Doi: 10.5212/Emancipacao.v.20. 2014258.022

Vigilância e segurança pública: preconceitos e segregação social ampliados pela suposta neutralidade digital

Surveillance and public security: prejudices and social segregation widened by the alleged digital neutrality

Camila Berlim Schneider[*]
Pedro Fauth Manhães Miranda[**]

Resumo: O presente artigo busca demonstrar como as novas implementações algorítmicas, alegadamente imparciais, acentuam a discriminação e os preconceitos por meio de mecanismos de vigilância. Quando as informações pessoais sobre a população são aplicadas no desenvolvimento de tecnologias de inteligência artificial, em uma sociedade já marcada pela seletividade, as consequências podem ser catastróficas. O ponto de partida é dado pela análise sobre vigilância, atualizada por Zygmunt Bauman, descrevendo como a sociedade da informação se delineou e ganhou a forma que possui hoje. Na sequência, por meio de revisão bibliográfica consubstanciada via método dedutivo, é possível observar que em países onde há permanente sensação de insegurança e a discriminação racial se institucionalizou, o uso pouco transparente de algoritmos preditivos, em especial pela justiça criminal, provoca efeitos negativos na eficácia das políticas públicas, fazendo cada vez mais vítimas e acentuando disparidades, ao invés de promover segurança.

Palavras-chave: Controle Social. Algoritmos. Segregação.

Abstract: This article attends to demonstrate how the new algorithmic implementations, allegedly unbiased, accentuate discrimination and prejudice through the surveillance mechanisms. When personal information about the population is applied to the development of artificial intelligence technologies, in a society already marked by selectivity, the consequences can be catastrophic. The starting point is given by the analysis on surveillance, updated by Zygmunt Bauman, describing how the information society was

[*] Graduanda em Direito pelo Centro Universitário Santa Amélia - UniSecal; Mestre em Engenharia e Ciência dos Materias pela Universidade Federal do Paraná - UFPR; Graduada em Física pela Universidade Federal do Paraná – UFPR. E-mail: camibs88@gmail.com

[**] Doutorando em Direito na Pontifícia Universidade Católica do Paraná - PUCPR; Mestre em Ciências Sociais Aplicadas na Universidade Estadual de Ponta Grossa - UEPG; Graduado em Direito pela Universidade Estadual de Londrina - UEL; Graduando em Ciência Política pelo Centro Universitário Internacional - UNINTER. Professor de Direito no Centro Universitário Santa Amélia – UNISECAL. E-mail: pedromiranda.adv@gmail.com.

shaped and gained the form it has today. Then, through a bibliographic review based on a deductive method, it is possible to observe that in countries where there is a permanent feeling of insecurity and racial discrimination has become institutionalized, the lack of transparent use of predictive algorithms, especially by criminal justice, causes negative effects on effectiveness of public policies, making more and more victims and accentuating disparities, instead of promoting security.

Keywords: Social Control. Algorithms. Segregation.

Recebido em 27/08/2019. Aceito em 23/07/2020.

Introdução

É verdade que as noções de vigilância, controle e disciplina não passaram a existir somente com a revolução informacional. Mas, também, é inegável que o advento da internet e o estabelecimento definitivo da sociedade da informação promoveram inúmeras transformações, especialmente sobre o contexto no qual tais práticas se realizam. As formas de poder disciplinar, antes restritas aos ambientes penitenciários, tornam-se universais. Qualquer ambiente se transforma em lugar de supervisão, e a obediência aos padrões impostos não é mais alcançada por meio da coerção. Agora, disfarçada de livre-arbítrio, a vigilância é operada por todas as pessoas, voluntariamente.

Com o desenvolvimento de novas tecnologias, a exemplo de algoritmos preditivos, muitos dados particulares passam a ser armazenados, o que possibilita a identificação de padrões comportamentais e o domínio de populações inteiras, sendo posteriormente aplicados em sistemas de segurança e monitoramento. Dessa maneira, fronteiras espaciais e temporais são rompidas. Mas há que se ter cuidado ao envolver direitos à privacidade e à liberdade.

Considerando esses aspectos, em um primeiro momento surgem diversos questionamentos: Quem alimenta o sistema de dados? Que tipo de informação é armazenada? Quais são as suas fontes? Quais as consequências da utilização desse mecanismo na elaboração de sistemas de vigilância? O que acontece se delegarmos o poder aos criadores dessas tecnologias de segurança?

Uma análise profunda dos modelos de vigilância, ao longo da história até os dias atuais, aponta novas estratégias para a formulação de sistemas de segurança pública, a partir da utilização de instrumentos de monitoramento baseados em inteligência artificial. Destarte, a persistência de preconceitos, estereótipos e demais práticas discriminatórias, quase sempre veladas, mostra que nem tudo mudou, apenas são exercidas de modo diferente, digital, cibernético. Neste ponto, as recentes políticas informatizadas de segurança pública, quando direcionadas para a previsão de delitos e identificação de potenciais indivíduos criminosos, acabam acentuando rótulos que perpassam a sociedade e suas instituições.

Sendo assim, o texto que segue promove uma revisão bibliográfica que tem por objetivo demonstrar, por meio do método dedutivo, como as formas de segregação e os antigos preconceitos são transformados e naturalizados, passando a ser mimetizados pelas novas tecnologias,

sob a justificativa de garantia da segurança. Tece-se, desta forma, uma inegável conexão entre a vigilância pretensamente preditiva e as novas tecnologias de informação.

Para tanto, o trabalho compõe-se de três seções. A primeira explora as diferentes sociedades de vigilância, a partir das definições de Jeremy Bentham, Michel Foucault, Zygmunt Bauman e Didier Bigo, sempre correlacionando tais teorias a certos exemplos. Adiante, é definido o estabelecimento da sociedade da informação, a partir da concepção de sociedade em rede, de Manuel Castells. Na sequência, os algoritmos baseados em tecnologias de inteligência artificial serão analisados e sua alegada neutralidade será colocada à prova. Dando seguimento, na mesma seção, é retomada a discussão de estigmas e segregação, agora sobre o contexto da sociedade pós-moderna e da globalização, revalidada pelos ensinamentos de Zygmunt Bauman. A derradeira seção discorre sobre as políticas de segurança pública e o encarceramento em massa americano. Embasado pela teoria do desvio de Howard Becker e pelo processo de vigilância de Didier Bigo, o estudo é finalizado pela comprovação de como os atuais algoritmos preditivos refletem e ampliam preconceitos consolidados.

A(s) Sociedade(s) de Vigilância

Em 1949, George Orwell (2017, p.12) profetizava no clássico *1984*: "O Grande Irmão está observando você". Algum tempo depois, no ano de 1975, na sua obra *Vigiar e Punir*, Michel Foucault (1999, p.162) afirmava: "Às portas, postos de vigilância; no fim de cada rua, sentinelas". Metafóricas ou não, estas ideias buscam retratar uma noção de vigilância. Contudo, por mais atuais que possam parecer tais afirmações, nem mesmo Orwell poderia imaginar uma forma de vigilância capaz de transpor a pele do indivíduo e espionar seus sentimentos mais secretos. Assim, mais recentemente, Zygmunt Bauman (2014, p.04) categorizou: "A vigilância se insinua em estado líquido". Porém, para a compreensão do panorama atual, vale a análise de alguns aspectos preliminares.

Em 1785, Jeremy Bentham (2008) já havia idealizado um projeto de construção prisional com vigilância constante, o panóptico. Neste modelo havia uma torre central que permitia observar os presos nas suas celas. Com isso, era possível a um único vigilante observar todos os prisioneiros, sem que estes soubessem se estavam ou não sendo observados. Um mecanismo de vigilância ininterrupta, baseado em uma estrutura física.

Michel Foucault utilizou esta construção para pensar não apenas a vigilância, mas também a disciplina. Para ele, os corpos individualizados poderiam ser adestrados, transformados e aperfeiçoados. Docilizados, enfim.

