uma população carcerária de, aproximadamente, 726 mil pessoas.

Em face do exposto, o medo passa a ser revelado através de mecanismos de defesa, como carros blindados, trancas para automóveis e residências, construção de condomínios fechados distantes do centro e vigilância crescente nos locais públicos.

> Os medos contemporâneos, os medos urbanos típicos, ao contrário daqueles que outrora levaram à construção de cidades, concentram-se no "inimigo interior". [...] Os muros construídos outrora em volta da cidade cruzam agora a própria cidade em inúmeras direções. Bairros vigiados, espaços públicos com proteção cerrada e admissão controlada, guardas bem armados no portão dos condomínios e portas operadas eletronicamente — tudo isso para afastar concidadãos indesejados, não exércitos estrangeiros, salteadores de estrada, saqueadores ou outros perigos desconhecidos emboscados extramuros. (BAUMAN, 1999, p.46)

Discorrendo sobre o cenário paulistano, já no final da década de 90, Caldeira (1997, p. 159) atestava:

> São Paulo é hoje uma cidade de muros. Ergueram-se barreiras por toda parte — em volta das casas, prédios de apartamentos, parques, praças, complexos de escritórios e escolas. [...] Uma nova estética de segurança modela todos os tipos de construção, impõe sua lógica de vigilância e distância como forma de status e muda o caráter da vida e das interações públicas.

Outrossim, é inegável o papel sensacionalizante da mídia na promoção do medo e da insegurança. Em seu livro intitulado *Medo Líquido*, Bauman (2008, p.188) demonstra esta relação viciosa, ao destacar uma reflexão do professor e sociólogo Loïc Wacquant:

> Loïc Wacquant sugeriu recentemente que "o carrossel da segurança é para a criminalidade o que a pornografia representa para as relações amorosas", pois ignora totalmente as causas e o significado de seus aparentes objetos e reduz seu tratamento a assumir "posições" escolhidas unicamente em virtude de serem espetaculares - e porque é exposto ao público não no seu próprio interesse, mas em benefício da publicidade. A exposição pública condensa a atenção sobre "mendigos reincidentes na impertinência, refugiados em deslocamento, imigrantes a serem expulsos, prostitutas nas calçadas e outros tipos de dejetos sociais que povoam as ruas das metrópoles para o desgosto das 'pessoas decentes'. Por esse motivo, a batalha contra o crime é apresentada como um 'excitante espetáculo midiático-burocrático'".

Tais veículos influenciam e estimulam uma política de repressão, punição e intervenção. O rigor das leis, impulsionando o encarceramento em massa, não torna efetivo o combate ao crime. Conquanto, o aparato punitivo, combinado às estratégias de vigilância, torna-se uma "poderosa e perigosa" ferramenta de controle social.

Assim declara Miranda (2011, p.5) quando explica:

> Vivemos, hoje, num contexto onde o medo de ser vitimado e o isolamento social, favorecido por este medo, têm transformado todo o cotidiano da vida social e também a interação entre as pessoas. As tecnologias usadas para a vigilância e, consequentemente, para o controle do crime e da violência, bem como as estratégias repressivas que se propõem, na retórica, a incidir efetivamente sobre tais ações indesejáveis transformam, custosamente, a qualidade de vida dos indivíduos. Trata-se de uma questão política que busca, de forma rápida e paliativa, responder às demandas da população. A inovação tecnológica, por outro lado, não será adequadamente destinada às pessoas que temem o crime e a violência, a menos que sejam acompanhadas de mudanças culturais e sociais.

Fato é que o Estado, para executar o controle social, adota uma política de segurança pública segregacionista e preconceituosa. Escolhe-se quem deve ser reprimido e quem deve ser protegido, considerando, na maioria dos casos, critérios raciais, de carência social e vulnerabilidade. Tomando como referência a "Teoria da Criminologia Crítica" de Alessandro Baratta, fica clara a politização da criminalidade:

> O direito penal tende a privilegiar os interesses das classes dominantes, e a imunizar do processo de criminalização comportamentos socialmente danosos típicos dos indivíduos pertencentes, e ligados funcionalmente à existência da acumulação capitalista, e tende a dirigir o processo de criminalização, principalmente, para formas de desvio típicas subalternas. (BARATTA, 2002, p.165)

Na sociedade do consumo e da informação, aqueles que vivem às margens parecem deslocados do restante da população. Com uma estratégia pautada na vigilância onipresente e onisciente, na punição e na exclusão, o controle é exercido sobre a classe dos "indesejados", resultando na criminalização da pobreza.

