Faces make cases: o caso *Clearview AI* e os desafios do uso de tecnologias algorítmicas no sistema de justiça criminal brasileiro

"Faces make cases": the Clearview AI case and the challenges of using algorithmic technologies in the Brazilian criminal justice system

Thallita Gabriele Lopes Lima[1]
Pontifícia Universidade Católica do Rio de Janeiro, PUC-Rio, Brasil.
thallita.gabriele@gmail.com

DOI: [doi.org/10.5281/zenodo.17058344].

Área do Direito: Penal; Digital

Resumo: O uso de tecnologias de reconhecimento facial (TRFs) no campo da segurança pública tem suscitado importantes debates sobre os limites entre uso de tecnologias algorítmicas, legalidade e proteção de direitos fundamentais. Este artigo examina o caso da *Clearview AI* – empresa norte-americana que desenvolveu um sistema de TRF baseado na raspagem massiva de imagens extraídas da *internet* – como ponto de partida para refletir sobre os modos de circulação,

Abstract: Facial recognition technologies (FRT) in public security have sparked important debates about the boundaries between using algorithmic technologies, legality, and protecting fundamental rights. This article examines the case of *Clearview AI* – a US company that developed an FRT system based on the massive scraping of images extracted from the internet–as a starting point for reflecting on the circulation, appropriation, and contestation modes of these technologies in

1. Doutora em Relações Internacionais pela Pontifícia Universidade Católica do Rio de Janeiro, possui mestrado pela mesma instituição e graduação em Relações Internacionais pela Universidade Federal Rural do Rio de Janeiro. Coordenadora de pesquisa do projeto O Panóptico do Centro de Estudos de Segurança e Cidadania (CESeC).
Currículo Lattes: [http://lattes.cnpq.br/4467147688792014].
ORCID: [https://orcid.org/0000-0003-3488-349X].
E-mail: thallita.gabriele@gmail.com

apropriação e contestação dessas tecnologias em regimes jurídicos assimétricos. Interroga-se como esse modelo de coleta e uso de dados desafia garantias processuais e tensiona princípios constitucionais como a legalidade da prova, o contraditório e a proteção de dados pessoais. A análise articula o caso *Clearview* às dinâmicas brasileiras de implementação de TRFs, marcadas por informalidade institucional, fragmentação normativa e seletividade penal estrutural. Metodologicamente, combina-se revisão crítica da literatura, análise documental (registros obtidos via LAI, normativas e materiais institucionais) e observação em eventos setoriais. A partir de uma abordagem ancorada nos Estudos de Ciência e Tecnologia (STS) e na criminologia crítica, argumenta-se que infraestruturas sociotécnicas emergentes estão reconfigurando práticas de policiamento e racionalidades probatórias, com impactos diretos na produção da verdade judicial e na distribuição desigual de incertezas e vulnerabilidades no sistema de justiça criminal.

Palavras-chave: Reconhecimento facial – Dados pessoais – *Clearview AI* – Tecnologias de vigilância – Justiça criminal.

asymmetric legal regimes. It examines how this data collection and use model challenges procedural guarantees and undermines constitutional principles such as the legality of evidence, adversarial proceedings, and the protection of personal data. The analysis links the *Clearview* case to the Brazilian dynamics of implementing FRTs, marked by institutional informality, normative fragmentation, and structural criminal selectivity. Methodologically, it combines a critical review of the literature, documentary analysis (records obtained via the Access to Information Act, regulations, and institutional materials), and observation of sectoral events. Based on an approach anchored in Science and Technology Studies (STS) and critical criminology, it is argued that emerging sociotechnical infrastructures are reconfiguring policing practices and evidentiary rationalities, with direct impacts on the production of judicial truth and the unequal distribution of uncertainties and vulnerabilities in the criminal justice system.

Keywords: Facial recognition – Personal data – Clearview AI – Surveillance technologies – Criminal justice.

Sumário: 1. Introdução. 2. Da raspagem ao reconhecimento: descompactando a *Clearview AI* como infraestrutura algorítmica de vigilância. 3. Expansão, controvérsias e ambiguidades regulatórias: localizando o Brasil na circulação de TRF. 4. Entre rostos e rastros: *Clearview AI* e os limites do devido processo legal no Brasil. 5. Conclusão. Referências. Legislação.

1. Introdução

O[2] avanço das tecnologias de inteligência artificial (IA) de algoritmos de aprendizado de máquina tem gerado transformações nos regimes contemporâneos de segurança pública e da justiça criminal. Ancoradas em promessas de maior previsibilidade, agilidade e objetividade, essas tecnologias vêm sendo incorporadas por

2. A frase *Faces make cases*, em destaque no título deste trabalho, foi utilizada na estratégia de *marketing* da empresa no painel da ISC Brasil 2022 e está presente nas apresentações realizadas ao Ministério da Justiça e Segurança Pública pela Secretaria Nacional de Segurança Pública adquiridas via Lei de Acesso à Informação. Processo 08198.023803/2022-21.

diferentes setores do Estado sob justificativas da modernização institucional, ganho de eficiência e do enfrentamento à criminalidade. Sua aplicação envolve desde sistemas preditivos e bases de dados interoperáveis até sensores biométricos e *softwares* de reconhecimento facial. Pelo menos 75 dos 176 países em todo o mundo utilizam ativamente tecnologias algorítmicas para fins de segurança e vigilância (Feldstein, 2019).

Nesse mesmo cenário, nos últimos anos, a implementação de tecnologias de reconhecimento facial (TRFs) para fins de segurança tem sido apresentada no discurso público como uma promessa e uma oportunidade para otimizar a gestão da segurança (Ferguson, 2017). Essas tecnologias são frequentemente descritas como ferramentas fundamentais para aumentar a eficiência das investigações criminais e fortalecer a segurança pública. As TRFs podem identificar e autenticar as identidades das pessoas detectando, capturando e combinando rostos com imagens de um banco de dados, e são compreendidas como uma "solução" à necessidade crescente de identificação contemporânea (Lyon, 2008, p. 500). Sob a lógica tecnopolítica algorítmica, TRF prometem identificar suspeitos, correlacionar informações de maneira precisa, objetiva e rápida (Lyon, 2008).

Segundo Bichoff (2021), 70% das forças policiais do mundo têm acesso a algum tipo de TRF, e 60% dos países já a utilizam em aeroportos. Essas tecnologias têm sido empregadas em operações de policiamento para identificar suspeitos ou localizar pessoas desaparecidas, além de servirem como ferramentas para verificação de identidade, investigação, categorização e análise estatística (Lyon, 2008). No entanto, o funcionamento dessas tecnologias levanta questões críticas e debates na sociedade civil, envolvendo falhas operacionais e técnicas (Lima, 2024), falta de transparência e ausência de *accountability* (Lima et al., 2024, p. 10), os impactos sob os direitos fundamentais (Nunes; Lima; Cruz, 2023) – em especial, o direito à privacidade, à proteção de dados pessoais e às garantias processuais –, bem como a forma como essas tecnologias podem reforçar padrões discriminatórios e dinâmicas de violência marcadas por raça, classe, nacionalidade e gênero (Amoore, 2020; Buolamwini; Gebru, 2018).

Apesar das críticas e controvérsias, as TRFs têm sido promovidas por um discurso de inovação tecnológica no combate ao crime. Essas ferramentas operam com base em dados biométricos, algoritmos e grandes volumes de imagens, muitas vezes coletadas em plataformas públicas, sem consentimento dos titulares dos dados. Entre essas tecnologias, a *Clearview AI* se destaca como um caso paradigmático, tanto pela radicalidade de seu método de coleta (raspagem de dados públicos da *internet*) quanto pelas controvérsias éticas, jurídicas e políticas que sua atuação vem gerando em diferentes países. Nesse sentido, este artigo examina o caso da utilização do *software* da empresa norte-americana *Clearview AI*, que se enquadra em

uma tendência global de aumento na demanda pela reutilização de dados coletados pelo setor privado para fins de segurança (Ferguson, 2017), por vezes, de modo a permitir que governos contornem salvaguardas legais em torno do acesso da aplicação da lei ao comércio de bases de dados (Brayne, 2017; Brayne; Christin, 2021; Crawford, 2021).

Fundada em 2017 nos Estados Unidos, a *Clearview AI* desenvolveu uma TRF baseada em um banco de dados que ultrapassa 50 bilhões de imagens, extraídas de redes sociais, *sites* de notícias, *blogs*, portais governamentais e outras fontes públicas[3]. Sem firmar acordos com as plataformas e sem solicitar autorização dos usuários. Assim, bastaria uma imagem – captada por câmeras de segurança, celulares ou redes sociais – para que o algoritmo cruzasse com seu repositório e devolvesse uma lista de rostos semelhantes, associando a eles nomes, perfis em redes e outras informações pessoais.

A atuação do algoritmo da *Clearview AI* expõe, de maneira aguda, os limites da regulação contemporânea diante da circulação global de dados biométricos, os riscos da centralização privada de tecnologias sensíveis e os desafios que essas ferramentas impõem aos fundamentos do processo penal, especialmente no que diz respeito à legalidade da prova, à proteção de dados sensíveis e à preservação das garantias fundamentais do contraditório e da ampla defesa. Portanto, partimos, das seguintes perguntas: como o modelo de raspagem de dados e uso da *Clearview AI* por órgãos públicos desafia e flexibiliza garantias processuais e direitos fundamentais no campo penal? Que riscos institucionais e políticos estão em jogo quando tais tecnologias operam em contextos marcados por seletividade penal, desigualdade estrutural e baixa capacidade regulatória?

A fim de explorar criticamente os dilemas levantados, o artigo se estrutura em três eixos analíticos interdependentes. A primeira seção examina o funcionamento técnico e o repertório discursivo da *Clearview AI*, com foco em seu modelo de negócios, na construção de uma suposta neutralidade algorítmica, ancorada em uma disputa técnica e na promessa de eficiência investigativa. Na segunda seção, o foco recai sobre o contexto brasileiro e sua inserção na expansão global das TRFs, evidenciando como a ausência de um marco regulatório específico, aliada à fragmentação das políticas de segurança pública, favorece a experimentação institucional desregulada dessas tecnologias. Mostra-se como a difusão descentralizada das TRFs contribui para consolidar um contexto de plasticidade de implantação, flexibilização dos direitos fundamentais e pouca transparência e responsabilização enquanto política pública.

