

Brazilian Journal of Forensic Sciences, Medical Law and Bioethics

Journal homepage: www.ipebj.com.br/forensicjournal



Aplicação dos Sistemas Biométricos de Reconhecimento Facial na Segurança Pública

Application of Biometric Facial Recognition Systems in Public Security

Renata Duarte^{1,2,*}, Rosane Pérez Baldasso^{1,2}, Luciano Beux³, Ana Carolina Fafreldines Albert^{1,3}, Nicole Cortelletti dos Santos¹, Mário Marques Fernandes^{1,4}

¹ Associação Brasileira de Odontologia – Seção Rio Grande do Sul (ABORS) – Departamento de Odontologia Legal, Porto Alegre, RS, Brasil

² Instituto Geral de Perícias – Departamento Médico-Legal, Porto Alegre, RS, Brasil

³ Instituto Geral de Perícias – Departamento de Criminalística, Porto Alegre, RS, Brasil

⁴ Ministério Público do Estado do Rio Grande do Sul – Serviço de Perícias em Saúde, Porto Alegre, RS, Brasil

* Corresponding author. Address: Associação Brasileira de Odontologia, Seção Rio Grande do Sul (ABORS). Departamento de Odontologia Legal. Rua Furriel Luiz Antônio de Vargas, 134, Mont Serrat, Porto Alegre, RS, Brasil. CEP 90470-130. Phone: +55 51 3330 8866. E-mail: perita.renataduarte@gmail.com

Received 23 June 2021; Accepted 11 October 2021

Resumo. O uso de sistemas biométricos de reconhecimento facial automatizado na Segurança Pública requer grande cuidado, considerando que estamos tratando da possibilidade de privação de liberdade. Dessa forma, é de extrema importância que o processo de identificação seja baseado em métodos técnicos científicos, respeitando os princípios de unicidade, imutabilidade, perenidade, praticabilidade e classificabilidade. O objetivo do presente estudo é revisar a literatura sobre a aplicação dos sistemas biométricos de reconhecimento facial no processo de identificação humana por meio de imagem e sua aplicação na Segurança Pública. Foi feita uma revisão de literatura narrativa, bem como a descrição e uma demonstração da técnica do exame pericial de comparação facial visando identificação humana. Os estudos revelaram que, por mais que se tenha avançado na tecnologia de reconhecimento facial automatizado, diversos fatores são sensíveis e influenciam a

acuracidade dos seus resultados em cenários práticos, sendo indicada a verificação humana. Em relação ao seu uso na segurança pública, são relatadas experiências de sucesso e de equívocos, tendo-se observado o seu banimento em vários locais em função da falta de acurácia, intromissão de privacidade e tendências discriminatórias. Deste modo, a melhor solução para o uso em Segurança Pública, dado o estado da arte da tecnologia de reconhecimento facial utilizada, aponta para uma convergência de dois elementos fundamentais nesse processo: máquina e humano. Por esta razão, este estudo indica o uso dos sistemas biométricos de reconhecimento facial como etapa prévia à identificação facial por imagem realizada por meio de técnica pericial.

Palavras-chaves: Antropologia forense; Reconhecimento facial; Identificação; Sistemas biométricos; Imagem; Odontologia legal.

Abstract. The use of facial recognition biometric systems in Public Safety requires special care, due the possibility that could result in a loss of liberty. Thus, it is extremely important that the identification process be based on scientific technical methods, according to the principles of uniqueness, immutability, perpetuity, practicability and classificability. The goal of this study is to review the literature on the application of facial recognition biometric systems in the process of human identification by image and its application in Public Safety. A narrative review of literature was carried out, as well as a description and a demonstration of the facial comparison forensic technique aiming at human identification. The studies revealed that, despite advances in automated face recognition technology, several factors are sensitive and influence the accuracy of their results in practical scenarios, with human verification being indicated. Regarding its use in Public Safety, successful and misleading experiences are reported, having been observed its banishment in several places due to lack of accuracy, intrusion of privacy and discriminatory tendencies. Thus, the best solution for use in Public Safety, given the state of the art of the face recognition technology adopted, points to a convergence of two fundamental elements in this process: machine and human. For this reason, this study indicates the use of facial recognition biometric systems as a step prior to face identification by image performed using a forensic technique.

Keywords: Forensic anthropology; Facial recognition; Identification; Biometric systems; Image; Forensic dentistry.

1. Introdução

Com os avanços da civilização e dos métodos tecnológicos de captura de imagens e movimentos, a vigilância eletrônica se faz cada vez mais presente no dia a dia da população, como se pode observar, por exemplo, nos aeroportos, nas ruas, nas casas e no comércio.

A mobilidade e a facilidade de captura de imagens e vídeos pelo uso massivo de *smartphones* trouxe uma maior exposição das pessoas e, com ela, diversos questionamentos sobre o impacto nas esferas privada e coletiva, acentuados pelo uso dessas tecnologias na Segurança Pública. Nesse contexto, se insere a utilização de sistemas biométricos de reconhecimento facial como mecanismo de controle de acesso, desbloqueio de telas, contagem de público, vigilância e localização de pessoas procuradas em locais de grande circulação e eventos.

O uso de sistemas biométricos de reconhecimento facial automatizados na Segurança Pública requer um cuidado maior considerando que estamos tratando da possibilidade de privação de liberdade e todos os efeitos que decorrem desta medida extrema de retirada do indivíduo do convívio social. Dessa forma, é muito importante que o processo de identificação seja baseado em métodos técnicos científicos.

