



A TRIÁDE DE RECONHECIMENTO FACIAL NA IDENTIFICAÇÃO HUMANA

The Face Recognition Triad for human identification

Tathiana Carla Honorato¹

RESUMO

A morfologia facial ganhou importância no âmbito da ciência forense, especialmente em processos comparativos para fins de identificação humana em investigações criminais. O presente estudo tem como objetivo avaliar a metodologia de comparação facial instituída, em 2019, pelo Instituto de Identificação do Paraná, que utiliza sistemas automatizados e examinadores faciais forense. Neste artigo, consideramos a implementação da *Triáde de Reconhecimento Facial*, ou seja, a combinação dos sistemas automatizados de inteligência artificial (IA), super-reconhecedores (SR) e examinadores faciais (EF), para oferecer um serviço público mais eficiente e reduzir a possibilidade de erros; destacando, ainda, aspectos positivos e vulnerabilidades dos *experts* envolvidos no processo de avaliação morfológica facial. Ao final, analisamos a possível colisão entre a necessidade de promover reconhecimento facial (para fins de segurança pública) e os direitos individuais à privacidade e à proteção de dados pessoais; oferecendo sugestões de procedimentos a serem adotados pelos órgãos de identificação, em atenção à interpretação oferecida pelo Supremo Tribunal Federal em casos relacionados à proteção de dados.

Palavras-chave: Reconhecimento Facial. Identificação Humana. Triáde de Reconhecimento Facial. FISWG. Lei Geral de Proteção de Dados (LGPD).

ABSTRACT

Facial morphology has gained importance in the field of forensic science, especially in comparative processes for human identification purposes in criminal investigations. The present study aims to evaluate the facial comparison methodology established in 2019 by the Paraná Identification Institute, which uses automated systems and forensic facial examiners. In this article, we consider the implementation of the *Facial Recognition Triad*, that is, the combination of automated artificial intelligence systems (AI), super-recognizers (SR) and facial examiners (EF), to offer a more efficient public service and reduce the possibility of errors; also highlighting positive aspects and vulnerabilities of the experts involved in the facial morphological evaluation process. In the end, we analyze the possible collision of the need to promote facial recognition (for public security purposes) and individual rights to privacy and the protection of personal data; offering suggestions for procedures to be adopted by the identification agencies, in view of the interpretation offered by the Brazilian Supreme Court in cases related to data protection.

Keywords: Facial recognition. Human Identification. Facial Recognition Triad. FISWG. General Data Protection Law (LGPD).

¹Especialista em Criminalística com Ênfase em Perícia Criminal pela Universidade Guarulhos (2017). Graduada em Direito, pela Faculdade Novo Ateneu de Guarapuava (2006). Técnica em Desenho Industrial, pelo Centro Federal de Educação Tecnológica do Paraná (CEFET/UTFPR, 1999). Papiloscopista Policial junto ao Instituto de Identificação do Paraná (IIPR/PCPR), desde 2009. E-mail: pp_tathianahonorato@ii.pr.gov.br.



1. INTRODUÇÃO

Com o intuito de avaliar a metodologia de comparação facial instituída, em 2019, no Instituto de Identificação do Paraná (IIPR) e oferecer um serviço público mais eficiente e com menor margem de erros, foram realizados estudos visando adequar o procedimento às normas internacionais e avaliar a implementação de uma nova etapa no processo atual de análise facial, por meio da inclusão de *experts* denominados super-reconhecedores (SR).

O estudo foi realizado nos anos de 2023-2024 e permitiu identificar três espécies de especialistas (ou *experts*) que promovem identificação facial, destacando seus pontos positivos e suas vulnerabilidades. Um sistema de identificação dotado dessas três classes profissionais é o que denominamos *Triade de Reconhecimento Facial*.

Reconhecer pessoas com base nas características de seus rostos representa um grande desafio diante das circunstâncias envolvidas no processo de comparação facial para fins de identificação humana, em especial se o reconhecimento for realizado em investigação criminal e instrução processual.

A disponibilidade de tecnologias mais acessíveis e o grande volume de videomonitoramento em locais públicos e privados se tornaram aliados das forças de segurança pública na prevenção e investigação de crimes. No ano de 2023, foram recebidos pelo IIPR trezentos e quarenta e três requisições (policiais e/ou judiciais) para realização de comparação facial, em investigações criminais; e foram obtidos duzentos e cinquenta e sete resultados positivos, que permitiram a identificação de pessoas suspeitas da prática de crimes no Estado do Paraná.

O impacto dessa revolução tecnológica digital traz consigo questionamentos sobre a constitucionalidade do reconhecimento facial, diante da colisão entre essa atividade forense e os direitos fundamentais à privacidade e à proteção de dados pessoais (previstos no art. 5º, inc. X e LXXIX, da Constituição de 1988) e sobre a legalidade das provas obtidas a partir do reconhecimento facial realizado por meio de sistemas automatizados de inteligência artificial (IA), diante das normas previstas na Lei Geral de Proteção de Dados (LGPD) e do entendimento adotado pelo Supremo Tribunal Federal (STF) em casos relacionadas à proteção de dados pessoais.

Aprimorar a metodologia de comparação facial utilizada pelos órgãos oficiais de identificação, com emprego de sistemas que combinem inteligência artificial (IA), super-



reconhecedor (SR) e examinador facial (EF), e adotar procedimentos que atendam aos pressupostos de validade exigidos pelo Supremo Tribunal Federal são necessidades destacadas neste estudo e que precisam ser incorporadas pelos Institutos de Identificação, de modo a proporcionar respostas válidas e efetivas, com maior precisão e segurança, em cumprimento ao dever de o Estado proporcionar segurança pública.

2. IDENTIFICAÇÃO FACIAL

O reconhecimento facial constitui atividade técnico-científica realizada para fins de identificação humana a partir da comparação dos elementos constitutivos da face, apresentados em imagens e/ou vídeos, visando estabelecer se a face questionada pertence (ou não) a uma determinada pessoa.

Três métodos de comparação facial são preconizados pelo *Facial Identification Scientific Working Group* (FISWG, 2019): sobreposição de imagens, análise morfológica e fotoantropometria. (i) A *sobreposição de imagens* consiste em promover a sobreposição de duas imagens alinhadas e compará-las visualmente. Esse método não deve ser utilizado como uma abordagem independente, apenas em conjunto com a análise morfológica. (ii) A *análise morfológica* é o método que permite a comparação facial por meio das características faciais e das particularidades das estruturas anatômicas de uma pessoa, imagem e/ou vídeo. Embora não exista um modelo universal e validado para classificar diferentes populações (fato que pode acarretar dificuldades em sua aplicação diante da diversidade étnica em nosso País), esse ainda é considerado o método mais confiável de reconhecimento facial. Por fim, a (iii) *análise fotoantropométrica* é o método que utiliza as medidas antropométricas faciais para estabelecer um padrão da face. Esse método, no entanto, não é recomendado, por exigir boa qualidade das imagens em análise, tornando o resultado altamente inseguro.

O FISWG preconiza que, dentre os métodos por ela mencionados, a *análise morfológica* da face é o método que possui menor interferência e fornece respostas seguras quando usado para fins de comparação facial.



2.1 Métodos de identificação facial

Dentre os métodos de comparação facial apontados pela literatura atual para o reconhecimento facial (acima mencionados), dois merecem destaque: a *análise fotoantropométrica* e a *análise morfológica*.

Um estudo sobre a estabilidade de medidas faciais realizado pela Fundação da Odontologia da USP/SP (FUNDECTO) afirma que referências métricas podem ser úteis para avaliação de crescimento, idade, sexo e ancestralidade, bem como um instrumento indicador da individualidade de dadas dimensões em uma específica população.

As referências métricas, no entanto, não são recomendadas para fins de comparação facial. Nesse sentido, Davis *et al.* (2010), ao analisarem a fotoantropometria assistida por computador, afirmam que “a verificação de identificação foi considerada não confiável, a menos que várias medições de distância e angulares de imagens de perfil e rosto inteiro fossem incluídas em uma análise”.

