

Governamentalidade algorítmica e tecnologias de reconhecimento facial: reconfigurações punitivas no contexto brasileiro*

Tiago Luis Schervenski da Silva e Ricardo Jacobsen Gloeckner

Recebido: 31 de março de 2025 | Aceito: 21 de julho de 2025 | Modificado: 11 de agosto de 2025
<https://doi.org/10.7440/res94.2025.05>

Resumo | Este artigo investiga as transformações das práticas punitivas contemporâneas no contexto social atual, no qual os dados e os algoritmos assumem um papel central nas dinâmicas de poder e controle. Procura-se responder à questão sobre qual é a função dos algoritmos nas práticas punitivas atuais e quais são os seus efeitos. Para isso, analisa-se o uso de tecnologias de reconhecimento facial na segurança pública brasileira, particularmente nos estados da Bahia e de Goiás. Por meio de revisão bibliográfica, explora-se o cenário *biopolítico* contemporâneo, marcado pela crise dos meios tradicionais de confinamento. Diante dessa crise, emergem novas formas de controle que se desvinculam das tecnologias carcerárias e estabelecem mecanismos de vigilância em espaços abertos, fundamentados em *dispositivos securitários* e na lógica da gestão de risco. Nesse contexto, os dados se tornam essenciais para as práticas punitivas, impulsionando o desenvolvimento de técnicas refinadas de vigilância. O artigo examina como os sistemas informáticos em rede capturam, processam e utilizam esses dados, investigando sua lógica e racionalidade. A pesquisa busca compreender como esses dispositivos podem produzir resultados enviesados, especialmente contra pessoas racializadas e em situação de vulnerabilidade de gênero. Os resultados evidenciam que (i) o uso dessa tecnologia apresenta viés discriminatório que reforça as desigualdades raciais e de gênero no contexto da vigilância; e (ii) essas tecnologias inflamam a vigilância e o gerenciamento de dados sob uma racionalidade pretensamente objetiva que, por fim, serve para criar perfis preditivos e proferir vereditos silenciosos sobre os sujeitos.

Palavras-chave | algoritmos; controle social; governamentalidade algorítmica; práticas punitivas; tecnologias de reconhecimento facial

* O presente artigo resulta do trabalho de conclusão de curso em Direito apresentado pelo primeiro autor em dezembro de 2024, na Pontifícia Universidade Católica do Rio Grande do Sul (Brasil), sob a orientação do coautor. Além disso, é fruto de uma pesquisa desenvolvida no âmbito da iniciação científica, entre 2023 e 2024. Um ensaio preliminar, elaborado no início de 2024, foi posteriormente publicado como capítulo de livro (*Algoritmos II*, editado por Augusto Jobim do Amaral, Jesús Sabariego e Ana Clara Elesbão, Valência: Tirant lo Blanch, 2025), igualmente derivado dessa investigação. A presente versão apresenta mudanças substanciais em relação ao ensaio, oferecendo maior densidade teórica, robustez argumentativa e rigor analítico, trazendo o embasamento teórico à análise de dados da experiência brasileira e sistematizando integralmente os resultados obtidos. O autor principal foi responsável pela revisão bibliográfica, pela sistematização das ideias e pela redação do manuscrito, enquanto o coautor colaborou com a supervisão, revisão crítica e aprimoramento do texto. Não foram utilizadas ferramentas de inteligência artificial na elaboração deste artigo.

Gubernamentalidad algorítmica y tecnologías de reconocimiento facial: reconfiguraciones punitivas en el contexto brasileño

Resumen | Este artículo investiga las transformaciones de las prácticas punitivas contemporáneas en el contexto social actual, en el que los datos y los algoritmos asumen un papel central en las dinámicas de poder y de control. Se busca responder a la pregunta sobre cuál es la función de los algoritmos en las prácticas punitivas actuales y cuáles son sus efectos. Para ello, se analiza el uso de tecnologías de reconocimiento facial en la seguridad pública brasileña, particularmente en los estados de Bahia y Goiás. A partir de una revisión de literatura, se explora el escenario *biopolítico* contemporáneo, marcado por la crisis de los medios tradicionales de confinamiento. Ante esta crisis, surgen nuevas formas de control que se desvinculan de las tecnologías penitenciarias y establecen mecanismos de vigilancia en espacios abiertos, basados en *dispositivos de seguridad* y en la lógica de la gestión de riesgos. En este contexto, los datos se vuelven esenciales para las prácticas punitivas impulsando el desarrollo de técnicas de vigilancia refinadas. El artículo examina cómo los sistemas informáticos en red capturan, procesan y utilizan estos datos ahondando en su lógica y racionalidad. La investigación busca comprender cómo estos dispositivos pueden producir resultados sesgados, especialmente contra personas racializadas y en situación de vulnerabilidad de género. Los resultados muestran que (i) el uso de esta tecnología presenta un sesgo discriminatorio que refuerza las desigualdades raciales y de género en el contexto de la vigilancia; y (ii) estas tecnologías encienden la vigilancia y la gestión de datos bajo una racionalidad supuestamente objetiva que, finalmente, sirve para crear perfiles predictivos y pronunciar veredictos silenciosos sobre los sujetos.

Palabras clave | algoritmos; control social; gubernamentalidad algorítmica; prácticas punitivas; tecnologías de reconocimiento facial

Algorithmic Governmentality and Facial Recognition Technologies: Punitive Reconfigurations in the Brazilian Context

Abstract | This article analyzes the transformations of contemporary punitive practices in today's social context, where data and algorithms have assumed a central role in dynamics of power and control. It addresses the question of what role algorithms play in current punitive practices and what effects they generate. To this end, it examines the use of facial recognition technologies in Brazilian public security, with a focus on the states of Bahia and Goiás. Based on a review of the literature, the study explores the contemporary *biopolitical* landscape, marked by the crisis of traditional mechanisms of confinement. In response to this crisis, new forms of control have emerged that move beyond penitentiary technologies and establish surveillance mechanisms in open spaces, grounded in *security devices* and the logic of risk management. Within this framework, data become essential to punitive practices, driving the development of increasingly sophisticated surveillance techniques. The article investigates how networked computer systems capture, process, and deploy this data, examining the underlying logic and rationality. The research seeks to understand how these devices can produce biased outcomes, particularly against racialized individuals and those in situations of gender vulnerability. The findings indicate that (i) the use of this technology embeds a discriminatory bias that reinforces racial and gender inequalities in the context of surveillance; and (ii) these technologies intensify surveillance and data management under a supposedly objective rationality that ultimately generates predictive profiles and delivers silent verdicts on individuals.

Keywords | algorithms; algorithmic governmentality; facial recognition technologies; punitive practices; social control

Breves apontamentos sobre as sociedades de controle

Diante da expansão global da tecnologia de reconhecimento facial, presente em diversos contextos sociais e comerciais, o presente artigo investiga a lógica desses dispositivos, definindo o escopo da análise realizada em relação à segurança pública no Brasil. Com esse objetivo, pretende-se desenvolver reflexões de caráter jurídico-filosófico, analisando os dados resultantes da atuação desses mecanismos, os quais revelam uma notável ineficiência, mesmo diante do expressivo investimento realizado para sua implementação no contexto brasileiro. Para o intento, procuramos lançar luz ao modo de funcionamento de tais ferramentas baseadas em algoritmos e, uma vez explicitado brevemente o seu funcionamento, busca-se desvelar a racionalidade desses dispositivos, argumentando-se que a lógica na implementação das tecnologias de reconhecimento facial busca a segurança, isto é, uma nova maneira de pensar a penalidade de modo que essas ferramentas passem a somar às estruturas de mecanismos de segurança já conhecidas. Por fim, busca-se suscitar os impactos sociais que o uso (in)discriminado do dispositivo causa, respaldado por trás de seu opaco véu da objetividade e da neutralidade.

Assim, o presente trabalho está estruturado em cinco seções. Na introdução, contextualizamos o problema e apresentamos os objetivos centrais da pesquisa. Na seguinte seção, abordam-se brevemente as sociedades de controle, com ênfase nos contornos da biopolítica contemporânea e na transição das disciplinas para os mecanismos securitários. Na terceira seção, examinamos a emergência da governamentalidade algorítmica, detalhando suas três etapas operacionais — *datavellance*, *datamining* e *datanticipating* — e discutindo críticas e consequências do uso de algoritmos em práticas de segurança. A quarta parte analisa a aplicação das tecnologias de reconhecimento facial na segurança pública brasileira, com atenção especial aos casos dos estados da Bahia e de Goiás, explorando seus impactos e a ausência de transparência e regulamentação adequada. Por fim, nas conclusões, enfatizamos que o principal aspecto a ser desvelado na lógica opaca das tecnologias algorítmicas reside no fato de que os modelos que as constituem são resultado de escolhas humanas, orientadas por interesses econômicos, políticos e sociais, além de marcadas por diferenças culturais. Assim, ainda que reivindicuem objetividade e neutralidade, tais tecnologias tendem a reproduzir — e, em certos casos, intensificar — efeitos discriminatórios como parte de seu funcionamento.

