RECONHECIMENTO FACIAL E INTELIGÊNCIA ARTIFICIAL: LIMITES REGULATÓRIOS ENTRE BRASIL E REINO UNIDO

FACIAL RECOGNITION AND ARTIFICIAL INTELLIGENCE: REGULATORY BOUNDARIES BETWEEN BRAZIL AND THE UNITED KINGDOM

Augusto Jobim do Amaral - Professor dos Programas de Pós-Graduação em Ciências Criminais e em Filosofia, ambos da PUCRS. Email: augusto.amaral@pucrs.br .

Gabriel Saad Travassos - Doutorando em Ciências Criminais. Mestre em Direito e Justiça Social. Defensor Público Federal. Email: travassosgabrielsaad@gmail.com

Samuel Medeiros Andreatta - Doutorando e Mestre em Ciências Criminais (PUCRS), com estágio de pesquisa doutoral na Queen Mary University of London. O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Código de Financiamento 001. E-mail: samuelandreatta@hotmail.com.

O artigo analisa criticamente o uso de tecnologias de reconhecimento facial no Brasil e no Reino Unido, com foco na regulação e nos impactos sobre direitos fundamentais. O objetivo é comparar os marcos legais, práticas institucionais e modelos de controle dessas tecnologias em ambos os países. Utilizando método genealógico-crítico, aliado à pesquisa documental e ao estudo comparado, a investigação evidencia que, enquanto o Reino Unido dispõe de diretrizes regulatórias mais consolidadas, o Brasil apresenta um cenário fragmentado e desregulado, com ampla atuação privada e ausência de transparência. Conclui-se, portanto, que a pulverização da vigilância e a tecnopolítica do risco impõem desafios urgentes à proteção de direitos civis.
PALAVRAS-CHAVE: Direito Processual Penal – Teoria Crítica – Reconhecimento Facial - Inteligência Artificial

This article critically examines the use of facial recognition technologies in Brazil and the United Kingdom, focusing on regulation and the impact on fundamental rights. The objective is to compare legal frameworks, institutional practices, and control models of these technologies in both countries. Using a genealogical-critical method, combined with documentary research and comparative analysis, the study reveals that while the UK has more consolidated regulatory guidelines, Brazil presents a fragmented and unregulated scenario, marked by significant private sector involvement and a lack of transparency. It concludes that the diffusion of surveillance and risk-based technopolitics pose urgent challenges to the protection of civil rights.
KEYWORDS: Procedural Penal Law – Critical Theory – Facial Recognition - Artificial Inteligence.

INTRODUÇÃO

Há um movimento global de expansão do reconhecimento facial automatizado. Do controle de fronteiras, passando pelo policiamento preditivo até um controle minucioso de identidades, a tarefa de coletar dados, localizar pessoas e identificar suspeitos a partir de avaliações de risco tem sido naturalizada.

Os espaços fronteiriços passam a assumir contornos inexoravelmente digitais, e diversos países como Austrália, França, Reino Unido, Alemanha, Holanda e Estados Unidos tem expandido seus instrumentos de vigilância. Segundo Matulionyte e Zalnieriute (2024, p.1), todas estas nações contam com câmeras de reconhecimento facial. No Brasil, por exemplo, o projeto IRIS, capitaneado pela Receita federal, realiza uma avaliação de risco dos viajantes sob um mote de eficiência, como indica o relatório de experiência do projeto.

Um elemento central da propagação dessas tecnologias é o risco. As câmeras são estruturadas por modelos algorítmicos (O'Neil, 2020, p. 19) para, a partir de comportamentos, identificar a existência de um risco ou, ainda, associar faces a bancos de suspeitos policiais. A opacidade de sua operacionalidade técnica levou estudiosos do tema a classificarem esses algoritmos como verdadeiras "caixas pretas" (Pasquale, 2015).

A abundância de espaços de controle aliada à sensação de resignação com a perda da privacidade, ou pelo menos sua vulnerabilização

permanente, é uma característica importante das sociedades de controle, pois seus dispositivos não estão mais restritos à tônica disciplinar dos corpos, mas sim ao monitoramento ao ar livre, ecoando perspectivas já aventadas no campo de pesquisa de estudos da tecnologia (Amaral; Dias, 2024, p. 15). É um controle que produz ativamente a circulação como forma de vigiar a liberdade segundo paradigmas do risco.

As pretensões de informação total acopladas à conquista de corações e mentes, cuja emergência é possível conectar às práticas de contrainsurgência (Harcourt, 2021), ganham garras tecnopolíticas e passam, cada vez mais rápido, do estranhamento à normalização. Conforme Matulionyte e Zalnieriute (2024), cerca de 70% das forças policiais possuem algum tipo de reconhecimento facial e 60% dessa tecnologia tem como objeto os aeroportos. Nos aeroportos britânicos, a exigência de retirada da burca, como indica a *Freedom of Information Release* (14660), para o reconhecimento facial pode parecer inofensiva, mas demonstra um reforço de uma lógica de gerenciamento de risco.

A lógica do aeroporto é transposta ao espaço urbano, como indica Bratton (2015). É um espaço no qual convivem em "harmonia" fluxos infinitos de pessoas, direcionados pelos mais finos controles policiais que impõem vigilância ao mesmo tempo que intencionam trazer uma sensação de conforto, sem qualquer aparente contradição.