> O momento histórico das disciplinas é o momento em que nasce uma arte do corpo humano, que visa não unicamente o aumento das suas habilidades, nem tampouco aprofundar sua sujeição, mas a formação de uma relação que no mesmo mecanismo o torna tanto mais obediente quanto é mais útil, e inversamente. Forma-se então, uma política das coerções que são um trabalho sobre o corpo, uma manipulação calculada dos seus elementos, de seus gestos, de seus comportamentos. (FOUCAULT, 1999, p.119)

Esse pensamento concretizou a análise da transição de uma estrutura física de panoptismo para uma tecnologia do poder, utilizada com a finalidade de obter o máximo de proveito e domínio sobre os indivíduos (homem-corpo), sempre conectada a um capitalismo liberal em ascensão, de modo a torná-lo o mais eficaz possível.

> O corpo humano entra numa maquinaria de poder que o esquadrinha, o desarticula e o recompõe. Uma "anatomia política", que é também igualmente uma "mecânica do poder", está nascendo; ela define como se pode ter domínio sobre o corpo dos outros, não simplesmente para que façam o que se quer, mas para que operem como se quer, com as técnicas, segundo a rapidez e a eficácia que se determina. (FOUCAULT, 1999, p.119)

Concomitantemente, surge a biopolítica, que direciona o foco para corpos coletivos. O poder passa a ser exercido sobre populações inteiras, e se encarrega de preservar a vida, eliminando o que ameaça o bem-estar social, a partir de noções econômicas liberais. Considerando os aspectos biológicos do corpo humano, previsões e estatísticas (referentes a índices de natalidade, mortalidade, epidemias etc.) se transformam em estratégias de poder. Michel Foucault, inclusive, frisa que quanto maior o número de informações sobre os indivíduos, maior a possibilidade de controle de comportamentos.

Este biopoder não se caracteriza pela execução de pessoas, mas valoriza o perigo que pode atingir toda a população, justificando um tipo de purificação da sociedade. Vários são os aspectos utilizados para discriminar grupos de pessoas, conforme explica Thomas C. Schelling (1969, p.488):

> As pessoas são separadas em diferentes linhas e de diferentes maneiras. Há segregação por sexo, idade, renda, idioma, cor, gosto, vantagem comparativa e acidentes de localização histórica. Algumas segregações são organizadas; algumas são determinadas economicamente; algumas são resultado de sistemas de comunicação especializados; e algumas são resultado da interação de escolhas individuais que discriminam (tradução dos autores).[1]

É, afinal, uma realidade semelhante à que Orwell denunciava em sua ficção - mais realista que muitas reportagens jornalísticas, vale dizer. Visando à preservação da vida e do bem-estar, os dados obtidos serviam à segregação dos enfermos e "anormais" de todo o tipo em hospícios, manicômios e demais instituições distantes da vista dos demais.

Como exemplo desta política, há o regime adotado pela África do Sul, durante o *Apartheid,* pelos governos do Partido Nacional. A legislação vigente dividia a população em quatro grandes grupos raciais: "pretos", "brancos", "de cor" e "indianos" (BALDWIN-RAGAVEN; LONDON; DU GRUCHY, 1999, p.18). O regime nacionalista aprovou mais de 300 leis relativas ao *Apartheid*. Estas leis incluíam, por exemplo, além da citada divisão racial: separação em diferentes áreas habitacionais, inclusive por meio de remoções forçadas; separação de serviços públicos como saúde e educação; proibição de casamentos inter-raciais; e privação do exercício da cidadania (HOSIE, 2004).

Uma motivação comum empregada para justificar tal discriminação é a crença de que determinadas raças são inferiores e, por este motivo, merecem tratamento inferior. Nesta conjuntura, estigmas e formas de segregação encontram-se fortemente vinculados. Estudiosos contemporâneos reconhecem que o modelo de vigilância panóptico representava uma fonte teórica altamente eficiente de segregação. Assim doutrina Pedro Scuro Neto quando afirma:

[1] "People get separated along different lines and in different ways. There is segregation by sex, age, income, language, color, taste, comparative advantage, and the accidents of historical location. Some segregation is organized; some is economically determined; some results from specialized communication systems; and some results from the interplay of individual choices that discriminate".

> O mesmo tipo de mecanismo é aplicado também a sujeitos submetidos à internação (encarceramento e/ou hospitalização), e no processo de segregação de minorias raciais, étnicas ou religiosas. Isolado, o indivíduo deve vivenciar a própria impotência diante da férrea objetividade dos mecanismos de controle aplicados – é compelido a experimentar uma sensação física e moral, profunda e "peculiar", uma dualidade, um sentimento de estar sempre olhando para si mesmo através dos olhos dos outros e medindo a própria alma com a fita métrica do mundo que o encara atemorizado, com desprezo ou piedade. (SCURO NETO, 2010, p.244)

Tal aparato, típico da modernidade de outrora, marca o surgimento de um modelo de vigilância que, comparativamente, permite melhor analisar o controle na atual sociedade da informação, na qual situa-se Zygmunt Bauman.

Esse sociólogo e filósofo polonês propõe uma nova representação. Para tanto, não utiliza a comumente aceita denominação "pós-modernidade", mas sim "modernidade líquida". Ele cunhou o referido termo com a finalidade de definir um estado de mudança fluído, que não conserva a sua forma por muito tempo. Diferentemente da "modernidade sólida" onde existia uma fixidez na relação entre o sujeito e as instituições, o novo conceito vem reforçar o caráter frágil e temporário das relações sociais e humanas.

Em vista disso, há uma mudança de paradigma na ideia de vigilância. Tal como a "modernidade líquida", surge a "vigilância líquida". Todavia, Bauman não nega o modelo panóptico; pelo contrário, o atualiza. Seu entendimento pode ser observado na seguinte fala: "Tal como eu vejo, o panóptico está vivo e bem de saúde, na verdade, armado de músculos eletronicamente reforçados, ('ciborguizados') tão poderosos que Bentham, ou mesmo Foucault, não conseguiria nem tentaria imaginá-lo" (BAUMAN, 2014, p.42).

Segundo ele, a disciplina e a segurança estão conectadas entre si, ao contrário do que pensavam os filósofos predecessores. Hoje, a segurança se concretiza pelo emprego de tecnologias digitais de vigilância, ainda que os reflexos dos primeiros mecanismos de controle possam ser facilmente identificados nos processos de estereotipia e nas atuais medidas de exclusão.

Neste sentido, Bauman discute duas variações dos mecanismos de vigilância. O banóptico, de Didier Bigo, e o sinóptico de Thomas Mathiesen.

O banóptico é usualmente aplicado a categorias de pessoas, analisando quem é bem-vindo e quem é indesejado no meio social, sempre digitalmente. No momento em que determinado grupo é rotulado como suspeito, sua mobilidade é limitada e a sua presença passa a não ser mais aceita em determinados espaços. Esse modelo é comumente utilizado nas questões de movimentação entre fronteiras (entrada e saída de imigrantes, por exemplo).

Sua concretização em aeroportos, postos de fronteira e imigração é inegável, sendo impossível não perceber que este aparato se intensificou após o atentado de 11 de setembro de 2011, nos Estados Unidos. O controle da população foi revisto e atualizado – não necessariamente de modo transparente e/ou democrático, mas sempre em nome da insofismável "segurança pública".

> Bigo analisa discursos (níveis de risco e ameaça, inimigos internos, e assim por diante), instituições, estruturas arquitetônicas (de centros de detenção a terminais de passageiros em aeroportos), lei e medidas administrativas – cada uma das quais seleciona certos grupos para tratamento especial. A função estratégica do diagrama banóptico é traçar o perfil de minorias "indesejadas".

> Suas três características são o poder excepcional em sociedades liberais, traçar perfis e normalizar grupos não excluídos. (BAUMAN, 2014, p.46)

Esse modelo se mostra adequado para monitorar pessoas (seja nas fronteiras, nos aeroportos ou nas grandes cidades) e, posteriormente, bani-las, sendo exercido pelo emprego de um raciocínio estatístico, implementado por técnicas digitais. Contudo, é bem verdade que diversos outros fatores exercem influência sobre os vigilantes e os vigiados, o que será exposto adiante.

Já o sinóptico, nas palavras de Bauman, seria o "panóptico faça você mesmo". Neste modelo de vigilância, o controle não se dá em um espaço físico localizado. Existe uma vigilância onde tanto o alvo quanto o controle estão em constante movimento. O vigilante, mais do que nunca, é onipresente e onisciente. E, ao vigiado, não restam dúvidas sobre a ocorrência da inspeção incessante, mesmo porque é ele próprio quem fornece, publicamente, dados particulares. A preocupação com invasões de privacidade não mais existe, vive-se um momento de evasão desta, a qual é concretizada pelos próprios vigiados.

