Revista Científica O DIREITO PENSA
v.4, n.2
ISSN 2675-844X

# A UTILIZAÇÃO DO RECONHECIMENTO FACIAL NA SEGURANÇA PÚBLICA BRASILEIRA

## *THE USE OF FACIAL RECOGNITION IN BRAZILIAN PUBLIC SECURITY*

Maria Eugênia Fachone Soares [86]
Bruna Beatriz Dutra Ferreira[87]
Ana Maria Molinari [88]

**Resumo:** As tecnologias de reconhecimento facial e de vigilância estão cada vez mais sendo implementadas hodiernamente, principalmente, nos âmbitos da segurança pública. Apesar da sua crescente utilização, não há no Brasil uma regulamentação específica que possa ser aplicada, e, considerando as taxas de erro e de discriminação, a problemática da violação de garantias fundamentais se mostra presente, ainda mais no que tange ao desrespeito dos princípios constitucionais, necessitando de uma normativa que atenda as demandas e as especificidades de tal tecnologia. O presente trabalho buscou, ao tratar da problemática, a revisão bibliográfica, utilizando-se de artigos e reportagens sobre o tema.

**Palavras-Chave**: Vigilância Pública; Regulamentação; Viés algoritmo; Armazenamento de dados.

**Abstract:** Facial Recognition and surveillance technologies are increasingly being implemented nowadays, mainly, in public security areas. Despite its increasing use, in Brazil, so far, there is no regulation that can be applied to, considering the possibilities of error and discrimination rates. Therefore, violation of fundamental guarantees is present, even more when there is constitutional principles disrespect. For instance, it's required to have a specific regulation about the subject involving new technologies. The themes discussed in this paper is going to talk about how it's possible to solve this problem, by a bibliographical review, using articles, academic papers and reports on the topic;

**Keywords**: Public surveillance; Regulation; Algorithm bias; Database.



## 1. Introdução

[86] Graduanda de Direito na Universidade Estadual de Maringá; estudante do segundo ano de Direito; Maringá, Paraná, Brasil; eugeniafachone@gmail.com.
[87]Graduanda de Direito na Universidade Estadual de Maringá; estudante do segundo ano de Direito; Cianorte, Paraná, Brasil; ra128780@uem.br.
[88] Graduanda de Direito na Universidade Estadual de Maringá; estudante do segundo ano de Direito; Paiçandu, Paraná, Brasil; anam.molinari02@gmail.com.

A insegurança pública é uma pauta que o Brasil reconhece enquanto uma de suas grandes falhas. Anualmente, o Fórum Brasileiro de Segurança Pública (FBSP) efetua um documento contendo dados de diversos aspectos do conteúdo de segurança pública no país, o Atlas da Violência, e os dados prosseguem alarmantes. Dentre os dados, destaca-se a desproporção da quantidade elevada de delitos existentes para com as soluções de casos; prova disso são as taxas baixas em relação aos homicídios no país, contabiliza-se 37% de resolução (Estadão Conteúdo, 2022). Assim, os motivos para a pouca efetividade podem ser variados, desde formulação e composição das polícias à falta de instrumentos que potencializem a dinâmica investigativa.

Em diversos casos em que problemas complexos surgem, é frequente a generalização nas decisões, por vezes sem muito critério e escolha, compreendendo as suas nuances. E no presente da segurança pública brasileira, seria possível um paralelo com a crescente implementação de uso desgovernado de inteligências artificiais para identificação de faces com objetivos gerais como o de prevenir incidentes, encontrar foragidos e pessoas desaparecidas. Dessa maneira, as tecnologias de reconhecimento facial (RF) "têm sido objeto de promessas tentadoras do setor privado e da Administração Pública, especialmente quando adotadas para fins de policiamento e segurança pública, ao argumento de mitigação da impunidade e aumento da eficiência do trabalho policial" (Costa, Kremer, 2022, p. 162). No entanto, apesar de crescentemente ser utilizada, ela pode porventura ser usada para outros fins não democráticos e, ainda, não ter tamanha aferência entre o identificado e a face base para identificação, demonstrando falhas que podem gerar consequências drásticas e violação de princípios basilares de nossa Constituição Federal e os direitos fundamentais, tais como o direito à imagem e à proteção de dados sensíveis que serão abordados no presente artigo.

O presente trabalho, então, a partir de revisão de literatura, pesquisa bibliográfica e consulta de notícias e reportagens, buscou traçar as principais questões que recaem na problemática da utilização das ferramentas de reconhecimento facial e de tecnologias de vigilância. Nesse sentido, buscou-se entender o que é e como pode ser aplicada, se há regulamentação, quais os riscos de sua implementação e como ela está sendo utilizada pela segurança pública.

## 2. O reconhecimento facial na segurança pública brasileira

A tecnologia de reconhecimento facial se baseia na utilização de algoritmos e aprendizado de máquinas que, juntos, buscam identificar um indivíduo, a partir de imagens, vídeos e fotos, coletadas simultaneamente à sua análise, com base em padrões de sua fisionomia (Almeida, 2022, p. 267). Inicialmente, a tecnologia pormenoriza os dados coletados para *templates* (reduções das características à ordem de representação matemática) para que elas sejam colocadas em comparação a outros *templates* presentes no banco de dados ao qual está sendo embasado. Para isso, a técnica de verificação busca na face humana os dados considerados relevantes e únicos, como a distância entre os olhos ou o formato do queixo" (Almeida, 2022, p. 267).

Após essa comparação, é possível ter como resultado a sua identificação de maneira precisa ou não. Assim, quando há imprecisão, a tecnologia de reconhecimento facial diferenciará a situação entre aquele que resulta como falso negativo (quando ocorre indeterminação na correlação entre dado e rosto de modo que não se identifica o indivíduo que estaria no banco de dados) e o falso positivo (incongruência na correspondência, identificando erroneamente a pessoa, afirmando que seria alguém que não é) (Almeida 2022, p. 268).

Ou seja, pode ocorrer não só a inferência na identificação, como pode-se deixar de verificar alguém que deveria ser identificado. Por isso, apesar da tecnologia via de regra ser analisada exclusivamente enquanto positiva, muitas das vezes por se tratar de uma ferramenta objetiva e mais precisa que o ser humano, os algoritmos inseridos na funcionalidade de identificação facial não são precisos; pelo contrário, são capazes de iniciar inferências complexas e perigosas.

Ainda por conta desse reconhecimento, essas tecnologias podem ser utilizadas tanto no âmbito público como em áreas da segurança privada. Essa aplicabilidade é notável em aplicativos de celular que precisam identificar, via dispositivo móvel, determinado sujeito que está usufruindo dos serviços daquele aplicativo, como é o caso da Latam, que executa a verificação de identidade com base no reconhecimento facial, que é utilizado através de dispositivos com acesso à câmera e *internet* (Tonetti, 2023). Tal perspectiva tem sido bem acolhida pelo público, uma vez que, por conta de a máquina efetivar análise de aspectos objetivos sem grandes possibilidades de subjugamento e baixos índices de imprecisão, ao menos do ponto de vista comum.