VIGILÂNCIA DIGITAL APLICADA À SEGURANÇA PÚBLICA

Segundo Bauman (2009), hodiernamente vivemos em uma sociedade caracterizada pela mixofobia (medo de misturar-se com o diferente). No mundo globalizado convivemos com pluralidades de culturas, raças e estilos de vida. Mas estes relacionamentos são ambivalentes, uma vez que podem atrair ou afastar indivíduos. Bauman (2009, p.17-29) assevera:

> Uma vez que a multiforme e plurilinguística cultura do ambiente urbano na era da globalização se impõe - e, ao que tudo indica, tende a aumentar -, as tensões derivadas da "estrangeiridade" incômoda e desorientadora desse cenário acabarão, provavelmente, por favorecer as tendências segregacionistas. [...] A uniformidade do espaço social, sublinhada e acentuada pelo isolamento espacial dos moradores, diminui a tolerância à diferença; e multiplica, assim, as ocasiões de reação mixofóbica, fazendo a vida na cidade parecer mais "propensa ao perigo" e, portanto, mais angustiante, em vez de mostrá-la mais segura e, portanto, mais fácil e divertida.

Insta destacar que, desde o atentado de 11 de setembro de 2001, nos Estados Unidos, elevou-se a tensão já existente entre os nativos e os estrangeiros. Por esta razão, ao longo do tempo foram desenvolvidos sistemas de vigilância capazes de identificar uma categoria de pessoas malquistas ao convívio social em determinados territórios.[2] Para Ball e Webster (2003, p.1) a vigilância "envolve a observação, a gravação e a categorização de informações sobre pessoas, processos e instituições" [3] (tradução dos autores).

Oscar Gandy explica que as empresas e o Estado são os responsáveis pela condução desta vigilância contínua: "O gênero do panóptico é uma tecnologia que foi desenhada e está em contínua revisão para servir aos interesses de quem toma decisões dentro do governo e nas burocracias empresariais"[4] (tradução dos autores) (GANDY, 1993, p.95). E, nesta revisão, surgem modos atualizados de vigilância, a nos cercar e, cada vez mais, preencher os espaços vazios e mitigar a liberdade humana.

O MODELO BANÓPTICO

À vista da expressiva sensação de insegurança gerada nos Estados Unidos, pós 11 de setembro, o professor francês Didier Bigo (2006) formulou um modelo de vigilância digital aplicável às questões

[2] Os Estados Unidos estão utilizando sistemas de reconhecimento facial para controlar a entrada e saída das pessoas do país. Segundo eles, o principal objetivo é identificar aqueles que estão em situação irregular. Chamado de Biometric Exit, o sistema recolhe a imagem do usuário antes do embarque e "cruza" os dados com o visto e o passaporte do Departamento de Segurança Interna dos Estados Unidos. Na existência de qualquer irregularidade, a pessoa é retirada do voo antes da decolagem, podendo ser proibida de entrar no país por um determinado período. Mais informações podem ser encontradas nos sites estadunidenses do *Department of Homeland Security* e da *U.S Customs and Border Protection*.

[3] "Surveillance involves the observation, recording and categorization of information about people, processes and institutions".

[4] "The panoptic sort is a technology that has been designed and is being continually revised to serve the interests of decision makers within the government and the corporate bureaucracies".

de fronteiras e imigrações. Tal modelo, denominado banóptico, é a atualização digitalizada e ampliada do conceito foucaultiano. Fundando-se em um conjunto de dados biométricos e técnicas digitais de reconhecimento facial, o banóptico é capaz de realizar o controle social por intermédio da identificação preventiva de indivíduos, banindo-os posteriormente. Conforme ensina Bigo (2006, p.63):

> A vigilância e o monitoramento do movimento de cada indivíduo estão crescendo, mas controles efetivos e restrições coercitivas da liberdade estão concentrados em alvos específicos. Esses alvos são construídos como "inimigos invisíveis e poderosos em redes" e as narrativas relativas a essas ameaças são anteriores a 11 de setembro e até mesmo ao fim da bipolaridade. No entanto, o 11 de setembro reforçou a ideia de que a luta contra essas ameaças justifica o perfil do comportamento potencial de certas pessoas, especialmente se elas estão "em movimento". A reação política ao 11 de setembro justifica uma estratégia proativa e preventiva, que tem a ambição de conhecer e monitorar o "futuro".[5] (tradução dos autores)

Em termos mais simples, o que Bigo propõe é um modelo que demonstra o modo pelo qual as tecnologias de elaboração de perfis são utilizadas para determinar quem será alvo desta vigilância específica.

Bauman (2014, p.46) destaca três características fundamentais do modelo banóptico:

> A função estratégica do diagrama banóptico é traçar o perfil de minorias "indesejadas". Suas três características são o poder excepcional em sociedade liberais (estados de emergência que se tornam rotineiros), traçar perfis (excluir certos grupos, categorias de pessoas excluídas de forma proativa em função de seu potencial comportamento futuro) e normalizar grupos não excluídos (segundo a crença no livre movimento de bens, capital, informações e pessoas).

