Tecnologias de reconhecimento facial: captura e vigilância na emergência do tipo digital-criminal

Helena Machado

Iscte — Instituto Universitário de Lisboa, Centro de Investigação e Estudos de Sociologia (CIES-Iscte), Lisboa, e Instituto de Ciências Sociais, Universidade do Minho, Braga, Portugal

Susana Silva

Departamento de Sociologia, Instituto de Ciências Sociais, Universidade do Minho e CRIA-UMinho/IN2PAST, Braga, Portugal

Introdução

Os avanços recentes no campo das ciências da computação, juntamente com a crescente disponibilidade de grandes volumes de dados digitais, têm impulsionado a capacidade de sistemas informáticos e algoritmos emularem comportamentos "inteligentes" típicos dos seres humanos, promovendo uma evolução exponencial da chamada Inteligência Artificial (IA). As aplicações desta tecnologia são vastas e, com estas, multiplicam-se os debates sobre as profundas transformações sociais, culturais e políticas que poderão ocorrer em diversas áreas. Um dos setores que tem atraído atenção crescente é o sistema de justiça, onde as expectativas sobre o potencial da IA se

multiplicam. Emerge, entre outros questionamentos, a seguinte interrogação: o sistema de justiça, cuja missão é garantir a ordem social, proteger os direitos individuais e assegurar a resolução equitativa de conflitos, poderá beneficiar da introdução da IA ou, pelo contrário, enfrentará riscos e desafios que comprometerão esses objetivos? O presente capítulo explora a utilização da IA no sistema de justiça, abordando essa questão a partir de um enfoque nas tecnologias de reconhecimento facial. Perspetivamos a IA como um fenómeno sociotécnico (Søraa, 2023: 12-13), considerando as interações complexas entre tecnologia, sistema de justiça e contextos históricos, sociais, culturais, económicos e políticos (Machado e Silva, 2024: 107-125), e discutindo as composições éticas imbricadas nessas interações para o caso particular das tecnologias de reconhecimento facial (Machado e Silva, 2025).

As tecnologias de reconhecimento facial funcionam com base na análise de características faciais extraídas de imagens ou vídeos — como a distância entre os olhos, a forma do nariz e os contornos do rosto —, desempenhando funções de autenticação (confirmar se uma pessoa é quem diz ser), de identificação (determinar quem é uma pessoa) e, abrindo caminho para usos mais controversos, de avaliação de estados emocionais e inferência de traços de personalidade e comportamentais (Hupont *et al*., 2022; Kaur *et al*., 2020). Originalmente desenvolvidas para aplicações militares nos Estados Unidos da América desde a década de 1960 (Gates, 2011), estas tecnologias têm avançado significativamente nos últimos anos e tornaram-se cada vez mais presentes em setores como a segurança pública, o comércio, as finanças e as tecnologias móveis. A pandemia da covid-19 acelerou essa expansão, abrindo novas oportunidades para as tecnologias de reconhecimento facial e outras formas de

monitorização biométrica possibilitadas pela cada vez mais sofisticada e normalizada identificação automatizada e rastreamento em tempo real, e atuando simultaneamente sobre populações e indivíduos (Andrejevic *et al*., 2024). Neste cenário, analistas do setor preveem que o tamanho do mercado global das tecnologias de reconhecimento facial mais do que quadruplicará entre 2020 e 2032 (Allied Market Research, 2023).

Atualmente, os sistemas de videovigilância com capacidades de reconhecimento facial tornaram-se padrão em muitos países do mundo. Presentes em locais como aeroportos, postos fronteiriços, estádios e espaços públicos, têm como objetivo controlar fluxos de migrantes e identificar pessoas de interesse, que, por exemplo, constem de listas de foragidos, de terroristas ou de bases de dados criminais nacionais (Dauvergne, 2022a, 2022b; Ellerbrok, 2011; Kloppenburg e van der Ploeg, 2018; Magnet, 2011; Sánchez-Monedero e Dencik, 2022). No caso específico das tecnologias de reconhecimento facial no sistema de justiça, são comummente apontadas como potencialidades a identificação de suspeitos de forma mais rápida e precisa, a localização de pessoas desaparecidas, a verificação de identidades em processos judiciais e prisões, e a monitorização de locais de alto risco em tempo real (Machado e Silva, 2024, 2025).

No entanto, são também referidos os riscos significativos que o uso de tecnologias de reconhecimento facial acarreta para o sistema de justiça, nomeadamente no que diz respeito à privacidade e aos direitos fundamentais (Bakiner, 2023; Machado, 2025). Existe uma crescente preocupação quanto à possibilidade de erros de identificação, especialmente no reconhecimento de pessoas de minorias étnicas, que podem estar mais sujeitas a falhas nos

algoritmos de reconhecimento facial, levando a acusações injustas e perpetuando discriminações já presentes no sistema de justiça (Buolamwini, 2023). Além disso, o uso massivo destas tecnologias pode contribuir para uma vigilância excessiva dos cidadãos, comprometendo a sua liberdade e a presunção de inocência (Dauvergne, 2022a). A falta de transparência nos algoritmos e a possibilidade de abuso por parte das autoridades reforçam os receios de que a adoção destas tecnologias, em vez de promover a justiça, possa agravar desigualdades e injustiças estruturais (Aradau e Blanke, 2022; Crawford, 2024 [2021]).

