

Reconhecimento facial: erros expõem falta de transparência e viés racista.

A prisão de um homem em um estádio de futebol após ser detectado erroneamente por um sistema de reconhecimento facial da polícia de Sergipe levantou a discussão sobre o uso da tecnologia para prender pessoas. Entidades alegam que o sistema rompe direitos humanos básicos e coloca em risco grupos marginalizados.

O que aconteceu

A polícia prendeu erroneamente João Antônio Trindade. Ele acompanhava a final do Campeonato Sergipano entre Confiança e Sergipe, no último dia 13, quando foi abordado por agentes que o algemaram e o levaram para interrogá-lo em uma sala.

Trindade relata constrangimento. Nas redes sociais, ele questionou a atuação da polícia e disse ter chorado após a prisão. Após o erro durante a partida de futebol, o governo sergipano suspendeu o uso da tecnologia.

“Cinco policiais vieram e eu dei passagem para um lado. Eles vieram em minha direção mais ainda, até que o primeiro pegou no meu braço e disse para eu não reagir, me 'convidando' a acompanhá-los com as mãos para trás, como mostra no vídeo. Fiquei altamente constrangido, tentando esconder o meu rosto. Não sabia o que fazer, pois estava a torcida do Confiança inteira me olhando.”

- João Antônio Trindade, via redes sociais

Caso não foi isolado e já havia ocorrido em 2023, também em Sergipe. Ao UOL, a auxiliar administrativa Thais Santos, que é negra, comentou que foi a uma micareta, onde havia essas câmeras, e a polícia a abordou três vezes por indicação da tecnologia. Numa das situações, ela chegou a urinar na roupa pelo constrangimento.

“Eu já estava chorando e nervosa, informando que eu não tinha feito nada. Um dos policiais dizia que eu sabia o que tinha feito. No mesmo momento, eu urinei nas calças. Fui conduzida para o camburão da polícia como uma marginal, como todo mundo ali presenciando todo o constrangimento pelo qual eu estava passando. Nunca fui tão humilhada em minha vida, sem nunca ter feito nada de errado.”

- Thaís Santos, auxiliar administrativa

Sistema falho e com viés racista

Uso de câmeras de reconhecimento facial tem falhas. Na avaliação de Ana Gabriela Ferreira, professora de Direito Penal e Criminologia que pesquisa inteligência artificial e necropolítica, o sistema é repleto de vieses, sem dados concretos de sua eficiência.

Prisões indevidas e direitos violados. “Nas pesquisas iniciais do NIST (Instituto Nacional de Padrões e Tecnologia - ligado aos EUA) e do Gender Shades (organização ligada ao MIT), demonstraram-se erros de reconhecimento e falsos positivos com impacto absurdo em prisões indevidas e violações de garantias”, diz Ana Gabriela.

Racismo algorítmico. Tanto a professora quanto outros especialistas consultados pelo UOL apontam que um dos maiores problemas do reconhecimento facial é o viés racista por trás dos padrões adotados no método.

“Os riscos e os danos do uso de reconhecimento facial, especialmente para finalidade de segurança, geram risco à população não branca, incluindo negros, asiáticos, muçulmanos e outras minorias. Não é difícil entender o porquê.”

- Ana Gabriela Ferreira, professora de Direito Penal e Criminologia.

“Câmeras de reconhecimento em locais com maior circulação populacional. De acordo com Ana, os locais escolhidos para a vigilância expõem o racismo do sistema. Geralmente, elas são usadas em eventos de apelo popular, como o carnaval, ou em lugares em que pessoas abonadas pouco circulam, como rodoviárias. Negros são alvo prioritário do vigilantismo no país, incluindo as informações prévias dos sistemas policiais, maior parte da população inserida no sistema de buscas e a escolha dos locais de monitoramento selecionados, voltados a bairros onde há mais circulação e acesso da população negra. Se você estabelece a seleção dos lugares onde há monitoramento, está também selecionando os alvos daquela ferramenta.”