Para o estudo da emergência dos novos mecanismos de controle da contemporaneidade, importa fazer uma breve digressão que ressalte como as formas características presentes nas *sociedades disciplinares* — fixadas nos limites da organização dos meios de confinamento (prisões, hospitais, escolas, fábricas), presentes nos séculos 18 e 19, com seu ápice no início do século 20 — apresentam-se em crise (Deleuze 1992b) ou, melhor, em franco processo de metamorfose desde, pelo menos, a transição do século 20 para o 21.

Ao fim do século 20, foi sentida a ineficácia relativa entre o cárcere e a vigilância — binômio presente nas *sociedades disciplinares* —, o que ocasionou a desconfiança das próprias instituições em suas técnicas de subjetivação (Rodriguez 2019). Destarte, foi atestada a incapacidade de essas formas sociais atingirem os fins que lhes eram dispostos — concentração e distribuição do espaço, bem como ordenação do tempo para maximizar a força produtiva dos sujeitos disciplinados (Deleuze 1992b) —, e a consciência da crise pelas próprias instituições foi o que propiciou o solo para antecipações e metamorfoses em suas técnicas (Rosa e Amaral 2017).

Assim, se a crise se faz incessantemente presente, esta só poderia ser vista como um “combate de retaguarda”, visando à implementação de novas formas de controle (Deleuze 1992a). Não por acaso, as próprias instituições de confinamento são as primeiras a perceberem a situação alarmante em que se encontram, ocasionando os diversos e constantes discursos de “reforma” (Amaral 2017). Não obstante, são das crises que surgem as

oportunidades dessas reformas, que servem, justamente, a propiciar uma fórmula de escape de sua ruína (Rosa e Amaral 2017). Daí depreende-se que, por meio das contínuas crises, na verdade ocorre um movimento de autofortalecimento do capitalismo — sendo esses momentos de “instabilidade” os instantes notáveis para percebermos a sua capacidade de metamorfose (Amaral 2020a). Logo, tomaremos a crise dos interiores — institucionais e subjetivos — como o ponto-chave para a compreensão do panorama *biopolítico*¹ da contemporaneidade (Rodríguez 2019), pois são “das candentes e sempre urgentes ‘reformas’, que nascem as novas configurações de *controle*” (Rosa e Amaral 2017, 52-53, grifos no original).

Nesse horizonte, pode-se perceber que, pelo menos desde os anos 1970, e com maior ênfase nos últimos 30 anos, as tecnologias de vigilância vêm operando um processo de deslocamento em relação às tecnologias de cárcere (Rodríguez 2019). Essas recentes transformações, inscritas em um hodierno contexto social em que o interior e o exterior possuem fronteiras arenosas, traçam um novo horizonte para a aplicação de um obscuro *biopoder*. Tal processo não implica substituição, mas antes o deslocamento das sociedades disciplinares em direção às sociedades de controle (Mendes 2020).

Importa compreender que não se está diante do esgotamento das *sociedades disciplinares*, mas já não nos limitamos mais a isso, e a ascensão dos novos mecanismos de sanção demonstram esse caráter (Amaral 2017). Não veremos, no entanto, os mecanismos de segurança tomarem o lugar por completo dos mecanismos disciplinares; ao contrário, esses mecanismos abrem novos espaços de punição, em que veremos as *disciplinas* e os *biopoderes* em constante interação (Chignola 2018). Não há, portanto, uma “era securitária”; a mudança que veremos será de aparição de novas técnicas punitivas e seus aperfeiçoamentos (Foucault 2008a). Da mesma forma, a própria disciplina se reconfigura no século 21. Basta uma rápida análise no campo do trabalho na transição para o século 21 para perceber a emergência de novas disciplinas: da insegurança perene no trabalho aos guias de boas práticas, *benchmarking* e outras técnicas. Trata-se de disciplinas que se reconfiguraram, o que é necessário reconhecer.

Considerando que as tecnologias de poder não podem ser vistas como sucessões, ou seja, uma era das disciplinas que antecederia uma era securitária (Amaral 2020a), essas tecnologias se manifestam de um modo muito mais complexo. É nesse horizonte que situamos o poder punitivo, assumindo-o, neste artigo, como um *conjunto prático*, isto é, “[...] uma espécie de homogeneidade, um domínio de referência daquilo que os homens fazem (tecnologias) e como fazem (estratégias)” (Amaral 2020b, 41). Isso quer dizer que esse conjunto de fenômenos, mecanismos e técnicas são dispostos em situações estratégicas (Foucault 1995). A homogeneidade, segundo Foucault, “[...] é assegurada, portanto, por esse domínio de práticas com sua versão tecnológica e sua versão estratégica” (2006, 94). Trata-se, enfim, de um conjunto de ações sobre ações possíveis, que estrutura o campo de ação dos outros, conduzindo condutas e ordenando possibilidades (Foucault 1995).

Desse modo, a coexistência estratégica das tecnologias de poder — de soberania, disciplinares ou securitárias — ajuda a formar edifícios complexos de punição que se retroalimentam, estando em constante trânsito e contaminações. Para a análise, vale perceber qual dos sistemas de correção que se estabelece na contemporaneidade, ou seja, qual deles se exerce com maior predominância (Amaral 2020a). Diante desse contexto, o problema da penalidade e das suas reconfigurações, atualmente, deve se estabelecer nos

1 “O conjunto dos mecanismos pelos quais aquilo que, na espécie humana, constitui suas características biológicas fundamentais vai poder entrar numa política, numa estratégia política, numa estratégia geral de poder; em outras palavras, como a sociedade, as sociedades ocidentais modernas, a partir do século 18, tomaram em conta o fato biológico fundamental de que o ser humano constitui uma espécie humana” (Foucault, 2008a, 3).

termos da *segurança*: “uma maneira de somar, de fazer funcionar, além dos mecanismos de segurança propriamente ditos, as velhas estruturas da lei e da disciplina” (Foucault 2008a, 26). Justamente por isso que não veremos o desaparecimento das práticas punitivas estatais que subjagam, corrigem e disciplinam os corpos — como as prisões. A *segurança*, enquanto forma de pensar a punição, faz erigir, multiplicar, reativar e transformar os antigos mecanismos disciplinares (Amaral 2020a).

Os moldes da biopolítica contemporânea

Os dispositivos securitários emergem das brechas criadas pelas crises das instituições de confinamento e serão utilizados como estratégia para organizar uma biopolítica focada no mote da segurança (Amaral 2017). Ressalta-se que o elemento essencial de uma biopolítica fundada no paradigma do *controle* é, paradoxalmente, a *liberdade* (Foucault 1995). Isso porque, para ter o governo como gestor dos perigos, é essencial que se instale um jogo permanente entre liberdade e segurança — dentro desse jogo, encontra-se o âmago da nova razão governamental. O risco, desse modo, torna-se um fator inserido em uma lógica de cálculo, ou seja, na prática, o que ocorre é um verdadeiro cálculo de riscos. A diferenciação desses cálculos ocorre de acordo com um maior grau de risco, a partir de uma possível identificação de zonas mais ou menos perigosas.

A noção de *perigo* e de *risco* estão postas, pois, no cerne da questão (Rosa e Amaral 2017). Da mesma forma, a liberdade não é apenas aceita ou tolerada; ao contrário, é criada e incentivada, tornando-se um fator indispensável para o funcionamento da gestão governamental. Para que a segurança seja estabelecida, uma margem de liberdade precisa estar disposta às relações de poder (Amaral e Dias 2024c). A liberdade, enfim, é verdadeira condição de existência do poder (Foucault 1995). Desse modo, a vida, sob o regime do controle contemporâneo, é exercida numa lógica de gestão de perigos (Amaral 2020a). Nesse sentido, o estímulo à vida e à produtividade não mais são efetivados em moldes estritos e fechados que visam subjugar o corpo enquanto mero objeto. Agora, as suas técnicas — voltadas ao controle e à gestão ao ar livre — possibilitam a liberdade que fundamenta as raízes do controle (Amaral e Dias 2024c).

A partir dessa biopolítica, aqui entendida como um conjunto de mecanismos (Rosa e Amaral 2017), surge um diferente arranjo na distribuição de uma série de fenômenos, em que se busca inserir os acontecimentos em termos de probabilidade. Para tanto, o instrumento ideal se torna a aplicação da estatística de uma média considerada ótima para balizar os limites do aceitável. A fixação dessa média estatística, assim, debruça-se sobre os efeitos dos fenômenos sobre a população — que deve ser entendida, aqui, como objeto de uma gestão de governo (Foucault 2008a).

A técnica política securitária busca, com esses instrumentos e fins, acondicionar um meio — compreendido como suporte e elemento de circulação de uma ação, ou seja, regular a aleatoriedade inscrita em um espaço dado (Amaral 2020a). Esse modo diferencial de tratar o acontecimento, introduzido pela lógica da racionalidade governamental securitária, implica algumas consequências que podem ser vistas claramente na implementação dos mecanismos de segurança estudados no presente artigo: enquanto a disciplina pretende isolar, concentrar e encerrar, baseando-se em uma lógica centrípeta, os dispositivos securitários tendem ampliar seus espaços de atuação, ou seja, são centrífugos. Esses dispositivos, dentro dessa lógica, buscam a organização e a ampliação de circuitos cada vez mais amplos a serem desenvolvidos (Foucault 2008a). Assim, novos elementos são implementados a todo tempo; Foucault assevera que se integram “[...] a produção, a psicologia, os comportamentos, a maneira de fazer dos produtores, dos compradores, dos consumidores, dos exportadores, integra-se o mercado mundial” (2008a, 59).

