ACADEMIA DE DIREITO
Editora UnC

A TECNOLOGIA DE RECONHECIMENTO FACIAL E SUA UTILIZAÇÃO COMO PROVA NO PROCESSO PENAL

FACIAL RECOGNITION TECHNOLOGY AND ITS USE AS EVIDENCE IN CRIMINAL PROCEEDINGS

Bruna Gonçalves Scopel[1]
Eduardo Puhl[2]

RESUMO

O presente artigo aborda a integração da tecnologia de reconhecimento facial na vigilância pública para o controle social pelas forças de segurança, especialmente sua compatibilidade como prova no âmbito do processo penal. Questiona se a prova produzida por meio da tecnologia de reconhecimento facial pode ser considerada lícita, para fins de utilização no processo penal, tendo em vista que não há uma regulamentação a seu respeito. O estudo tem como objetivo definir o reconhecimento facial, analisar de que maneira esta tecnologia tem sido utilizada pelas forças de segurança pública e identificar a compatibilidade ou não do reconhecimento facial com a produção de provas no processo penal. Por meio de uma abordagem exploratória, o artigo sugere o reconhecimento facial como uma forma de evidência digital. Conclui-se que, sob certas condições, a tecnologia de reconhecimento facial está alinhada com os padrões legais e pode ser um meio válido para comprovar identidade em processos criminais.

Palavras-chave: reconhecimento facial; prova; processo penal.

ABSTRACT

The present article addresses the integration of facial recognition technology in public surveillance for social control by security forces, especially its compatibility as evidence within the criminal process. It questions whether evidence produced through facial recognition technology can be considered lawful for use in criminal proceedings, given the absence of specific regulation. The study aims to define facial recognition, analyze how this technology has been employed by public security forces, and identify whether facial recognition is compatible with evidence production in criminal proceedings.

[1]Graduanda em Direito pela Universidade do Contestado – UNC. Campus Concórdia. Santa Catarina. Brasil. E-mail: bruna.scopel@aluno.unc.br.
[2]Doutorando em Direito na Universidade do Oeste de Santa Catarina – UNOESC. Mestre em Direito pela Universidade do Oeste de Santa Catarina – UNOESC (2020). Membro do Grupo de Estudo e Pesquisa “Proteção Das Liberdades Na Sociedade Do Controle” (CNPq/UNOESC). Professor do Curso de Direito da Universidade do Contestado (UNC). Campus Concórdia. Santa Catarina. Brasil. Orcid: https://orcid.org/0000-0002-9598-3892. E-mail: eduardopuhl@gmail.com.

Acad. Dir. (ISSN: **2763-6976**)
v. 6, p. 3678-3700, 2024

Through an exploratory approach, the article suggests facial recognition as a form of digital evidence. It concludes that, under certain conditions, facial recognition technology aligns with legal standards and can serve as a valid means to establish identity in criminal processes.

Key words: facial recognition; evidence; criminal procedure.

Artigo recebido em: 24/08/2024
Artigo aceito em: 11/10/2024
Artigo publicado em: 12/12/2024
Doi: https://doi.org/10.24302/acaddir.v6.5587

1 INTRODUÇÃO

Conforme Fernando Capez (2024), considera-se prova, para fins penais, o elemento que baseia a conclusão acerca da veracidade de fatos ou circunstâncias, a qual tem a finalidade de convencer seu destinatário, o juiz, na medida em que este não presenciou os fatos que são submetidos à sua apreciação. Dessa forma, é por meio da prova que o juiz pode reconstruir o momento em questão, para verificar se o delito, de fato, ocorreu e quem foi o seu autor.

O que se almeja com a prova é alcançar a verdade processual, visto ser impossível alcançar no processo, a verdade absoluta. Ademais, conceitua-se como prova, tudo aquilo que possa fornecer indicações úteis, cuja comprovação é necessária.

Nesse contexto, considerando os princípios previstos na Constituição da República Federativa do Brasil de 1988, dentre os quais destacam-se o devido processo legal, a inadmissibilidade de provas ilícitas e a proteção dos dados pessoais, infere-se que o tema do presente trabalho é a prova no processo penal.

O recorte do tema encontra delimitação na legitimidade da prova produzida por meio de tecnologia de reconhecimento facial, haja vista que, diante do amplo uso de câmeras de vigilância com a finalidade de promover a segurança, o reconhecimento facial por meio da inteligência artificial vem se expandindo.

A tecnologia de reconhecimento facial tem sido utilizada com mais frequência e com diversas finalidades, dentre as quais, o uso da referida tecnologia por órgãos públicos, a fim de realizar um controle mais efetivo, inclusive na investigação criminal.

Nesse sentido, questiona-se se a prova produzida por meio da tecnologia de reconhecimento facial pode ser considerada lícita, para fins de utilização no processo penal, tendo em vista que, no momento presente, não há uma regulamentação a respeito do uso do reconhecimento facial automatizado como meio de prova, gerando dúvidas a respeito de sua legitimidade.

Objetiva-se, de maneira geral, conceituar o que seja tecnologia de reconhecimento facial, identificando a legislação nacional e internacional pertinente, inclusive projetos de lei no Brasil, a fim de verificar como esta tecnologia vem sendo utilizada pelas forças de segurança pública no País.

Ademais, o presente trabalho busca identificar, de maneira específica, o conceito de prova no processo penal, no intuito de verificar a (in)compatibilidade da tecnologia de reconhecimento facial com o ordenamento jurídico brasileiro.

Este estudo baseia-se no método de abordagem dedutivo, consistente em analisar a tecnologia de reconhecimento facial de maneira ampla, para compreender suas características e como pode ser utilizado como meio de prova no processo penal, com utilização de técnica de revisão bibliográfica.