Visando ir além das abordagens convencionais que limitam o debate sobre o uso da IA (concretamente sobre tecnologias de reconhecimento facial no sistema de justiça) à dicotomia entre "riscos" e "benefícios", neste capítulo procuraremos compreender as complexas interações destas tecnologias com os contextos históricos, sociais, culturais, económicos e políticos em que são implementadas. A nossa análise desenvolver-se-á em duas fases principais. Numa primeira etapa, analisaremos o cruzamento entre os mitos culturais sobre o potencial transformador da IA (Bareis e Katzenbach, 2022) e os imaginários tecno-autoritários associados a tecnologias de reconhecimento facial (Machado, 2025; Schopmans e Ebetürk, 2023), com o intuito de mapear discursos dominantes sobre os impactos destas tecnologias. Fá-lo-emos a partir das perspetivas de grupos sociais diferenciados: quem desenvolve tecnologias de reconhecimento facial e quem contesta a sua utilização.

Em seguida, exploramos diversas implicações sociais e éticas das tecnologias de reconhecimento facial no contexto do sistema de justiça, inspiradas no que alguns autores referem como a coexistência de dois modelos culturais distintos de privacidade: o modelo de

vigilância e o modelo de captura (Agre, 1994; Vailly, 2024). Entre outros aspetos contrastantes (Agres, 1994: 756), o modelo de vigilância está mais associado à recolha de dados em larga escala e à sensação de estar constantemente a ser observado, enquanto o modelo de captura centra-se na categorização, classificação e reutilização de dados pessoais, suscitando preocupações relativas à precisão, ao consentimento e ao uso indevido dessas informações. O modelo de vigilância e o modelo de captura, conforme descritos por Agre (1994), não refletem apenas diferentes tecnologias e métodos de monitorização, como levantam preocupações sociais e éticas distintas que, porém, se revelam cada vez mais profundamente entrecruzadas. Na nossa perspetiva, esta coexistência manifesta-se nos atuais usos de tecnologias de reconhecimento facial no sistema de justiça, configurando a emergência daquilo que designaremos como tipo digital-criminal. Concretamente, a nossa análise do tipo digital-criminal far-se-á à luz da conexão entre vigilância e captura, refletindo criticamente sobre as profundas mudanças que o uso do reconhecimento facial no sistema de justiça pode provocar na forma como as categorias sociais e políticas de "suspeito" e "criminoso" são definidas e aplicadas.

As tecnologias de reconhecimento facial como um fenómeno sociotécnico

Podemos falar da IA, incluindo as tecnologias de reconhecimento facial, como um "fenómeno sociotécnico" (Machado e Silva, 2024; Søraa, 2023: 12-13). Este termo chama a atenção para a

forma como os valores, as práticas institucionais e as desigualdades sociais estão incorporados no código, na conceção e no uso de tecnologias de IA, no caso em apreço, nas tecnologias de reconhecimento facial no sistema de justiça. Além disso, esta perspetiva permite destacar os contextos históricos, sociais, culturais, económicos e políticos que moldam o desenvolvimento, a utilização e as perceções sobre as tecnologias de reconhecimento facial.

Uma dimensão central da análise sociotécnica diz respeito ao papel dos discursos dominantes no espaço público, na medida em que os mesmos influenciam fortemente o modo como as pessoas pensam e falam sobre IA e, considerando a tecnologia que analisamos neste texto, sobre o reconhecimento facial baseado em IA. Por exemplo, metáforas como "inteligência" e "aprendizagem" das máquinas são frequentemente utilizadas, mas, no contexto específico do reconhecimento facial, termos como "segurança" e "identificação em tempo real" tornam-se igualmente prevalentes, alimentando mitos e expectativas futuras (Bareis e Katzenbach, 2022; Campolo e Crawford, 2020; Machado e Silva, 2024; Machado *et al*. 2023; Natale e Ballatore, 2017).

Um dos discursos mais influentes sobre tecnologias de reconhecimento facial está ligado à ideia de que os computadores podem "ver", "identificar" e "reconhecer" características humanas. Esse discurso é muito comum na ficção científica atual e em mitos culturais que se mantêm ao longo do tempo (Mayor, 2018; Sheikh *et al*., 2023). Uma das consequências mais importantes desse discurso é a de que este ajuda a justificar a transferência de controlo dos seres humanos para a IA. No caso das tecnologias de reconhecimento facial baseadas em IA, existe um discurso prevalecente que argumenta que a computação visual pode detetar e interpretar os significados de

micro-expressões que passam despercebidas à visão humana (Black, 2023).