O objetivo do presente estudo é revisar a literatura a respeito da aplicação dos sistemas biométricos de reconhecimento facial no processo de identificação humana por meio de imagem e sua aplicação na Segurança Pública e demonstrar a técnica do exame pericial de comparação facial visando a identificação humana por imagem.

2. Métodos

Revisão de literatura narrativa do período entre 2010 e 2020, a partir de pesquisa nas bases de dados do Pubmed, Bireme, BVS, Lilacs e Google Scholar, baseada em livros, artigos científicos e reportagens de mídia impressa e na *internet*, bem como descrição e demonstração da técnica do exame pericial de comparação facial visando a identificação humana por imagem.

O exame de comparação facial demonstrado foi fundamentado em métodos analíticos e comparativos, com base no protocolo preconizado pela Academia Nacional de Polícia¹, mediante análise visual do material

questionado e padrão, utilizando *softwares* ImageJ (versão 1.46r, National Institute of Health, Maryland, USA)² e GIMP (versão 2.10.14, Gimp Development Team)³. Duas voluntárias cederam suas imagens mediante termo de consentimento livre e esclarecido – autorização de uso de imagem (Anexos 1 e 2). Assim, utilizamos uma imagem de cada indivíduo como faces questionadas e duas imagens de documentos oficiais como padrões. Primeiramente, as imagens questionadas e padrões foram analisadas por um Perito Criminal lotado na Seção de exames Periciais de Áudio e Imagem do Instituto-Geral de Perícias do Rio Grande do Sul para verificar sua adequabilidade e, após terem sido consideradas adequadas para o confronto, foram alinhadas e escalonadas para viabilizar as análises morfológica e métrica de suas estruturas faciais. Na sequência, as imagens questionadas foram comparadas entre si e, também, com a imagem padrão.

3. Resultados

3.1 Sistema biométrico de reconhecimento facial

A responsabilidade penal é pessoal, somente podendo responder pelo delito praticado quem dele participou⁴. Dessa forma, faz-se necessária a identificação do(s) autor(es), visando a efetividade da aplicação da lei.

Identidade pode ser definida como as características que tornam a pessoa única e diferente das demais⁵. Assim, é fundamental a diferenciação entre reconhecimento e identificação. O reconhecimento é um método empírico que consiste em acatar ser o mesmo ou, ainda, conhecer novamente, por certas características, considerando que uma pessoa é a mesma que já conhecemos em outro momento⁶. Já a identificação humana é um método científico fundamentado em cinco pilares (três biológicos e dois técnicos): unicidade (ser único, não repetir em outro indivíduo), imutabilidade (resistir à ação do tempo, permanecendo inalterado até o fim da vida), perenidade (não desaparecer com o envelhecimento), praticabilidade (ser passível de reprodução, pouco complexos, céleres e baratos) e classificabilidade (viabilizar o arquivamento e a pronta localização quando necessário) aplicados no confronto de dados registrados em momentos distintos, para definir a identidade de alguém⁵. Por ser um método científico baseado em elementos técnicos e biológicos, a identificação apresenta maior qualidade, confiabilidade

e assertividade quando comparada ao reconhecimento que se baseia na observação empírica.

A biometria é objeto de estudo da Segurança da Informação e consiste nas medições de propriedades mensuráveis dos seres vivos e no estudo dessas características em cada indivíduo para verificação automática da identidade⁷. Já os sistemas biométricos consistem na aplicação de características métricas a atributos biológicos para fins de aferição e reconhecimento ou identificação de um indivíduo. Entre estes, está o reconhecimento facial como um método automatizado que utiliza algoritmos matemáticos objetivando uma busca relativamente rápida para localizar, dentro de um banco de dados conhecido, uma face questionada⁸. É o que se denomina na ciência da computação de *machine learning* (aprendizado de máquina), portanto a máquina é calibrada através de critérios de aceitação e rejeição da comparação para evitar falsos-positivos ou falso-negativos. A eficácia destes sistemas depende desta calibragem da margem de erro, portanto, se baseia em padrões matemáticos, não humanos⁹.

Métodos mais sofisticados são os baseados em densidade de probabilidade, como as redes neurais que procuram “imitar” o cérebro humano e que consideram todas as variações possíveis das imagens do banco de dados⁹.

As pesquisas envolvendo reconhecimento de rosto humano revelam que, por mais que se tenha avançado na tecnologia de reconhecimento facial, diversos fatores são sensíveis e influenciam a acuracidade dos seus resultados em cenários práticos. Entre estes podemos citar como mais relevantes: (i) a velocidade de processamento e armazenamento; (ii) o tamanho e qualidade da imagem; (iii) o ângulo de vigilância; (iv) as variações de pose e de luz e (v) a variabilidade entre tipos de etnias. Como forma de resolver esses pontos, estudos sugerem o uso de sistemas de reconhecimento facial baseado em redes neurais convolucionais com aprendizagem profunda (do inglês *deep learning*) porque trabalham todas as variações possíveis nas imagens como brilho, ruído e outros fatores de indução de perda de acurácia. Em teste, os autores obtiveram eficácia de reconhecimento de 98,76%¹¹. Entretanto, a adoção dessa tecnologia esbarra na necessidade de máquinas mais robustas e mais tempo para processamento de dados, o que eleva o seu custo de

aquisição e manutenção, e no tempo de treinamento, que é bastante elevado (em torno de 4 horas) e influenciado pelo tamanho do banco de dados^{10,11}.

