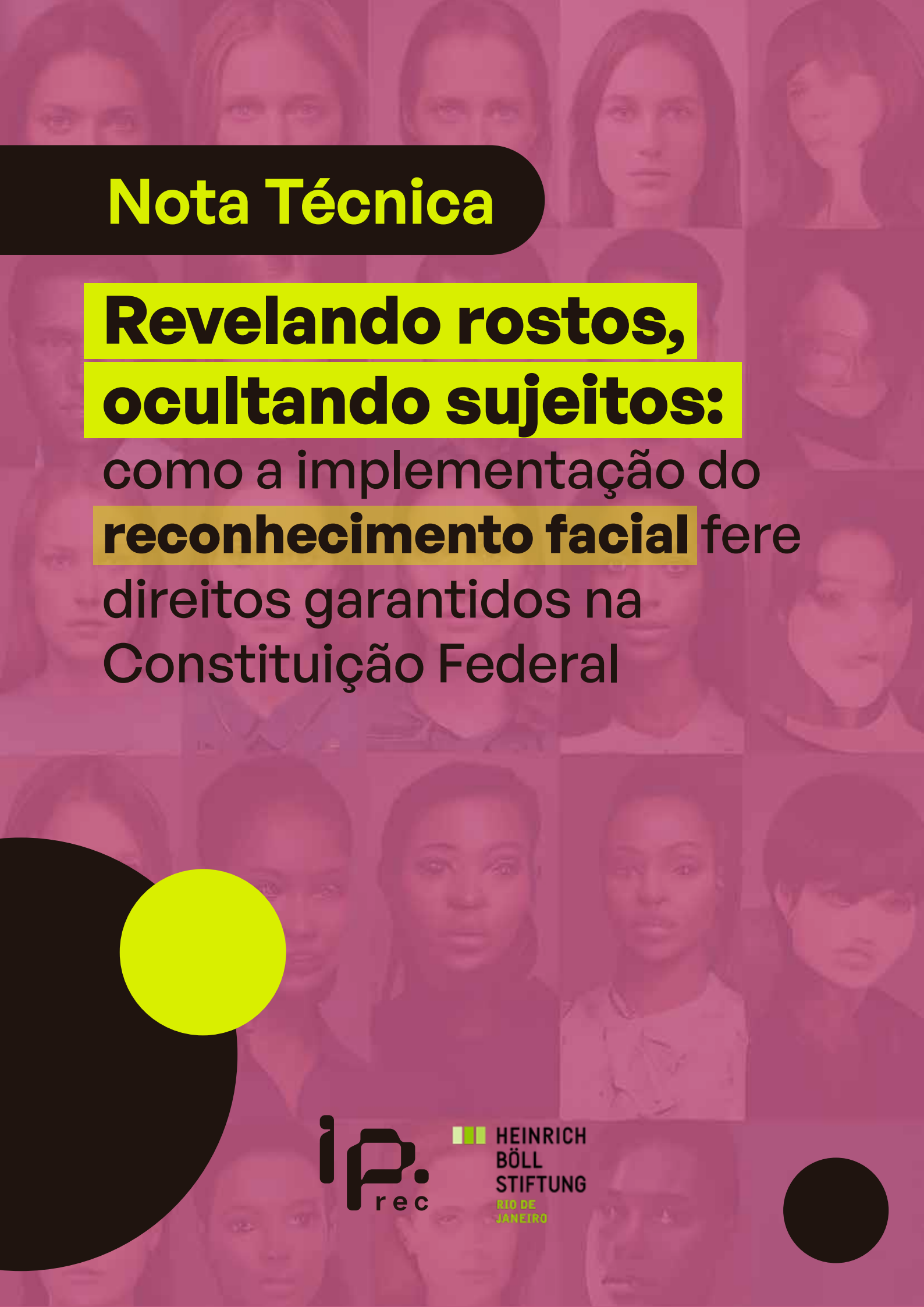

Nota Técnica

Revelando rostos, ocultando sujeitos:

como a implementação do **reconhecimento facial** fere direitos garantidos na Constituição Federal

ip.rec

HEINRICH BÖLL STIFTUNG RIO DE JANEIRO

Ficha Técnica

Realização:

Instituto de Pesquisa em Direito e Tecnologia do Recife - IP.Rec

Financiamento:

Heinrich-Böll-Stiftung - Brasil

Pesquisa e texto:

André Lucas Fernandes
Carolina Branco
Clarissa Mendes
Lunara Santana

Coordenador do Projeto:

André Lucas Fernandes

Revisão de conteúdo:

André Lucas Fernandes
Clarissa Mendes
Raquel Lima Saraiva

Projeto Gráfico:

Maria Clara Guimarães

INTRODUÇÃO

A aplicação de ferramentas de reconhecimento facial se tornou presente no cotidiano dos cidadãos brasileiros. Desde ferramentas para desbloquear celulares, acesso a serviços públicos e utilização na segurança pública, os mecanismos técnicos por trás de seu funcionamento por muitas vezes permanecem ocultos. Igualmente, na gana pela solução de problemas complexos, as implicações legais de sua utilização acabam por ser negligenciadas. Dessa forma, a presente nota técnica visa oferecer uma introdução ao debate da utilização de reconhecimento facial, em seu âmbito técnico, jurídico, aplicabilidade na administração pública, assim como exemplificar movimentos que advogam por seu banimento.

ASPECTOS TÉCNICOS DO RECONHECIMENTO FACIAL

Existem diversas definições de sistemas de reconhecimento facial, seu funcionamento e suas aplicações, principalmente dos últimos anos até os dias atuais. No entanto, ao observarmos as características centrais compartilhadas pela maioria dessas definições, podemos dizer que "reconhecimento facial" é uma área dentro da **visão computacional**, que faz parte da **inteligência artificial** (IA), e cujos sistemas são usados para **verificar** ou **identificar** uma pessoa e/ou fazer **predições** a partir do reconhecimento de um ou mais rostos utilizando **dados biométricos** em imagens captadas por sensores e processadas por um **modelo**. É importante ressaltar também que reconhecimento facial é diferente de **detecção facial**, que objetiva apenas detectar se há ou não um rosto em dada imagem.