3. CLEARVIEW AI. *Plataforma de reconhecimento facial para segurança pública e investigações*. Disponível em: [www.clearview.ai/]. Acesso em: 30.05.2025.

A terceira seção investiga a trajetória da *Clearview AI* no Brasil, reconstruindo os caminhos formais e informais de sua inserção nos órgãos de segurança e justiça. Essa dimensão da análise tem como ponto nodal a forma como essas tecnologias circulam e se legitimam no campo da segurança pública brasileira, a partir de um emaranhado entre agentes policiais, operadores do direito, fornecedores privados e estruturas administrativas. Com base na análise dos contratos, reuniões técnicas e testes não supervisionados, argumenta-se que a circulação dessa tecnologia cria desafios significativos e condições de possibilidade que comprometem garantias fundamentais, afetando diretamente o regime de produção de prova, especialmente no que diz respeito à cadeia de custódia digital, à opacidade do funcionamento algorítmico e à reconfiguração da figura do suspeito no processo penal.

O artigo se baseia em análise documental e bibliográfica, examinando relatórios públicos, registros obtidos via Lei de Acesso à Informação (LAI), documentos institucionais da *Clearview AI*, materiais jornalísticos e normativos. Foram também analisadas transcrições de entrevistas públicas concedidas por representantes da empresa em veículos de mídia e conferências abertas, acessadas por meio de fontes institucionais e plataformas digitais. A pesquisa também contou com duas participações em feiras de tecnologias de segurança no Brasil nas quais a empresa norte-americana foi expositora: a ISC Brasil 2022[4] e a LAAD Defense & Security 2023[5].

A abordagem teórica adotada é crítica e interdisciplinar, ancorada nos Estudos de Ciência e Tecnologia (STS, na sigla em inglês) e na criminologia crítica. Combinando aportes de diferentes campos e autoras/es, buscamos evidenciar como a materialidade técnica das TRFs contribui para a construção de verdades criminais, a consolidação de formas específicas de policiamento, e os efeitos que isso pode produzir em termos violências, distribuição desigual de insegurança e flexibilização de direitos fundamentais. Cabe pontuar que não é o objetivo deste trabalho se concentrar em realizar uma análise jurídica, mas sim, alinhando-se aos estudos da STS e compondo com a crítica feminista a tecnociência, explorar as implicações nas

4. A ISC Brasil é a edição brasileira da marca ISC Security Events – International Security Conference & Exhibitions. A feira foi realizada entre 21 de setembro de 2022 e 23 de setembro de 2022 no Expo Center Norte, em São Paulo. Disponível em: [www.iscbrasil.com.br/pt-br/o-evento.html]. Acesso em: 14.03.2025.
5. A LAAD Defense & Security (Feira Internacional de Defesa e Segurança), aconteceu entre os dias 11 e 14 de abril de 2023 no Rio de Janeiro. Essa é considerada a maior e mais importante feira de defesa e segurança da América Latina e reúne fabricantes e fornecedores de armas e tecnologias para as Forças Armadas, Polícias, Forças Especiais; militares das Forças Armadas, forças policiais e autoridades governamentais, além de expositores diversos. Disponível em: [www.laadexpo.com.br/]. Acesso em: 11.03.2025.

matérias discursivas[6] do modo algorítmico de produção de verdade e sua admissibilidade no aparato de justiça criminal.

2. Da raspagem ao reconhecimento: descompactando a *Clearview AI* como infraestrutura algorítmica de vigilância

A *Clearview AI* é uma empresa norte-americana fundada em 2017 por Ton-That e Richard Schwartz,[7] com apoio financeiro de investidores como Peter Thiel (também investidor da Meta e dono da empresa de tecnologia de segurança Palantir) e do fundo de investimento Kirenaga Partners. A empresa atua no ecossistema de TRFs algorítmicas, que vêm se tornando tanto ignição para práticas operacionais dos agentes de segurança (de policiais a militares) quando suporte para a produção de evidências no contexto do processo probatório penal (Lima, 2024, p. 55). As TRFs não apenas impulsionam práticas policiais, mas também reconfiguram os fundamentos da justiça criminal, ao desestabilizarem os limites entre vigilância, identificação e produção de prova, frequentemente à revelia de garantias constitucionais como o devido processo legal, o direito à privacidade e à proteção de dados pessoais.

A promessa de construção de "um mundo mais seguro a partir do uso de IA"[8], é apresentada pela *Clearview AI* em seu *site* e em suas redes sociais. Logo na primeira página de seu *site* oficial, a empresa afirma que sua missão é "simples e impactante": reduzir drasticamente o crime e tornar as comunidades mais seguras. Essa promessa, no entanto, está longe de ser simples como se apresenta, e oferecer uma ferramenta única capaz de torná-la possível é, no mínimo atraente. Como temos observado neste trabalho, o uso de tecnologias tem sido mobilizado por um discurso que as apresenta como soluções eficientes diante da incerteza que caracteriza problemas persistentes de segurança.

A empresa norte-americana ganhou notoriedade pública em janeiro de 2020, quando o *New York Times* publicou a reportagem intitulada "The Secretive

6. Conforme proposto por Karen Barad (2007), o termo material-discursivo expressa a inseparabilidade entre matéria e significação, indicando que os fenômenos não são dados previamente, mas emergem por meio de intra-ações entre elementos humanos e não humanos. Em sua perspectiva ontoepistemológica, práticas discursivas não apenas interpretam o mundo, mas o produzem materialmente, de modo que o social e o técnico, o jurídico e o algorítmico, não podem ser analisados separadamente.
7. Assessor de Rudolph W. Giuliani quando ele foi prefeito de Nova York.
8. CLEARVIEW AI. *Plataforma de reconhecimento facial para segurança pública e investigações*. Disponível em: [www.clearview.ai/]. Acesso em: 30.05.2025.

Company That Might End Privacy as We Know It" (A empresa secreta que pode acabar com a privacidade como a conhecemos) (Hill, 2020). Até então, a *Clearview* operava deliberadamente de forma discreta, oferecendo a sua TRF a agências de segurança pública e empresas privadas em diversos países, sem grande exposição midiática ou escrutínio público. A matéria lançou luz não apenas sobre a empresa, mas sobre o seu modelo de negócios: um sistema baseado não só em um algoritmo de correspondência facial, mas na raspagem massiva de imagens de fontes públicas e na oferta do serviço diretamente a instituições policiais e de segurança. Àquela altura, mais de 600 agências policiais nos Estados Unidos já utilizavam a ferramenta – número que, segundo documentos, poderia ultrapassar 2.900 organizações, incluindo o FBI, o Serviço Secreto, a Interpol, a agência de imigração dos EUA e corporações de segurança privada (Haskins; Mac; McDonald, 2020).

O rápido crescimento e a penetração institucional da *Clearview* não passaram despercebidos: apenas dezoito meses após a publicação da matéria investigativa, a empresa foi listada pela revista *Time* como uma das "100 empresas mais influentes do mundo" (*Clearview AI* named [...], 2021), apresentando-se como detentora da "maior rede de biometria facial do planeta" (Hill, 2020). A capacidade de raspar, capturar e indexar rostos públicos em escala global, aliada à oferta direta a autoridades de segurança, transformou a *Clearview* em um caso emblemático das novas formas de vigilância privada com implicações públicas – um modelo que opera nas fronteiras entre o legal e o extralegal, entre o visível e o opaco, entre a inovação e a erosão de direitos fundamentais.

A ferramenta da *Clearview AI* se diferencia de outras TRFs por dois elementos fundamentais: (i) o método de construção de seu banco de dados; e (ii) e a capacidade de seu algoritmo. O algoritmo da *Clearview* pode escanear mais de um bilhão de rostos em menos de um segundo[9], e a empresa afirma que a ferramenta é precisa "todas as demográficas"[10], ancorando essa alegação em uma patente que sua capacidade de criar algoritmos de reconhecimento facial precisos e "sem viés", a partir de informações publicamente disponíveis[11]. Em seu *site* oficial e no material distribuído na Laad 2023, no Rio de Janeiro, a empresa enfatiza um discurso de superioridade técnica, apresentando seu algoritmo como: "sem preconceitos", "assertivo", "preciso", "fidedigno" e "uma solução única e abrangente para inteligência e investigações, disponível no mercado mundial".

9. Apresentação da última versão do *Clearview* 2.0 ao Copaq/Senasp, via Lei de Acesso Informação.
10. Disponível: [www.clearview.ai/]. Acesso em: 15.03.2025.
11. Disponível em: [www.clearview.ai/patentes]. Acesso em: 15.06.2024.

O discurso da empresa busca neutralizar críticas recorrentes dirigidas às TRFs no contexto da segurança pública, especialmente no que se refere à baixa acurácia e aos vieses algorítmicos. Questões relacionadas a vieses demográficos, raciais e de gênero têm sido amplamente destacadas em propostas de moratórias e proibições do uso dessas tecnologias, geralmente associadas a preocupações com a proteção de direitos fundamentais, como o direito à privacidade (Lima, 2024, p. 62). A empresa, por sua vez, tenta reforçar a confiabilidade, precisão e alegada neutralidade de seu algoritmo, ao mesmo tempo em que enfrenta críticas relacionadas ao banco de dados que sustenta sua operação. No conjunto de documentos analisados nesta pesquisa, os algoritmos da *Clearview AI* são descritos como mais objetivos e eficientes do que o julgamento discricionário humano. A "alta eficiência" em problemas complexos e variados tem tornado a *Clearview* atraente, mas isso não implica que a ferramenta esteja livre de erros e vieses operacionais (Lima, 2024, p. 22).

Embora os recursos do seu algoritmo sejam descritos como "diferente de qualquer coisa já produzida" – uma afirmação respaldada por patentes –, o que de fato diferencia a empresa é o seu método de treinamento e coleta de imagens faciais. Ao invés de operar com bases de dados estatais, como registros criminais, arquivos de identidade civil ou cadastros governamentais, *Clearview* desenvolveu um algoritmo capaz de rastrear e indexar bilhões de imagens disponíveis na internet pública. Essa técnica, conhecida como raspagem de dados (*data scraping*), consiste na extração automatizada de conteúdo, como imagens, nomes e metadados, diretamente de redes sociais, *sites* jornalísticos e outras fontes digitais.