No contexto das tecnologias de reconhecimento facial, essa transferência de agência do humano para a máquina levanta questões éticas e sociais, uma vez que a vigilância e o controlo que lhe estão associados, muitas vezes considerados como avanços tecnológicos, podem, na verdade, resultar em práticas de discriminação e de invasão de privacidade. Ao mesmo tempo, estas implicações são frequentemente minimizadas em relação aos esperados efeitos benéficos do desenvolvimento de tecnologias de reconhecimento facial, por exemplo, na segurança pública e no sistema de justiça. A priorização da segurança em detrimento da privacidade e dos direitos civis e a ênfase na eficácia destas tecnologias em detrimento de erros e falhas permitem elucidar sobre as estruturas de poder e a hierarquia de valores sociais implícitas nos usos das tecnologias de reconhecimento facial no sistema de justiça, revelando a força de mitos bem-sucedidos construídos em torno da IA, em particular os mitos da sua inevitabilidade e da objetividade e neutralidade da tecnologia. Estes mitos bem-sucedidos permitem compreender processos de despolitização que reduzem a complexidade do reconhecimento facial à ideia do olhar "neutro" e "objetivo" da máquina, frequentemente associados a reivindicações de precisão e de eficácia irrefutáveis. No seu conjunto, estes mitos dissociam as tecnologias de reconhecimento facial dos contextos sociais, culturais, económicos e políticos em que são concebidas e usadas.

No entanto, a proliferação dessas tecnologias tem gerado preocupações significativas entre académicos, ativistas, especialistas em privacidade e reguladores sobre os possíveis efeitos para a sociedade. Entre os tópicos que suscitam preocupações, destacam-se:

a ampliação da vigilância em massa por governos e empresas e as ameaças à privacidade, às liberdades civis e aos direitos humanos (Bueno, 2020; Dauvergne, 2022a, 2022b; Machado, 2025); a perpetuação de discriminação contra comunidades e grupos vulneráveis, que são mais suscetíveis a processos de suspeição e vigilância (Søraa, 2023); e as falhas e imprecisões dessas tecnologias, que tendem a atingir sobretudo pessoas que saem fora do modelo dominante de treinamento da IA – o padrão de "homem branco" (Buolamwini, 2023; Cabitza *et al*., 2022). Neste contexto, as tecnologias de reconhecimento facial são frequentemente associadas àquilo que Schopmans e Ebetürk (2023) designam como "imaginários tecno-autoritários", a propósito de uma comparação entre movimentos sociais de contestação do uso de reconhecimento facial nos EUA e na Europa. Os autores definem os "imaginários tecno-autoritários" como "visões coletivas de um futuro social indesejável em que os atores públicos e privados utilizam sistematicamente tecnologias que, pela sua própria conceção, facilitam práticas não democráticas, para retirar os direitos democráticos de indivíduos ou grupos" (Schopmans e Ebetürk, 2023: 944).

Em síntese, podemos resumir as principais tendências discursivas em torno dos usos de tecnologias de reconhecimento facial, especialmente no contexto do sistema de justiça, da seguinte forma (Tabela 1), tendo em conta as perspetivas dos desenvolvedores destas tecnologias e dos críticos:

Tabela 1. Usos de tecnologias de reconhecimento facial no sistema de justiça: tendências discursivas de desenvolvedores e críticos

Aplicações	**Perspetivas dos**	**Perspetivas dos críticos**

	desenvolvedores	
Prevenção de crimes		
Identificação de suspeitos	Possibilidade de identificação de indivíduos com mandados de captura em locais públicos, aumentando a segurança em eventos e espaços públicos.	Risco de abuso por parte das autoridades, aumento da vigilância de massas e impacto sobre as liberdades civis.
Triagem de suspeitos em fronteiras, aeroportos e pontos de controlo	Aceleração da triagem e identificação de possíveis criminosos ou pessoas procuradas em fronteiras e pontos de controlo, melhorando a segurança nacional.	Questões sobre discriminação racial e étnica, risco de perfis raciais e erros que possam resultar em detenções arbitrárias ou deportações injustas.
Investigação criminal		
Identificação de suspeitos	Identificação mais rápida de suspeitos através de câmaras de segurança, bases de dados criminais e dispositivos e sensores inteligentes, acelerando investigações.	Preocupações sobre imprecisões, especialmente com grupos minoritários, que podem resultar em falsos positivos e detenções injustas.
Recolha de provas	Possibilidade de recolha de provas visuais de suspeitos em cena de crime, melhorando a eficiência das investigações e processos judiciais.	Preocupações sobre a validade das provas, manipulação tecnológica e falta de transparência no uso da tecnologia em investigações criminais.

Análise forense de imagens	Uso de imagens capturadas em câmaras de segurança para identificar indivíduos envolvidos em crimes.	Preocupações sobre a precisão da tecnologia em diferentes condições de iluminação e ângulos, bem como o potencial para erro humano ou dependência excessiva da tecnologia.
Contacto com instituições judiciais e penais		
Monitorização de indivíduos a cumprir penas	Maior controlo e monitorização de indivíduos em liberdade condicional ou sob vigilância.	Questões de privacidade e direitos humanos, com receios de vigilância excessiva e uso discriminatório.
Verificação de identidade em tribunais	Apoio na verificação da identidade de testemunhas, vítimas e acusados em tribunais, prevenindo fraudes ou falsificações.	Preocupações sobre erros no reconhecimento facial, falta de fiabilidade em condições variáveis e possíveis injustiças judiciais baseadas em falhas tecnológicas.