Para tanto, a presente pesquisa divide-se em três seções. A primeira seção tem como foco o entendimento do que seja tecnologia de reconhecimento facial, bem como aborda a legislação pertinente. A segunda seção busca verificar de que maneira a tecnologia de reconhecimento facial vem sendo utilizada pelas forças de segurança. Por fim, a terceira seção objetiva identificar a compatibilidade ou não do reconhecimento facial com a produção de provas no processo penal. Ao final são apresentadas as conclusões.

2 RECONHECIMENTO FACIAL E LEGISLAÇÃO PERTINENTE

Sabe-se que o processo é o meio pelo qual o Estado procede à composição da lide, aplicando o direito ao caso concreto e solucionando conflitos. Sem processo não meio adequado para solucionar litígios, visto ser instrumento essencial para a manutenção da paz social (CAPEZ, 2024).

O processo penal é fundamentado em direitos e garantias fundamentais, dentre os quais, destaca-se o devido processo legal, previsto no art. 5º, LIV, da Constituição Federal. Esse princípio assegura que ninguém pode ser privado de sua liberdade ou

de seus bens sem que sejam observadas as regras estabelecidas por lei durante todo o desenvolvimento do processo (CAPEZ, 2024).

Destaca-se ainda, a inadmissibilidade de provas obtidas por meios ilícitos, conforme estipulado no art. 5º, LVI, da referida Constituição. Ao considerar inadmissíveis as provas obtidas por meios ilícitos, a Constituição proíbe a utilização de todas as provas obtidas de forma ilegal, abrangendo tanto aquelas consideradas ilícitas quanto as que são ilegítimas, seja por violação de normas de direito material ou processual (CAPEZ, 2024).

Sob esse aspecto, considera-se notável a crescente adoção da tecnologia de reconhecimento facial no contexto do processo penal. Esta tecnologia tem sido aplicada não apenas para detectar atividades suspeitas, como o tráfico internacional de drogas em aeroportos brasileiros, mas também para localizar indivíduos foragidos da justiça (ROSA; BERNARDI, 2018).

O reconhecimento facial é uma técnica de identificação biométrica na qual um *software* mapeia os traços faciais de um indivíduo e, por meio de algoritmos, compara esses traços com uma imagem digital do mesmo indivíduo, determinando se há correspondência e reconhecendo ou negando sua identidade (MENA, 2018).

A fase de mapeamento do rosto considera os pontos nodais, que são características distintivas que diferenciam uma pessoa da outra. Alguns exemplos desses pontos nodais incluem a distância entre os olhos, a largura do nariz, a profundidade das órbitas oculares, a forma das maçãs do rosto e o comprimento da linha da mandíbula (MENA, 2018).

A relação entre esses pontos cria uma geometria espacial única, que é capturada e armazenada em forma de dados, chamada de *template* ou *faceprint*, e quando uma nova imagem é apresentada, o *software* faz a comparação (Mena, 2018).

Após serem processados e comparados com imagens previamente coletadas e armazenadas em *big data*, obtém-se um padrão único de identificação facial, que pertence a uma pessoa específica (MARTINS, 2020).

Entretanto, o reconhecimento facial opera de maneira probabilística por natureza. Ao invés de fornecer respostas binárias definitivas como "sim" ou "não", o sistema avalia correspondências com diferentes graus de probabilidade (GARVIE; BEDOYA; FRANKLE, 2016).

A aquisição da imagem geralmente ocorre por meio de câmeras de vigilância, que tira fotos da face do indivíduo em tempo real, o que pode afetar a precisão do reconhecimento facial de várias maneiras. Fatores como a qualidade da imagem, condições ambientais e o uso de acessórios podem influenciar significativamente a acurácia dessa tecnologia (SCHLOTTFELDT, 2022).

Algumas características faciais podem ser melhores indicadores de semelhança do que outras. Muitos algoritmos de reconhecimento facial descobrem quais recursos são mais importantes por meio do treinamento. Durante o treinamento, os algoritmos de reconhecimento facial são expostos a pares de imagens faciais da mesma pessoa. Com o tempo, esses algoritmos aprendem a identificar quais características faciais são mais consistentes e significativas para determinar a semelhança entre rostos (GARVIE; BEDOYA; FRANKLE, 2016).

Para o reconhecimento facial, a subárea mais importante é o *deep learning.* Segundo Peixoto e Silva (2019), o *deep learning* é uma forma específica de aprendizagem de máquina onde redes neurais, estruturas de processamento inspiradas nos neurônios e no cérebro humano, são treinadas com múltiplas camadas de unidades, o que aprofunda a capacidade de aprendizado do sistema.

Desse modo, atualmente é possível verificar que a tecnologia de reconhecimento facial está evoluindo, se tornando cada vez menos passível de erro, e capaz de reconhecer o perfil de uma pessoa.

A ferramenta incrementada que possibilita a sistematização destas informações foi, propriamente, o banco de dados que, conforme Doneda (2011) são, fundamentalmente, um conjunto estruturado com uma determinada lógica, que procura proporcionar a extração do máximo proveito possível a partir de um conjunto de informações.

Para alcançar este resultado, os dados precisam passar por um processo de processamento utilizando aplicativos de *software* específicos. Esses aplicativos operam sobre um conjunto de dados previamente extraídos desses bancos de dados (MARTINS, 2020).

Acerca disso, entrou em vigor na União Europeia, no ano de 2016, o Regulamento Geral sobre Proteção de Dados - *General Data Protection Regulation - GDPR*, bem como na legislação brasileira, o Decreto 8.771/2016, Regulamentador do

Marco Civil da Internet, que em seu art. 14 define o dado pessoal e o tratamento de dados.

Conforme o referido artigo, dado pessoal é o dado relacionado à pessoa natural identificada ou identificável, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa (BRASIL, 2016).

Já o tratamento de dados, define-se como a operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (BRASIL, 2016).

O referido tratamento de dados é aplicado aos bancos de dados que são definidos na legislação brasileira pela Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), em seu art. 5º, inciso IV, como “conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico” (BRASIL, 2018).

Dessa forma, as informações biológicas humanas, denominadas biometria, como impressões digitais, impressões de voz, DNA e reconhecimento facial, por exemplo, são utilizadas como base para a identificação de pessoas (MARTINS, 2020).

