

UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO TECNOLÓGICO
DEPARTAMENTO ENGENHARIA DO CONHECIMENTO
CURSO DE PÓS-GRADUAÇÃO EM INTELIGÊNCIA E INOVAÇÃO
NO ENFRENTAMENTO AO CRIME ORGANIZADO

Pedro Corrêa Guerra
Maurício Paraboni Detoni

Reconhecimento Facial Brasileiro para Fins Penais:
ensaio das balizas normativas

Florianópolis
2026

Pedro Corrêa Guerra
Maurício Paraboni Detoni

Reconhecimento Facial Brasileiro para Fins Penais:
ensaio das balizas normativas

Trabalho de Conclusão de Curso submetido ao curso de Especialização em Inteligência e Inovação Aplicadas no Enfrentamento ao Crime Organizado, do Centro Tecnológico da Universidade Federal de Santa Catarina como requisito parcial para a obtenção do título de especialista em Inteligência e Inovação Aplicadas no Enfrentamento ao Crime Organizado.

Orientador: Prof. Ronaldo David Viana Barbosa, Dr.

Florianópolis
2026

Detoni, Maurício Paraboni
Reconhecimento facial brasileiro para fins penais : ensaio das balizas normativas / Maurício Paraboni Detoni, Pedro Corrêa Guerra ; orientador, Ronaldo David Viana Barbosa, 2026.
24 p.

Monografia (especialização) - Universidade Federal de Santa Catarina, Centro Tecnológico, Curso de Inteligência e Inovação no Enfrentamento ao Crime Organizado, Florianópolis, 2026.

Inclui referências.

1. Inteligência e Inovação. 2. Reconhecimento Facial. 3. Segurança Pública. 4. LGPD. 5. Regulação. I. Guerra, Pedro Corrêa. II. Barbosa, Ronaldo David Viana. III. Universidade Federal de Santa Catarina. Inteligência e Inovação no Enfrentamento ao Crime Organizado. IV. Título.

Pedro Corrêa Guerra
Maurício Paraboni Detoni

Reconhecimento Facial Brasileiro para Fins Penais:
ensaio das balizas normativas

Este Trabalho de Conclusão de Curso foi julgado adequado para obtenção do título de especialista em Inteligência e Inovação Aplicadas no Enfrentamento ao Crime Organizado e aprovado em sua forma final pelo Curso de Especialização em Inteligência e Inovação Aplicadas no Enfrentamento ao Crime Organizado.

Florianópolis, 06 de março de 2026.

ICP-Edu
Documento assinado digitalmente
Marcelo Macedo
Data: 25/03/2026 19:13:36-0300
CPF: ***.190.199-**
Verifique as assinaturas em https://v.ufsc.br

Coordenação do Curso

GOV.BR
Documento assinado digitalmente
RONALDO DAVID VIANA BARBOSA
Data: 26/03/2026 16:29:02-0300
CPF: ***.483.713-**
Verifique as assinaturas em https://v.ufsc.br

Prof. Ronaldo David Viana Barbosa, Dr.
Orientador

ICP-Edu
Documento assinado digitalmente
Daniel Rodrigues Kinchescki
Data: 26/03/2026 16:50:00-0300
CPF: ***.956.699-**
Verifique as assinaturas em https://v.ufsc.br

Daniel Rodrigues Kinchescki, Msc
Membro da banca

ICP-Edu
Documento assinado digitalmente
Juliana de Souza Correa
Data: 26/03/2026 16:57:16-0300
CPF: ***.325.469-**
Verifique as assinaturas em https://v.ufsc.br

Juliana de Souza Correa, Msc
Membro da banca

RESUMO

A inexistência de uma legislação específica de proteção de dados pessoais para fins exclusivos de segurança pública no Brasil tem acarretado uma série de consequências prejudiciais aos operadores dos sistemas existentes e aos titulares dos dados pessoais tratados. Nesse contexto, o presente estudo bibliográfico e documental, pretende analisar a tecnologia de reconhecimento facial, descrever o cenário legislativo da matéria em nível nacional e apresentar as contribuições legais advindas da comunidade europeia. Com base nesse aparato, objetiva-se ofertar uma bússola normativa para regulação do reconhecimento facial, em específico para o tratamento de imagens geradas em tempo real, para fins de prevenção, investigação e repressão a infrações penais que equilibre os direitos fundamentais da segurança, privacidade, liberdade de expressão e proteção dos dados pessoais. Para tanto, são demonstrados os avanços da referida tecnologia e apresentadas diferenças terminológicas que muitas vezes levaram ao descrédito da ferramenta. Ainda, respondido quem, como e por quanto tempo poderá ser realizado o tratamento de dados pessoais para essa finalidade, propondo um modelo claro, objetivo e uniforme da utilização da tecnologia, em homenagem aos operadores do sistema e aos titulares dos dados pessoais tratados, instrumentalizando e garantindo segurança jurídica a todos envolvidos nesse processo.

Palavras-chave: reconhecimento facial; regulação; LGPD-Penal; segurança pública.

ABSTRACT

The lack of specific legislation for the protection of personal data exclusively for public security purposes in Brazil has led to a series of harmful consequences for operators of existing systems and for the owners of the personal data processed. In this context, this bibliographic and documentary study aims to analyze facial recognition technology, describe the legislative scenario of the matter at national level, and present the legal contributions from the European Community. Based on this framework, the objective is to offer a normative compass for the regulation of facial recognition, specifically for the processing of images generated in real time, for the purposes of prevention, investigation, and repression of criminal offenses, balancing the fundamental rights of security, privacy, freedom of expression, and protection of personal data. To this end, the advances of this technology are demonstrated, and terminological differences that have often led to the discrediting of the tool are presented. Furthermore, it addresses who, how, and for how long personal data can be processed for this purpose, proposing a clear, objective, and uniform model for the use of technology, in recognition of system operators and the holders of the personal data processed, providing tools and guaranteeing legal security to all involved in this process.

Keywords: facial recognition; regulation; criminal LGPD; public security.

1 INTRODUÇÃO

Uma das missões precípuas do Estado é contribuir para o desenvolvimento social a partir da garantia de ambientes seguros que respeitem a privacidade e intimidade das pessoas. Essa desafiadora tarefa impõe atenção ao cenário no qual se insere a sociedade.

Hodiernamente, as mudanças, os avanços (e às vezes até retrocessos), em especial na área da tecnologia, traduzem-se em transformações dinâmicas que alteram sobremaneira o cotidiano em pequeno espaço de tempo. Em uma janela de menos de cinquenta anos uma profusão de inovações se fez presentes: a informática, a telemática e a internet, por exemplo,

mudaram profundamente a sociedade.

Tais mudanças acabam por impactar a atuação estatal em face da criminalidade, alterando o modo de agir no intento da garantia da segurança da população. Soluções de videomonitoramento foram acrescentadas ao trabalho policial como forma de otimizar a vigilância preventiva e, com o desenvolvimento tecnológico crescente, novas tecnologias vão sendo acrescentadas, como leituras de caracteres, identificação de objetos e até mesmo o reconhecimento facial de pessoas.

