

CONTROLE SOCIAL E NOVAS TECNOLOGIAS: POR UM DEBATE ÉTICO

SOCIAL CONTROL AND NEW TECHNOLOGIES: FOR AN ETHICAL DEBATE

Assista aos
comentários da
autora sobre o
artigo



MARINA LIMA FERREIRA

Doutoranda em Direito Penal pela Faculdade de Direito da Universidade de São Paulo (USP). Mestre em Direito Penal pela mesma instituição (2020). Dupla-Graduação em Direito pela *Université de Lyon II*, França (2017). Bacharel em Direito pela USP (2015). Associada ao Instituto Brasileiro de Ciências Criminais (IBCCRIM) e ao Instituto de Defesa do Direito de Defesa (IDDD). Advogada em São Paulo (SP).

Lattes: [<http://lattes.cnpq.br/0455529435916299>].

ORCID: [<https://orcid.org/0000-0002-3104-9363>].

marina.lima.ferreira@usp.br

FERNANDO BOUSSO

Mestre em *Computer and Communications Law* pela *Queen Mary, University of London* (2015).

Bacharel em Direito pela Universidade Presbiteriana Mackenzie (2011). Membro do Comitê Jurídico e de Proteção de Dados do IAB Brasil – *Internet Advertising Bureau*. Membro atuante da *International Association of Privacy Professionals* (IAPP). Advogado em São Paulo (SP).

Lattes: [<http://lattes.cnpq.br/6645254699696450>].

ORCID: [<https://orcid.org/0000-0002-2183-9185>].

febousso@gmail.com

DOI: [<https://doi.org/10.54415/rbccrim.v193i193.323>].

Recebido em: 30.03.2021

Aprovado em: 20.07.2021

Última versão dos autores: 29.07.2021

ÁREAS DO DIREITO: Penal; Digital

RESUMO: Tendo em vista o largo desenvolvimento tecnológico das últimas décadas, o atuarialismo reinante ante a gestão de setores sociais de risco e o emprego maciço de técnicas de inteligência artificial para fins de controle, especialmente, penal, o presente artigo sustenta que, malgrado a evolução legislativa brasileira em matéria de privacidade e proteção de dados pessoais, não se pode prescindir da crítica à expansão da teia de controle, particularmente perigosa quando

ABSTRACT: Taking into account the broad technological development of the last decades, the reigning actuarialism before the management of high risk social groups, and the increasingly massive use of artificial intelligence techniques for control purposes, especially criminal control, the present paper argues that, despite the Brazilian legislative evolution in matters of privacy and data protection, it is essential to criticize the expansion of the web of control, which is

colocados em tela anseios tão arraigados quanto aquele da segurança a (quase) qualquer custo. Ainda, esta análise pretende demonstrar que são vários – e, talvez, irremediáveis – os riscos e problemas inerentes à banalização da inteligência artificial como técnica de controle, mormente no que diz respeito aos danos decorrentes da falta de transparência; à ilusão de eficiência vinculada a técnicas de predição; à problemática dos vieses algorítmicos e da discriminação; e à questão da seletividade – própria do sistema penal e potencializada pelas máquinas –, bem como de todos os seus efeitos adversos, sobretudo, no que se refere ao alargamento das distorções do sistema carcerário brasileiro e à incapacitação, no limite, de comunidades inteiras, sem que haja prevenção real da criminalidade de fato. Torna-se urgente, neste sentido, um debate ético.

PALAVRAS-CHAVE: Controle social – Atuarialismo – Privacidade – Inteligência artificial – Seletividade penal.

particularly dangerous when deep-rooted desires as security at (almost) any cost are put into question. Furthermore, this analysis intends to demonstrate that there are several – and, perhaps, unavoidable – risks and issues inherent to the trivialization of artificial intelligence as a control technique, especially with regard to damages resulting from the lack of transparency; to the illusion of efficiency linked to prediction techniques; to the problem of algorithmic biases and discrimination; and the issue of selectivity – inherent to the criminal system and enhanced by machines – as well as all of its secondary effects, especially regarding the widening of distortions in the Brazilian prison system and the incapacitation, at the limit, of entire communities, without any real prevention of actual criminality. In this sense, an ethical debate becomes urgent.

KEYWORDS: Social control – Actuarialism – Privacy – Artificial intelligence – Criminal selectivity.

SUMÁRIO: 1. Introdução. 2. Atuarialismo e segurança: questões preliminares. 2.1. Noções de privacidade, proteção de dados e impactos em matéria penal. 3. Crítica à banalização da inteligência artificial como técnica de controle. 3.1. A problemática da transparência e a demanda por parâmetros de inteligência artificial explicáveis. 3.2. Análise criminal e a ilusão de eficiência. 3.3. Reconhecimento facial, predição e gestão diferencial de pessoas: falsos-positivos e falsos-negativos. 3.4. Isomorfia da patrulha: automatizada, mas tão seletiva quanto sempre foi. 4. Da urgência de um debate ético: privacidade e segurança – a quem se destinam?. 5. Considerações finais. 6. Referências. Referências da internet.

1. INTRODUÇÃO

O ato de governar implica a disposição de coisas de que se assume o encargo, com o fim de conduzi-las, a partir de táticas de controle, a um fim que seja conveniente. Como em Foucault (2012, p. 429), o governo, em sua forma política, exerce-se de forma complexa sobre a população, a partir de instituições, procedimentos, análises, cálculos e tecnologias, sendo os dispositivos de segurança, nesse sentido, os seus instrumentos técnicos essenciais – por vezes, tão fluídos e silenciosos que sequer se fazem notar pelos próprios alvos do seu controle.

Em se tratando deste controle social, por sua vez, pode-se defini-lo como um conjunto de sistemas normativos – dentre eles, o direito – aptos a estabelecerem

uma rede de contenções que, mesmo quando invisível, garante a fidelidade da população aos valores de um dado sistema de dominação e, por consequência, a estabilidade do próprio sistema. A população, contudo, é demasiado vasta para que o controle se infiltre de maneira equalizada: não à toa e nunca inocentemente, os destinatários sociais do governo são diferentemente manejados (CASTRO, 2005, p. 50 e ss.).

Historicamente, essa gestão diferencial de pessoas se conecta diretamente à raça e à classe a que pertencem, constatação essa que pode ser observada, por exemplo, ao se analisar a emergência e o desenvolvimento, no Brasil e no mundo, de uma das táticas de controle mais bem assimiladas da modernidade: a prisão. Do aprisionamento para “correção” de escravos e negros alforriados, “agitadores” e pobres em geral – alicerçado em juízos de periculosidade altamente associados à sua existência em si mesma –, ao grande encarceramento das últimas décadas, pode-se dizer que o controle social do delito foi e segue fundado, em suas políticas de vigilância e contenção, sobre bases classistas, racistas e discriminatórias¹: não por menos, o cárcere brasileiro é majoritariamente pobre e, no mínimo, 61,7% negro², apesar de apenas 54% da população nacional ser identificada como tal³.

Não se pretende resumir a complexidade dessa análise, contudo, a esta breve menção introdutória. O que se sustenta desde já, por outro lado – e que se demonstrará nas páginas seguintes –, é que uma perspectiva histórica do controle social, especialmente da sua faceta formal, implica reconhecer que as suas táticas são enviesadas desde a raiz e que, em seu desenvolvimento, tendem muitas vezes a manter a sua função, apesar de distinto o seu formato; e, nesta linha, vale dizer, é fato que o controle social vem assumindo formas cada vez mais difusas, possibilitadas pelo intenso avanço tecnológico das últimas décadas.

1. Há farta bibliografia a esse respeito, de modo geral, no que se refere ao desvelamento das legitimações ideológicas historicamente atribuídas à pena – vide BARATTA (2011), MELOSSI; PAVARINI (2010) e RUSCHE; KIRCHHEIMER (2004), dentre outros; e, mais especificamente, sobre o surgimento da criminologia e do cárcere no Brasil – vide ALVAREZ (2003), BATISTA (2006), SALLA (1999) e SANTOS (1979), dentre outros.
2. Dados disponibilizados pelo Infopen – Levantamento Nacional de Informações Penitenciárias (atualizados até junho de 2018). Disponível em: [https://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-permanentes/cdhm/noticias/sistema-carcerario-brasileiro-negros-e-pobres-na-prisao]. Acesso em: 23.03.2021.
3. Dados disponibilizados pelo IBGE – Instituto Brasileiro de Geografia e Estatística. Disponível em: [https://jornal.usp.br/radio-usp/dados-do-ibge-mostram-que-54-da-populacao-brasileira-e-negra/]. Acesso em: 24.03.2021.

A população se vê observada o tempo todo, sem que saiba ao certo por quem e por quais motivos: trata-se da era digital. Mas não só: no específico campo do controle social – e do controle social do delito –, são inúmeras as novas tecnologias que se aproveitam (para além da mera observância) da chamada *lógica atuarial*, baseada na “predição”, a partir de representações probabilísticas, e apta a sustentar um cenário de contenção de grupos sociais inteiros, considerados de *alto risco*, segundo um regime de “desconfiança universal” (DE GIORGI, 2006, p. 100)⁴.

Para tanto, muitos são os métodos já aplicados, especialmente em países centrais. Desde técnicas de mapeamento e análise criminal, até *softwares* sofisticados e não menos controversos, como a tecnologia de análise criminal da *PredPol*, estadunidense, bem como a gigante chinesa da inteligência artificial aplicada à vigilância, a *Dahua* – ambas, vale dizer, já altamente questionadas por potenciais vieses intrínsecos e tendências preconceituosas, mormente no que se relaciona à raça e etnia⁵.

No caso do Brasil, já há alguns anos são desenvolvidos mecanismos baseados em ciências de dados e inteligência artificial, como as plataformas *CrimAnalyzer* e outra, mais recente, chamada *Mirante*, ambas concebidas pelo Centro de Ciências Matemáticas Aplicadas à Indústria (CeMEAI), em parceria com o Núcleo de Estudos da Violência (NEV), em São Paulo⁶. Para além do controle do delito em si, já se tem notícia, igualmente, de iniciativas de reconhecimento facial levadas a cabo por empresas de transporte, varejo e pelo setor bancário, a exemplos do Metrô de São Paulo, da loja Hering e do Banco Itaú (FRAGOSO; ROBERTO; SIMÃO, 2020, p. 22). Some-se a isso, ainda, o aparente interesse governamental pela introdução de técnicas similares no âmbito da segurança pública, com viagens patrocinadas à já mencionada (e ultraviçada) China, realizadas por alguns parlamentares brasileiros no ano de 2019, com o intuito específico de conhecer o sistema de reconhecimento facial chinês⁷.

4. Neste sentido, vide também DIETER (2012).

5. Vide as matérias de CHANG (2018) e BURT (2021). Disponíveis em: [<https://www.latimes.com/local/lanow/la-me-lapd-data-policing-20180724-story.html>]; e [<https://www.biometricupdate.com/202102/investigation-reveals-dahua-biometric-systems-sent-ethnicity-warnings-to-chinese-police>]. Acesso em: 28.03.2021.

6. Disponível em: [<https://agencia.fapesp.br/sistema-usa-inteligencia-artificial-para-prever-ocorrencias-de-crimes-em-areas-urbanas/33768/>]. Acesso em: 25.03.2021.

7. Disponível em: [<https://www1.folha.uol.com.br/mercado/2019/01/bancada-do-psl-vai-a-china-importar-sistema-que-reconhece-rostos-de-cidadaos.shtml>]. Acesso em: 24.03.2021.

Para além das táticas de controle em si, é verdade que o ambiente tecnológico e os impactos da digitalização do mundo nunca estiveram tão em voga no cenário nacional e internacional. A privacidade é a salvaguarda da vez; dados, em seu turno, um capital tão valioso quanto as pessoas que com eles se confundem. Não à toa, tais temas vêm sendo objeto de diferentes normas na última década, culminando na recente Lei Geral de Proteção de Dados Pessoais brasileira, aprovada em 2018 e em vigor desde setembro de 2020, consagrada como o grande diploma legal dos anos recentes.

Há quem diga, no entanto, que é preciso abrir mão de parcelas dos direitos à intimidade, à vida privada e à proteção de dados pessoais em prol da segurança de *todos* – como se existisse algo coeso o bastante quanto uma sociedade apta a ser protegida, de forma igualitária, em sua totalidade –, e que o emprego de recursos tecnológicos, para tanto, seria irrestrito e necessariamente bem-vindo. A introdução ilimitada e potencialmente irresponsável de tecnologias de observação, coleta, processamento de dados e governo de pessoas, todavia, particularmente no campo do controle social do delito, engloba uma série de riscos que serão esmiuçados na crítica a seguir – e que, acredita-se, vitimam grupos populacionais de forma desigual. Como se verá, a problemática vai muito além do discurso vulgar de *gestão eficiente*: trata-se de um embate direto, recheado de entraves éticos, entre privacidade, proteção de dados, segurança e, por que não, liberdade.

2. ATUARIALISMO E SEGURANÇA: QUESTÕES PRELIMINARES

É real a era das grandes metrópoles, da produção em larga escala, da informatização dos processos produtivos, das formas de trabalho e da própria vida privada, em níveis muito acentuados; ao mesmo tempo, a *multidão* é também uma realidade, assim como todas as questões a ela associadas – a expansão dos bolsões de pobreza, o desemprego, a maior disseminação de enfermidades em nível global, a criminalidade, dentre tantas outras, todas mais ou menos acentuadas pelas tendências consolidadoras do paradigma digital.