Assim, com a visão positiva dessa via possível, o Brasil tem explorado o uso do reconhecimento facial em esferas como a segurança pública. No entanto, uma vez que tal

ferramenta se utiliza de dados sensíveis para a efetivação de seu trabalho, é necessário maior cautela com a abrangência de sua atividade, de modo que a regulamentação acerca do tema seria de significativa relevância para que não fossem feitas exacerbações com as relações feitas pela máquina, bem como nas consequências práticas que podem ser geradas a partir do seu uso, como uso indevido de dados sensíveis e até predatismo criminal.

No entanto, a realidade prática é de que os estados e municípios brasileiros têm buscado providenciar a novidade às pressas, tanto que, "elas vêm sendo implementadas desde 2019 por vinte estados das cinco regiões do país" (Ventura, 2021 apud Costa, Kremer, 2022, p. 162)), isso, mesmo com a ausência de legislação específica que delimite os parâmetros de uso e de finalidade dessa tecnologia dentro do contexto da segurança pública. Por isso, em vista do uso desregulado, muitas das vezes, a sua utilização não permanece a par da transparência e pode infringir diretamente com questões de cunho ético, a depender de como sua utilização é verificada.

Um dos primeiros estados a mostrar interesse na implementação dessa tecnologia foi o Rio de Janeiro, que, a partir da Lei nº 7.123/2015, teve como objetivo a "intenção expressa de um banco de dados a fim de identificar pessoas e controlar acesso a determinados lugares" (Francisco, 2020, p. 13 apud Junior, 2021, p. 161). Diante disso, outros estados das demais localidades do país começaram a demonstrar interesse nessa ferramenta. Outro exemplo que é possível citar é o do Rio Grande do Sul, em que o deputado federal Bibo Nunes propôs um Projeto de Lei que buscou implementar o reconhecimento facial e tecnologias afins, na identificação de indivíduos e análise de comportamentos, e que, se for aprovada, servirá de base para os demais projetos (Brasil, 2019 apud Junior, 2021, p.162).

No Paraná, a tecnologia de reconhecimento facial tem sido recentemente implementada dentro do âmbito de segurança pública. Em 2022, foi autorizado projeto que viabiliza a utilização de câmeras com tecnologia de identificação de pessoas e placas de veículos em viaturas policiais, chamadas de "viaturas inteligentes" e que compõem o projeto intitulado "Olho Vivo" (Paraná, 2023). No entanto, em vista de diversas problemáticas, dezoito projetos que envolvem o reconhecimento facial no Paraná estão em debate na Comissão de Constituição e Justiça (CCJ) na Assembleia Legislativa do Estado (Garcia, 2023).

A utilização do reconhecimento facial, apesar de em um primeiro momento apresentar grande avanço na área da tecnologia, pode aumentar a capacidade preventiva e punitiva do Estado, principalmente no que diz respeito a criação de um padrão e de perfis criminosos a

partir de características físicas, emocionais e sociais, podendo ter um aumento ainda maior na discriminação de grupos já estigmatizados (Steffen, 2023, p. 113). Nesse sentido, segundo estudos de Babuta e Oswald (2019), foi possível perceber que a discriminação geográfica já é uma realidade, uma vez que a inteligência artificial colabora para que pessoas que moram em certas regiões sejam mais revistadas e paradas, além do aumento de prisões em determinadas localidades que são mais monitoradas e controladas (Babuta, Oswald, 2029 apud Steffen, 2023, p. 115). Em vista desse entendimento de que a tecnologia de reconhecimento facial pode ser prejudicial, movimentos político-sociais têm instigado o debate acerca da temática, de modo que, como um dos destaques, o movimento #TireMeuRostoDaSuaMira defende que, uma vez que o viés algoritmo é um fator prevalente nessa espécie de tecnologia, a utilização do reconhecimento facial na segurança pública deveria ser reduzida completamente.

Isso porque, em uma sociedade com uma quantidade de compartilhamento de dados intensa, em que não há transparência sobre o seu armazenamento, somado às tecnologias de vigilância e de reconhecimento facial, observa-se que a utilização dessas ferramentas pode gerar um controle massivo da população (Camara, 2021, p.66).

## 3. Aplicações concretas na segurança pública

O *machine learning* é um campo da IA que se aprimora de forma automática, conforme as respostas são processadas por meio de uma experiência, podendo envolver tanto imagens quanto modelos matemáticos. Quando se trata de desenvolver um sistema de aprendizado de máquina, o método empregado é a indução – *inputs* –, no qual hipóteses são geradas a partir de dados, independentemente de serem corretos ou incorretos. Dessa forma, o objetivo final desse sistema é criar suas próprias regras ou questões. Isso possibilita que *softwares* executem tarefas sem a intervenção do homem, se baseando em algoritmos para tomar decisões apenas se norteando pelos modelos gerados e não por instruções previamente programadas (Crippa, 2021, p. 162).

No entanto, a aplicação do reconhecimento facial no contexto da segurança pública no Brasil enfrenta desafios significativos. Um dos principais problemas destacados por cientistas sociais e juristas é a preocupação de que essa tecnologia possa reforçar a seletividade do sistema penal brasileiro, introduzindo vieses étnicos e de gênero que comprometem a confiabilidade dos resultados (Crippa, 2021, p. 167). Isso porque a ferramenta de reconhecimento facial tem levado diversas pessoas inocentes à prisão desde sua implementação. Especialistas apontam que o sistema se baseia em catálogos informais e é

fundamentado no racismo algorítmico, visto que estudos mostram que o índice de erro chega a quase 40% para mulheres negras e pessoas trans, enquanto para homens brancos o índice de erro é de 0.3% (Bragado, 2023.)

A correção dos vieses nas máquinas que utilizam *machine learning* é um desafio crucial. Como apontado por Vieira (2019, p. 3), esses vieses podem surgir em diferentes estágios do processo de *machine learning*. O primeiro ponto crítico é a função do programa e seu objetivo. O segundo ponto é a coleta de dados e seus bancos de dados originários a serem usados ou não por algoritmos treinados tendenciosos. O terceiro ponto refere-se à manipulação dos dados, especialmente se informações sensíveis, como raça, cor e gênero.

Assim, entendendo que a tecnologia de conferência facial necessita, como predisposição, de um banco de dados em que possa embasar e comparar *templates*, é preciso compreender a origem dos dados coletados. Diante disso, no que tange ao armazenamento e os locais em que são armazenados os dados utilizados pela segurança pública, em sua maioria estão sendo alimentados e alocados pelos álbuns de fotografia das delegacias de polícia e, ressalta-se novamente, sem uma normativa que regulamente quanto ao seu uso. Essa problemática pode ter consequências dentro da condução do processo criminal "em decorrência da ausência de cautela no momento do recebimento de uma denúncia ou condenação, fato que corrobora para que pessoas inocentes sejam presas" (Soares, 2020, p. 24).