Nesse contexto de mudanças, a preocupação com dados pessoais e privacidade cresceu, o que deu início a discussões legislativas sobre a proteção dos dados do cidadão. A legislação criada – a conhecida Lei Geral de Proteção de Dados (LGPD) –, contudo, expressamente deixou de fora da regulamentação a atividade de segurança pública. Ou seja, o tratamento dos dados pessoais, que ocorrem durante o videomonitoramento com uso de reconhecimento facial automatizado, expressamente ficou de fora da regulamentação legal da LGPD, permanecendo um vácuo legislativo.

Tal inexistência de lei específica sobre o tema gera uma insegurança jurídica, já havendo esforços no sentido da criação de legislação que venha a regulamentar a hipótese (Brasil, 2020). Entretanto, nesse contexto surge o problema sobre quais balizas devem integrar a referida norma regulamentadora do uso da tecnologia de reconhecimento facial em tempo real, para fins de prevenção criminal, de modo a equilibrar os direitos fundamentais e segurança pública no Brasil.

O presente estudo, portanto, pretende apresentar contribuição na seara da segurança pública, em especial no campo da identificação biométrica a partir do reconhecimento facial. Delimitando o respectivo escopo, será trazido um balizamento para regulamentação do reconhecimento facial pelos órgãos de segurança pública em tempo real, ou seja, não em investigações a partir de vídeos gravados ou imagens pretéritas, mas sim, buscar-se-ão subsídios para equalizar direitos que permitam identificar de forma imediata cidadãos foragidos, investigados, acusados, réus e desaparecidos, visando otimizar a prevenção e a repressão penal imediata (situações de flagrante delito).

Justifica-se a pertinência da temática, uma vez que ainda há desconhecimento e desinformação no que se refere às tecnologias aplicáveis, como mencionam Crumpler e Lewis (2021) e inexiste no Brasil legislação sobre a matéria. Assim, está presente um sério vácuo normativo que impede o acompanhamento ideal das novas tecnologias, o devido respeito aos direitos e garantias dos cidadãos, bem como o compartilhamento de informações com outros países.

Assim, a partir de uma análise qualitativa, apoiada em pesquisa bibliográfica e documental, procurou-se compreender e descrever o fenômeno da tecnologia de reconhecimento facial e sua respectiva regulação em nível europeu, para posteriormente balizar futura legislação brasileira. Objetiva-se, ao final, propor balizas normativas para a construção de uma legislação brasileira específica que regulamente o uso da tecnologia de reconhecimento facial em tempo real para fins de prevenção criminal, de modo a equilibrar os direitos fundamentais e a segurança pública no país.

De maneira específica, primeiramente vai ser conceituado o reconhecimento facial, a partir de seu funcionamento, suas aplicações e principais diferenças terminológicas. Após, será adentrada na verificação do cenário legislativo brasileiro acerca do tema, pontuando a inexistência legislativa, trazendo a explanação dos dois principais documentos normativos europeus (Diretiva 2016/680 e a Convenção 108 +) e seus princípios delineadores.

Ao final, serão apresentadas as balizas normativas para uma futura Lei Geral de Proteção de Dados – Penal brasileira, em específico para o tratamento de imagens geradas em tempo real, elencando autoridades competentes, exercício e período do tratamento, buscando albergar os direitos fundamentais da segurança, privacidade, liberdade de expressão e proteção dos dados pessoais.

2 O RECONHECIMENTO FACIAL E A SEGURANÇA PÚBLICA NO BRASIL: ANÁLISE DO CENÁRIO LEGISLATIVO ATUAL E A LACUNA REGULATÓRIA

2.1 BIOMETRIA E A IDENTIFICAÇÃO DE PESSOAS

A forma mais utilizada e conhecida de identificação biométrica é a impressão digital, empregada desde o início do século passado, onde são analisados e comparados detalhes únicos e específicos de cada dedo, chamadas de minúcias (Assumpção; Mendonça, 2015), como bifurcações e terminações de linhas, a partir de um banco de dados de impressões cadastradas (Searston *et al.*, 2025). Por sua vez, o reconhecimento facial é uma tecnologia de identificação biométrica realizada em um processo de validação de identidade, a partir de características biológicas, utilizando padrões geométricos para identificar uma pessoa.

A tecnologia de reconhecimento facial (TRF), desenvolvida a partir de pesquisas da década de 1960 (Greenbaum; Nakar, 2017), considera as características únicas de um indivíduo para confirmar sua respectiva identidade, tendo como aliado não ser um sistema intrusivo, eis que de forma passiva, ocorre a identificação de determinada pessoa.

A face humana possui cerca de oitenta pontos nodais e tais pontos são variáveis

biométricas que combinam diferentes elementos visuais e gestuais, tornando por isso cada rosto único (Simonitis, 2021). Assim, entre outras características, consideram-se a distância entre os olhos, a curvatura e espessura dos lábios, a largura do queixo, tamanho da mandíbula, o comprimento da boca e do nariz, objetivando a criação, através da utilização de algoritmos que determinam padrões da face humana em formatos geométricos, de uma espécie de "mapa facial", "modelo facial" ou "assinatura facial", possibilitando assim a identificação e avaliação com as demais imagens armazenadas previamente em uma base de dados.

Logo, é por meio do predicado[1] que o reconhecimento facial determina a probabilidade de um rosto ser o mesmo que foi apresentado. Em síntese, os algoritmos comparam as características de análise e fornecem uma pontuação de similaridade entre as faces comparadas.

2.2 VARIAÇÕES DO RECONHECIMENTO FACIAL

Vale salientar aqui as três mais importantes variações do reconhecimento facial existentes (Lynch, 2020, p. 4-6).

De um lado, a classificação um por um, também conhecida como autenticação, que compara a imagem com uma identidade única e conhecida, informando se a identidade corresponde à imagem recebida. Um exemplo é o sistema de login em um determinado sistema. Nessa modalidade, a aplicação estaria indagando "você é, quem afirmar ser?".

Já na classificação um por muitos, ou por identificação, pergunta-se "quem é você?" e desse modo a imagem é comparada a uma série de identidades para determinar qual delas apresenta o maior grau de similaridade. Uma imagem de interesse será comparada com várias outras de um banco de dados.

Por sua vez, a classificação muitos por muitos tem como objetivo identificar várias faces em uma determinada imagem. Dessa forma, uma identidade única é atribuída à cada uma das faces, e, após, é utilizada a classificação um por muitos. Seria o caso do reconhecimento facial utilizado em câmeras de videomonitoramento onde são capturadas várias faces aleatórias e comparadas com a base de dados.

2.3 ASSERTIVIDADE DA TECNOLOGIA DE RECONHECIMENTO FACIAL

No tocante à assertividade do sistema de reconhecimento, há estudos que apontam vieses de reconhecimento (Lynch, 2020; Greenbaum; Nakar, 2017; Simonitis, 2021),

[1] O predicado é uma expressão usada na programação para determinar se algo é verdadeiro ou falso, se corresponde a algo ou não.

apresentando maiores falhas em identificar pessoas negras, mulheres e grupos étnicos minoritários. Entretanto, reconhece-se que "à medida que a tecnologia se desenvolve, os sistemas de reconhecimento facial serão ainda mais eficazes" (Simonitis, 2021, p.96).

