# XII ENCONTRO INTERNACIONAL DO CONPEDI BUENOS AIRES – ARGENTINA

## DIREITO PENAL, PROCESSO PENAL E CRIMINOLOGIA IV

**NARA SUZANA STAINR**

**VALTER MOURA DO CARMO**

**ANTONIO CARLOS DA PONTE**

Copyright © 2023 Conselho Nacional de Pesquisa e Pós-Graduação em Direito

Todos os direitos reservados e protegidos. Nenhuma parte deste anal poderá ser reproduzida ou transmitida sejam quais forem os meios empregados sem prévia autorização dos editores.

**Diretoria – CONPEDI**
**Presidente** - Prof. Dr. Orides Mezzaroba - UFSC – Santa Catarina
**Diretora Executiva** - Profa. Dra. Samyra Haydêe Dal Farra Naspolini - UNIVEM/FMU – São Paulo
**Vice-presidente Norte** - Prof. Dr. Jean Carlos Dias - Cesupa – Pará
**Vice-presidente Centro-Oeste** - Prof. Dr. José Querino Tavares Neto - UFG – Goiás
**Vice-presidente Sul** - Prof. Dr. Leonel Severo Rocha - Unisinos – Rio Grande do Sul
**Vice-presidente Sudeste** - Profa. Dra. Rosângela Lunardelli Cavallazzi - UFRJ/PUCRio – Rio de Janeiro
**Vice-presidente Nordeste** - Profa. Dra. Gina Vidal Marcilio Pompeu - UNIFOR – Ceará

**Representante Discente:** Prof. Dra. Sinara Lacerda Andrade – UNIMAR/FEPODI – São Paulo

**Conselho Fiscal:**
Prof. Dr. Caio Augusto Souza Lara – ESDHC – Minas Gerais
Prof. Dr. João Marcelo de Lima Assafim - UCAM – Rio de Janeiro
Prof. Dr. José Filomeno de Moraes Filho – Ceará
Prof. Dr. Lucas Gonçalves da Silva – UFS – Sergipe
Prof. Dr. Valter Moura do Carmo – UNIMAR – São Paulo
**Secretarias**
**Relações Institucionais:**
Prof. Dra. Daniela Marques De Moraes – UNB – Distrito Federal
Prof. Dr. Horácio Wanderlei Rodrigues - UNIVEM – São Paulo
Prof. Dr. Yuri Nathan da Costa Lannes - Mackenzie – São Paulo
**Comunicação:**
Prof. Dr. Liton Lanes Pilau Sobrinho - UPF/Univali – Rio Grande do Sul
Profa. Dra. Maria Creusa De Araújo Borges - UFPB – Paraíba
Prof. Dr. Matheus Felipe de Castro - UNOESC – Santa Catarina
**Relações Internacionais para o Continente Americano:**
Prof. Dr. Heron José de Santana Gordilho - UFBA – Bahia
Prof. Dr. Jerônimo Siqueira Tybusch - UFSM – Rio Grande do Sul
Prof. Dr. Paulo Roberto Barbosa Ramos - UFMA – Maranhão
**Relações Internacionais para os demais Continentes:**
Prof. Dr. José Barroso Filho – ENAJUM
Prof. Dr. Rubens Beçak - USP – São Paulo
Profa. Dra. Viviane Coêlho de Séllos Knoerr - Unicuritiba – Paraná
**Eventos:**
Prof. Dr. Antônio Carlos Diniz Murta - Fumec – Minas Gerais
Profa. Dra. Cinthia Obladen de Almendra Freitas - PUC – Paraná
Profa. Dra. Livia Gaigher Bosio Campello - UFMS – Mato Grosso do Sul

**Membro Nato –** Presidência anterior Prof. Dr. Raymundo Juliano Feitosa – UMICAP – Pernambuco

D597

Direito Penal, Processo Penal e Criminologia IV [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Antonio Carlos da Ponte; Nara Suzana Stainr; Valter Moura do Carmo. – Florianópolis: CONPEDI, 2023.

Inclui bibliografia
ISBN: 978-65-5648-806-6
Modo de acesso: www.conpedi.org.br em publicações
Tema: Derecho, Democracia, Desarrollo y Integración

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Direito penal. 3. Processo penal e constituição. XII Encontro Internacional do CONPEDI Buenos Aires – Argentina (2: 2023 : Florianópolis, Brasil).

CDU: 34


Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

# XII ENCONTRO INTERNACIONAL DO CONPEDI BUENOS AIRES – ARGENTINA

## DIREITO PENAL, PROCESSO PENAL E CRIMINOLOGIA IV

---

## Apresentação

A presente obra é o resultado da compilação dos artigos apresentados no Grupo de Trabalho Direito Penal, Processo Penal e Criminologia IV, durante o XII ENCONTRO INTERNACIONAL DO CONPEDI. O evento aconteceu na cidade de Buenos Aires, entre os dias 12 e 14 de outubro de 2023, sendo realizado nas instalações da Faculdade de Direito da Universidade de Buenos Aires (UBA).

O contexto desse encontro, tendo como tema DERECHO, DEMOCRACIA, DESARROLLO Y INTEGRACIÓN se mostrou particularmente oportuno dado o cenário global do século XXI. Hoje, mais do que nunca, é essencial debater os limites e as possibilidades do Direito e da Democracia no contexto do sistema de Justiça e de suas instituições. O Estado, enfrenta crescentes desafios em seu papel de regulador das relações de poder por meio da representação democrática e da participação popular, e como veículo do exercício do poder por meio de normas jurídicas, precisa efetivamente cumprir os atributos de "Democrático" e "de Direito".

No entanto, os desafios são consideráveis. A cidadania em todas as suas dimensões se apresentou uma constante nos trabalhos apresentados, bem como a busca pelo desenvolvimento sustentável multidimensional, como projeto civilizatório, sendo realidades que precisam ser concretizadas e compartilhadas universalmente.

Além disso, essa aspiração somente será realizada por meio da plena inclusão social de todos, seja devido a carências econômicas e sociais, seja devido à falta de oportunidades de cidadania plena. Nesse sentido, uma reavaliação crítica do sistema penal, em todas as suas vertentes, mas sempre sob a luz da Constituição, com seus direitos e garantias, é mais oportuna e relevante do que nunca.

Os ensaios apresentados nesta obra abordam de maneira minuciosa as intrincadas e instigantes problemáticas que permeiam o campo do sistema penal. Com profundidade, eles exploram os aspectos do direito material e processual, tanto em âmbitos constitucionais quanto internacionais, revelando as complexas interações que desafiam as raízes históricas desse sistema.

No decorrer do evento, no dia 13 de outubro, o Grupo de Trabalho promoveu a exposição e discussão de 17 trabalhos científicos correlatos ao tópico em foco. Essas pesquisas representam o patamar mais elevado de investigação conduzida a nível nacional e constituem o alicerce desta obra. São eles:

1 RECONHECIMENTO FACIAL COMO MEIO DE PROVA NO PROCESSO PENAL.

2 O EXERCÍCIO CONSTITUCIONAL DO DIREITO DE DEFESA NA FASE PRÉ-PROCESSUAL NO SISTEMA ACUSATÓRIO BRASILEIRO.

3 O DISCURSO DE UMA EX-POLICIAL PENAL SOBRE O SISTEMA CARCERÁRIO.

4 A PSICOPATIA E SEUS IMPACTOS NO SISTEMA PRISIONAL.

5 ECOCÍDIOS NO BRASIL CONTEMPORÂNEO: UM OLHAR A PARTIR DA CRIMINOLOGIA VERDE.

6 A CONFISSÃO NO ACORDO DE NÃO PERSECUÇÃO PENAL E SUA IRRELEVÂNCIA PROBATÓRIA PARA O ACUSADO CONCORRENTE.

7 O EMPREGO DO DOLO EVENTUAL PELA COMISSÃO DE VALORES MOBILIÁRIOS.

8 A INFLUÊNCIA DA ESCOLA CORRECIONALISTA NA HISTÓRIA DA JUSTIÇA JUVENIL NO BRASIL.

9 DESIGUALDADE ENCARCERADA: O IMPACTO DO ENCARCERAMENTO EM MASSA NA POPULAÇÃO NEGRA E A OFENSA AOS SEUS DIREITOS FUNDAMENTAIS.