Nossas faces, expressão imediata da individualidade são traduzidas por linhas de código. Elas se tornam o novo marco de um controle cada vez mais ubíquo. Esse cenário de captura contínua de dados centrado numa razão que equaciona cálculo político-econômico e controle de risco tem gerado diversas tensões que concernem marcadores sociais, proteção de dados, a falta de transparência e violação de direitos civis e liberdades fundamentais.

Diante deste panorama, o artigo tem por objetivo questionar em que medida o quadro normativo e as práticas de controle podem aproximar o Reino Unido ao Brasil na utilização uma tecnologia tão problemática quanto controversa como o reconhecimento facial. O espaço amostral comparativo é delimitado pelas fontes jurídicas diretas compreendidas por legislação e regulamentação no Reino Unido. Tal opção metodológica diz respeito ao fato de que naquele país, além do alto grau tecnológico empregado pelas agências policiais, o tema do reconhecimento facial e seus riscos já foi objeto de apurada apreciação pelo Poder Judiciário local.

Não passa despercebido o fato de que no Brasil e no Reino Unido vigoram sistemas distintos. Contudo, além de não ser possível falarmos de um sistema puro, a influência globalizante da *common law* no sistema brasileiro é cada vez mais marcante, a exemplo dos mecanismos de uniformização das teses nos tribunais superiores, de institutos de negócio jurídico processual em âmbito penal e da óbvia inspiração na legislação de dados brasileira que provêm, em parte, do arcabouço jurídico europeu (cf. Damaska, 1991).

Um aspecto relevante para o estudo comparado com um país europeu é a possibilidade

de análise do impacto das diretrizes europeias sobre reconhecimento facial. Muito embora o Reino Unido não integre a União Europeia, a *"United Kingdom General Protection Regulation"*, tem inspiração na Lei Geral de Proteção de Dados da União Europeia, além da óbvia proximidade geográfica e cultural, entende-se que é pertinente investigar se normas como o *European Union Artificial Intelligence Act* tiveram alguma influência na regulamentação local das tecnologias de reconhecimento facial.

Por fim, como o debate da temática extravasa uma análise estritamente procedimental relativa aos sistemas jurídicos, acredita-se tais diferenças não prejudica a realização da pesquisa, visto que a aproximação crítica das praticas jurídicas deve ser munida de uma interdisciplinariedade que a revigora. Assim, propõe-se que sejam estruturados eixos de análise a partir dos usos, marcos regulatórios e precedentes judiciais sobre o emprego das tecnologias de reconhecimento facial, a fim de avaliar o tratamento conferido a temas como a proteção de dados, o risco à liberdade de expressão, o viés discriminatório e a moldura regulatória.

A pesquisa é qualitativa, assumindo como técnicas de pesquisa a revisão bibliográfica, o estudo comparado e a pesquisa documental. O método é o genealógico-crítico (Harcourt, 2024), demarcando a emergência do reconhecimento facial como tecnologia que é objeto de crítica pormenorizada. Assim, há um foco na diversidade de experiências entre diferentes países que pode oferecer subsídios valiosos para refletir sobre os caminhos possíveis para a regulamentação — ou mesmo a proibição — das tecnologias de reconhecimento facial em nível nacional. A comparação entre os distintos contextos permitirá identificar as lacunas, lembrando que um espaço de omissão gerado pela ausência de uma atuação proativa do poder público poderá implicar na transferência de funções eminentemente estatais para o âmbito privado, dada velocidade sob as quais as evoluções tecnológicas estão submetidas.

1 TECNOLOGIAS DE RECONHECIMENTO FACIAL

Os esforços de categorização biológica não são estranhos às ciências criminais. Não é demasiado lembrar das considerações fenotípicas lombrosianas, que continuam, até hoje em suas facetas neopositivistas, a demonstrar a importância do corpo para o poder punitivo. A expansão de formas de controle também é efeito da transposição de métodos coloniais para o espaço interno. A datiloscopia é efeito do processo de colonização britânico. O método de captura de impressões digitais teve seu momento privilegiado de aplicação por William Hershel (1916) no processo de colonização inglês de Bangladesh.

Tanto a biometria facial quanto a digital demandam procedimentos, em tese, menos intrusivos, afinal lidam com partes visíveis do corpo. Mas a diferença significativa é também a diferença que marca a passagem das técnicas disciplinares para as técnicas da sociedade de

controle: a biometria facial pode ser obtida sem a cooperação ou conhecimento do sujeito analisado, pode ser analisada em larga escala e é pulverizada.

Os estudos sobre esse método de captura da biometria por meio do rosto remontam ao século XX, no período da Guerra Fria, e se entrelaçam a táticas de defesa nacional e táticas de contrainsurgência internalizadas (Harcourt, 2021) . Com auxílio da *Rand Corporation*, como indica Kelly (2006), em 1967, Woody Bledsoe conduziu uma equipe de pesquisa em Palo Alto, nos Estados Unidos, que desenvolveu um método de atribuição de *scores* para faces comparadas a uma database de fotografias de quatrocentos homens causasianos.