Para além disso, é possível perceber a divergência e a dificuldade de comunicação e interligação das diversas polícias e suas instâncias no Brasil. Essa complicação resulta na Clique aqui para inserir texto. a utilização de bancos de dados diversos, não favorecendo na troca de informações ou até na efetividade de resultados. Por isso, na prática, a busca em identificar criminosos, tanto com a utilização de reconhecimento facial, ou não, faz com que cada instância policial gere "seu próprio conjunto de dados, atuando de forma distinta e perdendo, muitas vezes, a eficiência por falta de uma comunicação efetiva". (OBSERVATÓRIO DE SEGURANÇA PÚBLICA, *s.d* apud Soares, 2020, p. 10).

Por isso, dentro Judiciário, em mais de dez anos foi desenvolvido e implementação o "Banco Nacional de Mandados de Prisão" pelo Conselho Nacional de Justiça, já integrado em todos os tribunais, passando a ser uma ferramenta que possibilita o registro e a consulta sobre a existência de mandados de prisão contra determinados cidadãos" (BRASIL, 2018a apud Soares, 2020, p.10). Essa coleta de imagens dentro do "contexto de implementação de RF,

esse banco de dados se assemelha ao modelo do Reino Unido, no qual, a fim de reconhecer o indivíduo que passa por câmeras de vigilância, essa pessoa tem seu *template* comparado com o de uma pessoa que teve prisão determinada" (ALMEIDA, 2022, p. 272-273).

Destaca-se nesse cenário, como menciona Almeida (2022), que as imagens dos presos de custódia também são compiladas no banco de dados, mesmo que, nesse cenário, não sejam, obrigatoriamente, indivíduos que cometeram crimes. Por isso, também deve-se ser levado em consideração o teor racista que muitas das vezes os presos cautelares sofrem e que o Brasil perpetua. Assim, apesar da tecnologia ser uma ferramenta na sociedade moderna de grande credibilidade e que atrai entendimentos positivos, em detrimento de sua alta eficácia, baixo nível de erros e imprecisões, existem setores em que atua que ainda não foram desenvolvidos de maneira a serem irrevogáveis. Isso, levando-se em consideração que dentro do contexto do reconhecimento facial que, como descrito anteriormente, trabalha com reduções matemáticas denominadas *templates* e que se baseiam na distância entre pontos estratégicos do rosto - não exclusivos de cada indivíduo - e que sua identificação é afetada diretamente por condições de luminosidade adequadas e similares, de uma perspectiva frontal, e, fotos com diferenças significativas, podem aumentar as taxas de erro de maneira significativa (Lynch, 2018 apud Oliveira et al, 2022, p. 118).

Na prática, o reconhecimento e a comparação de imagens de humanos assumem dificuldades diversas, como é descrito por Timnit Gebru, à época um dos gestores técnicos de equipe ética da Google, em pesquisa realizada junto a Joy Buolamwini verifica que há maiores erros de identificação de gênero e raça no caso de mulheres de pele mais escura, ratificando estereótipos, principalmente quando se analisa o perfil da população carcerária, que é constituído em 60% por mulheres negras, mesmo sem o uso do Reconhecimento Facial e sua implementação (Buolamwini, Gebru, 2018 apud Silva, Silva, 2019 p. 13-14).

Ainda assim, diante de circunstâncias preocupantes que poderiam revelar o grande risco de sua utilização, a ferramenta tem sido exponencialmente exaltada e utilizada, como exemplo de comparação, dentro do contexto paulista, em estudo feito pela rede Observatório da Segurança, acerca das referências realizadas acerca da temática de reconhecimento facial na segurança pública, foi verificado que, "entre 2015 e 2018, o termo foi mencionado nos documentos 312 vezes, enquanto em 2019 foi mencionado 514 vezes e em 2020 foram 638 menções, mais que o dobro do intervalo entre 2015 e 2018" (Sousa, 2021, online).

Não à toa, em vista dos pontos falhos destacados e o crescente uso dessa inovação inserida no contexto público, são relatados casos de injustiças decorrentes de reconhecimentos

errôneos. Um caso emblemático que ilustra essa falha significativa ocorreu na cidade do Rio de Janeiro, onde o sistema de reconhecimento facial em uso pela Polícia Militar falhou de forma alarmante, levando à detenção equivocada de uma mulher. Após ser identificada pelas câmeras de reconhecimento facial instaladas em Copacabana, a mulher foi conduzida à delegacia, onde ficou evidente que ela não correspondia à pessoa procurada. Os policiais, equivocadamente, a abordaram acreditando que estavam detendo uma foragida da justiça, acusada de homicídio e ocultação de cadáver. No entanto, ao ser levada à 12ª delegacia de Copacabana, a identidade da mulher detida por engano foi minuciosamente verificada e os agentes constataram que ela não era a pessoa procurada, explicitando de maneira incontestável as sérias deficiências e riscos associados à utilização dessa tecnologia. (Camara, 2021, p.70-71)

Embora o reconhecimento facial possa parecer uma tecnologia indubitavelmente eficaz, esses recorrentes incidentes destacam a crucial necessidade de reconhecer suas falhas e limitações, além de assegurar a proteção dos direitos individuais e a equidade em sua aplicação. A excessiva dependência no reconhecimento facial pode conduzir a injustiças e discriminação, ressaltando a imperatividade de regulamentações e abordagens responsáveis para sua utilização.

Para além dos falsos positivos, a tecnologia pode ser utilizada para viabilizar o poder político. Isso porque, em sua essência, essa é uma ferramenta que os governos utilizam para administrar suas nações, garantindo a segurança e o bem-estar de seus cidadãos. Em um contexto globalizado, o poder político tem se manifestado de maneira cada vez mais intrusiva e abrangente. Conforme Mbembe (apud Soares, 2020), o Estado utiliza a tecnologia como instrumento de controle, frequentemente justificando essa ação como uma forma de proteger a sociedade. No entanto, o resultado desse uso excessivo de tecnologia muitas vezes é a submissão do povo diante do poder estatal visto que, o Estado, por meio de suas leis e regras, detém o poder de decidir quem vive e quem morre, quem é preso e quem mantém sua liberdade.

Tem-se como exemplo um caso ocorrido em Hong Kong, onde o reconhecimento facial foi extensivamente utilizado para reprimir manifestantes e controlar protestos contra o governo em 2019 (Pichonelli, 2021 apud Silva; Clemente, 2021, p.152). Isso levanta preocupações significativas sobre o abuso de poder por parte das autoridades, que usam essa tecnologia para sufocar a liberdade de expressão e o direito de protestar. A manipulação desse sistema deve ser motivo de contínua polêmica em países democráticos. A vigilância em massa

pode minar os direitos civis e individuais, ameaçando os alicerces da democracia (Lavado, 2020 apud Silva; Clemente, 2021, p.152).

Portanto, à medida que se navega por esse território incerto onde o poder político e a tecnologia se encontram, deve-se manter um olhar vigilante sobre as mudanças em curso e suas ramificações. Os desafios que se apresentam são complexos e multifacetados sendo crucial continuar a explorar e discutir essas questões em busca de soluções que equilibrem as necessidades da sociedade com a preservação dos valores democráticos.