- Ana Gabriela Pereira, professora de Direito Penal e Criminologia

Juristas concordam com tendência racista. Representantes de grupos da sociedade civil que estudam o tema dizem que a tecnologia que abastece o sistema é desenvolvida a partir de crenças e bases de uma sociedade preconceituosa.

Como a inteligência artificial está sendo aplicada? Para Guilherme Cernelós, coordenador do IDDD (Instituto de Defesa do Direito de Defesa), seria importante entender exatamente quais tipos de algoritmo são usados no reconhecimento facial, bem como qual o impacto jurídico sobre possíveis direitos violados pelo método.

“Existe um sistema que é criado e administrado por pessoas brancas, então a gente tem algoritmos e programações de brancos, a administração dos órgãos é majoritariamente composta por brancos. A maior parte da população carcerária é negra e a maior parte dos brasileiros são negros, então eu tenho muitas dúvidas sobre a adoção. Ela vai ajudar como? Como eu, enquanto injustiçado, posso provar o contrário e me defender disso?”

- Guilherme Cernelós, coordenador do IDDD (Instituto de Defesa do Direito de Defesa).

Mais critérios para a comprovação de identidade. Na avaliação de Felipe Angeli, advogado e coordenador do Justa, deveria haver um padrão de contraprova para complementar o sistema de reconhecimento facial.

“No reconhecimento facial a gente está vendo erro, elas repetem vieses humanos, então a gente tem a IA racista. Acho que a tecnologia sempre pode ser utilizada para o bem da sociedade, agora no direito penal, algo tão importante como a justiça, a gente tem que ter muito cuidado. Tem que ter uma série de provas que corroborem de forma inequívoca.”

- Felipe Angeli, advogado e coordenador do Justa.

Falta de transparência

Estados decidem e definem o uso do reconhecimento facial. Para o uso mais amplo da tecnologia a serviço da segurança pública, os estados criam as próprias leis e aplicam o sistema. Contudo, os projetos de lei que regulam a inteligência artificial (PL 2338) e a LGPD Penal podem entrar no tema e estipular ou afrouxar regras para o uso.

Falta de dados e clareza na divulgação das informações. Organizações que fiscalizam os órgãos de segurança pública narram que nem por meio da Lei de Acesso à Informação conseguem os dados. Sem precisão sobre a quantidade de pessoas presas por engano da máquina, não é possível comprovar a eficiência do método, como aponta Pablo Nunes coordenador do Cesec (Centro de Estudos de Segurança e Cidadania).

“Acho que o problema é o conceito de "dar certo". Do ponto de vista de quem acredita que a segurança pública precisa garantir direitos, com respeito a todos, e pensar no bem-estar da população, nenhuma experiência de uso de reconhecimento facial chegou nesse lugar.”

- Pablo Nunes, coordenador do Cesec.

Bahia lidera prisões

Investimentos e prisões. Na Bahia, onde o sistema funciona desde 2019, 1523 pessoas foram presas com o auxílio do reconhecimento facial. O estado investiu mais de meio bilhão de reais na tecnologia.

Nível de eficiência incerto. De acordo com o Cesec, a Bahia é o estado com maior número de prisões por meio do sistema. No entanto, consultada pela reportagem, a Secretaria de Segurança Pública do estado não soube informar quantas vezes o sistema errou.

Ao UOL, a pasta informou que apenas são identificadas pessoas que estão no Banco Nacional de Mandados de Prisões

“A SSP adota um protocolo para os casos de Reconhecimento Facial. A tecnologia aponta semelhança a partir de 90%. Na sequência, as equipes de campo são acionadas. Após localizar o possível foragido, os policiais iniciam o processo de identificação humana, inicialmente com a checagem da documentação. Em caso de confirmação, aquela pessoa é apresentada na Delegacia, a validade do mandado é verificada e a Justiça informada.”

- Secretaria de Segurança Pública da Bahia, em nota.