Trata-se de uma sociedade lastreada em risco e que, portanto, ambiciona como nunca antes o desenvolvimento de técnicas de “predição do futuro” propriamente dito. Mais que isso: se o governo do excesso é a prioridade, a definição das “melhores” estratégias de controle não se sustenta tão somente por análises de risco abstrato, mas sim, pela vigilância e pelo manejo de categorias inteiras de indivíduos consideradas de *alto risco*. Aqui se perfaz o *atuarialismo* enquanto técnica: monetiza-se o risco (tal como a lógica econômica típica das empresas de seguro) e vende-se gestão do perigo, materializado naquelas populações consideradas *problemáticas* e que, por isso, devem ser alvos preferenciais do gerenciamento.

Nessa esteira, as novas (nem tão novas) estratégias de controle – penal, principalmente, mas não só – passam a se caracterizar cada vez mais como dispositivos de administração de risco e, por conseguinte, de “repressão preventiva” dos grupos sociais considerados portadores desse risco. Não se trata mais, assim, de neutralização de fatores de *periculosidade* individual, tal como sustentado pela etiologia positivista, por exemplo, mas sim, de regulação social e contenção de populações em sua integralidade. Racionalidade, portanto, atuarial – e não disciplinar exclusivamente (DE GIORGI, 2006, p. 97).

Logo, no atuarialismo, o saber sobre o sujeito se torna quase irrelevante frente à construção e hierarquização da multidão em categorias, estruturadas sobre fluxos de informações e elaborações artificiais, como agregados estatísticos e probabilidades. A cidade acaba por se transformar, destarte, sob a racionalidade gerencial de controle de riscos pelo melhor “custo-benefício”, em um grande aparato de captura de dados e vigilância de populações observáveis à distância, e que se movimentam em uma verdadeira dança de inclusão e exclusão. A partir do seu *status* perante a ordem, permite-se ou restringe-se o acesso a determinadas áreas (centros comerciais, restaurantes, aeroportos, condomínios fechados, parques etc.), segmentação essa possibilitada por uma efetiva ecologia do medo: para parte da população, as barreiras, simbólicas ou não, são lidas como “aqui não se pode entrar”; para outra parte, como “daqui não se pode sair” (DE GIORGI, 2006, pp. 103-105).

Não é de se espantar que as mesmas forças que se alimentam da produção do medo criem, elas mesmas, demandas por mais controle – ainda que o ideal de segurança venha de encontro a direitos fundamentais da personalidade. Câmeras de circuito fechado, torres direcionais captadoras de movimentos e sons, instrumentos de detecção biométrica, ferramentas de reconhecimento facial (já aplicadas a telefones celulares, por exemplo); todas essas táticas – e muitas outras – contribuem para o agrupamento de “fragmentos factuais” (DE GIORGI, 2006, p. 102) que, ademais do manejo de grupos sociais *per se*, constroem eles mesmos, a partir de suas múltiplas conexões, o que se entende por categorias perigosas.

De onde se tem que o perigo não é ontológico, mas sim, edificado conforme os ditames da ordem. A rede se amplia para suprir a expectativa de regulação dos níveis de desvio, que não se volta, frise-se, para respostas a condutas individualizadas, necessariamente, mas, sim, para a definição ampla e categórica de determinados grupos, de modo que sejam estes “acomodados” nas rubricas corretas – a partir de testes de risco que pouco ou nada têm a ver com quaisquer dimensões materiais, senão morais (HARCOURT, 2007, pp. 180-181).

Ainda de acordo com a orientação econômica, o grande desafio dos governos se torna, a partir do balizamento entre privacidade e segurança (salvaguardadas

de maneira diferencial para uns e outros), maximizar o “bem-estar público” por meio do suposto aumento da sua capacidade de predição, detecção e prevenção de conflitos, desde que com o menor esforço e, principalmente, com o menor gasto possível. A tentação da eficiência é uma realidade – ainda que isso exija a colocação de estratos gerais e determinados de pessoas sob suspeita; o que explica, em boa parte, a seletividade como a base dos sistemas de gerenciamento de risco (YOUNG, 1998, p. 76). São muitos “criminosos em potencial” espalhados por áreas esparsas; ao controle social, então, cabe a seleção daqueles *perigosos* ou que, sobretudo, indiquem uma ameaça de perigo. A alegada necessidade de cobertura irrestrita de todo esse conjunto, por fim, acaba sendo o subterfúgio perfeito para a imersão do controle em *tecnologia*, em todos os seus formatos e usos, em toda a sua forma e estética; e, ainda mais importante, torna-se imprescindível o desenvolvimento e a aplicação de tecnologias da informação.

Se a tecnologia, tomada de forma ampla, pode ser definida como um meio particular, complexo e quase mágico de realização de certos fins, a tecnologia da informação, por sua vez, especializa-se na ingestão, manipulação, modelagem e estocagem de dados os mais multifacetados, transformando-os via códigos, formatos, *software* e *hardware*, e produzindo, em seguida, interpretações do mundo exterior expressas por telas, arquivos, imagens e sons (MANNING, 2008, pp. 63-67). A tecnologia da informação tem lastro e, dessa maneira, é sempre reflexiva – ou seja, converte matéria crua em resultados processados, para fins visíveis ou, o que é mais grave, nem sempre tão visíveis assim.

Tecnologias da informação são, por isso, muito dificilmente avaliadas – afinal, tanto o seu alimento quanto o seu produto se constituem por símbolos complexos que, no entanto, geram efeitos práticos na realidade. Ora, símbolos são modeláveis: para fins do emprego da tecnologia com o objetivo de seleção de alvos de controle, por exemplo, há que se, justamente, pré-determiná-los como tal; daí que, ainda que se queira sustentar que a tecnologia se constitui, do topo de sua autoridade, como uma variável neutra e independente, tem-se, de fato, uma relação de dependência pura do seu entorno.

Em comparação a outras ferramentas, contudo, a tecnologia se celebra na era digital como a mais elevada fonte de conhecimento, conquistado ao menor custo e, há quem acredite, de forma desinteressada. Situa-se como o verdadeiro elixir da eficiência e como uma *racionalidade*⁸ por si só, que dispensa explicações sobre o seu funcionamento. Para muitos, ela é o que é: um mero comunicador da

8. Tomado o conceito de racionalidade, em tradução livre, como uma “explicação do porquê de determinada ação” (MANNING, 2008, p. 6).

realidade – sem dúvida o melhor discurso possível a ser incorporado por agências de segurança e justiça. Afinal, quanto mais pretensamente objetivas, tecnológicas e, por isso, racionais, menos tais agências aparentam qualquer submissão a uma ordem específica.

Tendo em vista os referidos propósitos – processamento facilitado de informações, junto a uma seleção rápida, barata e pretensamente neutra de alvos –, polícia, justiça e administração como um todo se muniram de tecnologia; e, para fins desta análise, particularmente focada no controle social do delito, duas são as mais relevantes: as chamadas técnicas de (i) análise criminal (do inglês, *crime analysis*); e de (ii) reconhecimento facial. Antes mesmo do destrinchamento e da consequente crítica à banalização destes métodos, porém, passa-se a uma breve exposição sobre o tratamento da privacidade no contexto do mais recente enquadramento jurídico brasileiro relativo à proteção de dados, a supramencionada Lei Geral de Proteção de Dados Pessoais (LGPD), e eventuais impactos desta discussão sobre a seara penal.

2.1. *Noções de privacidade, proteção de dados e impactos em matéria penal*

Tanto a ideia de privacidade quanto a percepção dos danos associados à sua violação evoluíram significativamente ao longo do tempo, sendo certo que o entendimento de que tal direito se acosta ao controle (do indivíduo) sobre as informações pessoais surgiu, particularmente, em resposta aos desenvolvimentos tecnológicos. Por esse motivo, parece existir uma certa confusão entre os termos “privacidade” e “proteção de dados”, frequentemente usados como sinônimos. Veja-se que, se no ambiente europeu a proteção de dados parece ter se estabelecido como matéria bastante autônoma da privacidade, nos Estados Unidos, por outro lado, a doutrina se manteve restrita aos termos “privacidade informacional” ou apenas “privacidade”, tornando o contorno dos conceitos ainda mais desalumiado (KOUTSIAS, 2012, pp. 265-266).

Embora esta análise não vise abordar tais diferenças conceituais, tampouco analisar no detalhe a evolução histórica das discussões doutrinárias e legislativas que catapultaram o direito à privacidade, até o estabelecimento de um quadro regulatório de proteção de dados pessoais, parece importante, de toda sorte, compreender que se trata de conceitos ligados, mas de espectros bastante distintos – em especial, no contexto de uso de dados pelo Estado e, particularmente, para fins de controle social.

Inicialmente, a definição clássica do direito à privacidade esteve bastante ligada à concepção de isolamento social, ou seja, da manutenção de um círculo

privado em que o indivíduo poderia viver a sua vida como bem entendesse, sem qualquer interferência – conforme exploraram Warren e Brandeis, ainda em 1890, no famoso artigo *The Right to Privacy* (WARREN; BRANDEIS, 1890, pp. 193-220), em que se vinculou o conceito de privacidade ao “direito de ser deixado só”. Uma série de fatores, incluindo o aumento no fluxo informacional, a facilidade de se estabelecer mecanismos de processamento ocultos e a extração de valor das informações pessoais, contudo, contribuíram para a ocorrência de um desvio significativo das demandas relacionadas à privacidade. Afinal, o caráter individualista do “direito de ser deixado só” não seria suficiente para proteger os interesses sociais ou relacionais que, hoje, são abrangidos pela ideia de privacidade (O’BEIRNE, 2009, p. 15).

Como assevera Stefano Rodotà (1905, p. 102), o conceito de privacidade não mais se estrutura de acordo com o eixo “pessoa-informação-segredo”, mas sim, segundo o eixo “pessoa-informação-circulação-controle”, estando, portanto, associado à capacidade de ter controle sobre as próprias informações. Foi neste contexto, justamente, que se reconheceu um distanciamento entre o direito à privacidade e aspectos envolvendo a proteção de dados pessoais, especialmente, a partir do célebre julgamento da Corte Constitucional Alemã – cuja paradigmática sentença, ao tratar do censo demográfico que se realizava no país, em 1983, e da insegurança quanto à forma de coleta e aos usos secundários de dados sugeridos pelo Estado, alçou a construção do chamado direito à *autodeterminação informativa*, ou seja, ao controle dos indivíduos sobre como, por que, quando e sob quais limites os seus dados pessoais podem ser utilizados⁹. Era um anúncio dos novos tempos.

Ora, construções legislativas e jurisprudenciais não estão apartadas da realidade e é certo que a difusão de mecanismos de vigilância esteve, também, em muito ligada ao seu desenvolvimento e ao reconhecimento de novos direitos e interesses dos cidadãos. Daí que, se o principal estímulo para as reivindicações relativas à privacidade, no início do século XIX, esteve associado à proteção dos indivíduos da exposição a muita publicidade, por exemplo, o argumento norteador em fins de século associou-se, verdadeiramente, à alegada invisibilidade dos

9. Cf. Doneda (2019, p. 165 e ss.), a Corte alemã endossou a ideia de que a *autodeterminação informativa* não é um fim em si mesma, mas, acima de tudo, dedica-se a promover o direito à personalidade. Fato é que essa mudança de perspectiva quanto ao direito à privacidade permitiu compreender, em larga escala, a necessidade de estabelecimento de proteções regulatórias associados à proteção de dados pessoais – que, frise-se, vai muito além, inclusive, do próprio direito à autodeterminação informativa.

observadores; e eventos marcantes, a partir daí, retratariam o clamor público em face de atividades de tratamento irrestrito de dados.

Um caso emblemático, envolvendo o *National Data Center*, nos Estados Unidos, tornaria pública a criação de uma enorme base de informações pessoais e estatísticas, disponíveis em bancos de dados de diversas agências federais do país, para fins de centralização da inteligência dos dados, como então se sustentou, somada à redução de custos e, claro, ao estímulo à eficiência dos serviços públicos. À época, não foi antecipada qualquer preocupação acerca de eventuais questionamentos coletivos, uma vez que se tratava de uma mera agregação de informações, sem qualquer coleta adicional ou secreta – ideia que acabou caindo por terra quando se percebeu, em contrapartida, que o Estado não vinha apenas agregando informações já disponíveis em seus bancos, mas sim, gerando valor a partir da compreensão dos hábitos das pessoas, por meio de tecnologias deveras sofisticadas (IGO, 2018, p. 221 e ss.).

Nessa linha, se a passagem ao século XX trouxe expressivas preocupações no contexto de mecanismos de vigilância abertos (como ocorreu no caso do *National Data Center*), o cenário se agravaria consideravelmente nos anos que se seguiram, marcados, especialmente na conjuntura mais recente, pela intensificação de mecanismos de observação e controle, muitas vezes ocultados por seus idealizadores, impulsionados pela intensa digitalização da vida e pela publicização pelas próprias pessoas, usuárias da internet e de seus muitos aplicativos, de dados os mais diversos – as suas faces, por exemplo. Não seria possível saber, afinal, que fotos publicadas em redes sociais poderiam servir à alimentação de bases de dados de empresas privadas, como a norte-americana *Clearview AI* e seu impressionante número de 3 bilhões de imagens. Igualmente, seria difícil imaginar que plataformas similares, talvez pensadas inicialmente como simples “agregadores” de informação, pudessem ser capazes de levar à identificação de participantes de protestos, à microsegmentação de eleitores e até mesmo ao controle do deslocamento de minorias étnicas¹⁰.