Ocorre que, o art. 4º da Lei Geral de Proteção de Dados (LGPD), estabelece que a referida lei 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).

Outrossim, o parágrafo 1º do art. 4º estabelece que o tratamento dos dados pessoais supracitados será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei (BRASIL, 2018).

Desse modo, depara-se com a necessidade de regulamentação a respeito do uso do reconhecimento facial automatizado como meio de prova no processo penal, o qual deveria ser regido por legislação específica, atualmente inexistente no ordenamento jurídico brasileiro.

Em contrapartida, observa-se a aprovação da Lei de Inteligência Artificial na União Europeia, em abril de 2024, marcando um avanço significativo na

regulamentação desta tecnologia em rápida evolução. Essa legislação tem como objetivo garantir a proteção dos direitos fundamentais, da democracia, do Estado de direito e da sustentabilidade ambiental diante dos desafios apresentados pela IA avançada, enquanto impulsiona a inovação e consolida a liderança da Europa na indústria tecnológica (ALCASSA, 2024).

O texto normativo estabelece restrições específicas para o uso de sistemas de identificação biométrica pelas forças de segurança, permitindo seu emprego apenas em circunstâncias estritamente definidas e com salvaguardas rigorosas. O uso desses sistemas em tempo real só será permitido com autorização judicial ou administrativa prévia, aplicando-se em situações claramente definidas, como na busca direcionada de pessoas desaparecidas ou na prevenção de ataques terroristas (ALCASSA, 2024).

No Brasil, várias iniciativas estão em andamento, incluindo o Projeto de Lei 1.515/2022, que aborda a Lei Geral de Proteção de Dados (LGPD) com foco em segurança do Estado, defesa nacional, segurança pública e investigação e repressão de infrações penais. O objetivo principal deste projeto é regulamentar o artigo da LGPD que estabelece regras específicas para o tratamento de dados pessoais nessas circunstâncias (BRASIL; SEABRA, 2022).

O projeto está fundamentado em três pilares principais: proteção dos direitos fundamentais de segurança, liberdade e de privacidade; eficiência da atuação dos órgãos responsáveis; e intercâmbio de dados pessoais entre autoridades competentes (BRASIL; SEABRA, 2022).

De acordo com o Projeto de Lei 1.515/2022, caberá à Autoridade Nacional de Proteção de Dados (ANPD), atualmente responsável pela aplicação da LGPD, supervisionar a proteção dos dados pessoais nas circunstâncias estabelecidas por ele (BRASIL, 2022).

Ainda, no contexto do equilíbrio entre a proteção dos direitos fundamentais e o uso de inteligência artificial, destaca-se o Projeto de Lei 2.338/2023, cujo objetivo é regulamentar aspectos relevantes do uso de tecnologias de IA no território nacional (ALCASSA, 2024).

Ante o exposto, considerando-se que o reconhecimento facial é capaz de reconhecer o perfil de uma pessoa, podendo ser utilizado para fins de vigilância e segurança pública, e que ainda não existe legislação que o regulamente, passa-se a analisar como essa tecnologia vem sendo utilizada pelas forças de segurança.

3 A UTILIZAÇÃO DA TECNOLOGIA DE RECONHECIMENTO FACIAL PELAS FORÇAS DE SEGURANÇA

Após breves considerações sobre o reconhecimento facial, em que se conceitua tecnologia de reconhecimento facial, bem como aborda a legislação pertinente, é possível debater sobre a utilização desta tecnologia para fins de segurança pública.

Inicialmente, os órgãos de investigação que utilizam sistemas de reconhecimento facial o fazem de quatro maneiras, sendo estas a abordagem e identificação, na qual 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 e, a detenção e identificação, quando um indivíduo é detido, tem suas impressões digitais coletadas e uma foto de identificação é obtida (GARVIE; BEDOYA; FRANKLE, 2016).

Além disso, tem-se ainda a investigação e identificação, pois se o rosto de um suspeito estiver disponível em um elemento de informação durante uma investigação, uma foto ou vídeo dele é analisada no *software* de reconhecimento facial para fornecer pistas e, por fim, a *surveillance*, que ocorre quando o órgão de investigação está 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*, para pesquisar em vídeo em tempo real (GARVIE; BEDOYA; FRANKLE, 2016).

Segundo Schlottfeldt (2022), o reconhecimento facial também pode ser utilizado para reduzir significativamente o tempo necessário nas investigações criminais. Isso ocorre ao permitir que os investigadores identifiquem ou descartem rapidamente suspeitos após a ocorrência de um crime.

No cenário internacional, um exemplo do uso dessas tecnologias pode ser observado na China, onde o reconhecimento facial foi empregado pelo governo para monitorar o cumprimento das políticas de *lockdown* durante a pandemia de Covid-19. Com uma extensa rede de câmeras de monitoramento biométrico distribuídas pelo país, as autoridades exerceram um controle rigoroso sobre a população. Isso possibilitou a identificação de locais de disseminação do vírus, a aplicação do isolamento social para pessoas infectadas e a imposição de penalidades aos que violavam as medidas de quarentena (NABESHIMA, 2024).

Durante os Jogos Olímpicos de 2020, realizados em Tóquio em 2021 devido ao adiamento causado pela pandemia, o Japão se destacou pelo uso proeminente da tecnologia de reconhecimento facial. Medidas avançadas de segurança foram implementadas em várias facetas do evento, desde a recepção no aeroporto internacional até o controle de acesso aos locais de competição e a segurança em áreas públicas. Esses sistemas foram empregados para identificação e rastreamento de indivíduos, desempenhando um papel crucial na garantia da segurança do evento (NABESHIMA, 2024).