A sociedade da informação concebe vigilâncias que dispensam barreiras físicas. O panóptico, idealizado por Michel Foucault (1999) e elaborado para estruturas físicas, é atualizado para mecanismos de vigilância virtuais e livres de paredes, torres ou guardas. Em vista disso, para Fuchs (2011) a relação saber/poder é substituída por uma relação de dados digitais/poder. Ademais, segundo ele:

> Devido à disponibilidade das redes digitais, a vigilância opera com ajuda de redes globais descentralizadas e que podem, em princípio, ser exercidas por muitos atores com acesso a tais redes. Não há um único ponto geográfico de acesso à informação, ela pode ser acessada de qualquer lugar. Da mesma forma, não há uma única base de dados eletrônica para vigilância, mas muitas dispersas que podem ser usadas em conjunto por atores poderosos com o objetivo de realizar pesquisa interligada de dados. [6] **(**tradução dos autores) (FUCHS, 2011, p.120)

Com o pretexto de garantir a segurança pública, instituições estatais governamentais armazenam e analisam dados, organizando e gerenciando populações inteiras. Esta nova estruturação digital trouxe consigo a possibilidade de armazenar uma quantidade inimaginável de dados, o *Big Data*. Em decorrência disso, algoritmos preditivos são desenvolvidos para facilitar o trabalho de órgãos governamentais na prevenção de crimes, por meio de um método denominado aprendizado de máquina[7].

[5] "The surveillance and monitoring of the movement of each individual is growing, but effective controls and coercive restrictions of freedom are concentrated on specific targets. These targets are constructed as 'invisible and powerful enemies in networks' and the narratives concerning these threats predate September 11 and even the end of bipolarity. Nevertheless, September 11 has reinforced the idea that the struggle against these threats justifies the profiling of certain people's potential behaviours, especially if they are 'on the move'. The political reaction to September 11 justifies a proactive and pre-emptive strategy, which has the ambition to know, and to monitor the 'future'".

[6] "Due to the availability of digital networks, surveillance operates with the help of global decentralized networks and can in principle be exerted by many actors who have access to such networks. There is not one single geographical point of access to gathered data, it can be accesses from everywhere. Also there is not one central electronic database for surveillance, but many dispersed ones that can be used in combination by powerful actors in order to conduct interlinked data searches".

[7] *COMPAS* é um exemplo de algoritmo americano utilizado para indicar índices de reincidência criminal. *PredPol*, outro algoritmo americano, prevê onde e quando ocorrerão crimes.

Em suma, este método possibilita a criação de algoritmos capazes de fazer previsões sobre os dados que recebem. É a vigilância digital, por meio do cruzamento de dados, conferindo aplicabilidade a um sistema de segregação e exclusão social. Sem qualquer transparência e com uma neutralidade comprovadamente questionável, estes métodos podem se apresentar tendenciosos, amplificando preconceitos e estereótipos.[8]

O MODELO SINÓPTICO

É apropriado salientar que, na época atual, estamos imersos no mundo das mídias sociais. Este fato marca a transição de uma sociedade preocupada com a invasão de privacidade para outra com nítida evasão de privacidade. Ninguém mais precisa adentrar a vida alheia em busca de informações porque nós, voluntariamente (ou, em alguns casos, até involuntariamente), fornecemos todas elas. Ao criar um perfil em uma determinada rede social, por exemplo, o próprio usuário do sistema fornece seus dados para controle, monitoramento e uso.[9]

Nessa conjuntura, surge o modelo de vigilância cunhado por Thomas Mathiesen (1997), o sinóptico. Diferentemente do panóptico onde poucas pessoas vigiavam muitas, no sinóptico esta relação é invertida.

> Não importa mais se os alvos do sinóptico, que agora deixaram de ser os vigiados e passaram a ser os vigilantes, se movam ou fiquem parados. Onde quer que estejam e onde quer que vão, eles podem ligar-se – e se ligam – na rede extraterritorial que faz muitos vigiarem poucos. (BAUMAN, 1999, p. 50)

Fazendo sua própria leitura do mecanismo, Bauman o chama de "panóptico faça você mesmo". Para este autor, o trabalho de vigiar passa a ser "terceirizado" para o próprio vigiado. Forma-se um híbrido entre observador e observado, muito inerente à sociedade moderna, informatizada e globalizada.

> O que antes era visto como dever dos gerentes, a ser realizado à custa deles e por seu esforço, foi transferido para os objetos do gerenciamento (ou lhes foi "terceirizado", na insinuação de outro neologismo, agora comumente usado para disfarçar ou camuflar o zelo dos gerentes em se livrar das tarefas de controle que consideram enfadonha, inconveniente, difíceis e irritantemente constrangedoras, passando-as para os ombros dos controlados; e, portanto, em representar a passagem do fardo como um dote, uma ato de garantia de direitos de autonomia e autoafirmação, ou mesmo como "habilitação" ou "ressubjetivação" de objetos da ação gerencial antes passivos). (BAUMAN, 2014, p.51)

Mesmo sem saber qual será o uso dado as suas informações, o vigiado contribui, sem coerção alguma, para a formação do banco de dados e para a efetivação da visibilidade em relação aos vigilantes. Em verdade, "quanto mais informações sobre você contenha o banco de dados, mais livremente você poderá se movimentar. O banco de dados é um instrumento de seleção, separação e exclusão" (BAUMAN, 1999, p.49).