Dilemas como estes conduziram, naturalmente, ao aperfeiçoamento dos marcos regulatórios envolvendo a proteção de dados pessoais, que já superaram diferentes gerações nas últimas quatro décadas do seu desenvolvimento, notadamente marcado, como era de se esperar, pelos receios ante o uso desmedido de informações pelo Estado, sua baliza inaugural. No caso do direito brasileiro, especificamente, por uma série de particularidades históricas, há que se dizer que

10. Conforme a investigação-reportagem de HILL (2021), publicada pelo *The New York Times*. Disponível em: [<https://www.nytimes.com/interactive/2021/03/18/magazine/facial-recognition-clearview-ai.html?smid=li-share>]. Acesso em: 29.03.2021.

a evolução do tema de proteção de dados foi lenta, tendo o direito à privacidade se mantido como majoritariamente ligado a um caráter *individualista possessivo*, ressoado na proteção constitucional e em regulamentos esparsos e setoriais – e, quando muito, vinculado estritamente ao aspecto de controle, ou seja, da garantia de autorização, ou não, do uso de dados pessoais pelos indivíduos (DONEDA; SARLET; MENDES, 2021, p. 11). Até recentemente, assim, não havia um arcabouço legal amplo e que regulasse as múltiplas particularidades dos direitos à privacidade e proteção de dados, como se vê, agora, com a LGPD.

Esta foi a normativa legal que instituiu uma regulamentação geral para o tratamento de dados pessoais, de maneira ampla, nos ambientes *online* e *offline*, pelos setores público e privado, com o objetivo de restituir ao titular o controle sobre os seus dados – sendo um de seus fundamentos, exatamente, a autodeterminação informativa – e impor aos agentes de tratamento, por outro lado, uma ampla gama de obrigações. Pode-se dizer que a LGPD possui, assim, um escopo temático e territorial de aplicação bastante amplo; ao mesmo tempo, seguindo a lógica da regulamentação europeia que a inspirou¹¹, este dispositivo legal não estendeu a sua aplicação a atividades de tratamento voltados à segurança nacional ou, ainda, a atividades de investigação e repressão de infrações penais – em virtude da sensibilidade que envolve o uso de dados pessoais para estes fins.

Nessa esteira, o legislador entendeu por bem estabelecer um marco regulatório específico para o uso de informações para combate a infrações penais¹², e já existe um anteprojeto do que poderá ser a *Lei de Proteção de Dados para segurança pública e investigação criminal*, atualmente em tramitação na Câmara dos Deputados. Apresentado com a finalidade de suprir a lacuna legislativa a respeito do tema, em uma tentativa de regular o tratamento de dados pessoais no contexto de atividades de persecução e repressão de potenciais infrações penais, o anteprojeto

11. O *General Data Protection Regulation* (GDPR), que serviu de inspiração à lei brasileira, também possui abrangência limitada, contando com a *Law Enforcement Directive* (LED) para a regulamentação de atividades de tratamento de dados em matéria penal. Ambos os dispositivos se encontram disponíveis, na integralidade, em: [https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679]; [https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680&from=EN]. Acesso em: 29.03.2021.

12. Deve haver, contudo, alguma confusão, ao menos inicial, quanto à aplicação de cada norma a cada caso específico (se aprovado o anteprojeto), como já ocorre, inclusive, na União Europeia, seja pelo simples aproveitamento de sistemas privados pelo Poder Público ou, ainda, pelo uso secundário, pelo Estado, de informações coletadas inicialmente para uma determinada finalidade e que, posteriormente, podem passar a alimentar sistemas de inteligência artificial. Veja, nesse sentido, LYNKEY (2019).

visa, segundo a sua exposição de motivos, a um equilíbrio entre “a proteção do titular contra mau uso e abusos” e o “acesso de autoridades a todo potencial de ferramentas e plataformas modernas para segurança pública e investigações”, desde que assegurados os “direitos fundamentais de liberdade e de privacidade” dos titulares, bem como a dignidade, os direitos humanos, a autodeterminação informativa, a presunção de inocência, a garantia do devido processo legal, da ampla defesa e do contraditório, dentre outros princípios e direitos¹³.

A partir das disposições preliminares do anteprojeto (que, frise-se, ainda pode ser alterado), observa-se retratado, de maneira bastante emblemática, o embate entre indivíduo, sociedade e Estado, notadamente no que se refere aos mecanismos de proteção sugeridos pelo dispositivo (como balizas para a tomada de decisões automatizadas, mormente centradas na exigência de não discriminação, e garantias de correção de dados incorretos ou imprecisos pelos titulares, por exemplo), sopesados, de outra parte, com a “segurança do Estado” e a “defesa nacional” – que permitiriam limitações de acesso ou mesmo recusas por parte do Estado quanto ao fornecimento de informações em casos de eventual prejuízo para investigações ou processos.

Tendo tudo isso em vista, é possível dizer que, malgrado seja muito positivo o desenvolvimento legislativo brasileiro no que se refere à proteção de dados pessoais, já surtindo efeitos, também, na regulação penal da matéria, não parece concebível crer que a existência de leis, por si só, tornarão a era da vigilância em massa absolutamente segura – mormente no contexto da segurança pública, que não só envolve setores sociais altamente vulneráveis como, pelo seu próprio modo de ser, trabalha com profundas assimetrias de poder entre Estado-acusador e indivíduo-acusado. Em verdade, a materialidade da vida parece sempre ultrapassar os limites da lei, sobretudo quando colocados em jogo anseios tão viscerais quanto o da segurança a (quase) qualquer custo. Daí que boas Iniciativas, é verdade, não implicam necessariamente práticas mais responsáveis: diplomas legais, como se verá a seguir, não tornam prescindível a crítica.

3. CRÍTICA À BANALIZAÇÃO DA INTELIGÊNCIA ARTIFICIAL COMO TÉCNICA DE CONTROLE

Como se viu, não há como escapar à tecnologia que, em uma de suas facetas mais desenvolvidas, torna sistemas computacionais cada vez mais aptos

13. A íntegra do anteprojeto se encontra disponível em: [<https://static.poder360.com.br/2020/11/DADOS-Anteprojeto-comissao-protacao-dados-seguranca-persecuacao-FINAL.pdf>]. Acesso em: 24.03.2021.

a realizar tarefas que, em tempos não tão longínquos, eram vistas como tarefas exclusivamente humanas – aprimoramento da percepção visual, detecção de movimentos, atividades criativas e até mesmo tomada de decisões: tudo isso já pode ser feito pela inteligência artificial.

Progressivamente, as cidades se fortificam como uma grande rede punitiva, que tende à expansão e se materializa em tecnologias de controle orientadas, mais que nunca, à vigilância silenciosa, à limitação de acesso de certos grupos em determinados lugares e, sem dúvida, a uma tentativa de predição *eficaz*, especialmente, para fins de segurança pública. Menos supressão e mais prevenção – não importa a análise factual do fenômeno criminoso, mas sim, o risco de que ele ocorra; o temor, em larga medida, é maior que a própria concretude do delito.

Por decorrência disso, a sociedade caminha a passos largos para um cenário de ultravigilância, sendo iminente o ataque à privacidade da coletividade. Alguns efeitos adicionais, contudo, como se verá, parecem atingir grupos específicos de pessoas de forma diferencial – o que parece ser, no mínimo, esperado, haja vista a missão do atuarialismo, munido das novas tecnologias, no sentido de identificação daquelas classes de sujeitos *produtoras de risco* ou, em outras palavras, de desviantes iminentes. Concretamente, categorias inteiras de indivíduos deixam de cometer crimes para que se tornem, elas mesmas, um crime *per se* (DE GIORGI, 2006, p. 98) – e a banalização da inteligência artificial como tecnologia de controle, sem dúvidas, potencializa esta nova realidade.

A seguir, a crítica será direcionada a alguns pontos específicos, a saber: (i) os danos decorrentes da falta de transparência que uma situação de ampla vigilância pode acarretar, particularmente no que se refere ao uso secundário de dados pessoais; (ii) a ilusão de eficiência vinculada às técnicas de análise criminal que, mesmo em termos econômicos, não parecem corresponder de forma automática e infalível aos anseios de redução do número de crimes; (iii) a problemática dos falsos-positivos e falsos-negativos no contexto de utilização (discriminatória) de ferramentas de reconhecimento facial; e (iv) a questão da seletividade da vigilância, em potências paulatinamente mais elevadas conforme caminha a tecnologia, e de todos os efeitos adversos resultantes da amplificação da teia de controle, sobretudo no que diz respeito à incapacitação de comunidades inteiras – desacompanhada, vale reforçar, da prevenção real da criminalidade de fato.

3.1. *A problemática da transparência e a demanda por parâmetros de inteligência artificial explicáveis*

Conforme analisado anteriormente, a garantia sobre o controle de uso das informações é um aspecto estruturante da proteção de dados, e, no contexto de

legislações desse tipo, associa-se direta e fundamentalmente às ideias de transparência e responsabilização. Se no passado existia um entendimento – no Brasil, até a aprovação da LGPD – de que este controle só poderia se apresentar mediante um consentimento *informado* do titular dos dados, esta limitação se mostrou, todavia, falha ao longo do tempo, visto que a validade de uma autorização *informada* presumiria que o titular tivesse entendido e avaliado, por conta própria, os benefícios e riscos de um determinado tratamento.

Ora, a complexidade das novas tecnologias, a amplitude de eventuais autorizações coletadas e, especialmente no espectro das atividades de tratamento envolvendo o Estado, o desequilíbrio entre o controlador do dado e o titular, reforçavam a exigência de revisão dessa condição precedente – reconhecendo-se, a partir daí, a necessidade de se colocar maior peso sobre aspectos como transparência, prestação de contas e responsabilização. Para além da previsão e da garantia de direitos aos titulares¹⁴, tem-se, assim, a imposição de verdadeiras obrigações aos agentes de tratamento (TAYLOR, 2017, p. 73 e ss.).

Nesse sentido, é verdade que o ambiente legislativo de proteção de dados trouxe avanços importantes para o cenário ora debatido; entretanto, não parecem estas iniciativas suficientes para garantir satisfatoriamente o uso desenfreado de mecanismos de tratamento automatizado de dados sofisticados, particularmente no contexto de ações de controle social que, como se viu, sequer estão cobertas pelo recorte da lei, ao menos no Brasil – e isso se deve a uma série de fatores, não necessariamente conexos à estrita legalidade. A problemática da transparência é um bom exemplo: frequentemente limitada por decorrência de questões envolvendo segurança da informação e propriedade industrial (em especial, quando o Estado adquire os seus mecanismos de vigilância e avaliação de agentes privados, como no caso da já citada ferramenta *PredPol*¹⁵), a transparência, é dizer, a falta dela, impõe um fardo pesado aos titulares no sentido de compreenderem não só o funcionamento desses sistemas – e a complexidade de suas redes

14. No caso da LGPD, destaca-se a previsão do direito à informação, da obrigação de elaboração de relatórios de impacto à proteção de dados, inclusive pelo Estado, e de direitos de auditoria, por exemplo, dispostos, respectivamente, nos artigos 9º; 39 e 4º, § 3º; e 20, § 2º, do dispositivo.

15. Conforme a reportagem do *The Intercept* (WINSTON, 2018), que expôs uma decisão da Corte de Justiça de Nova York, exigindo que a *PredPol* e outras companhias esclarecessem os fundamentos de funcionamentos de suas plataformas de predição. Disponível em: [<https://theintercept.com/2018/01/27/nypd-predictive-policing-documents-law-suit-crime-forecasting-brennan/>]. Acesso em: 29.03.2021.

neurais artificiais, alimentadas por bases de dados volumosas –, mas, pior, os riscos e impactos a eles associados.

Tudo isso se potencializa na era da informação. A circulação massiva e desenfreada de dados e a facilidade de coleta automatizada de fontes publicamente acessíveis reforçam a preocupação quanto à clareza das fontes eventualmente utilizadas pelas plataformas de tratamento, sejam elas privadas ou públicas – e, não por outro motivo, vale dizer, as redes sociais expressamente proíbem o uso de seus dados, por desenvolvedores, para fins de vigilância e segurança pública¹⁶. Valendo-se do exemplo do *National Data Center* supramencionado, é fácil perceber que, sem qualquer incremento em sua base, o Estado já dispõe de uma quantidade relevante de dados sobre os cidadãos; mas, como os sistemas automatizados se alimentam de dados e, é sabido, tornam-se cada vez melhores quanto maior o seu agregado, parece que nenhuma base de dados, por maior que seja, será um dia suficiente.