Além das questões técnicas inerentes à tecnologia empregada, os sistemas de reconhecimento facial utilizados no mercado têm apresentado vieses, principalmente, em relação a mulheres de pele escura, como revela importante estudo feito por Joy Buolamwini do renomado Instituto de Tecnologia de Massachussets (MIT) e Timnit Gebru, cientista da computação e pesquisadora respeitada em ética e uso de Inteligência Artificial (IA) do Microsoft Research. Para afastar esse comportamento em relação aos bancos de dados onde os sistemas de reconhecimento facial pesquisados "aprenderam", as pesquisadoras utilizaram um banco de dados próprio, tendo a taxa de erro máxima em homens brancos ficado em 0,8% e para mulheres negras em quase 34,7%¹².

E esta descoberta é reforçada pelo relatório publicado pelo Instituto Nacional de Padrões e Tecnologia (NIST) do Departamento de Comércio dos Estados Unidos que avaliou 189 algoritmos de 99 desenvolvedores e concluiu que a tecnologia de reconhecimento facial apresenta viés e imprecisão em relação a dados demográficos (raça, idade, gênero e nacionalidade). O estudo utilizou como metodologia a medição de dois tipos de erros, os falsos positivos e os falsos negativos, tendo encontrado uma taxa maior de falsos positivos para rostos asiáticos, negros e indígenas em relação aos brancos e, maior, ainda, em mulheres negras¹³.

Com a pandemia de COVID-19, estes números se tornaram ainda mais alarmantes, como revela recente estudo do NIST sobre o desempenho de algoritmos de reconhecimento facial em rostos obstruídos por máscaras faciais protetoras utilizando a mesma base de teste do estudo anterior¹³, com uma taxa de erro de 5 a 50% nos reconhecimentos, maior em máscaras de cor escura e que sugere a necessidade de considerar mais esta variável em relação aos algoritmos utilizados nestas tecnologias¹⁴.

3.2 O uso dos sistemas biométricos de reconhecimento facial na segurança pública

O uso de sistemas biométricos de reconhecimento facial na Segurança Pública visando reconhecimento de criminosos tem se intensificado e alterna casos de

sucesso no País, como se verificou no Carnaval de Salvador em 2019, onde um homem que era procurado por homicídio desde 2017 foi capturado pelo sistema de reconhecimento facial do Governo da Bahia, fantasiado de mulher¹⁵ e de insucesso, como de uma mulher que foi detida, por engano, no Rio de Janeiro através do uso de sistema de reconhecimento facial¹⁶, abrindo espaço para o debate sobre os limites de uso da tecnologia.

Embora a Lei Geral de Proteção de Dados (LGPD) tenha excepcionado, à primeira vista, o tratamento de dados pessoais para fins de segurança pública¹⁷ estabelece, de forma expressa, a necessidade de lei específica para reger este tema e já despontam no legislativo algumas iniciativas para regular esta matéria, entre estas um anteprojeto para regular o uso de dados na segurança pública^{18,19} e propostas de lei para o tratamento da utilização destes sistemas de inteligência artificial para fins de investigação e repressão de crimes²⁰.

Nos Estados Unidos, cidades importantes como São Francisco, polo tecnológico de ponta e que abriga a sede de empresas importantes como *Google*, *Facebook* e *Uber*, proibiram o uso de sistemas biométricos de reconhecimento facial pela Polícia, motivadas pelos possíveis erros na identificação de pessoas através do uso dessas tecnologias²¹.

Na Europa, a Polícia Metropolitana de Londres (MET) utiliza sistema de reconhecimento facial em tempo real como mecanismo de redução da criminalidade²² e, apesar dos relatórios de performance publicados indicarem uma taxa de detecção de 70 a 80%²³, estes números são contestados por um Relatório Independente produzido pela Universidade de Essex na Inglaterra que analisou 10 (dez) testes de implantação realizados em operações de policiamento no período de 2016 a 2019. O relatório destaca uma série de problemas decorrentes da implantação da tecnologia e contesta, inclusive, sua base legal. Aponta o dado preocupante que a Polícia errou em 81% dos casos analisados (de 42 identificações de suspeitos, apenas 8 estavam corretas) e contesta a métrica utilizada pela Polícia para embasar sua boa performance, que compara o número total de identificações corretas ou não com o total de rostos processados no sistema e não com o total de reconhecimentos. Na sua conclusão, enfatiza que o fator do envolvimento humano na revisão do processo de reconhecimento é fator crítico para evitar abusos, imprecisões e

falsas detecções, como forma de dar efetividade à legislação de direitos humanos²⁴.

Recentemente, a União Europeia tem discutido um projeto de regulação do reconhecimento facial para procurar crianças desaparecidas, criminosos e pessoas em casos de ataques terroristas. Em contrapartida a Autoridade Europeia para a Proteção de Dados (AEPD) defende a proibição do dessa tecnologia para esse fim, baseado nos riscos à proteção de dados e à privacidade das pessoas²⁵.

Em 2010, os problemas e falhas relacionados ao processo de implementação de sistemas de reconhecimento facial, decorrentes de fatores técnicos como a limitação de desempenho dos sistemas ou mesmo questões morais, políticas e de expectativas sociais já foram objeto de estudo de pesquisadores da Universidade de Lancaster no Reino Unido²⁶.