Dessa forma, quer tenhamos consentido ou não, nossos rostos aparecem nas fotos que, em muitos casos, acabam se tornando dados de treinamento e integrado a base de dados da empresa. É importante destacar que muitos de nossos dados estão publicamente disponíveis gratuitamente para serem utilizados quando os postamos *online*, sem as salvaguardas típicas encontradas em infraestruturas físicas. Isso torna profundamente difícil até mesmo discernir quem está usando e para quais finalidades. Esse é o principal diferencial da *Clearview*, e o fator de maior controvérsia. Essa prática tem provocado reações contundentes de defensores dos direitos humanos, pesquisadores e órgãos reguladores de proteção de dados (McSorley, 2021; Rezende, 2021). Tanto a forma de processamento dessas imagens quanto a comercialização da ferramenta têm sido duramente questionadas, sobretudo por comprometerem a privacidade dos indivíduos retratados e por impactarem diretamente as plataformas digitais de onde essas imagens são extraídas.

Em uma audiência de prospecção da empresa junto ao Ministério da Justiça e Segurança Pública (MJSP) do Brasil realizada no dia 09 de fevereiro de 2022 pela Copaq – uma comissão composta por representantes de cada uma das unidades e setores da Secretaria Nacional de Segurança Pública (Senasp) –, da qual tivemos

acesso por meio da Lei de Acesso à Informação[12], o representante comercial da empresa reafirma que "o grande objetivo" da *Clearview AI* é ampliar continuamente sua base de dados. Segundo Lima (2024, p. 85), o que o algoritmo de *Clearview* é capaz de fazer – e sua eficácia – depende diretamente do tamanho e da diversidade da sua base de dados, não apenas para gerar resultados mais específicos nas buscas realizadas por agentes de segurança, mas também para alimentar e refinar o próprio modelo algorítmico.

Por isso, a comparação da tecnologia da *Clearview AI* com o Google é recorrente. Das quinze entrevistas publicamente disponíveis em vídeo ou em áudio utilizadas nesta pesquisa, em seis delas o *CEO* Ton-That explica a sua tecnologia como uma ferramenta de busca, como a Google, mas voltada para rostos, destinada às forças de segurança. A analogia com um dos buscadores de *internet* mais populares do mundo não acontece aleatoriamente. Trata-se de uma estratégia de apresentar a ferramenta da empresa como poderosa e "disruptiva" (como reforçado no material de *marketing*) e, ao mesmo tempo, fácil de compreender utilizar e aparentemente alinhada à legislação vigente, que não enfrenta grandes críticas quanto à metodologia de extração de dados públicos da *internet* indexadas pela Google.

Apesar da tecnologia da *Clearview* ser protegida por sigilo corporativo e seu método estar atualmente resguardado por patentes – enquanto propriedade intelectual –, é importante destacar como os dados públicos, o acesso livre à informação, são centrais tanto para a formação do seu banco de dados quanto para a circulação de conhecimento técnico que possibilitou o desenvolvimento de seu algoritmo e suas inovações no campo do reconhecimento facial. Segundo Thylstrup (2019), a reutilização de dados públicos está profundamente interligada à forma como os algoritmos são recalibrados, reempacotados e reaproveitados. No caso da *Clearview AI*, a análise de seu desenvolvimento técnico permite identificar a incorporação de recursos originalmente disponíveis em *softwares* livres como parte da base metodológica de seu sistema proprietário. Isso evidencia como tecnologias tidas como inovadoras frequentemente se constroem a partir de camadas de conhecimento

12. Essa comissão foi criada em 2019 para instituir parcerias entre empresas ou instituições públicas e privadas com o objetivo de inovações, soluções tecnológicas e boas práticas, para a promoção e fomentação da modernização e reaparelhamento dos órgãos de segurança pública. As reuniões do Copaq do Ministério da Justiça é um meio de apresentação da empresa a diversos órgãos, isso porque a audiência de apresentação é aberta a todos os órgãos que tenham interesse. Contudo, o teste, o modo e a aquisição dos contratos não precisam ser intermediados pelo governo federal. Ou seja, a aquisição ocorre de forma autônoma em cada agência, sem nenhuma forma de padronização e regulação (BRASIL. Ministério da Justiça e Segurança Pública. Processo 08198.023803/2022-21. *Pedido de acesso à informação com base na Lei 12.527, de 18 de novembro de 2011*. Brasília, 2022).

aberto, cuja origem é posteriormente encoberta por patentes e estratégias comerciais[13]. A linguagem das patentes, como argumenta Katz (2020, p. 14), reforça uma reivindicação de conhecimento, produz uma métrica de inovação "e deixa a porta aberta a uma cascata de novas utilizações". Atualmente, a empresa possui três patentes.

Essa retórica de inovação técnica é acompanhada por esforços legais e institucionais de legitimação. O banco da *Clearview* ultrapassa 50 bilhões de imagens e, segundo declarações de seus representantes, a empresa pretende atingir a marca de 100 bilhões em poucos anos (Lima, 2024). Embora o volume, por si só, já seja expressivo, o que torna essa base especialmente controversa é o fato de incluir imagens de pessoas que jamais tiveram qualquer interação com o sistema de justiça – ou mesmo conhecimento de que suas fotos estavam sendo utilizadas em contextos de investigação criminal.

Essa transformação do rosto público em dado policial produz uma ambiguidade fundamental: se, por um lado, as imagens foram disponibilizadas voluntariamente pelos usuários em redes sociais, por outro, a recontextualização dessas imagens em um algoritmo biométrico destinado à segurança pública altera completamente sua finalidade e seus efeitos. Essa transição – do rosto ao dado, do dado à identidade, da identidade à prova – é central para entender como tecnologias como a *Clearview* reconfiguram as fronteiras entre o que é considerado informação pública, evidência penal e material de vigilância.

Os dados biométricos capturados e organizados por sistemas como o da *Clearview* não são meramente coletados: eles são produzidos, performados e transformados por uma série de decisões sociotécnicas. Barad (2007) argumenta que fenômenos científicos e tecnológicos não existem de forma autônoma, mas emergem por meio de intra-ações – relações dinâmicas entre sujeitos, objetos, instituições e dispositivos. O dado não é neutro: carrega consigo a marca do contexto em que foi produzido, extraído e reclassificado. O rosto capturado de uma *selfie*, de um vídeo de protesto ou de uma rede social passa a ser mobilizado em outro campo de significado – o da vigilância e da investigação penal – e adquire, nesse processo, um novo estatuto jurídico e político.

Essa reclassificação, além de técnica, é profundamente epistêmica. Como aponta Seaver (2017), os algoritmos são entidades moldáveis, que respondem a incentivos institucionais, culturais e comerciais. O algoritmo da empresa não opera isoladamente, mas está imerso em uma cadeia de significações que vai desde o

13. Para uma análise mais detalhada sobre o processo de desenvolvimento técnico da *Clearview AI* e sua articulação com *softwares* livres, ver Lima (2024).

design do *software* até os contextos institucionais em que seus resultados são interpretados. O sistema responde à demanda por "eficiência" policial, à pressão por inovações rápidas no setor de segurança e à lógica comercial da vigilância como serviço. Sua autoridade é construída pela fusão entre promessa técnica, infraestrutura privada e delegação institucional.

Nesse sentido, o banco de dados da *Clearview AI* não é apenas um repositório: trata-se também de um aparato de inscrição algorítmica de identidades e reconhecimento, capaz de gerar pistas investigativas a alimentar decisões judiciais. Como demonstrado em diversos estudos (Amoore, 2020; Aradau; Blake, 2021; Lima, 2024; Nunes; Lima; Cruz, 2023), as TRFs operam como um filtro técnico de suspeição, reorganizando as relações entre aparência, identidade e culpabilidade. O risco de erro – amplamente documentado para mulheres, pessoas trans e negras (Buolamwini; Gebru, 2018) – é frequentemente naturalizado por discursos que exaltam a eficiência do algoritmo e minimizam os efeitos políticos e sociais de sua adoção.

As controvérsias em torno da *Clearview AI* emergem justamente da desnaturalização dessa cadeia de produção algorítmica. Embora, a empresa esteja enfrentando um escrutínio cada vez maior, em especial com relação a políticas de segurança dos dados e a privacidade, também há um crescente apoio às políticas de compartilhamento de informações pessoais em nome da segurança. Em fevereiro de 2020, a estratégia da empresa passou a focar seus investimentos nos mercados dos Estados Unidos e no Canadá, mas seguiu promovendo sua ferramenta globalmente por meio de oferta de testes gratuitos para agentes de segurança de diversos países europeus e do "Sul Global", em especial América Latina, com participação ativa em conferências policiais e feiras de segurança (Mac; Haskins; Pequeno, 2021). Nos Estados Unidos, a empresa registrou uma ampliação dos picos de utilização e requerimento de testes após o seu *software* ter sido uma ferramenta "essencial" para o reconhecimento dos invasores do Capitólio no dia 06 de janeiro de 2021 (Hill, 2021).

Como observado, dos debates públicos sobre a *Clearview AI* frequentemente reproduz a dicotomia entre privacidade e segurança, como se estivesse em jogo um suposto equilíbrio entre garantir direitos individuais e promover proteção coletiva, uma tensão que tem marcado os debates públicos convencionais sobre tecnologias de vigilância (Bauman et al., 2015). Contudo, é fundamental refletir sobre os limites dessa oposição simplificadora e insuficiente para compreender as implicações reais dessas tecnologias. Em primeiro lugar, porque sugere que a privacidade seria um obstáculo à segurança, quando, na verdade, são justamente os limites jurídicos e políticos ao uso arbitrário de dados que garantem formas legítimas de proteção coletiva. Em segundo lugar, porque essa dicotomia oculta as camadas sociotécnicas e institucionais que estruturam a produção, a circulação e o uso desses dados.

No caso da *Clearview*, os rostos são extraídos de imagens postadas voluntariamente em redes sociais, convertidos em dados biométricos sem consentimento e reorganizados em um sistema de busca policial, um processo que altera profundamente sua natureza, função e efeitos. O que está em jogo, portanto, não é apenas uma disputa entre dois valores abstratos (privacidade *versus* segurança), mas a constituição de uma nova ecologia sociotécnica na qual a coleta, o processamento e o uso dos dados escapam aos marcos tradicionais de regulação e controle.