A vigilância se concretiza, deste modo, pela união dos mecanismos sinóptico e banóptico, conforme é possível perceber na seguinte afirmação:

> O banóptico guarnece as entradas daquelas partes do mundo dentro das quais a vigilância do tipo "faça você mesmo" é suficiente para manter e reproduzir a "ordem"; basicamente, ele barra a entrada a todos os que não possuem nenhuma das ferramentas adequadas para

[8] Relatórios de organizações como *ProPublica* (2016) e *Human Rights Data Analysis Group* (LUM, 2016) revelaram, respectivamente, disparidades raciais e sociais nos algoritmos *COMPAS* e *PredPol*.

[9] No último ano, a empresa norte-americana Domo disponibilizou a sétima edição da Pesquisa "Data Never Sleeps", ou "os dados nunca dormem". A pesquisa (DOMO, 2019) mostra quantos dados são gerados a cada minuto nas principais redes sociais do mundo.

> isso (como cartão de crédito ou Blackberry); e que, portanto, não podem ser considerados confiáveis no que se refere à prática dessa vigilância por conta própria. Esse indivíduos (mais precisamente, essas categorias de indivíduos) devem ter "ajuda mecânica", por assim dizer, para se alinhar aos padrões comportamentais dos "espaços defensáveis". Outra tarefa dos dispositivos banópticos, e de não menor gravidade, é identificar prontamente indivíduos que deem sinais de não estarem dispostos a se manter na linha ou que planejam quebrar esses padrões obrigatórios. (BAUMAN, 2014, p.47)

O controle social torna-se universal, acompanhando a movimentação do ser humano por meio de dispositivos tecnológicos portados, autonomamente, pela própria população ou instalados, estrategicamente, em espaços frequentados pela "classe perigosa", ou mesmo onde a classe dominante possa se sentir mais protegida.

MULTIDÃO COMO DESORDEM EM POTENCIAL

É por meio da efetuação destas tecnologias de controle e poder que as aglomerações de pessoas se tornam alvos dos sistemas de vigilância. Isso porque, em ambientes públicos, há uma maior mistura de indivíduos e uma aparente "desordem" a ser controlada. Nas palavras de Bauman (2009, p.35-40):

> Podemos dizer que as fontes do perigo atingiram agora o coração da cidade. Os amigos e os inimigos – sobretudo os misteriosos e incompreensíveis estrangeiros que oscilam ameaçadoramente entre esses dois extremos - misturam-se, confundem-se nas ruas da cidade. [...] Um espaço é "público" à medida que permite o acesso de homens e mulheres sem que precisem ser previamente selecionados. Nenhum passe é exigido, e não se registram entradas e saídas. Por isso, a presença num espaço público é anônima, e os que nele se encontram são estranhos uns aos outros, assim como são desconhecidos para os empregados da manutenção. Os espaços públicos são os lugares nos quais os estrangeiros se encontram.

No espaço público, a referida "classe perigosa" se encontra em contato direto com os demais indivíduos, imiscuída a eles, passando (quase) imperceptível. Porém, é exatamente neste espaço público, plural em sua própria essência, que a coexistência democrática, entre os diferentes, ocorre em sua forma mais pura, sem privacidade. É no espaço público, inclusive, que as manifestações populares, a forma mais natural e básica da política acontece, de modo a concretizar, assim, a própria democracia.

> De certa forma eles [os espaços públicos] condensam - e, por assim dizer, encerram - traços distintivos da vida urbana. É nos locais públicos que a vida urbana e tudo aquilo que a distingue das outras formas de convivência humana atingem sua mais completa expressão, com alegrias, dores, esperanças e pressentimentos que lhe são característicos. (BAUMAN, 2009, p.40)

Por outro lado, a paranoia da modernidade líquida, para permanecer nos dizeres de Bauman, nos faz imaginar que estrangeiros, pobres, miseráveis, desconhecidos e, portanto, inimigos em potencial da ordem, quando não homicidas ou terroristas andam, incólumes, ao nosso lado. Mesmo que estejamos sozinhos, acredita-se haver sempre a possibilidade destes inimigos aparecerem, materializarem-se do nada ao nosso lado. É diante desta insegurança constante que surgem as ferramentas banóptico/sinóptico e, assim, uma tecnologia de monitoramento, desenvolvida pela empresa de telefonia Oi, foi testada durante o carnaval de 2019, no Rio de Janeiro. Seu funcionamento se deu do seguinte modo:

> Utilizando de forma integrada as câmeras instaladas em Copacabana, o sistema consiste no envio de informações online para uma central, que ficará instalada no Centro Integrado de Comando e Controle (CICC). As imagens faciais e das placas dos veículos serão analisadas por operadores que utilizarão os bancos de dados da Polícia Civil e do Detran. A gestão operacional do sistema ficará restrita ao Estado, que terá o controle do banco de dados. O suporte da Oi será apenas na tecnologia oferecida. (PMERJ, 2019, s/p)

Para o coronel Rogério Figueredo de Lacerda, secretário da Polícia Militar, "em uma blitz ou mesmo em um bloco de Carnaval, podemos detectar de forma imediata a presença de um criminoso ou de um carro roubado" (PMERJ, 2019, s/p).