Nos Estados Unidos, a utilização de tecnologia dentro da segurança pública também é controversa. O algoritmo COMPAS (Perfil de Gerenciamento Corretivo de Infratores para Sanções Alternativas), por exemplo, é uma ferramenta desenvolvida pela empresa Northpointe, hoje conhecida como Equivant, que tem como objetivo principal realizar avaliações de risco sobre pessoas que voltam a praticar crimes. Seu propósito é auxiliar na tomada de decisões judiciais e mitigar riscos futuros, fornecendo orientação aos juízes nos tribunais dos Estados Unidos, a fim de aprimorar o sistema de justiça penal (Vieira, 2019, p 01). No entanto, o uso do COMPAS foi objeto de controvérsias, sobretudo após um estudo da ProPublica, jornal investigativo estadunidense, que levantou questões preocupantes sobre sua eficácia e imparcialidade.

O estudo da ProPublica, baseado na análise de dados de mais de 7 mil pessoas presas no condado de Broward, Flórida, nos anos de 2013 e 2014, trouxe à tona sérias preocupações. O algoritmo COMPAS, quando avaliava o risco de reincidência, apresentou viés racial evidente. Segundo a pesquisa, as pessoas negras eram rotineiramente classificadas como de alto risco, enquanto as pessoas brancas eram designadas como de baixo risco. Esse viés racial é uma questão alarmante, pois pode agravar as disparidades raciais já existentes no sistema de justiça criminal. A principal constatação do estudo da ProPublica foi que, na prática, as previsões do COMPAS eram frequentemente equivocadas. Muitos indivíduos negros classificados como de alto risco não voltavam a cometer crimes, enquanto alguns brancos identificados como de baixo risco, na realidade, reincidiam. Esse descompasso entre as previsões do algoritmo e a realidade das reincidências demonstra que o COMPAS, apesar de sua pretensão de aprimorar a justiça criminal, pode, na verdade, agravar a desigualdade racial no sistema penal (Vieira, 2019, p.1).

No contexto brasileiro, as controvérsias em torno do algoritmo COMPAS ressaltam preocupações relevantes relacionadas ao uso de tecnologias de análise de dados e, por extensão, ao reconhecimento facial na segurança pública do Brasil. Como o estudo do

COMPAS revelou um viés racial, no Brasil, onde as disparidades raciais são igualmente uma questão premente, a aplicação do reconhecimento facial continua a levantar questões similares de viés racial, ameaçando a equidade no sistema de justiça.

As preocupações levantadas pelo estudo do COMPAS nos Estados Unidos sobre a eficácia e imparcialidade de algoritmos de avaliação de risco são especialmente relevantes em um cenário em que o sistema de justiça brasileiro também enfrenta desafios significativos. Segundo Alcântara (2021), dados do Superior Tribunal de Justiça (STJ) indicam que, em 2021, 78 pessoas que haviam sido presas com base em procedimentos de reconhecimento pessoal ou identificação por foto foram inocentadas, tiveram seus processos suspensos ou a prisão relaxada devido a irregularidades nesses procedimentos. Isso porque o STJ tem observado irregularidades em diversas ações judiciais com provas baseadas apenas nesse tipo de procedimento de identificação. A pesquisa realizada pelo tribunal teve como foco o método de reconhecimento pessoal após uma mudança na jurisprudência do STJ, conhecida como o "*leading case"*. Os resultados dessa pesquisa resultaram em decisões favoráveis aos acusados, incluindo sentenças que afastaram prisões preventivas, suspenderam o andamento de processos ou inocentaram os indiciados.

Embora os dados e análises específicos sobre o uso do reconhecimento facial no Brasil ainda sejam limitados, o Conselho Nacional de Justiça (CNJ) reconheceu a necessidade de abordar essas preocupações. O CNJ constituiu um grupo de trabalho para reduzir o número de prisões de inocentes, estabelecendo regras e procedimentos claramente definidos para o reconhecimento pessoal de criminosos.

É crucial destacar que, de maneira semelhante ao que ocorreu nos Estados Unidos com o COMPAS, no Brasil, o viés racial também se faz presente. Uma pesquisa realizada pela Defensoria Pública do Estado do Rio de Janeiro (DPRJ) concluiu que em 83% dos casos de erro em reconhecimentos, as pessoas eram negras. Isso sublinha a importância de abordar as questões relacionadas à equidade e ao viés racial na aplicação da justiça, especialmente no contexto do reconhecimento facial (Alcântara, 2021, *online*).

Assim, ao passo que o CNJ busca aprimorar os procedimentos de reconhecimento pessoal e o uso de tecnologias de análise de dados na segurança pública no Brasil, a discussão sobre a equidade, a imparcialidade e a confiabilidade das provas no sistema de justiça ganha destaque, refletindo as preocupações já observadas no contexto do COMPAS nos Estados Unidos. A esperança é que essas iniciativas contribuam para um sistema de justiça mais justo

e preciso no Brasil, evitando prisões injustas e garantindo os direitos fundamentais dos cidadãos.

## 4. Regulamentação do Reconhecimento Facial

A discussão do uso de inteligências de reconhecimento facial tem desenvolvido críticas quanto ao seu uso, mesmo quando inexiste regulação específica no território brasileiro. Recentemente, no Brasil, em vista da ampla crítica que pesquisadores e movimentos sociais têm feito acerca do uso do reconhecimento facial na segurança pública nacional, foi indicado na Câmara dos Deputados o Projeto de Lei 2.392 de 2022, que tem como demanda a proibição do uso dessas tecnologias na esfera penal. O PL, em seu artigo 3º, trata de propor o não uso dessa espécie de tecnologia para reconhecimento do indivíduo sem que antes seja realizado relatório de impacto à privacidade, com base na defesa da Lei Geral de Proteção de Dados. Ademais, o projeto legislativo prevê que o resultado de suposta aferência entre *templates* não deverá ser utilizado unicamente para identificação (artigo 4º). E, ainda, no artigo 2º do PL, avalia-se que os dados provenientes de bancos de dados dessas ferramentas não poderão ser terceirizados, esclarecendo que, em caso de existir cláusula em contrato permitindo essa terceirização, ela será nula (CAMARA DOS DEPUTADOS, 2023).

Até porque, como é possível de verificação do ordenamento jurídico brasileiro, o direito à imagem se trata de direito fundamental, tal como descreve o artigo 5º, inciso X, da Constituição Federal, sendo ele, portanto, um direito inviolável (BRASIL, 1988 apud Soares, 2020, p. 14). Além disso, a Lei Geral de Proteção de Dados vigente no país trata de maneira indireta alguns assuntos e temáticas de grande relevância para essa tecnologia, como a definição de dados sensíveis. Sendo válido ressaltar que os dados biométricos, enquanto dados sensíveis, possuem definição no artigo 5º, II, da referida lei.