O filósofo Byung-Chul Han, em seu livro "Psicopolítica: o neoliberalismo e as novas técnicas de poder", sintetiza o assunto de modo pertinente, ao também atualizar o conceito de panóptico para a era digital, afirmando que:

> O panóptico digital faz uso de uma revelação voluntária por parte de seus internos. A auto exploração e a auto exposição seguem a mesma lógica. A liberdade é sempre explorada. Ao panóptico digital falta aquele Grande Irmão que arranca informações contra nossa vontade. Em vez disso, nós nos revelamos, expomo-nos por iniciativa própria [...]. A comunicação coincide inteiramente com o controle. Cada um é o panóptico de si mesmo. (HAN, 2018, p.57-58)

Claramente, é nesse momento que é evidenciada a noção de vigilância atual: o controle virtual. Muitas pesquisas vêm sendo realizadas no sentido de compreender e explicar tal conceito (BIGO, 2006; O'NEIL, 2016; PROPUBLICA, 2016, dentre outros). Um empreendimento em que barreiras são transpostas, o monitoramento é feito a distância, as informações e as pessoas se movem de maneira fluída e tudo se encontra interligado. Observador e observado se tornam um único organismo indissociável, um híbrido entre a presença física e a presença virtual.

A Sociedade da Informação

A transição da era industrial para a era da informação não trouxe apenas mudanças tecnológicas. Paralelamente, a sociedade também foi se modificando, pois, como observado anteriormente, ela é mutável. A nova organização é pautada no desenvolvimento social e econômico, através da criação de um conhecimento que se apresenta, fundamentalmente, na produção de riquezas, na distribuição de bens e na busca do bem-estar social.

A sociedade da informação se estabelece como uma sociedade em rede, tal qual a ideia de Manuel Castells (1999). Para ele, as redes são conjuntos de nós interligados, e cada nó é um ponto no qual os fluxos se encontram. Essa nova estrutura social tem o seu funcionamento dependente das tecnologias digitais de informação e comunicação, basicamente erigidas a partir da internet. O autor continua na toada, afirmando que, em face das interações digitais, impossíveis de serem pensadas de modo deslocado do "mundo real", a internet, enquanto espaço de fluxos, não deve ser compreendida como fotocópia da sociedade, mas como a própria sociedade, com processos espaciais constituídos pela dinâmica de toda a estrutura social.

Pode-se afirmar, sem medo de errar, que grande parte do planeta está conectada, e a tendência é que a cobertura digital cresça ainda mais. A rede é uma realidade na vida cotidiana, nas empresas, no trabalho, na cultura e mesmo na política. Consequentemente, este novo contexto promove um necessário reexame da sociedade, agora conectada e digital.

Um relatório recente sobre economia digital publicado pela Conferência das Nações Unidas sobre Comércio e Desenvolvimento "colocou o Brasil em quarto lugar no ranking mundial de usuários de internet. Com 120 milhões de pessoas conectadas, o Brasil fica atrás apenas dos Estados Unidos, Índia e China" (ONU/BR, 2017). Esse panorama gera implicações muito importantes no que diz respeito ao controle e à vigilância de grandes populações.

Diante disso, ressurge a inúmeras vezes repetida, porém não menos fundamental, ambiguidade do potencial transformador das novas tecnologias. Não há como negar que a internet deu voz a minorias, antes muito mais invisíveis do que hoje. Movimentos por empoderamento feminino e igualdade racial, por exemplo, podem ganhar dimensão mundial em poucos dias. Desta feita, o espaço eletrônico, tanto pode originar um novo sistema de exclusão, como pode vir a constituir-se num instrumento de oposição.

Mas um fato importante continua intacto: aqueles que possuem as informações são detentores do poder. Conforme afirma Dupas (2001, p.42):

> Nas redes, o poder desloca-se para os que detêm o controle dos fluxos. Ordenar uma rede, estar presente nela e operar a dinâmica de sua inter-relação com outras redes define as estruturas de dominação e transformação de nossa sociedade.

Mesmo com a difusão da internet, o acesso não é igualitário. As comunidades carentes, as escolas públicas, as pessoas de baixo poder aquisitivo e aquelas com menor nível de escolaridade não têm acesso à rede. É nítida a relação entre a pobreza e a exclusão social/digital. A acentuação de desigualdades, neste meio, pode inviabilizar a efetivação de direitos fundamentais e enfraquecer a democracia, principalmente em países nos quais os presidentes governam por meio das redes sociais.

> Diante desse novo cenário social, político e econômico em que a principal riqueza é a informação, destaca-se o intensivo uso da tecnologia da informação para supervisão e para fiscalização dos indivíduos. São dois os principais mecanismos utilizados: formação de arquivos com informações pessoais e vigilância do comportamento das pessoas. (VIEIRA, 2007, p.195)

É, enfim, um desenvolvimento ambivalente, e qualquer que seja a análise sobre o espaço digital, deve-se levar em conta a realidade a partir da qual ela se erige.

Tecnologia de inteligência artificial e sua (alegada) imparcialidade

Com a chegada das redes sociais e dos sites de buscas e compras, nossas vidas foram transportadas, em grande parte, para o espaço digital. A maior parte dos processos econômicos, sociais e políticos depende da tecnologia para funcionar de modo eficiente.

Acontece que, ao utilizar estes recursos, o usuário perde uma parcela da privacidade e expõe, por vezes sem sequer perceber, muito de sua intimidade pelos "benefícios e comodidades" oferecidos em troca. O ato de "navegar" na internet deixa pegadas digitais que revelam pistas

sobre comportamento, personalidade, preferências e até sonhos de consumo do usuário. Pariser (2012, p.7) explica que:

> Segundo pesquisas, a ampla maioria das pessoas imagina que os mecanismos de busca sejam imparciais. Mas essa percepção talvez se deva ao fato de que esses mecanismos são cada vez mais parciais, adequando-se à visão do mundo de cada um. Cada vez mais, o monitor do nosso computador é uma espécie de espelho que reflete nossos próprios interesses, baseando-se na análise de nossos cliques feita por observadores algorítmicos.

A internet não esquece o que é registrado nos seus servidores. Consequentemente, uma série incalculável de dados é produzida e, portanto, processada, organizada e armazenada. Há um intercâmbio muito grande de informações pessoais, uma vez que as mídias sociais monitoram seus usuários constantemente. Neste contexto, engana-se quem acredita que as redes sociais são fabricadas com a finalidade exclusiva de estreitar laços afetivos ou proporcionar praticidade nas relações profissionais. Não se trata de negar os benefícios, mas de examinar a situação mais de perto. Gilberto Dupas (2001, p.16) descreve de forma magistral este mecanismo:

> [...] a máquina é substituída pela informação e o contato entre pessoas passa e ser mediado pela tela eletrônica. O mundo social se desmaterializa, transforma-se em signo e simulacro. Rouanet lembra que 'sob a implacável luz néon da sociedade informatizada, não há mais cena – a realidade tornou-se, literalmente, obscena, pois tudo é transparência e visibilidade imediata'.

Aquilo que era privado e particular se torna público e passa a ser compartilhado com qualquer "amigo virtual" – e com quem mais obtiver acesso a tais informações. A nossa sociedade rompe todas as barreiras do tempo, do espaço e, principalmente, da privacidade.

A análise e categorização de indivíduos passa a ser feita por algoritmos computacionais. Organizações do governo, empresas multinacionais e mesmo *hackers* acessam e analisam tais dados. Não é por acaso que cada usuário da internet recebe recomendações de filmes, músicas, roupas e notícias ajustadas ao seu gosto pessoal. E, mesmo sem perceber, transfere a autonomia e o poder de fazer escolhas importantes para os algoritmos. Cumpre ressaltar que muitas destas sugestões carregam uma carga de preconceito. Mas essas dicas não passam de algoritmos alimentados com dados que os próprios usuários produzem. As máquinas passam a conhecer seus clientes melhor que eles mesmos. E mais, passam a tirar conclusões (certas ou erradas, morais ou imorais) por toda a sociedade, desresponsabilizando-a de seus reflexos.