No Reino Unido, o uso do reconhecimento facial na segurança pública tem sido cada vez mais adotado, especialmente para fiscalizar e prevenir incidentes em grandes eventos. Exemplos notáveis incluem a coroação do Rei Charles e o Grande Prêmio da Grã-Bretanha de Fórmula 1, onde milhares de rostos foram escaneados ao vivo. Utilizando inteligência artificial, esses sistemas comparavam as imagens em tempo real com uma lista de observação de indivíduos procurados pela polícia, facilitando a identificação e detenção de suspeitos conforme registros policiais (NABESHIMA, 2024).

Nos Estados Unidos, o FBI tem uma base de dados com os rostos de 117 milhões de pessoas, segundo pesquisa de 2016 da Universidade Georgetown (SCHMIDT, 2022).

Ainda, um estudo realizado pela Pew Research Center (2019) demonstrou que 59% da população entrevistada aceita o 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.

Atualmente, não há uma lei federal estadunidense que regule a matéria, porém, em novembro de 2023, o deputado Ted Lieu apresentou o *Facial Recognition Act* à Câmara dos Representantes. Este projeto de lei propõe regulamentar o uso dessa tecnologia pela polícia, baseando-se na experiência de alguns estados. Ele estabelece limites significativos para a aplicação de vigilância por reconhecimento facial pelas forças de segurança, como a exigência de um mandado judicial que demonstre a causa provável de que um indivíduo tenha cometido um crime violento grave. Além disso, proíbe o uso do reconhecimento facial como única justificativa para busca, prisão ou outras ações policiais, e veda o uso dessa tecnologia para criar

registros que documentem como um indivíduo exerce seus direitos constitucionais, como participar de protestos legais (NABESHIMA, 2024).

Já no Brasil, o uso de sistemas biométricos de reconhecimento facial na segurança pública visando reconhecimento de criminosos tem se intensificado, 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 mulher (ALVES, 2019).

No Brasil, mais da metade do mercado de câmeras de vigilância e monitoramento é dominado por duas empresas, a brasileira Intelbras e a chinesa Dahua, conforme relatado pela Associação Brasileira das Empresas de Sistemas Eletrônicos de Segurança (Abese) e pela própria empresa asiática (SOUZA, 2024).

De acordo com a empresa chinesa, são vendidas entre 500 mil e 600 mil câmeras por mês para clientes públicos e privados. Além de Intelbras e Dahua, as chinesas Hikvision e Hawuei e a sueca Axis estão entre as empresas especializadas em câmeras com vendas no Brasil (SOUZA, 2024).

Além de identificar pessoas cujo rosto corresponde a alguém com mandado de prisão em aberto no banco de dados, a tecnologia de reconhecimento facial também possibilita a busca de pessoas suspeitas de crimes ou desaparecidas nas ruas. Isso pode ser feito com base em critérios como cor e tipo de roupa, presença de bolsa ou mochila, uso de boné, altura da pessoa e se estão acompanhadas de crianças (SOUZA, 2024).

Na Bahia, um dos estados onde o uso da ferramenta de reconhecimento facial é mais antigo, 1.438 pessoas já foram presas, sendo 185 delas nos primeiros meses deste ano. A precisão dos alertas tem sido aprimorada ao longo do tempo, e atualmente o sistema emite de três a quatro alertas por dia. Segundo a Secretaria de Segurança Pública da Bahia, desde a primeira prisão, houve apenas dois casos de "falsos positivos". Esses erros ocorreram porque os mandados de prisão associados aos indivíduos já haviam sido revogados (SOUZA, 2024).

Segundo relatório do Instituto Igarapé (2019), a utilização de sistemas de reconhecimento facial no Brasil em diferentes áreas é reportada pelo menos desde 2011.

Na cidade de São Paulo, o uso de câmeras de reconhecimento facial no sistema de transporte público ocorre desde 2017. Só nos dois primeiros anos, mais de 300 mil bilhetes foram bloqueados por suposto uso indevido (GARAY, 2019).

Em abril de 2018, a ViaQuatro, concessionária responsável pela linha 4-Amarela dos trens metropolitanos de São Paulo, anunciou a utilização de tecnologia de reconhecimento facial em painéis publicitários nas estações para monitorar as reações dos usuários. No entanto, essa iniciativa foi impedida judicialmente na época (CARVALHO, 2018).

A Secretaria de Segurança Pública do Estado de São Paulo também utiliza a tecnologia de reconhecimento facial como suporte durante operações em eventos de grande porte. Em parceria com o Allianz Parque, a pasta conseguiu capturar 52 indivíduos procurados pela Justiça. Além disso, identificou 56 pessoas em desacordo com medidas judiciais, cinco torcedores proibidos pelo Estatuto do Torcedor de frequentar estádios e 12 pessoas utilizando documentos falsos. A tecnologia também foi crucial na localização de 275 pessoas desaparecidas. Ao todo, o programa já foi utilizado para verificar 275.687 torcedores (TAJRA, 2024).

No Rio de Janeiro, a tecnologia de reconhecimento facial foi integrada às políticas de segurança pública a partir de 2019. Segundo informações da Polícia Militar do Estado do Rio de Janeiro (PMERJ), o projeto-piloto teve início durante o Carnaval com a instalação de 34 câmeras. A implementação dos sistemas foi realizada gratuitamente por meio de um convênio com a empresa de telefonia Oi. Esse sistema permite o envio de informações em tempo real para o Centro Integrado de Comando e Controle, onde operadores analisam os alertas de correspondência. Em julho de 2019, começou uma segunda fase para expandir o projeto na cidade, aumentando o número de câmeras com reconhecimento facial de 34 para 140. No entanto, no mesmo mês, pelo menos duas pessoas foram erroneamente identificadas como suspeitas no Rio de Janeiro, caracterizando falsos positivos (ALMEIDA, 2019).

Além disso, em Praia Grande, um total de 3.036 câmeras são operadas a partir do Centro Integrado de Comando e Operações Especiais (Cicoe). Marco Alves dos Santos, inspetor-chefe do Departamento de Planejamento e Tecnologia da Secretaria de Assuntos de Segurança Pública (Seasp), destaca que cada um dos programas tem uma função específica, mas todos são complementares entre si (PILIPAVICIUS, 2022).