Ressalta-se, contudo, que tecnologias semelhantes já foram testadas na Inglaterra. Apresentando um índice de erro de 92% na identificação de criminosos, tiveram sua eficácia contestada (BURGESS, 2018). Nesta lógica, Silkie Carlo, diretor do grupo Big Brother Watch, de forma pertinente, alerta que:

> Esses números mostram que não só é o reconhecimento facial em tempo real uma ameaça para as liberdades civis, é uma ferramenta de policiamento perigosamente imprecisa. [...] As estatísticas mostram que a tecnologia identifica erroneamente membros inocentes do público a uma taxa assustadora, enquanto há apenas um punhado de ocasiões em que apoiou um propósito de policiamento genuíno.[10] (tradução dos autores) (BURGESS, 2018, s/p)

Neste contexto exemplificativo, percebe-se que a produção de resultados falsos positivos acarreta consequências negativas ao indicar, de forma errônea, cidadãos como criminosos.[11] Dois pesquisadores do Instituto de Tecnologia de Massachusetts e da Universidade de Stanford, Joy Buolamwini e Timnit Gebru (2018), testaram alguns sistemas digitais de classificação de gênero e constataram margens de erro bastante significativas (de acordo com a cor da pele, por exemplo). Para homens brancos, a taxa máxima de erro foi de 0,8%. No caso de mulheres negras, a taxa de erro chegou a 34,7%. Observa-se, conforme já mencionado, os vieses e a marginalização quando determinadas raças e gêneros são colocados como objetos de análise de tais práticas posto que os modelos usados para desenvolver algoritmos de reconhecimento facial são, em sua maioria, desenvolvidos por homens brancos.

Acertadamente, o presidente da Microsoft, Brad Smith (2018), sustenta que:

> Embora os seres humanos não estejam imunes a erros ou vieses, acreditamos que, em determinados cenários de alto risco, é essencial que as pessoas qualificadas analisem os resultados do reconhecimento facial e tomem decisões importantes em vez de simplesmente entregá-las aos computadores. (SMITH, 2018, s/p)

Para o melhor funcionamento destes mecanismos, é preciso escanear os rostos e armazená-los em um banco de dados. Todas as pessoas presentes na área inspecionada são submetidas a essa vigilância. Ocorre que estes dados biométricos são considerados dados pessoais sensíveis pela Lei Geral de Proteção de Dados (BRASIL, 2018) (artigo 5º [12]). Seu tratamento e coleta necessitam de autorização para que sejam disponibilizados com outros fins (exigência disposta no mesmo instrumento normativo, em seu artigo 11[13]). Bárbara Simão, pesquisadora de Direitos Digitais do Idec, alerta:

[10] "These figures show that not only is real-time facial recognition a threat to civil liberties, it is a dangerously inaccurate policing tool. Statistics show that the tech misidentifies innocent members of the public at a terrifying rate, whilst there are only a handful of occasions where it has supported a genuine policing purpose".

[11] Em um curto período de utilização das câmeras de reconhecimento facial, em Copacabana, uma mulher já foi detida por engano (G1, 2019). Evento este que, além de gerar constrangimento e dano psicológico à pessoa, é passível de indenização por danos morais. Fica claro que existe um perigo ao fazer o uso desta tecnologia como meio de cumprimento da lei, colando em risco direitos tão importantes quanto a liberdade do indivíduo.

[12] "Art. 5º Para os fins desta Lei, considera-se:
[...]
II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural" (BRASIL, 2018).
[...]".

[13] "Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;
II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

> Ainda, é certo que ferramentas de reconhecimento facial com coleta de "dados sensíveis", dados biométricos de eventuais passantes, como as características do rosto que os identificam individualmente. Ao afetarem direitos de privacidade, exigem um grau maior de proteção e segurança, o que deve ser necessariamente garantido por parte dos responsáveis pelo tratamento, e auferido pelo Poder Público, a fim de se evitar graves danos indesejados. (IDEC, 2019, p.3)

Entretanto, sobre os dados colhidos pela ferramenta da empresa Oi, não houve qualquer esclarecimento por parte das autoridades se estes cuidados legais serão, de fato, tomados.

Outra preocupação real do Instituto de Defesa do Consumidor, o Idec (2019, s/p), está relacionada ao fato de os cidadãos terem ou não conhecimento do monitoramento, "para que tenham o direito de escolher se vão ou não para a área onde estão as câmeras". Além disso, e não menos importante, alertam que "é preciso ter cuidado para o propósito não ser desvirtuado, como, por exemplo, o compartilhamento de dados com empresas". Como aponta Harari (2018, p.78):

> Se quisermos evitar a concentração de toda a riqueza e de todo o poder nas mãos de uma pequena elite, a chave é regulamentar a propriedade dos dados. [...] No século XXI, os dados vão suplantar tanto a terra quanto a maquinaria como o ativo mais importante, e a política será o esforço por controlar o fluxo de dados.