Cathy O'Neil, cientista de dados e PhD em Matemática pela Universidade de Harvard, autora do livro *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* ("Armas de Destruição Matemática: Como o *Big Data* Aumenta a Desigualdade e Ameaça à Democracia"), não enxerga com tanto entusiasmo as novas tecnologias:

> O diferencial do *Big Data* é a quantidade de dados disponíveis. Há uma montanha gigantesca de dados que se correlacionam e que podem ser garimpados para produzir a chamada "informação incidental". É incidental no sentido de que uma determinada informação não é fornecida diretamente – é uma informação indireta. É por isso que as pessoas que analisam os dados do *Twitter* podem descobrir em qual político eu votaria. Ou descobrir se eu sou *gay* apenas pela análise dos *posts* que eu curto no Facebook, mesmo que eu não diga que sou gay. A questão é que esse processo é cumulativo. Agora que é possível descobrir

> a orientação sexual de uma pessoa a partir do seu comportamento nas redes sociais, isso não vai ser "desaprendido". Então, uma das coisas que mais me preocupam é que essas tecnologias só vão ficar melhores com o passar do tempo. Mesmo que as informações venham a ser limitadas - o que eu acho que não vai acontecer – esse acúmulo de conhecimento não vai se perder. (O'NEIL *apud* BARROS, 2017)

Com os novos sistemas tecnológicos, principalmente aqueles baseados em inteligência artificial, o conceito de vigilância também sofre mudanças. Há um costume de associá-los às câmeras das lojas, dos elevadores, das ruas ou ainda quando telefones são grampeados. Entretanto a vigilância está embutida em todos os aspectos da vida contemporânea. A segurança de determinadas coletividades que antes era feita por pessoas posicionadas, estrategicamente, em estruturas físicas, passa a ser realizada por máquinas "inteligentes". A monitoração eletrônica não tem mais a função de impor um comportamento previsto em alguma norma disciplinar, mas de impedir condutas indesejadas.

Nesse contexto, a maior preocupação não é referente aos números ou conteúdo de dados armazenados, muito menos ao progresso tecnológico. Está fortemente relacionada a *como* e *para quê* a análise destes dados é feita.

As tecnologias de inteligência artificial, mais precisamente os algoritmos, são alimentados com as visões de quem os cria. O processo de carregá-los com dados e instrumentalizá-los, aliás, tem um nome bastante sintomático: aprendizado de máquina. Assim, ao tentar parecer neutro, o algoritmo potencializa ainda mais as desigualdades, os preconceitos e os estereótipos. Um relatório do governo dos Estados Unidos (SMITH; PATIL; MUÑOZ, 2016) aponta:

> A era do Big Data também está cheia de riscos. O sistema algorítmico que transforma dados em informações não é infalível – ele se baseia na imperfeição de inserções, da lógica, da probabilidade e das pessoas que os desenvolvem. [...] Sem cuidado, essas inovações podem facilmente promover a discriminação, reforçar vieses e mascarar oportunidades (tradução dos autores).[2]

Observe-se, ilustrativamente, o caso do robô Norman, desenvolvido pelo Instituto de Tecnologia de Massachusetts – MIT (YANARDAG; CEBRIAN; RAHWAN, 2018). Utilizando o aprendizado de máquina, os pesquisadores alimentaram um algoritmo com imagens publicadas nos maiores (e piores) fóruns da internet. Para demonstrar como as novas ferramentas tecnológicas carregam as tendências das informações que recebem, e o quanto isso pode ser perigoso, submeteram o robô ao teste de *Rorschach*. Neste teste, era preciso que Norman descrevesse o que identificava nas imagens. Suas impressões foram comparadas às de um robô "normal". Numa delas, enquanto o robô padrão enxergou uma foto de um bolo de casamento, Norman identificou um homem sendo morto por um motorista em alta velocidade. A conclusão final: Norman apresentou claros traços de psicopatia.

Neste experimento também fica evidente a parcialidade dos algoritmos, que são apenas um reflexo da nossa humanidade (ou, a depender da interpretação, da falta dela). Muitas vezes, os preconceitos embutidos nos dados estão "escondidos", fazendo com que pareçam objetivos

[2] "The era of big data is also full of risk. The algorithmic systems that turn data into information are not infallible - they rely on the imperfect inputs, logic, probability, and people who design them. [...] Without deliberate care, these innovations can easily hardwire discrimination, reinforce bias, and mask opportunity".

ou neutros. No seu estudo sobre vigilância, Bauman demonstra como os aspectos morais e éticos são descartados nestes processos:

> Outro ângulo da adiaforização em termos de vigilância é a forma como dados do corpo (dados biométricos, DNA) ou por ele desencadeados (por exemplo, situações em que se faz um *login*, usa-se um cartão de acesso ou mostra-se a identidade) são sugados para bases de dados a fim de serem processados, analisados, concatenados com outros dados e depois cuspidos de volta com "replicação de dados". As informações que fazem as vezes da pessoa são constituídas de "dados pessoais" apenas no sentido de que se originam em seu corpo e podem afetar suas oportunidades e escolhas existenciais. A "replicação e fragmentação de dados" tende a inspirar mais confiança que a própria pessoa – que prefere contar sua própria história. Os designers de software dizem que estão simplesmente "lidando com dados", de modo que seu papel é "moralmente neutro" e suas avaliações e distinções são apenas racionais. (BAUMAN, 2014, p.10)

É capciosa a noção de que tais tecnologias podem ser neutras quando, diariamente, são inseridos dados totalmente subjetivos nos algoritmos, depositando exatamente aquilo que nos diferencia das máquinas: a incapacidade de sermos moralmente neutros.

Tratando da ideologia, não é menos interessante a observação de Marilena Chauí – feita em 1981, mas não menos atual, afinal as máquinas são criadas e abastecidas segundo noções ideológicas hegemônicas:

> O que é racionalidade que o discurso ideológico atribui à realidade social e política? É a racionalidade de uma representação. A ideologia é um discurso que se desenvolve sob o modo da afirmação, da determinação, da generalização e da redução das diferenças, da exterioridade face ao objeto (exterioridade que sempre é o ponto de vista do poder, pois o lugar separado, o olhar de sobrevoo do observador impessoal, é a figura do saber como ato de dominação), trazendo a garantia da existência de uma ordem, atual ou virtual. Esse discurso tende sempre para o anonimato ou para a neutralidade, a fim de testemunhar uma verdade que estaria inscrita nas próprias coisas. Discurso anônimo, sem autor e sem produtor, não precisa de suportes humanos através dos quais o real se cria e se recria, pois o mundo está dotado de uma racionalidade que já nem é mais sua, mas a de sua representação. (CHAUÍ, 1981, p.33)

A neutralidade não é argumento novo às ciências sociais, já que, no século XIX, o mundo do Direito era caracterizado pela tentativa de conferir a maior racionalidade possível à Lei, via Escola da Exegese. Com a promulgação do Código Napoleônico, em 1804, Laurent asseverava: "Os códigos nada deixam ao arbítrio do interprete, este não tem mais por missão fazer o direito: o direito está feito. Não existe mais incerteza, porque o direito está escrito nos textos, já há a segurança dos textos [...] (LAURENT *apud* DINIZ, 2009, p.51)".

Se não há jurista que, atualmente, enxergue a Lei como imparcial, também é difícil encontrar quem considere a parcialidade das máquinas. Em outras palavras, o caráter neutro das leis foi transferido às máquinas, não obstante a óbvia contradição decorrente de ambas serem criações humanas. O juiz boca-de-lei da Exegese não tem mais lugar na atualidade, mas o juiz boca-de-*software* já se encontra plena e literalmente conectado a ela. É como Chauí conclui: "Não há mais necessidade de alguém que o pense: ele [o discurso anônimo] está posto aí diante de nós,

como racional em si e por si" (CHAUÍ, 1981, p.33). Era assim na sociedade disciplinar, e é assim na sociedade da informação. Quando a autonomia é delegada, a manipulação é facilitada.

Estigmas e segregação líquidos.