Fonte: Sistematização inspirada em Gentzel, 2021, e Machado e Silva, 2025.

Captura e vigilância no reconhecimento facial: interconexões

As conceções tradicionais de vigilância estão geralmente vinculadas a imagens de poder militar, polícias secretas e sociedades autoritárias distópicas no estilo orwelliano. Já o modelo de captura descreve os processos pelos quais as atividades humanas (entre outras, trabalhar, consumir ou viajar) são transformadas em dados computacionais, os quais são reorganizados e manipulados por sistemas tecnológicos, influenciando a maneira como essas atividades são interpretadas e geridas. Esses sistemas tecnológicos redefinem e reorganizam a realidade social com base numa lógica informacional e computacional. Philip Agre, um informático e cientista da computação que se tornou professor de humanidades, destaca que vigilância e captura não são categorias necessariamente exclusivas e podem coexistir (Agre, 1994: 756), ponderando as suas implicações para a privacidade.

Adotando esta proposta de Agre, podemos refletir sobre a forma como a captura e a vigilância se manifestam no caso das tecnologias de reconhecimento facial. No modelo de vigilância, o reconhecimento facial pode ser utilizado de forma difusa e passiva, recolhendo imagens de faces que passam por câmaras, muitas vezes sem que as pessoas saibam. Esse modelo está focado na monitorização e na prevenção, sem que isso implique organizar formalmente (estruturar e classificar) os dados recolhidos. No modelo de captura, as tecnologias de reconhecimento facial são usadas para identificar e categorizar as características faciais com base em padrões e modelos predefinidos (como medições geométricas e categorias de género, idade, raça, tipo de emoções, etc.). Conforme explicado atrás, no modelo de captura os dados são processados e reorganizados para serem utilizados em diversas aplicações e comparados com bases de dados existentes, na medida em que o modelo de captura está

orientado para a organização e gestão de informações, estruturando os dados de forma a possibilitar a sua reutilização em processos de automatização, de previsão e de apoio à decisão. A seguir (Tabela 2), sintetizamos as principais características de cada um desses modelos a partir das tecnologias de reconhecimento facial.

Tabela 2. Modelos de vigilância e de captura aplicados às tecnologias de reconhecimento facial

Dimensões de análise	**Modelo de vigilância**	**Modelo de captura**
Propósito	Prevenção e controlo, usando os dados para identificar comportamentos suspeitos ou criminais.	Organização e gestão de dados com base em padrões definidos, como identificação e categorização de pessoas através de características faciais.
Foco principal	Monitorização de comportamentos através de observação contínua.	Estruturação e categorização formal de atividades com base em regras e padrões.
Tipo de dados	Imagens e vídeos.	Dados faciais (por exemplo, geometria do rosto, cor da pele).
Tecnologia usada	Tecnologias que permitem observação direta; por exemplo, câmaras de vigilância espalhadas pela cidade, que gravam	Sistemas formais que capturam dados e os organizam em estruturas e classificações predefinidas, como reconhecimento facial em sistemas de segurança

	faces e monitorizam comportamentos sem necessariamente integrar os dados com outros sistemas.	em aeroportos; e que cruzam características faciais de indivíduos com informações previamente armazenadas.
Interoperabilidade	Frequentemente limitada a sistemas de vigilância locais.	Fortemente integrada com bases de dados externas e sistemas de segurança globais.
Modo de operação	Vigilância passiva, feita à distância e a partir da observação externa, recolhendo dados visuais ou comportamentais sem intervenção direta e frequentemente sem consentimento explícito.	Vigilância ativa, que organiza, rotula e interpreta dados dentro de um sistema predefinido, como estruturas de reconhecimento facial que categorizam características faciais, com consentimento ou processos formalizados para capturar dados.
Consentimento e transparência	Geralmente, sem que as pessoas tenham conhecimento de que estão a ser monitorizadas.	Alguns casos de consentimento formalizado (como em pontos de controlo de segurança), mas a transparência do processo é frequentemente limitada.
Implicações para a privacidade	Possibilidade de as pessoas não terem consciência de que estão a ser vigiadas.	Possibilidade de o uso de dados pessoais e sua categorização levar, por exemplo, a perfis e categorias discriminatórios.

Fonte: Sistematização inspirada em Agre, 1994, e Machado e Silva, 2025.

Não obstante as tecnologias de reconhecimento facial configurarem, na nossa perspetiva, de modo acentuado, a coexistência da captura e da vigilância, a literatura sobre as implicações sociais e éticas dessas tecnologias no sistema de justiça tem-se circunscrito ao modelo de vigilância, sendo ainda muito limitada a reflexão crítica no âmbito do modelo de captura. Avançamos, por isso, na próxima secção com uma análise mais detalhada das implicações sociais e éticas do modelo de captura, debruçando-nos sobre dois aspetos particulares associados às tecnologias de reconhecimento facial: por um lado, a metáfora da automatização da identificação; por outro, a construção de categorias que estruturam e classificam as faces enquanto superfícies de legibilidade e controle.