Daí que, em algumas situações, as fontes serão relativamente simples e claras. Veja-se, a título exemplificativo, o projeto *City Cameras*¹⁷, formulado pela Prefeitura da Cidade de São Paulo, que propõe, com a participação da população, “formar [uma] ampla rede de monitoramento, [para] além das câmeras dos órgãos públicos, [com] câmeras de segurança residenciais e pontos comerciais, que já se encontram distribuídas por São Paulo”¹⁸. Em outras, por outro lado, a fonte de dados que venha a balizar o desenvolvimento de um certo sistema pode ser obscura; veja-se um exemplo hipotético de bases utilizadas para a promoção do controle social do delito provenientes, na verdade, de bases terceiras cuja finalidade serviria, a princípio, para o mero controle de fraudes no processo eleitoral – uso secundário de dados pessoais que, seguramente, passaria despercebido pelo indivíduo.

Como se não bastasse, a dificuldade de compreensão dos pormenores das novas tecnologias – a que todos estão submetidos – não está adstrita apenas aos titulares cujos dados pessoais poderão ser tratados, mas, o que é mais preocupante,

16. *Twitter e Facebook* são exemplos de plataformas que sustentam esta proibição, tal como disposto em seus termos de uso voltados a desenvolvedores. Disponíveis em: [<https://developer.twitter.com/en/developer-terms/agreement> e <https://developers.facebook.com/terms/>]. Acesso em: 29.03.2021.

17. Sem quaisquer juízos de valor quanto ao mérito da iniciativa, utilizada apenas para exemplificação, no que se refere à facilidade de identificação da fonte das informações.

18. Disponível em: [<https://www.citycameras.prefeitura.sp.gov.br/howworks/>]. Acesso em: 29.03.2021.

atinge os próprios operadores do sistema. É possível, por exemplo, que ferramentas de “predição” baseadas em reconhecimento facial (que serão discutidas adiante) sejam utilizadas para fins de *medição de risco* de indivíduos investigados ou processados em uma dada localidade – algo como um sistema de identificação de potenciais infratores, por exemplo; nestes casos, um dado agente público pode até captar a pontuação de um certo indivíduo, entendendo-o como “perigoso” ou não, mas dificilmente terá condições de justificar, sem apoio técnico, as decisões associadas ao próprio *design* do algoritmo e, conseqüentemente, aos seus resultados.

Donde, ademais da própria transparência, estende-se o direito à informação, no escopo das tecnologias baseadas em inteligência artificial, sobre o chamado *direito à explicação* (MONTEIRO, 2018); afinal, especialmente em situações de uso mais nebuloso de dados pessoais, entende-se como garantia do titular o acesso à lógica por trás de decisões automatizadas que possam vir a atingi-lo. Entretanto, e este é um grande risco, mecanismos de aprendizado e de identificação técnica dos motivos da tomada de decisão de máquinas podem ser demasiadamente complexos e aparentemente inacessíveis, o que levanta a demanda, cada vez mais latente, por parâmetros de *inteligência artificial explicáveis*¹⁹.

A adoção dessas técnicas é recente e deve ainda ser testada para que se tornem aptas, em alguma medida, a combater decisões algorítmicas discriminatórias – e não parece ser aceitável que, sem essa validação prévia da ética do algoritmo, por assim dizer, seja possível a utilização desenfreada de mecanismos de inteligência artificial para fins de controle, com destaque para o controle social do delito, haja vista que a ininteligibilidade das explicações (CHIAO, 2019, p. 7 e ss.), para dizer apenas um dos problemas, prejudicaria sobremaneira as salvaguardas fundamentais constitucionais do contraditório e da ampla defesa.

Somadas às exigências de transparência e explicação, outras medidas de contenção, mais associadas à prestação de contas e responsabilização, podem e devem ganhar espaço: é dizer, a adoção de práticas de fiscalização por autoridades competentes, por exemplo, a partir de auditorias periódicas, seja pelas próprias autoridades ou por entidades da sociedade civil, não só após, mas, principalmente, desde o momento da concepção dessas tecnologias que, sem dúvida, ocupam

19. Vide, nesse sentido, YU; ALI (2019). Bons exemplos de adoção de parâmetros de inteligência artificial explicáveis podem ser também encontrados *online*. Disponíveis em: [https://www.ibm.com/watson/explainable-ai; https://www.darpa.mil/program/explainable-artificial-intelligence] e [https://cloud.google.com/explainable-ai]. Acesso em: 29.03.2021.

cada vez mais o cotidiano das pessoas (EDWARDS, 2017, p. 76 e ss.). Se haverá recursos técnicos ou humanos para fiscalizar e auditar sistemas, com a devida independência, é um questionamento que subsiste. O que é certo, de toda maneira, é que a *tecnologização* do mundo traz muitos riscos que, em boa medida, podem ser mitigados; em contextos de vigilância em massa e de persecução penal, contudo, como se verá, os prejuízos podem se mostrar irreversíveis.

3.2. *Análise criminal e a ilusão de eficiência*

Das muitas tecnologias empregadas no contexto da segurança pública, as mais comuns talvez sejam aquelas ligadas à chamada análise criminal. Conforme a definição de Manning (2008, p. 4), entende-se por análise criminal uma família de técnicas designadas para a coleta e o processamento de informações sobre aspectos espaciais, temporais e sociais associados ao crime – incluindo, aqui, atributos tanto de potenciais delinquentes quanto de vítimas, tais como gênero, idade, classe e raça –, bem como para a posterior padronização e disponibilização geral dos dados processados, a fim de direcionar os recursos das agências policiais e de justiça à redução *eficaz* dos índices de criminalidade de uma dada região.

De visualização relativamente simples (na forma de texto, imagens, mapas, tabelas e gráficos), as informações advindas de uma análise criminal automatizada são normalmente capazes de demonstrar variações nas características dos delitos reportados, em determinados períodos de tempo, a partir da sua combinação com dados previamente apresentados pelas forças policiais. Mais que um mero traçado de elementos esparsos, o uso da inteligência artificial para análises criminais se constitui, assim, como uma coleção de métodos de interpretação de dados e planejamento de ações em segurança pública.

Logo, pode-se dizer que daquele mero mapeamento, popular entre as décadas de 1980 e 1990, de cunho apenas espacial-descritivo, passa-se mais recentemente a uma análise propriamente dita das informações apresentadas, assim como à sua aplicação, na prática, na forma de táticas de intervenção (MANNING, 2008, p. 15) – e, nesse sentido, já existem algumas iniciativas no Brasil, como as ferramentas elaboradas pelo CeMEAI, em parceria com o NEV, supramencionadas a título de introdução.

A primeira delas, denominada *CrimAnalyzer*, possibilita a identificação de padrões de criminalidade em regiões da cidade de São Paulo, de modo que se verifiquem os mais prevalentes em termos quantitativos. A segunda, chamada *Mirante*, mais robusta, permite a realização de tratamentos estatísticos dos dados, bem como o geoprocessamento em mapas de rua e a identificação de mudanças

no padrão dos delitos ao longo do tempo, associadas a variáveis externas, mormente no quesito da infraestrutura urbana. Tudo isso viabilizado, em um primeiro momento, pelo acesso a uma relevante quantidade de dados sobre crimes que já haviam sido anteriormente reunidos pelo NEV. Como complemento, desenvolveu-se, ainda, uma metodologia capaz de comparar séries temporais de crimes em diferentes bairros da cidade, a partir de tecnologias de “aprendizado de máquina” (ou *deep learning*, em inglês) que propiciam, justamente, o reconhecimento de padrões – para além da simples identificação. O resultado: o referido modelo matemático indicou que, de um total de 20 mil esquinas com os maiores registros de assalto da região central da cidade de São Paulo, apenas 1.535 (7,65%) concentram quase a metade das ocorrências – o que sugeriria, portanto, uma maior probabilidade de ocorrência de crimes e, consequentemente, a necessidade de maior policiamento nessas regiões²⁰.

Ora, economicamente falando, a princípio o raciocínio faz sentido. Não por menos, um dos mais fortes argumentos pelo uso de métodos atuariais consiste na ideia de dissuasão eficiente (HARCOURT, 2007, p. 111): presumindo que as pessoas respondam racionalmente aos custos e incentivos do policiamento, a utilização de previsões baseadas nas taxas de delinquência de certos grupos, em regiões específicas, resultará em uma maior detecção do crime. Maximizada essa detecção, assim, a polícia passa a deter a população-alvo, estatisticamente *mais criminosa*, alocando de forma mais eficiente os recursos de aplicação da lei.

Ocorre que, ao contrário do que possa parecer, a detecção de atividades delituosas não deveria ser a meta principal das agências de segurança pública, pois a simples constatação de que existem crimes não é boa por si mesma – a busca pela redução do número de delitos, esta sim, deveria se colocar como objetivo primário da polícia e da justiça. Dito isso, seria preciso questionar se o incremento (e direcionamento) da atividade policial para certas regiões, a partir da análise criminal, atua com efeito em prol dessa diminuição – e, frente a essa pergunta, já há estudos que demonstram que o argumento economicista não se sustenta por muito tempo.

Veja-se, para uma melhor compreensão: toda a atividade de policiamento direcionada, se baseada em análises, como as providenciadas pelas ferramentas descritas, sustenta-se, em um primeiro momento, em dados fornecidos pelas próprias agências de segurança, especialmente registros de ocorrências. Por isso, o questionamento sobre quem de fato vai preso em flagrante é de extrema

20. Disponível em: <https://agencia.fapesp.br/sistema-usa-inteligencia-artificial-para-prever-ocorrencias-de-crimes-em-areas-urbanas/33768/>. Acesso em: 25 mar. 2021.

importância – afinal, a eficiência policial pode esconder “nuances” que mais se identifiquem com *perfilamento*, ou seja, com a sujeição de categorias sociais específicas, fundada em generalizações diversas (seja sobre a raça, a nacionalidade, a regionalidade, ou mesmo o bairro a que pertencem), ao invés de evidências objetivas a respeito do comportamento de um indivíduo.

Para fim de exemplificação, de acordo com dados do Instituto de Defesa do Direito de Defesa (IDDD), publicados em maio de 2016, o perfil da população presa em flagrante na cidade de São Paulo é 90% masculino, 62% jovem (até 29 anos) e 61% negro (o que corresponde à estatística referente, também, ao sistema prisional em geral), com renda mensal de até dois salários mínimos para 94% dos casos²¹. Uma avaliação vulgar poderia concluir, por consequência, que, para fins de prevenção, esta é a categoria social a se manter no radar quando observadas as “zonas perigosas” (visto ser a que mais cometeria delitos) e que, quanto mais flagrantes, melhor o custo-benefício da atividade policial. Ocorre que, sem adentrar, por ora, à controversa da seletividade por si mesma ou a própria crítica ao funcionamento do sistema de justiça criminal em sua integridade, a verdade é que a tão sonhada eficiência não se deixa demonstrar pela matemática.

Ainda de acordo com as observações de Harcourt (2007, p. 123 e ss.), há uma suposição oculta no modelo econômico de perfilamento e, como ocorreria no exemplo apresentado, de perfilamento racial: a questão da *elasticidade*, ou seja, do impacto que a alteração de uma variável específica exerce sobre outra, neste caso, em um dado contexto de policiamento. Aqui, são duas as constatações: (i) primeiro, que a elasticidade do crime em relação à atividade policial depende da própria distribuição da justiça e, (ii) segundo, que distorções causadas pelo perfilamento podem levar, na verdade, ao aumento da criminalidade de setores subabordados.

Nessa linha, a pesquisa sobre o porquê de as pessoas obedecerem à lei, conduzida pelo estadunidense Tom Tyler, professor de psicologia e direito na Universidade de Yale, sugere que abordagens desproporcionais a minorias raciais – como parece acontecer em São Paulo, por exemplo, considerados os dados supra – podem prejudicar a percepção sobre a justiça geral do sistema, impactando de forma diferencial a sua resposta abstrata à lei. Afinal, se uma dada categoria social acredita que será injustamente assediada ou supervisionada pelas autoridades

21. No detalhe, as informações coletadas indicam renda inexistente para 14% dos presos em flagrante; renda de até um salário mínimo para 33%; e renda entre um e dois salários mínimos para os outros 47%. Disponível em: <http://www.iddd.org.br/wp-content/uploads/2016/05/Relatorio-AC-SP.pdf>. Acesso em: 28 mar. 2021.

independentemente do que faça, é possível que, em última análise, a sua “falta de fé” no sistema leve a uma menor taxa de cumprimento da lei ante à quebra de confiança – e a curva ofensiva, nesta linha, ascenderia (HARCOURT, 2007, p. 169)²².

Quanto ao segundo ponto, veja-se um exemplo diverso, trazido também por Harcourt (2007, p. 136): suponha-se, como descobriu a Receita Federal dos Estados Unidos (IRS), que a fraude fiscal no país é mais comum em contratos de *drywall* do que em outros negócios. Suponha-se, ainda, que o IRS realize, por isso, um perfilamento dos empreiteiros de *drywall* – e que essa informação se dissemine de alguma forma. Nesse caso, é possível que outros empreiteiros subcontratados – como pintores, eletricitistas, encanadores etc. – comecem a acreditar que o seu incentivo para cumprir com a lei diminuiu, haja vista não serem o foco da vigilância, incorrendo em mais fraudes na declaração de seus impostos. Nesse caso, não só seria expressivo o custo com auditorias e demais estratégias de vigilância (para fins de diminuição do índice de criminalidade relacionado aos contratos de *drywall*), como a realocação desses recursos, por sua vez, poderia engatilhar uma reação adversa em demais setores. Conclui-se, portanto, que mais crimes de evasão fiscal poderiam acontecer, matematicamente falando, sem que os seus autores fossem necessariamente flagrados – tudo dependeria das elasticidades e do grau de seletividade do próprio sistema.