A centralização destas informações, nas mãos do governo ou das empresas, concentra e fortalece o poder exercido sobre as populações. E não parece incongruente projetar o surgimento de novas ditaduras a partir disso.[14]

Por oportuno, Smith (2018) defendeu a regulação pública do tema e medidas de responsabilidade por parte das empresas porque, para ele, a adoção em larga escala destas tecnologias gera um alerta. Ocorre que tais medidas devem ser igualmente aplicadas pelos órgãos governamentais. Seguindo este raciocínio, Smith acredita que alguns problemas precisam ser abordados:

> Ao mesmo tempo, precisamos estar atentos aos riscos e ao potencial de abuso. À medida que continuamos a avaliar para onde essa tecnologia está indo, acreditamos que há três problemas que os governos precisam resolver.
>
> Primeiro, especialmente em seu estado atual de desenvolvimento, certos usos da tecnologia de reconhecimento facial aumentam o risco de decisões e, mais genericamente, de resultados tendenciosos e que, em alguns casos, violam leis que proíbem a discriminação.
>
> Segundo, o uso disseminado dessa tecnologia pode levar a novas intrusões na privacidade das pessoas.
>
> E terceiro, o uso da tecnologia de reconhecimento facial por um governo para a vigilância em massa pode invadir as liberdades democráticas. (SMITH, 2018, s/p)

a) cumprimento de obrigação legal ou regulatória pelo controlador; b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ; e) proteção da vida ou da incolumidade física do titular ou de terceiro; f) tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; ou g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais" (BRASIL, 2018).

[14] O sistema de vigilância executado na China é um exemplo da rápida proliferação da inteligência artificial pelo mundo. No país estão instaladas, aproximadamente, 170 milhões de câmeras que tudo sabem e tudo veem (BBC, 2017). Nada passa despercebido em um ambiente com pouquíssima proteção da privacidade.

A tendenciosidade levantada pelo entrevistado é real, pois não é difícil imaginar que, caso ocorra o furto de um automóvel nas redondezas da festa carnavalesca, a atuação policial se dará, primeiramente, em qualquer um dos membros da dita "classe perigosa" que estivessem presentes.

Para dar o primeiro passo na direção correta, Smith (2018) destaca que alguns princípios devem ser seguidos por todos aqueles que utilizam tais tecnologias, quais sejam: justiça, transparência, prestação de contas, não-discriminação, aviso e consentimento. Difícil asseverar, contudo, que qualquer um deles seja cumprido em níveis suficientes no Brasil.

Como corolário destes princípios, a cidade de San Francisco (EUA) proibiu, muito recentemente, a utilização de reconhecimento facial como instrumento de identificação de criminosos pelas agências governamentais (LEE, 2019). A votação foi aprovada pela Câmara de Supervisores da cidade por 8 votos a 1. Os argumentos sobre a medida são divergentes: alguns afirmam que a inexistência desta vigilância colocará as pessoas e o combate ao crime em risco, outros atestam que o reconhecimento facial está sujeito a erros (principalmente no caso de mulheres ou pessoas de pele mais escura) e representa uma violação da privacidade e liberdade dos indivíduos.

Segundo Matt Cagle da American Civil Liberties Union no norte da Califórnia: "Com esta votação, San Francisco declarou que a tecnologia de vigilância facial é incompatível com uma democracia saudável e que os residentes merecem uma voz nas decisões sobre vigilância de alta tecnologia"[15] (tradução dos autores) (LEE, 2019, s/p).

Trata-se de uma decisão que busca fomentar o uso responsável da tecnologia. Nas palavras de Joel Engardio, vice-presidente da Stop Crime SF:

> Concordamos que há problemas com a tecnologia de identificação de reconhecimento facial e ela não deve ser usada hoje. Mas a tecnologia vai melhorar e pode ser uma ferramenta útil para a segurança pública quando usada de forma responsável. Devemos manter a porta aberta para essa possibilidade.[16] (tradução dos autores) (LEE, 2015, s/p)

Ao que parece, os benefícios da vigilância por reconhecimento facial não justificam a limitação de direitos dos cidadãos, mesmo quando se apresenta disfarçada de política de segurança pública. Tais sistemas, da forma como estão formulados atualmente, podem avivar injustiças sociais e raciais preexistentes.

CONSIDERAÇÕES FINAIS

O uso da tecnologia de reconhecimento facial como forma de vigilância está se popularizando no mundo. Não há dúvida que o reconhecimento facial passou muito rapidamente de novidade tecnológica para vida real.[17] Porém, conforme as alternativas de monitoramento se desenvolvem, elevam-se também as preocupações relacionadas às aplicações e ao tratamento dos dados obtidos.

As questões apresentadas neste trabalho tratam da proteção de direitos humanos fundamentais como privacidade, liberdade de expressão e de locomoção. Não se trata de negar os benefícios, já que o sistema pode ser muito útil em casos de pessoas desaparecidas, indivíduos foragidos ou

[15] "With this vote, San Francisco has declared that face surveillance technology is incompatible with a healthy democracy and that residents deserve a voice in decisions about high-tech surveillance".