Todos estes vieses e externalidades do processo de reconhecimento facial por meio de sistemas biométricos automatizados, em especial a possibilidade de erro no reconhecimento da pessoa e a possibilidade privação de liberdade quando utilizado em Segurança Pública, levam à necessidade de compreender como é feita a identificação humana por meio do exame técnico de comparação facial utilizado pela perícia criminal oficial no Brasil.

3.3 Exame pericial de comparação facial visando identificação humana por imagem

3.3.1 O exame de comparação facial

O exame de comparação facial é um processo científico que compara morfológica e metricamente as estruturas faciais de imagens registradas em momentos diferentes buscando identificar uma pessoa. Está baseado na premissa que a face apresenta estruturas individualizadoras que podem, inclusive, ser avaliadas quando analisadas em forma plana e estática¹.

O reconhecimento por imagens se dá por meio de métodos científicos como o Processamento Digital de Sinais, a Fotogrametria e a Antropometria Craniofacial^{27,28}. Como se realiza de forma indireta, através de imagens, é necessário que elas apresentem qualidade mínima de resolução, iluminação e contraste, bem como incidência equivalente. Assim, é fundamental visualizar as estruturas faciais e suas delimitações anatômicas¹.

A primeira etapa do processo é a análise qualitativa dos materiais a fim de verificar sua adequabilidade aos exames comparativos. Essa análise é baseada em requisitos fundamentais para a comparação facial²⁹, que podem ser classificados, por sua importância, em absolutos (que se não forem atendidos inviabilizam a realização dos exames) e relativos (que podem dificultar o exame, mas não o impedem)¹.

São considerados requisitos absolutos: (a) desobstrução da face e de suas estruturas (a face e suas estruturas precisam ser visualizadas para serem comparáveis; o uso de acessórios obstruindo esta região inviabiliza o confronto) e (b) resolução e nitidez (é preciso ter resolução e nitidez suficientes para a marcação dos pontos de interesse e visualização das características morfológicas)¹.

Por requisitos relativos temos: (a) a disponibilidade dos arquivos originais (preferencialmente deve se ter a imagem ou vídeo original; o processo de digitalização e impressão pode acarretar perda de informação); (b) iluminação e contraste (o exame da topografia cutânea e os limites das estruturas da face são melhor visualizados com uma adequada iluminação e contraste da imagem ou vídeo; os excessos para mais ou para menos podem dificultar ou prejudicar o exame); (c) incidência (deve haver similaridade entre a imagem padrão e a questionada; incidências distintas podem permitir a comparação, apenas, se possível a visualização de estruturas individualizadoras) e (d) contemporaneidade (o tempo modifica as estruturas da face e o processo de envelhecimento afeta o tecido cutâneo, por isso é ideal que as imagens sejam próximas no tempo; se muito distantes o exame é feito sobre as estruturas não mutáveis; essas diferenças são ainda maiores em crianças e adolescentes)¹.

Os resultados obtidos neste exame devem ser interpretados do seguinte modo: (a) adequado (a imagem não limita a comparação); (b) parcialmente adequado (tem algum prejuízo à comparação) e (c) não adequado (no caso de requisito absoluto pode inviabilizar o exame)¹.

O procedimento de confronto entre questionado e padrão é feito através da observação da forma, localização, geometria e demais características das estruturas da face, além de elementos individualizadores (marcas, alterações faciais, linhas e sulcos etc.). No resultado, são apontadas

as convergências e divergências entre questionado e padrão. As convergências precisam ser analisadas em contexto dada a possibilidade de mais de uma face apresentar alguma característica elencada. Este método segue as diretrizes de institutos científicos internacionais³⁰. As conclusões seguem escalas qualitativas^{31,32}, conforme apresentado no quadro abaixo (Tabela 1).

Tabela 1. Escala qualitativa adotada na exposição da conclusão do trabalho pericial.

Grau	Correlato Verbal
+ 4	o resultado suporta muito fortemente a hipótese
+ 3	o resultado suporta fortemente a hipótese
+ 2	o resultado suporta moderadamente a hipótese
+ 1	o resultado suporta levemente a hipótese
0	o resultado nem suporta nem contradiz a hipótese
- 1	o resultado contradiz levemente a hipótese
- 2	o resultado contradiz moderadamente a hipótese
- 3	o resultado contradiz fortemente a hipótese
- 4	o resultado contradiz muito fortemente a hipótese

3.3.2 Demonstração do exame

Foi realizado exame pericial de comparação facial para identificação humana tendo como objeto duas faces questionadas (Faces 1 e 2) e duas faces padrão (Faces 3 e 4), Figura 1.



Figura 1. Imagem da Face 1 – questionada (1); Imagem da Face 2 – questionada (2); Imagem da Face 3 – padrão (3); Imagem da Face 4 – padrão (4).

As imagens questionadas e padrões foram analisadas segundo os seguintes requisitos de adequabilidade: absolutos (desobstrução da face e suas estruturas e resolução e nitidez na região da face) e relativos (disponibilidade dos arquivos originais; iluminação e contraste; incidência e

contemporaneidade). O resultado demonstrou que as imagens satisfazem, ainda que parcialmente, os critérios de adequabilidade para a realização do exame de comparação facial (Tabela 2). Os critérios sinalizaram como “parcialmente adequada” a imagem em que houve redução da visualização detalhada e comparação de algumas estruturas morfológicas, entretanto, não houve impedimento para a realização dos exames, viabilizando o confronto.