10 O ENCARCERAMENTO FEMININO A SERVIÇO DA SELETIVIDADE PENAL: UMA PERSPECTIVA DE NECROPOLÍTICA DE GÊNERO.

11 PROJETO XAPIRI: SOBRE A (IM)POSSIBILIDADE DE PROPOSTAS DO MEIO AMBIENTE PARA A ESFERA PENAL.

12 ASPECTOS PRÁTICOS DA LEI DOS JUIZADOS ESPECIAIS CRIMINAIS: ATUALIZAÇÃO DOUTRINÁRIA E JURISPRUDENCIAL.

13 A DOUTRINA DA CEGUEIRA DELIBERADA E A SUA APLICAÇÃO NO SISTEMA DE JUSTIÇA BRASILEIRO.

14 A PSICOPATIA COMO ESTIGMA: REFLEXÕES SOBRE AS CONSEQUÊNCIAS DE UMA ROTULAÇÃO SEGREGACIONISTA.

15 ANÁLISE DAS CONSEQUÊNCIAS NA IMPLANTAÇÃO DA BODYCAM NA ROTINA DA POLÍCIA MILITAR.

16 A LIBERDADE DE MICHEL FOUCAULT COMO CONDIÇÃO DE PODER.

17 DESAFIOS NA APLICAÇÃO DA CRIMINOLOGIA NA SEGURANÇA PÚBLICA: UM ESTUDO SOBRE DIREITO PENAL, PROCESSO PENAL E POLÍTICAS DE SEGURANÇA.

Inegavelmente, deparamo-nos com desafios de magnitude considerável. Os paradigmas teóricos se mostram diversificados, os conceitos apresentam facetas múltiplas e os instrumentos normativos frequentemente revelam a crua realidade que afeta corpo e mente. Contudo, a indagação que persiste em relação aos Direitos Fundamentais, que servem como salvaguardas das garantias mínimas, é a seguinte: por que a humanidade ainda se vê compelida a promulgar mais leis com o intuito de assegurar direitos tão elementares como a vida, a saúde, o meio ambiente e a sustentabilidade? A construção de uma reflexão sob a forma de diálogo, presente neste Grupo de Trabalho pode contribuir para a busca de soluções alicerçadas nos princípios de uma Democracia justa, fraterna e livre.

Profa. Dra. Nara Suzana Stainr – Faculdade de Ciências Jurídicas de Santa Maria (UNISM)

Prof. Dr. Valter Moura do Carmo – Universidade Federal do Semi-Árido (UFERSA)

Prof. Dr. Antonio Carlos da Ponte - Universidade Nove de Julho (UNINOVE)

# RECONHECIMENTO FACIAL COMO MEIO DE PROVA NO PROCESSO PENAL

# FACIAL RECOGNITION AS A MEANS OF PROOF IN CRIMINAL PROCEEDINGS

**Eduardo Puhl** [1]
**Matheus Felipe De Castro** [2]

**Resumo**

Considerando a ampliação do uso de câmeras de vigilância em espaços públicos com a finalidade de exercer controle social pelas forças de segurança, o presente artigo aborda o reconhecimento facial e sua compatibilidade com o sistema legal de provas no processo penal. Questiona de que maneira o uso da tecnologia de reconhecimento facial automatizado pode ser auditado para o controle da qualidade da prova produzida. Objetiva compreender o que seja reconhecimento facial, analisar a questão da prova e os requisitos da prova digital e, por fim, identificar critérios para viabilizar o controle da prova produzida por meio do reconhecimento facial. Por meio de uma abordagem exploratória, especula o reconhecimento facial como meio de prova digital de forma ampla. Conclui-se que o reconhecimento facial se mostra compatível e pode ser utilizado como meio de prova no processo penal. Além disso, foi possível identificar mecanismos para o realizar o controle da qualidade da prova produzida. Pesquisas futuras devem concentrar esforços no estudo da visão computacional e deep learning com vistas a fomentar as bases para melhor compreensão do impacto da tecnologia de reconhecimento facial automatizado no direito e, de modo especial, no que tange à fiabilidade da prova no processo penal.

**Palavras-chave:** Reconhecimento facial, Provas, Processo penal

**Abstract/Resumen/Résumé**

Considering the increasing use of surveillance cameras in public spaces with the aim of exercising social control by security forces, this article discusses facial recognition and its compatibility with the legal system of evidence in criminal proceedings. It questions how the use of automated facial recognition technology can be audited in order to control the quality of the evidence produced. It aims to understand what facial recognition is, to analyze the issue of evidence and the requirements of digital evidence and, finally, to identify criteria to enable the control of evidence produced through facial recognition. Through an exploratory approach, it speculates on facial recognition as a means of digital evidence in a broad way. It concludes that facial recognition is compatible and can be used as evidence in criminal

[1] Professor UNC - Concórdia/SC. Doutorando e Mestre em Direito pela UNOESC. Membro do Grupo de Estudo e Pesquisa “Proteção Das Liberdades Na Sociedade Do Controle” (CNPq/UNOESC).

[2] Pós-Doutorado em Direito UnB. Doutor em Direito UFSC. Professor de Direito Processual Penal no Programa de Mestrado Profissional em Direito e Acesso à Justiça UFSC. Professor Titular do PPGD UNOESC.

proceedings. It was also possible to identify mechanisms for controlling the quality of the evidence produced. Future research should focus on the study of computer vision and deep learning with a view to laying the foundations for a better understanding of the impact of automated facial recognition technology on the law and, in particular, on the reliability of evidence in criminal proceedings.

**Keywords/Palabras-claves/Mots-clés:** Facial recognition, Evidence, Criminal procedure

## 1. INTRODUÇÃO

Considerando que o processo penal é o caminho necessário para aplicação da pena, e que para condenar uma pessoa há que se provar sua culpa para além de qualquer dúvida razoável, o presente trabalho se desenvolve sob o tema da prova no processo penal.

Nesse contexto, ressalta-se que a Constituição da República Federativa do Brasil de 1988 faz previsão expressa de diversos direitos e garantias fundamentais, dentre as quais, para fins deste trabalho, destacam-se o devido processo legal, a inadmissibilidade das provas ilícitas, a presunção de inocência e a proteção dos dados pessoais, inclusive nos meios digitais.

O recorte proposto encontra delimitação na questão do reconhecimento facial e os cuidados necessários para que seja utilizado como prova no processo penal. O reconhecimento facial serviria como uma espécie de prova inominada, no qual uma identidade é atribuída a uma imagem de uma pessoa por meio de um *software*, ou programa de computador[1].

Com a ampliação do uso de câmeras de vigilância em espaços públicos, bem como de sua utilização pelos órgãos de segurança com a finalidade de exercer controle social, a tecnologia de reconhecimento facial automatizado, ou simplesmente reconhecimento facial, vem ganhando relevância.

A utilização desse tipo de tecnologia não é novidade, pois vem sendo utilizada hodiernamente com as mais diversas finalidades, como desbloqueio de celulares, permissão de acesso à lugares restritos, confirmação de contratos, entre outros.

O desenvolvimento da tecnologia e, nesse caso específico, das ferramentas utilizadas para o reconhecimento facial tem despertado interesse dos órgãos de segurança para viabilizar um controle mais efetivo, inclusive para fins de investigação criminal.

Nesse contexto, apresenta-se o problema a ser enfrentado pelo presente trabalho: de que maneira o uso da tecnologia de reconhecimento facial automatizado pode ser auditado para o controle da qualidade da prova produzida?