Implicações do modelo de captura: a emergência do tipo digital-criminal

A metáfora da automatização da identificação é, como refere Crawford (2024 [2021]), um dos argumentos mais frequentemente invocados para justificar a adoção de tecnologias de reconhecimento facial na segurança pública e no sistema de justiça.

A automatização nas tecnologias de reconhecimento facial constrói uma visão simplificada que captura e transforma a face. Aquilo que, no rosto, tradicionalmente veicula identidade e significado social, é transmutado em uma superfície quantificável e operável — uma face reduzida a dados. A automatização carrega consigo um poder de controle inscrito na própria ação de "ver": esta organiza o olhar e estrutura a categorização do visível. Por meio dessas tecnologias, o ato de ver uma face torna-se um ato político que distorce a relacionalidade sensível da visão (Plájas, 2023). Por outras palavras, reduz interações e interpretações complexas a binários simples, como "reconhecido" ou "não reconhecido", ou, pensando no caso concreto da identificação em contexto de sistema de justiça, "suspeito" ou "não suspeito", "criminoso" ou "não criminoso" e, neste processo, desconsidera o contexto social e a identidade pessoal. Este processo transforma a face em mero objeto, ignorando o seu papel como elemento de significado humano e relacional. A automatização da identificação, ao invés de ser neutra, cria uma representação distorcida do mundo ao abstrair os dados das realidades contextuais, relacionais e simbólicas; esta representação, porém, é frequentemente tratada como objetiva e verdadeira (Amoore, 2020).

Diferentemente da vigilância direta, o modelo de captura trabalha reorganizando as atividades humanas em dados que podem ser permanentemente armazenados, processados e utilizados para prever e controlar comportamentos futuros. Num contexto em que a captura e o processamento de dados biométricos são muitas vezes realizados sem transparência e supervisão e delegados em empresas privadas, o controlo democrático sobre essas tecnologias de reconhecimento facial afigura-se uma preocupação crucial. Isso torna-se especialmente problemático quando falamos de justiça preditiva

(Kaufmann *et al*., 2019), uma vez que esses sistemas passam a "prever" o comportamento humano com base em padrões extraídos de dados capturados, aumentando os riscos de reforçar determinismos pela associação de certos "perfis" a comportamentos criminais (Crawford, 2024 [2021]; Nieves Delgado, 2023).

Na nossa perspetiva, o policiamento preditivo associado ao uso de tecnologias de reconhecimento facial constitui um desdobramento dessas aplicações de tecnologias de captura, intensificando os desafios sociais e éticos. De facto, ferramentas de previsão de crimes baseadas em reconhecimento facial podem levar à rotulagem de indivíduos como "suspeitos" antes mesmo de qualquer infração ser cometida, desafiando o princípio da presunção de inocência. Essas previsões são geradas a partir de grandes volumes de dados – incluindo informações biométricas e dados demográficos – cruzados com perfis de comportamentos anteriores. Ao transformar esses dados em variáveis quantificáveis, o modelo de captura oculta ou invisibiliza os vieses que operam na recolha e interpretação dos dados, legitimando práticas potencialmente discriminatórias sob a alegação de objetividade técnica. Em suma, o processo de captura e reorganização de dados biométricos não altera apenas as práticas de vigilância e controlo, mas também a forma como os conceitos de "suspeito" e de "criminoso" são compreendidos e aplicados.

Importa, contudo, abordar estas metáforas e tendências de utilização de tecnologias de reconhecimento facial à luz da evolução histórica da criminologia. Se, no passado, a biologia e a criminologia se entrelaçaram na tentativa de criar classificações de criminosos com base nas suas características físicas (como no trabalho de Cesare Lombroso, que procurava identificar "criminosos natos" por características anatómicas) (Nieves Delgado, 2020; Kauffman e Vestad,

2023), mais recentemente a análise de dados genéticos e genómicos tem sido usada para tentar correlacionar predisposições genéticas e comportamentos, incluindo o crime (Kaufmann e Vestad, 2023). A análise de traços faciais por via de tecnologias de reconhecimento facial pode ser vista como uma continuação dessas tentativas de classificação na contemporaneidade, desta feita entrelaçando as ciências da computação e a criminologia através de tecnologias de IA. Enquanto o reconhecimento facial automatizado tenta capturar e classificar aquilo que aparece como "rosto" — transformando-o numa face codificável —, abordagens anteriores classificavam indivíduos com base em traços físicos ou predisposições biogenéticas. Apesar das mudanças tecnológicas, todas essas estratégias operam como mecanismos de controle que leem o corpo como índice de normalidade ou desvio.

Ao longo da história, diversas práticas de recolha de dados corporais (biológicos, anatómicos, genéticos, genómicos ou biométricos) contribuíram para a criação de “tipos corporais”, que posteriormente influenciaram julgamentos sobre predisposições para o crime (Machado e Granja, 2020; Vailly, 2024). A recolha de dados faciais nos atuais sistemas de segurança (como câmaras em espaços públicos ou aeroportos) segue uma lógica semelhante, em que a face é usado para tentar prever comportamentos (por exemplo, identificar criminosos ou pessoas com “potencial de risco”).