As técnicas de segurança, nesse contexto, sofreram certa modificação — baseando-se em cálculos de custos e limites do aceitável — expressando a emergência dessa nova racionalidade governamental atrelada à população. Isso ocorre porque, pelo menos desde os anos 1970, o crime passa a ser interpretado como um comportamento econômico (Rosa e Amaral 2017). Assim, a relação econômica se torna fundamental para a análise do custo da repressão e da delinquência (Amaral 2020a), ainda que não esgote a complexidade dos mecanismos de controle social. Nessa direção, não haveria tanto sentido em seguir investindo em apenas mecanismos de normalização geral e de exclusão (Rosa e Amaral 2017). O panorama que se configura tem por base a otimização dos sistemas de diferença, promovendo uma limpeza do terreno para processos oscilatórios e “tolerantes, nos quais a intervenção deixa de operar pela sujeição direta dos indivíduos, passando a uma intervenção do tipo ambiental” (Foucault 2008b, 354-355).

Para a melhor compreensão da dimensão estratégica dos dispositivos securitários, deve-se estar claro que essa alteração nos moldes da biopolítica surge diretamente da necessidade de organizar a força de trabalho como instrumento do Estado, é dizer, uma necessidade direta para o desenvolvimento dos objetivos do capitalismo (Amaral e Dias 2024c). Já havia enunciado Deleuze: “não é uma evolução tecnológica sem ser, mais profundamente, uma mutação do capitalismo” (1992b, 227). Importa destacar que o regime da disciplina foi central na constituição dos mecanismos necessários para a construção do capitalismo industrial — um arranjo que, embora ainda presente, já não determina os modos de regulação contemporâneos. É crucial ressaltar que ainda que não nos limitemos ao antigo modo de produção, a disciplina jamais deixou de ser um pilar central na gestão do trabalho.

Nesse horizonte, para a consolidação plena do capitalismo contemporâneo, a inclusão dos corpos no aparato de produção se torna agenda central, bem como a adaptação do fenômeno das populações aos processos econômicos, inserindo técnicas que visam à extração da mais-valia. Para atender a essa demanda, o exercício de poder sobre o corpo precisa ser reajustado, tendo sempre em vista que as técnicas de subjetivação utilizadas pelas instituições de confinamento estavam se tornando ineficazes. Assim, o exercício de poder voltado à disciplina individual dos corpos, em certa medida, perde força, atuando agora como dimensão complementar da regulação da população (Chignola 2018). O que importa, na contemporaneidade, não é tanto a destruição dos corpos — percebida como contraproducente para a geração de riqueza —, mas sim o conjunto de técnicas e táticas aplicadas à força de trabalho, a fim de organizá-la por meio da vigilância (Revel 2014).

Isso significa que não estamos mais limitados a um antigo modelo de capitalismo, centrado na fábrica, fundado na concentração do capital e voltado para a produção. O capitalismo torna-se um regime de sobreprodução. Logo, torna-se dirigido mais ao produto do que à produção, ou seja, para a venda ou para o mercado; daí se exprime a sua ampla capacidade dispersiva (Deleuze 1992b). Desse modo, veremos a substituição da fábrica pela empresa — pois se trata de um regime muito mais disperso — e a transformação da forma salário, agora inflamada pela premiação, condicionando a busca incessante pelo mérito (Amaral e Dias 2024c). A competição, assim, é introduzida como um emulador central e se torna um elemento essencial desse novo panorama, estimulando o indivíduo por meio de uma modulação permanente do salário por um “sistema de prêmios” (Rosa e Amaral 2017, 43-44), que excita e contrapõe os indivíduos (Deleuze 1992a).

Portanto, tomando por vista a radical mudança na dinâmica do *Capital*, a produção de novas formas ultrarrápidas de controle ao ar livre é produto direto da expansão inesgotável de um sistema que, ainda que se encontre entregue ao seu limite, não cessa de se expandir (Rosa e Amaral 2017). O novo clima penalógico, diante dos novos contornos na dinâmica do capitalismo, manifesta-se com a ampliação da malha penal, que, ao se utilizar das

novas técnicas de controle tecnológicas baseadas em dados, permeiam a sociabilidade agora também em meio aberto, de modo a complementar e reforçar as instituições de confinamento. Trata-se de uma nova *governamentalidade*² que, sustentada por dispositivos securitários, será exercida sobre a população, de forma alguma elidindo a função central da punição (Amaral 2017).

Nas sociedades de controle — que exsurtem exatamente das mencionadas mutações do capitalismo —, o essencial, acentua Deleuze, baseia-se em uma cifra: “a cifra é uma senha, ao passo que as sociedades disciplinares são reguladas por palavras de ordem” (1992b, 226). As cifras, por meio de uma linguagem numérica do controle, demarcam o acesso ou a rejeição à informação. Assim, os indivíduos são desarticulados em *divíduos* (Deleuze 1992b), sendo partes de si mesmos impressos em dados e amostras quantificáveis. Nesse sentido, a quantificação em dados, informações, senhas e cifras vem a facilitar a previsibilidade de sujeitos, grupos e comportamentos (Amaral e Dias 2024b), implicando uma verdadeira sublimação do controle para além do cárcere (Schervenski da Silva 2024).

Os dados, nesse horizonte, adquirem especial relevo para as práticas punitivas contemporâneas, demandando técnicas refinadas de vigilância. As práticas sociais hodiernas como o consumo, o salário e a dívida, acabam por criar condições de tornar as condutas dos indivíduos comportamentos previsíveis — como, por exemplo, informações sobre gastos no cartão de crédito, histórico de compras e localização registrada por aplicativos. Esse ambiente cria um solo fértil para que Estados e governos se utilizarem desses comportamentos previsíveis, inscritos em dados, a fim de alimentar seus complexos mecanismos de vigilância. Estes, para atingir os fins dos agenciamentos punitivos, alinham-se à própria ideia de controle da vida. Assim, para a prospecção desses dados em prol de seus interesses, os agenciamentos adotam as dinâmicas de vigilância e controle social, resguardando-se na justificativa da segurança (Amaral e Dias 2024c). Por consequência, a esfera securitária e a esfera econômica se encontram com barreiras totalmente nebulosas, criando um complexo que opera a favor da governança de possibilidades futuras (Amoore e De Goede 2005).

A emergência da governamentalidade algorítmica

A vigilância mediante algoritmos consolidou-se e disseminou-se de forma expressiva em nossa sociedade. Como mencionado, há pelo menos três décadas, os dispositivos de monitoramento — especialmente câmeras — passaram a integrar nosso cotidiano. Inicialmente restritos a ambientes privados, voltados ao controle de espaços laborais e de consumo, esses mecanismos, em seguida, estenderam-se às vias urbanas, apropriando-se progressivamente do espaço público. Não tardou para que as câmeras migrassem para dispositivos móveis, com suas funções de registro vinculadas à segurança, ao entretenimento, ao trabalho, à vigilância e à curiosidade (Rodríguez 2019).

Desse modo, ocorre um movimento duplo: de um lado, a digitalização, convertendo o analógico para o digital; de outro, a datificação, entendida como o processo de transformar eventos, acontecimentos e interações em dados passíveis de armazenamento, circulação e análise. Ambos os processos ocorrem tanto na vida cotidiana quanto nas práticas

2 “O conjunto constituído pelas instituições, os procedimentos, análises e reflexões, os cálculos e as táticas que permitem exercer essa forma bem específica, embora muito complexa, de poder que tem por alvo principal a população, por principal forma de saber a economia política e por instrumento técnico essencial os dispositivos de segurança. Em segundo lugar, por ‘governamentalidade’ entendo a tendência, a linha de força que, em todo o Ocidente, não parou de conduzir, e desde há muito, para a preeminência desse tipo de poder que podemos chamar de ‘governo’ sobre os outros — soberania, disciplina — e que trouxe, por um lado, o desenvolvimento de toda uma série de aparelhos específicos de governo [e, por outro lado], o desenvolvimento de toda uma série de saberes. Enfim, por ‘governamentalidade’, creio que se deveria entender o processo, ou antes, o resultado do processo pelo qual o Estado de justiça na Idade Média, que nos séculos XV e XVI se tornou o Estado administrativo, viu-se pouco a pouco ‘governamentalizado’” (Foucault 2008a, 143).

punitivas, confundindo as duas experiências em uma só. Assim, toda a vigilância que existia antes para fins coercitivos torna-se volvida aos prazeres do sujeito, criando um espaço de uma obscura *liberdade absoluta* (Harcourt 2015). Dentro dessa lógica, inserem-se os atuais bancos de dados: a sua entrada é garantida em algum deles — nas redes sociais, por exemplo — se o usuário oferecer suas informações e dados como contrapartida. Logo, ao ceder “livremente” seus dados, o usuário também se movimenta “livremente” dentro desses espaços digitais (Rosa e Amaral 2017). Desse modo, todas ações que praticamos nas redes de comunicação, em seus navegadores e plataformas, são rastreadas e arquivadas, constituindo um grande arquivo de nossas ações, escolhas e hábitos (Bruno 2016). O controle, nesse contexto, exerce-se com uma grande contribuição da liberdade (Rosa e Amaral 2017).