Principais conceitos apresentados nesta nota

Inteligência Artificial (IA): Encontrar uma definição única para IA é um desafio, autores diferentes trazem definições diferentes, mas em geral elas versam sobre a mimetização de capacidades cognitivas humanas pelas máquinas. Duas das principais abordagens da IA são a **simbólica,** baseada em inferências dedutivas sob regras lógicas, e **a estatística**, ou aprendizagem de máquina, que se baseia no conhecimento indutivo, capturando padrões e correlações em um dado conjunto de dados.

Visão Computacional: Área da inteligência artificial voltada a utilizar imagens, vídeos e sinais de sensores imagéticos para emular a capacidade de visão humana, realizando tarefas como reconhecer e detectar objetos, facilitar interação de sistemas com humanos e permitir a mobilidade e atuação de robôs.

Verificação e **Identificação**: Dentro do reconhecimento facial, um processo de verificação tem por objetivo saber se um rosto capturado por uma câmera e um outro rosto específico armazenado no sistema são ou não da mesma pessoa. Diferentemente,

no caso da identificação, essa imagem capturada de um rosto é comparada com um conjunto de outras imagens, contidas em um banco de dados, a fim de se descobrir se a pessoa da imagem coletada é ou não uma das pessoas registradas no banco.

Análise Preditiva: Trata-se de utilizar dados passados para se identificar um padrão que possa ou não ocorrer no presente ou futuro próximo. No contexto do reconhecimento facial, isso envolve tarefas como identificar que emoções uma pessoa está sentindo naquele momento ou diagnosticar, via imagem, doenças ou predisposições a doenças.

Dado Biométrico: Dado coletado de uma pessoa que advém de uma característica física/biológica dela e que a identifiquem de forma individual, como o rosto, a impressão digital, a íris, o DNA, etc. Segundo a Lei Geral de Proteção de Dados (LGPD), esse tipo de dado está categorizado como dado pessoal sensível. É importante ressaltar que a ideia de autenticação baseada em biometria parte do pressuposto que esses dados são imutáveis ou tenham características imutáveis. No entanto, alguns desses dados não contêm essa característica, como mais facilmente o rosto e até a impressão digital.

Modelo de IA: Programa que foi treinado a partir de dados, utilizando alguma estratégia estatística/algorítmica para detecção de padrões e correlações (como redes neurais, florestas randômicas, máquinas de vetores de suporte, etc) e que tenha sido validado, ajustado e testado com um conjunto de dados desconhecido.

Assim como qualquer modelo de inteligência artificial (ou, pelo que costuma acontecer, modelo de aprendizagem de máquina), os sistemas de reconhecimento facial possuem uma grande dependência de dados para que eles possam ser **treinados** (ou seja, construídos) e **testados** (ou seja, avaliados) e para que, quando em seu uso final, sejam generalizados o suficiente para funcionar com novos rostos.

Essa dependência torna esses modelos **enviesados** para os conjuntos de dados usados em seu desenvolvimento e causa, caso a coleta, análise e pré-processamento não sejam feitas com cuidado e rigor, riscos e prejuízos, principalmente para grupos minoritários e marginalizados na sociedade, como mulheres, pessoas negras e pessoas LGBTQIA+. Dessa forma, o modelo passa a emular e reforçar problemas sociais sérios como, por exemplo, racismo, misoginia e transfobia.

Para além desses problemas, existem outros obstáculos técnicos que tornam o uso de sistemas de reconhecimento facial ainda mais arriscado. Esses modelos, em sua grande maioria, apresentam uma alta **opacidade** e baixa **interpretabilidade** e **transparência**. Isso significa que, apesar de identificar padrões, os resultados desses sistemas não têm um **porquê** entendível para fins de auditabilidade ou justificativa.

Não é possível saber (salvo se forem usadas técnicas e ferramentas que geralmente são postas de lado por tornarem o modelo menos eficiente e mais custoso em tempo de processamento) que **atributos** e que **correlações** o sistema está usando como base para calcular o resultado, e isso se torna ainda mais crítico quando essas tecnologias são utilizadas para **tomar decisões** em vez de apenas dar suporte a uma decisão tomada, ou, no mínimo, **supervisionada**, por um ser humano.

Principais obstáculos técnicos

- Dependência de dados para treinamento e teste dos sistemas, que correm o r**isco de serem enviesados, especialmente para grupos minoritários**;
- **Alta opacidade; baixa interpretabilidade e transparência**, especialmente nos casos em que, ao invés de suporte a decisões supervisionadas, há tomada de decisões;
- Apesar de identificar padrões e correlações, ainda é um desafio atribuir explicações causais que sirvam de base para que os dados encontrados, por si, sejam considerados evidências suficientes para políticas públicas.

IMPACTOS JURÍDICOS DO RECONHECIMENTO FACIAL

O avanço do reconhecimento facial tem despertado discussões acerca das implicações significativas que essa tecnologia pode ter na vida das pessoas. À medida que o uso desses sistemas se expande, surgem preocupações relacionadas a privacidade, liberdades individuais, discriminação e segurança. Neste contexto, é essencial analisar cuidadosamente como essa ferramenta pode afetar direitos fundamentais e princípios jurídicos estabelecidos, buscando um equilíbrio entre a inovação tecnológica e a proteção dos valores essenciais da sociedade.

Esses são alguns dos principais direitos que são afetados de forma significativa:

Privacidade: O direito à privacidade, previsto pelo Art. 5º, inciso X, da Constituição Federal, é historicamente ligado à proteção da propriedade e ao direito de não ser importunado[1], assegurando que cada pessoa tenha o controle sobre suas informações pessoais, atividades e relações, protegendo-as de interferências indevidas por parte de governos, empresas ou outros indivíduos[2]. O direito à privacidade na Convenção Americana sobre Direitos Humanos (OEA)[3], da qual o Brasil é signatário, é associado ao Art. 11º, 1, que dispõe que ninguém pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada. A coleta e o processamento massivo de dados biométricos sem o consentimento adequado comprometem a esfera privada dos cidadãos, expondo-os a uma vigilância constante e invasiva. O monitoramento e a identificação de indivíduos sem critérios claros e regulamentações específicas criam um cenário permissivo de práticas desproporcionais e preocupantes. Mesmo em manifestações e espaços públicos, o uso dessa tecnologia pode capturar dados sensíveis sem a devida autorização, violando a privacidade das pessoas.