Buscava-se um modelo de aprendizado de máquina desenvolvido com o objetivo de identificar uma face específica a partir de suas características mensuradas. O *Briscoe Center for American History* conserva, entre suas coleções, os registros dessas medições, bem como uma carta de 1965 na qual Bledsoe solicita apoio financeiro para um projeto voltado à determinação da origem racial ou do local de desenvolvimento de um indivíduo (Bledsoe, 1965).

A utilização em larga escala do reconhecimento facial apenas ocorre, porém, no século XXI. A partir década de 2010, com a multiplicação exponencial de câmeras de alta definição instaladas em dispositivos pessoais, objetos, espaços públicos e privados, a matéria-prima para o desenvolvimento dos sistemas estava dada: bases gigantescas de imagens faciais para treinamento, processamento e sistematização.

Esse contexto alçou o reconhecimento facial a uma dimensão farmacológica, remédio e veneno, pois ele se materializa conjugando experiências positivas de acesso a serviços e produtos – circuitos de prazer – com experiências negativas de vigilância e discriminação – circuitos de controle (Bruno, 2013, p. 34). Em ambos os casos, há o reforço de um mecanismo protocolar sob o véu algorítmico da neutralidade. Este mecanismo não só cria seu próprio espaço de veridição, mas estabelece os próprios limites da identidade vinculada a identificação de um risco associado ao sujeito.

Quando tratamos de reconhecimento facial estamos basicamente falando de uma tecnologia que é capaz de detectar e extrair os dados de uma face humana e analisar a probabilidade de correspondência dessa com uma base de faces pré-identificadas (Selwyn et al, 2024). A confirmação de um rosto é feita a partir de um cálculo probabilístico denominado *match score* (Elesbão et al, 2020).

Essa complexa rede diversificada e heterogênea de uso e impacto das tecnologias de reconhecimento facial demanda uma reflexão sobre o quadro regulatório e sobre possíveis direitos fundamentais atingidos. Como destaca Helena Machado (2025, p. 27), preocupações emergem em torno da ampliação da vigilância massiva, das ameaças à privacidade, às liberdades civis e aos direitos humanos; da perpetuação da discriminação contra grupos estigmatizados; e da imprecisão da tecnologia para pessoas que não

estão no padrão do "homem branco". Ademais, as próprias noções jurídicas estão sob um espaço de tensão tecnopolítico, como demonstra Zuboff (2019), no âmbito da fragilização da privacidade a partir de *advocacy* das ditas *bigtechs*.

Questões sensíveis são levantadas desde logo: quais os critérios para a definição de onde, quando e por quanto tempo as faces serão capturadas; quais os critérios para a formação e manutenção da base de dados, bem como para a elaboração da lista de procurados pelas agências policiais ou o compartilhamento das faces capturadas com empresas privadas?

2 TECNOLOGIAS DE RECONHECIMENTO FACIAL NO REINO UNIDO

Atualmente, as tecnologias de reconhecimento facial (TRFs) utilizadas no Reino Unido operam com base em um software desenvolvido pela empresa japonesa NEC. Essa companhia fornece câmeras tanto para a Polícia Metropolitana quanto para a Polícia de South Wales (SWP). No entanto, ainda há opacidade sobre os critérios adotados na escolha dessa tecnologia e sobre o funcionamento interno do sistema (Gentile, 2025).

Até 2019, a fiscalização do uso desses sistemas biométricos era responsabilidade do *Law Enforcement Facial Images*. Hoje, essa tarefa está a cargo de dois órgãos: o *Information Commissioner's Office* (ICO) e o *Biometric and Surveillance Camera Commissioner*. O ICO é o órgão regulador independente do Reino Unido no que se refere à proteção de dados e ao direito à informação. Ele atua com base em dois pilares legais: o *Data Protection Act de 2018 e o Freedom of Information Act* de 2000. Sua atuação abrange amplamente qualquer atividade envolvendo o tratamento de dados pessoais. Relatório divulgado pelo órgão denotou que, em 2022, mais de 245.000 pedidos de quebra de sigilo de dados para fins de investigação penal haviam sido autorizados, a tendência, como demonstram os dados, é de um crescimento linear.

Por outro lado, o *Biometric and Surveillance Camera Commissioner* tem como missão monitorar especificamente o uso de dados biométricos e imagens de videovigilância conforme definido nas leis nacionais de segurança, investigação criminal e ordem pública. Esse órgão substituiu o antigo *Comissioner for the Retention and Use of Biometric Material* e fundamenta seu trabalho no *Protection of Freedoms Act de* 2012.

Essas duas entidades têm o papel de fiscalizar, emitir pareceres e produzir relatórios que avaliam se o tratamento de dados pessoais está alinhado com os direitos fundamentais. Porém, atuam dentro de uma estrutura regulatória bastante fragmentada e sobreposta, uma vez que ainda não há uma legislação específica dedicada às TRFs no país. Muito embora não haja legislação específica dedicada às TRFS, a mera existência de órgão regulatório implica em uma dupla análise da admissibilidade das medidas: tanto em sede judicial como em sede de análise pelo comissário.

Fussey e Murray(2024) delimitam o espaço geral das normas que compõem o arcabouço jurídica do uso das TRFs no Reino Unido, incluindo: o *Human Rights Act* de 1998, o *Freedom of Information Act* de 2000, o *Regulation of Investigatory Powers Act* de 2000, o *Protection of Freedoms Act* de 2012, o *Data Protection Act* de 2018 e o *Surveillance Camera Code of Practice* de 2013, revisado em 2021.