Em 2020, a União Americana pelas Liberdades Civis (sigla em inglês, ACLU) processou a *Clearview* por violar a Lei de Privacidade de Informações Biométricas (Bipa), de Illinois, uma lei estadual que proíbe a captura de identificadores biométricos de indivíduos, como rosto e impressões digitais, sem aviso prévio e consentimento. Em decorrência desse processo, a empresa foi impedida de vender a ferramenta a empresas privadas (*Clearview AI* Settles [...], 2022). Ademais, os órgãos reguladores de diversos países europeus baniram o uso da ferramenta sob a avaliação de que a Lei Geral de Proteção de Dados europeu (GDPR) (Ramage, 2022) exige consentimento explícito para o processamento de dados pessoais sensíveis (Rezende, 2020). Além disso, a Austrália e o Reino Unido acusaram a empresa de violar suas leis de privacidade e proteção de dados, e o Escritório do Comissário de Privacidade do Canadá segue investigando as atividades da empresa no Canadá (McSorley, 2021).

Apesar dessas ações, a circulação da ferramenta não foi interrompida. Alguns especialistas em privacidade descrevessem que o acordo entre a ACLU e a *Clearview AI* como um "divisor de águas" para avanço da proteção de dados e privacidade, e o banimento em países europeus como um "fechar de portas". No entanto, esses litígios não estancaram nem paralisaram a circulação e uso da tecnologia, que continuou a se expandir e ser remodelada em novos contextos, como na guerra da Ucrânia, onde foi empregada para identificação de corpos e reconhecimento em zonas de conflito (Lima, 2024).

É justamente nesse contexto que o sistema da *Clearview* deixa de ser apenas uma ferramenta técnica e se configura um ator político, com efeitos concretos sobre as práticas de segurança e direitos fundamentais. Ao fornecer resultados que vinculam rostos a perfis, redes e identidades, o algoritmo participa da construção de suspeitas, fundamenta decisões investigativas e pode influenciar a formação da prova. A opacidade do funcionamento do sistema, com códigos proprietários, segredos comerciais e ausência de auditoria externa, dificulta o exercício do contraditório, da ampla defesa e da contestação técnica.

Segundo Press (2023), uma questão importante é que o uso de TRFs tem levado os profissionais de segurança a desconsiderarem outros elementos relevantes dos casos. O resultado gerado pelo algoritmo tem sido representado uma evidência

contundente, adquirindo o status de "verdade técnica" (Amoore, 2020), o que por sua vez, dificulta a contestação. A evidência algorítmica passa a operar como um filtro de validação, estreitando o campo do contraditório corroendo os fundamentos do direito de defesa e do devido processo legal. Quando o julgamento da culpa se ancora na racionalidade algorítmica probabilística e em um emaranhado de diferentes práticas difusas dos operadores dessas ferramentas, a autoridade deriva não de sua transparência ou objetividade técnica, mas sim da legitimidade institucional e da credibilidade que o sistema ao ser incorporado aos circuitos policiais e judiciais.

Ao reduzir a distância entre o que é captado no cotidiano digital e o que é considerado elemento de ignição para ações penais, o uso de tecnologias como a *Clearview AI* representa uma mudança profunda na arquitetura da justiça criminal. Sua atuação desafia os limites entre o público e o privado, entre o dado e o direito, entre a imagem e a imputação penal. Mais do que uma tecnologia emergente, a *Clearview* encarna uma nova gramática da vigilância, na qual ver, reconhecer e rastrear se tornam operações contínuas, automatizadas e privatizadas.

3. Expansão, controvérsias e ambiguidades regulatórias: localizando o Brasil na circulação de TRF

Se na seção anterior observamos como sistemas como o da *Clearview AI* tensionam os limites entre o público e o privado, o legal e o extralegal. É no contexto brasileiro que essas tensões assumem contornos ainda mais complexos e opacos. Aqui, a circulação e normalização das TRFs operam por meio de mecanismos institucionais que mesclam inovação tecnológica, improvisação normativa, fragmentação burocrática-administrativa e opacidade operacional. Esse quebra-cabeça constitui um campo fértil para que tecnologias de segurança sejam experimentadas, testadas e, em alguns casos, utilizadas informalmente por agentes públicos – sem contratos formais, sem controle social e à margem dos marcos legais de contratação e transparência.

A ausência de uma política nacional sobre o uso dessas tecnologias, somada à falta de transparência na sua implementação e aos labirintos burocráticos que dificultam o acesso à informação, tem contribuído para a consolidação de um ecossistema no qual diferentes entes federativos adotam soluções tecnológicas com lógicas, fornecedores e critérios próprios. Movidos por uma agenda de modernização policial e por promessas de eficiência na identificação de suspeitos, governos estaduais e municipais passaram a investir em projetos-piloto, contratos diretos com empresas de tecnologia e parcerias informais com fornecedores privados. Nesse ambiente, projetos de TRFs s são implementados, testados e difundidos com

agilidade, ao passo que os marcos legais e institucionais que deveriam lhes dar sustentação permanecem ausentes ou em disputa.

Ao analisar como o Brasil se insere na circulação transnacional de TRF, esta seção examina os processos de institucionalização informal, os riscos da vigilância automatizada e os efeitos jurídicos, políticos e sociais da ausência de regulação específica, com especial atenção aos impactos sobre os direitos fundamentais e ao descompasso entre a promessa tecnológica e as garantias processuais. Trata-se, portanto, de compreender como o país tem construído aderência a essas tecnologias e de que maneira isso tem contribuído para a reconfiguração dos regimes de segurança pública.

No Brasil, todos os estados já utilizam ou estão em fase de testes de TRFs. Observa-se um aumento expressivo nos investimentos direcionados ao uso de tecnologias algorítmicas para segurança e vigilância, com destaque para essas ferramentas biométricas. Esse movimento tem seu início nos anos 2010 com os grandes eventos (como as Olimpíadas, Copa do Mundo e a Jornada Mundial da Juventude) (Lima et al., 2024). Apesar de uma certa desmobilização dos projetos após os eventos, tornou-se especialmente popular em 2019 (Nunes; Lima; Cruz, 2023, p. 8). Esse novo ciclo de adesão teve como catalizador a Portaria 793, de 24 outubro de 2019, que regulamenta a aplicação de recursos do Fundo Nacional de Segurança Pública para fomentar a implantação desses sistemas. Segundo a normativa, esses sistemas enquadram-se no conjunto de medidas para redução e controle da violência e da criminalidade. Esse incentivo, contudo, não foi acompanhado da criação de instâncias de controle, de mecanismos de avaliação de impactos ou de canais de participação social.

Essa expansão se dá em meio a um cenário de insegurança pública e violência, pressão por respostas rápidas por parte de gestores e crescente influência do "tecnosolucionismo" (Morozov, 2013) – a crença de que problemas complexos como a criminalidade podem ser resolvidos por meio de inovações tecnológicas. O discurso político em torno dessas ferramentas tende a enfatizar sua capacidade de otimizar o policiamento, reduzir custos operacionais e ampliar a eficiência das ações de segurança.

A ausência de normas unificadas e regulamentação sobre o uso de TRFs propiciou à proliferação de sistemas distintos em operação nos entes federativos, com objetivos, fornecedores e métodos variados. Na prática, observa-se a expansão e dispersão de projetos em todo o país sem a regulamentação adequada, padronização tecnológica ou adoção de mecanismos de publicidade, transparência e avaliação do uso dessas tecnologias como política pública. Além disso, o tratamento de dados para a segurança pública por meio do TRFs é realizado sem salvaguardas mínimas diante dos riscos associados à tecnologia, a despeito da emenda à

Constituição da República, que incluiu a proteção de dados como direito fundamental autônomo[14], dos princípios da administração[15] e da regulação infraconstitucional aplicável[16].

Segundo dados do projeto Panóptico, do Centro de Estudos de Segurança e Cidadania (CESeC), existem 442 projetos que utilizam TRF em espaços públicos, e aproximadamente 82,3 milhões de brasileiros estão potencialmente sob vigilância por câmeras com essa tecnologia[17]. A implementação dessa tecnologia tem avançado sem que haja garantias mínimas de proteção dos direitos fundamentais, tornando os espaços públicos, festas culturais e ambientes esportivos verdadeiros laboratórios de experimentação e coleta massiva de dados biométricos, incluindo crianças e adolescentes (Sousa et al., 2024).

A difusão dos projetos de segurança pública gera preocupações quanto a um possível cenário de desresponsabilização institucional, decorrente da adoção fragmentada dessas tecnologias sem a existência de diretrizes ou regulamentações mínimas. Cabe a cada ente federativo decidir autonomamente sobre a tecnologia a ser utilizada, os *softwares* empregados, as empresas contratadas, os bancos de dados acessados, os critérios para análise de vídeo e os locais de implementação, entre outros fatores. Além disso, faltam regras claras sobre coleta, armazenamento, uso e descarte de dados biométricos, bem como sobre os direitos dos cidadãos eventualmente identificados, detidos ou monitorados por essas tecnologias.

Essa forma descentralizada e pouco transparente de adoção dos sistemas gera inúmeros desafios operacionais, jurídicos, éticos e sociais. Há uma diversidade de pesquisas que demonstram, na prática, a disseminação do uso de TRFs leva à vigilância massiva, indiscriminada e desproporcional dos cidadãos (Amoore, 2020; Lyon, 2008). São amplamente conhecidos os limites, falhas e erros envolvidos na adoção dessas ferramentas, incluindo padrões discriminatórios que afetam desigualmente determinados grupos sociais em função de marcadores de diferenças sociais (Benjamin, 2019; Browne, 2015; Silva, 2020). Diversos estudos demonstraram que a maioria dos erros de identificação registrados pelas polícias no Brasil envolvem pessoas negras, muitas vezes presas de forma indevida e submetidas a processos criminais com base em reconhecimento equivocado (Nunes et al., 2022). Segundo levantamento do projeto Panóptico, entre os casos documentados de erro

14. Art. 5º, inc. LXXIX, Constituição da República.
15. Art. 37, Constituição da República.
16. Por exemplo, a Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018, LGPD) e a Lei de Acesso à Informação (Lei 12.257/2011, LAI).
17. Disponível em: [www.opanoptico.com.br]. Acesso em: 25.082025.

de reconhecimento facial no País em 2019, mais de 90% envolviam homens negros (Rede de Observatórios da Segurança, 2019). Essas falhas, muitas vezes decorrentes do uso de imagens de baixa qualidade e bancos de dados desatualizados, agravam-se pela ausência de protocolos uniformes para validação das identificações, registro das operações e auditoria independente dos sistemas.