Dessa forma, de maneira geral, objetiva-se analisar o uso do reconhecimento facial como meio de prova no processo penal. De maneira específica, objetiva-se compreender o que seja reconhecimento facial, analisar a questão da prova e os requisitos da prova digital e, por

[1]Art. 1º Programa de computador é a expressão de um conjunto organizado de instruções em linguagem natural ou codificada, contida em suporte físico de qualquer natureza, de emprego necessário em máquinas automáticas de tratamento da informação, dispositivos, instrumentos ou equipamentos periféricos, baseados em técnica digital ou análoga, para fazê-los funcionar de modo e para fins determinados (Brasil, 1998).

fim, identificar critérios para viabilizar o controle da prova produzida por meio do reconhecimento facial.

O ferramental metodológico se apoia em uma abordagem exploratória, consistente em especular o reconhecimento facial como meio de prova de forma ampla, buscando compreender suas características e critérios para o controle da prova produzida, além da utilização de técnica de pesquisa bibliográfica.

Para tanto, o trabalho se divide em três seções. Na primeira seção o foco será no reconhecimento facial, abordando conceitos e possibilidades de utilização. A segunda seção aborda a questão da prova no processo penal. A terceira seção, por fim, busca identificar critérios para viabilizar o controle da prova produzida por meio do reconhecimento facial.

## 2. CONSIDERAÇÕES SOBRE O RECONHECIMENTO FACIAL

Hodiernamente somos alvo de colheita de dados biométricos para acessar diversos sistemas e serviços dos quais dispomos, por exemplo, reconhecimento de face e/ou impressão digital no celular, comandos de voz, impressão digital nas operações bancárias, fornecimento de fotografia para identificação civil e impressão digital para cadastros públicos e votação (Araújo; Cardoso; Paula, 2021).

A inteligência artificial (IA), por sua vez, vem interagindo com diversas áreas do conhecimento há muito tempo, permitindo o desenvolvimento de soluções e a realização de tarefas repetitivas que demandariam esforços humanos, com acurácia superior, mas com tempo e custo inferiores. Nesse contexto, a IA se mostra ideal para atividades repetitivas e que exijam muita atenção e memória (Peixoto; Silva, 2019).

Desde os modelos presentes no *smartphone* até a utilização desses pelo Estado, a realidade é permeada pelo digital. A inteligência artificial e os mecanismos a ela relacionados são partes indissociáveis da atual vida em sociedade (Araújo; Cardoso; Paula, 2021).

É notável a expansão da tecnologia de reconhecimento facial nos mais diversos setores, inclusive no processo penal. Ainda em fase de implementação e teste na maioria dos casos, sua utilização vai do reconhecimento de suspeitos até o auxílio na localização de foragidos da Justiça. São novas coordenadas que se faz preciso compreender (Rosa; Bernardi, 2018).

O reconhecimento facial biométrico é uma das tecnologias de inteligência artificial mais significativas e em rápido desenvolvimento atualmente disponíveis para fins de segurança e aplicação da lei (Smith; Miller, 2021).

Essa tecnologia envolve a extração, digitalização e comparação automatizadas da distribuição espacial e geométrica das características faciais para identificar indivíduos. Utilizando uma fotografia digital do rosto de um indivíduo, um mapa de contorno da posição das características faciais é convertido num modelo digital, utilizando um algoritmo[2] para comparar uma imagem de um rosto com uma imagem armazenada numa base de dados. As imagens podem ser recolhidas em repositórios de fotografias de passaportes, carteiras de habilitação de condutores ou do vasto número de imagens que foram carregadas em sítios de redes sociais e na internet (Smith; Miller, 2021).

Conforme expõem Alexandre Morais da Rosa e Shara di Bernardi (2018), o reconhecimento facial é uma técnica de identificação biométrica que reconhece e diferencia rostos humanos por meio de um *software*, o qual mapeia de forma matemática os traços e espaços existentes em diferentes imagens digitais de uma mesma pessoa. A comparação é feita por um algoritmo, que afirma ou nega sua identidade.

Antes de realizar o reconhecimento facial, primeiramente o algoritmo precisa encontrar um rosto na imagem. Esse processo é chamado de detecção. Uma vez detectado, o rosto é "normalizado" (escalado, rodado e alinhado) para que todos os rostos que o algoritmo processa estejam na mesma posição, facilitando a comparação dos rostos. Em seguida, o algoritmo extrai características do rosto, as quais podem ser quantificadas numericamente, como a posição dos olhos ou a textura da pele. Finalmente, o algoritmo examina pares de faces e emite uma pontuação numérica que reflete a semelhança das suas características (Garvie; Bedoya; Frankle, 2016).

Após a captura do conjunto de medidas nodais de um rosto, esses dados são submetidos a uma série de algoritmos, armazenando-se geometricamente os dados em um *template*[3]. Dessa forma, armazenados esses dados junto ao *software*, viabiliza-se a comparação entre o banco de dados existente e a imagem apresentada, identificando-a biometricamente (Rosa; Bernardi, 2018). Conforme Garvie, Bedoya e Frankle (2016) o reconhecimento facial é, entretanto, probabilístico: ele não produz respostas binárias do tipo

[2] "Um algoritmo pode ser definido, de modo simplificado, como um conjunto de regras que define precisamente uma sequência de operações, para várias finalidades, tais como modelos de previsão, classificação, especializações" (Peixoto; Silva, 2019, p. 71).

[3] A medição de um rosto, ou seja, a relação entre esses pontos, cria uma geometria espacial única, que é armazenada em forma de dados (chamada de *template* ou *faceprint*). Quando uma nova imagem digital (que pode ser foto, vídeo ou captura ao vivo) é apresentada, o *software* faz a comparação (Mena, 2018).

"sim" ou "não", mas identifica correspondências mais prováveis ou menos prováveis. Esse modelo de engenharia de *software* é conhecido como IPO[4] (*input – process – output).*

A aquisição da imagem facial geralmente ocorre por meio de uma câmera de vigilância que tira fotos digitais da face do indivíduo em tempo real. Essa aquisição pode ocorrer em um ambiente controlado ou em movimento, quando a pessoal passa pelo campo de visão da câmera (Schlottfeldt, 2022).

A acurácia dessa tecnologia pode sofrer a influência de vários fatores, como, por exemplo, a qualidade da imagem (iluminação, resolução, fundo, ângulo de captura) condições ambientais (iluminação, posição da câmera) e uso de acessórios (Schlottfeldt, 2022).

Os algoritmos utilizados para o reconhecimento facial utilizam *deep learning*, que é uma forma específica de aprendizagem de máquina, na qual redes neurais[5] são treinadas com muitas camadas de unidades. O *deep learning* proporcionou melhoras significativas nas tarefas de reconhecimento visual. Quanto mais camadas, todavia, mais abstrata é a representação dos modelos, de forma que o fornecimento de *inputs* para o algoritmo gera um *output*, sem que se entenda realmente como o computador chegou àquela conclusão (Peixoto; Silva, 2019).

Os órgãos de investigação que utilizam sistemas de reconhecimento facial geralmente o usam de quatro maneiras (Garvie; Bedoya; Frankle, 2016, p. 10-12):

- Abordagem e identificação: quando um policial encontra um indivíduo que não quer ou não consegue se identificar, o policial obtém uma foto do indivíduo para processamento no sistema de reconhecimento facial, a fim de possibilitar sua identificação;
- Detenção e identificação: um indivíduo é detido, tem suas impressões digitais coletadas e uma foto de identificação é obtida. Essa foto é arquivada no banco de dados de reconhecimento facial para ser usada em consultas futuras. Ela também pode ser compartilhada com outras agências policiais;
- Investigação e identificação: se o rosto de um suspeito estiver disponível em um elemento de informação durante uma investigação, uma foto ou vídeo do

[4] Input-process-output (I-P-O) é uma metodologia estruturada para capturar e visualizar todos os inputs, outputs e etapas do processo necessários para transformar inputs em outputs. Muitas vezes, ela é chamada, de forma intercambiável, de modelo I-P-O ou diagrama I-P-O, sendo que ambos fazem referência à natureza visual pretendida do método. Disponível em: https://www.isixsigma.com/dictionary/input-process-output-i-p-o/.
[5] Redes neurais são estruturas de processamento inspiradas nos neurônios e no cérebro humano, as quais permitem a sobreposição de várias camadas de processamento, aprofundando a aprendizagem (Peixoto; Silva, 2019, p. 104).

rosto é analisada no *software* de reconhecimento facial para fornecer pistas. Se não houver correspondências, a foto poderá ser arquivada para uso futuro;

- *Surveillance*: se o órgão de investigação estiver procurando por um indivíduo específico ou um pequeno grupo de indivíduos, as forças policiais podem fazer o *upload* das imagens para criar uma "*watch list*", uma lista de observação, para pesquisar em vídeo em tempo real. Se uma possível correspondência for encontrada, o sistema alertará os usuários sobre a possível correspondência.