Assim, a *análise fotoantropométrica* não é recomendada como método para realizar comparação facial, uma vez que as imagens e/ou vídeos sob diferentes condições de iluminação, resolução e obstruções de informações, não são capazes de apresentar dimensões e proporções adequadas para eficácia desse método.

Por outro lado, a *análise morfológica* é o método mais confiável para comparar a face humana a partir de imagens e/ou vídeos. Essa análise é baseada na avaliação de correspondência entre características faciais (rosto, cabelo, testa, sobrancelhas, olhos, nariz, boca e queixo), estruturas anatômicas (como nariz ou orelha) e as particularidades desses componentes (quanto à forma, aparência, simetria, localização e proporção relativa, por exemplo), possibilitando identificar pontos de compatibilidade ou incompatibilidade facial para excluir ou confirmar a identidade da pessoa questionada.

Para realizar a análise morfológica no Brasil, os Institutos de Identificação seguem a metodologia internacional do FISWG, que desenvolve padrões de consenso, diretrizes e melhores práticas para comparação de características faciais humanas baseadas em imagens. O grupo é constituído por instituições renomadas de diversos países (Estados Unidos, Austrália, França, Canadá, Reino Unido, Holanda, Jamaica, Noruega, Inglaterra, Nova Zelândia, Suécia e Brasil). Dentre as instituições nacionais, merecem destaque a Universidade



de São Paulo (USP), o Instituto Nacional de Criminalística (INC) e o Instituto Nacional de Identificação (INI) do Distrito Federal.

As diretrizes do FISWG estão disponíveis ao público e fornecem recomendações para análise ética e legal de características faciais humanas, incluindo: contextualização da técnica, princípios de comparação, padronização da nomenclatura e áreas anatômicas de interesse, características do treinamento e indicação de fatores que influenciam no processo, tais como a idade e distorções de imagens, especificações para aquisição, implantação e uso de sistemas de reconhecimento facial.

Nas diretrizes também se encontram descritas as quatro etapas da metodologia, conhecida como método ACE-V (*Analysis, Comparison, Evaluation and Verification*), a ser empregada em exames faciais individuais: (1) *análise*: avaliação de uma imagem para determinar a adequação para comparação, incluindo a capacidade de discriminar características significativas; (2) *comparação*: exame de duas ou mais imagens para estabelecer semelhanças e diferenças, considerando estabilidades faciais; (3) *avaliação*: o *expert* avalia o valor dos detalhes observados durante as etapas de análise e comparação para chegar a um juízo de valor, e (4) *verificação*: etapa na qual as fases de análise, comparação e avaliação devem ser realizadas por um segundo *expert* independente, com o objetivo de ratificar (ou não) a *avaliação* oferecida pelo primeiro especialista. Nesta quarta fase, a verificação pode ser realizada de duas formas: (a) *verificação cega* – realizada sem conhecimento da opinião do primeiro especialista; ou (b) *verificação não cega* – realizada com conhecimento da opinião do outro especialista. As circunstâncias para esta verificação devem ser detalhadamente descritas (ou seja, justificadas) no laudo morfológico facial, como preveem as diretrizes do FISWG (2023).

Os componentes faciais humanos são multifacetados e, quando as condições das imagens permitirem, toda comparação morfológica facial deve considerar componentes, características e descritivos faciais: a pele, o contorno do rosto e da cabeça, a composição do rosto e da cabeça, o cabelo, a testa, as sobrancelhas, os olhos, as bochechas, o nariz, as orelhas, a boca, o queixo e a mandíbula, o pescoço, os pelos faciais, as linhas faciais, as cicatrizes, as marcas faciais e as alterações capazes de individualizar (FISWG, 2018).

Cada estrutura anatômica, assimetrias e instabilidades (em decorrência da idade, doenças, alterações perceptíveis de peso e modificações intencionais, por exemplo) também



devem ser avaliadas quando se trata de morfologia facial, vez que podem diferir em tamanho e forma, de acordo com a diversidade étnica e de gênero.

Outro ponto igualmente importante, a saber, é que a análise facial é altamente sensível à qualidade da imagem (tanto em fotografias quanto em vídeos); de modo que a perda de qualidade da imagem por obstruções de informações (como uso de bonés, capacetes, óculos, coberturas faciais e a pose do indivíduo em relação à câmera), distorções de perspectiva ou decorrentes da lente utilizada, artefatos de compressão (pixelização, por exemplo) e filtragem, iluminação (a sobre ou subexposição), sombras e falta de contraste, e a redução na resolução espacial são fatores que podem reduzir ou eliminar a visibilidade das características faciais. Como resultado, a capacidade de comparar duas ou mais imagens poderá ser reduzida e, assim, considerada inadequada como meio para a comparação facial. Neste caso, o FISWG (2021) recomenda que, toda vez que uma imagem ou vídeo necessite passar por processos de correção, o arquivo original seja armazenado (ou seja, preservado).

As diretrizes do FISWG, portanto, devem ser observadas por todos os *experts* que realizam comparação morfológica facial, sob pena de incorrerem em equívocos e prejudicarem o resultado da análise.

2.2 *Experts* ou especialistas em identificação facial

Em relação aos *experts* que realizam reconhecimento facial, Towler *et al.* (2023, p. 01) destacam três classes de especialistas, que emergem de distintas áreas do conhecimento: examinadores faciais (EF), super-reconhecedores (SR) e sistemas dotados de inteligência artificial (IA). Segundo os autores (Towler *et al.*, 2023, tradução pela autora):

A crescente dependência da sociedade no reconhecimento facial significa que esses erros estão sob maior escrutínio do que nunca, e necessitam de especialistas com precisão comprovada nessa tarefa desafiadora. Nos últimos anos, três tipos de "especialistas" em reconhecimento facial - examinadores forenses, super-reconhecedores e Redes Neurais Profundas - surgiram independentemente dos campos da ciência forense, psicologia e inteligência artificial, respectivamente. [...].

A combinação dessas três especialidades constitui a *Triade de Reconhecimento Facial*. Necessário, portanto, mencionar cada classe de *expert*, suas características, aspectos positivos e vulnerabilidades.



2.2.1 Inteligência artificial (IA)

Dentre as técnicas para promover a identificação facial, merece destaque o emprego da inteligência artificial (IA), igualmente conhecida como redes neurais artificiais (RNA).

Em publicação realizada pelo Parlamento Europeu (2020), atualizada em 2023, a inteligência artificial é considerada “A tecnologia que define o futuro”; e foi conceituada como a capacidade do sistema para reproduzir competências semelhantes às humanas, como é o caso do raciocínio, da aprendizagem, do planejamento e da criatividade.

As redes neurais artificiais não são necessariamente novas. Existem desde a década de 1950 e a unidade fundamental de uma rede neural artificial é um nó (ou neurônio matemático) que, por sua vez, é baseado no neurônio biológico. As conexões entre esses neurônios matemáticos também foram inspiradas em cérebros biológicos, especialmente na forma como essas conexões se desenvolvem ao longo do tempo com o *treinamento* da IA.

O processo de *treinamento* da IA envolve a coleta e a preparação dos dados, a escolha do modelo de inteligência artificial mais adequado e o refinamento gradual por meio de combinações entre neurônios matemáticos.

Segundo a *Data Science Academy* (2024), IA generativa é um subcampo da inteligência artificial que se concentra na criação de novos conteúdos, dados ou informações, a partir de um conjunto de entradas existentes. É um tipo de processo de *machine learning* (aprendizado da máquina) e *deep learning* (aprendizado profundo), que usa nós ou neurônios matemáticos interconectados em uma estrutura em camadas, que toma decisões de forma semelhante ao cérebro humano, para identificar fenômenos, avaliar opções e chegar a conclusões mais precisas com base nos dados de entrada.

Sistemas de reconhecimento facial baseados em IA generativa são capazes de adaptar seu comportamento, utilizando algoritmos por meio de uma análise dos efeitos anteriormente realizados, rastreando e mapeando padrões de uma face humana em formatos geométricos e algorítmicos, para então identificar suas características únicas; em especial: o contorno do rosto, a distância entre os olhos e o nariz, a profundidade, as marcas sinaléticas, os traços de aparência e até marcadores de expressão e emoção.