Proteção de Dados Pessoais: O direito à proteção de dados pessoais é um direito fundamental assegurado pelo inciso LXXIX, Art. 5º da Constituição, que visa salvaguardar informações pessoais contra uso indevido ou abusivo. O reconhecimento facial pode ferir esse direito ao coletar, processar e armazenar dados biométricos sem consentimento do titular dos dados. Ademais, o tratamento inadequado dos dados biométricos coletados por esse tipo de ferramenta pode resultar em vulnerabilidades de segurança, como acesso não autorizado ou uso indevido dessas informações.

Intimidade: O direito à intimidade é um dos pilares fundamentais de proteção dos direitos individuais no ordenamento jurídico brasileiro, e é abrangido pelo Art. 5º, inciso X, da Carta Magna. Esse direito também é assegurado pela Convenção

[1] (MELO, 2022)
[2] (TJDFT, 2023)
[3] Disponível em: https://www.cidh.oas.org/basicos/portugues/c.convencao_americana.htm.

Americana sobre Direitos Humanos, no Art. 11º, 1. Historicamente ligado ao livre desenvolvimento da personalidade[4], esse direito assegura que cada indivíduo tenha o resguardo de sua vida privada, segredos, sentimentos e hábitos, sem ser exposto a interferências invasivas[5]. O uso indiscriminado do reconhecimento facial, sem a devida proteção da privacidade e consentimento informado, pode comprometer a esfera íntima das pessoas, inibindo sua liberdade de ação e comportamento em espaços públicos e criando um ambiente de vigilância constante que ameaça o livre desenvolvimento de suas personalidades.

Honra e imagem: O direito fundamental à honra e à imagem, presente no Art. 5º, inciso X, da Constituição Federal, garante a proteção da reputação e da imagem de uma pessoa, resguardando-a de possíveis violações que possam prejudicar sua reputação na sociedade. A Constituição Federal estabelece essa proteção, garantindo que a imagem de um indivíduo não seja captada e divulgada sem seu consentimento[6]. A coleta massiva de imagens biométricas pode resultar em capturas e divulgações não autorizadas de suas imagens. A utilização dessa tecnologia em espaços públicos, nos quais as pessoas têm uma expectativa razoável de privacidade, pode permitir a captação e o armazenamento de imagens sem o conhecimento, dando oportunidade ao registro inadvertido de situações que podem comprometer a reputação e a imagem das pessoas envolvidas.

Segurança: O Art. 5º e 6º da Constituição Federal preveem o direito fundamental à segurança, sendo o direito que o homem tem de ser protegido pela lei e pela sociedade quanto à vida, à liberdade, à propriedade, à saúde, à reputação e aos seus[7]. Embora o uso da tecnologia de reconhecimento facial seja muitas vezes apresentado equivocadamente como uma ferramenta para aprimorar a segurança pública e prevenir crimes, há riscos significativos a direitos fundamentais nessa aplicação. Uma vigilância constante e invasiva leva ao monitoramento em massa das atividades das pessoas sem critérios claros e sem transparência, gerando uma sensação de vulnerabilidade e ameaça à segurança dos indivíduos, uma vez que suas ações e movimentos são constantemente observados. Isso tudo pode levar a um cenário em que o próprio Estado, responsável pelo uso desse mecanismo, se torne um potencial violador da segurança dos cidadãos.

Igualdade: O direito fundamental à igualdade está presente no Art. 5º da Carta Magna, e assegura que todas as pessoas sejam tratadas de forma justa e igual perante a lei, sem discriminação de qualquer natureza.[8] Estudos mostram que a tecnologia de reconhecimento facial é menos eficaz para detectar os rostos de pessoas negras e pardas

[4] (MELO, 2022)
[5] (TJDFT, 2023)
[6] (TJDFT, 2023)
[7] (PIMENTA BUENO, 1978 apud ROMÃO, 2020)
[8] (MORAES, 2016)

em comparação com pessoas brancas, e também apresenta problemas para identificar mulheres em relação a homens[9]. Sem mencionar que o sistema muitas vezes se baseia em visões binárias de gênero, o que pode levar a erros ao identificar pessoas transgênero. Essa disparidade na eficácia da tecnologia pode contribuir para práticas discriminatórias no policiamento preditivo e ranqueamento social, por exemplo, impactando determinados grupos de forma desigual. Além disso, a discriminação algorítmica pode reforçar e perpetuar estereótipos existentes, aumentando a marginalização de grupos vulneráveis e minoritários.

Liberdade de expressão: O direito à liberdade de expressão, estabelecido pelo inciso IV, Art. 5º, da Constituição Federal, é um dos alicerces principais de uma sociedade democrática, assegurando que as pessoas possam manifestar suas opiniões, ideias e pensamentos livremente, sem censura ou repressão.[10] A utilização de sistemas de reconhecimento facial em espaços públicos e locais de trabalho pode gerar um ambiente de vigilância constante, onde as pessoas se sentem observadas e coagidas a se autocensurar por medo de serem monitoradas, o que vem sendo referido na literatura como *chilling effect,* ou efeito inibitório. Essa inibição à liberdade de expressão pode ser especialmente preocupante em contextos de protestos e manifestações, onde indivíduos podem temer consequências negativas ou represálias ao expressarem suas opiniões divergentes ou críticas ao governo, por exemplo. Além disso, a tecnologia pode ser utilizada para identificar e monitorar dissidentes e ativistas, tornando ainda mais difícil o exercício pleno da liberdade de expressão, o que se torna especialmente perigoso em governos autoritários.

Reunião e Manifestação: Consagrado no artigo 5º, inciso XVI, da nossa Constituição, esse direito permite que as pessoas se reúnam para discutir ideias, expressar opiniões, protestar contra injustiças, reivindicar direitos e promover mudanças sociais.[11] O uso de reconhecimento facial em espaços públicos, que muitas vezes são palco de protestos e manifestações, cria um ambiente de vigilância constante, em que os participantes podem se sentir intimidados e coagidos, o que pode levar à autocensura e à redução da participação em eventos públicos. Ademais, essa tecnologia pode ser usada pelas autoridades para identificar e monitorar indivíduos presentes em protestos, o que pode resultar em práticas autoritárias e violações do direito à privacidade, além de existir a possibilidade de levar à criminalização indevida de protestos legítimos e ao enfraquecimento do direito à livre manifestação.