Daí que o problema dos modelos econômicos baseados em perfilamento e no direcionamento de recursos não está necessariamente relacionado, a partir desta análise, a uma supervalorização da ideia de eficiência, mas sim, na sua definição equivocada – se referente a um maior número de abordagens ou, o que seria correto, a uma diminuição dos índices de criminalidade de fato – e na desconsideração das elasticidades e da seletividade no contexto do policiamento e da atuação da justiça criminal como um todo.

Quaisquer noções de eficiência deveriam ser inteiramente subservientes não ao “sucesso” das abordagens policiais, mas, reforça-se, a um potencial de redução do crime como objetivo primário. Não basta aumentar o número de abordagens e a sua “taxa de acertos”, ou mesmo prender mais pessoas tidas por *criminosas* – tudo isso apenas distorce a concepção do que seria um policiamento adequado e, no limite, justo, em detrimento de uma real minimização da criminalidade.

-
22. Igualmente, Kaplow e Shavell sustentam economicamente que a responsabilização injusta de um indivíduo tende a diluir uma potencial dissuasão frente à prática de crimes, haja vista a redução do benefício marginal de cumprir com a lei (KAPLOW; SHAVELL, 2002, p. 1753).

E essa distorção prejudica seriamente a capacidade de se elaborarem quaisquer inferências precisas a partir de dados emergentes de ferramentas de análise criminal.

Ademais, importaria a questão da precisão destes balanços, veja-se, até mesmo se a utilização de uma dada tecnologia de análise criminal coincidissem, local e temporalmente, com a redução da criminalidade. Afinal, o delito é um fenômeno demasiado complexo para que quaisquer reduções em potencial sejam direta e inquestionavelmente relacionadas ao poder de um algoritmo; até porque, quando mais se procura por um crime, maior será a probabilidade de encontrá-lo – não só em áreas delimitadas como de alto risco, mas em qualquer lugar. Como sustenta a matemática, uma vez mais, seria até possível que apenas encorajar policiais a aleatoriamente fazerem rondas, saindo de seus carros, sem roteiro, conduzissem a uma redução da criminalidade nas localidades patrulhadas (FRY, 2018, p. 156). Igualmente, condições externas ao próprio patrulhamento poderiam contribuir para os mesmos fins: uma teórica redução de crimes relacionados à propriedade durante períodos de maior prosperidade econômica das classes mais pobres, por exemplo, e por aí vai. Simplesmente não é possível atribuir quaisquer resultados, única e exclusivamente, ao algoritmo – uma vez que o objeto das ciências sociais não pode ser isolado e testado em laboratório.

Dados resultantes de análises criminais apartadas e, principalmente, os diagnósticos e as técnicas de intervenção que deles decorrem, silenciam totalmente a respeito dessa elasticidade comparativa do delito em relação ao policiamento e, não somente, em resposta a mudanças das condições da sociedade como um todo – daí que, sem essas informações, pouco ou nada dizem empiricamente sobre o impacto das análises criminais embasadas em perfilamento, seja sobre o crime em si mesmo, seja sobre a própria população perfilada.

Por esse motivo, não há nenhuma boa razão para acreditar que fazê-lo resultará, *eficientemente*, em uma redução dos índices de criminalidade de um dado local; ao menos nenhuma boa razão matemática. O fato de assim se acreditar diz mais sobre o *desejo de acreditar*, na mesma linha dos anseios de previsão do futuro, e menos sobre a materialidade dos resultados (HARCOURT, 2007, pp. 140-144). A eficiência de táticas atuariais como a análise criminal, destarte, não passa de ilusão – e estar predisposto a querer que este modelo esteja certo não faz com que ele funcione de verdade.

3.3. *Reconhecimento facial, predição e gestão diferencial de pessoas: falsos-positivos e falsos-negativos*

Diferente da análise criminal, mas identificada, igualmente, como uma tecnologia de aprendizado de máquina, o reconhecimento facial é uma das funcionalidades

dos chamados *algoritmos classificatórios*, que utilizam, para fins de identificação de padrões, uma base de dados anteriormente estabelecida e pré-classificada – a partir de características como idade, gênero, raça, geolocalização ou demais qualificadores individuais, inseridas pelos desenvolvedores de um dado sistema de reconhecimento e aplicadas para o treinamento da plataforma. São as características inseridas que, uma vez categorizadas, padronizadas, normalizadas e analisadas, servirão como parâmetro de identificação ou classificação de novas pessoas (FRAGOSO; ROBERTO; SIMÃO, 2020, pp. 24-27). Dessa forma, para a identificação de uma pessoa desconhecida (que não necessariamente tem o seu rosto armazenado anteriormente pelo sistema), por exemplo, para fins de potencial responsabilização criminal, as plataformas de reconhecimento facial detectam as características pessoais do alvo e realizam o cruzamento da imagem obtida, uma vez analisada, com uma larga quantidade de dados já imputados – um pareamento “de um para muitos”, pode-se assim dizer (FRAGOSO; ROBERTO; SIMÃO, 2020, pp. 34-35).

Ora, tendo em vista que aparatos de reconhecimento facial, assim como outras ferramentas de inteligência artificial, só produzem os seus resultados se devidamente alimentados, há que se sustentar que não são eles instrumentos meramente informativos, mas sim, tecnologias que realizam, virtualmente, uma *representação* do real – ou, especificamente para os casos que aqui se retratarão, uma representação de informações relevantes sobre o crime, a partir do esforço cognitivo de atores, humanos ou não, aptos a empreender uma *interpretação* do que é visto (uma expressão), a partir de um conteúdo mentalmente ligado a essa expressão. Combinam-se expressão, conteúdo e contexto: o reconhecimento facial envolve, efetivamente, a criação de um signo e a interpretação do mundo propriamente (MANNING, 2008, p. 20).

Donde surge a problemática dos vieses, afinal, como quaisquer plataformas baseadas em algoritmos de *machine learning*, as tecnologias de reconhecimento facial envolvem o enorme risco de que as tendências e idiossincrasias dos desenvolvedores reflitam nos dados usados para treinamento do sistema e, consequentemente, sejam também reproduzidos nos seus resultados. Afinal, não é segredo que um grupo extremamente homogêneo de pessoas é, de fato, quem está à frente das gigantes de tecnologia e, consequentemente, do rápido desenvolvimento da inteligência artificial. Segundo dados de 2019, cerca de 80% dos profissionais do setor são homens e, no que se refere à raça, o desequilíbrio é ainda maior – funcionários negros são apenas 2,5% do quadro de contratados pelo *Google*, e 4% das companhias *Facebook* e *Microsoft*²³, por exemplo. Não à toa, os vieses inerentes à sua visão de mundo acabam infiltrados nos algoritmos e incorporados aos

23. Conforme dados expostos por Picchi (2019). Disponível em: [<https://www.cbsnews.com/news/ai-bias-problem-techs-white-male-workforce/>]. Acesso em: 26.03.2021.

códigos, ainda que inconscientemente, refletindo uma ideia no mínimo limitada sobre o que seria uma pessoa *normal* (o famoso “homem médio”), em detrimento de classes que, naturalmente, já sofrem inúmeros preconceitos.

Na prática, tudo depende de como uma dada plataforma é manejada (e por quem) para atingir determinados fins, tornando-se relativamente facilitada a impregnação de vieses quando (i) ou os dados coletados não são representativos da realidade; (ii) ou estes mesmos dados refletem, em sua raiz, preconceitos já existentes²⁴ – afinal, é possível introduzi-los desde a fase de preparação das informações, em que se *selecionam*, verdadeiramente, quais atributos se quer que um dado algoritmo considere ou ignore, o que, não por menos, influencia notadamente a precisão do modelo – sem que, no mais das vezes, o viés seja sequer assinalado.

E, veja-se, a discussão vai muito além da possibilidade de uma máquina, tal como um ser humano, ser deliberadamente preconceituosa. Tome-se o exemplo do reconhecimento de pessoas: cientificamente, já se sustenta com um bom grau de segurança a ideia de que existe um *other-race effect* (ou “efeito de outra raça”), conforme explica Garrett (2011, p. 72), a partir do qual se infere que a chance de identificação incorreta de uma pessoa tende a ser maior quando se trata de um reconhecimento inter-racial. No mesmo sentido, pesquisadores da *Florida State University* chegaram à dramática afirmação de que são 40% maiores as chances de uma identificação precisa quando se trata de reconhecimento de um rosto do próprio grupo racial, ao passo que a probabilidade de uma identificação equivocada torna-se 56% maior quando envolve um reconhecimento intergrupos (MEISSNER; BRIGHAM, 2001, pp. 3-17)²⁵.

24. O primeiro caso pode ocorrer em algoritmos de reconhecimento facial, por exemplo, quando a aprendizagem da máquina se dá com mais fotos de rostos de pele clara do que de pele escura, de modo que o sistema de identificação resultante seria inevitavelmente pior nos últimos. Já uma demonstração emblemática do segundo caso foi, justamente, a descoberta pela *Amazon* de que uma de suas ferramentas de recrutamento interno dispensava candidatas do sexo feminino – por ter sido treinada a partir de decisões históricas de contratação, que favoreciam homens em relação às mulheres, a inteligência artificial simplesmente “aprendeu” a fazer o mesmo. Disponível em: [https://www.technologyreview.com/2019/02/04/137602/this-is-how-ai-bias-really-happens-and-why-its-so-hard-to-fix/]. Acesso em: 26.03.2021.

25. Conforme a revisão bibliográfica realizada pelo IDDD no contexto do requerimento de sua admissão como *Amicus Curiae* no *Habeas Corpus* 619.327/RJ. Disponível em: [http://www.iddd.org.br/wp-content/uploads/2020/12/amicus-tiago-vianna-final-sem-assinaturas.pdf]. Acesso em: 26.03.2021.

Hoje já se sabe que um fenômeno “similar” pode acometer ferramentas de reconhecimento facial, cuja acurácia pode ser sensivelmente reduzida, para fins de identificação de pessoas de pele negra, por exemplo, como brevemente destacado anteriormente, nos casos em que o treinamento de uma dada plataforma é feito com referência a bancos de dados constituídos majoritariamente por pessoas de pele branca, gerando resultados discriminatórios (FRAGOSO; ROBERTO; SIMÃO, 2020, pp. 45-46). Ora, só se identifica bem aquilo que se conhece. Desenvolvedores de pele clara, “ensinando” plataformas inteligentes com informações de pessoas brancas, avaliadas mais à frente, muito provavelmente, por agentes igualmente brancos – o reconhecimento pela plataforma (branca) torna-se, destarte, praticamente inter-racial, dessa vez, no plano virtual.

Daí que, por mais que a tecnologia possa soar como neutra, independente, desinteressada e, em certos casos, imbatível, a verdade é que algoritmos, hoje já se sabe, podem reproduzir – e o tempo todo reproduzem – padrões discriminatórios, trazendo um impacto incomensurável para o sistema de justiça criminal. Ora, se um dado aparato de reconhecimento facial é alimentado de forma desigual, é possível que, caso aplicado para a identificação criminal, por exemplo, apresente menor precisão ao tratar dados de pessoas negras – resultando, potencialmente, em mais erros judiciais. De igual maneira, se uma certa ferramenta de predição, na seara da segurança pública, for alimentada com dados de prisões em flagrante no Brasil, por exemplo, rapidamente aprenderá que pessoas de pele negra são historicamente “mais criminosas” e que, por isso, devem ser reconhecidas como população de alto risco.

Nesse sentido foram os gravíssimos elementos fornecidos pela *ProPublica*, publicação estadunidense independente e sem fins lucrativos, no contexto de uma larga investigação conduzida em 2016 e cujos resultados confirmaram: para além do reconhecimento *per se*, existem *softwares* responsáveis por “prever” futuros criminosos, a partir de dados da face e demais identificadores pessoais; e, como se verificou, tais ferramentas são altamente enviesadas e tendenciosas em face da população negra²⁶.

A referida investigação, apresentada na forma de reportagem, debruçou-se sobre o uso de ferramentas de avaliação de risco por tribunais de vários estados norte-americanos, a partir das quais seria atribuída uma pontuação a cada investigado ou réu, pontuação essa compartilhada com juízes como meio de informar

26. As inferências que serão feitas a seguir são todas baseadas no artigo *Machine Bias* (ANGWIN; LARSON; MATTU, 2016). Disponível em: [<https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>]. Acesso em: 26.03.2021.

eventuais decisões concernentes à liberdade dos indivíduos acusados. Tendo isso em vista, a *ProPublica* acessou pontuações de risco atribuídas a mais de 7 mil pessoas presas no estado da Flórida, entre 2013 e 2014, verificando posteriormente quantas teriam sido acusadas pela prática de novos crimes nos dois anos subsequentes – referência temporal utilizada pelos próprios criadores do algoritmo.

A partir daí, foram várias descobertas de relevo: (i) primeiro, a análise de risco se mostrou, para os casos analisados, marcadamente não confiável para a previsão de crimes violentos – apenas 20% das pessoas “previstas” como passíveis do cometimento de novos delitos realmente o fizeram; (ii) segundo, foram detectadas disparidades raciais significativas. Ao “prever” quem iria reincidir, o algoritmo cometeu diversos erros ao lidar com réus brancos e negros, mais ou menos na mesma proporção, mas de formas bastante díspares – réus negros foram erroneamente rotulados como futuros criminosos quase duas vezes mais que os réus brancos, enquanto estes foram equivocadamente sinalizados como de *baixo risco* em uma frequência maior quando comparados aos negros. Ou seja, falsos-positivos para negros; falsos-negativos para brancos.