O sistema algorítmico não responde de forma definitiva (sim ou não), mas calcula a probabilidade que a nova imagem (imagem questionada) seja da pessoa cujo dado biométrico se encontra armazenado na base dos dados de entrada (imagem padrão).



2.2.2 Vulnerabilidades da inteligência artificial (IA)

Estudiosos e membros do FISWG não recomendam que a identificação facial humana seja realizada unicamente por meio de algoritmos pré-estabelecidos, sob pena de erros serem potencializados quando se utilizam apenas métodos automatizados, sem a verificação por *expert* humano.

De forma restritiva, afirmam Ramon *et al.* (2024, p. 143, tradução pela autora) que:

[...] o desejo relatado por transparência pode ser atendido [...] por meio da implantação de super-reconhecedores como profissionais de aplicação da lei exclusivamente e naturalmente capazes, que podem ser treinados no uso responsável de FRT (tecnologia de reconhecimento facial) de última geração e que podem agir dentro de uma estrutura legal clara e bem estabelecida que respeite os direitos fundamentais dos cidadãos.

Considerando, no entanto, que estudos realizados por Towler *et al.* (2023, p. 02) revelam que as três classes de *experts* “alcançaram níveis de precisão igualmente elevados”, acreditamos que a informação fornecida pelos sistemas de identificação dotados de IA deve, necessariamente, ser submetida à verificação (quarta fase do método ACE-V) por outra classe de *expert* humano, seja por um examinador facial (EF) ou super-reconhecedor (SR).

Nesse sentido, a exposição de motivos ao Projeto de Lei n.º 3069/2022, em trâmite no Congresso Nacional e que dispõe sobre o uso de tecnologia de reconhecimento facial automatizado no âmbito das forças de segurança pública, recomenda a “verificação final dos resultados apontados pelo sistema por um examinador humano”:

Conforme uma análise técnica restritiva, um sistema de reconhecimento facial (RF) é meramente um filtro de faces. Nesse sentido, deve haver necessariamente a revisão facial, ou seja, a verificação final dos resultados apontados pelo sistema por um examinador humano. Recomenda-se que o examinador tenha aptidão para identificar faces, boa memória fotográfica, além de capacitação específica em reconhecimento facial. Ademais, a literatura internacional recomenda treinamentos periódicos a fim de avaliar a capacidade do operador para identificar corretamente uma face e melhorar suas habilidades para operar sistemas biométricos faciais.

Vale destacar, em seguida, as outras duas classes de especialistas em identificação facial, denominados super-reconhecedores (SR) e examinadores faciais (EF).



2.2.3 Super-reconhecedores (SR)

O psicólogo Richard Russell, durante um estudo sobre *prosopagnosia*, na Universidade Harvard em 2006, identificou e passou a estudar um grupo de pessoas que possuem habilidades extraordinárias para reconhecer rostos.

Neste contexto, importante fazer alusão à doença denominada *prosopagnosia*, por corresponder ao extremo oposto da habilidade humana apresentada pelos super-reconhecedores.

Em matéria publicada por Putini em 2022, o neurologista Leonardo de Souza Bernardes (do Hospital Albert Sabin) afirma que a *prosopagnosia* é uma alteração da percepção, da capacidade de reconhecer e interpretar o significado de algum estímulo sensorial. Um dos tipos da doença, a *prosopagnosia visual* ou *cegueira facial*, é a incapacidade de reconhecer objetos ou outras pessoas visualmente.

Assim, *prosopagnosicos* não conseguem afirmar se já viram um rosto antes. Trata-se de uma deficiência que afeta tanto rostos bem conhecidos por eles, quanto aqueles vistos uma única vez.

Em contraposição, os super-reconhecedores são pessoas que possuem uma habilidade inata (base genética) de reconhecer rostos e armazenar esta informação a curto e longo prazo. Josh P. Davis, professor de psicologia aplicada na Universidade de Greenwich na área de Identificação Facial, define super-reconhecedores como sendo (tradução pela autora):

Indivíduos excepcionalmente bons em reconhecer rostos. Atualmente, não há evidências de que os super-reconhecedores sejam qualitativamente diferentes da população em geral – em outras palavras, não há indicação de que seus cérebros sejam de alguma forma conectados de forma diferente. Em vez disso, suas habilidades parecem estar no extremo superior de um amplo espectro de diferenças individuais na capacidade de reconhecimento facial.

Não há uma informação oficial, mas algumas pesquisas (por exemplo, Cambridge Face Memory Test (CFMT), Russell *et al.*, 2009) sugerem que apenas 2% da população possui tamanha destreza. Segundo Towler *et al.* (2023, p. 02, tradução pela autora):

Embora a grande maioria das pessoas seja propensa a erros ao identificar rostos desconhecidos, os psicólogos identificaram uma pequena proporção da população - conhecida como super-reconhecedores - que atinge níveis extraordinários de precisão sem qualquer formação ou experiência específica. Os super-reconhecedores representam a cauda superior de um continuum de variação natural na capacidade



das pessoas de identificar rostos, que parece ser fortemente hereditária. Como resultado, os psicólogos argumentaram que os super-reconhecedores fornecem um caminho para altos níveis de precisão no desafio de tarefas de identificação de rostos desconhecidos do mundo real, e algumas organizações policiais recrutam super-reconhecedores para tarefas de identificação de rostos.

De acordo com estudo da Universidade de New South Wales, em parceria com a Universidade de Wollongong (ambas na Austrália), “os super-reconhecedores olham para os rostos da mesma forma que qualquer outra pessoa – mas o fazem mais rápido e de maneira mais precisa” (Saba, 2022).

2.2.4 Quem pode ser considerado super-reconhecedor (SR)?

Segundo Davis (2019), para ser considerado um super-reconhecedor (de acordo com os testes da Universidade de Greenwich), normalmente é necessário que um participante obtenha uma pontuação consistente dentro da faixa típica de super-reconhecedor em uma bateria de 10 (dez) ou mais testes faciais multiétnicos, em que são avaliadas quatro capacidades:

- a) *aprendizagem e reconhecimento presencial de curto prazo*: distribuídos em quatro testes, os participantes visualizam uma sequência de rostos e são desafiados a identificá-los, posteriormente, a partir de diferentes imagens;
- b) *correspondência facial simultânea*: quatro testes empregam *designs* diferentes com qualidade de imagem variável, incluindo fotos de alta qualidade com enquadramento fechado (mostrando apenas uma parte da face), imagens do tipo CCTV (circuito interno de televisão) e imagens do tipo passaporte com até 10 anos de intervalo;
- c) *memória facial de longo prazo*: neste teste, os participantes assistem a 10 vídeos de diferentes atores-alvo durante um minuto cada e, após um intervalo mínimo de sete dias, retomam o teste para identificar os alvos selecionados, e
- d) *teste de identificação de um rosto na multidão*: neste teste, os participantes recebem quatro imagens de oito atores diferentes e são solicitados a localizá-los, quase sempre vestidos de forma diferente, em vídeos que contemplam diversos cenários (em locais que retratam pontos turísticos, ambientes escuros ou com objetos cobrindo a face, por exemplo).



Testes de memória (de curto e longo prazo) e correspondência simultânea de rostos são atualizados regularmente com a finalidade de estabelecer limiares de identificação facial e refinar as habilidades dos SR, simulando obstruções por meio de imagens e/ou vídeos em diversos cenários.

2.2.5 Vulnerabilidades e cautelas necessárias

Embora as conclusões oferecidas pelos super-reconhecedores apresentem alto grau de acerto, Towler *et al.* (2023, p. 01) ressaltam a necessidade de cautela, porque “os super-reconhecedores eram rápidos, tendenciosos para responder ‘mesma pessoa’ e identificar erroneamente pessoas com extrema confiança”. Resumindo o estudo, Towler *et al.* (2023, p. 02, tradução pela autora) esclarecem que:

Para resumir nossos principais resultados relatados abaixo, encontramos diferenças marcantes entre a experiência em reconhecimento facial dos examinadores forenses, dos super-reconhecedores e das Redes Neurais Profundas (DNNs), apesar de alcançarem níveis de precisão igualmente elevados. A expertise dos super-reconhecedores é caracterizada por decisões rápidas tomadas com elevada confiança e uma tendência de resposta relativamente forte para dizer “a mesma pessoa” – o que poderia levar a erros de identificação com resultados catastróficos em ambientes forense. Os examinadores forenses, por outro lado, tomam decisões lentas e cuidadosas, mostram um viés de resposta neutro e moderam estrategicamente os seus índices de confiança. Redes Neurais Profundas (DNNs) mostram divergência adicional de ambos os grupos de especialistas humanos na forma como calculam a similaridade facial.