Esses casos expõem não apenas falhas técnicas, mas também um problema estrutural: a incorporação das TRFs em um sistema penal marcadamente seletivo e estruturalmente desigual (Flauzina, 2006). Assim, a produção sistemática de falsos positivos – os chamados "erros do sistema" – tem gerado diversas formas de constrangimento e violência, em geral, contra pessoas que já se encontram em condições de vulnerabilidade social (Nunes; Lima; Cruz, 2023). Isso é especialmente importante no contexto da segurança pública no Brasil, onde a suspensão dos direitos humanos é cotidiana na vida de grupos já marginalizados e frequentemente enquadrados como elementos de "desordem", como a população negra e periférica (Flauzina, 2006).

Ao revés de corrigirem esses problemas, os algoritmos tendem a reproduzi-los e amplificá-los, ao replicar padrões históricos de suspeição e incriminação com base em dados passados e vieses de classificação e suspeição. A promessa de neutralidade técnica, frequentemente mobilizada pelos fornecedores e operadores da TRFs, oculta o fato de que essas tecnologias são construídas sobre infraestruturas de desigualdade, tanto na coleta de dados quanto na maneira como os sistemas são operacionalizados no cotidiano das práticas policiais. A questão que se coloca não é apontar os erros e possíveis falhas das TRFs, mas entender como, apesar deles, essas tecnologias têm sido utilizadas criado condições de possibilidade de um modo específico de pensar e fazer práticas de identificação e reconhecimento de suspeitos (Lima, 2024, p. 10).

Do ponto de vista normativo, o Brasil possui um marco legal importante com a Lei Geral de Proteção de Dados Pessoais (LGPD – Lei 13.709/2018), que reconhece dados biométricos como sensíveis e estabelece princípios como finalidade, necessidade, transparência e segurança. A Emenda Constitucional 115/2022 elevou a proteção de dados pessoais à condição de direito fundamental. No entanto, ainda não há regulamentação específica para o uso de TRF por órgãos de segurança pública, um vácuo jurídico que permite interpretações diversas e usos muitas vezes arbitrários ou informalizados.

A situação se agrava diante da falta de diretrizes sobre como compatibilizar a proteção de dados com as necessidades de investigação criminal. O anteprojeto da chamada "LGPD Penal" (Projeto de Lei 1.515/2022) – elaborado por comissão de juristas e ainda em tramitação– tenta preencher essa lacuna ao propor regras específicas para o tratamento de dados pessoais para fins de segurança

pública, persecução penal, defesa nacional e segurança do Estado (Azevedo et al., 2022). Entre seus objetivos, estão a delimitação de finalidades, a definição de responsabilidades institucionais e a previsão de direitos e salvaguardas aos titulares dos dados.

No entanto, o projeto tem sido criticado por organizações da sociedade civil por apresentar uma estrutura excessivamente permissiva e vaga, permitindo ampla margem de discricionariedade às autoridades de segurança[18]. Um dos principais problemas identificados é a inversão do princípio da excepcionalidade: ao invés de impor limites rigorosos e salvaguardas à coleta e ao uso de dados sensíveis, o texto cria brechas que legitimam práticas invasivas sob a justificativa genérica de "interesse público". Além disso, o projeto falha em estabelecer mecanismos robustos de controle externo, auditoria independente e direito à contestação por parte dos titulares dos dados. Esse desenho normativo contrasta com marcos regulatórios internacionais mais protetivos, como o Regulamento Geral sobre a Proteção de Dados da União Europeia (GDPR), que impõe critérios mais restritivos ao uso de dados sensíveis em contextos de segurança. Assim, ainda que represente um esforço de normatização, o projeto evidencia os limites atuais para compatibilizar, na prática, as exigências da investigação penal com os princípios fundamentais da proteção de dados.

No campo judicial, o Conselho Nacional de Justiça (CNJ) tem discutido o uso de tecnologias digitais e sistemas de IA no Judiciário, inclusive com diretrizes sobre ética, transparência e *accountability*. Em março de 2025, o CNJ promulgou a Resolução 615, estabelecendo diretrizes para o uso de inteligência artificial no Poder Judiciário brasileiro (Brasil, 2025). Essa normativa proíbe expressamente o uso de sistemas de IA para prever crimes com base em características pessoais ou comportamentais, bem como a aplicação de TRFs para detecção de emoções, visando prevenir discriminações e violações de privacidade. Apesar desses avanços, a resolução permanece omissa quanto à admissibilidade de provas obtidas por meio de TRF em processos judiciais.

As lacunas regulatórias contribuem para o crescimento da autoridade epistêmica dos algoritmos, cuja atuação escapa ao controle externo e ao contraditório

18. AZEVEDO, Cynthia Picolo Gonzaga de; LIMA, Eliz Marina Bariviera de; SILVA, Felipe Rocha da; RODRIGUES, Gustavo Ramos; DUTRA, Luiza Corrêa de Magalhães; SANTARÉM, Paulo Rená da Silva; RODRIGUES, Victor Barbieri Vieira. *Nota técnica: análise comparativa entre o anteprojeto de LGPD penal e o PL 1515/2022.* Brasília: Laboratório de Políticas Públicas e Internet (LAPIN) e Instituto de Referência em Internet e Sociedade (IRIS), nov. 2022. Disponível em: [https://lapin.org.br/wp-content/uploads/2022/11/Nota-tecnica-Analise-comparativa-entre-o-anteprojeto-de-LGPD-Penal-e-o-PL-15152022-1.pdf]. Acesso em: 21 out. 2025.

efetivo no processo penal. Em um contexto em que algoritmos se tornam fontes e aparatos de investigação, essa brecha agrava a assimetria entre acusação e defesa, deixando advogados e réus sem acesso à origem dos dados, aos parâmetros técnicos utilizados ou à possibilidade de auditoria independente (Lima, 2024, p. 65).

Dessa forma, o Brasil se encontra diante de um desalinhamento: de um lado, um sistema jurídico que reconhece a proteção de dados como direito fundamental; de outro, um aparato de segurança pública que incorpora tecnologias altamente invasivas sem base legal clara, sem transparência e com elevado potencial de violação de garantias fundamentais. Esse conjunto de fatores – expansão acelerada, ausência de regulação, incentivos estatais, seletividade estrutural e opacidade técnica – cria uma infraestrutura socio-legal "ideal" para a atuação de empresas como a *Clearview AI*, cujas práticas de raspagem massiva de dados e oferta direta a órgãos de segurança operam justamente nesses interstícios regulatórios. É justamente nesse contexto que a empresa tem encontrado brechas para oferecer suas "soluções tecnológicas" e legitimar sua atuação no Brasil, como será analisado na próxima seção.

4. Entre rostos e rastros: *Clearview AI* e os limites do devido processo legal no Brasil

A trajetória da *Clearview AI* no Brasil ilustra como tecnologias de policiamento têm se inserido nas estruturas do Estado por vias informais e, posteriormente, vêm sendo institucionalizadas sem debate público ou definição de uma política clara. Inicialmente, a empresa buscou acesso ao mercado brasileiro por meio de apresentações em feiras de segurança, reuniões técnicas, testes gratuitos para agentes públicos e parcerias com intermediárias comerciais. Essa estratégia de penetração por entre frestas revela não apenas uma lógica de atuação empresarial da empresa, mas também uma ecologia regulatória permissiva e fragmentada, típica de contextos em que a implantação de tecnologias digitais avança mais rapidamente do que os marcos normativos e os mecanismos de controle institucional. Esse arranjo produz condições de possibilidades de experimentação e o uso de tecnologias com baixo *accountability* e alta plasticidade organizacional.

Documentos obtidos por meio da Lei de Acesso à Informação, reportagens investigativas e análise de transcrições públicas de entrevistas com representantes da empresa demonstraram que, desde 2019, a *Clearview AI* busca estabelecer vínculos com agências de segurança pública e autoridades brasileiras. Um ponto a destacar é que a empresa norte-americana não possui representação no Brasil, sendo necessária a presença de uma subsidiária para compra e uso formal no país. A prática de empregar revendedoras nacionais ou intermediárias, embora não caracterize ilegalidade flagrante, expõe uma lacuna significativa em termos de transparência,

uma vez que oculta o nome da empresa nos registros públicos disponíveis em portais da transparência.

A operacionalização dessas tecnologias no Brasil ocorre em um ambiente marcado por labirintos burocráticos e opacidade processual, como discutido na seção anterior. A ausência de regulamentação específica permite que contratos sejam firmados sem o devido escrutínio público e sem diretrizes claras sobre a proteção de dados pessoais. Essa lacuna regulatória favorece a adoção de sistemas cuja eficácia e ética são frequentemente questionadas, comprometendo princípios fundamentais como a privacidade e o devido processo legal. Ainda que o devido processo seja um conceito aberto, ele é fundamental para a garantia de direitos nas engrenagens dos sistemas jurídicos.

Em abril de 2022, a *Clearview* participou da feira ISC Brasil, um dos maiores eventos de segurança da América Latina, realizada em São Paulo. Na ocasião, representantes da empresa apresentaram a tecnologia a agentes de segurança pública, prometeram "testes gratuitos" e demonstraram a capacidade da TRF com base em imagens extraídas de redes sociais. Pouco tempo depois, a empresa participou de 3 reuniões técnicas com a Copaq da Secretaria Nacional de Segurança Pública (Senasp), órgão vinculado ao MJSP. Na primeira reunião, conforme relatado por jornalistas e confirmado por documentos obtidos para essa pesquisa, a *Clearview* ofereceu acesso experimental à ferramenta a agentes públicos, reafirmando seu interesse em atuar no Brasil (Martins, 2023). Como esses testes não entram nos registros burocráticos das agências (uso formalmente sancionado) e podem ser testados por agentes individuais, é difícil obter uma fotografia mais completa da extensão do histórico do uso da ferramenta no Brasil. Esse tipo de atuação revela uma lógica de penetração informal, na qual a empresa evita a via tradicional da contratação pública, optando por estratégias de aproximação técnica e comercial. Ademais, ao apresentar-se como empresa "de apoio à investigação" e não como fornecedora de *software* de reconhecimento facial, a *Clearview AI* reposiciona seu discurso jurídico e político para evitar obrigações contratuais, das exigências da LGPD e mecanismos de controle social. No plano discursivo, também se distancia de controvérsias e críticas públicas ao envolvendo o uso de TRFs no Brasil.