No mesmo estudo, verificou-se se essa disparidade poderia, de alguma maneira, ser explicada pela ficha criminal dos réus ou, ainda, como uma decorrência dos crimes pelos quais a prisão se efetuará. A resposta foi negativa: a partir de um teste estatístico que isolou o efeito da raça do histórico criminal e de eventuais situações de reincidência, bem como de indicadores de idade e gênero, chegou-se à constatação de que réus negros tinham 77% mais probabilidade de serem considerados inclinados ao cometimento de crimes violentos futuros, e 45% mais chance de serem sinalizados como futuros criminosos, desta vez para delitos de qualquer tipo.

Mais uma vez, a falácia da neutralidade tecnológica parece tentar esconder que, sim, algoritmos são enviesados, ainda que não intencionalmente, para desfavorecer determinadas categorias populacionais, especialmente minorias raciais. E, para além disso, desenvolvedores de plataformas similares, tanto de reconhecimento facial quanto de predição baseada em dados pessoais, não parecem tão preocupados (senão muito recentemente) com a verificação e publicação desses vieses: no caso da desenvolvedora do algoritmo analisado pela *ProPublica*, chamada *Northpointe*, apenas alguns aspectos básicos da sua fórmula de predição foram revelados, incluindo fatores como níveis educacionais e empregabilidade. Por outro lado, não foram expostas as especificidades dos cálculos de risco, de modo que os reais motivos das disparidades denunciadas restam ainda desconhecidos tanto pelo público em geral quanto pelos próprios objetos da ferramenta.

Em resumo, conhecidas ou não, são muitas as explicações para tantos vieses, seja no que se refere às falhas no reconhecimento de pessoas negras; ao prejuízo, em termos gerais, a indivíduos de categorias sociais minoritárias; ou à distribuição desigual de falsos-positivos e falsos-negativos por ferramentas de predição. O que é comum a todos esses casos, conectando-os, é a existência de uma gestão diferencial de pessoas que, por mais que não seja nada recente, aparece potencializada pelas novas tecnologias – dificílimas de refutar ou combater, haja vista o mito tão impregnado da neutralidade (e consequente autoridade) da ciência tecnológica. O governo de pessoas já se faz pela inteligência artificial, e isso é uma novidade – para o sistema de justiça criminal, por outro lado, a seletividade, ora automatizada, parece tão presente quanto sempre foi, com ou sem algoritmos.

3.4. Isomorfia da patrulha: automatizada, mas tão seletiva quanto sempre foi

Novas tecnologias aplicadas ao controle social – do delito, em particular – suscitam uma série de questões problemáticas, dos anseios de vigilância total e de (pretensa) eficiência a qualquer custo à questão da gestão diferencial de indivíduos, com prejuízos altamente desproporcionais a setores sociais específicos. Tendo isso em vista, alguns sustentam que uma solução simples para estes problemas estaria na construção de máquinas superiores, que fossem corrigidas em seus algoritmos enviesados e, consequentemente, em sua acurácia e efetividade, e cuja utilização fosse legalmente delimitada para que se evitassem abusos. Em se tratando de segurança pública, contudo, nada é tão elementar quanto parece.

O que se sustenta aqui, nesse sentido, é que as agências policiais e de justiça podem se deixar infiltrar por tecnologias melhores, constituir-se (à primeira vista) de racionalidade, munir-se de manuais de boas práticas, consentir com reformas de fato – ainda assim, as suas maiores sensibilidades seguirão na estrutura, o que confere a essas instituições um potencial notadamente isomórfico. Tecnologias vêm e vão; os alicerces continuam os mesmos.

Existe um sistema perfeito, mas ele se limita apenas aos sonhos. A realidade do sistema de justiça criminal é que, ainda que abertamente fundado em pretensões universais e na proteção de interesses sociais tidos por gerais, a sua materialidade é de proteção de relações e interesses muito caros aos setores dominantes (BATISTA, 2007, pp. 112-116). A violência do sistema é estrutural e institucionalizada, e expressa, no mais das vezes, reações sociais irracionais mascaradas por devaneios de medo, distribuídas desigualmente pelo conjunto das pessoas – no Brasil, majoritariamente, pela população jovem, pobre e negra.

A seletividade é cruel, e as estatísticas são sangrentas. Ora, se as tecnologias de análise criminal já apontam que algumas esquinas da cidade de São Paulo são mais arriscadas para transeuntes e proprietários em geral, a verdade é que toda a capital tende a ser mais perigosa para alguns adolescentes e jovens adultos preferenciais, tudo a depender, é claro, da cor da sua pele. De acordo com dados da Rede de Observatórios da Segurança, referentes ao estado de São Paulo, 867 pessoas foram mortas durante intervenções policiais, em 2019, sendo 62,8% negros, mesmo que estes correspondam somente a 34,8% da população paulista²⁷.

Há também aquela violência mais “sutil”, própria dos tempos atuariais, que se concretiza no “cordão sanitário” traçado entre ordenadores e ordenados, classes de baixo e de alto risco: é o planejamento urbano hostil, o custo do transporte público, o preço das mercadorias nas áreas centrais, a segurança privada, o policiamento direcionado – tudo isso como meio de remoção de incertezas e varredura de grupos indesejados. Calcula-se o que pode causar desordem (ou mero descontentamento) e ali se estabelece o alvo: em que certas categorias são selecionadas como bode expiatório da sociedade em geral (YOUNG, 1998, p. 79).

O uso da inteligência artificial e de métodos atuariais como um todo tende, sim, a acentuar os vieses embutidos nas normas e leis em que se debruça o controle social – o que pode parecer um tremendo “sucesso” quando se está do lado dos *vigilantes* e não dos *vigiados*. Tudo em matéria penal, contudo, é uma grande área cinzenta; o que se sabe, de toda maneira, é que novas tecnologias aplicadas ao atuarialismo fazem alavancar quaisquer inclinações estruturais do próprio sistema, explorando de forma desproporcional as associações entre criminalidade e um dado grupo social e, por conseguinte, ampliando distorções já conhecidas.

Some-se a isso o fato de que a alegada racionalização das agências de segurança pública por meio da tecnologia – o que, como muitos acreditam, atua em prol da redução de disfuncionalidades – não parece ser uma grande verdade. Burocracias podem se modernizar, claro, mas aquelas mais tradicionais, como a polícia, seguirão em boa parte baseadas em meios verbais e não-verbais de persuasão para atingir os seus objetivos, ainda que no contexto de utilização de tecnologias de ponta, que, como se viu, não produzem conhecimento neutro, mas sim, informações sujeitas à interpretação do elemento humano que as analisa.

Nessa linha vão os estudos de Manning nos Estados Unidos (2008, pp. 25-27), que indicaram que a “sacralidade” da instituição policial, aos olhos da sociedade

27. Disponível em: [http://observatorioseguranca.com.br/wp-content/uploads/2020/12/A-Cor-da-Violência-Policial-A-Bala-Não-Erra-o-Alvo.pdf]. Acesso em: 27.03.2020.

ordeira, fez com que esta fosse por muito tempo poupada de pressões para ser eficiente ou de qualquer maneira orientada economicamente, o que todavia mudou mais recentemente, haja vista o barateamento da tecnologia e o desenvolvimento de ferramentas mais “amigáveis” e de fácil acesso. A ênfase no trabalho *científico* da polícia, assim, é o atual reflexo de reformas policiais de longo prazo, em uma tentativa de profissionalização e despersonalização da sua função. Ocorre que, embora mudanças tenham sido introduzidas, como observado por Manning, a tecnologia primária da polícia segue sendo simbólica, o que faz dela, ainda nos dias de hoje, uma instituição bastante *low-tech* – é dizer, a tecnologia da informação não é a ela fundamental, não é o meio de realização do seu trabalho e, via de regra, a instituição como um todo é especialmente resistente a mudanças; consequentemente, quando estas ocorrem, pouco modificam ou refinam as práticas de policiamento de fato (MANNING, 2008, pp. 62-64).

A verdade é que as agências de segurança pública (e também de justiça), sobretudo, no Brasil, sequer têm sistemas unificados, integrados, que façam um conjunto coerente. São informações relativamente desconexas que parecem dispensar qualquer tipo de *inteligência*²⁸, artificial ou não, para a sua explicação e conversão em conhecimento útil. A tecnologia é que se adapta à estrutura existente e aos processos tradicionais de organizações muito burocratizadas, e não o contrário, até porque um potencial conhecimento “novo” não é necessariamente interessante – no policiamento e na justiça hoje praticados, não parece importar o porquê da incidência de um dado delito ou o motivo pelo qual os processos de criminalização secundária atingem algumas populações determinadas com mais vigor; basta responder aos anseios de “mais punição”, “mais ordem”, “mais rigor”, independentemente do que isso signifique na prática.

As organizações de segurança pública e de justiça criminal são conservadoras, reativas e resistentes à inovação, além de investidas de altas doses de confiança por boa parte da população, majoritariamente nos estratos dominantes. A tecnologia simula o ambiente em que se encontra, como um camaleão (MANNING, 2008, p. 64), e daí que se conclui: imersa ou não em inteligência artificial, a patrulha seguirá seletiva como sempre foi, mantendo-se tradicional e fiel às suas perspectivas fundamentais. A informação é moldada para se adequar a quem a detém, o que pode ser feito de forma aparentemente racional e desafetada de crenças individuais e, no limite, institucionais – que, na prática, são as responsáveis pela ordem do dia. Não basta discutir apenas os meios (tecnologia ou não tecnologia)

28. Não no sentido de capacidade cognitiva, mas sim, de habilidade de organização de informações e inferência de novos conhecimentos para fins de solução de problemas.

e não os fins e, principalmente, aqueles fins tácitos, não ditos. Ainda que existisse uma tecnologia perfeita, o que se sabe ser impossível, não seria possível confiar que, no âmbito do controle social do delito, a sua utilização seria *justa*, até porque o próprio conceito de justiça já seria enviesado.

O sistema de justiça criminal não se fundamenta em um conjunto neutro de regras e práxis, mas sim, em moralidade e política, ambos responsáveis por codificar as normas e os valores éticos *esperados*, assim como as próprias hierarquias sociais. O uso (e o abuso) de métodos atuariais, nessa seara, serve em grande escala para acentuar as dimensões ideológicas do sistema, endurecendo as disparidades de raça, classe e poder entre certos grupos, assim como para reforçar a percepção pública de que alguns são mais propensos ao crime do que outros (HARCOURT, 2007, p. 190). De onde, se as *sentinelas* seguem seletivos como sempre foram, aparelhados de tecnologia eles o fazem de forma mais “desprendida” e quase “imparcial”²⁹, remodelando e distorcendo ainda mais as frágeis concepções de justiça da sociedade. O mundo está moldando a tecnologia e esta, sim, remodela o mundo – produzindo conformidade.

4. DA URGÊNCIA DE UM DEBATE ÉTICO: PRIVACIDADE E SEGURANÇA – A QUEM SE DESTINAM?

É comum que entusiastas da *tecnologização* do controle social sugiram que a cessação de uma parcela da privacidade é sacrifício necessário para o incremento da segurança de todas as pessoas, como se tanto os custos quanto eventuais benefícios desta tendência tivessem impacto igualitário sobre o conjunto da população. Ora, nem neste, nem em qualquer outro contexto; a “sociedade como um todo” é apenas uma ficção e intervenções sociais são altamente complexas, especialmente no que se refere aos seus efeitos.

É empiricamente impossível a existência de sistemas perfeitos em sua vigência e suas consequências. Para que assim o fosse, seria necessária a existência, igualmente, de algo como uma inteligência ilimitada, de velocidade infinita, apta a gerir tal sistema em todas as suas falhas reais e potenciais. Como isto se sabe inalcançável – mesmo no auge da era digital –, a verdade é que inevitavelmente haverá vítimas, em maior ou menor escala, das imperfeições, dos erros, das exclusões, enfim, das injustiças do sistema (DUSSEL, 2000, p. 373).

29. “There is a real danger that algorithms can add an air of authority to an incorrect result (...). Just because the computer says something doesn’t make it so” (FRY, 2018, pp. 158-159).

A afirmação de que todo sistema faz vítimas (ainda que ocultas, ante a falsificações da verdade) é categórica, e, por isso, este deve ser o ponto de partida da crítica. Não existe uma pulsão interventora, em matéria social, que tende a atuar de maneira absolutamente gratuita, como se fizesse parte de um esquema perfeito. Para cada intervenção, há uma escolha de mediação: normas, ações, instituições e, sim, tecnologias, podem, apesar de pretenderem *fazer o bem*, causar vítimas – e o fazem o tempo todo. Daí a urgência de um debate ético: é dever de todos evitar que haja mais vítimas, conter desequilíbrios e injustiça, especialmente em sociedades muito desiguais, como a brasileira, nas quais existem *vítimas-padrão*, normalmente com classe e cor determinadas. Trata-se, sim, de uma obrigação ética (DUSSEL, 2000, p. 379).