Finalmente, mostramos que aproveitar a diversidade entre esses grupos fornece um método robusto para maximizar a precisão do reconhecimento facial. Mostramos que isso pode ser alcançado por meio da colaboração em laboratórios forenses ou pela fusão estatística de respostas de diversos tipos de especialistas em reconhecimento facial.

Regressando às diretrizes do FISWG, faz-se necessário lembrar que a *avaliação* realizada por super-reconhecedores também precisa ser submetida à *verificação* (quarta fase do método ACE-V) por outro *expert* humano, ou seja, por um examinador facial (EF).

Nesse caso, acreditamos que a *verificação cega* (mencionada no item 2.1.) seja o procedimento mais adequado, para evitar que a avaliação do super-reconhecedor (SR) influencie a conclusão exposta na verificação do examinador facial (EF).



2.2.6 Examinadores faciais (EF)

A terceira classe de *experts* ou especialistas em identificação facial é constituída por examinadores faciais ou examinadores forense (EF).

Ao início, faz-se necessário salientar que, ao contrário dos super-reconhecedores (SR), os examinadores faciais ou examinadores forense não detêm uma habilidade inata de reconhecer rostos humanos. Essa capacidade pode ser adquirida e desenvolvida, até certo ponto, por meio de treinamento, variando de pessoa para pessoa. Sobre essa classe de especialistas, Towler *et al.* (2023, p. 01) esclarecem que:

Na ciência forense, os profissionais conhecidos como examinadores forense faciais identificam pessoas de interesse em investigações policiais e casos suspeitos de fraude de identidade em procedimentos de identificação governamentais. A ciência forense da comparação de imagens faciais faz parte de uma disciplina mais ampla de métodos de comparação de características que receberam um escrutínio científico significativo nos últimos anos. A falta de evidências da fiabilidade destes métodos levou a apelos da Academia Nacional de Ciências, de influentes comitês consultivos do governo dos EUA e de outros para estudos de validação e medição de taxas de erro. Em resposta a este apelo, estudos recentes mostraram que os examinadores forense superaram os grupos de participantes padrão em tarefas de identificação de rostos desconhecidos. As evidências sugerem que os peritos forense adquirem os seus conhecimentos por meio de formação profissional, prática deliberada e experiência.

Considerações relevantes apontadas por Towler *et al.* (2023, p. 02) reforçam que, diferentemente da tendência de autoconfiança extrema do super-reconhecedores, “os examinadores forenses tomam decisões lentas e cuidadosas, mostram um viés de resposta neutro e moderam estrategicamente os seus índices de confiança”.

Examinadores faciais são servidores públicos, ligados aos órgãos de Segurança Pública, com atribuição para realizar perícia em identificação humana por meio de técnicas de reconhecimento facial, em que são analisadas correspondências ou dissimilaridades entre rostos e/ou imagens.

O art. 5º, do Projeto de Lei n.º 3069/22, dispõe que “toda e qualquer sinalização de identificação positiva, a partir do uso de sistemas de reconhecimento facial, deverá ser confirmada por agente público responsável”.

No âmbito do Estado do Paraná, o perfil profissiográfico do Papiloscopista Policial se encontra previsto na Lei Complementar n.º 259/2023, que dispõe sobre a estrutura



organizacional das carreiras da Polícia Civil do Estado do Paraná, e confere ao Papiloscopista Policial a função de realizar Perícia de Reconhecimento Facial.

No mesmo sentido, o parágrafo único, do art. 5º, do Projeto de Lei n.º 3069/22, atribui ao Perito Papiloscopista, como especialista em identificação facial, a função de confirmar a identificação facial realizada por meio de sistema automatizado, quando houver restrição à liberdade de ir e vir de qualquer cidadão.

Desta forma, além da capacitação específica na área de comparação e identificação facial, é necessário que o examinador facial apresente aptidão e seja constantemente estimulado a se aprimorar por meio de cursos; bem como ser avaliado periodicamente quanto à sua memória fotográfica e processamento visual para rostos, a fim de avaliar sua capacidade de identificar uma face.

Embora o art. 159, *caput*, do Código de Processo Penal (CPP), permita que as perícias sejam realizadas por apenas um perito oficial, sustentamos que a identificação facial pelos especialistas da *Triade de Reconhecimento Facial* deve observar as diretrizes do FISWG e as quatro fases da metodologia ACE-V (*Analysis, Comparison, Evaluation and Verification*), de modo a submeter a *avaliação* do primeiro *expert* à *verificação* de um segundo especialista humano com habilitação técnica em comparação facial.

Assim, recomendamos que a análise não seja realizada por um único profissional em reconhecimento facial e que, em atenção às fases da metodologia ACE-V e das diretrizes do FISWG, faz-se necessário que a *avaliação* realizada pelo examinador forense também seja submetida à *verificação* de outro *expert* humano, seja examinador facial (EF) ou super-reconhecedor (SR).

3. VULNERABILIDADE DOS ATUAIS SISTEMAS DE RECONHECIMENTO FACIAL – CASOS REAIS

As recentes falhas nos sistemas de reconhecimento facial dotados de IA, no Brasil, acendem o alerta sobre os riscos da utilização desta tecnologia de forma isolada (sem a necessária *verificação* por um *expert* humano), diante das garantias trazidas pela Emenda Constitucional n.º 115/2022, que elevou a proteção de dados pessoais à categoria de direito fundamental (art. 5º, inc. LXXIX, da Constituição de 1988), e das normas previstas na Lei n.º 13.709/2018 (denominada *Lei Geral de Proteção de Dados Pessoais* - LGPD).



Casos emblemáticos, como o do *personal trainer* preso por engano em um estádio de futebol, no estado de Sergipe; do vigilante preso durante uma festa junina, em Salvador; da auxiliar administrativa identificada, por duas vezes, como foragida da Justiça, em Aracaju, e até o ator norte-americano Michael B. Jordan (que interpretou o vilão Erik Killmonger no filme *Pantera Negra*, produzido pela Marvel Studios em 2018) foi apontado como um dos suspeitos na chacina de Sapiiranga, em Fortaleza, apontam inconsistências na verificação dos sistemas de reconhecimento facial baseados em IA, sem a verificação final por um *expert* humano (seja, por SR ou EF).

Nesse mesmo contexto, o Instituto Brasileiro de Defesa do Consumidor (IDEC) propôs Ação Civil Pública contra o sistema de câmeras com tecnologia de reconhecimento facial implantado no Metrô de São Paulo, arguindo violação do direito à privacidade da imagem e à liberdade de informação dos usuários do sistema metroviário. Sustenta o IDEC que o sistema capturava emoções, gênero e faixa etária das pessoas que circulavam pelas estações em determinados locais e horários, para fins publicitários e comerciais, sem comunicação (prévia ou posterior) sobre a captação e/ou o uso das imagens. O questionamento, neste caso, volta-se ao uso da tecnologia de Reconhecimento Facial, sem o conhecimento ou consentimento dos usuários do metrô, o que pode representar ameaça à privacidade, à liberdade individual e ao direito fundamental à proteção de dados, expressamente previsto no art. 5º, inc. LXXIX, da Constituição de 1988.

Uma discussão sobre privacidade e vigilância em segurança digital se faz necessária. No item 4, *infra*, o tema será tratado em nível constitucional, destacando a interpretação e os pressupostos de validade oferecidos pelo Supremo Tribunal Federal.