A atuação da *Clearview* se articula com a lógica de funcionamento do sistema de segurança pública brasileiro, que é altamente descentralizado, permeável à inovação tecnológica e vulnerável a pressões políticas e comerciais. Como observado nesta pesquisa, a incorporação de tecnologias de vigilância no Brasil frequentemente se dá por meio de demonstrações, testes-piloto, convênios improvisados ou parcerias informais, que escapam às exigências legais de contratação pública, fiscalização e prestação de contas (Lima et al., 2024). A *Clearview* se insere exatamente nesse modelo, oferecendo seu produto com "testes grátis" para agências

de segurança e como "recurso adicional", sem que isso passe pelo crivo institucional adequado. Dessa forma, o *software* circulou entre diversas agências ao redor do mundo, inclusive no Brasil, sem qualquer formalização contratual, bastando, em muitos casos, o uso de um *e-mail* institucional para obter acesso à ferramenta (Lima, 2024).

Os testes gratuitos geralmente oferecem dias de utilização aos policiais com um número limitado de buscas no sistema, e operam como forma de mostrar a capacidade da ferramenta e incentivar os agentes a promoverem sua aquisição em seus departamentos. Além disso, os próprios agentes passam a disseminar o uso da TRF em conferências ou por meio de redes de contato *online*, ampliando sua visibilidade entre diferentes corporações policiais (Hill, 2023; Haskins; Mac; McDonald, 2020). O uso de *e-mails* institucionais, vinculados a departamentos de polícia ou a endereços governamentais, nesses testes gratuitos gerou situações ambíguas, nas quais as próprias agências de segurança, por vezes, alegavam não ter plena ciência de que a tecnologia estava sendo utilizada por seus agentes. Essa lógica de "informalidade" expõe uma delegação tácita de autoridade tecnológica ao agente individual, sem qualquer protocolo organizacional, treinamento técnico ou orientação administrativa e jurídica claras.

Várias questões empíricas surgem em relação aos usos operacionais da *Clearview* e, de forma mais abrangente das TRFs. Os policiais constroem e, em consequência entendem o conhecimento que recebem de diferentes maneiras (Brayne; Christin, 2020). Entre essas questões, destacam-se: a forma como os julgamentos de risco dos operadores é enquadrada pela informação trazida à sua atenção pela interface com o algoritmo; o impacto nos julgamentos operacionais subsequentes; a natureza dinâmica da interação humano-computador; e como isso afeta os níveis de risco e, portanto, a vontade de intervir (Fussey; Davis; Innes, 2021). Os dados, a informação, não apenas informam, mas também cria forma (Heidegger, 1997, p. 182) de como a suspeita tem sido compreendida pelo operador do sistema e quais ações podem ser tornadas possíveis.

Em 2023, o MJSP adquiriu acesso ao sistema da *Clearview AI* por meio da empresa Inspect Inteligência e Tecnologia Ltda., em um processo sigiloso que omitiu o nome da *Clearview* dos registros oficiais. A contratação, feita sem licitação e sem consulta pública, demonstra como a formalização institucional pode ocorrer à revelia da transparência e da legalidade substancial (Martins, 2025). Ao ocultar a titularidade da tecnologia adquirida, o governo federal evitou o escrutínio social sobre o uso de uma ferramenta altamente controversa, proibida em diversos países da Europa e alvo de ações judiciais nos Estados Unidos, Reino Unido, Canadá e Austrália por violações à privacidade. Além do MJSP, também a polícia do Senado Federal firmou contrato com a *Clearview*, por meio da mesma intermediária, com vigência

entre novembro de 2024 e 2025 (Brasil, 2024). Da mesma forma, o Ministério Público e a Polícia Civil de Minas Gerais adquiriram acesso à tecnologia por três anos (Minas Gerais, 2025), evidenciando a consolidação da presença e operação da empresa no sistema de justiça e segurança brasileiro. Esses contratos marcam uma transição de práticas informais para a institucionalização de uma ferramenta cuja arquitetura tecnológica se baseia na coleta massiva e não autorizada de dados biométricos, o que desafia diretamente os princípios da LGPD e da Emenda Constitucional 115/2022, que reconhece a proteção de dados como direito fundamental.

Além disso, a tecnologia se beneficia de um ambiente jurídico ambíguo, no qual a ausência de norma específica para TRF em segurança pública permite a interpretação de que imagens publicamente disponíveis na *internet* podem ser utilizadas em investigações, mesmo sem autorização judicial, sem consentimento dos titulares e sem qualquer tipo de controle sobre sua origem, qualidade ou contexto. Essa ambiguidade facilita e legitima a circulação da ferramenta e, ao mesmo tempo, compromete os direitos dos cidadãos cujas imagens são capturadas, processadas e comercializadas.

O uso de dados de fontes abertas – prática central no modelo da *Clearview* – insere-se no debate mais amplo sobre o uso de Osint (*Open Source Intelligence*) em investigações criminais (Chermak et al., 2025). Apresentada frequentemente como alternativa legítima ao acesso direto a bases protegidas, essa estratégia de coleta de dados exige, no entanto, critérios jurídicos rigorosos relacionados à finalidade, necessidade e proporcionalidade de uso (Macêdo, 2019). Isso porque o fato de um dado estar acessível e público não significa que ele esteja disponível para qualquer finalidade. No entanto, no caso da *Clearview*, há um deslocamento dessa lógica: as imagens deixam de ser meros insumos investigativos auxiliares e passa a ser ponto de partida para a formulação de suspeitas. Rostos são vinculando automaticamente a identidades, redes de sociabilidades, localizações ações passadas, produzindo associações que ganham status de indícios investigativos. Nesse processo, a TRF não se limita a refletir uma realidade preexistente, mas contribui para materializá-la (Barad, 2007) – criando condições para que determinadas identidades se tornem suspeitas, mesmo sem evidências tradicionais. Trata-se de uma operação que transforma dados visuais processados algoritmicamente em narrativas incriminadoras, tensionando os princípios do devido processo legal, da ampla defesa e da legalidade da prova.

Apesar do uso crescente, a confiabilidade das TRFs em investigações criminais e sua validade como como evidência ainda não foram estabelecidas. Falta transparência mínima sobre como os algoritmos são utilizados na prática e como as evidências produzidas por eles têm sido enquadradas processualmente. Advogados de defesa, procuradores, os juízes e até mesmo os agências de segurança não tem

clareza de como os algoritmos estão sendo operados (Lima, 2024, p. 115). O exemplo da *Clearview AI*, mostra como esse uso pode ocorrer mesmo sem que, de fato, o departamento adquira formalmente a licença de uso, mas sim por meio de testes gratuitos. Isso representa um exemplo mais latente das maneiras pelas quais os a pulverização do uso das TRFs tem acontecido de maneira flexível, uma prática remodelável conforme o contexto organizacional de cada instituição.

Os danos e as violências das abordagens, detenções e investigações errôneas ancoradas nos resultados probabilísticos do algoritmo tendem a se materializar em ações práticas, embora muitas vezes sejam difíceis de quantificar. Trata-se de um problema difundido: a maioria das agências de segurança que usam a tecnologia ao redor do mundo não produzem os dados de buscas feitos pela TRFs, os casos de falso positivos e quais ações eles deram ignição, como número de abordagens ou prisões (Brayne; Christin, 2020; Fussey; Davis; Innes, 2021).

Há também uma outra camada complexa que desafia os regimes jurídicos estabelecidos, quando os resultados dessas ferramentas passam a integrar o processo penal sem observância à cadeia de custódia da prova digital. A ausência de mecanismos claros para garantir a integridade, a autenticidade e a rastreabilidade das provas digitais comprometem sua validade jurídica (Sanglard, 2023; Santos et al., 2021). Esse *déficit* de garantias como a preservação da cadeia de custódia de provas digitais compromete o devido processo legal, um dos pilares do sistema acusatório. Os dados não são entidades neutras, mas efeitos de relações intra-ativas entre atores, dispositivos, normas e materialidades (Barad, 2007; Lima, 2024). O dado gerado pelo algoritmo da *Clearview* não apenas emerge de práticas extrajudiciais de raspagem de dados, mas é reclassificado e recontextualizado como prova penal sem qualquer mediação institucional. Além de criar condições de possibilidade de não apenas ligar a imagem a um reconhecimento de identidade, mas a outros dados de rede sociais, metadados de localização, data e hora, *hashtag* e redirecionar a outras páginas da *internet*. E a partir desses metadados gerar *links* entre indivíduos e lugares.

O que se observa é a ampliação dos espectros de suspeição: rostos e perfis que precisam ser vigiados e/ou neutralizados para a manutenção da ordem e gerenciamento de risco (Amoore, 2020). Nesse sentido, o sistema não opera só sob a lógica do crime que foi cometido, mas também de forma a antecipar outros possíveis crimes, alinhando-se a uma lógica amplamente compartilhada entre os vários esforços para gerenciar risco, dentro do domínio da segurança. O reconhecimento de padrões e classificação algorítmica de pessoas tornam-se, assim, parte do *modus operandi* de diversas práticas históricas de controle de grupos e indivíduos para a manutenção da "ordem" (Cole, 2002).