A análise do impacto das TRFs sobre o direito à privacidade geralmente se baseia no artigo 8º do *Human Rights Act*, que reflete a Convenção Europeia de Direitos Humanos ao garantir o direito ao respeito pela vida privada e familiar, domicílio e correspondência. Qualquer intervenção estatal nesse direito só é permitida quando prevista em lei e necessária, em uma sociedade democrática, para fins como segurança nacional, ordem pública, saúde, moral, ou proteção dos direitos alheios. Esses critérios — legalidade, necessidade e proporcionalidade — foram utilizados pelo Judiciário britânico para estabelecer diretrizes sobre o uso das TRFs.

O *Data Protection Act* (DPA) de 2018 incorpora à legislação britânica os preceitos do Regulamento Geral de Proteção de Dados (RGPD) da União Europeia, também de 2018. Segundo Gentile (2024), essa legislação tem um papel central na regulamentação das TRFs, ao impor limites para o uso de dados sensíveis e estabelecer exigências para as entidades públicas.

Entretanto, o RGPD exclui explicitamente de seu escopo as operações realizadas por autoridades responsáveis por prevenir, investigar ou reprimir crimes, ou por aplicar sanções penais. Assim, enquanto o uso de TRFs em ambientes comerciais pode ser analisado à luz do RGPD, sua aplicação por órgãos públicos em contextos criminais segue uma regulação distinta: a Diretiva Europeia 2016/680. Essa norma determina, entre outras exigências, que os países membros definam prazos para o armazenamento de dados pessoais e realizem revisões periódicas desses registros

Mais recentemente, *o European Union Artificial Intelligence Act* de 2024 tratou diretamente dos sistemas de reconhecimento facial, proibindo a comercialização e o uso de tecnologias de IA que ampliem a base de dados de TRFs por meio da coleta indiscriminada de imagens faciais da internet ou de sistemas de CFTV.

O Data Protection Act também traz diretrizes específicas para o uso de dados por órgãos públicos, baseadas em seis princípios fundamentais: i) legalidade; ii) finalidade específica e legítima; iii) adequação e limitação à necessidade; iv) precisão e atualização dos dados; v) limitação do armazenamento ao tempo necessário; e vi) segurança no processamento das informações.

Outro documento essencial é o *Protection of Freedoms Act* de 2012 que regula o uso de provas, inclusive dados biométricos obtidos por TRFs. Com base nessa lei, o Reino Unido criou o *Surveillance Camera Code of Practice*, publicado em 2013 e atualizado em 2021. Este código estabelece 12 princípios orientadores para a utilização de sistemas de vigilância por câmeras. Entre esses princípios, destacam-se: definição clara de propósito, revisões periódicas,

transparência, responsabilidade, regulação prévia e comunicação com o público, limitação do tempo de armazenamento, restrição de acesso, conformidade com padrões operacionais, proteção contra abusos, auditorias regulares, efetividade e atualização constante.

O Código reconhece que o uso de câmeras em locais públicos pode afetar direitos fundamentais como privacidade, liberdade de expressão, religião, pensamento, associação e proteção contra discriminação. Assim, ele determina que sistemas de reconhecimento facial só devem ser utilizados quando alternativas menos invasivas forem inviáveis, e sempre com supervisão humana antes que qualquer decisão que afete um indivíduo seja tomada.

Além disso, é exigido que o público seja informado sobre os locais monitorados, os responsáveis pelo sistema, suas finalidades, desempenho e formas de auditoria. As empresas que operam tais sistemas devem estar abertas a demandas do público e fornecer informações claras sobre seu funcionamento, com direito a recurso em caso de resposta insatisfatória.

Antes da instalação de qualquer sistema de vigilância, a comunidade impactada deve ser consultada e suas opiniões levadas em consideração. Para que possam operar legalmente, os operadores devem solicitar uma licença *à Security Industry Authority,* comprovando os requisitos técnicos necessários. Essa autoridade também é responsável pela fiscalização do setor. Por fim, os dados coletados não podem ser armazenados por mais tempo do que o necessário, respeitando os limites definidos pela legislação de proteção de dados, conforme regulado pelo *Information Commissioner's Office.*

Nossas sociedades de controle, centradas na pulverização da vigilância e mecanismos de governo difusos, geram efeitos específicos nas TRF. O caso de Londres é emblemático: a polícia metropolitana contará com um investimento de 55 milhões de libras nos próximos três anos (Sing, 2024) para a compra e implementação de câmeras de reconhecimento facial ao vivo por meio de vans equipadas com tecnologia de reconhecimento facial.

O espaço de atuação dessa tecnologia é regrado pelo *Metropolitan Police Policy Document*, que disciplina o uso de tecnologia de reconhecimento facial em tempo real ou ao vivo. Trata-se de um código de conduta da atuação policial que estabelece limites quanto aos deveres de retenção e obtenção dos dados dos rostos, bem como, determina a observância de pressupostos de proporcionalidade na aplicação da medida.