Informação: Assegurado pelo inciso XIV, Art 5º da Carta Magna, o direito à informação busca garantir que as pessoas tenham acesso a informações relevantes e

[9] (MAGNO; BEZERRA, 2020)
[10] (TJDFT, 2021)
[11] (BRASIL, 1988)

transparentes sobre assuntos que afetam suas vidas e o funcionamento do Estado.[12] A tecnologia de reconhecimento facial faz com que uma quantidade massiva de dados biométricos sejam coletados e isso pode ocorrer sem o conhecimento e o consentimento adequado das pessoas, o que levanta preocupações em relação à transparência e ao acesso às informações sobre como seus dados estão sendo coletados, usados e armazenados. Isso pode gerar uma falta de transparência em relação aos dados coletados e dificultar o exercício do direito ao habeas data, um instrumento processual garantido pela CF, presente no seu Art. 5º, inciso LXXII - que assegura às pessoas o acesso a informações e dados que estejam sendo armazenados sobre elas, sejam eles em bancos de dados governamentais ou privados[13] -, já que as pessoas podem não estar cientes de que suas informações estão sendo mantidas em sistemas de vigilância. A falta de divulgação de informações relevantes sobre o uso dessa ferramenta pode limitar a capacidade das pessoas de compreenderem como suas informações pessoais estão sendo tratadas e quais os impactos disso em suas vidas. O exercício do direito à informação também sofre influência da ausência de propriedades de explicabilidade, interpretabilidade e transparência nos sistemas de identificação biométrica, pois não será possível solicitar informações sobre como os sistemas operam e quais as diretrizes e parâmetros de utilização.

Principais direitos fundamentais afetados

- **Privacidade -** o risco se apresenta na medida em que o reconhecimento facial se baseia num mapeamento dos rostos sem o consentimento adequado, sem critérios claros e regulamentações específicas;
- **Proteção de dados pessoais -** na medida em que a coleta, processamento e armazenamento forem feitos sem os consentimentos dos titulares; além disso, o tratamento inadequado dos dados pode acarretar em vulnerabilidades de segurança;
- **Intimidade -** sem a devida proteção da privacidade e consentimento informado, o RF pode comprometer a esfera íntima das pessoas, inibindo a liberdade de ação e comportamento em espaços públicos e criando um ambiente de vigilância;
- **Honra e Imagem -** Na medida em que podem ocorrer capturas inadvertidas e sem autorização, há o risco de ocorrência de registros que comprometam a reputação e a imagem das pessoas;
- **Segurança -** por se basear em vigilância constante e invasiva e levar ao monitoramento em massa das atividades dos cidadãos sem critérios claros e sem transparência;
- **Igualdade -** por conta dos riscos de discriminação algorítmica e da disparidade na eficácia da tecnologia, especialmente para rostos de pessoas negras, pessoas não-binárias e mulheres;
- **Liberdade de expressão -** ao manter vigilância constante, pode-se criar um efeito inibitório,

[12] (SARLET; MOLINARO, 2014)
[13] (SARLET; MOLINARO, 2014)

em que as pessoas se sentem observadas e coagidas à autocensura, especialmente em protestos e manifestações; há também possibilidade de identificação e monitoramento de dissidentes e ativistas;

- **Reunião e Manifestação** - na medida em que é utilizado em espaços públicos, que muitas vezes são palco de protestos e manifestações, os indivíduos podem se sentir intimidados e coagidos. Há possibilidade do monitoramento levar à criminalização e a práticas autoritárias;

- **Informação** - na falta de transparência, explicabilidade e interpretabilidade dos dados coletados, as pessoas podem não estar cientes de que suas informações estão sendo mantidas em sistemas de vigilância, de como é feito o tratamento de tais informações e dos impactos disso em suas vidas.

Além dos direitos fundamentais mencionados anteriormente, alguns **princípios fundamentais** são diretamente afetados pelo uso dessa tecnologia:

Proporcionalidade: O princípio da proporcionalidade estabelece que as ações tomadas devem ser proporcionais ao objetivo buscado e não devem ser excessivas ou desnecessárias.[14] Na utilização de reconhecimento facial, isso significa que o uso dessa tecnologia deve ser proporcional aos fins legítimos pretendidos. Portanto, usar esse mecanismo indiscriminadamente em espaços públicos sem uma justificativa sólida e sem critérios adequados de seleção pode ser considerado desproporcional e uma violação da privacidade das pessoas.

Minimização de Dados: O princípio da minimização de dados, conferido pela Lei Geral de Proteção de Dados Pessoais, estabelece que apenas os dados necessários para atingir a finalidade específica devem ser coletados e processados. Isso significa que a quantidade de dados coletados deve ser a mínima possível para alcançar o objetivo pretendido, evitando a coleta excessiva de informações pessoais.[15] Se não houver leis claras que estabeleçam limites na coleta, uso e retenção de dados, bem como penalidades para seu mau uso, as organizações podem coletar mais informações do que o necessário, com finalidades duvidosas ou desconhecidas.

Acesso à justiça: O acesso à justiça é um princípio fundamental assegurado a todos os cidadãos, que consiste em proporcionar a todos, sem qualquer restrição, o direito de pleitear a tutela jurisdicional do Estado e de ter à disposição o meio constitucionalmente previsto para alcançar esse resultado, e está previsto pelo art. 5°, XXXV, da Constituição Federal.[16] A falta de transparência e das propriedades de explicação e interpretação das decisões tomadas pelo sistema, além da ausência de uma regulação

[14] (MARQUES, 2010)
[15] (BUCHAIN, 2022)
[16] (BEDAQUE, 1994 *apud* RUIZ, 2021)

adequada no contexto das tecnologias de reconhecimento facial, pode dificultar o acesso a informações sobre como esses dados são coletados e utilizados, prejudicando a possibilidade de identificar violações e buscar reparação. Não obstante, o uso inadequado dessa ferramenta pode resultar em casos de identificações errôneas e detenções injustas, o que pode ter um impacto devastador na vida das pessoas afetadas, e, por consequência, a falta de mecanismos efetivos para contestar e corrigir esses erros pode prejudicar o acesso à justiça e dificultar a reparação para as vítimas.