A aplicação de tecnologias de inteligência artificial em larga escala, para fins penais, pode trazer benefícios? Talvez sim, a exemplo do aprimoramento de técnicas de reconhecimento facial em investigações e julgamentos (sem dúvidas, uma máquina bem treinada completa melhor esta tarefa que um humano, de memória muito mais limitada); da facilitação da localização e investigação de suspeitos de crimes muito graves, tais como estupro e homicídio³⁰; e até mesmo da viabilização de contraprovas mais robustas, que poderiam levar até mesmo à absolvição de pessoas inocentes. Mas a que custo? E o pior, a custo de quem?

Reforça-se: o sistema de justiça criminal age sob um regime de seletividade operativa que lhe é próprio, o que faz com que se criminalizem certas condutas, praticadas por determinadas pessoas, em detrimento de outras. Não existe isonomia ou proporcionalidade: existe uma ideia de conformação à ordem que se infiltra no tecido social por diversas vias – sendo a do controle do delito uma das principais –, a fim de manter determinados estratos em posição de comando e, ao mesmo tempo, conter os demais – sob uma expectativa de violência institucional caso não aceitem por completo as condições de vida a que estão expostos. E, sobre isso, é como se houvesse consenso: há ricos e há pobres, e o trabalho é a única via, seja ele qual for, ainda que o objetivo seja a sobrevivência pura e simples, e não o enriquecimento progressivo. Daí que, em algumas zonas, a violência é aceita, em todos os seus matizes, como normal e esperada.

Para além disso, a rede de contenção se amplia de forma ainda mais fluida, a partir das iniciativas atuariais; somado ao controle do delito e da desordem tradicionais, o manejo social do risco foca crescentemente no ideal

30. Que, diga-se de passagem, têm incidência ínfima se comparados, no Brasil, a delitos não violentos, como tráfico de drogas e furto, além de outros delitos patrimoniais, como roubo.

de segurança, desenvolvendo intervenções preventivas que possam, acreditar-se, diminuir as oportunidades de transgressão. Estratos populacionais inteiros tornam-se o delito em si mesmos; e a vigilância, por sua vez, concretiza-se como massificada e ininterrupta.

Para grupos que se encontrem no comando da ordem, talvez não seja um problema que agências de segurança pública detenham milhões de fotografias para a alimentação de seus sistemas; não parece problemático, igualmente, que a área em que residem seja um *hotspot* de controle, até porque, no mais das vezes, ela não o será – e, ainda que o fosse, a sua relação com a instituição policial é sempre muito amigável. Parece razoável abrir mão de parcelas de privacidade em prol de mais segurança; porque, no fim das contas, estas populações nunca ou quase nunca serão *selecionadas*. O mesmo não pode ser dito pelos estratos populacionais que, por sua mera existência, são tidos por incivilizados, imorais, desrespeitosos, perigosos e criminosos, no limite.

Para os alvos do controle, a delegação da privacidade não implica mais segurança – pelo contrário, potencializa distorções já existentes. Afinal, são enormes agrupamentos historicamente vivendo sem quaisquer garantias do Estado, sem acesso a serviços públicos de qualidade, sem códigos ou garantias, sem propriedade ou cidadania. O único braço estatal que os envolve, muitas vezes, é o penal – ainda que não tenham cometido crime algum; um *sucesso* do atuarialismo, frente ao suposto risco que apresentam.

Por tudo o que aqui se expôs, é possível sustentar que a associação de novas tecnologias à expansão do controle social amplia também este abismo social, por quatro motivos básicos: (i) a distribuição desproporcional de erros e injustiças das ferramentas de análise criminal, reconhecimento facial e predição como um todo; (ii) o aumento e a perpetuação das larguíssimas deturpações do sistema penal brasileiro; (iii) o incremento da violência a que estão sujeitas as populações marginais; e (iv) a estigmatização e o efeito social lateral, e não menos importante, de desmantelamento das comunidades locais.

O primeiro motivo é consequência direta, como se viu, dos preconceitos enraizados nas tecnologias mais comumente usadas em matéria de criminalidade, notadamente aquelas embasadas em aprendizado de máquina. Algoritmos, já se sabe, são enviesados e desfavorecem setores determinados da população, com destaque para as minorias raciais. Com efeito, se a identificação de rostos de pele negra, por exemplo, é assumidamente menos eficaz que o reconhecimento de rostos de pele branca, é de se esperar que a população negra sofra desproporcionalmente com falsos-positivos, do que decorreriam investigações ou, o que é pior, condenações injustas – e, não por isso, menos estigmatizantes. De igual

maneira, uma vez que o sistema carcerário brasileiro seleciona jovens negros como seu alvo preferencial, é razoável a expectativa de que, caso sejam objeto de tecnologias de predição, estes sejam alocados em faixas de risco alto no que se refere a delinquências futuras – o que poderia justificar sentenças maiores ou, quiçá, impedimentos à liberdade condicional, por exemplo.

Quanto ao segundo motivo, em boa parte conectado ao primeiro, não é difícil visualizar que o uso de métodos atuariais e inteligência artificial deve acentuar disparidades sistemáticas reinantes, como o encarceramento em massa da população negra. Afinal, se a máquina aprende que este setor populacional é o alvo, vez que historicamente mais preso (provisória e definitivamente), perpetua-se esta condição ao longo do tempo; igualmente, se as áreas em que se encontram são sinalizadas como mais perigosas, incrementando-se o seu policiamento, mais prisões serão realizadas, visto que, logicamente, onde mais se procura, mais se acha. O raciocínio é simples: se se dedicam mais recursos para investigar e prender membros de um mesmo grupo perfilado, a distribuição de abordagens e prisões no interior deste grupo os representará, contínua e desproporcionalmente, como mais infratores – ainda que a mesma quantidade de crimes esteja ocorrendo em outras áreas e por intermédio de autores diversos (HARCOURT, 2007, pp. 147-149). Quanto mais o algoritmo prevê, mais a polícia se desloca para um dado lugar, mais crimes são encontrados, e o ciclo se perpetua (FRY, 2018, p. 157). A amostragem nunca será aleatória e a representação de uma dada população, assim, no caso brasileiro, provavelmente pobre e negra, será inescapavelmente desproporcional. Mais negros vigiados; mais negros processados; mais negros presos.

O terceiro motivo, por sua vez, em muito diz respeito ao fato de que existe uma espécie de consenso tácito no sentido de que a violência como *modus operandi* é realidade das comunidades periféricas, o que quase legitimaria ações policiais violentas que, apesar de subnotificadas, fazem parte do ciclo de agressões diárias a que se submete uma considerável parte da população mais pobre e negra. Não é incompreensível, destarte, que ações direcionadas por algoritmos possam levar consigo doses ainda mais altas de barbaridade – e que as pessoas se sintam, portanto, incomodadas ou até mesmo amedrontadas com a simples presença da polícia ao redor das suas casas, ainda que não estejam cometendo qualquer crime.

Nessa linha, pesquisas demonstram que o direcionamento excessivo do policiamento para determinadas áreas (e certos grupos) frequentemente anda de mãos dadas com o aumento das queixas de brutalidade policial – muito difícil de metrificar e quantificar, frise-se, haja vista a áurea de medo que paira sobre eventuais denúncias. Conforme a análise de Jon Gould e Stephen Mastrofski, que acompanharam operações de busca junto a um dado departamento de polícia

norte-americano, durante ações de policiamento direcionado, cerca de 30% das ações, segundo uma estimativa conservadora, foram inconstitucionais – ainda que quaisquer impactos legais tenham sido observados a este respeito. Ainda, a taxa de buscas inconstitucionais se mostrou ainda mais alta para suspeitos posteriormente libertados, acometendo 44% destes casos, além de os dados sugerirem que as abordagens se embasaram em perfilamento racial: 84% das buscas estudadas envolveram pessoas negras (HARCOURT, 2007, pp. 169-170). A violência se renova e se acomoda no tempo – a segurança garantida por cálculos e estatísticas certamente não abarca todas as pessoas com similitude.

Por fim, o quarto motivo, sem dúvidas resultante de todos os anteriores, está centrado, principalmente, na distribuição diferencial de registros criminais, com inúmeras implicações devastadoras para os membros de um dado grupo perfilado. Não é mistério que uma única passagem pela polícia pode ser extremamente prejudicial à consecução de garantias fundamentais como educação e emprego, e à manutenção de laços familiares. Vigilância, processamento e encarceramento desproporcionais reduzem oportunidades de trabalho, desagregam famílias e, não raramente, comunidades inteiras. Há crianças que crescem com a convicção de que algum dia serão presas ou, no mínimo, abordadas – e aprendem com seus pais como reagir (ou não reagir) a essas situações, ainda que nada tenham feito. Grupos sociais visados, ante à chance generalizada de captação pelo sistema de justiça criminal, podem ver comprometida a sua própria capacidade de investimentos em capital humano (HARCOURT, 2007, pp. 160-161) – inúteis, visto que, como se pode imaginar, o investimento de dinheiro e tempo em educação ou treinamento profissional não superará o estigma de uma condenação ou prisão, devidas ou não, comprometendo interações interpessoais e a formação de núcleos familiares estáveis.

Daí que, no debate ético-crítico da introdução de novas tecnologias para fins de controle social, há que se reconhecer que as vítimas da inteligência artificial serão as mesmas vítimas de sempre, às quais se veem negadas as possibilidades de viver propriamente, seja na totalidade, seja em algum momento específico da vida. No mínimo, vale a confirmação dos direitos humanos (de todos eles) como um *standard* de avaliação das condições que práticas e instituições devem atender se quiserem ser consideradas legítimas (MATTHEWS, 2014, p. 48). Dever ético, contudo, para além disso, é tomar a responsabilidade pela vitimização e cumprir com exigências transformadoras o bastante para que a vítima deixe de sê-lo, não só individual, mas comunitariamente (DUSSEL, 2000, pp. 380-382).

A tecnologia muda o mundo, mas, assim como ocorre com outras ferramentas, ações e instituições, os seus benefícios não se distribuem de forma homogênea.

Mais que isso, as falhas do seu emprego também se repartem distintamente, com prejuízos concentrados em setores sociais específicos, o que se torna particularmente grave em âmbito criminal. A paz a qualquer custo é custosa (WILLIS, 2015, p. 156) e, daí, a necessidade da crítica: apenas a obrigação ética de transformação da realidade que vitimiza certos estratos apenas pela sua existência enquanto tal pode, de fato, garantir-lhes, em alguma medida, a realização plena da vida.

5. CONSIDERAÇÕES FINAIS

O mundo vive a era da informação e da digitalização, mas, nem por isso, as estratégias de governo de pessoas se deixam conhecer totalmente – e, quando o fazem, não costumam expor as suas finalidades latentes. Como consequência disso, problemas reais, como a criminalidade, acabam sendo erroneamente interpretados; e estas percepções equivocadas acabam levando à formulação, como se viu, de monstros imaginários. A partir daí, os anseios desmedidos por proteção (advindos de classes que, no geral, estão altamente protegidas nas grandes cidades) servem como um pretexto perfeito para a implementação de técnicas modernas de vigilância e controle, sob a contrapartida, em um primeiro momento, da “entrega” de quinhões de privacidade a agências privadas e públicas de segurança – o que se mostra, sem dúvida, como apenas uma pequena parcela da enorme problemática que envolve a inserção de novas tecnologias, particularmente de inteligência artificial, no contexto do controle social formal.

A tecnologia é melindrosa; parece superar a própria capacidade humana quando, na verdade, depende totalmente do ambiente em que está inserida e, é claro, dos “alimentos” fornecidos pelos seus desenvolvedores. Na prática, contudo, apresenta-se como exclusivamente racional e soberana, o que dificulta sobremaneira o combate a quaisquer dos seus produtos decisórios; afinal, as máquinas nem sempre são compreensíveis, sequer para os seus operadores, e, no limite, não se busca efetivamente qualquer explicação – o que se quer, com efeito, é *acreditar*.

Acreditar que existem grupos criminosos em potencial e que a sua exclusão é esperada e justa, e que, não por menos, como em uma profecia autorrealizável, serão eles continuamente selecionados pelo sistema, em um ciclo infinito. Acreditar que computadores podem prever o futuro e que, por isso, jamais errarão em suas análises. Acreditar, por fim, que o prejuízo de alguns pobres coitados, “confundidos” pelos algoritmos, não é suficiente para impedir a guarida da sociedade como um todo – ao menos do *todo* que, apenas muito raramente, cairá nas malhas da teia punitiva.

A realidade que se apresenta nesta pesquisa, contudo, mostra que estas crenças não só são absurdas como são, de igual maneira, absolutamente infundadas. O crime é um fenômeno multifatorial e complexo, e não pode ser explicado pela associação direta a determinadas classes de pessoas. Máquinas não preveem o futuro, mas apenas refletem o aprendizado a que foram submetidas, tomando decisões, no plano prático, com potencial altamente discriminatório. Não existe, finalmente, *confusão*, mas seleção historicamente associada às distorções a que, ao que parece, sociedades tão desiguais, como a brasileira, já se acostumaram.