Em princípio, poder-se-ia pensar que, no mundo de pluralismos da "pós-modernidade", todas as formas de vida e de convivência seriam possíveis, sem a necessidade de delimitação racial ou territorial. Todavia, segundo Bauman (1999, p.77), "A essência do estigma é enfatizar a diferença; e uma diferença que está em princípio além do conserto e que justifica, portanto, uma permanente exclusão". E, na sequência, pontua:

> Uma vez que os sinais do estigma são essencialmente irremovíveis, uma categoria só pode deixar de ser estigmatizada se o significante do estigma for reinterpretado como inócuo ou neutro ou se lhe for completamente negada significação semântica e se tornar assim socialmente invisível. Na sociedade moderna há uma constante pressão para fazer exatamente isso. A pressão não pode ser facilmente neutralizada. Ela decorre de atributos bem essenciais e constitutivos da sociedade moderna, como o princípio da igualdade de oportunidades, da liberdade pessoal, da responsabilidade do indivíduo por seu próprio destino — e pode não ser efetivamente cancelada sem contradições e sem gerar novas incongruências. (BAUMAN, 1999, p.78)

Neste ponto, não é apenas a discriminação pela cor da pele e pela raça que condicionam a segregação, mas, similarmente, a falta de capacidade de produção e de consumo de determinados grupos. As pessoas que não se adequam às novas regras do mundo globalizado – sujeitos desempregados e incapazes de consumir – constituem a classe dos refugos, dos descartáveis. No seu livro Vidas Desperdiçadas, Zygmunt Bauman descreve o refugo humano:

> A produção de "refugo humano", ou, mais propriamente, de seres humanos refugados (os "excessivos" e "redundantes", ou seja, os que não puderam ou não quiseram ser reconhecidos ou obter permissão para ficar), é um produto inevitável da modernização, e um acompanhante inseparável da modernidade. É um inescapável efeito colateral da construção da ordem (cada ordem define algumas parcelas da população como "deslocadas", "inaptas" ou "indesejáveis") e do progresso econômico (que não pode ocorrer sem degradar e desvalorizar os modos anteriormente efetivos de "ganhar a vida" e que, portanto, não consegue senão privar seus praticantes dos meios de subsistência) (BAUMAN, 2005, p.12).

No processo de globalização, os refugos são aqueles que seguem para campos de refugiados, os imigrantes ilegais, as vítimas de conflitos internacionais. Ao mesmo tempo que precisam sair de seu território de origem, não conseguem entrar em território distinto. Refugos humanos são, também, aqueles habitantes de bairros problemáticos, ruas perigosas e guetos urbanos, excluídos pela via do depósito nas penitenciárias. Uma metáfora que se ajusta perfeitamente à questão do encarceramento em massa.

Segundo Bauman (2005, p.14), "a florescente indústria da segurança se torna rapidamente um dos principais ramos da produção de refugo e fator fundamental no problema de sua remoção". Para este autor:

> A expansão global da forma de vida moderna liberou e pôs em movimento quantidades enormes e crescentes de seres humanos destituídos de formas e meios de sobrevivência – até então adequados, no sentido tanto biológico quanto social/cultural dessa noção. Para as pressões populacionais daí resultantes – as antigas e familiares pressões colonialistas, só que na direção inversa -, não há escoadouros prontamente disponíveis, seja para a "reciclagem" ou para a "remoção" segura. Daí os alarmes sobre a superpopulação do globo; daí também a nova centralidade dos problemas dos "imigrantes" e das "pessoas em busca de asilo" para a agenda política moderna, e o papel crescente que os vagos e difusos "temores relacionados à segurança" desempenham nas estratégias globais emergentes e na lógica das lutas pelo poder. (BAUMAN, 2005, p.14)

Na modernidade líquida, estigmas e preconceitos se naturalizaram e se institucionalizaram. Indivíduos de determinado perfil étnico e social, quando submetidos aos sistemas de controle e segurança, permanecem em secular desvantagem, perpetrada pelo próprio Estado, ainda detentor do poder de rotular e segregar.

A Sociedade "Segura".

Frente a ausência de controle na qualidade dos dados e a falta de transparência de seus operadores, alguns problemas graves podem surgir quando os algoritmos são aplicados em políticas de segurança pública. David Lyon (*apud* MARCOLINI, 2015) sociólogo e professor, descreve esta condição em apenas uma frase: "Os cidadãos estão cada vez mais transparentes para as grandes organizações, enquanto elas são cada vez menos transparentes". Isso porque o acúmulo desenfreado de dados leva a uma categorização social potencialmente discriminatória, que grande parte da população nem imagina acontecer.

Os Outsiders e o Banóptico.

A rotulação de determinados grupos sociais é tema recorrente, sendo objeto de estudos e pesquisas na área da criminologia e em muitas outras. Por muito tempo tenta-se descrever o perfil do criminoso.

Howard Becker, um sociólogo americano, deu importantes contribuições para a sociologia do desvio. Seus trabalhos buscam explicar a escolha das pessoas que serão categorizadas e quais comportamentos serão considerados desviantes. Para ele, o comportamento desviante ocorre quando os indivíduos se tornam alheios à coletividade por não respeitarem mais as normas sociais.

Para expor o assunto, de forma breve e ilustrativa, convém observarmos a seguinte fala de Becker (2008, p.15):

> Todos os grupos sociais fazem regras e tentam, em certos momentos e em algumas circunstâncias, impô-las. Regras sociais definem situações e tipos de comportamento a elas apropriados, especificando algumas ações como "certas" e proibindo outras como "erradas". Quando uma regra é imposta, a pessoa que presumivelmente a infringiu pode ser vista como um tipo especial, alguém de quem não se espera viver de acordo com as regras estipuladas pelo grupo. Essa pessoa é encarada como um *outsider*.

Então, a criminalidade não seria uma característica intrínseca do sujeito. É uma "etiqueta" atribuída a certas pessoas que a sociedade entende como delinquentes, em setores sociais específicos. Nota-se que estes critérios são utilizados pelo sistema penal no exercício do controle social, rotulando-se os desviantes como "bandidos" ou "criminosos". Ocorre que o aprofundamento de estereótipos relacionados a crimes traz consigo preconceitos e interpelações pré-determinadas, como, por exemplo, a noção de que pessoas da periferia e/ou pretos são mais propensas ao cometimento de crimes.

Cecília Coimbra (2001, p.163), relatando pesquisas realizadas no Rio de Janeiro na década de 90, montou o perfil do criminoso na guerra contra o tráfico: "homem pobre, preto ou pardo, entre 18 e 24 anos, morador de periferia, que não chegou a terminar o primário e é morto em logradouro público". Não significa que pessoas fora deste padrão não trafiquem, mas é fato que "[...] o grau em que um ato será tratado como desviante depende também de quem o comete e de quem se sente prejudicado por ele. Regras tendem a ser aplicadas mais a algumas pessoas que a outras" (BECKER, 2008, p.25).

Na sociedade da informação, por meio da dramatização midiática, o criminoso se torna fonte imediata de perigo e incerteza, necessitando ser reconhecido e neutralizado. E, uma vez identificado pelas características comumente atribuídas aos criminosos, torna-se difícil ao indivíduo dissociar-se da conclusão heterônoma de que ele pertence àquele grupo. Nas palavras do professor Túlio Lima Vianna (2007, p.83):

> Nesta nova sociedade, a monitoração eletrônica pode ser reconhecida como um desenvolvimento tecnológico da antiga vigilância hierárquica, mas o poder punitivo não mais se manifesta por meio de uma sanção normalizadora, mas por um intricado sistema de registro e reconhecimento. Não mais é função social transformar o "anormal" em "normal" nas instituições disciplinares, mas registrar e reconhecer o "anormal" para filtrá-lo da sociedade dos "normais".

Nesse cenário, o estabelecimento da informática como fonte de dados e da biometria como ferramenta de identificação estabeleceu e fortaleceu um novo mecanismo de vigilância: o referenciado banóptico. Por meio de técnicas para elaboração de perfis, torna-se exequível efetuar vigilâncias estritas no espaço transnacional. Inclusive, o banóptico pode ser adaptado e adotado por diversas organizações governamentais, na prática de políticas de segurança pública.