Tabela 2. Análise da adequabilidade das faces questionadas e padrões.

Requisitos	Face 1	Face 2	Face 3	Face 4
Desobstrução da face e suas estruturas	Adequada	Adequada	Adequada	Adequada
Resolução e nitidez na região da face	Adequada	Adequada	Parcialmente adequada	Parcialmente adequada
Disponibilidade dos arquivos e originais	Adequada	Adequada	Parcialmente adequada	Parcialmente adequada
Iluminação e contraste	Adequada	Adequada	Parcialmente adequada	Parcialmente adequada
Incidência	Adequada	Adequada	Adequada	Adequada
Contemporaneidade	Adequada	Adequada	Adequada	Adequada

Após a análise de adequabilidade, partimos para os confrontos. Primeiramente, comparamos as duas imagens questionadas (Faces 1 e 2) para verificar que se tratavam ou não de indivíduos distintos. Após, realizamos a comparação entre cada face questionada e seu suposto padrão, buscando a identificação humana.

3.3.2.1 Confronto entre a imagem da Face 1 e Face 2

As análises morfológica e morfométrica da Face 1, quando comparadas às da Face 2, demonstram predomínio de divergências, observadas na proporção dos terços faciais, largura facial, linha de implantação capilar, formato, densidade e distanciamento das sobrancelhas, formato, distanciamento e cor dos olhos, ponte e base nasal, formato e espessura dos lábios, linhas e sulcos frontais, palpebrais, palpebronasais, periorbitais e nasogenianos, bem como divergências significativas na quantidade e disposição das marcas faciais (Figura 2).

Dessa forma, podemos concluir que os vestígios elencados contradizem muito fortemente a hipótese de convergência entre a face

questionada – Face 1 e a face questionada – Face 2, equivalente ao nível -4 da citada escala.



Figura 2. A: Análise morfológica - Face 1 - questionada (A1) e Face 2 - questionada (A2); B: Análise morfométrica - Face 1 - questionada (B1) e Face 2 - questionada (B2).

3.3.2.2 Confronto entre a imagem da Face 1 e a imagem da Face 3

As análises morfológica e morfométrica da Face 1 - questionada, quando comparadas às da Face 3, demonstram predomínio de convergências, observadas na linha de implantação capilar, linhas frontais, formato, densidade e distanciamento das sobrancelhas, formato e cor dos olhos, sulcos palpebrais, formato da ponte nasal, sulco nasogeniano, formato e abertura das narinas e formato das asas nasais, formato e espessura dos lábios e comissuras labiais, linha mentolabial, formato do mento, bem como divergências explicáveis pela incidência fotográfica. As análises de superposições: (i) superposição dos contornos das estruturas faciais da Face 1 – questionada sobre a Face 3 – padrão e (ii) superposição da Face 3 – padrão sobre a Face 1 – questionada com Blend (opacidade) de 0%, 25%, 50%, 75% e 100%, também demonstram predomínio de convergências (Figura 3).

Então, podemos concluir que os vestígios elencados suportam muito fortemente a hipótese de convergência entre a face questionada – Face 1 e a face padrão – Face 3, equivalente ao nível +4 da citada escala.



Figura 3. A: análise morfológica - Face 1 - questionada (A1) e Face 3 - padrão (A2);
B: análise morfométrica - Face 1 - questionada (B1) e Face 3 - padrão (B2);
C: superposições dos contornos das estruturas faciais – Face 1 questionada (C1) e superposição da Face 1 - questionada sobre a Face 3 - padrão (C2); D: superposições da Face 3 - padrão sobre a Face 1 - questionada utilizando opacidade (Blend) de 0% (D1), 25% (D2), 50% (D3), 75% (D4) e 100% (D5).

3.3.2.3 Confronto entre a imagem da Face 2 e a imagem da Face 4

As análises morfológica e morfométrica da Face 2 - questionada, quando comparadas da à Face 4 - padrão, demonstram predomínio de convergências, observadas na linha de implantação capilar, linhas frontais, formato, densidade e distanciamento das sobrancelhas, formato e cor dos olhos, visualização dos sulcos palpebrais, linhas periorbitais, formato da ponte nasal, sulco nasogeniano, formato e abertura das narinas e formato das asas nasais, formato e espessura dos lábios, linha mentolabial e linhas cervicais, bem como divergências explicáveis pela incidência fotográfica. As análises de superposições: (a) superposição dos contornos das estruturas faciais da Face 2 – questionada sobre a Face 4 – padrão e (b) superposição da Face 4 – padrão sobre a Face 2 – questionada com Blend (opacidade) de 0%, 25%, 50%, 75% e 100%, também demonstram predomínio de convergências (Figura 4).

Dessa forma, podemos concluir que os vestígios elencados suportam muito fortemente a hipótese de convergência entre a face questionada – Face 2 e a face padrão – Face 4, equivalente ao nível +4 da citada escala.

4. Discussão

A utilização dos sistemas biométricos de reconhecimento facial já é uma realidade mundial e aponta uma evolução tecnológica para diversas funcionalidades como controles de acesso, desbloqueio de telas de celulares e vigilância. Na Segurança Pública, tem sido utilizada na localização de indivíduos foragidos do sistema penal ou procurados pela polícia em razão de crimes cometidos, em eventos e locais de grande circulação de pessoas^{16,22}.