O documento estabelece a distância de 300m a 500m como o limite do raio de atuação da câmera de reconhecimento facial ao vivo ou em tempo real. Há dois casos específicos nos quais a instauração da tecnologia de reconhecimento facial em tempo real ou ao vivo é adequada: pontos de alta incidência de práticas de crimes e pontos de alta incidência de desaparecimento de pessoas. Os pontos de alta incidência de crimes concernem uma ampla gama de delitos, como crimes contra a propriedade, crimes contra a pessoa, tráfico de drogas e condutas relativas à evasão carcerária. A organização do espaço de vigilância deve ser precedida de aviso ao público

que circula por aquela região, e demonstra a perda da centralidade do polo vigilante, visto que o equipamento é montado em vans, o que confere mobilidade a essas técnicas:

Figura 1 – Van de policiamento equipada com tecnologia de reconhecimento facial: Registro de van policial no distrito de Hammersmith, Londres, próxima a centros comerciais. A imagem evidencia o uso de tecnologia de reconhecimento facial como parte das operações de vigilância. Fonte: autores.

Figura 2 – Aviso informativo sobre uso de reconhecimento facial em tempo real.
Cartaz localizado no centro comercial Kings Mall, no distrito de Hammersmith, Londres. O aviso informa:“Agentes policiais estão usando a Tecnologia de Reconhecimento Facial em Tempo Real para encontrar pessoas que estão sendo buscadas pela polícia ou pelo judiciário. Se você passar pelo sistema de detecção de reconhecimento facial, seus dados biométricos faciais serão processados. Não há nenhum requerimento legal que gere a obrigação de passar por esse sistema. Caso você passe, e o sistema não encontre qualquer alerta, o sistema irá automaticamente e imediatamente deletar seus dados biométricos.” (Tradução livre). Fonte: autores.

Para além da pulverização da vigilância materializada pela mobilidade das vans de monitoramento, essa dissipação da centralidade estatal da atividade de vigilância advém da privatização desses serviços. A indústria teve um crescimento de 60% entre 2008 e 2021 no Reino Unido (Pazzona e White, 2024). É preciso destacar a presença constante de vans equipadas com câmera de segurança (CCTV) coordenadas por

empresas privadas em toda cidade, produzindo um cenário de privatização tácita da segurança pública, por meio do deslocamento de funções tipicamente estatais para o setor privado (Cf. Rigakos, 2002).

O tamanho da indústria de segurança privada foi o problema de pesquisa de Pazzona e White (2024). Os pesquisadores concluíram que a base de dados da SIA, por si só, não confere uma imagem fidedigna da dimensão da indústria. Assim, os autores optaram por incorporar dados coletados pelo registro de empresas e relações empregatícias. O espaço amostral gerado pela confluência destes bancos de dados é compreendido por quase 390.000 empresas licenciadas pela (SIA) e cerca de 187.000 trabalhadores registrados, como indicam Pazzona e White (2024, p. 14).

A SIA (*Security industry Authority*) não lista o reconhecimento facial como atividade distinta, tornando incerta a afirmação de inexistência de sistemas de reconhecimento facial por empresas privadas. Todavia, em sede de atuação das agências punitivas estatais, o *Surveillance Camera Code of Practice (SCCP)* se refere especificamente ao reconhecimento facial em tempo real. Quando a polícia utilizar um sistema de reconhecimento facial ao vivo para localizar uma pessoa com base em uma lista de monitoramento deve: i) definir os critérios sobre quando e onde será empregado o sistema; ii) garantir que qualquer dado biométrico que não produza um alerta contra alguém da lista de monitoramento seja imediatamente excluído do sistema; iii) levar em conta o potencial impacto do algoritmo sobre membros de grupos vulneráveis; iv) e instaurar um processo de autorização para a implantação do sistema.

De acordo com o Código de Práticas, portanto, existe uma série de requisitos e procedimentos prévios à licitação, à contratação e à operacionalização da TRF. Esses padrões deveriam garantir alguma salvaguarda diante do risco de violações decorrentes do uso indevido das imagens capturadas. Ocorre que, apesar da relevância desses documentos para guiar as ações policiais, ainda não está clara a força vinculante de suas disposições, sobretudo para sistemas operados em espaços controlados por empresas privadas, que não estão mencionados no Código de Prática. Essa constelação de normas sobrepostas e heterogêneas têm dificultado o enfrentamento da matéria e deixado lacunas no contexto das operações que utilizam TRF (Gentile, 2024, p. 185).

3 TECNOLOGIAS DE RECONHECIMENTO FACIAL NO BRASIL

Até janeiro de 2025, o Brasil registrava 364 projetos de reconhecimento facial em funcionamento no país, o que significa uma estimativa de mais de 82 milhões de pessoas potencialmente vigiadas pelo mecanismo biométrico (O Panóptico, 2025).

Analisando a trajetória dessa tecnologia no país, podemos situar a Copa do Mundo de 2014 como um evento-chave de virada metodológica na gestão das multidões, com gastos orçamentários aproximados de R$ 957,5 bilhões (Augusto *et al*,

2024). Por meio da adaptação da legislação e investimentos em estruturas de monitoramento em larga escala, a exemplo dos Centros Integrados de Comando e Controle (CICC), o Estado brasileiro buscava se adaptar ao Manual de Procedimentos da FIFA e tornou seu espaço territorial um grande laboratório de testes de reconhecimento facial.