Interessante notar o entendimento exposto, na fala de Bigo (2008, p.44):

> Este dispositivo aparece como uma montagem virtual (morphing) de todas as posições dos indivíduos no processo de fluxo. De uma imagem inicial (do imigrante, dos jovens do gueto) a uma imagem final (do terrorista, do traficante), todos os passos de transformação são reconstituídos virtualmente. Neste sentido, os canais do dispositivo fluem em vez de examinar corpos. Como o dispositivo panóptico, este dispositivo banóptico de "montagens" produz um conhecimento, bem como declarações sobre ameaças e sobre segurança que reforçam a crença na capacidade de decifrar, antes mesmo do próprio indivíduo, quais serão suas trajetórias e seus itinerários. Este dispositivo depende do controle de movimento mais do que o controle da ação em um território (tradução dos autores).[3]

[3] "This dispositif appears like a virtual montage (morphing) of all the positions of individuals in the process of flux. From an initial image (the immigrant, the ghetto youth) to a final image (terrorist, drug-runner), all the steps of transformation are re-constituted virtually. In this respect, this dispositif channels flows instead of dissecting bodies. Like the panopticon

Ocorre que, no Brasil – assim como em vários outros países, sejam mais ou menos desenvolvidos –, a sociedade e as instituições policiais apresentam um comportamento altamente seletivo. Então, quando os algoritmos, alimentados com os dados obtidos diretamente dos cidadãos, buscam prever futuros criminosos, eles podem se provar tendenciosos. A união dos modos de vigilância digitais, ligados ao processo de rotulação de indivíduos, compõe uma ferramenta perigosa de controle social, conforme ilustra o próprio Didier 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 ao 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" (tradução dos autores).[4]

Noutras palavras, a vigilância líquida, que se amolda à vida em movimento, cria ferramentas banópticas, na qual o poder não é mais disciplinar e sim preventivo, de modo a neutralizar reflexos possivelmente negativos antes mesmo das ações que possivelmente os originariam ocorrerem.

Políticas digitais de segurança pública e suas consequências

A garantia da segurança pública é uma das justificativas mais frequentes para o armazenamento e análise dos nossos dados. O crime se espalha, a insegurança parece quase palpável e o escalonamento da violência é inegável. Se é realidade de fato ou projeção insuflada pelo sensacionalismo midiático, não é uma questão a ser abordada por ora, pois o fato é que tanto representantes políticos como magistrados estão, atualmente, tentando promover esta segurança por vias mais reativas e paliativas do que por mudanças estruturais. Mais verbas para construção de presídios e menos investimentos em saúde e educação.

Nesse sentido, vários países, inclusive Brasil e Estados Unidos, tentam conter as ameaças e perigos à sociedade por meio do encarceramento em massa. A taxa de encarceramento nos Estados Unidos, aliás, é a maior do mundo, superando o Brasil, que ocupa a terceira posição no ranking mundial, segundo estimativas do banco de dados *World Prision Brief* (WPB, 2014).

Diante desse fato, a *Sentencing Project*, uma organização sem fins lucrativos com sede em Washington, busca promover reformas na política de justiça criminal americana e defende

dispositif, this banopticon dispositif of morphing produces a knowledge, as well as statements on threats and on security that reinforce the belief in a capacity to decrypt, even prior to the individual himself, what its trajectories, its itineraries will be. This dispositif depends on the control of movement more than the control of stocks in a territory".

[4] "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 behaviors, 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'".

alternativas ao encarceramento em massa (THE SENTENCING PROJECT, 1986). Associadamente, traz à tona um problema grave: a discriminação étnico-racial nos sistemas de justiça criminal.

Os dados americanos da "guerra contra as drogas", por exemplo, apontam disparidades raciais intrigantes. De 1999 a 2005, os afro-americanos representavam, em média, cerca de 13% dos usuários de drogas. Não obstante, corresponderam a 36% das pessoas presas por crimes de drogas e 46% dos condenados por crimes de drogas. Outro estudo, publicado em 2012, examinou o uso de substâncias ilegais entre alunos do ensino secundário nos Estados Unidos, de 1975 até 2011. Tais dados apontaram que os estudantes brancos eram ligeiramente mais propensos ao uso do que os estudantes pretos. No entanto, entre os anos de 1980 e 2010, os jovens pretos foram presos por crimes de drogas em taxas que representaram mais que o dobro dos jovens brancos. De forma complementar, entre 1980 e 2000, a taxa de apreensão de drogas entre pretos nos Estados Unidos subiu de 6,5 a 29,1 por 1.000 pessoas. Durante o mesmo período, a taxa de captura de drogas entre brancos aumentou de 3,5 a 4,6 por 1.000 pessoas (THE SENTENCING PROJECT, 2013).

Para facilitar a identificação de criminosos, surgem novas tecnologias que alegam ser capazes de impor uma vigilância e um controle neutro e objetivo da sociedade, além de antecipar comportamentos indesejados, prevenindo novos crimes. Vale destacar aqui que esses sistemas são, teoricamente, projetados a partir do ponto de vista da responsabilidade, justiça e devido processo legal. Se, no começo do texto, foi proposta a comparação da modernidade sólida para com o clássico de Orwell, agora é possível relacionar o atual estado líquido com "Minority Report – a nova lei", filme dirigido por Steven Spielberg em 2002, no qual o sistema previa e impedia crimes antes de eles se concretizarem.

Uma pesquisa da corporação sem fins lucrativos *ProPublica* (2016) prova como a prevenção de crimes, associada às aplicações tecnológicas de informação, escancara os vieses das ferramentas. A pesquisa examina o funcionamento do algoritmo *COMPAS*, produto da *Northpointe* (empresa com fins lucrativos), que cria pontuações, indicando os riscos de reincidência criminal. O perfil dos réus é traçado por meio de um questionário (O'NEIL, 2016, p.27). Vale apontar que este *software* é dos instrumentos mais utilizados pelos Estados Unidos nesse tipo de avaliação.

Segundo a própria *ProPublica* (2016), foram descobertas disparidades raciais significativas nos resultados apontados pelo computador. São elas:

> Ao prever quem iria reincidir, o algoritmo cometeu erros com os réus brancos e pretos mais ou menos na mesma proporção, mas de maneiras muito diferentes. 1- A fórmula era particularmente suscetível de sinalizar falsamente os réus pretos como futuros criminosos, rotulando-os erroneamente dessa maneira com quase o dobro da taxa dos réus brancos. 2- Os réus brancos foram erroneamente rotulados como de baixo risco com mais frequência do que os réus pretos (tradução dos autores).[5]

Ainda, seguem afirmando que:

> Essa disparidade poderia ser explicada pelos crimes anteriores dos réus ou pelo tipo de crimes pelos quais foram presos? Não. Fizemos um teste estatístico que isolou o efeito raça da história criminal e reincidência, bem como da idade e

[5] "In forecasting who would re-offend, the algorithm made mistakes with black and white defendants at roughly the same rate but in very different ways. 1 – The formula was particularly likely to falsely flag black defendants as future criminals, wrongly labeling them this way at almost twice the rate as White defendants. 2 – White defendants were mislabeled as low risk more often than black defendants".

> sexo dos réus. Os réus pretos ainda tinham 77% mais chances de estarem em risco de cometer um futuro crime violento e 45% mais propensos a cometer um crime futuro de qualquer tipo (tradução dos autores).[6]

Os operadores dos algoritmos transportam a carga de preconceito para o programa. O próprio Tim Brennan, fundador da *Northpointe*, afirma ser difícil "construir uma pontuação que não inclua itens que possam ser correlacionados com a raça – como a pobreza, o desemprego e a marginalização social (tradução dos autores)"[7]. E confirma: "se esses dados são omitidos da sua avaliação de risco, a precisão diminui"[8] (tradução dos autores) (PROOUBLICA, 2016).

Sobre as heteronomias classificatórias, socialmente impositivas, Becker (2008, p.15) assinala:

> Mas a pessoa assim rotulada pode ter uma opinião diferente sobre a questão. Pode não aceitar a regra pela qual está sendo julgada e pode não encarar aqueles que a julgam competentes ou legitimamente autorizados a fazê-lo. Por conseguinte, emerge um segundo significado do termo: aquele que infringe a regra pode pensar que seus juízes são *outsiders*.

Outro programa utilizado nos Estados Unidos, o *PredPol,* é um algoritmo que afirma prever quando e onde ocorrerão os crimes. O objetivo era ajudar a reduzir o viés humano no policiamento. Porém, a mundialmente conhecida organização sem fins lucrativos *Human Rights Data Analysis Group* (LUM, 2016) descobriu que o programa pode direcionar, injustamente, a polícia para certos bairros. Quando os pesquisadores efetuaram a simulação, o programa enviou policiais a bairros com maior proporção de pessoas pertencentes a minorias raciais, independentemente da taxa de criminalidade ali existente.