As experiências nesta área têm demonstrado que a tecnologia automatizada comete erros e que, por mais que as máquinas aprendam novos algoritmos, não são poucos os casos de tendências discriminatórias e até mesmo problemas de reconhecimento de imagem que ocasionam a detenção ou até mesmo a prisão de pessoas equivocadas^{12,13,14,16,24}. Desta forma, fica evidente a necessidade da inclusão de uma etapa de verificação humana neste processo para evitar os falsos positivos e negativos²⁴.



Figura 4. A: análise morfológica - Face 2 - questionada (A1) e Face 4 - padrão (A2);
B: análise morfométrica - Face 2 - questionada (B1) e Face 4 - padrão (B2);
C: superposições dos contornos das estruturas faciais – Face 2 questionada (C1) e superposição da Face 2 - questionada sobre a Face 4 - padrão (C2); D: superposições da Face 4 - padrão sobre a Face 2 - questionada utilizando opacidade (Blend) de 0% (D1), 25% (D2), 50% (D3), 75% (D4) e 100% (D5).

O estudo também demonstrou que o método científico de identificação está sustentado em cinco requisitos: unicidade, perenidade, imutabilidade (biológicos), praticabilidade e classificabilidade (técnicos)⁵. A face de cada um é única e, por mais que se modifique ao longo do tempo por fatores naturais ou artificiais, há elementos imutáveis que resistem ao tempo e que permitem a individualização da pessoa¹.

Analisando os pilares científicos, o reconhecimento automatizado não captura estes requisitos biológicos com a acurácia que necessita a identificação criminal dada a sua sensibilidade, uma vez que o seu objeto é a privação da liberdade. Além disso, quando se tenta resolver esta questão através da utilização de redes neurais CNN não se atende ao requisito técnico da praticabilidade, considerando o tempo e custo elevado de uso desta tecnologia^{10,11}. Soma-se a isso o fato da proibição do uso de sistemas biométricos de reconhecimento facial para identificar suspeitos em várias localidades, em função dos possíveis erros²¹.

No que diz respeito ao uso dos sistemas biométricos de reconhecimento facial em segurança pública, é necessário reforçar a diferenciação entre reconhecimento e identificação, enquanto o primeiro apresenta indivíduos semelhantes e a segunda individualiza a pessoa. O exame de comparação facial atende os requisitos biológicos e técnicos do processo de identificação humana¹, sendo uma ótima ferramenta para esse fim, porém necessita de uma face de comparação, o que muitas vezes não é possível em virtude de ausência de suspeitos para o cotejo.

Nesse contexto e considerando a escassa literatura científica sobre o uso dos sistemas biométricos de reconhecimento facial na Segurança Pública, é recomendável que os sistemas biométricos automatizados sejam utilizados como ferramentas auxiliares nos processos de identificação humana, não devendo substituir a atuação técnica pericial, tampouco serem utilizados de forma única, indiscriminada e categórica, evitando assim as externalidades já descritas. Assim, por responderem por similaridade na localização das faces em seu banco de dados, sugerimos o seu uso como etapa prévia ao exame de comparação facial visando identificação humana, indicando possíveis faces e agregando mais agilidade ao exame pericial e possibilitando em muitos casos a análise quando não são apontados suspeitos. Abaixo apresentamos uma

proposta de fluxo para a aplicação dos sistemas biométricos de reconhecimento facial como ferramenta auxiliar no processo de identificação humana pelo exame de comparação facial (Figura 5).

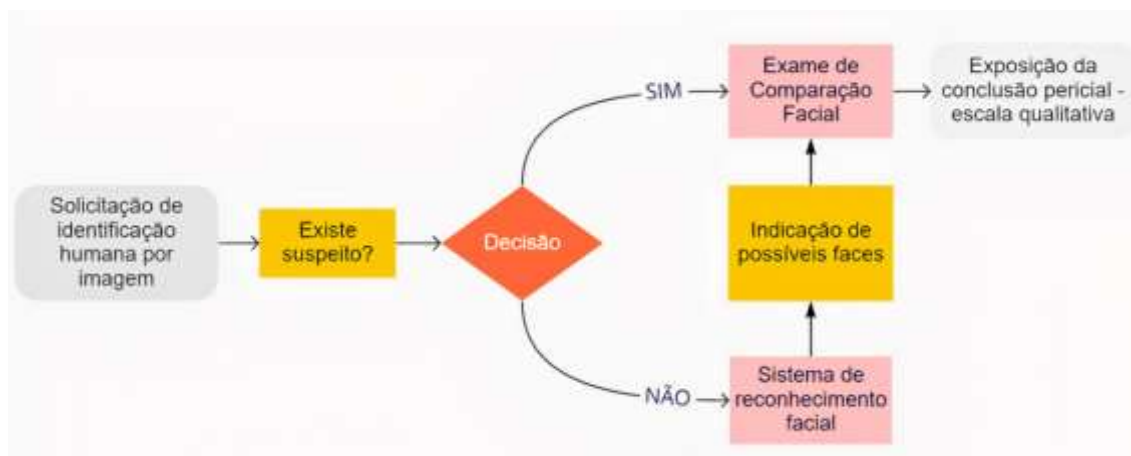


Figura 5. Fluxo para a aplicação dos sistemas biométricos de reconhecimento facial como ferramenta prévia e auxiliar ao exame de comparação facial para na identificação humana.