Estudo do *National Institute of Standards and Technology*[2]- NIST (Grother; Ngan; Hanaoka, 2019), agência governamental norte americana vinculada ao Departamento de Comércio dos EUA, buscou avaliar a precisão do reconhecimento facial de noventa e nove desenvolvedores, processando mais de dezoito milhões de imagens, de vinte e quatro países, distribuídos em sete regiões globais distintas. Sobre essa pesquisa a SIA (*Security Industry Association*), apresentou a seguinte conclusão (Parker, 2020, p. 2):

> No geral, a tecnologia moderna de reconhecimento facial é altamente precisa. De fato, variações na qualidade da imagem, como pose, iluminação e expressão, têm sido o principal fator de erros no desempenho do reconhecimento facial, e não efeitos demográficos. A crescente imunidade a esses problemas é, segundo o NIST, a "razão fundamental pela qual a precisão melhorou desde 2013".

Ainda, o *Government Accountability Office*[3] - GAO (2024), em relatório sobre tecnologias de identificação biométrica apontou melhoras na precisão da tecnologia de reconhecimento facial, mas apontou a necessidade e ampliação de amostras nos diversos grupos demográficos, bem como difundir as informações sobre a tecnologia, realizar as devidas regulamentações legais e treinar os usuários.

> De acordo com informações coletadas durante nossa revisão de literatura e entrevistas relevantes, as tecnologias de identificação biométrica variam em precisão para diferentes populações, mas avanços recentes levaram a melhorias na tecnologia de reconhecimento facial. A precisão do reconhecimento facial, por exemplo, melhorou significativamente nos últimos 4 anos, com os sistemas de melhor desempenho apresentando variação muito pequena nas taxas de falsos negativos entre diferentes populações em testes de laboratório. Isso não se aplica às taxas de falsos positivos, onde as diferenças de desempenho diminuíram, mas as diferenças permanecem. No entanto, ainda existem lacunas na compreensão do desempenho real das tecnologias de identificação biométrica (GAO, 2024, p.16).

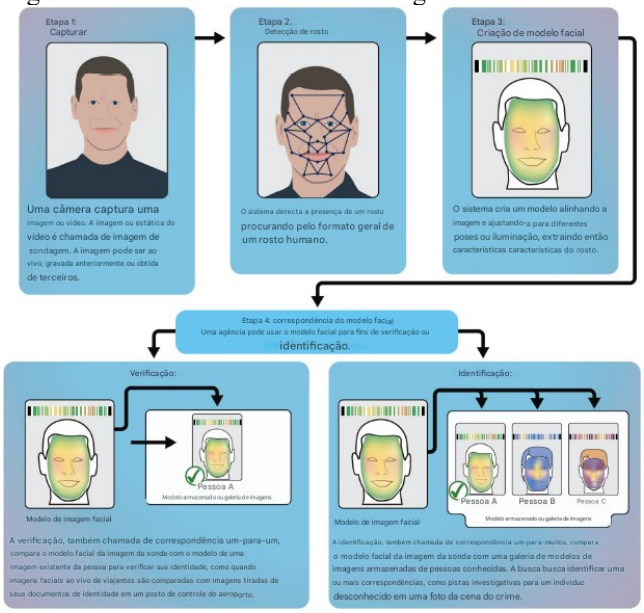
O mencionado relatório, apresenta uma figura (GAO, 2024, p.07), que ilustra de modo objetivo o funcionamento da ferramenta.

---

[2] Instituto Nacional de Padrões e Tecnologia.

[3] Escritório de prestação de contas do Governo Norte Americano. Ferreira e Aragão (2022, p. 151) referem que o GAO é "uma agência independente e apartidária, que trabalha para o Congresso. Também chamado de órgão de fiscalização do Congresso, sua principal função é investigar como o governo federal gasta os recursos dos contribuintes".

Figura 1 – Funcionamento da Tecnologia de Reconhecimento Facial



Fonte: (GAO, 2024, p.07) traduzido pela ferramenta *Google Tradutor*

Cabe lançar uma importante observação, as rápidas transformações tecnológicas que vêm ocorrendo, impõem ao pesquisador estar atento às mais novas publicações, sob pena de construir sua linha argumentativa em dados obsoletos. Nesse sentido, Crumpler e Lewis (2021, p. 01):

> A TRF está melhorando rapidamente, e qualquer crítica baseada em dados de apenas alguns anos atrás corre o risco de estar completamente equivocada. Determinar a verdade básica em questões de precisão e viés — algo que atualmente é escasso — é essencial para uma boa política.

Ainda, Li (2025) demonstra melhorias significativas na tecnologia de reconhecimento facial a partir da aplicação de modelos de *deep learning*[4], os quais produzem *embeddings*[5] faciais precisos, em aplicações de tempo real, demonstrando alcance de precisão acima de 95% nos mais diversos ambientes. Entretanto, a citada autora também alerta para o desenvolvimento de métodos para mitigar eventuais vieses e fortalecer as proteções à privacidade, a fim de que a tecnologia seja cada vez mais expandida e seu uso ocorra dentro dos mais elevados padrões éticos.

O reconhecimento facial pode ser utilizado em uma série de serviços e funcionalidades, desde permitir o acesso a um smartphone, controlar acessos, confirmar identidade de passageiros, trabalhadores, estudantes ou pacientes, até buscar pessoas desaparecidas,

[4] Ramo da machine learning – aprender da máquina sem respectiva programação - que praticamente imita o funcionamento do cérebro humano, a partir de múltiplas camadas.

[5] Representações para utilização no aprendizado da aplicação, possibilitando que encontrem objetos semelhantes.

criminosos ou terroristas.

Vale salientar, como afirmado anteriormente, tratar-se de uma tecnologia em evolução a qual pode apresentar falsos positivos (identificar diversamente uma pessoa) ou falsos negativos (não identificar uma pessoa que era realmente). Entretanto, essa variação de precisão, vem diminuindo paulatinamente (Albiero *et al.*, 2021), pois vão sendo identificados os fatores que levam às incorreções (iluminação, oclusão facial, qualidade da imagem, tom da pele e gênero), possibilitando cada vez mais que o sistema se torne assertivo.

Outra questão a ser levada em conta é a diferenciação entre "análise facial" ou "caracterização facial" e a tecnologia de reconhecimento facial. Crumpler e Lewis (2021) apontam um equívoco grave de interpretação acerca da TRF onde as críticas à tecnologia confundem ambos conceitos. A análise facial tem como objetivo caracterizar a imagem por gênero, idade, raça ou até mesmo aspectos de humor, enquanto o reconhecimento, por sua vez, como visto acima, busca comparar imagens e apontar a probabilidade de uma ser igual a outra.

> Muitas das críticas à TRF são, na verdade, sobre a caracterização facial. **Alegações sobre a imprecisão da TRF estão desatualizadas ou se referem erroneamente à caracterização facial**. É claro que a precisão depende de como a TRF é usada. Quando a qualidade da imagem é ruim, a precisão é menor, mas frequentemente ainda melhor do que a do ser humano médio (Crumpler e Lewis, 2021, p. 01) *grifo nosso*.