O Forense, ou *Briefcam*, é um *software* israelense que desempenha um papel crucial na elucidação de crimes ao reduzir o tempo necessário para analisar imagens gravadas por câmeras, utilizando filtros de busca avançados. Com ele, é possível realizar levantamentos detalhados, como contabilizar quantos carros vermelhos passaram por uma determinada área em um período específico. O *software* é amplamente requisitado pela Polícia Civil e pelo Poder Judiciário para auxiliar nas investigações criminais (PILIPAVICIUS, 2022).

As câmeras de OCR (Reconhecimento Óptico de Caracteres) formam o que é conhecido como "cerco eletrônico" em grande parte do Município, focando especialmente nas entradas, saídas e outros pontos estratégicos da cidade. Essas câmeras são capazes de identificar placas de veículos que circulam pela região. Quando um veículo registrado como furtado ou roubado tem sua placa comunicada à Polícia Militar ou ao Cicoe (Centro Integrado de Comando e Operações Especiais), os dados são inseridos no sistema. Assim que o veículo passa por uma dessas câmeras de OCR, um alarme é ativado no centro de monitoramento e as viaturas são despachadas para intervir (PILIPAVICIUS, 2022).

Essa tecnologia é creditada pela redução significativa de mais de 60% nos índices de roubo e furto de veículos na cidade (PILIPAVICIUS, 2022).

Conforme o exposto, verifica-se uma expansão no uso da tecnologia de reconhecimento facial para fins de segurança pública, tanto no âmbito internacional quanto no País, com o intuito de aprimorar o controle social e facilitar a identificação de possíveis criminosos.

No entanto, faz-se necessário analisar se esta tecnologia é compatível com o ordenamento jurídico brasileiro, a fim de ser utilizada como meio de prova no processo penal.

4 A (IN)COMPATIBILIDADE DA TECNOLOGIA DE RECONHECIMENTO FACIAL COM O ORDENAMENTO JURÍDICO BRASILEIRO

Inicialmente, é fundamental destacar que meios de prova são todos os recursos, diretos ou indiretos, utilizados para estabelecer a verdade dos fatos durante o processo judicial. Esses meios podem ser classificados em lícitos, que são permitidos conforme as normas jurídicas, ou ilícitos, que são contrários ao

ordenamento jurídico. No entanto, somente os meios de prova lícitos devem ser considerados pelo juiz para formar sua convicção no julgamento do caso (NUCCI, 2024).

Constituem-se provas ilícitas aquelas obtidas em violação às normas constitucionais ou legais. Naturalmente, as provas ilegais são aquelas que violam qualquer norma da legislação ordinária, abrangendo tanto as normas penais quanto as processuais penais (NUCCI, 2024).

Ademais, a finalidade da prova é convencer o juiz a respeito da verdade de um fato litigioso. Busca-se a verdade processual, ou seja, a verdade atingível ou possível (NUCCI, 2024).

No entanto, para que o órgão julgador entregue uma decisão, a prova apresentada deve cumprir critérios de suficiência probatória. O preenchimento desses critérios é o que legitima a decisão, sendo que o critério mais exigente é o *beyond a reasonable doubt* (além da dúvida razoável), utilizado na sentença penal (LOPES JR., 2019).

Dessa forma, ao consagrar a presunção de inocência e o *in dubio pro reo*, a Constituição adota o critério de "além da dúvida razoável", que, somente se preenchido, autoriza um juízo condenatório (LOPES JR., 2019).

Nesse contexto, Norberto Avena (2019) ensina que o juiz não está restrito aos meios de prova estritamente regulamentados pela lei, ou seja, aqueles que são lícitos e legítimos. Mesmo as provas inominadas, que não estão explicitamente previstas no Código de Processo Penal (CPP), como filmagens, fotografias, gravações e outras formas não regulamentadas, podem ser admitidas de acordo com o princípio da liberdade das provas. Essas evidências podem ser consideradas na formação da convicção do julgador.

Apesar da ampla autorização conferida pelas legislações penais ordinárias, as limitações constitucionais ao direito à prova devem ser rigorosamente respeitadas. Estas incluem a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, bem como a inviolabilidade do domicílio e o sigilo de correspondência e das telecomunicações (MARTINS, 2020).

Tendo em vista a viabilidade da utilização das provas digitais e que o reconhecimento facial é uma realidade, questiona-se se a tecnologia de reconhecimento facial é compatível com a produção de provas no processo penal, a

fim de ser utilizada para tal, haja vista ser uma prova digital sem regulamentação específica.

A aplicação do reconhecimento facial levanta questões complexas relacionadas aos direitos fundamentais e à ética. Existe um limite tênue entre o uso dessa tecnologia e a proteção dos direitos individuais. Há preocupações éticas quanto ao potencial uso da tecnologia para propósitos ilícitos e manipulação indevida. O acesso rápido aos dados e antecedentes criminais de qualquer pessoa também levanta o debate sobre o direito ao esquecimento, especialmente diante da proliferação e uso cotidiano dessa tecnologia por plataformas de redes sociais, que contribuem para a criação de vastos repositórios de dados faciais (ROSA; BERNARDI, 2018).

Além disso, ao aplicar o reconhecimento facial para identificação em massa, falhas no sistema podem resultar na identificação incorreta de suspeitos, o que é uma preocupação significativa (ROSA; BERNARDI, 2018).

A ausência de uma regulação ou orientação de alcance geral, combinada com o fato de que bases de dados públicas e privadas já acumulavam registros biométricos faciais mesmo antes da aprovação da Lei Geral de Proteção de Dados (LGPD), reforça as preocupações éticas em torno do uso do reconhecimento facial (FRANCISCO; HIUREL; RIELLI, 2020).