Em Sergipe, o uso da tecnologia foi suspenso após os dois casos relatados no início desta reportagem. "Lamento a falha na ferramenta de reconhecimento facial ocorrida durante final do Campeonato Sergipano. Reconhecemos a importância da tecnologia para a segurança pública e, devido ao ocorrido, determinei a suspensão do uso do sistema até que novo protocolo seja implantado", disse o governador do estado, Fábio Mitidieri (PSD)

Caso Escolhido: Reconhecimento Facial

Análise e Reflexão sobre o Reconhecimento Facial

Com base na reportagem fornecida, é possível estruturar uma reflexão crítica sobre o uso da tecnologia de reconhecimento facial na segurança pública, utilizando frameworks de tomada de decisão para abordar questões éticas, sociais e de governança.

1 - Viés e Justiça:

- **Viés de dados e de algoritmo:** A reportagem aponta que a tecnologia de reconhecimento facial é "repleta de vieses". Especialistas consultados no texto afirmam que um dos maiores problemas é o "viés racista por trás dos padrões adotados no método". A tecnologia seria desenvolvida a partir das "crenças e bases de uma sociedade preconceituosa". Guilherme Carnelós, do IDDD, destaca que o sistema é "criado e administrado por pessoas brancas" e que as programações e algoritmos também são criados por brancos. Além disso, estudos do NIST e do Gender Shades já demonstraram erros de reconhecimento e falsos positivos. A advogada Ana Gabriela Ferreira também menciona que a ferramenta gera riscos para a "população não branca, incluindo negros, asiáticos, muçulmanos e outras minorias".
- **Grupos desproporcionalmente afetados:** A reportagem evidencia que grupos minoritários, principalmente a população negra, são desproporcionalmente afetados. A auxiliar administrativa Thaís Santos, que é negra, relata ter sido abordada três vezes pela polícia por indicação da tecnologia, chegando a urinar na roupa de constrangimento. A reportagem também menciona que as câmeras são usadas em locais com maior circulação da população negra, como eventos populares e rodoviárias, o que expõe o "racismo do sistema".
- **Distribuição de benefícios e riscos:** A tecnologia, conforme a reportagem, não promove uma distribuição justa de benefícios e riscos. Ao contrário, ela gera "risco à população não branca", causando prisões indevidas e violações de direitos. Os casos relatados de João Antônio Trindade e Thaís Santos demonstram os riscos de constrangimento e humilhação, além da possibilidade de prisão errônea.

2 - Transparência e Explicabilidade:

- **Transparência do sistema:** A reportagem aponta uma "falta de transparência" no uso do reconhecimento facial. Organizações de fiscalização não conseguem obter dados sobre o sistema, nem mesmo por meio da Lei de Acesso à Informação.
- **Explicabilidade da decisão:** Devido à falta de transparência, não é possível, a partir da reportagem, determinar por que uma decisão específica foi tomada. A Secretaria de Segurança Pública da Bahia, por exemplo, não soube informar quantas vezes o sistema errou.
- **Modelo "black box":** A falta de acesso a dados sobre a eficiência e os erros do sistema sugere que o modelo funciona como uma "black box". Para o coordenador do IDDD, Guilherme Carnelós, é fundamental entender quais tipos de algoritmos são usados e qual o impacto jurídico, levantando dúvidas sobre a possibilidade de uma pessoa provar sua inocência diante de um erro da tecnologia.

3 - Impacto Social e Direitos:

- **Impacto no mercado de trabalho e na autonomia:** A reportagem não detalha os impactos diretos no mercado de trabalho. No entanto, o uso da tecnologia afeta a autonomia e a liberdade de ir e vir das pessoas, uma vez que elas podem ser abordadas e presas sem motivo, como nos casos de João Antônio Trindade e Thaís Santos.
- **Direitos fundamentais:** A tecnologia, segundo entidades, "rompe direitos humanos básicos e coloca em risco grupos marginalizados". Os erros de reconhecimento resultam em "prisões indevidas e violações de garantias". Isso impacta o direito à liberdade, à dignidade, à privacidade e à não discriminação. A Lei Geral de Proteção de Dados (LGPD) pode ser aplicada, já que os dados biométricos são considerados sensíveis e devem ser tratados com cautela.