Um estudo conduzido por Suresh Venkatasubramanian, da Universidade de Utah, demonstrou que, como o programa aprende com os relatórios registrados, o *PredPol* cria um "ciclo de *feedback*" que ampliaria preconceitos (COSSINS, 2018). Os policiais seriam enviados repetidamente para os mesmos bairros, acentuando disparidades e tornando o processo de controle ineficiente.

Para Cathy O'Neil (2016, p.73), mesmo que o *PredPol* não se preocupe em mapear indivíduos (sendo "cego" à raça e etnia), mas sim a geografia (tipos de crimes, localização e ocorrências), o resultado se mantém tendencioso:

> Isso cria um loop de feedback pernicioso. O policiamento gera novos dados, o que justifica mais policiamento. E nossas prisões se enchem de centenas de milhares de pessoas consideradas culpadas de crimes sem vítimas. A maioria deles vem de bairros pobres e a maioria é preta ou hispânica. Portanto, mesmo que um modelo não enxergue cores, o resultado é tudo menos isso. Em nossas cidades amplamente segregadas, a geografia é um substituto altamente eficaz para a raça (tradução dos autores).[9]

[6] "Could this disparity be explained by defendants' prior crimes or the type of crimes they were arrested for? No. We ran a statistical test that isolated the effect of race from criminal history and recidivism, as well as from defendants' age and gender. Black defendants were still 77 percent more likely to be pegged as at higher risk of committing a future violent crime and 45 percent more likely to be predicted to commit a future crime of any kind".

[7] "Brennan said it is difficult to construct a score that doesn't include items that can be correlated with race – such as poverty, joblessness and social marginalization".

[8] "If those are omitted from your risk assessment, accuracy goes down".

[9] "This creates a pernicious feedback loop. The policing itself spawns new data, which justifies more policing. And our prisons

Salienta-se que a predominância de pretos encarcerados não significa que eles, necessariamente, cometam mais crimes que os brancos, mas, sim, que existem elementos transversais à tal conjuntura, como a própria geografia, escolaridade, renda, dentre outros fatores.

No Brasil, durante o carnaval de 2019, no Rio de Janeiro, a empresa de telefonia Oi implantou um sistema de monitoramento com a finalidade de identificar possíveis criminosos em meio a grandes multidões e garantir a segurança pública. Segundo a Polícia Militar do Estado, o funcionamento se deu da seguinte forma:

> 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).

É de extrema relevância ressaltar que a eficácia destas tecnologias é amplamente contestada, apontando como uma das implicações sociais mais importantes a possibilidade de identificar, erroneamente, uma pessoa inocente[10]. Dois pesquisadores do Instituto de Tecnologia de Massachusetts e da Universidade de Stanford, Joy Buolamwini e Timnit Gebru (2018), demonstraram que, quando determinadas raças e gêneros são objetos deste tipo de análise, a margem de erro se mostra muito expressiva. Segundo eles, 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%.

Ainda nesta lógica, Silkie Carlo, diretor do grupo *Big Brother Watch*, evidencia 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. (tradução dos autores) (BURGESS, 2018, s/p).[11]

Recentemente, a cidade de São Francisco (EUA), representada pela Câmara de Supervisores, decidiu proibir a utilização do reconhecimento facial como ferramenta de identificação de criminosos por entidades governamentais (LEE, 2019, s/p). Segundo Matt Cagle da *American Civil Liberties Union* no norte da Califórnia: "Com esta votação, São Francisco declarou que a tecnologia de vigilância facial é incompatível com uma democracia saudável e que os residentes merecem

fill up with hundreds of thousands of people found guilty of victimless crimes. Most of them come from impoverished neighborhoods, and most are black or Hispanic. So even if a model is color blind, the result of it is anything but. In our largely segregated cities, geography is a highly effective proxy for race".

[10] Através do sistema de reconhecimento facial implantado pela Polícia Militar, em Copacabana, no Rio de Janeiro, uma mulher foi detida por engano. Ela foi confundida com uma foragida da Justiça. Segundo a Polícia Militar, "pelo princípio da presunção da inocência e como em qualquer ação policial, reforçamos o compromisso com o total respeito às garantias constitucionais de todos os cidadãos". (RIO, 2019)

[11] "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".

uma voz nas decisões sobre vigilância de alta tecnologia"[12] (tradução dos autores) (LEE, 2019, s/p). Enquanto alguns argumentos destacam que tal decisão prejudicará o combate ao crime, outros reconhecem que a tecnologia está sujeita a erros, violando a privacidade e a liberdade dos indivíduos.

Diante desta conjuntura cada vez mais tecnológica – e menos humana –Cathy O'Neil (2016, p.26), sabiamente, questiona:

> A questão, no entanto, é se eliminamos o preconceito humano ou simplesmente o camuflamos com a tecnologia. Os novos modelos de reincidência são complicados e matemáticos. Mas, dentro desses modelos, há uma série de suposições, algumas delas prejudiciais (tradução dos autores).[13]

Ao invés de servirem apenas como suporte, tais algoritmos tomam decisões finais complexas, em domínios como a justiça criminal. E, tal como a neutralidade, a objetividade e a transparência tornam-se meramente um discurso político falacioso, restando ao sujeito se resignar e aceitar o que diz o computador.

Acertadamente, o presidente da Microsoft, Brad Smith (2018), assevera 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)

Em suma, as tecnologias tornam explícitos os problemas sociais que a sociedade ainda precisa combater de modo que seu uso consciente deve estar vinculado a princípios como reponsabilidade e não discriminação.

Por fim, a discussão ora proposta pode ser do seguinte modo sintetizada, segundo Bauman (2014, p.10):

> Assim, até que ponto a noção de modernidade líquida – e, aqui, de vigilância líquida – nos ajuda a entender o que está ocorrendo no mundo de monitoramento, rastreamento, localização, classificação e observação sistemática que é a vigilância? A resposta simples, em uma só palavra, é "contexto". É fácil interpretar a difusão da vigilância como fenômeno tecnológico ou como algo que lida simplesmente com "controle social" e "Grande irmão". Mas isso é colocar toda ênfase em instrumentos e tiranos, e ignorar o espírito que anima a vigilância; as ideologias que a impulsionam; os eventos que a possibilitam; e as pessoas comuns que concordam com ela, a questionam ou decidem que, se não podem vencê-la, é melhor juntarem-se a ela.

Sem o devido direito ao contraditório, uma vez que o público alvo não tem a chance de auditar ou debater o uso de tais mecanismos, é de se imaginar que a grande maioria da população

[12] "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".

[13] "The question, however, is whether we've eliminated human bias or simply camouflaged it with technology. The new recidivism models are complicated and mathematical. But embedded within these models are a host of assumptions, some of them prejudicial".

sequer pensa nas possibilidades sugeridas pelo sociológico, de vencer ou mesmo questionar a vigilância virtual. E, neste sentido, torna-se igualmente difícil antever um futuro menos vigiado.

Considerações finais

Há fatos da realidade hodierna que não podem ser desconsiderados: inúmeros países recebem refugiados diariamente; várias nações passam por crises carcerárias, nas quais a superlotação é apenas uma das adversidades; no Brasil, os estados do Rio de Janeiro e Roraima passam por generalizadas crises de segurança, que contam com a paliativa resposta das intervenções federais. Antigas ferramentas de segurança não parecem ser mais eficazes. E é natural que ideias sejam esquecidas, modifiquem-se, voltem a ganhar força, reapareçam em outro contexto e sejam readaptadas.

Assim, novas formas de promoção da segurança pública acabam surgindo. Destacam-se as medidas que permitem a elaboração de tendências e comportamentos, para possíveis eventos criminosos e a análise facial, capaz de diferenciar e identificar pessoas em multidões. Essas automatizações contribuem para a construção de cidades cada vez mais inteligentes, otimizando o trabalho de agentes de segurança.

Porém parecem não se descolar dos preconceitos e modelos de segregação já estruturais, sistêmicos e institucionalizados. George Orwell provavelmente ficaria assustado ao constatar que seus maiores temores estão se tornando realidade. Diversos países já utilizam de modelos de vigilância associados a algoritmos de previsão e contenção de crimes, trazendo consequências nem sempre eficazes na prevenção de crimes, mas muito certeiras na propagação de preconceitos, agora blindados pela suposta neutralidade das máquinas e dos algoritmos.