Uma outra forma de utilização do reconhecimento facial é apontada por Schlottfeldt (2022, p. 23): "ajudar a reduzir o tempo de investigação, permitindo que investigadores identifiquem ou excluam rapidamente os suspeitos logo após um crime ter sido cometido".

Os exemplos acima elencam apenas alguns dos empregos possíveis para o reconhecimento facial. Nem todas as formas de utilização, entretanto, se enquadram nos limites da ética (Schlottfeldt, 2022).

As vantagens das tecnologias de reconhecimento facial sobre outras modalidades biométricas, todavia, a tornam um alvo em potencial para emprego na vigilância e na segurança pública. Com uma base de dados ampla o suficiente, como tende a ser o caso da Identificação Civil Nacional[6], criada pela Lei n° 13.444/2017, um sistema de monitoramento seria capaz de identificar, em tempo real, transeuntes anônimos em logradouros públicos através da comparação de pontos faciais registrado no banco de imagens, aplicação esta denominada vigilância facial (Oliveira *et al*, 2022).

Sobre banco de dados, verifica-se que o Tribunal Superior Eleitoral (TSE), que é responsável pelo maior banco de dados biométricos das Américas, concentra informações cujo repositório, em 2021, já contava com mais de 120 milhões de eleitoras e eleitores cadastrados em arquivo eletrônico, armazenando foto, assinatura e impressões digitais (Tribunal Superior Eleitoral, 2021).

Outra possibilidade diz respeito à utilização do Banco Nacional Multibiométrico e de Impressões Digitais. A Lei nº 12.037/2009, que dispõe sobre a identificação criminal do

[6] Art. 1º É criada a Identificação Civil Nacional (ICN), com o objetivo de identificar o brasileiro em suas relações com a sociedade e com os órgãos e entidades governamentais e privados.
Art. 2º A ICN utilizará:
I – a base de dados biométricos da Justiça Eleitoral;
II – a base de dados do Sistema Nacional de Informações de Registro Civil (SIRC), criado pelo Poder Executivo federal, e da Central Nacional de Informações do Registro Civil (CRC Nacional), instituída pelo Conselho Nacional de Justiça, em cumprimento ao disposto no art. 41 da Lei nº 11.977, de 7 de julho de 2009;
III – outras informações, não disponíveis no SIRC, contidas em bases de dados da Justiça Eleitoral, dos institutos de identificação dos Estados e do Distrito Federal ou do Instituto Nacional de Identificação, ou disponibilizadas por outros órgãos, conforme definido pelo Comitê Gestor da ICN.

civilmente identificado, regulamentando o art. 5º, inciso LVIII, da Constituição Federal, foi modificada em 2019 pela Lei 13.964, o chamado "Pacote Anticrime". Esse novo banco de dados tem como objetivo armazenar dados de registros biométricos, de impressões digitais e, quando possível, de íris, face e voz, para subsidiar investigações criminais federais, estaduais ou distritais.

Apesar das polêmicas envolvendo o uso de tecnologias de reconhecimento facial, verifica-se que sua utilização parece encontrar respaldo na opinião da população. Segundo um estudo da Pew Research Center (2019), 59% da população entrevistada demonstrou aceitação do uso do reconhecimento facial para a aplicação da lei avaliando ameaças à segurança em espaços públicos, enquanto apenas 15% demonstraram ser inaceitável a utilização para esse fim.

Levando-se em consideração que o reconhecimento facial é realizado a partir da comparação de imagens, obtidas tanto de fotografias quanto de filmagens, e que seu objetivo é o de atribuir identidade à um indivíduo, mister analisar a questão do reconhecimento de pessoas no que tange ao processo penal.

## 3. A QUESTÃO DA PROVA NO PROCESSO PENAL

Até agora o presente trabalho discutiu sobre a questão de como se processa o reconhecimento facial e suas aplicações pelos órgãos de investigação. Após esta breve apresentação sobre essa tecnologia, emerge a necessidade de analisar como ela se encaixa no processo penal, especialmente como meio de prova.

Segundo Tavares e Casara (2020), prova seria a atividade cuja finalidade demonstraria a ocorrência de um fato, bem como poderia ser um meio à demonstração do acerto de uma hipótese e o de resultado produzido na convicção do julgador. Há, ainda, quem identifique a prova jurídica com o elemento capaz de demonstrar o acontecimento de um fato.

> "A ideia de prova no direito é construída a partir de uma relação dialética entre saber e verdade, em uma dinâmica que envolve a possibilidade de saber e os efeitos que são conferidos à verdade. Em certo sentido, pode-se definir "prova" como um ato voltado à obtenção dos efeitos inerentes à verdade em relação a uma proposição ou hipótese" (Tavares; Casara, 2020).

Nesse contexto, prova é tudo aquilo que contribui para a formação do convencimento do magistrado, a fim de demonstrar os fatos alegados pelas partes no processo. O convencimento do julgador é a pretensão das partes que litigam em juízo, que deverão fazê-lo por intermédio do manancial probatório carreado aos autos (Távora; Alencar, 2015).

As provas visam reconstruir os fatos e, dessa maneira, formar o convencimento do órgão julgador para a resolução da demanda. A prova seria então a verificação do *thema probandum* e tem como principal finalidade o convencimento do juiz (Rangel, 2023).

Verifica-se, portanto, que prova é tudo aquilo que as partes apresentam em juízo, com a finalidade de convencer o órgão julgador de que um fato efetivamente aconteceu. Para isso, as partes podem utilizar todos os meios legítimos de prova, ainda que não previstos em lei, vedada a prova ilícita.

Para que o órgão julgador entregue uma decisão, todavia, a prova apresentada deve cumprir critérios de suficiência probatória. O preenchimento desses critérios é o que legitima a decisão. O critério mais exigente é o *beyond a reasonable doubt* (além da dúvida razoável), que é o critério utilizado na sentença penal. Não obstante, é possível um rebaixamento do *standard* probatório conforme a fase procedimental. Dessa forma, verifica-se que a exigência probatória seja menor para receber uma acusação ou decretar uma medida cautelar do que o exigido para proferir uma sentença condenatória. É por isso que o CPP fala em indícios razoáveis para decisões interlocutórias com menor exigência probatória. Ao consagrar a presunção de inocência e o *in dubio pro reo*, a Constituição adota o *standard* probatório de "além da dúvida razoável", que, somente se preenchido, autoriza um juízo condenatório (Lopes Jr., 2021).

O procedimento de reconhecimento de pessoas constitui-se como meio de prova no processo penal. O art. 226 do Código de Processo Penal (CPP) estabelece que o ato deverá ocorrer da seguinte forma: a pessoa que tiver de fazer o reconhecimento será convidada a descrever o indivíduo que deva ser reconhecido (art. 226, I); a pessoa, cujo reconhecimento se pretender, será colocada, se possível, ao lado de outras que com ela tiverem semelhança, convidando-se quem tiver de fazer o reconhecimento a apontá-la (art. 226, II); se houver razão para recear que a pessoa chamada para realizar o ato, por intimidação ou outra influência, não diga a verdade em face da pessoa a ser reconhecida, a autoridade providenciará para que esta não veja aquela (art. 226, III); do ato de reconhecimento lavrar-se-á termo pormenorizado, subscrito pela autoridade, pela pessoa chamada para proceder ao reconhecimento e por duas testemunhas presenciais (art. 226, IV) (Brasil, 1941).