Se a vigilância algorítmica já redefine a noção de privacidade, a sua materialização no espaço público — por meio de tecnologias de reconhecimento facial — radicaliza ainda mais o seu alcance. Isso porque a sua implementação monitora não apenas ações digitais, mas significa também o monitoramento do corpo nos espaços físicos (Beiguelman 2021). O implemento das câmeras é um bom exemplo para perceber a acentuação da vigilância sobre as nossas vidas; no entanto, é certo que cada vez mais atividades são incorporadas às redes sociais, e não apenas as atividades que as câmeras conseguem capturar (Rodríguez 2019). Assim, na medida em que as tecnologias de reconhecimento facial evoluem, elas se integram cada vez mais às redes e aos sistemas computacionais, resultando em maior frequência do procedimento do mapeamento do rosto. Dessa forma, o rosto pode ser compreendido como a nova “digital”, pois, uma vez identificado, permite rastrear o corpo em um espaço dado (Beiguelman 2021). A vigilância, destarte, não precisa mais necessariamente das instituições de confinamento, mas integra o cárcere ao espaço de circulação geral (Rodríguez 2019). Nesse novo contexto, as vidas digitais, conseqüentemente, passam a ser obscuramente semelhantes à existência monitorada dos sujeitos carcerários supervisionados (Harcourt 2015).

Esse novo regime de controle em emergência pode ser chamado de “governamentalidade algorítmica”, ou seja, a racionalidade que se vale da coleta, agregação e análise automatizada de quantidade massiva de dados, de modo a antecipar e afetar os comportamentos possíveis (Rouvroy e Berns 2015). Tais mecanismos funcionam por meio de redes baseadas no processo de vigilância e coleta massiva de dados, sua classificação e análise, com o fim de gerenciar, influenciar e disciplinar o comportamento de indivíduos. Para tanto, a estrutura da rede mundial de computadores e de seus navegadores se utilizam de toda a ação e rastros realizados digitalmente, com a finalidade de constituir “[...] um vasto, dinâmico e polifônico arquivo de ações, escolhas, interesses, hábitos, opiniões, etc.” (Bruno 2016, 36).

Esses dados, segundo Harcourt (2015), possuem ampla variedade de informações, incluindo comunicações telefônicas, mídias sociais, e-mails, vídeos, chats, estatísticas vitais, informações do censo do governo. Todos esses dados são produzidos por computadores, celulares ou dispositivos digitais, por meio de e-mails, mensagens, tuites e vídeos. Ou seja, com a digitalização da vida cotidiana, vemos também a acentuação da lógica de acumulação de dados dos sujeitos, o que leva a uma datificação da vida. Logo, esse conjunto massivo de dados — derivados de diferentes meios — pode ser minerado, armazenado e analisado para diversas finalidades e em diferentes contextos. Assim, o uso dos dados e dos metadados que alimentam bancos de análise e softwares de vigilância urbana não é visto apenas como “histórico” ou “informativo”. A sua lógica, na verdade, baseia-se em um intenso cruzamento de dados com inúmeras possibilidades a partir da obtenção de conteúdo pessoal (Amaral e Dias 2024c).

O valor desse conjunto de dados reside na sua capacidade de produzir perfis preditivos, ou seja, a sua utilidade quanto à capacidade de mensurar a probabilidade de acontecimentos, como, por exemplo, o cometimento de um crime por um sujeito — ou até de este ser

preso antecipadamente (Mayer-Schönberger e Cukier 2013). Com o acúmulo de dados, procura-se, então, prever e modificar o comportamento humano (Zuboff 2018). Para tanto, a gestão dessa quantidade massiva de informações produzidas diariamente consiste em atribuir-lhes sentido mediante a aplicação desses dados em “algoritmos poderosos”, definidos como “uma sequência finita de instruções precisas que são implementáveis em sistemas computacionais” (Osoba 2017, 4-6).

As três etapas da governamentalidade algorítmica

Pode-se dizer, de maneira mais esquemática, que o regime da *governamentalidade algorítmica* atua a partir da estatística para a extração automática de informações de bases de dados para os fins de previsão ou exclusão. Para melhor compreensão desse sistema, esse mecanismo pode ser decomposto em três etapas. Assevera-se que uma etapa não implica a inexistência de contaminação com a outra etapa; ao contrário, quanto mais elas se confundirem, maior a sua eficácia na coleta de dados dos sujeitos (Rouvroy e Berns 2015).

A primeira etapa é chamada de *dataveillance*, ou seja, a coleta e conservação automática de uma grande quantidade de dados não classificados (Rouvroy e Berns 2015). Os dados advindos das mais diversas fontes sofrem uma explosão de recompilação e conservação automáticas (Rodríguez 2019) — informações provenientes de segurança, controle, gestão de recursos, marketing, publicidade, individualização de ofertas ou até indivíduos compartilhando benevolmente seus dados nas redes sociais. Assim, esses dados perdem a vinculação com o seu “conhecimento verdadeiro”, aquele das finalidades almejadas por essa coleta de informações, ou seja, há um esvaziamento e uma minimização do sujeito e de algum possível consentimento que poderia ser dado a essa correlação de informações. Os dados, então, deixam de fazer sentido coletivamente, apresentando-se meramente como uma múltipla faceta do real (Rouvroy e Berns 2015).

A pretensa racionalidade dessa gestão de dados reside exatamente no fato de que os dados, *per se*, parecem inofensivos; um traço deixado de uma compra, o uso de uma palavra em específico, um deslocamento dentro da cidade: elementos que são tão heterogêneos, tão pouco intencionados e tão pouco subjetivos supostamente não poderiam mentir. Assim, cada elemento é reconduzido à sua natureza mais bruta, ao mesmo tempo que é abstraído de seu real contexto, sendo reduzido a dado (Rouvroy e Berns 2015).

A segunda etapa é aquela do *datamining*, a qual busca realizar o tratamento automatizado dos dados coletados massivamente na primeira etapa, explorando esse grande depósito de informações (Rodríguez 2019). A sua finalidade é fazer emergir correlações sutis entre dados. Estamos presentes, nesse ponto, diante de uma produção de saberes estatísticos constituídos de simples correlações automatizadas, partindo de informações completamente heterogêneas. Ressalta-se que o grande avanço dessa etapa consiste na aplicação da estatística sem a necessidade de postar uma hipótese prévia, ou seja, dispensando mais uma vez toda forma de subjetividade (Rouvroy e Berns 2015).

Nesse horizonte, com a aparição de tecnologias de aprendizado de máquina, largamente se espalha um discurso da criação de algoritmos que teriam a capacidade de “aprender indutivamente”, isto é, que seriam capazes de serem treinados para criar correlações efetivas entre dados dentro desse grande conjunto de informações capturadas. Todavia, ocorre que os processos de mineração e análise de dados são incapazes de “ensinar” máquinas a pensar; a inteligência artificial funciona com base na aplicação matemática em grandes quantidades de dados para inferir probabilidades a partir de correlações e padrões (Mayer-Schönberger e Cukier 2013). Desse modo, inverte-se a lógica da estatística: as hipóteses são produzidas a partir dos próprios dados capturados (Rouvroy e Berns 2015) — para não dizer furtados, como já exposto anteriormente.

Os sistemas algorítmicos, assim, são utilizados para a criação de perfis preditivos, direcionados a uma tentativa de previsão futura (Amaral e Dias 2024c), baseando-se exaustivamente na estatística de dados históricos para antecipar o futuro, fornecendo futuros prováveis para decisões comerciais imediatas e iminentes (Amoore e De Goede 2005); é o que poderíamos chamar de *datanticipating*, isto é, o terceiro momento da governamentalidade algorítmica. Essa terceira etapa se baseia no uso dos saberes probabilísticos e estatísticos e almeja a antecipação de comportamentos individuais, sendo vinculados a perfis criados pelas correlações descobertas pelo *datamining* (Rouvroy e Berns 2015). Assim, a eficácia da criação desse dito perfil será maior quanto mais dados forem coletados.

Nesse sentido, os processos de decisão são terceirizados a máquinas sofisticadas de processamento de dados que, como já indicado, apenas seguem instruções matemáticas. Desse modo, emerge-se uma ideia de um saber em que a objetividade se parece absoluta, uma vez que não se admite qualquer intervenção subjetiva — logo, as normas parecem surgir do real (Rouvroy e Berns 2015). No entanto, muitos dos procedimentos algoritmos são inacessíveis, funcionando como uma “caixa preta”. Conseguimos analisar seus dados de entrada (*inputs*) e seus dados de saída (*outputs*), mas não sabemos o que acontece no meio-tempo, ou seja, no processo de transformação do dado de entrada para o dado de saída, tampouco os critérios de análise ou outras informações de grande relevância. Visto que esses sistemas algoritmos são respaldados e reforçados por uma opacidade — ou seja, estão fora do alcance de qualquer verificação, os problemas advindos dessas máquinas são tratados como questões técnicas (Pasquale 2015). Assim, os operadores dessas máquinas têm uma grande margem para afastar os debates sobre os seus efeitos, bem como inviabilizar a possibilidade de discussão de saber quais são os interesses inseridos nos operadores dos algoritmos (Amaral *et al.* 2021).