Com as tecnologias de reconhecimento facial, assistimos hoje a uma nova forma de “tipo corporal” no sistema de justiça – o “tipo digital”, no qual os traços faciais são analisados, categorizados e classificados para distinguir quem é “suspeito” ou “criminoso”, daqui emergindo o tipo digital-criminal.

Conclusão

O reconhecimento facial, quando analisado à luz do modelo de captura, revela como essas tecnologias não são meramente ferramentas neutras de identificação e de monitorização. Pelo contrário, participam ativamente na reorganização das relações sociais e na produção de novas formas de controlo associadas ao sistema de justiça, redefinindo não apenas os modos como suspeitos são identificados, mas também como o próprio conceito de suspeição é construído e aplicado. Esta representação do mundo, potenciada pela crença na objetividade e maior eficiência da IA e das tecnologias de reconhecimento facial, está associada a tentativas de afastamento da agência humana e tende a ignorar os efeitos subjetivos das pré-noções de suspeição que recaem sobre determinadas comunidades, um processo que é, aliás, conjuntamente elaborado por várias instâncias do sistema de justiça (Machado *et al*., 2020). Ignora, igualmente, que a política de classificação é uma prática central na IA, que tende a produzir resultados discriminatórios em matéria de raça, classe, género, deficiência ou idade, o que nos leva a questionar que teorias sociais e que políticas táticas lhe estão subjacentes e são respaldadas por estas classificações do mundo (Crawford, 2024 [2021]: 128-129).

O uso de reconhecimento facial para identificar suspeitos cria uma forma de "tipo" criminal baseado em características digitais (dados faciais), em vez de genéticas ou anatómicas, mas o princípio subjacente de vincular biologia a comportamentos criminais persiste (Nieves Delgado, 2020). Historicamente, a recolha de dados anatómicos ou genéticos tinha como objetivo o controlo social, por meio de perfis que associavam características físicas ou genéticas a

um maior risco de criminalidade. Assim como os métodos históricos de catalogação anatómica ou os mais recentes perfis genéticos foram usados para marginalizar e estigmatizar grupos, o reconhecimento facial levanta questões sociais e éticas semelhantes.

Em resumo, tanto as práticas históricas de criar "tipos anatómicos" quanto as tecnologias de reconhecimento facial compartilham uma lógica de controlo social por meio da recolha de dados biométricos. Ambas tentam mensurar características físicas e/ou digitais para identificar, categorizar e, em alguns casos, criminalizar indivíduos. No entanto, o reconhecimento facial contemporâneo acrescenta a camada de vigilância digital e a automação da captura de dados, potencializando o alcance e a influência desses sistemas no controlo social e na criação de "tipos" criminais ou comportamentais.

Ao automatizar e sistematizar a categorização de indivíduos, as tecnologias de reconhecimento facial reconfiguram profundamente as definições de suspeição e perigosidade, transformando-as em processos algorítmicos. Nesse cenário, a decisão humana, historicamente central nos julgamentos, é progressivamente substituída por uma lógica de eficiência técnica e tecnológica. A "facialidade produzida pela máquina", no sentido definido por Deleuze e Guattari (1987: 168), torna-se particularmente visível: os computadores não apenas capturam rostos humanos, mas os convertem em dados que são classificados de acordo com padrões e categorias predeterminados por instituições de poder. No sistema de justiça, isso traduz-se num enquadramento em que as faces são avaliadas com base em conceções estabelecidas sobre o que é considerado "normal" e "desviante" (Deleuze e Guattari, 1987: 182). Esse processo não só amplifica as capacidades de vigilância e controlo,

como também inaugura novas formas de biopoder, nas quais a vida e os corpos dos indivíduos são continuamente monitorizados, mediados e recriados por máquinas (Andrejevic *et al*., 2024).

Autores como Crawford (2024 [2021]) e Steven e Keyes (2021) salientam que o enfoque exclusivo nas críticas ao viés algorítmico tende a desviar a atenção da análise das práticas fundamentais de classificação que sustentam a IA e conduz a procurar soluções tecnológicas capazes de produzir "sistemas de IA mais justos" em vez de lidar com as estruturas sociais, políticas e económicas subjacentes. No contexto do sistema de justiça, isso é particularmente problemático, pois as classificações, uma vez incorporadas nas infraestruturas tecnológicas, tornam-se invisíveis, apesar de continuarem a moldar profundamente o mundo social e material (Bowker e Star, 1999). No caso do reconhecimento facial, essa situação pode significar a perpetuação de injustiças sistémicas, pois essas tecnologias tendem a reproduzir e amplificar os preconceitos raciais e sociais historicamente enraizados, legitimando-os sob a aparência de uma precisão algorítmica supostamente neutra (Crawford, 2024 [2021]: 129 e 137-140).