A interpretação vigente sobre o reconhecimento de pessoas, respeitando o critério *beyond a reasonable doubt*, estabeleceu que as formalidades prescritas no art. 226 do CPP são obrigatórias, e não meras formalidades, pois constituem garantia mínima do suspeito, sob pena de nulidade. Veja-se:

> “O reconhecimento de pessoas deve, portanto, observar o procedimento previsto no art. 226 do Código de Processo Penal, cujas formalidades constituem garantia mínima para quem se vê na condição de suspeito da prática de um crime, não se tratando, como se tem compreendido, de "mera recomendação" do legislador. Em verdade, a inobservância de tal procedimento enseja a nulidade da prova e, portanto, não pode servir de lastro para sua condenação, ainda que confirmado, em juízo, o ato realizado na fase inquisitorial, a menos que outras provas, por si mesmas, conduzam o magistrado a convencer-se acerca da autoria delitiva. Nada obsta, ressalve-se, que o juiz realize, em juízo, o ato de reconhecimento formal, desde que observado o devido procedimento probatório” (BRASIL, 2020).

Depreende-se da ementa do HC 598.886/SC acima que a observância do procedimento previsto no art. 226 do CPP é obrigatória, sob pena de tornar-se inválido, não podendo ser utilizado como lastro probatório para eventual condenação.

Apesar da jurisprudência fomentar uma adequação do procedimento descrito no CPP ao que prescreve o Estado Democrático de Direito previsto constitucionalmente, a evolução da tecnologia, bem como a necessidade de efetivar a segurança pública (dever de proteção estatal), conduz à adoção de novas técnicas de reconhecimento: ganha destaque o reconhecimento facial.

Para realizar o reconhecimento de pessoas, além do procedimento previsto no CPP, também são aceitos os reconhecimentos por fotografias, corroborados posteriormente, e inclusive de filmagens:

> "Habeas Corpus - filmagem realizada, pela vítima, em sua própria vaga de garagem, situada no edifício em que reside - gravação de imagens feita com o objetivo de identificar o autor de danos praticados contra o patrimônio da vítima - legitimidade jurídica desse comportamento do ofendido - desnecessidade, em tal hipótese, de prévia autorização judicial - alegada ilicitude da prova penal - inocorrência - validade dos elementos de informação produzidos, em seu próprio espaço privado, pela vítima de atos delituosos - considerações em torno da questão constitucional da ilicitude da prova - alegação de inépcia da denúncia - existência, no caso, de dados probatórios mínimos, fundados em base empírica idônea - peça acusatória que satisfaz, plenamente, as exigências legais - pedido indeferido” (Brasil, 2004).

Depreende-se que o uso das tecnologias vem paulatinamente adentrando o tema das provas, tendo em vista que as Cortes superiores vêm autorizando sua utilização (no caso acima, a filmagem) como meio de prova, legitimando o reconhecimento realizado por esta via.

Mas realizar o reconhecimento de uma pessoa quando se conhece sua identidade ou quando se tem suspeitos ou pessoas detidas é uma coisa. Outra é realizar o reconhecimento de uma pessoa cuja identidade é desconhecida. É nesse momento que o reconhecimento facial demonstra sua relevância, pois apresenta a possibilidade de identificar uma pessoa ao associar sua imagem com outras que estão à disposição em um banco de dados.

Para além das experimentações, tais como as que ocorreram na Copa do Mundo[7] em 2014, ou no Carnaval da Bahia[8] em 2023, o reconhecimento facial já começa a ser utilizado para fins criminais aqui no Brasil.

Em decisão exarada em 12/01/2023, o ministro Alexandre de Moraes determinou à Polícia Federal a obtenção todas as imagens das câmeras do Distrito Federal que possam auxiliar no reconhecimento facial dos terroristas que praticaram os atos do dia 8 de janeiro, a lista e identificação de hóspedes que chegaram em Brasília junto a todos os hotéis e hospedarias do Distrito Federal, bem como a filmagem do saguão para a devida identificação de eventuais participantes dos atos terroristas. Determinou, também, ao Tribunal Superior Eleitoral que utilizasse a consulta e acesso aos dados de identificação civil mantidos naquela Corte, bem como de outros dados biográficos necessários à identificação e localização de pessoas envolvidas nos atos terroristas do dia 8 de janeiro (Brasil, 2023).

No mesmo inquérito mencionado acima, o ministro Alexandre de Moraes deferiu requerimento da Polícia Federal, que pediu autorização para acesso ao Banco Multibiométrico e de Impressões Digitais, conforme decisão do dia 3 de fevereiro (Brasil, 2023).

A questão é que o reconhecimento facial (ainda sem regulamentação específica) se encaixaria na questão da prova digital, ainda que inominada. Como visto anteriormente, o reconhecimento facial é realizado por uma inteligência artificial, que analisa as imagens fornecidas para identificar a identidade de uma pessoa após realizar comparações.

A prova digital, então, pode ser conceituada como o elemento jurídico apto a demonstrar a ocorrência ou não de um fato, delimitando suas características e circunstâncias, bem como os sujeitos a ele envolvidos e a dinâmica das ações. Seria um instrumento jurídico vocacionado a demonstrar a ocorrência de um fato e suas circunstâncias, tendo ele ocorrido total ou parcialmente em meios digitais ou, se fora deles, esses sirvam como instrumento para sua demonstração (Thamay; Tamer, 2022).

A viabilidade da evidência digital como prova é inicialmente fundamentada pelo art. 369[9] do Código de Processo Civil (CPC), que autoriza as partes a empregar todos os meios legal ou moralmente legítimos de prova, ainda que não previstos em lei, vedada a prova

[7] A intenção, à época, era impedir a entrada de torcedores que estavam proibidos de frequentar estádios de futebol. Mais detalhes disponíveis em: https://copadomundo.uol.com.br/noticias/redacao/2014/04/19/beira-rio-ira-testar-sistema-de-reconhecimento-facial-contra-bagunceiros.htm

[8] Nesse caso, o reconhecimento facial foi utilizado para identificar foragidos da polícia. Ver: https://g1.globo.com/fantastico/noticia/2023/02/26/com-ajuda-de-cameras-de-reconhecimento-facial-77-foragidos-da-policia-sao-presos-no-carnaval-da-bahia.ghtml

[9] Art. 369. As partes têm o direito de empregar todos os meios legais, bem como os moralmente legítimos, ainda que não especificados neste Código, para provar a verdade dos fatos em que se funda o pedido ou a defesa e influir eficazmente na convicção do juiz (BRASIL, 2015).

ilícita. A questão é o quanto se pode confiar nessa prova, de forma que existe uma demanda por maior cuidado no que diz respeito à extração e documentação, para conferir confiabilidade e correspondência com a realidade dos fatos (Souza; Munhoz; Carvalho, 2023).

Há meios de preservar evidências com alta confiança para embasar as decisões judiciais, com histórico de discussão e validação, passíveis de serem questionados, cabendo às partes se munir de embasamentos sólidos para argumentar ou não sobre a adequação da evidência no caso concreto. A confiança em relação ao conteúdo de uma evidência digital está intrinsicamente ligada aos meios utilizados para abstrair a realidade ou validar seu conteúdo (Souza; Munhoz; Carvalho, 2023).

Segundo Badaró, no caso das provas digitais, para que seja atestada a sua autenticidade e integridade, devem ser seguidos os métodos informáticos de obtenção, registro, armazenamento, análise e apresentação dos elementos de prova digitais que registrem as melhores práticas nacionais e internacionais. Sua apresentação judicial deve se dar por meio de prova pericial, sendo essencial a completa documentação da cadeia de custódia, para que tenha potencial epistêmico adequado (2021).

Elenca-se, dessa forma, os requisitos mais adequados para documentação de uma prova digital: 1) autenticidade, sobre a identificação da origem e autoria da prova; 2) completude, sobre a integralidade do fato; 3) integridade, em que a documentação se mantém imutável e confiável; 4) temporalidade, marcando sua referência temporal; 5) auditabilidade, em que haja integrabilidade e publicidade da prova; e 6) cadeia de custódia (Souza; Munhoz; Carvalho, 2023).