Nesse contexto, os algoritmos são legitimados a proferir verdadeiros vereditos silenciosos sobre a vida dos sujeitos, ainda os deixando sem qualquer capacidade de contestação efetiva sobre eles (Amaral *et al.* 2021). Isso acaba por configurar um moderno paradigma kafkiano — aquele vivido por Josef K, protagonista de *O processo*, de Kafka (2006) —, em que não se entende se a imputação do crime foi correta, pois a decisão se baseia em dados manipulados por algoritmos, que afirmam que ele cometeu o crime e deve responder judicialmente (Amaral e Dias 2024c).

O uso dos algoritmos em mecanismos de segurança: críticas e consequências

Dentro desse intrincado e multifacetado contexto, também se mostra complexa a transformação das práticas punitivas diante dos desafios que se apresentam aos seus modos antiquados — e ainda presentes — de punição (Schervenski da Silva e Curcio 2025). Nesse novo cenário, a tomada de decisões passa a ser delegada a máquinas sofisticadas, capazes de operar sobre métodos codificados de processamento de dados. A tecnologia de reconhecimento facial é um tipo de identificação biométrica que analisa os traços fisiômicos para criar um modelo matemático único, representando cada rosto, baseando-se em tecnologias de computação visual³. Esses softwares são fundados e orientados em uma perspectiva de *machine learning*, isto é, as ações da máquina são moldadas a partir

3 “A computação visual (*visual computing*) é um termo que engloba áreas da computação e iniciativas interdisciplinares dedicadas a construir sistemas para o entendimento automatizado de imagens e vídeos. Ou seja, busca-se fazer softwares e hardwares computacionais capazes de entender objetos, entidades e situações a partir de informação visual, como imagens ou frames de vídeo. Suas implicações são amplas, a indústria e mecânica até o marketing e publicidade” (Silva 2020, 433).

de ações anteriores. Independentemente do elemento corporal que será analisado pelo sistema tecnológico, o corpo não é analisado inteiramente, mas apenas pontos específicos, os quais servirão como base para os cálculos probabilísticos (Nunes 2019a).

Podemos dizer, esquematicamente, que a máquina, seguindo um conjunto de métodos, verifica um padrão e automaticamente determina ações e realiza projeções. Assim, baseado nesse método, as tecnologias de reconhecimento facial organizam dois procedimentos: o primeiro preocupa-se com o rastreamento, isto é, é realizada a detecção de pontos considerados essenciais da face do indivíduo. Dessa forma, são identificadas as características específicas do rosto, como a distância entre os olhos e o contorno do queixo, a fim de criar um modelo que reproduza as particularidades de cada indivíduo. Após a identificação desses pontos, inicia-se a segunda etapa, denominada “extração”, na qual os detalhes faciais são transformados em uma representação matemática. A equação resultante é então armazenada em um banco de dados e confrontada com os modelos matemáticos de outras pessoas, buscando-se uma correspondência (Electronic Frontier Foundation 2023). Assim, esse procedimento busca a equivalência ou a diferenciação de rostos de sujeitos com os demais rostos — codificados em dados — submetidos ao *big data*⁴. Todos esses procedimentos, enfim, são submetidos a algoritmos e seguem a lógica exposta anteriormente. O que ocorre nesse conjunto de procedimentos é a substituição do significado de rostos por uma matemática dos rostos, a qual busca reduzir a complexidade e multidimensionalidade de um rosto em critérios mensuráveis e previsíveis (Kember 2014).

De forma intrínseca, essa tecnologia apresenta problemas. Sua própria programação produz dois tipos de erros: falso negativo e falso positivo. No caso do falso negativo, o algoritmo falha em reconhecer o rosto correspondente à imagem fornecida, mesmo que ele conste em seu banco de dados. No falso positivo, por sua vez, o sistema comete um erro de reconhecimento, atribuindo a identidade de uma pessoa a outro indivíduo de forma errônea.

Esses dois tipos de erro são antecipados pelos programadores e são calibrados de formas distintas conforme o resultado pretendido. Uma maior tolerância a falsos positivos aumenta o número de rostos reconhecidos, mas reduz a precisão; ao passo que privilegiar a minimização de falsos negativos dificulta a detecção de correspondências (Elesbão, Dos Santos e Medina 2020). No contexto da segurança pública, é crucial reduzir ao máximo os falsos positivos, uma vez que seu impacto pode levar à abordagem e punição de inocentes (Electronic Frontier Foundation 2023). Nesse sentido, um estudo do Instituto Nacional de Padrões e Tecnologias dos Estados Unidos, realizado em 2019, aponta que:

Os falsos positivos ocorrem em sistemas biométricos quando as amostras de dois indivíduos produzem uma pontuação de comparação igual ou superior a um limiar definido. A maioria dos sistemas está configurada com um limiar que é fixo para todos os utilizadores. Os falsos positivos representam um risco de segurança para as aplicações de verificação um-para-um. Têm consequências igualmente graves nas aplicações de identificação de um para muitos. Por exemplo, em aplicações em que as pessoas se candidatam a um determinado benefício mais do que uma vez com identidades biográficas diferentes, por exemplo, para obtenção de vistos, emissão de carteiras de habilitação, fraude em matéria de prestações sociais, um falso positivo não detectado pode ter várias consequências, como perdas financeiras. Numa aplicação de vigilância, um falso positivo pode levar a uma falsa acusação. (Grother 2019, 28)

4 “O *big data* é, acima de tudo, o componente fundamental de uma nova lógica de acumulação, profundamente intencional e com importantes consequências, que chamo de capitalismo de vigilância. Essa nova forma de capitalismo de informação procura prever e modificar o comportamento humano como meio de produzir receitas e controle de mercado” (Zuboff 2018, 18).

O sistema, naturalmente, visa alcançar a máxima precisão. Para isso, o algoritmo precisa ser alimentado com um volume cada vez maior de dados, de modo a identificar com maior exatidão os traços físicos das pessoas. Quanto maior a quantidade de imagens disponíveis, mais detalhes são incorporados ao mapeamento facial, reduzindo a taxa de erro. Consequentemente, torna-se necessária a vigilância em massa da população, com a captura de rostos sem consentimento prévio e sem que os indivíduos tenham acesso ou conhecimento sobre a finalidade do uso de seus dados. A despeito de uma vigilância inflada que alimenta esses sistemas e um farto banco de imagens, capturadas inclusive das redes sociais, essa quantidade de dados é insuficiente para o sistema. Além disso, existem fatores limitantes intrínsecos ao próprio sistema. Assim, tanto a iluminação do ambiente quanto o ângulo da fotografia servem como coeficientes que interferem na precisão da leitura de rostos pelo sistema (Beiguelman 2021). No mesmo sentido, as expressões faciais afetam também a eficiência da máquina, provocando erros (Lobato *et al.* 2024).

A situação se torna ainda mais grave quando se leva em conta que os dados coletados são particularmente sensíveis, por serem únicos e de difícil modificação. As feições de uma pessoa mudam apenas com o tempo ou por meio de intervenções cirúrgicas. Uma vez registrado o modelo facial no banco de dados — geralmente sem o conhecimento do indivíduo —, ele só deixará de ser identificado pelo algoritmo caso consiga remover ou apagar esses dados.

Outro problema crítico desses sistemas é a distorção de reconhecimento em termos raciais e de gênero, resultando em decisões enviesadas e discriminatórias. Os bancos de dados contêm menos referências de rostos de pessoas não brancas, o que aumenta a incidência de falsos positivos nesses grupos. Um exemplo é o caso da empresa IJB-A, cuja base de dados apresentava 59,4% de fotos de homens brancos, 20,2% de mulheres brancas, 16% de homens negros e apenas 1,4% de mulheres negras (Silva 2019, 7-8). Essa deficiência no treinamento das máquinas não é um caso isolado, mas um problema sistêmico da tecnologia. Ela reflete, na verdade, uma sociedade racista, que realiza testes predominantemente com populações brancas e não ajusta os algoritmos para reconhecer rostos racializados com a mesma precisão.

A situação se torna ainda mais alarmante quando se examinam os efeitos na segurança pública, com seu histórico notoriamente racialmente seletivo. Essa discriminação automatizada intensifica o cenário de seletividade (Elesbão *et al.* 2020), representando segurança para alguns e repressão para outros (Reis *et al.* 2021). A consequência dessa nova dimensão advinda desse cenário baseado em dados é a emergência do racismo algorítmico (Beiguelman 2021). Em 2019, o número de presos por meio de sistemas de reconhecimento facial que são pessoas negras foi de 90,5% (Nunes 2019a). Importante destacar que, nesse mesmo ano, ao menos quatro estados haviam registrado prisões com o uso das tecnologias de reconhecimento facial (Lima *et al.* 2024). Assevera-se que as autoridades policiais insistem no investimento de tais tecnologias para fins de identificação de suspeitos, ainda que esses mecanismos apresentem taxas alarmantes de erros quando se trata da identificação de pessoas negras (Electronic Frontier Foundation 2023).