Considerando que o escopo do presente artigo é contribuir para uma regulamentação do reconhecimento facial pelos órgãos de segurança pública em tempo real, ou seja, não em investigações a partir de vídeos gravados ou imagens pretéritas, buscar-se-á subsídios para equalizar direitos que permitam identificar de forma imediata cidadãos foragidos, investigados, acusados, réus e desaparecidos, visando otimizar a prevenção e a repressão penal imediata (situações de flagrante delito). Para tanto, cabe analisar o cenário legislativo acerca do tema.

2.4 CENÁRIO LEGAL SOBRE O RECONHECIMENTO FACIAL

Em 2018, no Brasil, foi sancionada a Lei Geral de Proteção de Dados (LGPD), Lei n.º 13.709/18 (Brasil, 2018), dispondo normas gerais para o tratamento de dados pessoais, com vistas a proteger os direitos fundamentais de liberdade e privacidade. Entretanto, a citada legislação não se aplica quando houver finalidade exclusiva de segurança pública (art. 4º, III, a), determinando elaboração de legislação específica, a qual deverá observar os princípios da finalidade (âmbito da segurança pública), proporcionalidade/necessidade (limitação de condutas e lapso temporal adequado) e transparência (publicidade do que está sendo realizado, possibilitando controle).

Logo, verifica-se a necessidade de legislar acerca da temática, a fim de estabelecer

parâmetros seguros de atuação aos órgãos de segurança pública e cidadãos envolvidos, uma vez que realizado o tratamento de uma determinada imagem[6] por meio do reconhecimento facial, tem-se um dado sensível, nos termos do art. 5º, III, da LGPD, *in verbis*:

> Art. 5º Para os fins desta Lei, considera-se:
> (...)
> II - **dado pessoal sensível**: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, **dado** genético ou biométrico, quando **vinculado a uma pessoa natural** (*grifo nosso*).

Devido à atualidade do tema, duas iniciativas legislativas foram propostas no intuído de estabelecer a "LGPD penal". Em 2019, foi instituída, por Ato do Presidente da Câmara dos Deputados, uma Comissão de Juristas que, em 2020, finalizou um Anteprojeto de Lei (Brasil, 2020). De igual forma, tramita na Câmara dos Deputados o Projeto de Lei n.º 1.515/2022 (Brasil, 2022). Até o presente momento nenhuma das proposições foi votada, havendo, deste modo, espaço para debates e colaborações[7].

3 LIÇÕES DO DIREITO COMPARADO: O MODELO EUROPEU DE PROTEÇÃO DE DADOS PENAIS COMO REFERÊNCIA REGULATÓRIA

3.1 PANORAMA GERAL DA LEGISLAÇÃO EUROPEIA

Como afirmado anteriormente, o objetivo do presente estudo é contribuir com diretrizes para uma parcela da "LGPD penal" – reconhecimento facial voltado à atividade de segurança pública para sua utilização em tempo real. Para tanto, utilizar-se-á como norte a Diretiva 2016/680 do Parlamento Europeu e do Conselho da União Europeia (União Europeia, 2016) relativo à proteção de cidadãos em relação ao tratamento de dados para fins de prevenção, investigação e repressão de infrações penais e a Convenção 108 + (Conselho da Europa, 2018) para a proteção das pessoas relativamente ao tratamento de dados de caráter pessoal. A utilização desses documentos legais justifica-se a partir da sua sedimentação e aceitação no cenário internacional, servindo de base normativa para uma série de outros países, possibilitando, inclusive, o respectivo intercâmbio de informações.

A Diretiva 2016/680 antes de enunciar os dispositivos legais traz cento e sete parágrafos

---

[6] Tratar uma imagem, para fins de reconhecimento facial, significa atribuir informações de uma determinada pessoa, individualizando a respectiva imagem.

[7] Em vigor, aplicável, de regra, aos órgãos federais, a Portaria MJSP n.º 961/25 que estabelece diretrizes sobre uso de soluções de tecnologia da informação aplicadas às atividades de investigação criminal e inteligência de segurança pública.

de considerações[8] fazendo um importante balizamento. Assim, importante realizar análise para posterior sugestionamento a futura legislação brasileira.

Ab initio posiciona a proteção do cidadão em relação ao tratamento de seus dados pessoais como um direito fundamental (1), visando um espaço de liberdade, segurança e justiça (2). Ainda, propugna seja facilitado o intercâmbio de dados entre as autoridades dos Estados-Membros (7). Estabelece as funções de polícia como as ações de prevenção, investigação ou repressão de infrações penais, mesmo sem conhecimento prévio de que um incidente se constitua ou não em infração penal, incluindo medidas coercitivas em manifestações, grandes eventos esportivos e distúrbios - prevenção de ameaças à segurança pública (12). Exclui do escopo de abrangência atividades de segurança nacional (14).

Foca objetivamente em harmonizar regras de proteção e livre circulação de dados pessoais tratados para fins penais justamente para prevenir ameaças à segurança pública (15), assegurada a neutralidade tecnológica, ou seja, independentemente da tecnologia utilizada - tratamento em fichas ou sistemas de inteligência artificial - haverá a devida proteção (18). Todo tratamento deverá ser lícito, leal – direito a um tribunal imparcial - e transparente – alertar os cidadãos dos riscos, regras e garantias acerca do tratamento dos dados e respectivos meios para exercício de direitos, bem como vedação a excessos de tratamento e de efeitos prolongados para além da finalidade posta, permitindo sempre o apagamento ou revisão periódica (26). Garantia de segurança e confiabilidade, buscando sempre as melhores técnicas e tecnologias (28).

O tratamento deverá observar que a finalidade seja determinada, explícita e legítima. Logo, vedada utilização para marketing ou controle político, tendo sua permissão apenas no universo penal (29). Aplicação do princípio da exatidão dos dados – corretos, completos e atualizados, com o alerta de levar em conta que eventuais informações testemunhais são percepções, ou seja, não são necessariamente um fato comprovado (30 e 32). Quando do tratamento, observar-se-á a distinção entre as categorias de suspeitos, indiciados, condenados, vítimas, testemunhas, observando o princípio da presunção de inocência, uma vez que o fato de estar em uma base de dados não torna a pessoa, de regra, culpada (31).

Os Estados-Membros ao preverem o tratamento, deverão, em suas respectivas normativas informar, por que os dados estão sendo coletados; quais dados podem ser usados; para que serão utilizados; como serão protegidos; e quando deverão ser destruídos (33). O tratamento realizado pelas autoridades competentes na matéria criminal/penal abrange todo tipo

[8] Tendo em vista que o objetivo do estudo é construir proposições a uma estrutura legislativa em nível nacional, mostra-se mais eficaz a análise das considerações do que propriamente o texto legal em si.

de operação necessária a finalidade proposta, respeitando a Diretiva 2016/680. Caso os dados sejam utilizados fora do contexto penal, *v.g.*, estatísticas ou pesquisas, aplicar-se-á a Diretiva 2016/679 – Regulamento Geral de Proteção de Dados (34).