[16] "We agree there are problems with facial recognition ID technology and it should not be used today. But the technology will improve and it could be a useful tool for public safety when used responsibly. We should keep the door open for that possibility".

[17] Um levantamento do Instituto Igarapé (2019) mostrou que a utilização do reconhecimento facial é aplicada, principalmente, em quatro setores públicos, sendo eles: educação, transporte, controle de fronteiras e segurança pública. Ainda, segundo a mesma pesquisa, foram reportados 48 casos de implementação deste recurso desde 2011.

identificação de criminosos em flagrante. Mas é necessário evitar abusos, para que não seja mais um instrumento de controle e perseguição.

Frente aos erros e vieses destes recursos, nota-se que camadas socialmente vulneráveis estariam significativamente mais sujeitas a constrangimentos e violências, mediante abordagens policiais descabidas e imputação inverídica de atos criminosos. E mais que isso: o medo e a insegurança social fazem com que a população seja complacente com a restrição de direitos fundamentais e a segregação da "classe perigosa".

O Estado, visando resgatar a ordem social, mostra-se ineficiente para debelar tal problemática. São projetos e programas que aparecem e desaparecem sem atingir os objetivos desejados. E verdade seja dita: criminalidade se combate através de um conjunto de políticas públicas sérias, alinhadas com o desenvolvimento social e com a garantia de direitos. Políticas que contem com a adesão da própria comunidade e dos órgãos ligados à segurança pública. Repressão, legislação severa, construção de prisões e ações armamentistas são apenas medidas paliativas para problemas estruturais de enorme gravidade.

É possível que as novas tecnologias auxiliem neste enfrentamento. Todavia, há que ter cuidado, responsabilidade e transparência. O uso governamental e empresarial deve estar sujeito às leis, ou corremos o risco de reproduzir o cenário descrito por George Orwell em seu livro "1984", com uma vigilância em massa sem precedentes, quiçá voltada para o extermínio do supostamente perigoso.

REFERÊNCIAS

BALL, Kirstie; WEBSTER, Frank. **The intensification of surveillance**. In: *The intensification of surveillance*, ed. Kiristie Ball and Frank Webster, 1-15. London: Pluto Press, 2003.

BARATTA, Alessandro. **Criminologia crítica e crítica do direito penal:** introdução à sociologia do direito penal. 3. ed. Rio de Janeiro: Revan, 2002.

BAUMAN, Zygmunt. **Confiança e medo na cidade**. Rio de Janeiro: Jorge Zahar, 2009.

_____. **Globalização: as consequências humanas**. Rio de Janeiro: Jorge Zahar Editor, 1999.

_____. **Medo Líquido**. Rio de Janeiro: Jorge Zahar, 2008.

_____. **Vigilância Líquida**. Rio de Janeiro: Editora Jorge Zahar. 2014.

BBC**. Como funciona o 'Big Brother' da China, com 170 milhões de câmeras que fazem identificação visual.** 15 dez. 2017. Disponível em: <http://www.bbc.com/portuguese/internacional-42361047>. Acesso em: 21 set. 2019.

BECKER, Howard Saul. **Outsiders:** estudos de sociologia do desvio. 1.ed., Rio de Janeiro: Jorge Zahar, 2008.

BIGO, Didier et al. **Theorizing Surveillance:** The panopticon and beyond. Portland: Willan Publishing, 2006.

BRASIL. **Lei no 13.709, de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da República Federativa do Brasil. Brasília, DF, 14 de agosto de 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 16 mai. 2019.

BUOLAMWINI, JOY and GEBRU, Timnit. **Gender Shades:** Intersectional Accuracy Disparities in Commercial Gender Classification. Proceedings of the 1st Conference on Fairness, Accountability and Transparency, PMLR 81:77-91, 2018.

BURGESS, Matt. **Facial recognition tech used by UK police is making a ton of mistakes:** South Wales Police, London's Met and Leicestershire have all been trialling automated facial recognition in public places. But a lack of legal oversight exists around the technology. 2018. Disponível em: <https://www.wired.co.uk/article/face-recognition-police-uk-south-wales-met-notting-hill-carnival>. Acesso em: 30 abr. 2019.

CALDEIRA, Teresa. Enclaves Fortificados: A Nova Segregação Urbana. Tradução de Heloísa Buarque de Almeida. **Novos Estudos Cebrap**, nº 47, março de 1997, p. 155-176. Disponível em: <http://reverbe.net/cidades/wp-content/uploads/2011/08/Enclaves-fortificados_segregacao-urbana.pdf>. Acesso em 26 set. 2019.

CASTEL, Robert. **A insegurança social**: o que é ser protegido?. Rio de Janeiro: Vozes. 2005.

COIMBRA, Cecília. **OPERAÇÃO RIO**: O mito das classes perigosas: um estudo sobre a violência urbana, a mídia impressa e os discursos de segurança pública. Rio de Janeiro: Oficina do Autor. 2001.