Tendo em vista a viabilidade da utilização das provas digitais (desde que atendidos os requisitos) e que o reconhecimento facial é uma realidade, deve-se atentar para os fatos: ao final de 2021, já haviam mais de um bilhão de câmeras de monitoramento no mundo (Bischoff, 2023), e mais da metade delas tem capacidade analítica (IHS Markit, 2016).

O avanço das tecnologias e seu uso cada vez mais incorporado ao cotidiano da humanidade o que implica análise crítica e reflexões sobre sua utilização, especialmente quando juridicamente relevante, tendo em vista os possíveis impactos nos direitos e, nesse caso, no devido processo penal.

## 4. CONTROLE DA PROVA NO RECONHECIMENTO FACIAL

O avanço tecnológico tende a possibilitar a criação de um verdadeiro Leviatã digital, com poderes absolutos de vigilância, o que requer cuidadoso regramento em leis específicas que visem a proteção da privacidade dos cidadãos (Fernandes; Meggiolaro; Prates, 2022).

A questão que surge quanto à aplicação desses recursos é o limite tênue que existe entre os direitos fundamentais e a utilização do reconhecimento facial, em alusão ao sistema Panóptico de Bentham. Também implica questões éticas em relação ao uso que se possa fazer da tecnologia para finalidades ilícitas e ampla manipulação. O rápido acesso a dados e antecedentes criminais de qualquer pessoa levanta um novo debate quanto ao direito de esquecimento, à medida que se ingressa em uma espécie de *Black Mirror* da vida real. O uso desenfreado e cotidiano dessa tecnologia por redes sociais possibilita a criação de amplo repositório de dados faciais, permitindo maior precisão e amplitude aos sistemas, aos custos de reiteradas violações aos direitos de personalidade. Ainda, com a aplicação do reconhecimento facial à identificação em massa, eventuais falhas no sistema podem significar a identificação incorreta de suspeitos (Rosa; Bernardi, 2018).

A ausência de uma regulação ou orientação de alcance geral, somada ao fato de que bases de dados públicas e privadas – algumas contendo informações detalhadas sobre as vidas civil e penal das pessoas – já coletavam registros biométricos faciais mesmo antes do país aprovar a LGPD, confirma a preocupação sobre o caráter ético do emprego do reconhecimento facial (Francisco; Hiurel; Rielli, 2020).

Assim como qualquer outra tecnologia emergente, o reconhecimento facial representa uma novidade radical com crescimento relativamente rápido, capaz de causar impactos proeminentes de forma incerta e ambígua. Regular o uso de uma tecnologia emergente é algo complexo e deve preservar direitos civis sem privar a sociedade de eventuais benefícios da inovação, sem que se tenha exata clareza dos possíveis impactos daquela tecnologia (Francisco; Hiurel; Rielli, 2020).

O fato é que não há uma regulação específica sobre o uso do reconhecimento facial como meio de prova no processo penal. Observa-se que, embora o Código de Processo Penal seja defasado em relação às novas metodologias de investigação digital, aparentemente o reconhecimento facial algorítmico não violaria o art.  226 do CPP. As peculiaridades do funcionamento deste tipo de modelo matemático computacional exigem que, ao menos, sejam sopesadas as questões que surgem, sob pena de deixar-se de observar direitos processuais mínimos que devem ser assegurados ao indivíduo (Cenci, 2023).

O Decreto n° 10.046/2019, que dispõe sobre governança no compartilhamento de dados no âmbito da administração pública, definiu atributos biométricos como “características biológicas e comportamentais mensuráveis da pessoa natural que podem ser coletadas para reconhecimento automatizado, tais como a palma da mão, as digitais dos dedos, a retina ou a íris dos olhos, o formato da face, a voz e a maneira de andar” (Brasil, 2019). Interessante

ressaltar a possibilidade de utilização desses atributos biométricos para fins de reconhecimento automatizado.

A Lei 13.709/2018, Lei Geral de Proteção de Dados (LGPD), veio para regular o tratamento de dados pessoais, inclusive nos meios digitais, de pessoas naturais e jurídicas, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (Brasil, 2018).

Em seu art. 3º, a LGPD dispõe que ela deve ser aplicada a qualquer operação de tratamento realizada por pessoas, naturais ou jurídicas, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados. No art. 5º, II, identifica-se uma definição importante para o presente trabalho, ao conceituar 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" (Brasil, 2018)

Extrai-se da LGPD, portanto, que dado biométrico é dado sensível. E esse fato implica uma limitação de seu uso, nos termos do art. 11. O art. 4, entretanto, faz uma ressalva importante: estabelece que a LGPD não se aplica ao tratamento de dados pessoais realizado para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais (Brasil, 2018).

Logo, o uso de dados biométricos sensíveis para fins de segurança pública e investigação criminal não é regulado pela LGPD. O art. 4, §1° estabelece que tratamento de dados pessoais para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, desde que observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos na LGPD (Brasil, 2018).

Esta legislação específica ainda não existe. Há, todavia, um projeto de lei que pretende regular a matéria, preenchendo a lacuna. O Projeto de Lei nº 1.515/2022 objetiva regulamentar o tratamento de dados pessoais para fins exclusivos de segurança do Estado, de defesa nacional, de segurança pública, e de investigação e repressão de infrações penais (Brasil, 2022).

A despeito das críticas, a regulação deve servir a uma dupla finalidade: proteger os direitos e liberdades fundamentais dos cidadãos e, ao mesmo tempo, viabilizar o tratamento automatizado de dados pessoais para fins de otimizar a persecução penal, especialmente

levando-se em consideração os desafios impostos pela sociedade global do risco (Fernandes; Resende, 2023).

No que diz respeito especificamente ao uso do reconhecimento facial, o ordenamento jurídico brasileiro também apresenta lacuna. Há, entretanto, tramitação do Projeto de Lei 3069/2022[10], que regulamenta o uso do reconhecimento facial automatizado pelas forças de segurança pública em investigações criminais ou procedimentos administrativos.

O problema atual e iminente é que não há transparência acerca dos algoritmos utilizados para realizar o reconhecimento facial automatizado. Algumas empresas não expõem ao certo como funciona o algoritmo, o que dificulta e até mesmo impede o questionamento do resultado. Fato é que os únicos com acesso total aos algoritmos são os próprios programadores (Araújo; Cardoso; Paula, 2021).

A transparência e a prestação de contas são imprescindíveis. Somente tecnologias auditáveis poderiam ser utilizadas pelo Estado, sem prejuízo das garantias constitucionais. Na mesma linha, também se mostra indispensável o controle da fonte primária dos algoritmos. Os responsáveis por sua elaboração e programação merecem atenção dos responsáveis, a fim de que essa influência não perpetue pré-conceitos (Araújo; Cardoso; Paula, 2021).

A exposição algorítmica, com a disponibilização de códigos-fonte ou auditorias irrefletidas, poderiam gerar uma ilusão de clareza. Dessa forma, a regulação da aplicação algorítmica em *softwares* poderia trazer benefícios, como oferecer clareza sobre alcances e verificações, permitindo uma estrutura e conformidade (Peixoto; Silva, 2019).

A Lei 13.709/2018, LGPD, trata da questão da transparência no tratamento de dados. O Art. 6º, VI, entretanto, faz ressalva aos segredos comercial e industrial. Segundo Fekete (2017) o segredo de negócio constitui uma categoria específica de direito da propriedade intelectual. Sua tutela jurídica encontra fundamento no art. 5º, X, XII e XXIX, da Constituição Federal, garantindo aos brasileiros e aos estrangeiros residentes no país a inviolabilidade da intimidade, do sigilo da correspondência e das comunicações e a proteção

[10] Art. 1º Esta Lei dispõe sobre o uso de tecnologia de reconhecimento facial automatizado no âmbito das forças de segurança pública.
Art. 2º O principal uso dessa tecnologia diz respeito à identificação de pessoas no âmbito de investigações policiais e/ou procedimentos administrativos.
§ 1º No âmbito da investigação criminal empregar-se-á o reconhecimento facial sempre que houver necessidade de se averiguar a identidade de autores, coautores, testemunhas e/ou vítimas relacionadas a algum fato criminoso.
(...)
Art. 3º Para os efeitos desta Lei considera-se:
I - Reconhecimento Facial (RF): procedimento biométrico automatizado com fim de identificação humana, realizado a partir da captura de uma imagem facial; (...)