Para o tratamento dos dados pessoais, será dispensado consentimento do cidadão, podendo os Estados-Membros preverem algumas exceções, onde o consentimento será necessário ou suprido por ordem judicial (35).

Considera que dados sensíveis do ponto de vista dos direitos e liberdades fundamentais – etnia, opinião política, religião, opção sexual, saúde, merecem proteção especial, não sendo objeto de tratamento, salvo previsão legal, ou para proteção de interesses vitais do próprio titular ou terceiro, ou ainda se o titular tornou público tais dados. Ressalta-se, o consentimento do titular, fora das hipóteses referidas, não autoriza o tratamento de dados sensíveis (37 e 38).

Estabelece previsão de regras que facilitem ao titular dos dados o acesso, solicitação, retificação e apagamento, de forma gratuita (40). Ao titular dos dados serão asseguradas, sem burocracias, informações sobre eventual tratamento, quem o realizou, qual finalidade, duração, com quem compartilhado e acesso aos dados tratados, possibilitada a retificação, apagamento ou limitação (42 e 43). O direito ao acesso aos dados pode, justificadamente, ser limitado para proteger investigações criminais, garantir a segurança pública ou proteger pessoas (44, 45 e 46).

Todas as atividades relevantes de tratamento - inserção, alteração, consulta, divulgação ou transferência, cruzamento de informações ou apagamento, deverão ser registradas em ordem cronológica, identificando, sempre, quem acessa os dados, justamente para possibilitar o autocontrole da administração (57).

Quando houver elevado risco aos direitos dos titulares deverá ser elaborada uma Avaliação de Impacto na Proteção de Dados, detalhando medidas técnicas – encriptação, controle de acesso, garantias jurídicas e organizacionais e mecanismos de conformidade – auditorias, analisando os sistemas utilizados – software - e os procedimentos (58).

É estabelecido o prazo de 72h para que o responsável pelo tratamento comunique eventual violação de dados pessoais à autoridade de controle. De igual forma, o mais breve possível, devem ser comunicados os respectivos titulares, salvo se resultar prejuízo às atividades de prevenção a segurança pública em curso (61).

Faz-se necessária a nomeação de um Encarregado da Proteção de Dados para auxiliar no cumprimento das funções (63). As transferências de informações a outros países ou organizações internacionais deverão observar a mesma finalidade de utilização dos dados e respectiva atribuição, bem como se o receptor possuí legislação específica, garanta nível adequado de proteção, mediante verificações periódicas, não podendo ser subsídio para

eventual aplicação de pena de morte ou tratamento cruel/desumano (64, 67, 69 e 71).

As autoridades de controle possuirão autonomia e independência no exercício de suas atribuições (75 e 77). Ainda, possibilidade do titular dos dados peticionar a uma autoridade de controle única (85). Estipula prazo não superior a dois anos para adequação dos Estados Membros (96).

No mesmo sentido, a Convenção 108 + traz em seu bojo a mesma base conceitual da Diretiva, tendo por objetivo proteger as pessoas em relação ao tratamento de seus dados para garantia do direito à vida privada (art. 1º). Refere, também, que o tratamento de dados de pessoais para fins penais somente poderá ser realizado se houver previsão legal de garantias adequadas que complementem o previsto na Convenção (art. 6.1).

Prevê exceções, desde que previstas em lei, necessárias e proporcionais, para fins de investigação e repressão de infrações penais e execução de sanções penais (art. 11.1). Vale salientar, em seu item 59 do Relatório Explicativo a definição de que dado sensível são os tratamentos destinados a revelar informações sobre raça, etnia, saúde, religião ou opção sexual, salientando que imagens tratadas a partir de câmeras, de regra, não são dados sensíveis, veja-se:

> 59. O contexto do tratamento de imagens está relacionado com a determinação da natureza sensível dos dados. O tratamento de imagens não envolverá, em geral, o tratamento de dados sensíveis, uma vez que as imagens só serão abrangidas pela definição de dados biométricos quando forem tratadas através de um meio técnico específico que permita a identificação ou autenticação única de uma pessoa. Além disso, sempre que o tratamento de imagens se destine a revelar informação sobre raça, etnia ou saúde (ver ponto seguinte), esse tratamento será considerado como tratamento de dados sensíveis. Pelo contrário, **as imagens tratadas por um sistema de videovigilância apenas por razões de segurança numa zona comercial não serão, geralmente, consideradas como tratamento de dados sensíveis** (Conselho Da Europa, 2018, p. 21) *grifo nosso*.

Percebe-se, desta feita um balanço coerente entre os bens jurídicos tutelados em uma nação, onde privacidade e segurança são elevados ao mesmo patamar em homenagem à harmoniosa convivência[9].

[9] Conforme entendimento do Ministro Celso de Mello (BRASIL, STF, MS 23.452/99). OS DIREITOS E GARANTIAS INDIVIDUAIS NÃO TÊM CARÁTER ABSOLUTO. Não há, no sistema constitucional brasileiro, direitos ou garantias que se revistam de caráter absoluto, mesmo porque razões de interesse público relevante ou questões derivadas do princípio de convivência das liberdades legítimas, ainda que sejam específicas, a adoção, por parte dos órgãos estatais, de medidas restritivas das prerrogativas individuais ou coletivas, desde que respeitados os termos estabelecidos pela própria Constituição. O estatuto constitucional das liberdades públicas, ao delinear o regime jurídico a que estas estão sujeitas - e considerado o substrato ético que as informa - permite que sobre elas incidam limitações de ordem jurídica, designadas, de um lado, a proteger a integridade do interesse social e, por outro, a garantir a coexistência harmoniosa das liberdades, pois nenhum direito ou garantia pode ser exercido em detrimento da ordem pública ou com desrespeito aos direitos e garantias de terceiros.

3.2 PRINCÍPIOS RELATIVOS AO TRATAMENTO DE DADOS PESSOAIS

Passa-se à verificação dos princípios relativos ao tratamento de dados pessoais, constante no art. 4º da Diretiva 2016/680.

Princípio da Licitude e Lealdade – o tratamento de dados deve ser feito com base legal e de forma justa, sem manipulações, abuso ou uso indevido.

Princípio da Finalidade – a coleta deve ser realizada apenas para o fim específico para qual foi autorizada e sua posterior utilização manterá o proposito original da coleta.

Princípio da Necessidade – o tratamento deve limitar-se ao estritamente necessário para atingir a finalidade proposta, sem excessos de informações e de prazo na respectiva manutenção, devendo ser eliminados ou anonimizados, inclusive de forma automática uma vez expirado, evitando retenções indevidas.

Princípio da Qualidade e Exatidão – os dados devem ser corretos e mantidos atualizados, devendo ser retificados ou apagados sem demora.

Princípio da Segurança e Integridade – adoção de medidas técnicas e organizativas para proteção contra acessos não autorizados, perdas ou danos.

Princípio da Transparência – prestação de informações claras sobre o tratamento realizado, informando quais dados foram coletados, para que fins, quem tratou e seus respectivos direitos.