Portanto, é importante refletir os impactos do uso da tecnologia no regime probatório da justiça criminal de modo que sua legalidade ou validade sejam

adequadamente questionadas nos processos. Trata-se de uma mutação nas formas de reconhecimento legalmente válidas, onde a mediação algorítmica passa a eclipsar outros mecanismos de investigação, produção de evidências e mediação pericial. Em entrevistas e investigações conduzidas por organizações da sociedade civil, defensores públicos relataram que materiais obtidos via TRFs, inclusive de sistemas informais, têm sido utilizados como elementos de convencimento judicial, mesmo sem laudo técnico formal, cadeia de custódia ou auditoria externa (Lima, 2024). O modo de dizer uma verdade do algoritmo ganha *status* de verdade técnica – e o risco de erro, viés ou manipulação torna-se parte da disputa e do debate a ser travado para garantia dos direitos fundamentais.

Nesse sentido, a figura do perito e o enquadramento do algoritmo enquanto *expert*, está inserida e são produtos do que Cole (2002, p. 15) chamou de "compromissos históricos da ciência e da lei para a produção de ordem". Esse processo revela uma transformação profunda: o algoritmo não apenas auxilia a investigação, mas reconfigura os modos de produzir verdade e culpabilidade no processo penal. Os sistemas algorítmicos operam por padrões probabilísticos, e não por certezas jurídicas – mas, ao serem apresentados como "evidências técnicas", acabam ganhando autoridade epistêmica e processual (Lima, 2024). A inteligibilidade pode resultar também na exclusão de narrativas alternativas e outros modos de "contar a verdade". No caso da *Clearview*, essa autoridade se constrói com base em um repositório de dados biométricos com origem contestável, mas cujos resultados são tomados como suficientemente credíveis (Lima, 2024, p. 73). O ciclo se fecha quando promotores, juízes e defensores não têm acesso aos parâmetros técnicos, às imagens comparadas, à taxa de erro do sistema, aos critérios utilizados na identificação e aos procedimentos operacionais padrão de uso institucional da ferramenta.

No Brasil, esse circuito é problemático porque reforça práticas históricas de policiamento e suspeição. Em um sistema penal marcado por seletividade estrutural e desigualdade institucional, o uso de TRF para fins de segurança exige não apenas uma discussão regulatória, jurídica, política e social, mas também um debate mais amplo sobre o regime de segurança pública e do aparato de justiça criminal. Como produzir justiça quando os operadores do direito não têm acesso às bases de funcionamento das ferramentas que sustentam as acusações e que derem ignição a abordagens? Como garantir o contraditório em um ecossistema de provas algorítmicas que escapa aos mecanismos institucionais clássicos de verificação? O que está em jogo não é apenas a proteção de dados pessoais e os desafios à privacidade, mas também a arquitetura de um regime de produção de conhecimento e verdade de segurança e jurídica que opera como condição de possibilidade para uma distribuição desigual de insegurança e direitos.

Nossa tendência é nos tornarmos confortáveis com nossos quadros interpretativos. Por isso, desestabilizar os imaginários sobre o que os algoritmos são e o que podem fazer no sistema de justiça criminal é um passo que pode nos ajudar o entender como essas tecnologias podem sufocar possibilidades de ação e legitimar práticas violentas e excludentes na tentativa de estabilizar uma ordem e domesticar o risco.

5. Conclusão

A trajetória da *Clearview AI* e sua circulação transnacional evidenciam com nitidez os impasses contemporâneos entre inovação tecnológica, segurança pública e efetivação de direitos fundamentais. Ao consolidar uma infraestrutura algorítmica baseada na raspagem massiva de dados biométricos extraídos de fontes públicas, a empresa desafia os direitos fundamentais, marcos regulatórios de proteção da privacidade e dispositivos de *accountability* democrática.

No caso brasileiro, esse modelo se insere em um regime de segurança pública marcado por fragmentação regulatória, improvisação institucional e seletividade estrutural. A circulação da *Clearview,* por meio de testes gratuitos, feiras, reuniões técnicas e contratos pouco claros, ilustra como tecnologias de alto risco a direitos podem ser integradas a práticas policiais e judiciais sem passar por filtros mínimos de controle, transparência ou avaliação pública.

Mais do que uma controvérsia sobre coleta ilícita de dados, o caso *Clearview AI* demonstra a formação de redes sociotécnicas de vigilância nas quais empresas privadas, agentes públicos e operadores do direito coproduzem novas formas de identificar, classificar e incriminar. As TRFs, longe de serem ferramentas neutras, atualizam e automatizam práticas históricas de suspeição ancoradas em marcadores sociais de diferença. Elas não apenas transformam rostos em dados, mas reconfigura as formas de produção de insegurança, alimentando práticas discriminatórias, violentas e atravessadas por desigualdades sociais, tecnológicas e epistemológicas.

No campo da justiça criminal, essas tecnologias impõem desafios concretos: como garantir o contraditório e a ampla defesa quando os dados são opacos, os algoritmos são protegidos por segredo comercial e os critérios de identificação não são auditáveis? Como assegurar a legitimidade da prova penal quando sua origem está ancorada em bancos privados não supervisionados por nenhuma instância pública? A questão não se resume aos riscos de erro ou aos falsos positivos. O que está em jogo é a consolidação de uma nova racionalidade penal, sustentada por tecnologias que tornam rotineira a vigilância massiva, naturalizam a suspeição preditiva e esvaziam as garantias processuais e de direitos. Em um cenário de baixa

transparência, as próprias agências públicas – e a sociedade como um todo – não têm clareza sobre como as TRFs operam nem quais impactos essas tem produzido.

As TRFs vêm sendo utilizadas de maneira persistente por órgãos de segurança mesmo diante de falhas conhecidas e controvérsias em torno de erros, abordagens vexatórias e violações de direitos fundamentais. Na prática, a ausência de regulação inverte o princípio da inocência: exige-se do cidadão uma demonstração contínua de que "não tem nada a esconder" para evitar ser enquadrado como suspeito. Em muitos casos, as buscas através de TRFs sequer se limitam a indivíduos sob investigação, ampliando o escopo da vigilância para a população em geral, como as possibilidades de uso da *Clearview AI.* Várias questões éticas e políticas decorrem do poder crescente dessas tecnologias, especialmente quando operam em contextos marcados pela flexibilização de garantias processuais, que tende a se tornar regra, e não exceção.

Segundo Deleuze e Guattari (1995, p. 175), as próprias máquinas não explicam nada, "é preciso analisar os aparatos coletivos dos quais as máquinas são apenas um componente". Nessa perspectiva, a TRFs não devem ser analisadas isoladamente, mas como parte de arranjos sociotécnicos e institucionais mais amplos. Enfrentar seus impactos exige, portanto, não apenas regulação normativa, mas também uma análise crítica sobre os aparatos coletivos que tornam sua adoção possível – e que a legitimam como forma eficiente, embora opaca, de governar a insegurança. Diante disso, analisar o caso *Clearview* é também refletir sobre os contornos emergentes de uma nova arquitetura do processo penal – mais opaca, mais automatizada e cada vez mais distante das promessas constitucionais de justiça.

Referências

AMERICAN CIVIL LIBERTIES UNION. *ACLU v. Clearview AI*. [S.l.]: ACLU, [s.d.]. Disponível em: [https://aclu.org/cases/aclu-v-clearview-ai]. Acesso em: 21.06.2023.

AMOORE, L. *Cloud ethics*: Algorithms and the attributes of ourselves and others. Durham: Duke University Press, 2020.

ARADAU, C.; BLAKE, T. Algorithmic Surveillance and the Political Life of Error. *Journal for the History of Knowledge*, v. 2, n. 1, p. 10, 2021. [https://doi.org/10.5334/jhk.42].

AZEVEDO, Cynthia Picolo Gonzaga de; LIMA, Eliz Marina Bariviera de; SILVA, Felipe Rocha da; RODRIGUES, Gustavo Ramos; DUTRA, Luiza Corrêa de Magalhães; SANTARÉM, Paulo Renã da Silva; RODRIGUES, Victor Barbieri Vieira. Nota técnica: análise comparativa entre o anteprojeto de LGPD penal e o PL 1515/2022. Instituto de Referência em Internet e Sociedade (IRIS) e Laboratório de Políticas Públicas e Internet (LAPIN), nov.

2022. Disponível em: [https://lapin.org.br/wp-content/uploads/2022/11/Nota-tecnica-Analise-comparativa-entre-o-anteprojeto-de-LGPD-Penal--e-o-PL-15152022-1.pdf]. Acesso em: 15.03.2025.

BARAD, K. *Meeting the universe halfway*: Quantum physics and the entanglement of matter and meaning. Durham: Duke University Press, 2007.

BAUMAN, Zygmunt et al. Após Snowden: repensando o impacto da vigilância. *Revista Eco-Pós*, v. 18, n. 2, p. 8-35, 2015.

BENJAMIN, R. Assessing risk, automating racism. *Science*, v. 366, n. 6464, p. 421-422, 2019.

BISCHOFF, Paul. *Facial recognition technology (FRT)*: 100 countries analyzed. Comparitech, 28 de junho de 2021. Disponível em: [https://www.comparitech.com/blog/vpn-privacy/facial-recognition-statistics/]. Acesso em: 21.10.2025.

BRASIL. SENADO FEDERAL. *Transparência e prestação de contas*. Licitações e contratos. Contrato 196/2024. Atualizado em: 13.12.2024. Disponível em: [www6g.senado.gov.br/transparencia/licitacoes-e-contratos/contratos/7982]. Acesso em: 31.03.2025.

BRAYNE, Sarah. Big data surveillance: The case of policing. *American Sociological Review*, v. 82, n. 5, p. 977-1008, 2017.

BRAYNE, Sarah; CHRISTIN, Angèle. Technologies of crime prediction: The reception of algorithms in policing and criminal courts. *Social Problems*, v. 68, n. 3, p. 608-624, 2021.

BROWNE, S. *Dark matters*: On the surveillance of blackness. Durham: Duke University Press, 2015.

BUOLAMWINI, J.; GEBRU, T. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. *Proceedings of Machine Learning Research*, v. 81, p. 1-15, 2018. Disponível em: [https://proceedings.mlr.press/v81/buolamwini18a.html].

CHERMAK, S. M. et al. Open-Source Research in Criminology and Criminal Justice. *Annual Review of Criminology*, v. 8, 2025.

CLEARVIEW AI NAMED to Time's inaugural list of the Time100 most influential companies. *Clearview AI*, New York, 29.04.2021. Disponível em: [www.clearview.ai/press-room/clearview-ai-named-to-times-inaugural-list-of--the-time100-most-influential-companies]. Acesso em: 17.04.2025.