Novas tecnologias de vigilância populacional foram adquiridas e testadas, como o sistema Pacificador, utilizado pelo Exército para coordenação das operações. Drones militares para vigilância do território e o uso de ferramentas de tecnologia facial para entrada em estádios e monitoramento durante as partidas passaram a não serem mais novidade (Augusto *et al*, 2024). Esse modelo de vigilância não se limitou às arenas esportivas, havendo estudos recentes que apontam a dispersão de tecnologias de reconhecimento facial em espaços públicos como praças, paradas de ônibus e, até mesmo, escolas (Israel, 2023).

Atualmente, os projetos alcançam custos de operação na ordem de mais de R$ 969 milhões e envolvem diversas empresas privadas que operam *softwares* de captura, armazenamento, tratamento e compartilhamento das imagens faciais (Lima *et al*, 2024). Relatório sobre a transparência dessas contratações aponta que empresas como a Axxon Next SW-ANV-FRCT-RTL, HikiCenter Professional, SecurOS, SAFR, Holosens Huawei, VMS Digifort versão Enterprise 7.3.0.1, Digifort e Dahua estão entre as que recebem recursos públicos e autorização para operar a captura de dados biométricos faciais (Lima *et al*, 2024). Não há transparência sobre os critérios de escolha das empresas, o operador do projeto, o custo total e políticas de proteção de dados.

O projeto *O Panóptico,* que realiza o monitoramento das tecnologias de reconhecimento facial no Brasil, aponta que em 72,5 % dos casos as entidades não apresentaram informações sobre a elaboração de relatórios de impacto à proteção de dados pessoais (Lima *et al*, 2024). De acordo com a equipe de pesquisa, os projetos operam sem atender os padrões mínimos de transparência ativa e passiva, o que fragiliza o controle social, abre espaços para abusos, desvios, usos desproporcionais e práticas discriminatórias.

Diferentemente do modelo britânico, o sistema de reconhecimento facial no Brasil não possui um Código de Práticas com diretrizes para definir os limites e a auditabilidade do processo de armazenamento, captura e tratamento dos dados biométricos faciais (Almeida, 2022). As empresas operam livremente em diversos Estados e municípios, sem que haja um controle concentrado sobre a eficácia da tecnologia, os gastos envolvidos, a transparência, a minimização dos vieses discriminatórios e a proteção do cidadão que tem a imagem armazenada.

Esse cenário é potencializado em virtude da falta de um órgão responsável por monitorar o funcionamento das empresas contratadas para operar câmeras de reconhecimento facial e as bases de dados, tanto na formação quanto no tratamento. A Autoridade Nacional de Proteção de Dados, prevista a partir da Lei n. 13.709, de 2018, além de ter um mandato mais genérico, não inclui o tratamento de dados pessoais para fins de

segurança pública e atividades de investigação e repressão de ações penais.

A ausência de lei não impediu que fossem dirigidos recursos para a contratação de sistemas de reconhecimento facial à distância. A Portaria n. 793, de 2019, do Ministério da Justiça e Segurança Pública, incentivou o financiamento de novas tecnologias para a "implantação de sistemas de videomonitoramento com soluções de reconhecimento facial, por Optical Character Recognition – OCR, uso de inteligência artificial ou outros".

Essa política incentivou Estados como o Rio de Janeiro, Bahia, Goiás e São Paulo a investirem vultosos recursos em políticas de captura e análise de imagens faciais no modelo *livestream,* isto é, em tempo real. Tal funcionalidade se utiliza da comparação um-para-muitos e se estrutura a partir da comparação de uma lista de suspeitos com as imagens faciais capturadas em meio a multidão em espaços públicos ou até mesmo privados, como é o caso do projeto de câmera interativa baiano (Nunes *et al*, 2023 e Ferreira; Amaral, 2024, pp. 45-58).

Na Bahia, mais de 1.750 pessoas foram presas nos últimos seis anos a partir do reconhecimento facial, em geral em virtude de delitos de menor potencial ofensivo ou de natureza cível, como furtos e inadimplência de pensão alimentícia (Lima *et al,* 2024). Contudo, não são apresentados registros dos falsos positivos identificados nessas operações. Estudos apontam que a taxa de falso positivo dos equipamentos de reconhecimento facial pode alcançar aproximadamente 72% dos alertas[178].

Além dos Estados, o reconhecimento facial tem sido implementado por municípios em meio ao processo de municipalização da segurança pública. O Estado de Goiás é um exemplo emblemático, onde por meio de emendas parlamentares com escassa transparência foram destinados recursos para a organização de pregões e a contratação de empresas para instalação de câmeras de reconhecimento facial a nível municipal "de forma autônoma, desregulada e sem qualquer proteção aos dados dos cidadãos". De acordo com dados atualizados, 51 municípios goianos receberam verbas para a utilização de câmeras de reconhecimento com base na Portaria n. 793, do Ministério da Justiça e Segurança Pública, totalizando o montante de R$ 8 milhões e o orçamento médio de R$ 260 mil por contrato (Nunes; Lima; Rodrigues, 2023, p. 8).