Finda a descrição dos princípios e da legislação aplicável em solo europeu, cabe traçar um horizonte para a futura legislação nacional.

4 PROPOSTA DE BALIZAS NORMATIVAS PARA O USO DO RECONHECIMENTO FACIAL EM TEMPO REAL NO BRASIL

Como afirmado anteriormente, o presente estudo não pretende fazer uma construção legislativa geral da LGPD-Penal, mas ofertar colaboração especificamente no que diz com as questões da tecnologia de reconhecimento facial, e delimitando a análise, apenas às imagens geradas em tempo real. Assim, pretende-se responder quem, como e por quanto tempo poderá ser realizado o tratamento de dados pessoais para essa finalidade.

4.1 DAS AUTORIDADES COMPETENTES

Respondendo a quem poderá realizar o tratamento de dados pessoais, considerando o seu potencial lesivo aos direitos e garantias fundamentais, sugere-se que os órgãos previstos no art. 144 da Constituição Federal (Brasil, 1988) estejam autorizados a fazê-lo, *in verbis*:

> Art. 144. A segurança pública, dever do Estado, direito e responsabilidade de todos, é

> exercida para a preservação da ordem pública e da incolumidade das pessoas e do patrimônio, através dos seguintes órgãos:
> I - polícia federal;
> II - polícia rodoviária federal;
> III - polícia ferroviária federal;
> IV - polícias civis;
> V - polícias militares e corpos de bombeiros militares.
> VI - polícias penais federal, estaduais e distrital.

Ainda, cabível o respectivo tratamento ao Ministério Público, nos termos do art. 128 da Constituição Federal (Brasil, 1988):

> Art. 128. O Ministério Público abrange:
> I - o Ministério Público da União, que compreende:
> a) o Ministério Público Federal;
> b) o Ministério Público do Trabalho;
> c) o Ministério Público Militar;
> d) o Ministério Público do Distrito Federal e Territórios;
> II - os Ministérios Públicos dos Estados.

De igual forma, ao Poder Judiciário *ex vi* art. 92 da Carta Magna (Brasil, 1988):

> Art. 92. São órgãos do Poder Judiciário:
> I - o Supremo Tribunal Federal;
> I-A o Conselho Nacional de Justiça;
> II - o Superior Tribunal de Justiça;
> II-A - o Tribunal Superior do Trabalho;
> III - os Tribunais Regionais Federais e Juízes Federais;
> IV - os Tribunais e Juízes do Trabalho;
> V - os Tribunais e Juízes Eleitorais;
> VI - os Tribunais e Juízes Militares;
> VII - os Tribunais e Juízes dos Estados e do Distrito Federal e Territórios.

Tratar-se-ia de um rol taxativo de autoridades competentes, possibilitando eventual expansão mediante previsão expressa em lei. Sempre salientando que teriam a supervisão/fiscalização da Autoridade Nacional de Proteção de Dados – ANDP (art. 4º, § 3º, c/c art. 5º, XIX, da Lei 13.709/18), autarquia de natureza especial, criada pela Lei n.º 14.460/22.

4.2 DO EXERCÍCIO DO TRATAMENTO

Para devida implementação e utilização da tecnologia de reconhecimento facial, primeiramente deverá ser precedida à uma Avaliação de Impacto na Proteção de Dados, detalhando medidas técnicas (encriptação, controle de acesso, garantias jurídicas e organizacionais e mecanismos de conformidade) auditorias, analisando os sistemas utilizados (software) e os respectivos procedimentos de registro do autor do tratamento e autores da visualização, modificação, transferência ou exclusão de cada dado pessoal. Essas informações são importantes para segurança do sistema, a autotutela da administração e eventual direito do titular dos dados em solicitações acerca de tratamentos existentes.

Ademais, a finalidade de tratamento de dados pessoais deverá estar obrigatoriamente relacionada a prevenção, investigação, detecção ou repressão de atos infracionais e infrações penais ou execução de sanções penais incluindo a salvaguarda e a prevenção de ameaças à segurança pública.

Como medida proporcional e objetiva, sugere-se que os autores de condutas previstas como contravenções penais (Decreto–Lei n.º 3.688/41) não integrem o banco de dados de reconhecimento facial. Seguindo, não deverão ser inseridas informações que não digam respeito à conduta do titular dos dados, tais como etnia, opinião política, religião, opção sexual e questões de saúde.

Restringir-se-ão, assim, os dados a identificação/individualização da pessoa, número do procedimento que levou ao tratamento[10] (registro policial, inquérito ou ação penal), bem como a condição em que se encontra (suspeito, indiciado, condenado, vítima ou testemunha), taxa de acurácia ou assertividade, seguido de um alerta que a imagem gerada se trata de uma evidência preliminar, sendo necessária a confrontação com outros elementos (abordagem e entrevista da pessoa, análise de cicatrizes ou tatuagens). Já o nome da autoridade que realizou o tratamento ou eventuais alterações, consultas e respectivo prazo, ficariam restritas ao campo auditoria.

Para a devida legalidade e transparência, o banco de dados de reconhecimento facial para fins penais deverá possuir base própria, integrando, mediante Termo de Cooperação, dados de todos os órgãos que trataram informações com essa finalidade[11]. Sugere-se, assim, um layout simples, claro, objetivo e uniforme nos moldes da figura abaixo.

Figura 2 – Layout do Sistema de Reconhecimento Facial Brasileiro



Fonte: Desenho gerado por meio de Inteligência Artificial – ChatGPT.

[10] Para ser realizado o tratamento de uma imagem, obrigatoriamente precisará estar vinculada a algum registro formal prévio, demonstrando, desta forma a respectiva necessidade e adequação.

[11] A integração de dados e padronização de sistemas são elementos preponderantes para evitar dados escuros (*dark data*). Sobre o tema, ver Albuquerque e Dorneles (2022).

Logo, seria possível advir informações de banco de dados do Poder Judiciário, informando condenados; sentenciados com suspensão condicional da pena (art. 78 do Código Penal c/c art. 698, § 3º, do Código de Processo Penal); sentenciados com livramento condicional (art. 718 do Código de Processo Penal); foragidos; acusados com suspensão condicional do processo (art. 89, da Lei n.º 9.099/95); autores que receberam transação penal (art.76, § 4º, da Lei n. 9.099/95); torcedores impedidos de ingressar em Estádios (art. 201, §2º, da Lei n.º 14.597/23); recolhidos em prisão domiciliar (art. 317 do CPP); agressores afastados (art. 12-C, da Lei n.º 11.340/06); bem como acusados possuidores de outras medidas cautelares (art. 319 do CPP).

Por sua vez, no âmbito dos órgãos do art. 144 da Constituição Federal, o banco de dados pessoais tratados poderia ser composto de registros policiais ou inquéritos policiais de suspeitos ou indiciados; e registro de fugitivos do sistema prisional. Já em relação ao Ministério Público, seria possível incluir dados pessoais tratados de Procedimentos Investigatórios Criminais (Resolução n. 181/17 do CNMP) ou de acordos de não persecução penal (art. 28-A, V, do Código de Processo Penal).