Também dentro do contexto da LGPD, em relação aos direitos da personalidade, enquanto essenciais na era da informação, envolvem o dado pessoal como pertencente aos direitos individuais, podendo eles serem fornecidos exclusivamente por meio de autorização do titular ao adquirente (Pereira, 2022, p. 3). De maneira inicial, a LGPD, no caso brasileiro, permite que, de antemão, haja um direcionamento do que é possível incrementar dentro do sistema de reconhecimento facial e aquilo que não o é. Até porque, em vista da complexidade que os cruzamentos de dados disponíveis na somatória dos bancos de dados interligados, pode invadir de diversas maneiras a privacidade do indivíduo que tem suas informações armazenadas, de modo que “o perigo é tão maior quanto mais a utilização da informática facilita a interconexão de fichários com a possibilidade de formar grandes bancos de dados

que desvendem a vida dos indivíduos, sem sua autorização e até sem seu conhecimento" (SILVA, 2015, p. 211- 212 apud Soares, 2020, p. 14). A realidade de uso de dados sem o consentimento, inclusive, é, ao contrário do que se define ético e coerente com normas de privacidade, uma atividade relativamente comum entre *big techs*. Isso, em vista de que algumas delas estariam usando "fotografias, existentes numa base de dados da IBM, sem a sua permissão" (Musil, 2020 apud Melo e Serra, 2022, p. 210).

Diante disso, alguns projetos de lei sobre o tema buscaram uma efetiva implementação da LGPD, como o Projeto de lei nº 1.515/22, do deputado Coronel Armando. Neste Projeto, visa-se, sendo respeitadas as garantias dos indivíduos, a aplicação da Lei Geral de Proteção de Dados Pessoais, como disposto no art. 4º, inciso III, para fins de investigação e repressão de infrações penais, como uma política de segurança e defesa nacional (De Castro, De Paula, 2022). Além deste, o Projeto de Lei nº 9.736/2018 busca propor um acréscimo à Lei de Execuções Penais, no qual seria feito um banco de dados daqueles que integram o sistema prisional, para manter um controle e identificação daqueles que já estiveram nas condições de detido em algum momento. Como consequência desse projeto se tem "a criação de um banco de dados de ex-detentos, sem que haja, entretanto, qualquer menção sobre o tratamento e o armazenamento desses dados" (De Castro, De Paula, 2022, p. 344).

Dessa maneira, entendemos que os dados analisados pela inteligência de reconhecimento facial são sensíveis e que, portanto, precisam ser tratados com demasiada cautela e especialidade. Tanto que o Conselho Nacional de Justiça compreende que "para o direito, essas inovações trazem desafios para a efetividade de normas e princípios que podem evitar a incidência de condutas que vão de encontro ao interesse coletivo, como a salvaguarda da igualdade de direitos, sem discriminação de raça, cor ou etnia" (CNJ, 2023, online). Ou seja, sem regulamentação específica em vigência, os avanços da tecnologia que poderia ser aprimorada, melhor estudada e adequadamente utilizada passam a apresentar sinais de possíveis avanços perigosos, contrários a diversas diretrizes que preconizam a segurança individual e coletiva dentro de uma sociedade democrática.

Em vista de tal importância, a União Europeia, em debates legais, estabeleceu a necessidade inclusive de determinação de principiologias acerca da temática, justamente por compreender que os algoritmos aplicados nessa tecnologia, uma vez que em contato com dados sensíveis, devem estar de acordo com o princípio da transparência, com possibilidade de rastreamento e verificação com avaliações periódicas analisando seu funcionamento e resultados. Ainda, o debate foi ampliado para as tecnologias em geral que se utilizam de

Inteligência Artificial (IA). Destacando-se a necessidade de regular auditoria desses sistemas de modo recorrente e impositivo (Steffen, 2023, p.117).

No entanto, ainda se trata de discussão com amplo ambiente de debate, uma vez que não basta identificar a principiologia, mas também "os momentos em que esses princípios devem ser implementados por regras jurídicas, bem como os instrumentos legais mais adequados para essa regulação" (Maranhão, Florêncio, Lasmar Almada, 2021, p. 162). Isso porque, por vezes, "o melhor caminho para discussões éticas que pretendam aplicabilidade seja por meio da análise "*bottom-up*", buscando equilíbrio reflexivo entre princípios gerais e casos concretos em setores específicos" (Maranhão, Florêncio, Lasmar Almada, 2021, p. 162). Nesse sentido, prever o que uma tecnologia emergente pode atingir em questões principiológicas e práticas depende das experiências empíricas, para então, poder ter a regulamentação, de modo a proteger os direitos civis individuais e, ao mesmo tempo, usufruir dos aspetos positivos e benéficos da novidade tecnológica (Francisco, Hurel, Rielli, 2020 apud Oliveira et al, 2022, p.126).

A União Europeia (UE), na tentativa de desenvolver regulamentação geral sobre o uso da IA em diversos setores da sociedade, tem desenvolvido o *AI Act*. A expectativa é que haja também delimitação da utilização de ferramentas como reconhecimento facial, em especial no uso da Administração Pública. Além disso, também será regulada a definição de grau de risco que a tecnologia utilizada aferirá, desde o risco mínimo ao inaceitável. Em paralelo, "no Brasil, ao menos quatro projetos de lei que procuram criar regras sobre o desenvolvimento, a implementação e o uso de sistemas de IA tramitam no Congresso Nacional e devem ser discutidos ainda em 2023" (Schmidt, 2023). De modo a espelhar o desponte europeu, o Brasil tem o PL 2.338 de 2023, o qual dispõe de similaridade à lei sendo desenvolvida pela UE, uma vez que também determina os níveis de risco que a tecnologia analisada dispõe. Ademais, "para evitar que o sistema de classificação fique engessado e possa acompanhar um ambiente tecnológico dinâmico, uma futura autoridade fiscalizadora, prevista no projeto, poderá reavaliar o risco de determinada aplicação" (Schmidt, 2023).

Ainda que com perspectivas de melhoramento e regulamentação, a atual ausência de regulação específica, as questões violadas pelo uso da tecnologia de reconhecimento facial permanecem atuando na realidade diária em vista de não existir controle sobre a utilização dessas ferramentas pelo Poder Público, gerando não só insegurança jurídica, mas violação de princípios básico constitucionais e processuais.

Sob esse viés, é preciso que esses serviços atuem de modo ético e respeitem diretrizes legislativas, mas também questões principiológicas e éticas (Amaral, 2023, p. 121-141). Uma das consequências diretas dessa inexistência, geradora de disparidades entre o Estado e indivíduos, é a ausência de transparência em sua atuação, principalmente na persecução criminal, no que tange as novas técnicas de vigilância e monitoramento implementadas (Oliveira et al, 2022, p.125). Sendo a transparência um princípio da Administração Pública predisposta pelo artigo 5º, inciso LX, artigo 216-A, inciso IX, artigo 37, §1º, artigo 225, inciso IV e artigo 93, IX, 1.ª parte, da Constituição Federal, além do artigo 792, *caput*, do Código de Processo Penal.