3.1. Riscos dos atuais sistemas de reconhecimento facial

Nenhum sistema pode ser considerado 100% seguro. Sempre há margem de erro nos sistemas e nas decisões humanas. O meio de reduzir as falhas de cada um é promover a integração dos especialistas, de modo que o resultado da pesquisa pelos sistemas dotados de IA seja revisto por SR e/ou EF, e que a *verificação* (quarta fase do método ACE-V) das análises realizadas por SR sejam igualmente analisadas por EF. Neste sentido, Towler *et al.* (2023, p. 07) afirmam que “A precisão ideal no reconhecimento facial é alcançada por meio da agregação de respostas de diversos especialistas”.



Sistemas de Reconhecimento Facial, baseados em IA, consistem na interligação entre características do rosto de uma pessoa e a base de dados de registro, analisando pontos faciais equidistantes entre si e calculando a probabilidade daquela face ser da pessoa cadastrada no banco de dados.

Importante ressaltar que a possibilidade de haver diferenças ou modificações nessas distâncias morfológicas são bem maiores do que em uma impressão digital, por exemplo, já que a imagem pode sofrer diversas alterações conforme condições ambientais e técnicas, como já mencionado no item 2, *supra*.

No Brasil, em 2019, passou-se a usar o reconhecimento facial na segurança pública. Estudo realizado pela Rede de Observatórios de Segurança (OSP), no entanto, afirma que a ferramenta de reconhecimento facial tem sido ineficiente e tendenciosa na prisão de negros.

Segundo o relatório (Nunes, 2019), durante o carnaval da Bahia, o sistema de videomonitoramento com utilização de 100 câmeras capturou os rostos de mais de 1,3 milhões de pessoas, gerando 903 alertas às unidades policiais, o que resultou no cumprimento de 18 mandados e na prisão de 14 pessoas. Monitorando 151 casos de prisões nos Estados da Bahia, Rio de Janeiro, Santa Catarina e Paraíba, o relatório afirma que 90,5% das pessoas presas pelo uso da tecnologia eram negras e 9,5% eram brancas.

De acordo com o relatório da organização britânica *Big Brother Watch* (BBW), 95% das correspondências feitas por reconhecimento facial resultaram em indicação incorreta de pessoas inocentes (Carlo, 2018).

Nos EUA, um projeto de lei junto ao Senado limita o uso da tecnologia de reconhecimento facial por agências federais; mas, ao mesmo tempo, permite que seja utilizado sem prévia decisão judicial (S2878, 2019).

Em 2020, no estado de Washington, foi aprovada uma lei que permite o uso desta tecnologia por agências governamentais estaduais e aponta a necessidade de revisão humana nos casos em que os direitos fundamentais estejam em risco. Do texto legal (SB 6280, 2019-2020, p. 03 e 08, tradução pela autora), destacam-se as normas previstas nas seções 2 e 7:

Seção 2. “Revisão humana significativa” significa revisão ou supervisão por um ou mais indivíduos treinados de acordo com a seção 7 deste ato e que têm autoridade para alterar a decisão sob revisão. [...].

Seção 7. Uma agência governamental estadual ou local que usa um serviço de reconhecimento facial deve conduzir treinamento periódico de todos os indivíduos que operam um serviço de reconhecimento facial ou que processam dados pessoais



obtidos do uso de um serviço de reconhecimento facial. O treinamento deve incluir, mas não se limitar a, cobertura de: (1) Os recursos e limitações do serviço de reconhecimento facial; (2) Procedimentos para interpretar e agir sobre a saída do serviço de reconhecimento facial; e (3) Na medida aplicável ao contexto de implantação, o requisito de revisão humana significativa para decisões que produzem efeitos legais em relação a indivíduos ou efeitos igualmente significativos em relação a indivíduos.

Normas regulatórias sobre o uso de sistemas biométricos ainda precisam ser implementadas no Brasil. Um amplo debate sobre cadeia de custódia (art. 158-A a 158-F, do CPP) e procedimentos para promover a captura, armazenamento e compartilhamento das imagens, bem como o período pelo qual poderão ser monitoradas e utilizadas em investigações criminais, merece ser conduzido com o objetivo de proteger o interesse coletivo, em especial a segurança pública (por se tratar de direito coletivo expressamente previsto no art. 144, da Constituição de 1988) e, ao mesmo tempo, respeitar os direitos individuais igualmente previstos em nível constitucional.

4. SEGURANÇA PÚBLICA E A IMPORTÂNCIA DE PRESERVAR OS DIREITOS FUNDAMENTAIS

A expressão *"A tecnologia move o mundo"*, de Steve Jobs (um dos fundadores da Apple), revela o impacto que a tecnologia vem causando na sociedade nas últimas duas décadas.

Dispositivos cada vez mais interconectados trouxeram transformações significativas para o dia a dia das pessoas, como por exemplo: a automação industrial; o acesso à informação em tempo real; a chegada das redes sociais, que revolucionaram a forma como as pessoas se comunicam, se aperfeiçoam e se inter-relacionam; a robótica e a inteligência artificial, com a promessa de expandir nossas capacidades e nos tornar melhores naquilo que fazemos.

Segundo Mikhail Cancelier (2016, p. 62), em Tese de Doutorado para obtenção de titulação perante a UFSC, em 2016:

Com o alto nível (quantitativo e qualitativo) de informações circulando e com o maior interesse das pessoas por tais informações, as definições sobre o que se transmite, como se transmite e para quem se transmite tornam-se ainda mais complexas. Ao mesmo tempo em que se percebe a intensificação do movimento jurídico de busca por compreender e proteger essas informações, verifica-se o aumento da ingerência a elas. Seja por parte do próprio indivíduo, do Estado ou de



corporações privadas, num mundo repleto de novas tecnologias, o desrespeito à privacidade é uma das marcas do século XX.

O impacto dessa revolução tecnológica digital traz consigo questionamentos sobre a constitucionalidade do reconhecimento facial, diante da possibilidade de colisão dessa atividade forense com os direitos fundamentais à privacidade e à proteção de dados pessoais (previstos no art. 5º, inc. X e LXXIX, da Constituição de 1988), e sobre a legalidade das provas obtidas a partir do reconhecimento de uma pessoa como suspeita da prática de crime, diante das normas previstas na LGPD e da interpretação do STF.

4.1 Colisão entre privacidade e informação necessária à segurança pública

A Lei Geral de Proteção de Dados (LGPD) surge como um pêndulo capaz de ponderar e normatizar a utilização de dados sensíveis, com o objetivo de proteger os direitos fundamentais à privacidade e ao livre desenvolvimento da personalidade da pessoa natural. Segundo Camila Cristo, em Dissertação de Mestrado defendida perante a UFSC, no ano de 2021, a privacidade pode ser definida como “um limite ao direito à informação, um respeito à liberdade do indivíduo de escolher com quem compartilha sua vida privada e sua intimidade” (2021, p. 68).

Não se pode, no entanto, confundir privacidade e dados pessoais, em especial porque alguns elementos identificados como dados não se encontram na esfera da vida privada, e sim na esfera da segurança pública, que constitui “dever do Estado, direito e responsabilidade de todos” (art. 144, *caput*, da Constituição de 1988). Em relação à distinção entre esses institutos, destaca-se a exposição de Camila Cristo (2021, p. 207):

Comparamos os conceitos de proteção à privacidade e a proteção de dados pessoais. Averiguamos que são institutos que protegem coisas distintas. A privacidade visa a interromper/barrar o fluxo da informação, diferentemente da proteção de dados pessoais, que visa a controlar esse fluxo informacional, porém permitindo que ele flua. A proteção de dados está relacionada com controle informacional, é uma proteção procedimental. Proteção de dados diz respeito a diretrizes, os modos de tratamento, o processamento de dados, logo a proteção de dados permite o fluxo informacional. No entanto, esse fluxo deve ser regulado de modo a promover responsabilidades públicas significativas para os agentes que tratam dados pessoais. Por fim, percebeu-se que privacidade e dados pessoais, apesar de distintos em vários pontos, possuem algumas semelhanças, de modo que há uma zona de intersecção entre os conceitos de privacidade e dados pessoais.