Em síntese, o uso de tecnologias de reconhecimento facial no sistema de justiça transcende uma simples questão técnica ou tecnológica; envolve consequências sociais, éticas e políticas complexas que exigem uma análise crítica sobre como esses algoritmos categorizam, julgam e afetam a vida das pessoas mais vulneráveis à discriminação e à criminalização. Num contexto onde as tecnologias de reconhecimento facial operam como ferramentas poderosas para a manutenção de regimes de controlo, a sua abrangência não se limita à captura e à vigilância, incluindo também a classificação e avaliação dos indivíduos dentro de uma estrutura

punitiva que perpetua relações de poder, discriminação e preconceitos históricos e institucionais. Enquanto essa estrutura punitiva ganha nova legitimidade, urge questionar, inadiável e urgentemente, o poder e as desigualdades que permeiam as nossas sociedades, revelando a necessidade de uma reflexão crítica sobre o impacto das tecnologias de reconhecimento facial na vida dos mais marginalizados que, invariavelmente, se cruzam com o sistema de justiça.

Agradecimentos

Este trabalho foi realizado com o apoio do projeto "fAICES – Facial Recognition Technologies. Etho-Assemblages and Alternative Futures", financiado pelo Conselho Europeu de Investigação (Grant n.º 101140664, ERC-2023-ADG). Agradecemos às colegas da Rede de Investigação em Ciências Sociais dedicada ao estudo da Inteligência Artificial, dados digitais e algoritmos (AIDA – Artificial Intelligence, Data & Algorithms), e, de um modo particular, a Rafaela Granja (CECS-ICS, Universidade do Minho) pelos comentários críticos a uma versão inicial deste artigo.

Referências bibliográficas

Agre, P. E. (1994). Surveillance and capture: Two models of privacy. *The Information Society*, 10(2), 101–127. https://doi.org/10.1080/01972243.1994.9960162

Allied Market Research (2023). Facial Recognition Market Size, Share, Competitive Landscape and Trend Analysis Report, by

Technology, by Application, by End User: Global Opportunity Analysis and Industry Forecast, 2022-2032. https://www.alliedmarketresearch.com/facial-recognition-market

Amoore, L. (2020). *Cloud Ethics: Algorithms and the attributes of ourselves and others*. Duke University Press. https://doi.org/10.1215/9781478009276

Andrejevic, M., O'Neill, C., Smith, G., Selwyn, N., & Gu, X. (2024). Granular biopolitics: Facial recognition, pandemics and the securitization of circulation. *New Media & Society*, 26(3), 1204-1226. https://doi.org/10.1177/14614448231201638

Aradau, C., & Blanke, T. (2022). *Algorithmic Reason: The new government of self and others*. Oxford University Press. https://doi.org/10.1093/oso/9780192859624.001.0001

Bakiner, O. (2023). The promises and challenges of addressing artificial intelligence with human rights. *Big Data & Society*, 10(2). https://doi.org/10.1177/20539517231205476

Bareis, J., & Katzenbach, C. (2022). Talking AI into being: The narratives and imaginaries of national AI strategies and their performative politics. *Science, Technology, & Human Values*, 47(5), 855-881. https://doi.org/10.1177/01622439211030007

Black, D. (2023). Facial analysis: Automated surveillance and the attempt to quantify emotion. *Information, Communication & Society*, 26(7), 1438-1451. https://doi.org/10.1080/1369118X.2021.2011948

Bowker, G., & Star, S. L. (1999). *Sorting Things Out: Classification and its consequences*. MIT Press. https://doi.org/10.7551/mitpress/6352.001.0001

Bueno, C. (2020). The face revisited: Using Deleuze and Guattari to explore the politics of algorithmic face recognition. *Theory, Culture & Society*, 37(1), 73–91. https://doi.org/10.1177/0263276419867752

Buolamwini, J. (2023). *Unmasking AI: My mission to protect what is human in a world of machines*. Random House.

Cabitza, F., Campagner, A., & Mattioli, M. (2022). The unbearable (technical) unreliability of automated facial emotion recognition. *Big Data & Society*, 9(2), 1-17. https://doi.org/10.1177/20539517221129549

Campolo, A., & Crawford, K. (2020). Enchanted determinism: Power without responsibility in artificial intelligence. *Engaging Science, Technology, and Society*, 6, 1-19. https://doi.org/10.17351/ests2020.277

Crawford, K. (2024 [2021]). *Atlas da IA: Poder, política e custos planetários da inteligência artificial*. Relógio D'Água.

Dauvergne, P. (2022a). *Identified, Tracked, and Profiled: The politics of resisting facial recognition technology*. Edward Elgar Publishing. https://doi.org/10.4337/9781803925899

Dauvergne, P. (2022b). Facial recognition technology for policing and surveillance in the Global South: A call for bans. *Third World Quarterly*, 43(9), 2325–2335. https://doi.org/10.1080/01436597.2022.2080654

Deleuze, G., & Guattari, F. (1987). *A Thousand Plateaus: Capitalism and schizophrenia*. University of Minnesota Press.

Ellerbrok, A. (2011). Playful biometrics: controversial technology through the lens of play. *Sociological Quarterly*, 52(4), 528–547. https://doi.org/10.1111/j.1533-8525.2011.01218.x

Gates, K. (2011). *Our Biometric Future: Facial recognition technology and the culture of surveillance*. New York University Press.