Assim, é por trás do pretenso véu da objetividade e neutralidade que os processos de decisão têm sido cada vez mais terceirizados a máquinas que processam dados codificados, em que os sistemas algorítmicos são utilizados para a elaboração de perfis preditivos, implicando punições direcionadas, vinculadas a práticas discriminativas (Amaral *et al.* 2021). Nesse horizonte, arremata Zuboff: “o *big data* tem origem no social e é ali que devemos encontrá-lo e estudá-lo” (2018, 8). Logo, concordamos com Amaral e Dias quando estabelecem que “abandonar a pretensa neutralidade tecnológica dos algoritmos supostamente intrínseca à composição de seus programas é tão relevante quanto entender as fórmulas dos seus cálculos” (2024a, 32).

Tecnologias de reconhecimento facial e sua aplicação na segurança pública: a experiência brasileira

No início de 2020, foi inaugurado, pelo governo de São Paulo, o Laboratório de Identificação Biométrica para estabelecer uma nova frente de avanços nessa nova empreitada de gestão de dados biométricos digitais, visando à promoção e ao uso das tecnologias de reconhecimento facial. Foi o momento em que o então governador João Dória festejou que esse laboratório “localize o bandido antes que ele execute o crime”, bem como parabenizou o delegado-geral da Polícia Civil, destacando que “nunca prendeu tanto quanto nestes 13 meses” (Governo do Estado de São Paulo 2020). O laboratório integra o Instituto de Identificação Ricardo Gumbleton Daunt — nomeado como inovador criminólogo e datiloscopista, que herdou o nome do avô médico escravista (Silva 2022).

A adoção dessa técnica em solo brasileiro ganhou grande destaque devido à Portaria 793, de 24 de outubro de 2019, que estabeleceu a utilização de recursos do Fundo Nacional de Segurança Pública para estimular a instauração de sistemas de videomonitoramento que se valem de tecnologias de reconhecimento facial, inteligência artificial e outras (Ministério da Justiça e Segurança Pública 2019). A portaria baseia a sua implementação em um discurso de segurança, sendo esses sistemas considerados parte integrante das estratégias de redução e controle da violência e criminalidade (Lima *et al.* 2024). Desde então, essas técnicas se alastraram no cenário nacional. Atualmente, 421 projetos utilizam técnicas de reconhecimento facial no Brasil, com 87.199.831 pessoas possivelmente vigiadas. Na Região Sul, temos 82 projetos ativos e 11.150.413 pessoas vigiadas⁵.

No entanto, o uso das tecnologias de reconhecimento facial, mediante essa portaria e outras medidas subsequentes, não foi acompanhado pela implementação de um padrão adequado que assegure a transparência e a possibilidade de análise desses dados inseridos nos sistemas. Ressalta-se que o direito à proteção de dados foi reconhecido como direito fundamental autônomo mediante emenda à Constituição (Brasil 1988). Nesse sentido, a Lei 13.709/2018, conhecida como Lei Geral de Proteção de Dados (LGPD), sancionada em agosto de 2018, estabelece princípios e regras para o tratamento de dados pessoais no Brasil, impondo limites e deveres aos agentes de tratamento e garantindo direitos aos titulares. Sua origem decorreu da necessidade de harmonizar práticas de coleta e uso de dados com padrões internacionais, assegurando transparência, segurança e responsabilização, especialmente diante do avanço de tecnologias capazes de realizar vigilância em larga escala, como o reconhecimento facial.

Contudo, a implementação dos projetos avança em solo brasileiro sem que exista qualquer regulação que proteja os direitos fundamentais dos indivíduos vigiados. A consequência é um uso descabido dessas tecnologias, tornando os espaços públicos laboratórios de experimentação (Lima *et al.* 2024). À vista desse laboratório a céu aberto, podemos estar diante de um renovado momento obscuro dos modos de punição: “Poderemos estar, portanto, na direção de algo ainda mais profundo que a gestão da morte de grupos específicos, mais agudo que a emulação da autodestruição, para, assim, experienciar um estado de pacificação mortal, de gestão terrífica de uma condição de sobrevivência” (Amaral 2023, 15).

Um caso que ilustra a maneira como a tecnologia de reconhecimento facial é implementada em geral — apoiando-se somente em autorização genérica — é o da Secretaria de Segurança Pública do Estado da Bahia. Ela se utiliza apenas do *caput* do artigo 144 da Constituição Federal, que prescreve que qualquer meio pode ser empregado para melhor garantir a segurança pública. O estado da Bahia, nesse sentido, experienciou um uso alardeado das tecnologias de reconhecimento facial no Carnaval de 2019 (Nunes *et al.* 2023b),

5 Ver mais no site *O Panóptico*. Disponível em: <https://www.opanoptico.com.br/#mapa>

a partir da iniciativa da Secretaria de Segurança Pública do Estado da Bahia, obtendo números frustrantes: foram capturados rostos de 1,3 milhões de pessoas, originando 903 alertas. Contudo, 96% dos avisos não resultaram em nada. Assim, assertivamente, Pablo Nunes declara que:

Esses alertas podem ser comparados ao envio de uma ambulância para socorrer um possível paciente. Se em 9 de cada 10 chamadas não houver uma emergência real, teremos o desperdício de dinheiro público e a alocação inútil de tempo e pessoal. É o que tem ocorrido na aplicação da tecnologia de reconhecimento facial. (2019b, 68)

É uma taxa alarmante de erro, porém isso não conteve o estado baiano, que continuou a investir na tecnologia, desembolsando, em 2021, cerca R\$ 665 milhões (Falcão 2021). Já em 2020, também no Carnaval de Salvador, foram presos 42 foragidos e foi capturada a identidade biométrica de 11,7 milhões de pessoas (Gama 2020). O que pode parecer, inicialmente, um sucesso, quando colocada em perspectiva, se torna aterrorizante. O registro fotográfico dos rostos foi de 278 mil vezes a quantidade de indivíduos detidos (Reis *et al.* 2021, 38). E os resultados, similares aos de 2019: 34 pessoas presas (Falcão 2021). Não obstante, o uso das tecnologias de reconhecimento facial se estendeu para o interior do estado, agora estando presente em mais de 70 municípios, a despeito de indicadores claros da efetividade na redução da criminalidade. Na verdade, segundo os dados da Secretaria de Segurança Pública do Estado da Bahia, entre 2018 e 2022, os índices de criminalidade e violência permaneceram inertes ou até aumentaram em algumas regiões do estado (Lima *et al.* 2024).

Da mesma forma, é interessante o destaque para a experiência do estado de Goiás, em que se percebe um projeto em curso de expansão da lógica da vigilância por meio do uso das tecnologias de reconhecimento facial. Isso porque, diante da falta de regulação específica para a implementação dessas tecnologias, percebe-se uma dinâmica diferente na interiorização desses mecanismos: o fenômeno ocorre acompanhado da municipalização da gestão dos recursos e dados produzidos pelas câmeras (Nunes *et al.* 2023a).

Nesse contexto, o delegado Waldir (na época, deputado federal, representando o estado pelo partido União) capitaneou a interiorização municipalizada do uso de câmeras nas cidades de Goiás, destinando cerca de 30% dos seus recursos parlamentares para esse fim. Com todo o incentivo, os municípios foram organizando pregões e contratando empresas para instalar câmeras de forma autônoma. O resultado foi que, atualmente, Goiás é o estado brasileiro com mais programas municipais de implementação de videomonitoramento e reconhecimento facial. Destaca-se que foi realizado um investimento de quase 50 milhões de reais em apenas dois anos, sob a justificativa de “modernização do policiamento”, mas sem especificação dos serviços, empresas e responsáveis (Nunes *et al.* 2023a).

Ainda assim, diante de um movimento de “modernização da segurança” por parte dos municípios, os projetos não foram acompanhados de mecanismos de responsabilização, prestação de contas e transparência (Lima *et al.* 2024). Ressalta-se que as tecnologias de reconhecimento facial, já disseminadas no município desse estado, contam com um software próprio denominado “Harpia”, criado em 2017 pelo Instituto de Identificação da Polícia Civil, em parceria com a Universidade Federal de Goiás. No momento do seu lançamento, o mecanismo já contava com 50 mil fotos em seu banco de dados, sem que qualquer autoridade houvesse explicitado de onde elas teriam sido retiradas e como os dados seriam tratados. Até hoje, não há informações da Polícia Civil sobre o uso que é feito a partir do software Harpia (Nunes *et al.* 2023a).