Há, portanto, dois direitos fundamentais que podem entrar em colisão durante o



procedimento de reconhecimento facial: o direito individual à proteção dos dados pessoais (inicialmente reconhecido no julgamento da Ação Direta de Inconstitucionalidade n.º 6.387, perante o Supremo Tribunal Federal, no ano de 2020; e incorporado ao rol de direitos fundamentais no art. 5º, inc. LXXIX, por meio da Emenda Constitucional n.º 115/2022) e o direito coletivo à segurança pública, que impõe ao Estado o dever de investigar e combater a prática de crimes.

A proteção de dados pessoais, no Brasil, se encontra atualmente regida pela LGPD, que “dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural” (art. 1º), e oferece conceitos essenciais à compreensão do tema, em especial a distinção entre *dados pessoais* e *dados pessoais sensíveis*:

Art. 5º. Para os fins desta Lei, considera-se:

I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Os *dados pessoais sensíveis* constituem o núcleo de proteção legal, pois a divulgação inadequada ou não autorizada dessas informações pode acarretar violação ao direito fundamental à intimidade e à privacidade.

De outra sorte, alguns dados pessoais, em especial quando relacionados à identificação da pessoa para fins de segurança pública, não se encontram abrangidos no conceito de dados sensíveis e, desse modo, não integram o conceito de intimidade, tampouco ingressam na esfera de proteção dos direitos fundamentais previstos no art. 5º, inc. X e LXXIX, da Constituição de 1988.

Nesse sentido, a LGPD (em seu art. 4º, inc. III) expressamente afasta sua aplicação nas hipóteses de tratamento de dados pessoais quando realizado para fins exclusivos de segurança pública, defesa nacional ou atividades de investigação e repressão de infrações penais.

A não incidência da LGPD, no entanto, não autoriza o uso abusivo ou indiscriminado das imagens pelos órgãos de segurança pública. Faz-se necessário ponderar os direitos



fundamentais que poderão entrar em colisão, durante a realização da atividade forense de comparação facial.

4.2. Ponderação entre interesse público e direito à privacidade e proteção de dados

A necessidade de promover ponderação entre direitos fundamentais em colisão (ou conflito) é tema sedimentado na doutrina constitucional. Segundo Canotilho (1999, p. 1191), “considera-se existir uma *colisão autêntica de direitos fundamentais* quando o exercício de um direito fundamental por parte do seu titular colide com o exercício do direito fundamental por parte de outro titular.” Para a solução do conflito, leciona José Carlos Vieira de Andrade (1987, p. 221):

A solução dos conflitos e colisões não pode ser resolvida com o recurso à ideia de uma ordem hierárquica dos valores constitucionais. Não se pode sempre (ou talvez nunca) estabelecer uma hierarquia entre os bens para sacrificar os menos importantes. Os próprios bens da vida e integridade pessoal, que o n.º 4 do art. 19. parece positivamente considerar como bens supremos, podem ser sacrificados, total ou parcialmente (basta lembrar, em geral, os casos de rapto em que os Governos se recusam a negociar com os terroristas e proíbem até as famílias de satisfazerem os pedidos de resgate). Não pode, além disso, ignorar-se que, nos casos de conflito, a Constituição protege os diversos valores ou bens em jogo e que não é lícito sacrificar pura e simplesmente um deles ao outro.

A Declaração Universal dos Direitos Humanos (DUDH), de 1948, prevê em seu art. 12 que “Ninguém será sujeito à interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques”.

A Convenção Americana sobre os Direitos Humanos (CADH), conhecida como Pacto de San José de Costa Rica, de 1969, dispõe em seu art. 11, itens 2 e 3 sobre “Proteção da honra e da dignidade”, afirmando que:

2. Ninguém pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada, na de sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra ou reputação.
3. Toda pessoa tem direito à proteção da lei contra tais ingerências ou tais ofensas.

Diante da possibilidade de colisão entre os direitos individuais à privacidade e à proteção de dados em relação ao direito coletivo à segurança pública, faz-se necessário promover a ponderação desses valores constitucionais.



Sobre o tema, vale destacar a interpretação oferecida pelo Supremo Tribunal Federal (STF), durante o julgamento da Ação Direta de Inconstitucionalidade (ADI) 6387/DF, sob a relatoria da Ministra Rosa Weber (STF, 2020):

2. Na medida em que relacionados à identificação – efetiva ou potencial – de pessoa natural, o tratamento e a manipulação de dados pessoais não de observar os limites delineados pelo âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (art. 5º, caput), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII), sob pena de lesão a esses direitos. (...).

No ano de 2022, a Suprema Corte Brasileira (no julgamento da ADI 6649, sob a relatoria do Ministro Gilmar Mendes) fixou alguns pressupostos para que o compartilhamento de dados pessoais entre órgãos da Administração Pública seja lícito e produza efeitos jurídicos:

4. Interpretação conforme à Constituição para subtrair do campo semântico da norma eventuais aplicações ou interpretações que conflitem com o direito fundamental à proteção de dados pessoais. O compartilhamento de dados pessoais entre órgãos e entidades da Administração Pública, pressupõe: a) eleição de propósitos legítimos, específicos e explícitos para o tratamento de dados (art. 6º, inciso I, da Lei n.º 13.709/2018); b) compatibilidade do tratamento com as finalidades informadas (art. 6º, inciso II); c) limitação do compartilhamento ao mínimo necessário para o atendimento da finalidade informada (art. 6º, inciso III); bem como o cumprimento integral dos requisitos, garantias e procedimentos estabelecidos na Lei Geral de Proteção de Dados, no que for compatível com o setor público.

Interessante observar que os três primeiros requisitos (acima destacados a partir da decisão na ADI 6649) são aplicáveis ao reconhecimento facial, para fins de investigação e repressão de infrações penais: (a) propósitos legítimos: tratamento de dados pessoais, contendo imagens e/ou vídeos de locais ou de pessoas suspeitas da prática de crimes, para fins de investigação criminal e instrução processual; (b) compartilhamento das imagens e/ou dos vídeos entre os *experts* que promovem as etapas da metodologia ACE-V, com base nas diretrizes do FISWG; e (c) limitação do compartilhamento das imagens e/ou dos vídeos ao mínimo necessário para o atendimento da finalidade informada.

Além dos requisitos constantes do item 4, da interpretação constante da ADI 6649, os Ministros do STF também indicaram alguns elementos que devem ser inseridos na requisição da Autoridade Policial ou Judiciária, que dará origem à realização da análise ou tratamento dos dados pessoais:



6. O compartilhamento de informações pessoais em atividades de inteligência deve observar a adoção de medidas proporcionais e estritamente necessárias ao atendimento do interesse público; a instauração de procedimento administrativo formal, acompanhado de prévia e exaustiva motivação, para permitir o controle de legalidade pelo Poder Judiciário; a utilização de sistemas eletrônicos de segurança e de registro de acesso, inclusive para efeito de responsabilização em caso de abuso; e a observância dos princípios gerais de proteção e dos direitos do titular previstos na LGPD, no que for compatível com o exercício dessa função estatal.

Desse modo, a prova obtida a partir do procedimento de reconhecimento facial, ainda que realizado sem o conhecimento ou autorização da pessoa investigada pela prática de um (ou mais) crime(s), não viola os direitos constitucionais à intimidade ou à proteção de dados pessoais, se for realizado: (i) para fins exclusivos de investigação criminal e repressão de infrações penais (na forma do art. 4º, inc. III, da LGPD); (ii) de forma adequada e proporcional à necessidade de garantir o direito fundamental à segurança pública, e (iii) com observância dos pressupostos descritos pelo STF, nos julgamentos das ADI 6387 e 6649.

A ponderação constitucional também é uma das conclusões oferecidas por Meike Ramon *et al.* (2024, p.143, tradução pela autora): “As decisões sobre o uso presente e futuro da FRT [Tecnologia de Reconhecimento Facial] envolvem o equilíbrio de interesses relacionados ao combate ao crime grave, ao direito à vida privada e ao que é aceitável ou desejável em uma sociedade democrática”.