Ainda, destaca-se a Lei da Transparência de 2011 que visou regular a relação jurídica que o cidadão tem para com o direito à informação e de ser informado pelo Poder Público em sentido bem amplo. O princípio, também chamado de princípio da publicidade, é aquele que determina que a relação estatal deve estabelecer "transparência aos seus atos, reforçando, com isso, as garantias da independência, imparcialidade e responsabilidade do juiz. Além disso, consagra-se como uma garantia para o acusado, que, em público, estará menos suscetível a eventuais pressões, violências ou arbitrariedades" (Avena, 2023, p.23). Com relação à ligação que o princípio tem para com o reconhecimento facial, as questões concernentes à transparência são apontadas como: "(i) qual o banco de dados está sendo explorado pela polícia; (ii) o que o responsável pelo tratamento deve informar e registrar; e (iii) qual a necessidade de desenvolvimento de um relatório de impacto pelo uso da tecnologia de RF" (Almeida, 2022, p. 271).

Com base no que foi exposto anteriormente, é possível verificar que o banco de dados brasileiro se baseia especialmente na coleta de imagens proveniente do sistema dos estabelecimentos reunidos pelo CNJ em seu Banco Nacional de Monitoramento de Prisões e que são incluídos os presos sob prisão cautelar no banco de dados. A autora comentada afirma que se deve levar em consideração a Diretiva 2016/680 da UE para se comparar como o uso de dados poderiam ser lidados diante da efetivação do princípio da transparência. Para isso, seria preciso que fossem previstas avaliações da utilização da tecnologia que se apossa de dados sensíveis para seu funcionamento, com base em legislações vigentes que determinem a proteção de dados de modo periódico. Isso levando-se em conta, como determinou a diretiva e destacou Almeida (2022, p. 273):

i. os riscos para os direitos e para as liberdades dos titulares dos dados;

ii. as medidas previstas para fazer face a esses riscos;

iii. as garantias dos sujeitos previstas em lei;

iv. as medidas de segurança; e

v. os mecanismos para assegurar a proteção dos dados pessoais (art. 27º)

A análise de riscos desempenha um papel central na prestação de contas (*accountability)*, permitindo a avaliação de questões de justiça e direitos humanos. Os relatórios de impacto, como destaca Silva (2022, p.55), são ferramentas fundamentais para documentar a transparência, auxiliar reguladores e indivíduos, além de possibilitar o controle de qualidade e a análise de eficiência da tecnologia.

O princípio da finalidade, previsto pelo art. 4º, 1, b, da Diretiva 2016/680 da EU e, como define Almeida (2022, p. 269) "as finalidades de tratamento de dados pessoais autorizadas pela diretiva para se atingir a segurança pública são: prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública" tal como também prevê o art. 1º, nº 1 da mesma Diretiva. E, como destaca Melo (2020, p.20), o princípio determina a necessidade de informar de maneira clara e específica a finalidade para a qual os dados serão utilizados, visando proteger o titular dos dados, assegurando que suas informações não sejam usadas de forma incompatível com o propósito original. Esse princípio é especialmente relevante no contexto do compartilhamento de dados entre órgãos da Administração Pública, que deve ser feito de forma transparente e restrito à finalidade original da coleta, como previsto na LGPD (Silva, 2022, p.42). Essa delimitação de finalidade é importante no armazenamento dos dados uma vez que, consequentemente, guardar o *template* facial de alguém que cometeu um crime só faz sentido enquanto a pessoa está cumprindo a pena, depois disso não se torna útil e gera alto risco de uso indevido dos dados (Almeida, 2022, p. 271).

E ainda, levando-se em consideração a limitada visualização dos indivíduos presentes nos bancos de dados dispostos, já comentada, e a evidente seletividade daqueles que são direcionados o reconhecimento facial, a finalidade de segurança pública geral é substituída por uma busca de indivíduos que as autoridades policiais e Estado estão interessados em identificar e que são suscetíveis a enfrentar provável processo judicial diante do devido processo legal (Almeida, 2022, p. 270).

Destarte, também deve ser analisado o subprincípio constitucional da necessidade em vista do todo desta temática, que está englobado no princípio da proporcionalidade, nele,

"preza-se pela limitação do tratamento ao mínimo necessário para a realização de suas finalidades" (Gov.br, 2020, p. 14 apud Almeida, 2022, p. 271). Na lógica do subprincípio, aqueles dados que não estiverem de acordo com a finalidade do que o projeto se propõe, devem, necessariamente, ser excluídos, sendo essa também é uma das orientações presentes na Diretiva 2016/680. Dessa maneira:

> "compreende-se que manter o *template* do rosto de uma pessoa que cometeu crime só é relevante para fins de reconhecimento facial até o momento em que essa pessoa está cumprindo sanção penal, já que após esse período, armazenar o *template* não é mais útil ou necessário e o risco de vazamento, compartilhamento ou uso indevido do dado é alto" (Almeida, 2022, p. 271)

Portanto, a regulamentação e aplicação dos princípios da transparência, a restrição ao compartilhamento de dados e a adoção de medidas de segurança são medidas que contribuem para a preservação da privacidade e a mitigação de riscos, especialmente em um cenário de avanço tecnológico e coleta massiva de informações. A *accountability*, aliada à análise de riscos, desempenha um papel fundamental nesse contexto, promovendo a proteção dos direitos individuais e a segurança da sociedade como um todo. Já os princípios da finalidade, segurança e precaução são fundamentais para garantir a proteção dos dados pessoais em posse das entidades públicas.

## 5. **Conclusão**

Portanto, conclui-se que, ainda que com alta receptividade na Administração Pública, as tecnologias de reconhecimento facial, dentro do contexto de segurança pública, são complexas e, em vista da não regulamentação específica no legislativo brasileiro, acabam por ferir princípios constitucionais e processuais, tais como o da transparência, da finalidade, da necessidade, da segurança e da precaução.

A regulamentação é essencial para lidar com os desafios éticos e práticos apresentados pelo uso do reconhecimento facial. A ausência de regras claras expõe a sociedade a riscos, como o uso indevido de dados e a possibilidade de discriminação, principalmente considerando que o direito à imagem é um direito fundamental e inviolável. Por isso, é de tal importância a regulamentação de sua utilização, principalmente para garantir os direitos fundamentais dos indivíduos e, também, para combater a discriminação e os estereótipos que podem ser alimentados, a partir, do viés algoritmo. A Lei Geral de Proteção de Dados (LGPD) estabelece diretrizes importantes para a proteção de dados, mas a regulamentação específica do reconhecimento facial se faz necessária.

Ademais, foi possível observar o panorama em que se encontra o cenário brasileiro, com as diversas propostas de leis tanto no que tange a implementação das tecnologias, quanto nas normativas que regulamentem e limitem a atuação do Poder Público.

## 6. Referências bibliográficas

ALENCAR, I. Com mais de mil prisões na BA, sistema de reconhecimento facial é criticado por "racismo algorítmico"; inocente ficou preso por 26 dias. **G1**: Salvador, 1 set. 2023. Disponível em: < http://bit.ly/3Q8JUTG>. Acesso em: 29 out. 2023.

ALCÂNTARA, Manoela. Em um ano, STJ cassou 78 decisões baseadas em reconhecimento facial. **Metrópoles**. 2021. Disponível em: <https://bit.ly/49fUjpk>. Acesso em: 26 out. 2023.