Devido Processo Legal: O princípio do devido processo legal, estabelecido pelo artigo 5º, inciso LIV, da Constituição Federal, é um dos pilares do ordenamento jurídico brasileiro e garante que nenhuma pessoa será privada de seus direitos ou sofrerá punições sem que seja assegurado um processo justo, com respeito às garantias fundamentais e ao devido procedimento legal.[17] No contexto do reconhecimento facial, esse princípio pode ser afetado quando essa tecnologia é utilizada como meio de identificação e tomada de decisões sem a devida transparência e controle. Casos em que a identificação é realizada de forma indiscriminada e sem critérios bem definidos podem resultar em consequências graves para os indivíduos, como a detenção ou acusação injusta de uma pessoa inocente. A falta de clareza sobre como os sistemas operam e como são utilizados pode tornar o processo opaco e dificultar o acesso das pessoas aos meios de contestação e defesa. Dessa forma, o uso inadequado do reconhecimento facial, especialmente em sistemas de vigilância em massa, pode levar a uma inversão do ônus da prova, onde a pessoa monitorada precisa provar sua inocência em vez de o Estado provar sua culpa, o que é uma violação clara do princípio do devido processo legal.

Presunção de Inocência: A presunção de inocência, garantido pelo artigo 5º, inciso LVII, da Carta Magna, é um princípio jurídico fundamental que garante que toda pessoa seja considerada inocente até que sua culpa seja comprovada por meio de um processo justo e imparcial.[18] Na conjuntura do reconhecimento facial, esse direito pode ser afetado quando a ferramenta é utilizada para fins de investigação e segurança pública. Tal tecnologia pode levar a casos de "falsos positivos", ou seja, identificações errôneas de indivíduos como suspeitos de crimes, mesmo que sejam inocentes. Esses erros podem ocorrer devido a falhas no algoritmo, à má qualidade das imagens ou a outros fatores. Como resultado, pessoas inocentes podem ser injustamente acusadas, o que viola a presunção de inocência. Também é importante notar que o uso indiscriminado desse mecanismo em investigações pode levar a uma "reversão da presunção de inocência", onde todas as pessoas são tratadas como suspeitas em potencial. Esse tratamento generalizado pode prejudicar a reputação e a dignidade das pessoas, sem que

[17] (MENEZES LIMA, 2007)
[18] (TJDFT, 2023)

haja qualquer evidência ou motivo legítimo para suspeitar delas, apenas em virtude da sua imagem ou aparência.

Desenvolvimento da Personalidade: É um princípio fundamental que reconhece a importância de cada indivíduo buscar seu crescimento pessoal, educacional, cultural e profissional de acordo com suas aspirações e interesses.[19] Ele está explicitado pelo Art. 22 da Declaração Universal dos Direitos Humanos, e faz parte do sistema jurídico brasileiro, sendo reconhecido como direito fundamental atípico a partir do art. 5º, §2 da Constituição.[20] A utilização indiscriminada de sistemas de reconhecimento facial pode limitar o desenvolvimento pessoal ao criar um estado de hipervigilância, onde as pessoas se sentem constantemente monitoradas e inibidas em suas ações e escolhas. Esse ambiente de vigilância constante pode levar as pessoas a restringirem suas atividades, a fim de evitar qualquer forma de identificação ou rastreamento. Não obstante, a falta de transparência sobre como os dados biométricos são coletados, armazenados e utilizados por essa tecnologia pode dificultar a confiança das pessoas em utilizar serviços ou participar de atividades que a envolvam. O medo de ter suas informações pessoais comprometidas ou utilizadas de forma inadequada pode afetar negativamente o desejo de buscar novas oportunidades de desenvolvimento.

Dignidade da Pessoa Humana: A dignidade da pessoa humana, consagrada no art. 1º, III, da nossa Constituição Federal, é um princípio fundamental do ordenamento jurídico brasileiro e é considerado um dos valores supremos da sociedade. Esse princípio garante que todas as pessoas devem ser tratadas com respeito e consideração, reconhecendo sua individualidade, autonomia e liberdade.[21] Ao serem tratadas como objetos de análises automatizadas, as pessoas têm sua individualidade reduzida a dados biométricos e emoções que são coletados e processados sem o devido consentimento. Ademais, o uso do reconhecimento facial pode categorizar e rotular as pessoas com base em características superficiais, como aparência ou expressões faciais, o que pode levar a estereótipos e preconceitos. Isso pode resultar em tratamentos discriminatórios e desumanizadores, violando a dignidade das pessoas afetadas.

[19] (MOREIRA, 2015)
[20] (MOREIRA, 2015)
[21] (ANDRADE, 2008)

Princípios afetados	
Proporcionalidade	O uso da tecnologia deve ser justificado e proporcional aos fins legítimos pretendidos, sendo considerado desproporcional seu uso indiscriminado em espaços públicos sem critérios adequados de seleção.
Minimização de dados	Se não houver leis claras que estabeleçam limites na coleta, uso e retenção de dados, bem como penalidades para seu mau uso, as organizações podem coletar mais informações do que o necessário, com finalidades duvidosas ou desconhecidas.
Acesso à justiça	A dificuldade no acesso a informações sobre coleta e uso dos dados prejudica a identificação de violações e a busca por reparação. Além disso, a possibilidade de identificações errôneas e detenções injustas podem ter um impacto devastador. A falta de mecanismos efetivos para contestar e corrigir esses erros pode prejudicar o acesso à justiça
Devido processo legal	O uso inadequado do RF, especialmente para fins de segurança, pode levar a uma inversão indevida do ônus da prova, onde a pessoa monitorada precisa provar sua inocência em vez de o Estado provar sua culpa. Além disso, a falta de transparência e de critérios bem definidos pode dificultar o acesso a meios de contestação e defesa.
Presunção de inocência	Quando usado para fins de vigilância, o RF trata todas as pessoas como suspeitas em potencial, revertendo a presunção de inocência. Além disso, há a possibilidade de "falsos positivos", identificações errôneas que podem ocorrer devido a falhas no algoritmo, à má qualidade das imagens ou a outros fatores.
Desenvolvimento da personalidade	A criação de um estado de hipervigilância pode inibir ações e escolhas, limitando o desenvolvimento pessoal, e a falta de transparência dificulta a confiança em utilizar serviços relacionados às tecnologias.
Dignidade da pessoa humana	A análise automatizada pode rotular as pessoas com base em características superficiais, reforçando estereótipos e preconceitos, e sujeitando-as a tratamentos discriminatórios e desumanizadores.