Ademais, todos usuários do Sistema de Reconhecimento Facial deverão passar por instrução específica prévia à sua utilização. Na oportunidade, a partir de diretrizes gerais, seriam repassadas condutas esperadas dos profissionais, esclarecendo as responsabilidades jurídicas e potenciais danos ao titular dos dados em caso de utilização indevida da ferramenta. Ainda, os usuários seriam chamados para novo treinamento e atualização a cada três anos.

4.3 DO PERÍODO DE TRATAMENTO

Para garantir que os dados pessoais tratados não permaneçam nos bancos de dados de forma eterna, os respectivos softwares deverão possuir mecanismos de alerta de expiração do prazo ou até mesmo exclusão automática, caso não haja alguma exceção legal de manutenção. Logo, a fim de evitar discricionariedades no tocante a qual período observar, sugestiona-se a regra do prazo de prescrição antes do trânsito em julgado da sentença (art. 109 do Código Penal), observando a conduta criminal descrita no primeiro tratamento[12].

O início da contagem do prazo, ocorreria na data do fato, sem aplicação de qualquer causa de diminuição, interrupção ou suspensão. Em caso de prática de outra ação criminal, seria

[12] Nos Estados Unidos, o FBI, nos termos da Avaliação de Impacto à Privacidade (2022, p.15), informou que retém os dados biométricos da pessoa tratada até o atingimento de 110 anos de idade.

realizado novo tratamento, e para fins de observância do prazo em relação a essa conduta, seriam individualizados por ação praticada. No caso de condenação, não haveria qualquer alteração na contagem do prazo de tratamento, sempre observados a data do fato e o período da prescrição antes do trânsito em julgado da sentença previsto no art. 109 do Código Penal.

Por sua vez, em caso de arquivamento do inquérito policial por parte do Ministério Público (art. 28 do Código de Processo Penal), sentença absolutória transitada em julgado ou extinção da punibilidade, o Poder Judiciário determinaria a exclusão do tratamento existente em relação ao fato, permanecendo eventuais tratamentos diversos anteriores ou posteriores.

Exemplificando, Zé dos Anzóis praticou um roubo no dia 01/04/2025. Foi preso em flagrante delito na mesma data, tendo seus dados pessoais tratados pela Seção de Inteligência da Polícia Militar no dia 10/04/2025. Foi indiciado, em 09/07/2025. Denunciado, 15/12/2025. Finalizada a ação penal no primeiro grau, condenado em 05/08/2027. Adveio recurso da defesa, não prosperando, tendo trânsito em julgado em 05/05/2030. Observadas as regras expostas no parágrafo anterior, o termo do prazo se daria passados dezesseis anos da prática do fato.

4.4 COMPARATIVO ENTRE A PROPOSTA E O DIREITO COMPARADO

Pelo que foi tratado anteriormente acerca da Legislação Europeia, bem como as propostas que foram feitas para a legislação nacional acerca do uso da TRF, pode se fazer a comparação que segue no quadro abaixo, a fim de melhor visualização:

Tabela 1 – Comparativo entre a proposta e a Legislação Europeia.

Tópico de Comparação	**Proposta**	**Legislação Europeia**
Avaliação de Impacto e Gestão de Riscos	Realização de uma Avaliação de Impacto na Proteção de Dados antes da implementação.	Realização de uma Avaliação de Impacto sempre que a utilização de uma nova tecnologia representar um risco para os direitos e liberdades (Diretiva 2016/680, Art. 27).
Categorização dos Titulares	O sistema deve registar expressamente a condição processual: suspeito, indiciado, condenado, vítima ou testemunha.	Deve haver distinção clara entre as diferentes categorias de titulares de dados (suspeitos, condenados, vítimas, terceiros) (Diretiva 2016/680, Art. 6º).
Proteção contra Vieses (Dados Sensíveis)	Proíbe informações que não digam respeito à conduta criminal, tais como etnia, opinião política, religião, etc.	"Categorias especiais de dados" (que incluem origem étnica, religião, biometria) só é podem ser tratados em casos de absoluta necessidade (Diretiva 2016/680, Art. 10).

Proporcionalidade e Finalidade	Deve ser obrigatoriamente ligado à prevenção, investigação ou repressão de atos infracionais e penais, não sendo utilizado para contravenções penais.	Exige o respeito pela necessidade e proporcionalidade estrita; as tecnologias intrusivas não devem ser banalizadas e utilizadas para infrações menores.
Intervenção Humana (Decisões Automatizadas)	O sistema deve apresentar um alerta de que é uma "evidência preliminar". É exigida a confrontação por um agente humano através de outras informações, como abordagem.	Proíbe que sejam tomadas decisões baseadas unicamente no tratamento automatizado que produzam efeitos jurídicos adversos, garantindo sempre a intervenção humana (Diretiva 2016/680, Art. 11).
Limitação de Armazenamento e Exclusão	Os softwares devem ter alerta de expiração de prazo ou exclusão automática - prazo sugerido: prescrição do Código Penal. O registo também é excluído em caso de arquivamento ou absolvição.	Princípio da "limitação de conservação" (Diretiva 2016/680, Art. 5º), proibindo bases de dados criminais perpétuas e exigindo prazos adequados e mecanismos automáticos para o apagamento ou a revisão da conservação dos dados.
Autoridades Competentes e Supervisão	Restringe o acesso aos órgãos previstos no Art. 144 da Constituição Federal, Ministério Público e Poder Judiciário. A supervisão e fiscalização ficariam a cargo da Autoridade Nacional de Proteção de Dados (ANPD).	Permite o tratamento estrito apenas por "autoridades competentes" da área policial/penal, mas exige a existência de uma Autoridade de Controle dotada de total independência institucional em relação aos órgãos fiscalizados.

Fonte: Elaborado pelos autores (2026).

5 CONSIDERAÇÕES FINAIS

Ampliar as perspectivas de uma convivência harmoniosa deve ser a busca incessante daqueles que orbitam na gestão pública. Nesse sentido, o presente estudo demonstrou a possibilidade de construção de uma legislação brasileira regulatória da tecnologia de reconhecimento facial em relação ao tratamento de dados para fins de prevenção, investigação e repressão de infrações penais que equilibra os direitos fundamentais da segurança, privacidade, liberdade de expressão e proteção dos dados pessoais.

Da pesquisa, restou cristalina a evolução crescente da tecnologia e as diferenças terminológicas que muitas vezes levaram ao descrédito da ferramenta. Ademais, foram pontuadas as autoridades competentes a realizar o tratamento de dados pessoais, limitando o rol à autorização legal específica. De igual forma, demonstrou-se a necessidade da Avaliação de Impacto na Proteção de Dados, bem como a importância da observância do princípio da finalidade, proporcionalidade e necessidade, não permitindo o tratamento de dados de autores de contravenções penais e informações acerca de etnia, opinião política, religião, opção sexual e questões de saúde, utilizando, ainda, por analogia, o prazo de retenção de imagens do art. 109 do Código Penal. Outrossim, visando a integração, propôs-se um modelo claro, objetivo e uniforme da utilização da tecnologia, em homenagem aos operadores do sistema e aos titulares

dos dados pessoais tratados, instrumentalizando e garantindo segurança jurídica a todos envolvidos nesse processo.