CLEARVIEW AI SETTLES ACLU. Illinois Lawsuit confirming continuity of business supporting public safety. *Clearview AI*, New York, 12.05.2022. Disponível em: [www.clearview.ai/press-room/clearview-ai-settles-aclu--illinois-lawsuit-confirming-continuity-of-business-supporting-public--safety]. Acesso em: 17.04.2025.

COLE, Simon A. *Suspect identities*: A history of fingerprinting and criminal identification. Harvard University Press, 2002.

CRAWFORD, K. *The atlas of AI*: Power, politics, and the planetary costs of artificial intelligence. New Haven: Yale University Press, 2021.

FELDSTEIN, Steven. *The global expansion of AI surveillance*. Washington, DC: Carnegie Endowment for International Peace, 2019. Disponível em: [https://carnegieendowment.org/research/2019/09/the-global-expansion-of-ai-surveillance?lang=en]. Acesso em: 21.10.2025.

FERGUSON, A. G. *The rise of big data policing*: Surveillance, race, and the future of law enforcement. New York: NYU Press, 2017.

FLAUZINA, A. L. P. *Corpo negro caído no chão*: o sistema penal e o projeto genocida do Estado brasileiro. 2006.

FUSSEY, Pete; DAVIES, Bethan; INNES, Martin. 'Assisted' facial recognition and the reinvention of suspicion and discretion in digital policing. The British journal of criminology, v. 61, n. 2, p. 325-344, 202.

DELEUZE, Gilles; GUATTARI, Félix. *Introdução*: rizoma. Mil platôs: capitalismo e esquizofrenia, v. 1, p. 11-37, 1995.

HASKINS, C.; MAC, R.; MACDONALD, L. Clearview AI facial recognition software's use by authoritarian regimes. *BuzzFeed News*, 2020. Disponível em: [www.buzzfeednews.com/article/carolinehaskins1/clearview-ai-facial--recognition-authoritarian-regimes-22]. Acesso em: 10.06.2024.

HEIDEGGER, Martin. *Kant and the Problem of Metaphysics, enlarged*. Indiana University Press, 1997.

HILL, K. *Your Face Belongs to Us*: A Tale of AI, a Secretive Startup, and the End of Privacy. New York: Random House, 2023.

KATZ, Yarden. *Artificial whiteness*: Politics and ideology in artificial intelligence. Columbia University Press, 2020.

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

LIMA, T. G. L. *Better justice through better science-technology?* The entanglements of algorithms and security and legal professionals. 2024. Tese (Doutorado) – Pontifícia Universidade Católica do Rio de Janeiro, Rio de Janeiro, Brasil.

LYON, D. Biometrics, identification and surveillance. *Bioethics*, v. 22, n. 9, p. 499-508, 2008. DOI: [https://doi.org/10.1111/j.1467-8519.2008.00697.x].

MAC, R.; HASKINS, C.; PEQUENO IV, A. Police In At Least 24 Countries Have Used Clearview AI. Find Out Which Ones Here. *Buzzfeed*, 25.08.2021. Disponível em: [www.buzzfeednews.com/article/ryanmac/clearview-ai-international-search-table]. Acesso em: 27.03.2024.

MACÊDO, A. S. *A intersecção entre* Osint *e* Humint *através da abordagem de* crowdsourcing *como subsídio para ações de inteligência policial*. 2019. Dissertação (Mestrado em Ciência da Informação) – Universidade Federal de Santa Catarina, Florianópolis, 2019. [https://repositorio.ufsc.br/handle/123456789/219176]. Acesso em: 27.03.2024.

MARTINS, Laís. Exclusivo: em reuniões secretas, Clearview ofereceu 3 bilhões de imagens de brasileiros para polícias e Ministério da Justiça. *Intercept Brasil*, 16.05.2023. Disponível em: [www.intercept.com.br/2023/05/16/em-reunioes-secretas-clearview-policias-ministerio-da-justica/]. Acesso em: 27.03.2024.

MARTINS, Laís. Vigilância turbinada: Ministério da Justiça comprou secretamente tecnologia que coleta fotos sem autorização para reconhecimento facial. *Intercept Brasil*, São Paulo, 03.02.2025. Disponível em: [www.intercept.com.br/2025/02/03/ministerio-da-justica-comprou-secretamente-tecnologia-que-coleta-fotos-sem-autorizacao-para-reconhecimento-facial/]. Acesso em: 31.03.2025.

MCSORLEY, Tim. The case for a ban on facial recognition surveillance in Canada. *Surveillance & Society*, v. 19, n. 2, p. 250-254, 2021.

MINAS GERAIS. *Portal da Transparência do Estado de Minas Gerais*. Contrato 9437287. Belo Horizonte: Governo do Estado, 2025. Disponível em: [www.transparencia.mg.gov.br/licitacoes-e-contratos/compras-e-contratos/comprasecontratos-filtros/5/2024/01-01-2024/31-12-2024/91/87547]. Acesso em: 27.03.2025.

MOROZOV, E. *To save everything, click here*: Technology, solutionism and the urge to fix problems that don't exist. London: Allen Lane, 2013.

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

O PANÓPTICO. *O Panóptico*. [S.l.]: o Panóptico, [s.d.]. Disponível em: [www.opanoptico.com.br/]. Acesso em: 27.12.2024.

PRESS, E. Does A.I. Lead Police to Ignore Contradictory Evidence? *The New Yorker*, 20 nov. 2023. Disponível em: [www.newyorker.com/magazine/2023/11/20/does-a-i-lead-police-to-ignore-contradictory-evidence]. Acesso em: 13.04.2024.

RAMAGE, Jack. Facial recognition company Clearview AI permanently banned from selling data to private companies. *Euronews*, 10.05.2022. Disponível em: [www.euronews.com/next/2022/05/10/facial-recognition-company--clearview-ai-permanently-banned-from-selling-data-to-private-co]. Acesso em: 13.04.2024.

REDE DE OBSERVATÓRIOS DA SEGURANÇA. *1º Relatório da Rede de Observatórios da Segurança*. [S.l.]: Observatório da Segurança, 2019. Disponível em: [https://observatorioseguranca.com.br/wordpress/wp-content/uploads/2019/11/1relatoriorede.pdf]. Acesso em: 21.10.2025.

REZENDE, Isadora Neroni. Facial recognition in police hands: Assessing the 'Clearview case' from a European perspective. *New Journal of European Criminal Law*, v. 11, n. 3, p. 375-389, 2021.

SANGLARD, J. F. *Cadeia de custódia da prova digital no processo penal brasileiro*. Tese. São Paulo, Universidade Presbiteriana Mackenzie, 2023.

SANTOS, A. J. S.; BORGES, A. F. M.; RODRIGUES, G. L. M. T. A cadeia de custódia na coleta da prova digital de acordo com a Lei 13.964/2019, dos seus artigos 158-A ao 158-F. *RECIMA21:* Revista Científica Multidisciplinar, v. 2, n. 8, e28612, 2021.

SEAVER, Nick. Algorithms as culture: Some tactics for the ethnography of algorithmic systems. *Big data & society*, v. 4, n. 2, p. 2053951717738104, 2017.

SILVA, Tarcízio. *Racismo algorítmico em plataformas digitais*: microagressões e discriminação em código. Comunidades, algoritmos e ativismos digitais: olhares afrodiaspóricos, 2020. p. 121-135.

SOUSA, R. et al. *Sport, data and rights*: use of facial recognition in Brazilian stadiums. Rio de Janeiro: CESeC, 2024.

THYLSTRUP, Nanna Bonde. *The politics of mass digitization*. MIT Press, 2019.

Legislação

BRASIL. Conselho Nacional de Justiça. *Resolução 615, de 11 de março de 2025*. Estabelece diretrizes para o desenvolvimento, utilização e governança de soluções desenvolvidas com recursos de inteligência artificial no Poder Judiciário. Disponível em: [https://atos.cnj.jus.br/files/original155530202 5031467d4517244566.pdf]. Acesso em: 31.03.2025.

BRASIL. Portaria 793, de 24 de outubro de 2019. Ministério da Justiça e Segurança Pública/Gabinete do Ministro. *Diário oficial da União*. Disponível em: [www.in.gov.br/en/web/dou/-/portaria-n-793-de-24-de-outubro-de-2019-223853575].

Recebido em: 31.03.2025.
Aprovado em: 26.05.2025.
Última versão da autora: 05.06.2025.

PESQUISA DO EDITORIAL

Área do Direito: Penal; Digital

Veja também Doutrina relacionada ao tema

- Dados pessoais no processo penal: tutela da personalidade e da inocência diante da tecnologia, de Flaviane de Magalhães Barros Bolzan de Morais, Leonardo Augusto Marinho Marques e Jamilla Monteiro Sarkis – *RBCCrim* 190/117-156;
- Nota técnica sobre o uso de biometria facial no Metrô de São Paulo, de Cristiano Colombo e Guilherme Damasio Goulart – *BRTO* 25;
- O reconhecimento facial na segurança pública e a proteção de dados pessoais como garantia fundamental, de Beatriz Daguer, Luiz Antonio Borri e Rafael Junior Soares – *RDTec* 16;
- Reconhecimento facial e prova ilícita: a possibilidade de se considerar o reconhecimento facial como meio de prova ilícito, de Matheus Della Monica e Rodrigo Marchetti Ribeiro – *RDTec* 13; e
- Vigiar e Punir 4.0: efeitos das tecnologias de policiamento preditivo e reconhecimento facial no brasil e a perpetuação do racismo estrutural, de Fernanda Mateus Rosa da Silva – *RDTec* 16.

Veja também Jurisprudência relacionada ao tema

- TJSP, AgIn 2079077-58.2022.8.26.0000, j. 10.10.2022, *DJe* 18.10.2022.

Lima, Thallita Gabriele Lopes. *Faces make cases*: o caso *Clearview AI* e os desafios do uso de tecnologias algorítmicas no sistema de justiça criminal brasileiro. *Revista Brasileira de Ciências Criminais*. vol. 211. ano 33. p. 85-114. São Paulo: Ed. RT, nov./dez. 2025. DOI: [doi.org/10.5281/zenodo.17058344].