RECONHECIMENTO FACIAL NA ADMINISTRAÇÃO PÚBLICA

A adoção de mecanismos de reconhecimento facial na Administração Pública está ligada, anteriormente, aos desafios da adoção de modelos de inteligência artificial em geral. Ao menos duas dimensões precisam ser analisadas, de forma cruzada, para entender os desafios e oportunidades de implementação destes modelos: o aspecto legal-regulatório e o aspecto técnico.

O aspecto legal-regulatório

Além dos impactos jurídicos e principiológicos citados na seção anterior, a adoção de inteligência artificial na administração pública deve ser lida a partir das regras jurídicas específicas a serem aplicadas no setor, que está limitado ao princípio da legalidade estrita. Os princípios (ou regras) da legalidade, impessoalidade, moralidade, publicidade e eficiência estão postos, expressamente, no artigo 37 da Constituição Federal e servem como baliza geral para a atuação pública no Brasil.

Ademais, a adoção de mecanismos de reconhecimento facial, atrelados a políticas públicas, passa por um necessário diálogo de fontes, entre normas específicas de regência, como a Lei Geral de Proteção de Dados e regramentos futuros acerca da Inteligência Artificial.

Nota-se, com base nos relatos recentes sobre iniciativas envolvendo a adoção destes sistemas em projetos relacionados à segurança pública, controle de acesso em prédios públicos e outros, uma constante e elevado risco de desrespeito ao cumprimento de diretrizes de publicidade, legalidade e eficiência, condizente com o regime constitucional.

Ao menos três razões merecem ser destacadas:

(1) os modelos adotados são implementados com a **promessa de aumento de uma eficiência** em específico, mas eles, tecnicamente, **não garantem essa promessa** (há mais propaganda do que entrega efetiva dos produtos envolvendo estes modelos de inteligência artificial);

(2) a **adoção de modelos em políticas públicas não vem sendo acompanhada dos devidos processos de escuta e participação pública significativas**, resultando em decisões de "portas fechadas";

(3) a **ausência de diálogo com as regras e princípios** do ordenamento jurídico brasileiro é caso específico de **ofensa à legalidade** estrita (formal) e material. Desta irregularidade central, podem advir consequências no campo da responsabilização do ente público ou da anulação da regra aprovada em âmbito estadual ou federal, em virtude de inconstitucionalidade por arrastamento ou inconstitucionalidade direta perante a Constituição Federal (art. 5º, inciso LXXIX).

O debate global sobre reconhecimento facial tem avançado, com o mapeamento dos usos diversos pelo Poder Público de outro países: de acordo com o escritório de conformidade do governo americano (GAO)[22], as agências daquele país têm manejado esta tecnologia para controle de acesso ou segurança de dispositivos móveis, uso em investigações criminais, controle massivo de presença de pessoas em ambientes públicos, pesquisa e controle migratório.

De acordo com a Agência Reguladora do Reino Unido (ICO)[23], a adoção dessa tecnologia deve vir acompanhada de salvaguardas e testes de segurança, com alto nível de responsabilização caso o compliance não seja efetivamente adotado. Medidas como o Relatório de Impacto de Proteção de Dados (DPIA, em inglês), com minucioso registro da justificativa e uso legítimo pelo Poder Público (controlador de dados), benefícios e consequências para os cidadãos, consulta prévia à população, mecanismos de controle da necessidade de proporcionalidade, identificação prévia de riscos, medidas de mitigação de danos entre outros. Na França, a autoridade francesa (CNIL) aconselhou o governo a não implementar reconhecimento facial em espaços públicos, sob a justificativa de gerenciar a segurança nos Jogos Olímpicos de 2024[24].

Esses elementos servem para, em diálogo direto com o contexto da Lei Geral de Proteção de Dados no Brasil, mostrar que ainda quando se busca implementar esse tipo de sistema de inteligência artificial (modelo de reconhecimento facial/biométrico), o conjunto de ações prévias para o compliance com a lei são vastos e as possibilidades de responsabilização pelo tratamento indevido de dados também.

O aspecto técnico implementação na administração pública

Existem também tensões técnicas a serem tratadas como desafios na implementação destes sistemas. É importante destacar os elementos técnicos, pois eles são a base para confirmar ou não que o tratamento de dados se deu em conformidade com a legislação. A ausência das balizas técnicas pode ocasionar a insuficiência de provar que o

[22] (ESTADOS UNIDOS DA AMÉRICA, 2021)
[23] (REINO UNIDO, 2021)
[24] (POLITICO, 2023)

tratamento é legítimo e a criação de um cenário de processos administrativos, perante a Autoridade Nacional de Proteção de Dados, ou perante o Poder Judiciário.

Alguns pontos merecem destaque nos desafios, como as relações entre: **explicabilidade** x **beneficiência/maleficência** x **justiça**; **automação pelo modelo** x **beneficência/maleficência** x **justiça**.

Estas relações podem ser endereçadas com algumas perguntas centrais, nas quais os princípios legais ganham concretude. Ao responder as questões principais de um relatório de impacto, é possível mapear as necessárias medidas de mitigação de risco ou, eventualmente, a necessidade de abandono e modificação da política pública planejada.

1. **Identificar o processamento em toda a sua extensão.** Os dados a serem processados foram identificados? Quais dados pessoais serão processados no contexto do projeto? Quem são os responsáveis pelo processamento desses dados?
2. **Avaliar o cumprimento entre Necessidade e Proporcionalidade**. O processamento de dados é necessário para atingir os objetivos propostos? O escopo do processamento é proporcional aos objetivos pretendidos?
3. **Mapear os riscos.** Quais são os possíveis riscos para os direitos e liberdades dos indivíduos? Existem vulnerabilidades no sistema que podem comprometer a segurança dos dados?
4. **Mitigar os riscos mapeados.** Quais medidas podem ser implementadas para minimizar os riscos identificados? Como garantir a segurança e a privacidade dos dados durante o processamento?
5. **Criar meios de participação pública significativa.** Como as preocupações das partes interessadas, incluindo os titulares dos dados, serão consideradas? Existe um processo de consulta eficaz para obter feedback sobre o processamento de dados?
6. **Analisar o Impacto na Privacidade.** Qual é o impacto potencial do processamento de dados na privacidade dos indivíduos? Como esse impacto pode ser minimizado ou mitigado?
7. **Documentar todo o processo de construção da política.** Todas as conclusões e medidas de mitigação foram documentadas adequadamente? O relatório foi apresentado e aprovado pela autoridade competente (ANPD)?
8. **Monitorar de forma contínua.** Como será realizado o monitoramento contínuo do processamento de dados? Existem mecanismos para ajustar as práticas em resposta a novos riscos ou mudanças no contexto?