Outro ponto importante nessa discussão é a questão relacionada à proteção de dados e a Segurança Pública que está fora do escopo da lei, recentemente, aprovada e necessita de regulamentação específica. Como foi relatado, já estão surgindo propostas para essa normatização, inclusive, foi organizada uma comissão para elaboração de um anteprojeto, cujas regras ainda não são pacíficas e necessitam de amplo debate social¹⁹. A discussão sobre o reconhecimento facial está no centro desse debate, reforçando a importância deste trabalho na área de Odontologia legal.

Todas estas questões reforçam a necessidade de verificação humana no uso dos sistemas biométricos de reconhecimento facial como forma de impedir as externalidades decorrentes da sua aplicação automatizada, como os erros cometidos e os vieses discriminatórios para proporcionar uma maior governança do uso destes dados na identificação penal.

Como limitação deste estudo, destaca-se que a tecnologia de reconhecimento facial é, ainda, incipiente na Segurança Pública, necessitando de regulamentação e padronização dos procedimentos de implantação. Além disso, não foram encontrados outros estudos para suportar as conclusões deste trabalho no sentido da utilização dos sistemas biométricos de reconhecimento facial como ferramenta auxiliar/etapa prévia ao exame de

comparação facial. Assim, sugerimos para estudos futuros ensaios práticos com a utilização deste fluxo aqui proposto.

5. Conclusão

A solução mais adequada para o uso em Segurança Pública, dado o estado da arte da tecnologia de reconhecimento facial utilizada, aponta para uma convergência de dois elementos fundamentais nesse processo: máquina e humano. Os sistemas biométricos de reconhecimento facial (máquinas) devem servir como ferramenta prévia de indicação de possíveis faces para viabilizar o exame de comparação facial realizado por Perito Oficial no processo de Identificação Humana nos casos em que não são apontados suspeitos.

Referências

1. Machado CEP, Lacerda Filho EM, Arruda GHM, Flores MRP, Reis PMGI, Baldasso, RP. Apostila do curso de comparação facial. Ministério Extraordinário da Segurança Pública. Polícia Federal. Academia Nacional de Polícia: 2018.
2. Rasband, WS, ImageJ, US. National Institutes of Health, Bethesda, Maryland, USA, 1997-2018. Disponível em: <https://imagej.nih.gov/ij/>
3. The GIMP Development Team. GIMP. 2019. [acesso em abril 2021]. Disponível em: <https://www.gimp.org>
4. Brasil. Art. 5º, inciso XLV. Constituição da República Federativa do Brasil. Brasília, DF: Senado Federal, 1988. [acesso em jun 2021]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm
5. Daruge E, Daruge Júnior E, Francesquini Júnior L. Tratado de odontologia legal e deontologia 1ª Ed [reimpr.]. Rio de Janeiro: Guanabara: Koogan, 2019.
6. Dicionário On Line. [publicação online]. [acesso em 07 jun. 2021]. Disponível em: <https://dicionario.priberam.org/reconhecer>
7. Dicionário On Line. [publicação online]. [acesso em abr 2021] Disponível em: <https://dicionario.priberam.org/biometria>
8. Kawulok M, Celebi ME, Smolka B. Advances in Face Detection and Facial Image Analysis. Springer, 2016. Resenha de: Baldasso RP, Fernandes MM. Revista Brasileira de Odontologia Legal - RBOL, 2018: 5(1):103-107. <https://doi.org/10.21117/rbol.v5i1.181>
9. Braga LFZ. Sistemas de Reconhecimento Facial [Trabalho de conclusão de curso da Escola de Engenharia de São Carlos da Universidade de São Paulo]. São Carlos, 2013. [acesso em fev 2021]. Disponível em:

http://www.tcc.sc.usp.br/tce/disponiveis/18/180450/tce-08112013-145721/publico/Braga_Luiz_Filipe_Zenicola.pdf

10. Zulfiqar M, Syed F, Khan MJ, Khurshid K. Deep Face Recognition for Biometric Authentication. International Conference on Electrical, Communication, and Computer Engineering (ICECCE), 2019, pp. 1-6. <https://doi.org/10.1109/ICECCE47252.2019.8940725>
11. Tolba. AS, El-Baz AH, El Harby AA. Face Recognition: A Literature Review. In: International Journal of Signal Processing. 2006. [acesso em jan 2021]. Disponível em: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.179.2182&rep=rep1&type=pdf>
12. Buolamwini J, Gebru T. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. In: Proceedings of Machine Learning Research 81 of Conference on Fairness, Accountability, and Transparency. 2018. [acesso em nov 2020]. Disponível em: <http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf>
13. Grother P, Ngan M, Hanaoka K. Face Recognition Vendor Test Part 3: Demographic Effects, NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg, MD, 2019. [internet] [acesso em jun 2021]. <https://doi.org/10.6028/NIST.IR.8280>
14. Grother P, Ngan M, Hanaoka K. Ongoing Face Recognition Vendor Test (FRVT) Part 6B: Face recognition accuracy with face masks using post-COVID-19 algorithms, NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg, MD, 2020 [internet]. [acesso em jun 2021]. <https://doi.org/10.6028/NIST.IR.8331>
15. G1 Rio. Sistema de reconhecimento facial da PM do RJ falha, e mulher é detida por engano. Globo.com [internet]. [acesso em jun 2021]. Disponível em: <https://g1.globo.com/rj/rio-de-janeiro/noticia/2019/07/11/sistema-de-reconhecimento-facial-da-pm-do-rj-falha-e-mulher-e-detida-por-engano.ghtml>
16. Alves AT. Flagrado por câmera vestido de mulher no carnaval na BA matou um homem após vítima passar perto dele de moto em alta velocidade. Globo.com [internet]. [acesso em jun 2021]. Disponível em: <https://g1.globo.com/ba/bahia/carnaval/2019/noticia/2019/03/07/flagrado-por-camera-vestido-de-mulher-no-carnaval-na-ba-matou-homem-apos-vitima-passar-perto-dele-de-moto-em-alta-velocidade.ghtml>
17. Brasil. Lei 13.709 de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). art. 4, caput, inciso III, alíneas “a” e “d” c/c § 1º. Diário Oficial da