4 - Responsabilidade e Governança:

- **Ações da equipe de desenvolvimento:** A equipe de desenvolvimento do sistema de reconhecimento facial poderia ter agido de forma mais responsável. Em vez de simplesmente implantar o sistema, deveriam ter garantido que os dados de treinamento fossem representativos e que não perpetuassem preconceitos.
- **Princípios de "Ethical AI by Design":** A aplicação de princípios como a equidade, a transparência e a responsabilidade seria crucial. A equidade, por exemplo, exigiria testes rigorosos para garantir que o sistema não tivesse um "viés racista". A transparência exigiria que os dados sobre o desempenho do sistema, incluindo o número de erros, fossem públicos. A responsabilidade exigiria que houvesse um mecanismo claro de contestação de uma decisão do sistema.
- **Leis e regulações aplicáveis:** A reportagem menciona que os estados criam suas próprias leis para o uso da tecnologia. No entanto, a reportagem cita a LGPD Penal e o PL 2338 como regulações que podem entrar no tema. A reportagem também aponta que o sistema viola "direitos humanos básicos" e gera "violações de garantias", o que sugere a aplicabilidade de leis e normas que regem direitos constitucionais e civis. A necessidade de um padrão de contraprova para complementar o sistema de reconhecimento facial é citada por Felipe Angeli, advogado e coordenador do Justa.

Posicionamento

Com base na análise da reportagem, o sistema de reconhecimento facial, da forma como é utilizado atualmente, deveria ser redesenhado e aprimorado, mas com a suspensão do seu uso até que isso ocorra, como já fez o governo de Sergipe. A reportagem aponta que a tecnologia possui falhas, "viés racista" e gera violações de direitos fundamentais. Simplesmente aprimorar o sistema sem uma mudança profunda na sua concepção e governança seria insuficiente para resolver os problemas de viés e falta de transparência. Por outro lado, o banimento total seria uma medida extrema, ignorando o potencial da tecnologia para o bem da sociedade, desde que utilizada com os devidos cuidados.

Com base nessa posição, as seguintes recomendações práticas e concretas são propostas:

1. **Redesenho com foco em "Ethical AI by Design" e auditoria externa:** O sistema de reconhecimento facial deve ser completamente redesenhado desde suas fases iniciais, seguindo os princípios de "Ethical AI by Design". Isso significa que a equidade, a transparência e a responsabilidade devem ser priorizadas. Além disso, a tecnologia deve ser submetida a auditorias externas e independentes, com dados de acesso público, para comprovar sua eficiência e identificar vieses. Essas auditorias devem incluir testes com diferentes grupos étnicos e sociais para garantir que o sistema não seja "racista".
2. **Criação de um protocolo de validação humana e contraprova:** A tecnologia não deve ser usada como prova única para uma prisão. A Secretaria de Segurança Pública da Bahia, por exemplo, informou que, além de a tecnologia apontar 90% de semelhança, os policiais devem checar a documentação e só em caso de confirmação, a pessoa é conduzida à Delegacia. No entanto, casos como o de João Antônio Trindade e Thaís Santos mostram que esse protocolo falhou ou não foi seguido de forma adequada. Portanto, é essencial estabelecer um protocolo de validação humana robusto e claro, além de um padrão de contraprova que corrobore a identificação de forma inequívoca.
3. **Maior transparência e acesso à informação:** É crucial que o funcionamento do sistema seja transparente. As organizações de fiscalização devem ter acesso irrestrito aos dados de desempenho da tecnologia, incluindo a quantidade de falsos positivos e a taxa de erros. Essa transparência permite que a sociedade civil, especialistas e a própria justiça fiscalizem a ferramenta e garantam que ela não viole direitos fundamentais. A falta de transparência impede a comprovação da eficiência do método, como apontado pelo coordenador do Cesec, Pablo Nunes.