ALMEIDA, Eduarda Costa. Os grandes irmãos: O uso de tecnologias de reconhecimento facial para persecução penal. **Revista brasileira de segurança pública.** São Paulo, v. 16, n. 2, 264-283, fev/mar de 2022. DOI: <https://doi.org/10.31060/rbsp.2022.v16.n2.1377>. Acesso em: 19 jun. 2023.

AMARAL, Ana Luiza Lacerda. Entre a utopia e a distopia tecnológica no direito – Análises e predições do sistema judiciário brasileiro. **Revista dos Tribunai**s. vol. 1050. ano 112. p. 121-141. São Paulo: Ed. RT, abril 2023. Acesso em: 29 jul. 2023.

ARTICLE 29. Parecer sobre algumas questões importantes da Diretiva relativa à proteção de dados na aplicação da lei (Diretiva [UE] 2016/680). **European Comission**: [S. l], 7 dez. 2017. Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610178. Acesso em: 5 maio 2023.

BAX, Sophia Gianturco. **A implementação e utilização dos sistemas de reconhecimento facial ("facial recognition technology") no Brasil: uma análise crítica no âmbito da segurança pública e da persecução penal**. 2023. 33-55 f. Trabalho de Conclusão de Curso – Faculdade de Direito do Centro Universitário Curitiba, Curitiba, 2023. Disponível em: <https://bit.ly/3se2iCY> Acesso em: 28 out. 2023.

BRAGADO, Louise. Algoritmos têm vieses, e primeiro passo é admitir este problema, defende a pesquisadora Meredith Broussard. **Época – Negócios**: São Paulo, 10 jul. 2023. Disponível em: < https://bit.ly/3QaK0KG>. Acesso em: 24 out. 2023.

CAMIMURA, Lenir. Direito precisa dar diretrizes para a produção e uso de reconhecimento facial sem distorções raciais. **Agência CNJ de Notícias**: Brasília, 16 ago. 2023. Disponível em:<https://bit.ly/3FDKbcK>. Acesso em: 29 out. 2023.

CAMARA, Geysa. **Do reconhecimento facial**. 2022. Tese (Mestrado em Direito e Segurança) - Nova School Of Law. Lisboa, 2021. Disponível em: http: //hdl.handle.net/10362/141162 Acesso em: 29 out. 2023.

CAMARA DOS DEPUTADOS. Projeto de Lei 2.392/2022. **Câmara dos Deputados**: Brasília, 2023. Disponível em: <https://bit.ly/46Pj1vm>. Acesso em: 29 out. 2023.

COSTA, R. S.; KREMER, B. Inteligência artificial e discriminação: desafios e perspectivas para a proteção de grupos vulneráveis frente às tecnologias de reconhecimento facial. **Revista Brasileira de Direitos Fundamentais & Justiça**, Porto Alegre, v. 16, n. 1, 2022. DOI: 10.30899/dfj.v16i1.1316. Disponível em: https://dfj.emnuvens.com.br/dfj/article/view/1316. Acesso em: 29 out. 2023.

CRIPPA, Margarete Esteves Nunes et al. Uso do reconhecimento facial aplicado à segurança pública no Brasil. **Controversias y Concurrencias Latinoamericanas**. v. 12, n. 22, p. 159-173, Abr.-Set. 2021. Disponível em: < https://ojs.sociologia-alas.org/index.php/CyC/article/view/248>. Acesso em: 20 out. 2023.

ARAÚJO, Romulo de Aguiar;, Naiara Deperon; PAULA, Amanda Marcélia de. Regulação e uso do reconhecimento facial na segurança pública do Brasil. **Revista de Doutrina Jurídica**, Brasília, DF, v. 112, n. 00, p. e021009, 2021. DOI: 10.22477/rdj.v112i00.734. Disponível em: <https://revistajuridica.tjdft.jus.br/index.php/rdj/article/view/734>. Acesso em: 30 out. 2023.

CASTRO, Kátia Shimizu de; PAULA, Luciana Veiga de. O reconhecimento biométrico facial e a utilização pelo Poder Público. **Revista de Direito Internacional e Globalização Econômica**, São Paulo, v. 9, n. 9, p. 339-354, 2022. Disponível em: <https://doi.org/10.23925/2526-6284/2022.v9n9.60092>. Acesso em: 25 out. 2023.

DUARTE, Renata et al. Aplicação dos Sistemas Biométricos de Reconhecimento Facial na Segurança Pública. **Brazilian Journal of Forensic Sciences, Medical Law and Bioethics**, *[S. l.]*, v. 11, n. 1, p. 1–21, 2021. Disponível em: <https://www.bjfs.org/bjfs/bjfs/article/view/848>. Acesso em: 30 oct. 2023.

GARCIA, Pedritta Marihá. CCJ retoma debate sobre tecnologia de reconhecimento facial. **Câmara municipal de Curitiba**: Curitiba, 4 set. 2023. Disponível em: <https://bit.ly/47aBke9. Acesso em: 25 out. 2023.

ESTADÃO CONTEÚDO. Estudo mostra que Brasil esclarece só 37% dos homicídios. **Mobilidade Estadão: Na perifa**: São Paulo, 3 ago. 2022. Disponível em: < https://bit.ly/40g4TZs>. Acesso em: 29 out. 2023.

JUNIOR, Ilberto da Silva. Reconhecimento facial como prova fundamental nos processos penais. In: Congresso internacional de direito e inteligência artificial, 2., 2021, Belo Horizonte, **Anais** [...]. Florianópolis: Conselho Nacional de Pesquisa e Pós-graduação em Direito (CONPEDI), 2021. Disponível em: < site.conpedi.org.br/publicacoes/b3vv7r7g/760jvn58>. Acesso em: 13 jun. 2023.

MAGNO, M. E. da S. P.; BEZERRA, J. S. Vigilância negra: O dispositivo de reconhecimento facial e a disciplinaridade dos corpos. **Novos Olhares**, São Paulo, v. 9, n. 2, p. 45-52, 2020. DOI: 10.11606/issn.2238-7714.no.2020.165698. Disponível em: https://www.revistas.usp.br/novosolhares/article/view/165698. Acesso em: 29 out. 2023.

MARANHÃO, Juliano Souza de Albuquerque, FLORÊNCIO, Juliana Abrusio, LASMAR ALMADA, Marco Antonio, Inteligência artificial aplicada ao direito e o direito da inteligência artificial, **Suprema: revista de estudos constitucionais**, 2021, Vol. 1, No. 1, pp. 154-180. Disponível em: <https://hdl.handle.net/1814/71840>. Acesso em: 24 out. 2023.

MELO, J. S. S.; NEVES, T. A.; SANTOS, L. E. SAREF: Sistema de Apresentação Remota por Reconhecimento Facial. **Revista CNJ, Brasília,** v. 6, n. 2, p. 77–92, 2022. Disponível em: <https://www.cnj.jus.br/ojs/revista-cnj/article/view/389>. Acesso em: 12 jun. 2023.