As empresas contratadas por esses municípios, geralmente associadas a famílias poderosas locais, sequer divulgam a forma de armazenamento, o tipo de dados coletados, as

[178] Os dados foram apresentados no julgamento do caso *Bridges* a partir da análise do emprego da tecnologia de reconhecimento facial na partida final da Liga dos Campeões da UEFA, em junho de 2018 (ROYAL COURTS OF JUSTICE, 2020).

funções e os limites para os usos das imagens e dados pessoais. Esse cenário está em direta oposição aos princípios balizadores do reconhecimento facial, como a finalidade, a transparência e a necessidade (Almeida, 2022). A pesquisa conduzida pelo O Panóptico concluiu, nesse caso, que não há um projeto estruturado de segurança pública com metas e objetivos, não constam indicadores de eficiência, relatórios de impacto e políticas de proteção efetiva de dados.

Os indicadores também não permitem associar a utilização do reconhecimento facial com a diminuição dos índices de delito, sobretudo se considerarmos que, como no caso Goiano, muitos municípios são interioranos e possuem índices muito baixos de delitos de natureza grave. Por outro lado, os contratos têm fomentado o discurso policialesco eleitoral e o enriquecimento de empresas privadas. É que Nils Christie (1998) aborda quando trata da indústria do controle do crime e do mercado que se estrutura em torno dos estímulo a novas infraestruturas de policiamento.

A utilização de inteligência artificial em questões atinentes ao reconhecimento facial gera uma mudança de paradigma que nos faz perceber as condições de emergência que fundamentam tal discurso. Por um lado, o efeito de uma máquina de visão que não só reconhece padrões e formas, mas apresenta-se como polo interpretativo gerando o que Virilio (1998, p. 73) denomina de "automatização da percepção". Essa transferência de funções humanas para a máquina faz emergir questões sobre a construção de pontos de vista. Por outro, a aparente neutralidade técnica fundada em perspectivas solucionistas tecnológicas, como indica Morozov (2016), reduzem o espaço de discussão quanto a aplicabilidade de determinadas tecnologias de poder aos termos logísticos de uma solução técnica.

CONCLUSÃO

Do estudo comparado entre os usos e marcos regulatórios dos sistemas de reconhecimento facial no Brasil e no Reino Unido foi possível notar que, apesar das similaridades no que diz respeito à rápida expansão das tecnologias de reconhecimento facial, existem sensíveis diferença no que tange à regulamentação dos limites do uso dessas tecnologias.

Enquanto o Reino Unido estabeleceu uma autoridade central para o monitoramento do emprego da biometria facial e um Código de Práticas, no Brasil não foram implementadas estruturas parecidas. Por aqui, Estados e municípios têm realizado contratações de empresas e *softwares* variados para o monitoramento dos cidadãos sem base legal, tampouco análise de necessidade e proporcionalidade da intervenção. O estudo comparado permitiu compreender os riscos em curso no cenário nacional e levantar relevantes paradigmas para a reflexão sobre o banimento ou a regulação das tecnologias de reconhecimento facial.

Em resumo, o ensaio apreende o binômio de implementação dessa tecnologias: a transferência da capacidade interpretativa para as máquinas fundamentada por uma aparente

neutralidade técnica e uma limitação do campo de pensamento por conta de uma razão centrada em um solucionismo tecnológico. Ao mesmo tempo, denota-se uma tendência geral de pulverização dos locais de vigilância, seja por conta da mobilidade dos instrumentos técnicos que as viabilizam, seja pela transferência de funções tradicionalmente desempenhadas pelo estado para entidades privadas.

REFERÊNCIAS

ALMEIDA, Eduarda Costa. Os grandes irmãos: o uso de tecnologias de reconhecimento facial para persecução penal. In: **Revista Brasileira de Segurança Pública**, São Paulo, v. 16, n. 2, 2022, p. 264-283.

AMARAL. Augusto Jobim do; DIAS, Felipe da Veiga. **Tecnopolítica criminal**. 1ª Ed., São Paulo: Tirant lo Blanc, 2024.

AUGUSTO, Acácio et al. O legado securitário após 10 anos da Copa do Mundo FIFA no Brasil. **Boletim (Anti)Segurança**, n. 36, LASINTEC, p. 2-8.

BLEDSOE, W.W. Letter from Woody Bledsow to Dr. Samuel Koslov regarding facial recognition to determine racial and environmental backgrounds. **The University of Texas History**. Briscoe Center for American History. Palo Alto, CA, 1965.

BRASIL. Ministério da Fazenda. Coordenação-Geral de TI da Receita Federal. Relatório de experiência. **Projeto IRIS – Reconhecimento Facial de Viajantes**. Disponível em *http://repositorio.enap.gov.br/handle/1/4132*. Acesso em Acesso em 21/04/2025.

BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**, Brasília, DF, 15.08.2018.

BRASIL. Ministério da Justiça. Portaria n. 793, de 24 de outubro de 2019. Regulamenta o incentivo financeiro das ações do Eixo de Enfrentamento à Criminalidade Violenta, no âmbito da Política Nacional de Segurança Pública e Defesa Social e do Sistema Único de Segurança Pública, com recursos do Fundo Nacional de Segurança Pública, previstos no inciso I do art. 7º da Lei n. 13.756, de 12 de dezembro de 2018**. Diário Oficial da União**, Brasília, DF, 25.10.2019.

BRATTON, Benjamin. **The stack: On Software and Sovereignty.** Cambridge: MIT Press, 2015.

BRUNO, Fernanda. **Máquinas de ver, modos de ser**: vigilância, tecnologia e subjetividade. Porto Alegre, Sulina, 2013.