DOMO. **Data Never Sleeps 7.0.** 2019. Disponível em: <https://www.domo.com/learn/data-never-sleeps-7>. Acesso em: 21 set. 2019.

FOUCAULT, Michel. **Vigiar e Punir:** nascimento da prisão. 20.ed., Petrópolis: Vozes, 1999.

FUCHS, Christian. Como podemos definir vigilância?. **MATRIZes**, Ano 5 – nº 1 jul./dez. 2011. São Paulo, Brasil. p.109-136. Disponível em: <https://www.revistas.usp.br/matrizes/article/download/38311/41154>. Acesso em: 29 abr. 2019.

G1-RIO. **Sistema de reconhecimento facial da PM do RJ falha, e mulher é detida por engano:** Secretaria reconheceu o erro e lamentou o fato. Segundo a corporação, a pessoa foi levada para a delegacia, onde foi confirmado que não se tratava da criminosa procurada. 11 jul. 2019. Disponível em: <http://g1.globo.com/rj/rio-de-janeiro/noticia/2019/07/11/sistema-de-reconhecimento-facial-da-pm-do-rj-falha-e-mulher-e-detida-por-engano.ghtml>. Acesso em: 20 set. 2019.

GALLUP. **2018 Global Law and Order.** 2018. Disponível em: <http://www.insightcrime.org/wp-content/uploads/2018/06/Gallup_Global_Law_And_Order_Report_2018.pdf>. Acesso em: 29 abr. 2019.

GANDY, Oscar H. **The panoptic sort.** A political economy of personal information. Boulder: Westview Press. 1993.

HARARI, Yuval Noah. **21 lições para o século 21**. São Paulo: Companhia das Letras, 2018.

HOMELAND SECURITY. **Biometric Exit System.** Disponível em: <https://www.dhs.gov/taxonomy/term/7404/all/feed>. Acesso em: 16 mai. 2019.

IDEC – Instituto Brasileiro de Defesa do Consumidor. **Idec alerta PM do RJ sobre riscos no uso de câmera inteligente no Carnaval:** Projeto-piloto com câmeras "inteligentes" que reconhecem pessoas será utilizado pelo governo do Rio de Janeiro durante o Carnaval, mas ainda é necessário discutir mecanismos de proteção de dados. 07 fev. 2019. Disponível em: <https://idec.org.br/noticia/idec-alerta-pm-do-rj-sobre-riscos-no-uso-de-camera-inteligente-no-carnaval>. Acesso em: 30 abr. 2019.

INFOPEN. **Levantamento Nacional de Informações Penitenciárias Atualização - Junho de 2017.** Disponível em: <http://depen.gov.br/DEPEN/depen/sisdepen/infopen/relatorios-sinteticos/infopen-jun-2017-rev-12072019-0721.pdf>. Acesso em: 20 set. 2019.

INSTITUTO IGARAPÉ. **Reconhecimento facial no Brasil:** Desde 2011 vem sendo utilizado o Reconhecimento Facial no Brasil. 2019. Disponível em: <https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/>. Acesso em: 20 set. 2019.

LEE, Dave. **San Francisco is first US city to ban facial recognition.** 2019. Disponível em: <https://www.bbc.com/news/technology-48276660>. Acesso em: 16 mai. 2019.

LOMBROSO, Cesare. **O Homem Delinquente**. Tradução: Sebastian José Roque. São Paulo: Ícone, 2010.

LUM, Kristian. **Predictive Policing Reinforces Police Bias.** 10 out. 2016. Disponível em: <https://hrdag.org/2016/10/10/predictive-policing-reinforces-police-bias/>. Acesso em: 29 abr. 2019.

MATHIESEN, Thomas. **The viewer society:** Michel Foucault's 'Panopticon' revisited from Theoretical criminology. London: Sage, 1997.

MIRANDA, Márcia Mathias de. Sociedade, violência e políticas de segurança pública: da intolerância à construção do ato violento. **Revista Eletrônica Machado Sobrinho**, Minas Gerais, 2011. Disponível em: <http://www.machadosobrinho.com.br/revista_online/miolo.php?miolo=artigos03>. Acesso em: 28 abr. 2019.

PMERJ. **Polícia Militar vai implantar programa de reconhecimento facial e de placas de veículos.** 2019. Disponível em: <http://www.pmerj.rj.gov.br/2019/01/policia-militar-vai-implantar-programa-de-reconhecimento-facial-e-de-placa-de-veiculos/>. Acesso em: 30 abr. 2019.

PROPUBLICA. **Machine Bias:** There's software used across the country to predict future criminals. And it's biased against blacks. 23 maio 2016. Disponível em: <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>. Acesso em: 29 abr. 2019.

SMITH, Brad. **Reconhecimento facial:** é hora de agir. 2018. Disponível em: <https://news.microsoft.com/pt-br/reconhecimento-facial-e-hora-de-agir/>. Acesso em: 2 mai. 2019.

U.S. CUSTOMS AND BORDER PROTECTION. **Biometrics.** Disponível em: <https://www.cbp.gov/travel/biometrics>. Acesso em: 16 mai. 2019.