Assim como qualquer outra tecnologia emergente, o reconhecimento facial representa uma novidade com crescimento relativamente rápido, capaz de gerar impactos significativos de maneira incerta e ambígua. Regular o uso de uma tecnologia emergente é uma tarefa complexa que deve equilibrar a proteção dos direitos civis com a promoção dos potenciais benefícios da inovação. Isso se torna ainda mais desafiador devido à falta de clareza exata sobre os impactos potenciais desta tecnologia (FRANCISCO; HIUREL; RIELLI, 2020).

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).

A Lei 13.709/2018, conhecida como Lei Geral de Proteção de Dados (LGPD), foi estabelecida para regular o tratamento de dados pessoais, tanto em meios digitais quanto físicos, por pessoas naturais ou jurídicas. Seu principal objetivo é proteger os direitos fundamentais de liberdade e privacidade, assim como promover o livre desenvolvimento da personalidade das pessoas naturais (BRASIL, 2018).

O artigo 5º, II da Lei Geral de Proteção de Dados (LGPD) define dados biométricos como dados pessoais sensíveis, o que implica em restrições específicas para seu uso, conforme estabelecido no artigo 11. No entanto, o artigo 4º da LGPD faz uma ressalva importante ao estabelecer que a lei não se aplica ao tratamento de dados pessoais realizado exclusivamente para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais (BRASIL, 2018).

O uso de dados biométricos sensíveis para fins de segurança pública e investigação criminal não está diretamente regulado pela LGPD. Conforme o artigo 4º, §1º da Lei Geral de Proteção de Dados, o tratamento de dados pessoais exclusivamente para esses propósitos é disciplinado por legislação específica. Esta legislação deve contemplar medidas proporcionais e estritamente necessárias para atender ao interesse público, garantindo o devido processo legal, os princípios gerais de proteção de dados e os direitos dos titulares conforme estabelecido na LGPD (BRASIL, 2018).

A regulação deve cumprir uma dupla finalidade: proteger os direitos e liberdades fundamentais dos cidadãos e, simultaneamente, permitir o tratamento automatizado de dados pessoais para otimizar a persecução penal. Isso é especialmente importante considerando os desafios enfrentados pela sociedade na era 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 3.069/2022, que regulamenta o uso do reconhecimento facial automatizado pelas forças de segurança pública em investigações criminais ou procedimentos administrativos (BRASIL, 2022).

No entanto, observa-se que o uso dessa tecnologia está progressivamente entrando no âmbito da prova judicial, uma vez que decisões de cortes superiores têm

autorizado sua utilização como meio de prova, validando o reconhecimento realizado por essa tecnologia.

Na decisão proferida em 12/01/2023, o ministro Alexandre de Moraes ordenou à Polícia Federal a obtenção de imagens das câmeras localizadas no Distrito Federal para auxiliar no reconhecimento facial dos terroristas responsáveis pelos atos ocorridos em 8 de janeiro. Além disso, determinou ao Tribunal Superior Eleitoral que utilizasse a consulta e acesso aos dados de identificação civil armazenados naquela Corte, bem como outros dados biográficos necessários para identificar e localizar as pessoas envolvidas nos eventos terroristas daquele dia (BRASIL, 2023).

Ainda, no mesmo inquérito, 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).

Dessa maneira, a prova digital pode ser definida como o elemento jurídico capaz de comprovar a ocorrência ou não de um evento, detalhando suas características, circunstâncias, os indivíduos envolvidos e a dinâmica das ações. É um instrumento jurídico destinado a demonstrar a existência de um fato e suas circunstâncias, independentemente se ocorreram inteiramente em meios digitais ou se estes foram utilizados como meio para sua demonstração (THAMAY; TAMER, 2022).

Acerca disso, a viabilidade da evidência digital como prova é inicialmente respaldada pelo artigo 369 do Código de Processo Civil, que permite às partes utilizar todos os meios legais ou moralmente legítimos para prova, mesmo que não especificamente previstos em lei, desde que não sejam ilícitos. No entanto, surge a questão da confiança depositada nessa prova, o que demanda maior cuidado na extração e documentação para assegurar sua confiabilidade e correspondência com a realidade dos fatos (SOUZA; MUNHOZ; CARVALHO, 2023).

Conforme Badaró (2021), no contexto das provas digitais, é crucial seguir métodos informáticos para garantir a autenticidade e integridade dessas evidências. Isso inclui procedimentos adequados para obtenção, registro, armazenamento, análise e apresentação dos elementos probatórios digitais, alinhados às melhores práticas nacionais e internacionais. A apresentação dessas provas em juízo deve ser

realizada por meio de perícia técnica, sendo essencial a documentação completa da cadeia de custódia para assegurar seu potencial epistêmico adequado.

Dessa forma, são elencados os requisitos mais apropriados para a 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).

Além disso, devido a todas as suas diferenças em relação às provas tradicionalmente utilizadas no processo penal, especialmente as chamadas fontes reais de prova, a *digital evidence* ou produção de prova informática demandaria uma intervenção legislativa com regras específicas para sua produção, admissão e valoração. Frequentemente, as regras tradicionais aplicadas às provas clássicas do processo penal mostram-se inadequadas para lidar com evidências digitais (BADARÓ, 2021).

Assim sendo, diante do silêncio por parte do legislador, o aplicador do direito se encontra na posição de utilizar os meios de prova tradicionais e os métodos de obtenção de prova existentes para lidar com as particularidades da obtenção de dados digitais (BADARÓ, 2021).

Como observado, o Brasil já implementou sistemas de reconhecimento facial em alguns estados e também tem projetos de lei em curso para regularizar essa tecnologia. Em relação aos dados sensíveis, a LGPD trouxe uma regulamentação aguardada há muito tempo, embora ainda esteja progredindo lentamente em termos de aplicabilidade efetiva. Esta legislação abrange também os setores de segurança pública, defesa nacional, atividades de investigação e repressão, bem como segurança do Estado (PEREIRA, 2020).

Por fim, entende-se que a tecnologia de reconhecimento facial, mesmo sem regulamentação específica, se encaixaria na questão da prova digital, ainda que inominada, sendo aplicáveis dispositivos legais análogos para sua legitimação.