Como visto, os direitos e garantias individuais não possuem caráter absoluto. Assim, uma vez construída uma legislação coerente, no caso presente ancorada em importantes normativas europeias, jamais algum direito poderá ser exercido em detrimento da ordem pública ou com desrespeito aos direitos e garantias de terceiros (Brasil, STF, MS 23.452/99).

Postas essas observações, acredita-se ter sido estabelecido terreno fértil para elaboração de uma legislação nacional capaz de contribuir para otimização da segurança pública, em especial a partir da regulação do uso da tecnologia de reconhecimento facial, respeitando os ditames constitucionais.

REFERÊNCIAS

ALBIERO, Vitor; ZHANG, Kai; KING Michael; BOWYER Kevin W. Gendered differences in face recognition accuracy explained by hairstyles, makeup, and facial morphology. **IEEE Transactions on Information Forensics and Security**, v. 17, p. 127-137, 2021. Acesso em: 03 jun 2025.

ALBUQUERQUE, Alessandro Marinho de; DORNELES, Carina F.. Dados escuros à luz do controle público. In: SIMPÓSIO BRASILEIRO DE BANCO DE DADOS (SBBD), 37., 2022, Búzios. **Anais** [...]. Porto Alegre: Sociedade Brasileira de Computação, 2022. p. 78-89. ISSN 2763-8979. Disponível em: https://doi.org/10.5753/sbbd.2022.224331. Acesso em: 16 ago 2025.

ASSUMPÇÃO, Paulo S. de S. L. de; MENDONÇA, Luziane F. de. **Detecção e reconhecimento de minúcias em imagens datiloscópicas: uma abordagem holística.** In: CONGRESSO NACIONAL DE MATEMÁTICA APLICADA E COMPUTACIONAL (CNMAC), 35., 2015. Disponível em: https://scispace.com/pdf/deteccao-e-reconhecimento-de-minucias-em-imagens-1ddq849l1q.pdf. Acesso em: 4 jun. 2025.

BRASIL. **Lei nº 13.709/2018**. Brasília, DF. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 09 jul. 2025.

BRASIL. Câmara dos Deputados. **Anteprojeto de lei – proteção de dados para segurança pública e persecução penal. Brasília**, DF. 2020. Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica/outros-documentos/DADOSAnteprojetocomissaoprotecaodadossegurancapersecucaoFINAL.pdf. Acesso em: 09 jul. 2025.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 1.515/2022**. Brasília, DF, 2022. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2182274&filename

=PL%201515/2022. Acesso em: 09 jul. 2025.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Senado Federal, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 28 jul. 2025.

BRASIL. Supremo Tribunal Federal. **Mandado de Segurança n. 23.452/DF**. Relator: Ministro Celso de Mello. Julgado em: 16 set. 1999. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=85966. Acesso em: 04 ago. 2025.

CONSELHO DA EUROPA**. Convenção 108+**. Elsinore, 2018. Disponível em: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1. Acesso em: 11 jul. 2025.

CRUMPLER, William; LEWIS, James A. **Facial Recognition Technology - Responsible Use Principles and the Legislative Landscape**. CSIS. 2021. Disponível em: https://www.csis.org/analysis/facial-recognition-technology-responsible-use-principles-and-legislative-landscape. Acesso em 02 jun. 2025.

FBI. **Privacy Impact Assessment For The Next Generation Intestate Photo System** (PIA). 2022. Disponível em: https://www.fbi.gov/file-repository/pias/pia-ngi-interstate-photo-system.pdf/view. Acesso em 05 ago. 2025.

FERREIRA, Lucas Oliveira Gomes; ARAGÃO, Priscila da Costa Mesquita. **Aderência das auditorias financeiras das Instituições Superiores de Controle: Um estudo comparativo das metodologias entre Brasil, Estados Unidos, Reino Unido e Austrália**. REVISTA DO TCU, Brasília, v. 150, n. 150, p. 59–84, 2022. Disponível em: https://revista.tcu.gov.br/ojs/index.php/RTCU/article/view/1889. Acesso em: 21 mai. 2025.

GAO**. Biometric Identification Technologies:Considerations to Address Information Gaps and Other Stakeholder Concerns**. 2024. Disponível em: https://www.gao.gov/products/gao-24-106293. Acesso em: 21 mai. 2025
GREENBAUM, Dov; NAKAR, Sharon. **Now You See Me. Now You Still Do: Facial Recognition Technology and the Growing Lack of Privacy**. JOURNAL OF SCIENCE & TECHNOLOGY LAW, vol.23.1. 2017. Disponível em: https://www.bu.edu/jostl/archives/vol-23-1-winter-2017/. Acesso em 25 jun. 2025.

GROTHER, Patrick; NGAN, Mei; HANAOKA, Kayee. **Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects**. NIST. 2019. Disponível em: https://nvlpubs.nist.gov/nistpubs/ir/2019/nist.ir.8280.pdf. Acessado em: 11 de jun. de 2025.

LI, Minghan. **Research and Analysis of Facial Recognition Based on FaceNet, DeepFace, and OpenFace**. In: INTERNATIONAL CONFERENCE ON DATA SCIENCE, ADVANCED ALGORITHM AND INTELLIGENT COMPUTING. v. 70, 2025. Disponível em: https://doi.org/10.1051/itmconf/20257003009. Acesso em: 14 mai. 2025.

LYNCH, Jennifer. **Face Off: Law Enforcement Use of Face Recognition Technology**. ELECTRONIC FRONTIER FOUNDATION. 2020. Disponível em: https://www.eff.org/wp/law-enforcement-use-face-recognition. Acesso em: 02 mai. 2025.

PARKER, Jake. **What NIST Data Shows About Facial Recognition and Demographics**. SAI. 2020. Disponível em: https://www.securityindustry.org/wp-content/uploads/2020/02/SIA-NIST-data-and-facial-recognition.pdf. Acesso em: 11 jun. 2025.

SIMONITIS, Mark. **Facial Recognition Technology and the Constitution**. NOTRE DAME J. ON EMERGING TECH**.** vol.2, n.2, 2021. Disponível em: https://scholarship.law.nd.edu/ndlsjet/vol2/iss2/5/. Acesso em: 23 jun. 2025.

SEARSTON, Rachel. A.; THOMPSON, Matthew. B.; ROBSON, Samuel. G.; TANGEN, Jason. M. **Beyond minutiae: inferring missing details from global structure in fingerprints**. COGNITIVE RESEARCH: PRINCIPLES AND IMPLICATIONS, v. 10, art. 3, 2025. Disponível em: https://doi.org/10.1186/s41235-025-00610-z. Acesso em: 31 mai. 2025.

UNIÃO EUROPEIA. Parlamento Europeu; Conselho da União Europeia. Diretiva (UE) 2016/680. **Jornal Oficial da União Europeia**, L 119, p. 89–131. 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32016L0680. Acesso em: 10 jul. 2025.