Dados objetivos dos matemáticos e estatísticos não são facilmente refutados, ou mesmo questionados, como são as conclusões subjetivas dos historiadores e sociólogos. Assim, enquanto estes são vistos com desconfiança, aqueles têm liberdade para exercerem suas atividades, inclusive aplicando-as sobre ferramentas cibernéticas cujos resultados serão analisados por aqueles cientistas sociais. Resultados estes que, por sua vez, serão refutados por cidadãos desejosos de uma neutralidade impossível de ser atingida – o que não significa que a transparência padeça do mesmo fim. As sociedades e seus cidadãos, que serão avaliados pelas máquinas, têm o direito de ser informados sobre quais dados serão coletados e quais critérios servirão à análise daqueles. É necessário aumentar a transparência e a auditabilidade dos sistemas, protegendo direitos e liberdades individuais e coibindo o uso abusivo dos mecanismos de segurança.

Ressalta-se, porém, que a discussão exposta neste trabalho não representa uma tentativa reacionária de frear o desenvolvimento tecnológico. O problema não são as novas tecnologias de inteligência artificial em si, mas, antes, as ações de seus operadores. A internet deixa de ser gratuita na medida em que os usuários cedem seus dados pessoais, e este processo de geração de informações, por vezes inconsciente, não nos permite dimensionar as suas implicações.

Em suma, o uso das tecnologias não deve pautar-se apenas na proteção do indivíduo, mas também em valores éticos, minimamente justos, regulamentados por uma legislação humanista e garantista, voltada sempre para o bem-estar social.

Referências

BALDWIN-RAGAVEN, Laurel; LONDON, Lesley; DU GRUCHY, Jeanelle. **An ambulance of the wrong colour:** health professionals, human rights and ethics in South Africa. Juta and Company Limited. 1999, p.18,

BARROS, Carlos Juliano. **Algoritmos das rede sociais promovem preconceito e desigualdade, diz matemática de Harvard. 24 de dezembro de 2017.** Disponível em: <https://www.bbc.com/portuguese/geral-42398331>. Acesso em: 11 nov. 2018.

BAUMAN, Zygmunt. **Modernidade e Ambivalência**. Rio de Janeiro: Editora Jorge Zahar. 1999.

BAUMAN, Zygmunt. **Vidas Desperdiçadas**. Rio de Janeiro: Editora Jorge Zahar. 2005.

BAUMAN, Zygmunt. **Vigilância Líquida**. Rio de Janeiro: Editora Jorge Zahar. 2014.

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

BENTHAM, Jeremy. **O Panóptico**. 2. Ed., Belo Horizonte: Autêntica Editora, 2008.

BIGO, Didier. Globalized (In)Security: The field and the Ban-Opticon. In: BIGO, Didier; TSOUKALA, Anastassia. **Illiberal practices of liberal regimes**: the (in)security games. Nova Iorque: Routledg, 2008. p.5-45.

BIGO, Didier. Security, exception, ban and surveillance. In: LYON, David (org.). **Theorizing Surveillance:** The panopticon and beyond. Portland: Willan Publishing, 2006. p.46-68.

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.

CASTELLS, Manuel. **A Sociedade em Rede**. 8.ed., Editora Paz e Terra, 1999.

CHAUÍ, Marilena de Sousa. **Cultura e democracia:** o discurso competente e outras falas. 2.ed., São Paulo: Editora Moderna, 1981.

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.

COSSINS, Daniel. **Discriminating algorithms: 5 times AI showed prejudice**: artificial intelligence is supposed to make life easier for us all - but it is also prone to amplify sexist and racist biases from the real world read more. 2018. Disponível em: <https://www.newscientist.com/article/2166207-discriminating-algorithms-5-times-ai-showed-prejudice/>. Acesso em: 10 jan. 2019.

DINIZ, Maria Helena. **Compêndio de introdução à ciência do Direito.** 20.ed. São Paulo: Editora Saraiva, 2009.

DUPAS, Gilberto. Ética e Poder na Sociedade da Informação. 2.ed., São Paulo: Editora UNESP, 2001.

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

HAN, Byung-Chul. **Psicopolítica:** o neoliberalismo e as novas técnicas de poder. Belo Horizonte: Editora Âyiné, 2018.

HOSIE, Robin. **Memórias do Século XX:** Vol. 1 – O Surgimento da Era Moderna. Rio de Janeiro: Reader's Digest, 2004.

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.

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

LYON, David. **Surveillance Studies Centre.** Disponível em: <http://www.sscqueens.org>. Acesso em: 11 nov. 2018.

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

MARCOLINI, Barbara. **David Lyon, sociólogo:** 'A vigilância hoje é parte de nós'. 13 de maio de 2015. Disponível em: <https://oglobo.globo.com/sociedade/conte-algo-que-nao-sei/david-lyon-sociologo-vigilancia-hoje-parte-de-nos-16143232>. Acesso em: 11 nov. 2018.

ONU/BR. **Brasil é o quarto país com mais usuários de Internet do mundo, diz relatório da ONU. 03 outubro de 2017.** Disponível em: <https://nacoesunidas.org/brasil-e-o-quarto-pais-com-mais-usuarios-de-internet-do-mundo-diz-relatorio-da-onu/>. Acesso em: 11 nov. 2018.

O'NEIL, Cathy. **Weapons of Math Destruction:** How Big Data Increases Inequality and Threatens Democracy. New York: Crown, 2016.

ORWELL, Geroge. **1984**. 36.ed., São Paulo: Companhia das Letras, 2017.

PARISER, Eli. **O filtro invisível: o que a internet está escondendo de você**. Trad. Diego Alfaro. Rio de Janeiro: Zahar, 2012.

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. 26 de maio de 2016. Disponível em: <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>. Acesso em: 15 nov. 2018.

RIO, G1. **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.. 2019. Disponível em: <https://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: 29 jul. 2019.

SCHELLING, Thomas C.. **Models of segregation**, The American Economic Review, Washington, v. 59, n. 2, 1969, p.488-493.

SCURO NETO, Pedro. **Sociologia Geral e Jurídica**, 7. ed. São Paulo: Saraiva, 2010.

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.

SMITH, Megan; PATIL, Dj; MUÑOZ, Cecilia. **Big Risks, Big Opportunities: the Intersection of Big Data and Civil Rights. 04 de maio de 2016.** Disponível em: <https://obamawhitehouse.archives.gov/blog/2016/05/04/big-risks-big-opportunities-intersection-big-data-and-civil-rights>. Acesso em: 9 jan. 2019.

SSP-SP. Secretaria da Segurança Pública de São Paulo. **Ações de Segurança:** Mapa de crimes. 17 de abril de 2014. Disponível em: <http://www.ssp.sp.gov.br/acoes/leAcoes.aspx?id=33833>. Acesso em: 15 fev. 2019.

THE SENTENCING PROJECT. **About The Sentencing Project.** 1986. Disponível em: <https://www.sentencingproject.org/about-us/>. Acesso em: 07 jan. 2019.

THE SENTENCING PROJECT. **Shadow Report to the United Nations on Racial Disparities in the United States Criminal Justice System.** 2013. Disponível em: <https://www.sentencingproject.org/publications/shadow-report-to-the-united-nations-human-rights-committee-regarding-racial-disparities-in-the-united-states-criminal-justice-system/>.Acesso em: 07 jan. 2019.

VIANNA, Túlio Lima. **Transparência Pública, Opacidade Privada:** O Direito como instrumento de limitação do poder na sociedade de controle. Rio de Janeiro: Editora Revan, 2007.

VIEIRA, Tatiana Malta. **O Direito à privacidade na sociedade da informação: efetividade desse direito fundamental diante dos avanços da tecnologia da informação**. Porto Alegre: Sergio Antônio Fabris Editor, 2007.

WPB. **World Prison Brief data: United States of America.** Disponível em: <http://www.prisonstudies.org/highest-to-lowest/prison-population-total?field_region_taxonomy_tid=All>. 2014. Acesso em: 7 jan. 2019.

YANARDAG, Pinar; CEBRIAN, Manuel; RAHWAN, Iyad. **Norman, world's first psychopath AI.** Abril de 2018. Disponível em: <http://norman-ai.mit.edu>. Acesso em: 11 nov. 2018.