A ponderação para solucionar a colisão entre esses direitos fundamentais também se encontra presente na exposição de motivos no Projeto de Lei n.º 3069/22. Na justificação ao projeto de lei, merece destaque:

Trata-se de proposição inovadora que tem por objetivo disciplinar o uso de uma excelente ferramenta de tecnologia. E como tal, deve ser regulamentada para sua melhor utilização, a fim de assegurar sua máxima eficácia e uso adequado, garantindo igualmente a preservação dos direitos fundamentais dos cidadãos. Essa ferramenta, como outra qualquer, se corretamente regulamentada, seguramente contribuirá para a redução dos índices de criminalidade em nossa sociedade.

O reconhecimento facial para fins de Segurança Pública é uma necessidade e precisa ser executado de forma técnica, proporcional e fundamentada por seus órgãos, de modo a proporcionar proteção à sociedade, como meio de prova válida em investigações policiais e processos de natureza criminal.



5. CONSIDERAÇÕES FINAIS

Com o avanço da tecnologia e a crescente disponibilidade de imagens e vídeos na era digital, a identificação facial evoluiu como uma atividade científica capaz de produzir provas válidas em investigações criminais e processos judiciais.

Sistemas automatizados, dotados de inteligência artificial (IA), tornaram-se ferramentas essenciais no combate à criminalidade e, assim, integram a *Triade de Reconhecimento Facial*. Entretanto, o uso isolado dessa tecnologia, sem a devida *verificação* de um *expert* humano, tem gerado controvérsias devido a falsos positivos que resultaram em prisões ilegais; violando o método ACE-V, ao ignorar a quarta fase do procedimento recomendado pelo FISWG.

Neste estudo, identificamos que a comparação facial deve ser realizada por meio da combinação (de pelo menos dois) dos especialistas que compõem a *Triade de Reconhecimento Facial*. Esse procedimento integra a capacidade de processamento de dados da inteligência artificial (IA), a habilidade inata dos super-reconhecedores (SR) e o conhecimento técnico dos examinadores faciais (EF), permitindo uma análise neutra e baseada em características faciais distintivas. Desse modo, a avaliação realizada pelo primeiro especialista (IA, SR ou EF) deve, necessariamente, ser submetida à verificação de um segundo especialista humano.

A validade da prova produzida pelo reconhecimento facial, para fins de investigação criminal ou instrução processual, exige respeito aos direitos fundamentais à privacidade e à proteção de dados pessoais (previstos no art. 5º, inc. X e LXXIX, da Constituição de 1988) e o cumprimento das orientações do Supremo Tribunal Federal (STF).

Desse modo, sustentamos que a validade e a admissibilidade das provas derivadas do reconhecimento facial dependem da observância de três elementos essenciais: (i) a identificação facial deve ser realizada pelos especialistas que integram a *Triade do Reconhecimento Facial*; (ii) a aplicação adequada das fases do método ACE-V (Análise, Comparação, Avaliação e Verificação), previsto nas diretrizes do FISWG, que exigem a verificação final por um especialista humano, e (iii) o cumprimento das orientações oferecidas pelo STF, de modo a preservar os direitos fundamentais à privacidade e à proteção de dados e, ao mesmo tempo, garantir o direito constitucional à Segurança Pública.



As informações reunidas no presente estudo permitem que os órgãos oficiais de identificação avaliem a metodologia de comparação facial atualmente utilizada e aprimorem suas práticas; adotando procedimentos que atendam aos pressupostos de validade exigidos pelo Poder Judiciário e, principalmente, forneçam informações seguras e confiáveis capazes de contribuir como meio de prova válido para a investigação policial e identificação de autores de crimes.

A essência da atividade dos profissionais dedicados à identificação facial forense reside na combinação de metodologia, tecnologia avançada, habilidades pessoais e formação profissional contínua, aliada ao compromisso de assegurar identificações precisas e confiáveis, fundamentais para garantir a aplicação das leis e fortalecer a Justiça e a Segurança Pública.

REFERÊNCIAS

ANDRADE, José Carlos Vieira de. **Os Direitos Fundamentais na Constituição Portuguesa de 1976**. Coimbra: Livraria Almedina, 1987. 350 p.

BBC News. **Teste indica se você tem habilidade rara de reconhecer rostos**. Publicado on line em 17 de junho de 2015. Disponível em: https://www.bbc.com/portuguese/noticias/2015/06/150616_super_reconhecedores_rosto_teste_rb. Acesso em: 12 ago. 2024.

BBW. Big Brother Watch. **Big Brother Watch Briefing on facial recognition surveillance**. Publicado on line em junho de 2020. Disponível em: <https://bigbrotherwatch.org.uk/wp-content/uploads/2020/06/Big-Brother-Watch-briefing-on-Facial-recognition-surveillance-June-2020.pdf>. Acesso em: 30 jul. 2024.

_____. **Understanding live facial recognition statistics**. Publicado on line em 22 de maio de 2023. Disponível em: <https://bigbrotherwatch.org.uk/blog/understanding-live-facial-recognition-statistics/>. Acesso em: 30 jul. 2024.

BRASIL. **Decreto-Lei n.º 3.689, de 3 de outubro de 1941. Código de Processo Penal**. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del3689.htm. Acesso em: 02 ago. 2024.

_____. **Constituição da República Federativa do Brasil**. Promulgada em 5 de outubro de 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 02 ago. 2024.



_____. **Emenda Constitucional n.º 115, de 10 de fevereiro de 2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais.** Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm#:~:text=EMENDACONSTITUCIONAL%20N%C2%BA%20115%2C%20DE,e%20tratamento%20de%20dados%20pessoais . Acesso em: 28 jul. 2024.

_____. **Lei n.º 13.709 de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD).** Brasília/DF: Diário Oficial da União, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm . Acesso em: 28 jul. 2024.

_____. Câmara dos Deputados. **Projeto de Lei n.º 3069/2022, de 22 de dezembro de 2022. Dispõe sobre o uso de tecnologia de reconhecimento facial automatizado no âmbito das forças de segurança pública e dá outras providências.** Brasília/DF: Câmara dos Deputados, 2022. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2228103&filename=Tramitacao-PL%203069/2022 . Acesso em: 23 jun. 2024.

CANCELIER, Mikhail Vieira de Lorenzi. **Infinito particular: privacidade no século XXI e a manutenção do direito de estar só.** Tese de Doutorado, UFSC, Florianópolis, 2016. Disponível em: <https://repositorio.ufsc.br/xmlui/handle/123456789/174424> . Acesso em 15 ago.2024.

CANOTILHO, José Joaquim Gomes. **Direito Constitucional e Teoria da Constituição.** 3. ed., Coimbra: Almedina, 1999. 1414 p.

CARLO, Silkie; KRUECKERBERG, Jennifer; FERRIS, Griff. **Face off - The lawless growth of facial recognition in UK policing.** Publicado on line em maio de 2018, Big Brother Watch. Disponível em: <https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf> . Acesso em: 30 jul. 2024.

CRISTO, Camila K. **Proteção da Privacidade e dados relativos pessoais à saúde após aprovação Lei n.º 13.853/2019.** Dissertação de Mestrado, UFSC, Florianópolis/SC, 2021.

DAVIS, Josh P. **O que são super-reconhecedores?** Disponível em: <https://www.superrecognisers.com/research-and-general-information> . Acesso em: 04 fev. 2024.

_____; VALENTINE, T.; DAVIS, Robert E. **Computer assisted facial comparison of photographic images taken from full-face and profile viewpoints.** Forensic Science International, July 2010. Disponível em: <https://www.sciencedirect.com/science/article/abs/pii/S0379073810001842?via%3Dihub> . Acesso em: 30 jul. 2024.



_____. **The worldwide impact of identifying super-recognisers in police and business.** The Cognitive Psychology Bulletin_2019, 4. pp. 17-22. ISSN 2397-2653. Disponível em: <https://gala.gre.ac.uk/id/eprint/24017> . Acesso em: 15 jul. 2024.

DSA. Data Science Academy. **Deep Learning Book Brasil, Capítulo 1 – Deep Learning e a Tempestade Perfeita.** Disponível em: <https://blog.dsacademy.com.br/guia-completo-sobre-inteligencia-artificial-generativa/> . Acesso em: 23 jul. 2024.