RECONHECIMENTO FACIAL EM CAMPANHAS NACIONAIS E INTERNACIONAIS

Campanhas Nacionais

❖ Tire o Meu Rosto da Sua Mira[25] - O projeto é uma iniciativa da Coalizão Direitos na Rede e busca trazer mais clareza sobre os problemas que o reconhecimento facial traz para a segurança pública. Durante o Fórum da Internet no Brasil, foi lançado um site onde é possível assinar uma carta cujo objetivo é o banimento total das tecnologias digitais de Reconhecimento Facial na Segurança Pública brasileira, além de um mapeamento de projetos de lei sobre o tema nos estados brasileiros.

❖ Sai da Minha Cara[26] - A iniciativa, capitaneada pelo MediaLab.UFRJ, Coding Rights, O Panóptico e Idec, é um "protocolaço". As organizações realizaram um trabalho de *advocacy* com parlamentares do poder legislativo do país inteiro para que eles e elas protocolassem, ao mesmo tempo, projetos de lei – tanto nas câmaras municipais quanto nas assembleias legislativas – pelo banimento do reconhecimento facial. Mais de 50 parlamentares, de diversos partidos diferentes, demonstraram apoio e protocolaram projetos. A articulação continua, agora centrada na tramitação e aprovação destes projetos.

❖ Sem Câmera na Minha Cara[27] - A articulação é uma resposta às 108 câmeras de reconhecimento facial que estão sendo implementadas pela Prefeitura de Recife. A rede Meu Recife se juntou às organizações IP.Rec, Rede de Justiça Criminal, Rede Lavits, Articulação Negra de Pernambuco, OAB Pernambuco, Centro Popular de Direitos Humanos e Natrape e lançaram a campanha, que já enviou mais de 700 e-mails ao prefeito João Campos para barrar a instalação.

Campanhas internacionais

❖ Con Mi Cara No (Argentina)[28] - A a entidade argentina *Asociación por Derechos Civiles* (ADC) lançou a campanha #ConMiCaraNo sobre as fragilidades das tecnologias de reconhecimento facial para as liberdade individuais no espaço público, promovendo um debate a respeito do avanço da vigilância e do controle da população de Buenos Aires. Após se juntar com outras entidades da sociedade civil, em setembro de 2022, a

[25] Endereço: https://tiremeurostodasuamira.org.br/
[26] Endereço: https://www.instagram.com/p/CfEdOLkrTAD/
[27] Endereço: https://www.semcameranaminhacara.meurecife.org.br/
[28] Endereço: https://conmicarano.adc.org.ar/

Justiça de Buenos Aires declarou inconstitucional o sistema que vinha sendo aplicado na cidade[29].

❖ No Los Vean La Cara (México)[30] - O governo de Coahuila, no México, implementou um sistema de vigilância com reconhecimento facial. Diante do contexto de repressão e hostilidade ao direito de protesto que persiste no país, o sistema implicaria em uma nova forma de assédio e inibição desse direito. A campanha, portanto, defende o seu banimento em todo o país.

❖ Al Sur (América Latina)[31] - A pesquisa realizada pelo *Consorcio Al sur* visa traçar um panorama geral da implantação das tecnologias de reconhecimento facial na América Latina, seus usos e provedores, caracterizados até agora por uma opacidade excessiva e pouca discussão pública.

❖ Access Now - Ban Biometric Surveillance[32] - Campanha global, composta por membros de mais de 20 países em seis continentes. Mais de 200 organizações da sociedade civil, ativistas, tecnólogos e outros especialistas em todo o mundo já assinaram a carta aberta pedindo aos tomadores de decisão que se oponham ao uso abusivo de direitos das tecnologias de vigilância biométrica.

❖ Ban Facial Recognition (Estados Unidos)[33] - A campanha reúne mais de 40 organizações e defende um projeto de lei pelo banimento do reconhecimento facial, o *Facial Recognition and Biometric Technology Moratorium Act of 2020*. Entre suas atividades, realiza um mapeamento de iniciativas envolvendo reconhecimento facial em todo o país, além de esforços locais e estaduais para contê-la, montando um placar de congressistas que atuam a favor e contra essas implementações.

❖ Reclaim Your Face (Europa)[34] - Trata-se de uma iniciativa da sociedade civil para a proibição de práticas de vigilância biométrica em massa. A campanha apela à Comissão Europeia para que regule rigorosamente a utilização de tecnologias biométricas para evitar interferências indevidas nos direitos fundamentais.

❖ Big Brother Watch (Reino Unido)[35] - É um grupo de campanha por liberdades civis do Reino Unido, tendo como foco de atuação a garantia de privacidade em meio às mudanças tecnológicas, buscando reverter o estado de vigilância. Suas atividades se concentram no desenvolvimento de investigações e campanhas públicas, promovendo

[29] Mais informações sobre o caso em: https://frenteacano.com.ar/la-justicia-portena-declaro-inconstitucional-el-sistema-de-reconocimiento-facial/. Visitado em 11 de agosto de 2023.
[30] Endereço: https://nonosveanlacara.r3d.mx/
[31] Endereço: https://estudio.reconocimientofacial.info/
[32] Endereço: https://www.accessnow.org/ban-biometric-surveillance/
[33] Endereço: https://www.banfacialrecognition.com/
[34] Endereço: https://reclaimyourface.eu/
[35] Endereço: https://bigbrotherwatch.org.uk/

informação e capacitando o público. A campanha contra o reconhecimento facial é uma entre várias associadas ao tema.

❖ Ban the Scan (Nova York, Estados Unidos)[36] - Campanha desenvolvida pela Anistia Internacional em parceria com organizações de privacidade, liberdades civis e direitos humanos sediadas na cidade de Nova York, pedindo a proibição do uso governamental de tecnologias de reconhecimento facial.