Assim, em ambos os casos, ocorre um verdadeiro processo de desresponsabilização do uso da tecnologia, uma vez que diversos projetos estão sendo aplicados na segurança pública brasileira de modo descentralizado. No Brasil, cada entidade tem a arbitrariedade

de decidir qual tecnologia irá utilizar, o tipo de software, as empresas fornecedoras, os bancos de dados a serem utilizados, os requisitos de análise de vídeo e a localidade onde as tecnologias serão empregadas (Lima *et al.* 2024). Agrava-se o cenário pelas lacunas de informação, uma vez que em nenhum dos projetos implementados no Brasil foi produzido uma avaliação de seus impactos.

Nesse sentido, a LGPD dispõe, no artigo 4º, inciso III, parágrafo 3º, a elaboração de uma avaliação de impacto em todos os casos, e a impõe quando se trata do meio penal: segurança pública, investigação e repressão de infrações penais. A pesquisa, denominada “Relatório de impacto à proteção de dados” (RIPD), tem a função de apontar quais efeitos que determinada política, programa ou serviço têm sobre a privacidade e a proteção de dados pessoais (Universidade Federal do Ceará 2024), para estabelecer quais os riscos e quais ações tomar. Inclusive, na esfera internacional, a União Europeia exige que sejam realizados RIPD para a adoção de equipamentos de reconhecimento facial. Entretanto, a tecnologia está sendo ostensivamente utilizada no Brasil sem o devido acompanhamento e exame de riscos. Outrossim, as autoridades que a utilizam não são qualificadas para tanto: desconhecem o funcionamento do sistema e suas possíveis consequências, além de não receberem treinamentos para adequar seus conhecimentos sobre o assunto e guiar suas ações.

Se essa tecnologia é, de fato, tão eficaz quanto os seus discursos afirmam, é necessário apresentar informações que comprovem essa eficácia. Dessa forma, confere-se mais legitimidade à sua utilização. Inclusive, a LGPD dispõe o direito ao acesso público a esses dados de maneira gratuita, fácil, clara e precisa. No entanto, atualmente, poucas instituições compartilham essas informações de forma adequada. Algumas nem mesmo liberam os dados com pedidos de entes interessados, tampouco os disponibilizam de maneira ampla para o público. A principal fonte de estatísticas sobre o tema vem de instituições independentes que realizam pesquisas próprias. Diante dessas circunstâncias, o escrutínio popular sobre a proporcionalidade e a eficiência dos sistemas de reconhecimento facial fica comprometido (Reis *et al.* 2021). Portanto, o acesso às informações de modo simples por parte dos cidadãos deve ser proporcionado pelas autoridades que implementam tais práticas, a partir de canais específicos.

Conclusões

Quanto à reestruturação das barreiras das sociedades disciplinares, estando a vigilância volvida também agora aos meios abertos, alerta-se para o uso indiscriminado dos dispositivos de reconhecimento facial, tendo em vista que, por trás da roupagem democrática que os dispositivos securitários podem assumir (Negri e Hardt 2001), existem, na verdade, sistemas algorítmicos que se retroalimentam em um ciclo discriminatório (Amaral *et al.* 2021). Amparadas em legislações frágeis, essas tecnologias inflamam a vigilância e o gerenciamento de dados sob uma racionalidade pretensamente objetiva que, por fim, servem para criar perfis preditivos e proferir vereditos silenciosos sobre os sujeitos (Amaral *et al.* 2021), de modo a antecipar e afetar os comportamentos possíveis, configurando uma “gestão de possíveis” (Bruno 2016, 37). O cenário brasileiro, diante da falta de transparência — respaldada pela falta de regulação centralizada do assunto, permite uma grande margem para discricionariedade de como serão utilizadas essas ferramentas, conferindo ao Brasil um status de “laboratório” a céu aberto. O cenário é deveras delicado, visto que esses mecanismos podem “condenar o presente ao futuro antecipado” (Bruno 2016, 37). Não se trata mais de isolar o sujeito no cárcere, mas a nova lógica penal precipita-se sob a interceptação do sujeito em seu trajeto (Amaral 2017).

Pode-se afirmar, portanto, que o elemento central a ser revelado na lógica opaca das tecnologias algorítmicas é que as decisões que estruturam os modelos dessas máquinas são tomadas por seres humanos, carregando consigo interesses econômicos, políticos, sociais e variações culturais (Amaral *et al.* 2021). Assim, apesar da pretensa objetividade e neutralidade dessas tecnologias, é inevitável que elas reproduzam efeitos discriminatórios em decorrência de seu funcionamento.

Referências

1. Amaral, Augusto Jobim do. 2017. *A governamentalidade em tempos securitários*. Caxias do Sul: Editora da Universidade de Caxias do Sul.
2. Amaral, Augusto Jobim do. 2020a. “Biopolítica e biocapitalismo”. Em *Política da criminologia*, editado por Augusto Jobim do Amaral, 103-163. São Paulo: Tirant Lo Blanch.
3. Amaral, Augusto Jobim do. 2020b. *Política da criminologia*. São Paulo: Tirant Lo Blanch.
4. Amaral, Augusto Jobim do, Ana Clara Elesbão dos Santos e Felipe da Veiga Dias. 2021. “Gubernamentalidad algorítmica y nuevas prácticas punitivas”. *Derechos en Acción* 20 (20): 549. <https://doi.org/10.24215/25251678e549>
5. Amaral, Augusto Jobim do. 2023. “Neoliberalismo, contrarrevolução e pós-fascismo no Brasil”. *Destroços: revista de pensamento radical* 4 (1): 1-22. <https://doi.org/10.53981/destroos.v4i1.46400>
6. Amaral, Augusto Jobim do e Felipe da Veiga Dias. 2024a. “Algoritmos e novos desdobramentos biopolíticos do controle”. Em *Tecnopolítica criminal*, editado por Augusto Jobim do Amaral e Felipe da Veiga Dias, 29-59. São Paulo: Tirant Lo Blanch.
7. Amaral, Augusto Jobim do e Felipe da Veiga Dias. 2024b. “Controle social e governo de dados”. Em *Tecnopolítica criminal*, editado por Augusto Jobim do Amaral e Felipe da Veiga Dias, 13-28. São Paulo: Tirant Lo Blanch.
8. Amaral, Augusto Jobim do e Felipe da Veiga Dias. 2024c. “Surveillance no estado penal e as ‘novas’ tecnologias de controle biopolítico”. Em *Tecnopolítica criminal*, editado por Augusto Jobim do Amaral e Felipe da Veiga Dias, 60-84. São Paulo: Tirant Lo Blanch.
9. Amoore, Louise e Marieke de Goede. 2005. “Governance, Risk and Dataveillance in the War on Terror”. *Crime, Law and Social Change* 43: 149-173. <https://doi.org/10.1007/s10611-005-1717-8>
10. Beiguelman, Giselle. 2021. *Políticas da imagem: vigilância e resistência na dadosfera*. São Paulo: Ubu.
11. Brasil. 1988. *Constituição da República Federativa do Brasil*. Brasília, DF: Câmara dos Deputados.
12. Bruno, Fernanda. 2016. “Rastrear, classificar e performar”. *Ciência e Cultura* 68 (1): 34-38. <http://dx.doi.org/10.21800/2317-66602016000100012>
13. Chignola, Sandro. 2018. “A toupeira e a serpente”. *Revista de Direitos e Garantias Fundamentais* 19 (3): 239-269. Traduzido por Augusto Jobim do Amaral. <http://dx.doi.org/10.18759/rdgf.v19i3.1599>
14. Deleuze, Gilles. 1992a. “Controle e devir”. Em *Conversações*, 213-222. Traduzido por Peter Pál Pelbart. São Paulo: Editora 34.
15. Deleuze, Gilles. 1992b. “Post-scriptum sobre sociedade de controle.” Em *Conversações*, 223-230. Traduzido por Peter Pál Pelbart. São Paulo: Editora 34.
16. Electronic Frontier Foundation. 2023. *Street Level Surveillance: Face Recognition*. Electronic Frontier Foundation. <https://sls.eff.org/technologies/face-recognition>
17. Elesbão, Ana Clara Santos, Jádía Timm dos Santos e Roberta Medina. 2020. “Quando as máscaras (do reconhecimento facial) caírem, será um grande carnaval”. Em *Algoritmos*, editado por Jesús Sabariego, Augusto Jobim do Amaral e Eduardo Baldissera Carvalho Salles, 247-259. São Paulo: Tirant Lo Blanch.
18. Falcão, Cíntia. 2021. “Lentes racistas. Rui Costa está transformando a Bahia em um laboratório de vigilância com reconhecimento facial”. *The Intercept Brasil*, 20 de setembro. <https://www.intercept.com.br/2021/09/20/rui-costa-esta-transformando-a-bahia-em-um-laboratorio-de-vigilancia-com-reconhecimento-facial/>
19. Foucault, Michel. 1995. “O sujeito e o poder”. Em *Michel Foucault: uma trajetória filosófica (para além do estruturalismo e da hermenêutica)*, editado por Hubert Dreyfus e Paul Rabinow, 231-249. Traduzido por Vera Porto Carrero. Rio de Janeiro: Forense Universitária.
20. Foucault, Michel. 2006. “¿Qué es la Ilustración?”. Em *Sobre la ilustración*, editado por Javier de la Higuera, 71-97. Traduzido por Javier de la Higuera, Eduardo Bello e Antonio Campillo. Madri: Tecnos.
21. Foucault, Michel. 2008a. *Segurança, território, população: curso dado no Collège de France (1977-1978)*. Traduzido por Eduardo Brandão. São Paulo: Martins Fontes.
22. Foucault, Michel. 2008b. *Nascimento da biopolítica: curso dado no Collège de France (1978-1979)*. Traduzido por Eduardo Brandão. São Paulo: Martins Fontes.
23. Gama, Aliny. 2020. “Reconhecimento facial por app captura 42 foragidos no Carnaval de Salvador”. *UOL*, 26 de fevereiro. <https://carnaval.uol.com.br/2020/noticias/redacao/2020/02/26/reconhecimento-facial-por-app-captura-42-foragidos-no-carnaval-de-salvador.htm>