às criações industriais, respectivamente e nas normas que regulam a lealdade concorrencial, estabelecidas no art. 195, XI e XII da Lei 9.279/1996, a Lei da Propriedade Industrial.

De forma mais específica, verifica-se que a Lei 9.609/1998 (Lei do *Software*), estabelece que o programa de computador recebe proteção da propriedade intelectual, de forma que seus direitos ficam assegurados por 50 anos. Nos termos do art. 3º, §2º, as informações sobre os trechos do programa e outros dados capazes de identificá-lo e caracterizar sua originalidade são de caráter sigiloso, não podendo ser reveladas, salvo por ordem judicial ou a requerimento do próprio titular (Brasil, 1998). Ou seja, não há como auditar, a princípio, como o algoritmo trabalha para realizar o reconhecimento.

Há possibilidade, entretanto, de controlar os *inputs*. Um exemplo é a utilização do código HASH. Para Souza, Munhoz e Carvalho (2023) esse código é o resultado de um algoritmo que produz uma sequência de caracteres com base no conteúdo do arquivo digital. Qualquer alteração feita no conteúdo desse arquivo implica alteração do código HASH. Ou seja, há como verificar se o arquivo foi modificado. Segundo os autores, enviar arquivos por meio de aplicativo de mensagens, comprimir arquivos para reduzir tamanho, ou mesmo abrir e salvar arquivos podem efetivamente alterar o código HASH. Por outro lado, enviar arquivos por e-mail, transportar em pen drives ou HD externos, salvar na nuvem ou compartilhar link são procedimentos que não alteram a integridade do arquivo.

Além de verificar possível modificação, pode ser necessário proteger a evidência contra alteração de maneira confiável. Nesse caso, há possibilidade de uso da tecnologia de *blockchain*, em que um *software* realiza a verificação da modificação nos dados e correção automática com base em replicadores desses dados, gerando sua imutabilidade, não permitindo modificação do conteúdo inserido (Souza; Munhoz; Carvalho, 2023).

A cadeia de custódia também deve ser preservada. Segundo Carvalho (2020), a evidência digital deve ser mantida em segurança, preservando sua integridade. Todo procedimento forense deve ser realizado com uma cópia no intuito de preservar o material original. Ademais, todos os dispositivos de armazenamento devem estar limpos (não podem conter sequer um bit de informação anterior), sob pena de contaminar a evidência e gerar um resultado equivocado.

Identificam-se, portanto, alguns cuidados que devem ser observados para o controle da qualidade da prova do reconhecimento facial: verificar as condições de aquisição de imagem como a qualidade (iluminação, resolução, fundo, ângulo de captura) condições ambientais (iluminação, posição da câmera), uso de acessórios que poderiam modificar características pessoais, a maneira como a imagem foi isolada, extraída e preservada, se o meio físico de

acondicionamento do arquivo digital foi adequado e estava “limpo”, se o arquivo foi modificado (HASH) e sua integridade preservada (blockchain).

Não se descarta, por fim, a possibilidade de solicitar a revisão da decisão automatizada, conforme art. 20 da LGPD, que afirma que o titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses.

## 5. CONSIDERAÇÕES FINAIS

O reconhecimento facial biométrico automatizado vem se desenvolvendo rapidamente. Ele consiste numa técnica de identificação biométrica que reconhece e diferencia rostos humanos por meio de um *software*, o qual mapeia de forma matemática os traços e espaços existentes em diferentes imagens digitais de uma mesma pessoa.

A capacidade de reconhecimento da tecnologia a torna atraente para o uso dos órgãos de segurança, ampliando o número de câmeras de vigilância em espaços públicos. Como consequência, sua utilização pelas forças policiais para identificar foragidos e suspeitos tem se tornado uma realidade.

Apesar da utilidade de suas aplicações, o uso do reconhecimento facial ainda encontra alguns limites, tendo em vista a preocupação dos direitos fundamentais e a questão da acurácia e transparência dos algoritmos. Ainda assim, a utilização da ferramenta parece encontrar respaldo da população, cuja maioria demostrou aceitação para aplicação na segurança pública. Inclusive vem sendo utilizado pelo Poder Judiciário.

A lacuna legislativa verificada, especialmente no que diz respeito à chamada LGPD Penal e à uma regulamentação específica sobre a utilização da tecnologia de reconhecimento facial impõe limitações hermenêuticas e implicam aplicações analógicas de vários dispositivos legais.

Levando-se em consideração que prova é tudo aquilo que contribui para a formação do convencimento do magistrado a fim de demonstrar os fatos alegados pelas partes no processo, a limitação para a produção e meios de prova é fixada pela vedação das provas ilícitas.

A formação da prova no processo penal deve obedecer a alguns requisitos, para só então atingir o *standard* probatório mais confiável e exigido pelo ordenamento jurídico brasileiro. A prova digital, nesse caso, deve ser transparente, íntegra, auditável e a utilização do reconhecimento facial deve atender a esses requisitos.

O fato é que as forças de segurança têm a sua disposição mais de um bilhão de câmeras de vigilância ao redor do mundo e que o avanço das tecnologias está cada vez mais incorporado ao cotidiano da humanidade.

Dessa forma, elenca-se os requisitos para documentação de uma prova digital: autenticidade sobre a identificação da origem e autoria da prova; completude sobre a integralidade do fato; integridade, em que a documentação se mantém imutável e confiável; temporalidade, marcando sua referência temporal; auditabilidade, em que haja integrabilidade e publicidade da prova; e cadeia de custódia.

Além disso, identificam-se alguns cuidados que devem ser observados para o controle da prova do reconhecimento facial: verificar as condições de aquisição de imagem como a qualidade (iluminação, resolução, fundo, ângulo de captura), as condições ambientais (iluminação, posição da câmera), uso de acessórios que poderiam interferir nas características individuais, a maneira como a imagem foi isolada, extraída e preservada, se o meio físico de acondicionamento do arquivo digital foi adequado e se estava "limpo", se o arquivo foi modificado (HASH) e sua integridade preservada (blockchain).

Por fim, verifica-se que o assunto demanda uma pesquisa mais profunda e robusta, especialmente no que diz respeitos ao modo como se dá o processamento da imagem para o reconhecimento facial automatizado.

Pesquisas futuras devem concentrar esforços no estudo da visão computacional e *deep learning* com vistas a fomentar as bases para melhor e maior compreensão do impacto da tecnologia de reconhecimento facial automatizado no direito e, de modo especial com o que se relaciona com a presente pesquisa, no que tange à fiabilidade da prova no processo penal.

## REFERÊNCIAS

ARAÚJO, Romulo de Aguiar; CARDOSO, Naiara Deperon; PAULA, Amanda Marcélia de. Regulação e uso do reconhecimento facial na segurança pública do Brasil. **Revista de Doutrina Jurídica**, Brasília, DF, v. 112, n. 00, p. e021009, 2021. DOI: 10.22477/rdj.v112i00.734. Disponível em: https://revistajuridica.tjdft.jus.br/index.php/rdj/article/view/734. Acesso em: 14 jul. 2023.

BADARÓ, Gustavo Henrique. Os standards metodológicos de produção na prova digital e a importância da cadeia de custódia. **Boletim IBCCRIM**, ano, v. 29, p. 7-9, 2021. Disponível em: https://www.ibccrim.org.br/publicacoes/edicoes/747/8544. Acesso em: 29 jul. 2023.