[36] Endereço: https://banthescan.amnesty.org/

REFERÊNCIAS BIBLIOGRÁFICAS

ANDRADE, André Gustavo Corrêa de. **O princípio fundamental da dignidade humana e sua concretização judicial.** Banco do Conhecimento, 18 de agosto de 2008. Disponível em: http://www.tjrj.jus.br/c/document_library/get_file?uuid=5005d7e7-eb21-4fbb-bc4d-12affde2dbbe. Acesso em: 7 ago. 2023.

BRASIL. **Constituição da República Federativa do Brasil**. Promulgada em 5 de outubro de 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 4 ago. 2023.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais.** Diário Oficial da União, Brasília, 15 ago. 2018.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. **Marco Civil da Internet.** Diário Oficial da União, Brasília, 24 abr. 2014.

ESTADOS UNIDOS DA AMÉRICA. GAO. FACIAL RECOGNITION TECHNOLOGY - Current and Planned Uses by Federal Agencies, 2021. Disponível em: https://www.gao.gov/products/gao-21-526. Acesso em: 4 ago. 2023.

MAGNO, Madja Elayne da Silva Penha; BEZERRA, Josenildo Soares. **Vigilância negra: O dispositivo de reconhecimento facial e a disciplinaridade dos corpos.** Novos Olhares, v. 9, n. 2, jul.-dez. 2020. Disponível em: https://www.revistas.usp.br/novosolhares/article/view/165698. Acesso em: 3 ago. 2023.

MARQUES, Andréa Neves Gonzaga. **Princípio da Proporcionalidade e seus fundamentos**. Tribunal de Justiça do Distrito Federal e Territórios (TJDFT). Publicado em: 2010. Disponível em: https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/artigos-discursos-e-entrevistas/artigos/2010/principio-da-proporcionalidade-e-seus-fundamentos-andrea-neves-gonzaga-marques. Acesso em: 3 ago. 2023.

MELO, Rafael. **Os limites do direito à privacidade e sua extensão: diferença de privacidade e intimidade.** Publicado por Jusbrasil em 06/01/2022. Disponível em: https://www.jusbrasil.com.br/artigos/os-limites-do-direito-a-privacidade-e-sua-extensao-diferenca-de-privacidade-e-intimidade/1347835992. Acesso em: 7 ago. 2023.

MENEZES LIMA, I. (2007). **O Devido Processo Legal e Seus Principais Corolários: Contraditório e ampla defesa.** Revista Brasileira De Estudos Políticos, 96, 161-190. https://doi.org/10.9732/38. Acesso em: 4 ago. 2023.

MORAES, Vânila Cardoso André de. **A igualdade - formal e material - nas demandas repetitivas sobre direitos sociais.** Série Monografias do CEJ, vol. 24, p. 23-48, 2016. Disponível em: https://www.cjf.jus.br/cjf/corregedoria-da-justica-federal/centro-de-estudos-judiciarios-1/publicacoes-1/monografias-do-cej2/volume-24-2013-2016/@@download/arquivo. Acesso em: 2 ago. 2023.

MOREIRA, R. P. (2015). **Direito ao livre desenvolvimento da personalidade: caminhos para a proteção e promoção da pessoa humana**. (Dissertação de Mestrado). Universidade Federal de Uberlândia, Programa de Pós-Graduação em Direito.

POLITICO. **French privacy chief warns against using facial recognition for 2024 Olympics**, 2023. Disponível em: https://www.politico.eu/article/french-privacy-chief-warns-against-using-facial-recognition-for-2024-olympics/. Acesso em: 4 ago. 2023.

ROMÃO, L. F. F. **A segurança pública na Constituição de 1988: direito fundamental, dever do Estado e responsabilidade de todos**. Revista do Ministério Público do Estado do Rio de Janeiro, v. 75, n. 75, jan./mar. 2020. Disponível em: https://www.mprj.mp.br/documents/20184/1606558/Luis_Fernando_de_Franca_Romao.pdf. Acesso em: 11 ago. 2023.

RUIZ, Ivan Aparecido. **Princípio do acesso à justiça.** Enciclopédia Jurídica PUC-SP, Tomo Processo Civil, Edição 2, Julho de 2021. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/201/edicao-2/principio-do-acesso-justica. Acesso em: 7 ago. 2023.

SARLET, Ingo Wolfgang; MOLINARO, Carlos Alberto. **Direito à Informação e Direito de Acesso à Informação como Direitos Fundamentais na Constituição Brasileira.** Revista da Advocacia-Geral da União (AGU), Brasília-DF, ano XIII, n. 42, p. 09-38, out./dez. 2014. Disponível em: https://repositorio.pucrs.br/dspace/bitstream/10923/11403/2/Direito_a_768_Informac_807_a_771_o_e_Direito_de_Acesso_a_768_Informac_807_a_771_o_como_Direitos_Fundamentais_na.pdf. Acesso em: 4 ago. 2023.

TJDFT - Tribunal de Justiça do Distrito Federal e Territórios. **Jurisprudência em temas: Direito Constitucional - Direitos de Personalidade: Intimidade, Privacidade, Honra, Imagem e Liberdade de Expressão.** Publicado em: 2023. Disponível em: https://www.tjdft.jus.br/consultas/jurisprudencia/jurisprudencia-em-temas/direito-constitucional/direitos_de_personalidade_intimidade_privacidade_honra_imagem_e_liberdade_de_expressao. Acesso em: 1 ago. 2023.

TJDFT - Tribunal de Justiça do Distrito Federal e Territórios. **Liberdade de Imprensa X Liberdade de Expressão.** Publicado em: 2021. Disponível em: https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/direito-facil/edicao-semanal/liberdade-de-imprensa-x-liberdade-de-expressao. Acesso em: 4 ago. 2023.

TJDFT - Tribunal de Justiça do Distrito Federal e Territórios. **Princípio da Presunção da Inocência.** Publicado em: 2023. Disponível em: https://www.tjdft.jus.br/consultas/jurisprudencia/jurisprudencia-em-temas/direito-constitucional/principio-da-presuncao-da-inocencia. Acesso em: 7 ago. 2023.

ip.rec

HEINRICH BÖLL STIFTUNG
RIO DE JANEIRO