Gentzel, M. (2021). Biased face recognition technology used by government: A problem for liberal democracy. *Philosophy & Technology*, 34, 1639–1663. https://doi.org/10.1007/s13347-021-00478-z

Hupont, I., Tolan, S., Gunes, H., & Gomez, E. (2022). The landscape of facial processing applications in the context of the European AI Act and the development of trustworthy systems. *Scientific Reports*, 12, Article 10688. https://doi.org/10.1038/s41598-022-14981-6

Kaufmann, M., & Vestad, M. (2023). Biology and criminology: Data practices and the creation of anatomic and genomic body 'types'. *Critical Criminology*, 31, 1217–1232. https://doi.org/10.1007/s10612-023-09732-6

Kaufmann, M., Egbert, S., & Leese, M. (2019). Predictive policing and the politics of patterns. *The British Journal of Criminology*, 59(3), 674–692. https://doi.org/10.1093/bjc/azy060

Kaur, P., Krishan, K., Sharma, S., & Kanchan, T. (2020). Facial-recognition algorithms: A literature review. *Medicine, Science and the Law*, 60(2), 131-139. https://doi.org/10.1177/0025802419893168

Kloppenburg, S., & van der Ploeg, I. (2018). Securing identities: Biometric technologies and the enactment of human bodily

differences. *Science as Culture*, 29(1), 57-76. https://doi.org/10.1080/09505431.2018.1519534

Machado, H. (2025). Imaginários tecno-autoritários na América Latina: a contestação das tecnologias de reconhecimento facial. *Sociologia, Problemas e Práticas*, 107, 9-27.

Machado, H., Silva, S., & Neiva, L. (2023). Publics' views on ethical challenges of artificial intelligence: A scoping review. *AI & Ethics*. https://doi.org/10.1007/s43681-023-00387-1

Machado, H., Granja, R., & Amelung, N. (2020). Constructing suspicion through forensic DNA databases in the EU: The views of the Prüm professionals. *The British Journal of Criminology*, 60(1), 141–159. https://doi.org/10.1093/bjc/azz057

Machado, H., & Granja, R. (2020). *Forensic Genetics in the Governance of Crime*. Palgrave Macmillan. https://doi.org/10.1007/978-981-15-2429-5

Machado, H., & Silva, S. (2024). *Desafios Sociais e Éticos da Inteligência Artificial no Século XXI*. UMinho Editora. https://doi.org/10.21814/uminho.ed.130

Machado, H., & Silva, S. (2025). *Ethical Assemblages of Artificial Intelligence. Controversies, uncertainties, and networks*. Palgrave Macmillan. https://doi.org/10.1007/978-981-96-4158-1

Magnet, S. (2011). *When Biometrics Fail: Gender, race, and the technology of identity*. Duke University Press. https://doi.org/10.1215/9780822394822

Mayor, A. (2018). *Gods and Robots: Myths, machines, and ancient dreams of technology*. Princeton University Press.

Natale, S., & Ballatore, A. (2017). Imagining the thinking machine: Technological myths and the rise of artificial intelligence. *Convergence: The International Journal of Research into New Media Technologies*, 26(1), 3–18. https://doi.org/10.1177/1354856517715164

Nieves Delgado, A. (2020). Facial recognition technologies and the new physiognomic era. *Psychosozial*, 43(2), 45–56. https://doi.org/10.30820/0171-3434-2020-2-X

Nieves Delgado, A. (2023). Race and statistics in facial recognition: Producing types, physical attributes, and genealogies. *Social Studies of Science*, 53(6), 916–937. https://doi.org/10.1177/03063127221127666

Plájás, I. Z. (2023). InterFaces: On the relationality of vision, face, and race in practices of identification: A multimodal intervention. *Social Studies of Science*, 53(6), 938–953. https://doi.org/10.1177/03063127231151237

Sánchez-Monedero, J., & Dencik, L. (2020). The politics of deceptive borders: 'Biomarkers of deceit' and the case of iBorderCtrl. *Information, Communication & Society*, 25(3), 413–430. https://doi.org/10.1080/1369118X.2020.1792530

Schopmans, H., & Ebetürk, I. (2023). Techno-authoritarian imaginaries and the politics of resistance against facial recognition technology in the US and European Union. *Democratization*, 31(5), 943–962. https://doi.org/10.1080/13510347.2023.2258803

Sheikh, H., Prins, C., & Schrijvers, E. (2023). Artificial intelligence: Definition and background. In *Mission AI: The new system*

technology. Springer. https://doi.org/10.1007/978-3-031-21448-6_2

Søraa, R. (2023). *AI for Diversity*. Routledge.

Stevens, N., & Keyes, O. (2021). Seeing infrastructure: Race, facial recognition and the politics of data. *Cultural Studies*, 35(4-5), 833-853. https://doi.org/10.1080/09502386.2021.1895252

Vailly, J. (2024). *Genetics and the Politics of Security: A social science perspective*. Routledge Frontiers of Criminal Justice.