CHRISTIE, Nils. **A indústria do controle do crime**: a caminho dos Gulags em estilo ocidental. Trad.: Luis Leiria. Rio de Janeiro: Editora Forense, 1998.

DAMASKA, Mirjan R.. **The faces of Jsutice and State Authority**: a comparative aproach to the legal process. New Haven: Yale University Press: 1991.

ELESBÃO, Ana Clara S.; DOS SANTOS; Jádia L. T.; MEDINA, Roberta da S. Quando as Máscaras (do reconhecimento facial) caírem, será um grande carnaval. In: **Algoritarismos**. Org.: Jesús Sabariego, Augusto Jobim do Amaral e Eduardo Baldissera Carvalho Salles. 1ª Ed., São Paulo: Tirant lo Blanch, 2020, p. 247-259.

ENGLAND. **R(Bridges) vs. South Wales Police**. Case No: C1/2019/2670. Court of Appel (Civil Division). Royal Courts of Justice. 11.aug.2020. Disponível em: https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf. Acesso: 21/03/2025.

EUROPEAN UNION. Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. **Official Journal of the European Union**. L 119/1. 4.5.2016.

FERREIRA, Ana Gabriela; AMARAL, Augusto Jobim do. Solucionismo Tecnológico na Segurança Pública Brasileira: o caso do reconhecimento facial na Bahia. In: SARLET at. al. (orgs.). **Tecnologia e**

Antidiscriminação. Londrina: Thoth, 2024, pp. 45-58.

FUSSEY, Pete; MURRAY, Daragh. **Independent report on the London Metropolitan Police service's trial of live facial recognition technology**. Essex: University of Essex Repository, July, 2019; KUHLMANN, Simone. Government Use of Facial Recognition Technologies under European Law. In:

GATES, Kelly. The past perfect promise of facial recognition technology. **ACDIS Occasional Paper** (2006). Disponível em: https://www.ideals.illinois.edu/items/40 Acesso em: 20/03/2025.

GENTILE, Giulia. Does Big Brother Exist? Facial Recognition Technology in the United Kingdom. In: **The Cambridge Handbook of Facial Recognition in the Modern State**. Org.: Rita Matulionyte and Monika Zalnieriute. Cambridge: Cambridge University Press, 2024.

HARCOURT, Bernard. On critical genealogy. **Contemporary Political Theory**, https://doi.org/10.1057/s41296-024-00715-y, 2024.

HARCOURT, Bernard. **Contra-revolução: Como o governo entrou em guerra contra os próprios cidadãos**. São Paulo: Glac Edições, 2021.

HERSHEL, William. **The origin of Finger- Printing**. Londres: Oxford University Press, 1916. Edição digital disponível em: https://galton.org/fingerprints/books/herschel/herschel-1916-origins-1up.pdf

ISRAEL, Carolina B. et al. **Reconhecimento facial nas escolas públicas do Paraná**. Curitiba, UFPR, 2023.

LIMA, Thallita. et al. **Vigilância por lentes opacas**: mapeamento da transparência e responsabilização nos projetos de reconhecimento facial no Brasil. Rio de Janeiro: CESeC, 2024.

MACHADO, Helena. Imaginários tecno-autoritários na América Latina: a contestação das tecnologias de reconhecimento facial. In: **Sociologia, problemas e práticas**, n. 107, 2025, p. 9-27.

MATULIONYTE, Rita; ZALNIERIUTE, Monika. **The Cambridge Handbook of Facial Recognition in the Modern State**. Cambridge: Cambridge University Press, 2024.

MOROZOV, Evgeny. **La locura del solucionismo tecnológico.** Traducido por Nancy Viviana Piñero. Buenos Aires: Katz Editores, 2016.

NUNES, Pablo; LIMA, Thallita G. L.; CRUZ, Thaís G. **O sertão vai virar mar**: expansão do reconhecimento facial na Bahia. Rio de Janeiro: CESeC, 2023.

NUNES, Pablo; LIMA, Thallita G. L.; RODRIGUES, Yasmin. **Das planícies ao planalto**: como Goiás influenciou a expansão do reconhecimento facial na segurança pública brasileira. Rio de Janeiro: CESeC, 2023.

O'NEIL, Cathy. **Algoritmos de destruição em massa**: como o big data aumenta a desigualdade e ameaça a democracia. Trad.: Rafael Abraham, 1ª Ed., Santo André, SP: Editora Rua do Sabão, 2020.

O Panóptico. **Monitor de novas tecnologias na segurança pública do Brasil**. Disponível em: https://www.opanoptico.com.br/#regioes. Acesso em 20.03.2025.

PASQUALE, Frank. **The Black Box Society: The Secret Algorithms That Control Money and Information**. Massachusetts: Harvard University Press, 2015.

PAZZONA, MATTEO; WHITE, Adam. Size matters: measuring the private security industry in the United Kingdom. In: **Crime Prevention and Community Safety**, 26 (3), 2024, pp. 333-346. Disponível em: https://doi.org/10.1057/s41300-024-00213-8

RIGAKOS, Georg S.. **The New Parapolice**: risk market and the commodified social control. Toronto: University of Toronto Press, 2002.

SELWYN, Neil; ANDREJEVIC, Mark; O'NEILL, Chris; GU, Xin; SMITH, Gavin. Facial Recognition Technology: Key Issues and Emerging Concerns.