- União, 15 ago 2018. [acesso em jun 2021]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm
18. Brasil. Anteprojeto de Lei de Proteção de Dados para segurança pública e perseguição penal. Brasília, DF: Câmara dos Deputados, Comissão de Juristas instituída em 26 nov. 2019. [acesso em jun 2021]. Disponível em: <https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica/documentos/outros-documentos/DADOSAnteprojetoComissaoProtecaoDadosSegurancaPersecucaoFINAL.pdf>
19. Câmara dos Deputados [homepage na internet]. Anteprojeto sobre uso de dados na segurança pública deve ficar pronto em novembro. Comunicação, Notícias. 22 set 2020. [acesso em jun 2021]. Disponível em: <https://www.camara.leg.br/noticias/694562-anteprojeto-sobre-uso-de-dados-na-seguranca-publica-deve-ficar-pronto-em-novembro/>
20. Brasil. Projeto de Lei: PL 1969/2021. Brasília, DF: Câmara dos Deputados. [acesso em jun 2021]. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2284814>
21. San Francisco proíbe a polícia de usar reconhecimento facial. Globo.com [internet]. [acesso em jan 2021]. Disponível em: <https://g1.globo.com/pop-arte/noticia/2019/05/16/san-francisco-proibe-a-policia-de-usar-reconhecimento-facial.ghtml>
22. Metropolitan Police [homepage na internet]. Live Facial Recognition [acesso em jun 2021]. Disponível em: <https://www.met.police.uk/advice/advice-and-information/facial-recognition/live-facial-recognition/>.
23. Metropolitan Police. Metropolitan Police Service Live Facial Recognition Trials. National Physical Laboratory. [Evaluation Report]. February 2020. [acesso em set 2020]. Disponível em: <https://www.met.police.uk/SysSiteAssets/media/downloads/central/advice/met/facial-recognition/met-evaluation-report.pdf>
24. Fussey P, Murray D. Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology. [Project Report]. University of Essex Human Rights Centre, 2019. [acesso em set 2020]. Disponível em: <http://repository.essex.ac.uk/id/eprint/24946>
25. Reuters. Reconhecimento facial deve ser banido, diz regulador de privacidade da EU. Globo.com [internet]. [acesso em jun 2021]. Disponível em:

<https://g1.globo.com/economia/tecnologia/noticia/2021/04/27/reconhecimento-facial-deve-ser-banido-diz-regulador-de-privacidade-da-ue.ghtml>.

26. Introna L, Nissenbaum H. Facial Recognition Technology A Survey of Policy and Implementation Issues. Lancaster University: The Department of Organisation, Work and Technology. 2010. Organisation, Work and Technology Working Paper Series. [acesso em out 2020]. Disponível em: <https://eprints.lancs.ac.uk/id/eprint/49012>
27. George RM. Facial Geometry: Graphic Facial Analysis for Forensic Artists. Springfield, EUA: Charles C. Thomas Publisher, 2007.
28. Kolar JC, Salter EM. Craniofacial Anthropometry: Practical measurement of the head and face for clinical surgical and research use. Springfield, EUA: Charles C. Thomas Publisher, 1997.
29. Morisson ALC, Machado CEP, Reis PMGI. Exames de registros de áudio e imagens: recomendações técnicas para a padronização de procedimentos e metodologias. In: Tocchetto D, Espindula A. Criminalística: procedimentos e metodologias, 3ª Edição, Editora Millennium. Cap. 12. 2015.
30. FISWG. Guidelines for Facial Comparison Methods. Facial Identification Scientific Working Group, versão 1.0, aprovada em 02 fev. 2012 e publicada em 20 abr. 2012 [acesso em jun 2021]. Disponível em: <http://www.fiswg.org/documents.html>
31. Eriksson A. Aural/ Acoustical vs. Automatic Methods in Forensic Phonetic case Work. In: NEUSTEIN, A.; PATIL, H.A. Forensic Speaker Recognition: Law Enforcement and Counter-terrorism. New York: Springer-Verlag, 2012.
32. Ali T, Veldhuis RNJ, Spreeuwiers LJ. Forensic Face Recognition: A Survey. Enschede: Centre for Telematics and Information Technology (CTIT), 2010. 12 p. (CTIT Technical Report Series; TR-CTIT-10-40). [acesso em jun 2021]. Disponível em: http://eprints.eemcs.utwente.nl/19145/01/ReviewForensic_FR3.pdf