5 CONSIDERAÇÕES FINAIS

Considera-se notável a expansão do uso da tecnologia de reconhecimento facial no processo penal, sendo utilizada tanto para identificar atividades suspeitas de tráfico internacional de drogas em aeroportos brasileiros, quanto para localização de foragidos da Justiça.

O reconhecimento facial é uma técnica de identificação biométrica na qual um *software* mapeia matematicamente os traços faciais de determinado indivíduo e, através de algoritmos, é capaz de compará-lo a uma imagem digital do mesmo indivíduo, reconhecendo ou negando sua identidade.

Entretanto, o reconhecimento facial é probabilístico, ou seja, não produz respostas binárias certas, mas identifica correspondências mais ou menos prováveis.

Dessa forma, apesar da utilidade de suas aplicações, o uso desta tecnologia ainda encontra alguns limites, tendo em vista a preocupação com os direitos fundamentais e a questão da acurácia e transparência dos algoritmos.

Atualmente, é possível verificar a utilização do reconhecimento facial para fins de segurança pública, no entanto, não existe ainda legislação que o regulamente, apesar dos diversos Projetos de Lei com o intuito de preencher esta lacuna deixada pela LGPD.

Ainda, considerando-se que a finalidade da prova é convencer o juiz a respeito da verdade de um fato litigioso, e que o juiz não se limita aos meios de prova regulamentados em lei, ou seja, sendo lícitas e legítimas, mesmo as provas inominadas, as quais não estão previstas taxativamente no CPP, verifica-se legítimo o uso do reconhecimento facial como prova no processo penal, haja vista ser uma prova digital, ainda que sem regulamentação específica.

Nesse sentido, a prova digital é 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 e sua viabilidade é fundamentada pelo art. 369 do Código de Processo Civil, que autoriza as partes a empregar todos os meios legais ou moralmente legítimos de prova, ainda que não previstos em lei, vedada apenas a prova ilícita.

Dessa forma, elencam-se alguns requisitos para documentação de uma prova digital, sendo estes, a autenticidade sobre a identificação da origem e autoria da prova;

a completude sobre a integralidade do fato; integridade, em que a documentação se mantém imutável e confiável; a temporalidade, marcando sua referência temporal; a auditabilidade, em que haja integrabilidade e publicidade da prova; e cadeia de custódia.

Além disso, identifica-se que alguns cuidados devem ser observados para o controle da prova do reconhecimento facial pois, com a aplicação do reconhecimento facial à identificação em massa, eventuais falhas no sistema podem significar a identificação incorreta de suspeitos.

Por fim, entende-se que a tecnologia de reconhecimento facial, mesmo sem regulamentação específica, pode ser considerada uma prova legítima. Ela se enquadra na categoria de prova digital, ainda que não explicitamente mencionada, sendo aplicáveis dispositivos legais análogos para sua utilização.

REFERÊNCIAS

ALCASSA, Flávia. Aprovação da lei da inteligência artificial na União Europeia e os desafios no Brasil. **Migalhas**, São Paulo, 15 abr. 2024. Disponível em: https://www.migalhas.com.br/depeso/405358/aprovacao-da-lei-da-inteligencia-artificial-na-ue-e-desafios-no-brasil. Acesso em: 28 abr. 2024.

ALMEIDA, Emily. Homem é preso por engano em Copacabana. **Band News FM Rio**, 24 jul. 2019. Disponível em: https://bit.ly/3dEUflp. Acesso em: 7 jun. 2024.

ALVES, Alan Tiago. Flagrado por câmera vestido de mulher no carnaval na BA matou homem após vítima passar perto dele de moto em alta velocidade, 7 mar. 2019, **G1 Bahia.** 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. Acesso em: 3 jun. 2024.

AVENA, Norberto. **Processo penal.** 11. ed. Rio de Janeiro: Forense, São Paulo: MÉTODO, 2019.

BADARÓ, Gustavo Henrique. Os standards metodológicos de produção na prova digital e a importância da cadeia de custódia. **Boletim IBCCRIM**, v. 29, p. 7-9, 2021. Disponível em: https://www.ibccrim.org.br/publicacoes/edicoes/747/8544. Acesso em: 24 jun. 2024.

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: 28 abr. 2024.

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: 28 abr. 2024.

BRASIL. **Decreto 8.771, de 11 de maio de 2016.** Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8771.htm. Acesso em: 3 maio 2024.

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: 20 jun. 2024.

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: 21 jun. 2024.

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/_ ato20152018/2018/lei/l13709.htm. Acesso em: 17 maio 2024.

BRASIL. Senado Federal. **Projeto de Lei n. 2.338/2023.** Dispõe sobre o uso da Inteligência Artificial. Disponível em: https://www25.senado.leg.br/web/atividade/ materias/-/materia/157233. Acesso em: 28 abr. 2024.

BRASIL, Emanuelle; SEABRA, Roberto. Projeto altera Lei de Proteção de Dados para resguardar segurança pública e defesa nacional. **Agência Câmara de Notícias,** 12 ago. 2022. Disponível em: https://www.camara.leg.br/ noticias/893704-projeto-altera-lei-de-protecao-de-dados-para-resguardar-seguranca-publica-e-defesa-nacional/. Acesso em: 3 jun. 2024.

BRASIL. Supremo Tribunal Federal. **Inquérito 4923/DF.** Relator: Min. Alexandre de Moraes, protocolado em 12 jan. 2023. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=6547024. Acesso em: 24 jun. 2024.

CARVALHO, Lucas. Metrô de São Paulo vai usar reconhecimento facial em anúncios. **Olhar Digital**, 13 abr. 2018. Disponível em: https://bit.ly/2tM3Cic. Acesso em: 14 jun. 2024.

CAPEZ, Fernando. **Curso de processo penal.** 23 ed. São Paulo: SaraivaJur, 2024.