Sistemas perfeitos não existem e, a todo o tempo, fazem suas vítimas. Torna-se preciso, assim, combater a naturalização dessa vitimização, no que se refere ao avanço de técnicas informatizadas de controle social, expondo os seus matizes e buscando, por meio de balizas reais, a redução de injustiças. Nesse sentido, há que se dizer que é difícil “resistir” à tecnologia e à urgência preditiva do tempo presente, mas esta tarefa se torna facilitada quando se apontam as suas contradições. Reforça-se: apesar de quaisquer benefícios em potencial, a utilização massiva de novas tecnologias para fins de vigilância e controle, especialmente do delito, tende apenas a potencializar o cenário de enorme marginalização a que já está submetida boa parcela da população, marcada por classe e cor. E cabe à crítica ética conter, no que lhe for possível, o avanço desta fábrica de distorções.

6. REFERÊNCIAS

- ALVAREZ, Marcos César. *Bacharéis, criminologistas e juristas: saber jurídico e nova escola penal no Brasil*. São Paulo: Método, 2003.
- BARATTA, Alessandro. *Criminologia crítica e crítica do direito penal*. Introdução à sociologia do direito penal. 6. ed., Rio de Janeiro: Revan, 2011.
- BATISTA, Nilo. *Introdução crítica ao direito penal brasileiro*. 11. ed. Rio de Janeiro: Revan, 2007.
- BATISTA, Nilo. Pena pública e escravidão. *Cap. Crim.* v. 34, n. 3, pp. 279-321, jul./set. 2006.
- CASTRO, Lola Anyar. *Criminologia da libertação*. Rio de Janeiro: Revan: ICC, 2005.
- CHIAO, Vincent. Fairness, accountability and transparency: notes on algorithmic decision-making in criminal justice. In: *International Journal of the Law in Context*. Cambridge: Cambridge University Press, 15(2), 2019, pp. 126-139.
- DE GIORGI, Alessandro. *A miséria governada através do sistema penal*. Rio de Janeiro: Revan: Instituto Carioca de Criminologia, 2006.
- DIETER, Maurício Stegemann. Política criminal atuarial: a criminologia do fim da história.

- DONEDA, Danilo. *Da privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de Proteção de Dados*. São Paulo: Thompson Reuters Brasil, 2019.
- DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel; RODRIGUES JUNIOR, Otavio Luiz. *Tratado de proteção de dados pessoais*. Rio de Janeiro: Forense, 2021.
- DUSSEL, Enrique. *Ética da libertação na idade da globalização e da exclusão*. Petropolis: Vozes, 2000.
- EDWARDS, Lilian; VEALE, Michael. Slave to the algorithm? Why a 'right to an explanation' is probably not the remedy you are looking for. In: *Duke Law and Technology Review*, Durham: Duke Law and Technology Review, v. 16, pp. 18-84, 2017.
- FOUCAULT, Michel. *Microfísica do poder*. 25. ed. São Paulo: Graal, 2012.
- FRY, Hannah. *Hello world: being human in the age of algorithms*. New York: W. W. Norton & Company, 2018.
- GARRETT, Brandon L. *Convicting the innocent: where criminal prosecutions go wrong*. Cambridge: Harvard University Press, 2011.
- HARCOURT, Bernard E. *Against prediction: profiling, policing, and punishing in an actuarial age*. Chicago: The University of Chicago Press, 2007, 336 p.
- HORNUNG, Gerrit; SCHNABEL, Christoph. Data protection in Germany I: the population census decision and the right to informational self-determination. In: *Computer Law & Security Review*, London: Sweet & Maxwell, v. 25, pp. 84-88, 2009.
- IGO, Sarah E. *The unknown citizen: a history of privacy in modern America*. Cambridge: Harvard University Press, 2018.
- KAPLOW, Louis; SHAVELL, Steven. Economic analysis of law. In: *Handbook of Public Economics*. Amsterdam: Elsevier, v. 3, pp. 1661-1784, 2002.
- KOUTSIAS, Marios. Privacy and data protection in an information society: how reconciled are the English with the European Union privacy norms? In: *Computer and Telecommunications Law Review*, London: Sweet & Maxwell, 18(8), pp. 261-270, 2012.
- LYNSKEY, Orla. Criminal justice profiling and EU data protection law: precarious protection from predictive policing. In: *International Journal of the Law in Context*, Cambridge: Cambridge University Press, pp. 162-176, 2019.
- MANNING, Peter K. *The technology of policing: crime mapping, information technology, and the rationality of crime control*. New York and London: New York University Press, 2008.
- MATTHEWS, Roger. *Realist criminology*. London: Palgrave Macmillan, 2014.
- MELOSSI, Dario; PAVARINI, Massimo. *Cárcere e fábrica: as origens do sistema penitenciário (séculos XVI-XIX)*. 2. ed. Rio de Janeiro: Revan, 2010.

- MONTEIRO, Renato Leite. Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil? In: *Instituto Igarapé*. Artigo estratégico, n. 39, dez. 2018.
- O'BEIRNE, Brian. The European Court of Human Rights' recent expansion of the right of privacy: a positive development? In: *Coventry Law Journal*, Coventry: Coventry University, 14(2), pp. 14-22, 2009.
- RODOTÀ, Stefano. *Tecnologie e diritti*. Bologna: Mulino, 1995.
- RUSCHE, Georg; KIRCHHEIMER, Otto. *Punição e estrutura social*. 2. ed. Rio de Janeiro: Revan, 2004.
- SALLA, Fernando. *As prisões em São Paulo: 1822-1940*. São Paulo: Annablume/Fapesp, 1999.
- SANTOS, Juarez Cirino dos. *A criminologia da repressão: uma crítica ao positivismo em criminologia*. Rio de Janeiro: Forense, 1979.
- SIMÃO, Bárbara; FRAGOSO, Nathalie; ROBERTO, Enrico; *Reconhecimento facial e o setor privado: guia para a adoção de boas práticas*. InternetLab/IDEC, São Paulo, 2020.
- TAYLOR, Roger. No privacy without transparency. In: LEENES, Ronald; VAN BRAKEL, Rosamunde; GUTWIRTH, Serge; DE HERT, Paul. *Data protection and privacy: the age of intelligent machines*. Oxford: Hart Publishing, 2017.
- TESE (Doutorado) – Faculdade de direito da Universidade Federal do Paraná. Curitiba, 2012.
- WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. In: *Harvard Law Review*, Cambridge: The Harvard Law Review Association, v. 4, n. 5, pp. 193-220, 1890.
- WILLIS, Graham Denyer. *The killing consensus: police, organized crime, and the regulation of life and death in Urban Brazil*. Oakland: University of California Press, 2015.
- YOUNG, Jock. From inclusive to exclusive society: nightmares in the European dream. In *The new European criminology: crime and social order in Europe*. London and New York: Routledge, 1998, pp. 64-91.
- YU, Ronald; ALI, Gabriele Spina. What's inside the black box? AI challenges for lawyers and researchers. In: *Legal Information Management*, Cambridge: Cambridge University Press, 19 (1), 2019, pp. 2-13.

Referências da internet

- ALISSON, Elton. Sistema usa inteligência artificial para prever ocorrências de crimes em áreas urbanas. *Agência FAPESP*, São Paulo, 31 jul. 2020. Disponível em: [<https://agencia.fapesp.br/sistema-usa-inteligencia-artificial-para-prever-ocorrencias-de-crimes-em-areas-urbanas/33768/>]. Acesso em: 25.03.2021.

- ANGWIN, Julia; LARSON, Jeff; MATTU, Surya. Machine Bias: there's software used across the country to predict future criminals. And it's biased against blacks. *ProPublica*, New York, 23 mai. 2016. Disponível em: [https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing]. Acesso em: 26.03.2021.
- BRASIL. Câmara dos Deputados. *Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal*, 2020. Disponível em: [https://static.poder360.com.br/2020/11/DADOS-Anteprojeto-comissao-protacao-dados-seguranca-persecucao-FINAL.pdf]. Acesso em: 24.03.2021.
- BURT, Chris. Investigation reveals Dahua biometric systems sent ethnicity warnings to Chinese police. *BiometricUpdate.com*, Toronto, 10 fev. 2021. Disponível em: [https://www.biometricupdate.com/202102/investigation-reveals-dahua-biometric-systems-sent-ethnicity-warnings-to-chinese-police]. Acesso em: 28.03.2021.
- CHANG, Cindy. LAPD officials defend predictive policing as activists call for its end. *Los Angeles Times*, Los Angeles, 24 jul. 2018. Disponível em: [https://www.latimes.com/local/lanow/la-me-lapd-data-policing-20180724-story.html].
- HAO, Karen. This i show AI bias really happens – and why it's so hard to fix. *MIT Technology Review*, Massachusetts, 4 fev. 2019. Disponível em: [https://www.technologyreview.com/2019/02/04/137602/this-is-how-ai-bias-really-happens-and-why-its-so-hard-to-fix/]. Acesso em: 26.03.2021.
- HILL, Kashmir. Your face is not your own. *The New York Times*, New York, 18.03.2021. Disponível em: [https://www.nytimes.com/interactive/2021/03/18/magazine/facial-recognition-clearview-ai.html?smid=li-share]. Acesso em: 29.03.2021.
- INFOPEN. *Levantamento Nacional de Informações Penitenciárias*, jun. 2018. Disponível em: [https://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-permanentes/cdhm/noticias/sistema-carcerario-brasileiro-negros-e-pobres-na-prisao]. Acesso em: 23.03.2021.
- INSTITUTO DE DEFESA DO DIREITO DE DEFESA. *Monitoramento das audiências de custódia em São Paulo*. São Paulo, SP, 2016. Disponível em: [http://www.iddd.org.br/wp-content/uploads/2016/05/Relatorio-AC-SP.pdf]. Acesso em: 28.03.2021.
- MEISSNER, Christian A.; BRIGHAM, John C. Thirty years of investigating the own-race bias in memory for faces: a meta-analytic review. *Psychology, Public Policy, and Law*, v. 7, n. 1, 2001, 3-17. In: SUPERIOR TRIBUNAL DE JUSTIÇA. *Habeas Corpus* 619.327/RJ. Disponível em: [http://www.iddd.org.br/wp-content/uploads/2020/12/amicus-tiago-vianna-final-sem-assinaturas.pdf]. Acesso em: 26.03.2021.
- PICCHI, Aimee. How tech's white male workforce feeds bias into AI. *CBS News*, New York, 17 abr. 2019. Disponível em: [https://www.cbsnews.com/news/ai-bias-problem-techs-white-male-workforce/]. Acesso em: 26.03.2021.

- PRUDENTE, Eunice. Dados do IBGE mostram que 54% da população brasileira é negra. *Jornal da USP*, São Paulo, 31 jul. 2020. Disponível em: [https://jornal.usp.br/radio-usp/dados-do-ibge-mostram-que-54-da-populacao-brasileira-e-negra/]. Acesso em: 24.03.2021.
- REBELLO, Aiuri. Bancada do PSL vai à China conhecer sistema que reconhece rosto de cidadãos. *Folha de S. Paulo*, São Paulo, 16 jan. 2019. Disponível em: [https://www1.folha.uol.com.br/mercado/2019/01/bancada-do-psl-vai-a-china-importar-sistema-que-reconhece-rosto-de-cidadaos.shtml]. Acesso em: 24.03.2021.
- REDE DE OBSERVATÓRIOS DE SEGURANÇA. *A cor da violência policial: a bala não erra o alvo*. Rio de Janeiro: Centro de Estudos de Segurança e Cidadania, 2020. Disponível em: [http://observatorioseguranca.com.br/wp-content/uploads/2020/12/A-Cor-da-Violência-Policial-A-Bala-Não-Erra-o-Alvo.pdf]. Acesso em: 27.03.2020.
- UNIÃO EUROPEIA. Regulation (EU) 2016/679 of the European Parliament and of the Council. 27 abr. 2016. *Official Journal of the European Union*. Disponível em: [https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679]. Acesso em: 29.03.2021.
- UNIÃO EUROPEIA. Regulation (EU) 2016/680 of the European Parliament and of the Council. 27 abr. 2016. *Official Journal of the European Union*. Disponível em: [https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680&from=EN]. Acesso em: 29.03.2021.
- WINSTON, Ali. Transparency advocates win release of NYPD “predictive policing” documents. *The Intercept*, Los Angeles, 27 jan. 2018. Disponível em: [https://theintercept.com/2018/01/27/nypd-predictive-policing-documents-lawsuit-crime-forecasting-brennan/]. Acesso em: 29.03.2021.



PESQUISAS DO EDITORIAL



ÁREAS DO DIREITO: Penal; Digital

Veja também Doutrinas relacionadas ao tema

- Controle social, punição e racismo: os casos encaminhados ao centro de referência em direitos humanos da DPE/RS, de Rodrigo Ghiringhelli de Azevedo, Luíza Correa de Magalhães Dutra e Osmar Antônio Belusso Júnior – *RBCCrim* 148/549-577;
- Responsabilidade penal de inteligência artificial: uma análise sob a ótica do naturalismo biológico de John Searle, de Sthéfano Bruno Santos Divino – *RBCCrim* 171/153-183;
- Seletividade penal no estado de exceção permanente: um estudo sobre a exclusão dos dados sobre violência policial do relatório de direitos humanos, de Nelson Camatta Moreira e Ronaldo Félix Moreira Júnior – *RBCCrim* 188/423-445; e
- Uma proposta taxonômica para um *big data* jurisdicional: o problema do uso da inteligência artificial e a proteção de dados processuais no ambiente da justiça 4.0, de Alexandre Freire Pimentel – *RePro* 330/391-413.