BISCHOFF, Paul. ***Surveillance camera statistics: which cities have the most CCTV cameras?*** Coluna publicada em 23 de maio de 2023. Comparitech, Kent, United Kingdom. Disponível em: https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/. Acesso em: 29 jul. 2023.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 1515/2022**. Lei de Proteção de Dados Pessoais para fins exclusivos de segurança do Estado, de defesa nacional, de segurança pública, e de investigação e repressão de infrações penais. Brasília, DF: Câmara dos Deputados, 2022. Disponível em: https://www.camara.leg.br/propostaslegislativas/2326300. Acesso em: 14 jul. 2023.

BRASIL. **[Constituição Federal (1988)]. Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 14 jul. 2023.

BRASIL. **Decreto 10.046, de 9 de outubro de 2019**. Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm. Acesso em: 03 ago. 2023.

BRASIL. **Decreto-lei nº 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: 14 jul. 2023.

BRASIL. **Lei 9.609, de 19 de fevereiro de 1998**. Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9609.htm. Acesso em: 12 ago. 2023.

BRASIL. **Lei 13.105, de 16 de março de 2015**. Código de Processo Civil. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em: 14 jul. 2023.

BRASIL. **Lei 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jul. 2023.

BRASIL. Superior Tribunal de Justiça. **Habeas Corpus n. 598.886/SC – Brasília.** Reconhecimento fotográfico de pessoa realizado na fase do inquérito policial. Inobservância do procedimento previsto no art. 226 do CPP. Prova inválida como fundamento para a condenação. Rigor probatório. Necessidade para evitar erros judiciários. Participação de menor importância. Não ocorrência. Ordem parcialmente concedida. Relator: Min. Rogerio Schietti Cruz, 27 de outubro de 2020. Disponível em: https://www.stj.jus.br/sites/portalp/SiteAssets/documentos/noticias/27102020%20HC598886-SC.pdf Acesso em: 14 jul. 2023.

BRASIL. Supremo Tribunal Federal. **Habeas Corpus n. 84.203/RS.** Filmagem realizada pela vítima. Gravação de imagens feita com o objetivo de identificar o autor de danos praticados contra o patrimônio da vítima. Legitimidade jurídica desse comportamento do ofendido. Desnecessidade, em tal hipótese, de prévia autorização judicial. Alegada ilicitude da prova penal. Inocorrência. Peça acusatória que satisfaz, plenamente, as exigências legais Pedido indeferido. Relator: Min. Celso de Mello, Segunda Turma, julgado em 19 de outubro de 2004.

Disponível em: https://jurisprudencia.stf.jus.br/pages/search/sjur166711/false. Acesso em: 14 jul. 2023.

BRASIL. Supremo Tribunal Federal. **Inquérito 4923/DF**. Relator: Min. Alexandre de Moraes, protocolado em 12 de janeiro de 2023. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=6547024. Acesso em: 12 ago. 2023.

CARVALHO, Romullo Wheryko Rodrigues De. A Importância da Cadeia de Custódia na Computação Forense. **Revista Brasileira de Criminalística**, [S. l.], v. 9, n. 2, p. 134–138, 2020. DOI: 10.15260/rbc.v9i2.463. Disponível em: https://revista.rbc.org.br/index.php/rbc/article/view/463. Acesso em: 12 ago. 2023.

CENCI, Gabrielle Casagrande. O panóptico digital e o reconhecimento facial pela IA no CPP brasileiro. Coluna publicada em 20 de junho de 2023, **Revista Eletrônica CONJUR**, São Paulo. Disponível em: https://www.conjur.com.br/2023-jun-20/gabrielle-cenci-reconhecimento-facial-ia-cpp-brasileiro. Acesso em: 14 jul. 2023.

FEKETE, Elisabeth Kasznar. Segredo de empresa. **Enciclopédia jurídica da PUC-SP**. Celso Fernandes Campilongo, Alvaro de Azevedo Gonzaga e André Luiz Freire (coords.). Tomo: Direito Comercial. Fábio Ulhoa Coelho, Marcus Elidius Michelli de Almeida (coord. de tomo). 1. ed. São Paulo: Pontifícia Universidade Católica de São Paulo, 2017. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/248/edicao-1/segredo-de-empresa. Acesso em: 14 jul. 2023.

GARVIE, C.; BEDOYA, A. M.; FRANKLE, J. *The perpetual line-up. Unregulated police face recognition in America*. **Georgetown Law Center on Privacy & Technology**. 2019. Disponível em: https://www.perpetuallineup.org/background. Acesso em 29 jul. 2023.

IHS MARKIT. ***Video surveillance: How technology and the cloud is disrupting the market. Technical Report***, 2016. Disponível em: https://cdn.ihs.com/www/pdf/IHS-Markit-Technology-Video-surveillance.pdf. Acesso em: 31 jul. 2023.

MENA, Isabela. **Verbete Draft: o que é Reconhecimento Facial**. Coluna publicada em 30 de maio de 2018. Disponível em: https://www.projetodraft.com/verbete-draft-o-que-e-reconhecimento-facial/. Acesso em: 05 ago. 2023.

OLIVEIRA, Loryne Viana *et al*. Aspectos ético-jurídicos e tecnológicos do emprego de reconhecimento facial na segurança pública no Brasil. **Revista Tecnologia e Sociedade**, v. 18, n. 50, p. 114-135, 2022. Disponível em: https://periodicos.utfpr.edu.br/rts/article/view/12968. Acesso em: 14 jul. 2023.

PEIXOTO, Fabiano Hartmann; SILVA, Roberta Zumblick Martins da. **Inteligência artificial e direito**. Curitiba: Alteridade, v. 1, 2019.

PEW RESEARCH CENTER. ***More Than Half of U.S. Adults Trust Law Enforcement to Use Facial Recognition Responsibly*.** Publicado em 05 de setembro de 2019. Disponível em: https://www.pewresearch.org/internet/2019/09/05/more-than-half-of-u-s-adults-trust-law-enforcement-to-use-facial-recognition-responsibly/. Acesso em: 30 jul. 2023.

RANGEL, Paulo. **Direito processual penal**. 30. ed. Barueri: Atlas, 2023.

ROSA, Alexandre Morais da; BERNARDI, Sahra di. Quando o reconhecimento facial chega ao processo penal. Coluna publicada em 03 de agosto de 2018, **Revista Eletrônica CONJUR**, São Paulo. Disponível em: https://www.conjur.com.br/2018-ago-03/limite-penal-quando-reconhecimento-facial-chega-processo-penal. Acesso em: 14 jul. 2023.

SCHLOTTFELDT, Shana. ***All eyes on me*: riscos e desafios da tecnologia de reconhecimento facial à luz da Lei Geral de Proteção de Dados**. Rio de Janeiro: Lumen Juris, 2022.

SMITH, Marcus; MILLER, Seumas. *The ethical application of biometric facial recognition technology*. **Ai & Society**, p. 1-9, 2022. DOI https://doi.org/10.1007/s00146-021-01199-9. Disponível em: https://link.springer.com/article/10.1007/s00146-021-01199-9. Acesso em: 29 jul. 2023.

SOUZA, Bernardo de Azevedo e; MUNHOZ, Alexandre; CARVALHO, Romullo. **Manual prático de provas digitais**. São Paulo: Thomson Reuters Brasil, 2023.

THAMAY, Renan; TAMER, Maurício. **Provas no direito digital – conceito da prova digital, procedimentos e provas em espécie**. 2 ed. São Paulo: Thomson Reuters, 2022.

TAVARES, Juarez; CASARA, Rubens. **Prova e Verdade**. 1 ed. São Paulo: Tirant lo blanch, 2020.

TÁVORA, Nestor; ALENCAR, Rosmar Rodrigues. **Curso de direito processual penal**. 10 ed. Salvador: JusPodivm, 2015.

TRIBUNAL SUPERIOR ELEITORAL (TSE). **Em 2021, TSE ampliou ações para implementar a Identificação Civil Nacional (ICN)**. Notícia publicada em 23 de dezembro de 2021. Disponível em: https://www.tse.jus.br/comunicacao/noticias/2021/Dezembro/em-2021-tse-ampliou-acoes-para-implementar-a-identificacao-civil-nacional-icn. Acesso em: 30 jul. 2023.