DONEDA, Danilo. **A proteção dos dados pessoais como um direito fundamental.** Disponível em: http://editora.unoesc.edu.br/index.php/espacojuridico/article/view/1315/658. Acesso em: 17 maio 2024.

FERNANDES, F. A.; BOUGLEUX ANDRADE RESENDE, A. P. Regulamentação do tratamento automatizado de dados pessoais em matéria penal. **Suprema - Revista de Estudos Constitucionais**, Distrito Federal, Brasil, v. 3, n. 1, p. 471–500, 2023. Disponível em: https://suprema.stf.jus.br/index.php/suprema/article/view/207. Acesso em: 21 jun. 2024.

FRANCISCO, P. A. P.; HUREL, L. M.; RIELLI, M. M. **Regulação do reconhecimento facial no setor público**: avaliação de experiências internacionais. Instituto Igarapé, *Data Privacy Brasil Research*, 2020. Disponível em: https://igarape.org.br/wp-content/uploads/2020/06/2020-06-09-Regulação-doreconhecimento-facial-no-setor-público.pdf. Acesso em: 21 jun. 2024.

GARAY, Vladimir. Mal de Ojo: Reconocimiento Facial em América Latina. **Derechos Digitales**. Latin America in a Glimpse. 2019. Disponível em: https://bit.ly/2H2baQA. Acesso em: 14 jun. 2024.

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: 17 maio 2024.

INSTITUTO IGARAPÉ. **Data Privacy BR Research.** Disponível em: https://igarape.org.br/infografico-reconhecimentofacial-no-brasil/. Acesso em: 20 jun. 2024.

LOPES JR., Aury; ROSA, Alexandre Morais da. Limite penal: Sobre o uso do *standard* probatório no processo penal. **Revista Eletrônica CONJUR**, 26 jul. 2019, São Paulo. Disponível em: https://www.conjur.com.br/2019-jul-26/limite-penal-uso-standard-probatorio-processo-penal/. Acesso em: 14 jun. 2024.

MARTINS, Maria Luisa Penteado. Uso da inteligência artificial em sistemas de reconhecimento facial e sua aplicação no direito penal. III Congresso Internacional Information Society and Law, 3. 2020. São Paulo. **Anais [...].** São Paulo: Centro Universitário das Faculdades Metropolitanas Unidas (FMU), 2020. Disponível em: https://informationsocietyandlaw.fmu.br/wp-content/uploads/2023/10/informationsocietyandlawreviewV3.pdf#page=230. Acesso em: 17 maio 2024.

MENA, Isabela. **Verbete Draft**: o que é Reconhecimento Facial, 30 maio 2018. Disponível em: https://www.projetodraft.com/verbete-draft-o-que-ereconhecimento-facial/. Acesso em: 3 maio 2024.

NABESHIMA, Yuri. Uso do reconhecimento facial na segurança pública. **Revista Eletrônica CONJUR,** São Paulo, 6 jan. 2024. Disponível em: https://www.conjur.com.br/2024-jan-06/uso-do-reconhecimento-facial-na-seguranca-publica/. Acesso em: 17 maio 2024.

NUCCI, Guilherme de Souza. **Manual de processo penal, volume único**. 5 ed. Rio de Janeiro: Grupo GEN, 2024.

PEREIRA, Débora Freitas Mendes. **O uso de câmeras de reconhecimento facial em contexto de pós democracia**: uma ferramenta contra o inimigo no direito penal? 2020. Artigo (Pós-Graduação) Instituto de Tecnologia Social e Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2020.

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

PEW RESEARCH CENTER. **More Than Half of U.S. Adults Trust Law Enforcement to Use Facial Recognition Responsibly.** 5 set. 2019. Disponível em: https://www.pewresearch.org/internet/2019/09/05/more-than-half-of-u-s-adults-trust-lawenforcement-to-use-facial-recognition-responsibly/. Acesso em: 17 maio 2024.

PILIPAVICIUS, Ludmila. **Softwares complementam eficácia do sistema de monitoramento por câmeras em PG**. Prefeitura Praia Grande, 18 fev. 2022**.** Disponível em: https://www2.praiagrande.sp.gov.br/noticia/id/54808. Acesso em: 7 jun. 2024.

ROSA, Alexandre Morais da; BERNARDI, Sahra di. Quando o reconhecimento facial chega ao processo penal. Coluna publicada em 3 de agosto de 2018, **Revista Eletrônica CONJUR**, São Paulo. Disponível em: https://www.conjur.com.br/2018-ago-03/limite-penalquando-reconhecimento-facial-chega-processo-penal. Acesso em: 2 mai. 2024.

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.

SCHMIDT, Thales. Mesmo sem regulamentação federal, reconhecimento facial avança no Brasil. **Brasil de Fato**, São Paulo, 04 set. 2022. Disponível em: https://www.brasildefato.com.br/2022/09/04/mesmo-sem-regulamentacao-federal-reconhecimento-facial-avanca-no-brasil. Acesso em: 2 jun. 2024.

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

SOUZA, Marcos de Moura e. Aposta contra o crime, reconhecimento facial se espalha pelo país. Publicado em 19 de março de 2024, **Valor Econômico**, São Paulo. Disponível em: https://valor.globo.com/brasil/noticia/2024/03/19/aposta-contra-o-crime-reconhecimento-facial-se-espalha-pelo-pais.ghtml. Acesso em: 7 jun. 2024.

TAJRA, Alex. Veja como cada estado usa o reconhecimento facial para fins policiais. **Revista Eletrônica CONJUR**, São Paulo, 17 maio 2024. Disponível em: https://www.conjur.com.br/2024-mai-17/veja-como-cada-estado-usa-o-reconhecimento-facial-para-fins-policiais/. Acesso em: 2 jun. 2024.

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

UNIÃO EUROPEIA. GDPR - **General Data Protection Regulation.** Regulamento Geral sobre Proteção de Dados. Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-constitutes-data-processing_pt. Acesso em: 3 maio 2024.