_____. **Deep Learning Book Brasil, Guia Completo Sobre Inteligência Artificial Generativa.** Publicado on line em 26 de abril de 2024. Disponível em: <https://blog.dsacademy.com.br/guia-completo-sobre-inteligencia-artificial-generativa/> . Acesso em: 23 jul. 2024.

FISWG. Facial Identification Scientific Working Group. **Facial Image Comparison Feature List for Morphological Analysis. Version 2.0, 2018.** Disponível em: https://fiswg.org/FISWG_Morph_Analysis_Feature_List_v2.0_20180911.pdf . Acesso em: 24 de jul. 2024.

_____. **Facial Comparison Overview and Methodology Guidelines. Version 2.0, 2019.** Disponível em: <https://fiswg.org/documents.html> . Acesso em: 23 jun. 2024.

_____. **Image Factors To Consider In Facial Image Comparison. Version 1.0, 2021.** Disponível em: <https://fiswg.org/documents.html> . Acesso em 26 jul. 2024

_____. Facial Identification Scientific Working Group. **ACE-V Methodology for the Use in One-to-one Comparisons. Version 1.0, 2023.** Disponível em: <http://www.fiswg.org/documents> . Acessado em: 23 jun. 2024.

FUNDECTO. Fundação da Odontologia USP/SP. **Avaliação da estabilidade de medidas faciais: um estudo longitudinal fotoantropométrico.** Disponível em: www.fundecto.com.br/srp/word/19.pdf . Acesso em 15 ago. 2024.

G1. PUTINI, Júlia. **'Cegueira facial': entenda a condição que Brad Pitt afirma ter.** Publicado on line em 07/07/2022. Disponível em: <https://g1.globo.com/saude/noticia/2022/07/07/cegueira-facial-entenda-a-condicao-que-brad-pitt-afirma-ter.ghtml> . Acesso em: 13 ago. 2024.

HUDOC. European Court of Human Rights. **Case of Gaughran v. The United Kingdom** (Application n.º 45245/15), 13 February 2020. Disponível em: [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-200817%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-200817%22]}). Acesso em: 30 jul. 2024.

IBGE. **Censo 2022.** Publicado em 22 de dezembro de 2023 e atualizado em 26 de janeiro de 2024. Disponível em: <https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de->



[noticias/noticias/38719-censo-2022-pela-primeira-vez-desde-1991-a-maior-parte-da-populacao-do-brasil-se-declara-parda](#) . Acesso em 04 ago. 2024.

NUNES, Pablo. **Retratos da Violência – Cinco meses de monitoramento, análises e descobertas, 2019. Novas ferramentas, velhas práticas: reconhecimento facial e policiamento no Brasil.** Rede de Observatórios da Segurança, de junho a outubro de 2019. Disponível em: <https://observatorioseguranca.com.br/wordpress/wp-content/uploads/2019/11/1relatoriorede.pdf> . Acesso em: 28 jul. 2024.

OEA. Organização dos Estados Americanos. **Convenção Americana sobre Direitos Humanos.** Disponível em: <https://www.oas.org/pt/cidh/mandato/basicos/convencion.pdf> . Acesso em: 15 ago. 2024.

ONU. Organização das Nações Unidas. **Pacto Internacional sobre os Direitos Civis e Políticos.** Assembleia Geral das Nações Unidas (ONU), de 16 de dezembro de 1966. Disponível em: <https://www2.mppa.mp.br/sistemas/gcsubsites/upload/39/LGBTI/Pacto%20Internacional%20sobre%20Direitos%20Civis%20e%20Políticos.pdf> . Acesso em: 15 ago. 2024.

PARLAMENTO EUROPEU. **O que é Inteligência Artificial e como funciona?** Publicação on line em 04 de setembro de 2020. Última atualização em 19 de junho de 2023. Disponível em: <https://www.europarl.europa.eu/topics/pt/article/20200827STO85804/o-que-e-a-inteligencia-artificial-e-como-funciona> . Acesso em: 04 fev. 2024.

RAMON, Meike; BARBEY, Alexandre; MÉTILLE, Sylvain. **Recognition technology in swiss law enforcement.** Deployment, Legal Basis and Super-Recognizer-Centered Solution, 2024.

RODRIGUES, Anair; PRADO BOLOGNANI, Sílvia Adriana; DOZZI BRUCKI, Sonia Maria; MODEO BUENO, Orlando Francisco. **Developmental prosopagnosia and adaptative compensatory strategies. Case study Dementia & Neuropsychologia, vol. 2, núm. 4, outubro-diciembre, 2008.** Associação Neurologia Cognitiva e do Comportamento São Paulo, Brasil. Disponível em: <https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=cf786de4eea89103ebc0c3cc19d3d38e8db76d1a> . Acesso em: 23 jul. 2024.

RUSSELL, Richard, DUCHAINE, Brad; NAKAYAMA, Ken. **Super-reconhecedores: Pessoas com capacidade extraordinária de reconhecimento facial.** Psychon Bull Rev. Abril, 2009. Disponível em: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3904192> . Acesso em: 23 jul. 2024.

SABA, Lucas. **Estudo revela como algumas pessoas têm o dom de nunca esquecerem um rosto.** Portal Planeta Cultura. Publicado on line em 30/12/2022. Disponível em: <https://portalplanetacultura.com.br/artigos/estudo-revela-como-algumas-pessoas-tem-o-dom-de-nunca-esquecerem-um-rosto/> . Acesso em: 13 ago. 2024.



SENATE OF THE STATE OF WASHINGTON. 66th Legislature. **SB 6280 – Facial Recognition – State and Local Government, 2019-20. Concerning the use of facial recognition services.** Aprovada em 31 de maio de 2020. Disponível em: <https://lawfilesexst.leg.wa.gov/biennium/2019-20/Pdf/Bills/Session%20Laws/Senate/6280-S.SL.pdf?q=20200617151732>. Acesso em: 17 de junho de 2020.

SENATE OF THE UNITED STATES. 116th Congress. 1st. Session. **S. 2878 – Facial Recognition Technology Warrant Act of 2019.** Projeto de lei. Apresentado em 14 de novembro de 2019. Disponível em: <https://www.congress.gov/bill/116th-congress/senate-bill/2878/text>. Acesso em: 30 jul. 2024.

STF. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade (ADI) 6.387-DF.** Relatora Min. Rosa Weber. Julgamento em 07.05.2020. Acórdão disponível em: <https://portal.stf.jus.br/processos/downloadPeca.asp?id=15344949214&ext=.pdf> . Acesso em 12 de ago. 2024.

_____. **Ação Direta de Inconstitucionalidade (ADI) 6.649-DF.** Relator Min. Gilmar Mendes. Julgamento em 15.09.2022. Acórdão disponível em: <https://portal.stf.jus.br/processos/downloadPeca.asp?id=15358978491&ext=.pdf> . Acesso em 12 de ago. 2024.

TJSP. Tribunal de Justiça de São Paulo. **Ação Civil Pública n.º 1090663-42.2018.8.26.0100. 37.ª Vara Cível TJSP. Instituto Brasileiro de Defesa do Consumidor (IDEC) x Concessionária da Linha 4 do Metrô de São Paulo S.A. (Via Quatro).** Disponível em: https://www.migalhas.com.br/arquivos/2023/5/CFC680ADB37F5F_acordao-metro.pdf . Acesso em: 28 jul. 2024.

TOWLER, Alice; DUNN, James D.; CASTRO MARTÍNEZ, Sergio; MORETON, Reuben; EKLOF, Frederick; RUIFROK, Arnout; KEMP, Richard L.; WHITE, David. **Diverse types of expertise in facial recognition.** *Sci Rep* 13, 11396 (2023). Disponível em: <https://doi.org/10.1038/s41598-023-28632-x> . Acesso em: 23 jul. 2024.

UNICEF BRASIL. Fundo das Nações Unidas para a Infância. **Declaração Universal dos Direitos Humanos (DUDH).** Resolução 217 A (III) da Assembleia Geral das Nações Unidas (ONU), de 10 de dezembro de 1948. Disponível em: <https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos>. Acesso em: 15 ago. 2024.