24. Governo do Estado de São Paulo. 2020. “Discurso de João Doria na inauguração do Laboratório de Identificação Biométrica em 28 de janeiro”. <https://soundcloud.com/governosp/discurso-de-joao-504599548>
25. Grother, Patrick, Mei Ngan e Kayee Hanaoka. 2019. *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*. National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.IR.8280>
26. Harcourt, Bernard. 2015. *Exposed: Desire and Disobedience in the Digital Age*. Cambridge: Harvard University Press.
27. Kafka, Franz. 2006. *O processo*. Traduzido por Marcelo Backes. Porto Alegre: L&PM.
28. Kember, Sarah. 2014. “Face Recognition and the Emergence of Smart Photography”. *Journal of Visual Culture* 13 (2): 182-199. <https://doi.org/10.1177/1470412914541767>
29. Lima, Thallita, Thaís Cruz, Pedro Diogo e Felipe da Silva. 2024. *Vigilância por lentes opacas: mapeamento da transparência e responsabilização nos projetos de reconhecimento facial no Brasil*. Rio de Janeiro: Centro de Estudos de Segurança e Cidadania.
30. Lobato, Luisa Cruz, Pedro Augusto P. Francisco e Louise Marie Hurel. 2024. “Videomonitoramento”. Instituto Igarapé. <https://igarape.org.br/videomonitoramento-webreport/>
31. Mayer-Schönberger, Viktor e Kenneth Cukier. 2013. *Big Data: A Revolution That Will Transform How We Live, Work, and Think*. Boston: Houghton Mifflin Harcourt.
32. Mendes, Celso Helder Furtado e Fernando Vechi. 2020. “Tecnovigilância e controle e(m) tempos securitários: quem são os alvos?”. Em *Algoritmos*, editado por Jesús Sabariego, Augusto Jobim do Amaral e Eduardo Baldissera Carvalho Salles, 219-232. São Paulo: Tirant Lo Blanch.
33. Ministério da Justiça e Segurança Pública. 2019. *Portaria n.º 793, de 24 de outubro de 2019*. Diário Oficial da União, seção 1, edição 208, 55-56. <https://dspace.mj.gov.br/handle/1/1380>
34. Negri, Antonio e Michael Hardt. 2001. *Império*. Traduzido por Berilo Vargas. Rio de Janeiro: Record.
35. Nunes, Pablo. 2019a. “EXCLUSIVO: levantamento revela que 90,5% dos presos por monitoramento facial no Brasil são negros”. *The Intercept Brasil*, 21 de novembro. <https://www.intercept.com.br/2019/11/21/presos-monitoramento-facial-brasil-negros/>
36. Nunes, Pablo. 2019b. “Novas ferramentas, velhas práticas: reconhecimento facial e policiamento no Brasil”. Em *Retratos da violência: cinco meses de monitoramento, análise e descobertas*, coordenado por Silvia Ramos, 67-70. Rio de Janeiro: Centro de Estudos de Segurança e Cidadania.
37. Nunes, Pablo, Thallita G. L. Lima e Yasmin Rodrigues. 2023a. *Das planícies ao planalto: como Goiás influenciou a expansão do reconhecimento facial na segurança pública brasileira*. Rio de Janeiro: Centro de Estudos de Segurança e Cidadania.
38. Nunes, Pablo, Thallita G. L. Lima e Yasmin Rodrigues. 2023b. *O sertão vai virar mar: Expansão do reconhecimento facial na Bahia*. Rio de Janeiro: Centro de Estudos de Segurança e Cidadania.
39. O Panóptico. 2024. *Monitor de novas tecnologias de segurança pública no Brasil*. <https://www.opanoptico.com.br/#mapa>
40. Osoba, Osonde e William Welser. 2017. *An Intelligence in Our Image: The Risks of Bias and Errors in Artificial Intelligence*. Santa Monica: RAND Corporation. <https://doi.org/10.7249/rr1744>
41. Pasquale, Frank. 2015. *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge: Harvard University Press.
42. Reis, Carolina, Eduarda Almeida, Felipe da Silva e Fernando Dourado. 2021. *Relatório sobre o uso de tecnologias de reconhecimento facial e câmeras de vigilância pela administração pública no Brasil*. Brasília: Laboratório de Políticas Públicas e Internet.
43. Revel, Judith. 2014. *Foucault, un pensamiento de lo discontinuo*. Traduzido por Irene Agoff. Buenos Aires: Amorrortu.
44. Rodríguez, Pablo Esteban. 2019. *Las palabras en las cosas: saber, poder y subjetivación entre algoritmos y biomoléculas*. Buenos Aires: Cactus.
45. Rosa, Alexandre Moraes da e Augusto Jobim do Amaral. 2017. “A ostentação penal”. Em *Cultura da punição: a ostentação do horror*, 13-92. Florianópolis: Empório do Direito.
46. Rouvroy, Antoinette e Thomas Berns. 2015. “Governamentalidade algorítmica e perspectivas de emancipação: o dispar como condição de individuação pela relação?”. *Revista Eco Pós: Tecnopolíticas e Vigilância* 18 (2): 36-56. Traduzido por Pedro Henrique Andrade. <https://doi.org/10.29146/eco-pos.v18i2.2662>
47. Schervenski da Silva, Tiago Luis. 2024. “Governamentalidade algorítmica e as tecnologias de reconhecimento facial: reconfigurações Punitivas no Contexto Brasileiro”. Graduação em Direito, Pontifícia Universidade Católica do Rio Grande do Sul, Brasil.
48. Schervenski da Silva, Tiago Luis e Valentina Simões Pires Curcio. 2025. “A ineficiência da aplicação da tecnologia de reconhecimento facial na segurança pública brasileira: uma análise jurídico-filosófica do uso do dispositivo securitário”. Em *Algoritmos II*, 732-742. Valência: Tirant Lo Blanch.
49. Silva, Tarcizio da. 2019. “Visão computacional e vieses racializados: branquitude como padrão no aprendizado de máquina”. *Anais do II Congresso de Pesquisadoras/es Negras/os do Nordeste, Epistemologias negras e lutas antirracistas*, editado por Sérgio Rodrigues de Santana, Solange P. Rocha e Ana Marinho Cristina Lúcio, 811-823. <https://www.periodicos.ufpb.br/index.php/ci/issue/view/2402>

50. Silva, Tarcízio da. 2022. *Racismo algorítmico: inteligência artificial e discriminação nas redes digitais*. São Paulo: Edições Sesc.
51. Universidade Federal do Ceará. 2024. *RIPD — Relatório de Impacto de Proteção de Dados*. <https://lgpd.ufc.br/pt/ripd-relatorio-de-impacto-de-protecao-de-dados/>
52. Zuboff, Shoshana. 2018. “*Big other*: capitalismo de vigilância e perspectivas para uma civilização de informação”. Em *Tecnopolíticas da vigilância: perspectivas da imagem*, editado por Fernanda Bruno, Bruno Cardoso, Marta Kanashiro, Luciana Guilhon e Lucas Melgaço, 17-68. São Paulo: Boitempo.

Tiago Luis Schervenski da Silva

Mestrando em Filosofia pela Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS), Brasil. Pesquisador vinculado ao grupo de pesquisa Criminologia, Cultura Punitiva e Crítica Filosófica (PUCRS). <https://orcid.org/0009-0000-9780-1274> | tiago.silva01@edu.pucrs.br

Ricardo Jacobsen Gloeckner

Doutor em Direito pela Universidade Federal do Paraná, Brasil. Professor do Programa de Pós-Graduação em Ciências Penais da Pontifícia Universidade Católica do Rio Grande do Sul, Brasil. Publicações recentes: “Tre tesi sull’incostituzionalità sostanziale dell’articolo 383 del codice di procedura penale brasiliano” (em coautoria), *Diritto e Giustizia Minorile* 3-4: 76-92, 2024; e “Um sistema de informantes? Notas sobre o direito ao confronto e o estímulo a uma justiça criminal *underground*” (em coautoria), *Revista Brasileira de Políticas Públicas* 13: 180-211, 2023, <https://doi.org/10.5102/rbpp.v13i1.8751>. <https://orcid.org/0000-0002-1205-380X> | ricardo.gloeckner@pucrs.br