MELO, Paulo Victor; SERRA, Paulo. Tecnologia de Reconhecimento Facial e Segurança Pública nas Capitais Brasileiras: Apontamentos e Problematizações. **Comunicação e sociedade**, [S. l], n. 42, p. 205-220, 2022. Disponível em: <https://journals.openedition.org/cs/8111>. Acesso em: 25 out. 2023.

MELO, Pedro Raphael Vieira. **Reconhecimento facial automatizado para fins de segurança pública e seus riscos aos titulares dos dados biométricos**. 2020. 31 f. Trabalho de Conclusão de Curso (Graduação em Direito) – Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa, Brasília, 2022.

NIC.BR. [FIB13] #TireMeuRostoDaSuaMira: debate sobre banimento do reconhecimento facial na segurança pública.**Nic.br vídeos**: Belo horizonte, 2023. 1 vídeo (1 h., 38 min., 56s.). disponível em:< https://bit.ly/47a0jhD>. Acesso em: 25 ago. 2023.

OLIVEIRA, Loryne Viana et al. Aspectos ético-jurídicos e tecnológicos do emprego de reconhecimento facial na segurança pública no Brasil. **Revista Tecnologia e Sociedade**, Curitiba, v. 18, n. 50, p. 114-135, 2022. Disponível em: <https://periodicos.utfpr.edu.br/rts/article/view/12968>. Acesso em: 20 ago. 2023.

PARANÁ. Tecnologia de reconhecimento facial na chamada chega a 1,6 mil colégios da rede estadual. **Agência Estadual de Notícias**: Curitiba, 17 maio 2023. Disponível em: <https://bit.ly/3tSzNLq>. Acesso em: 25 out. 2023.

PARANÁ. PM utiliza **"**viatura inteligente" com quatro câmeras para identificar placas e pessoas. **Agência Estadual de Notícias**: Curitiba, 21 dez. 2022. Disponível em: < https://bit.ly/40fQOv3>. Acesso em: 25 out. 2023.

PEREIRA, Débora Freitas Mendes. O uso de câmeras de reconhecimento facial em contexto de pós democracia– uma ferramenta contra o inimigo no direito penal. **ADPEB**, Salvador, v. 28, p. 12, 2022. Disponível em: <https://bit.ly/40gsCJ6>. Acesso em 28 out. 2023**.**

PIRES, Ana Beatriz Santos; et al. Alvos Predeterminados: Um estudo de caso sobre a implementação da tecnologia de reconhecimento facial na Bahia, p. 18-59, 2022 In: ALMEIDA, Eloísa Machado de et al. **Dados, privacidade e persecução penal: cinco estudos**. 2022. Disponível em: <https://bibliotecadigital.fgv.br/dspace/handle/10438/31784>. Acesso em: 29 out. 2023.

RIBEIRO, Zeca. Projeto condiciona uso de reconhecimento facial a inviabilidade de outros meios de identificação. **Agência Câmara de Notícias**: Brasília, 6 out. 2022. Disponível em: <https://bit.ly/3QifMoZ>. Acesso em: 29 out. 2023.

SANTOS, Jéssica Guedes. Reconhecimento facial: entre a criminologia, a mídia e a LGPD penal. **Revista Internetlab**, v. 2, n. 1, jun. 2021, p. 214-232. Disponível em: <https://bit.ly/3QgMiYH>. Acesso em: 24 out. 2023.

SCHMIDT, Sarah. Os desafios para regulamentar o uso da inteligência artificial. **Nexo Jornal**: São Paulo, 09 set. 2023. Disponível em: <https://bit.ly/47egc6Z>. Acesso em: 29 out. 2023.

SILVA, João Paulo Terra; CLEMENTE, Leticia Rodrigues. O uso de algoritmos de reconhecimento facial como auxiliar na segurança pública. *In*: Congresso internacional de direito e inteligência artificial, 2., 2021, Belo Horizonte, **Anais** [...]. Florianópolis: Conselho Nacional de Pesquisa e Pós-graduação em Direito (CONPEDI), 2021. Disponível em: <site.conpedi.org.br/publicacoes/b3vv7r7g/760jvn58>. Acesso em: 13 jun. 2023.

SILVA, Maria Luiza Sousa. **As tecnologias de reconhecimento facial para Segurança Pública no Brasil: perspectivas regulatórias e a garantia de Direitos Fundamentais**. 2022. 87f. Monografia (Graduação em Direito) - Centro de Ciências Sociais Aplicadas, Universidade Federal do Rio Grande do Norte, Natal, 2022.

SILVA, Rosane Leal da; Fernanda dos Santos Rodrigues da. Reconhecimento facial e segurança pública: os perigos do uso da tecnologia no sistema penal seletivo brasileiro SILVA,. In: **Congresso Internacional de Direito e Contemporaneidade**, Santa Maria, Anais [...], 2019. Disponível em: <https://bit.ly/46MhsOT>. Acesso em: 15 jul. 2023.

SILBERG, Jake; MANYIKA, James. Como lidar com vieses na inteligência artificial (e nos seres humanos). **McKinsey & Company**: [S. l], 6 jun. 2019. Disponível em: <https://bit.ly/3Mj5zra>. Acesso em: 24 out. 2023.

SOARES, Everson Rangel. **Reconhecimento facial e política criminal: da segurança pública às garantias fundamentais**. 2020. Trabalho de Conclusão de Curso (Graduação em Direito) – Antonio Meneghetti Faculdade, Restinga Sêca, RS, 2020.

SOUSA, Bruno. Panóptico: reconhecimento facial renova velhas táticas racistas de encarceramento. **Rede de observatórios da segurança**: São Paulo, 22 abr. 2021. Disponível em: <https://bit.ly/40eCwLo>. Acesso em 29 out. 2023.

STEFFEN, Catiane. A Inteligência Artificial e o Processo Penal: A Utilização da Técnica na violação de Direitos. **Revista EMERJ**, Rio de Janeiro, v. 25, n. 1, p. 105-129, Jan.-Abr. 2023. Disponível em: < https://ojs.emerj.com.br/index.php/revistadaemerj/arti>. Acesso em: 08 maio 2023.

TONETTI, Igor. LATAM passa a utilizar reconhecimento facial na recuperação de conta. **Passageiro de primeira**, São Paulo, 30 jan. 2023. Disponível em: <https://bit.ly/3QLvL0B>. Acesso em: 26 out. 2023.

UNIÃO EUROPEIA. Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. **Jornal Oficial da União Europeia**, 4 maio 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L0680&from=EN. Acesso em: 6 maio 2023.

VIEIRA, Leonardo Marques. A problemática da inteligência artificial e dos vieses algorítmicos: caso COMPAS. In: Brazilian Technology Symposium, 2019. Disponível em: <https://bit.ly/45KQLZq>. Acesso em: 24 out. 2023.

WALL, M. Inteligência Artificial: Por que as tecnologias de reconhecimento facial são tão contestadas. **BBC News Brasil**, 5 jul. 2019. Disponível em: https://www.bbc.com/portuguese/geral-48889883 Acesso em: 29 out. 2023.