REDE DE ENSINO DOCTUM
CURSO DE DIREITO
UNIDADE DE MANHUAÇU

Adriano José Pereira
Ana Lívia Oliveira de Freitas
Deivid Sebastian Souza Dornelas

O USO DE TECNOLOGIAS DE RECONHECIMENTO FACIAL E SEGURANÇA PÚBLICA: intertextualidade entre a criminologia e direitos constitucionais de proteção de dados

Manhuaçu/MG
2024

REDE DE ENSINO DOCTUM
CURSO DE DIREITO
UNIDADE DE MANHUAÇU

Adriano José Pereira
Ana Lívia Oliveira de Freitas
Deivid Sebastian Souza Dornelas

O USO DE TECNOLOGIAS DE RECONHECIMENTO FACIAL E SEGURANÇA PÚBLICA: intertextualidade entre a criminologia e direitos constitucionais de proteção de dados

Trabalho de Conclusão apresentado ao como requisito parcial para a obtenção do título de Bacharel em Direito.Curso de Direito da Rede de Ensino Doctum, Unidade de Manhuaçu/MG,

Professor(a) supervisor(a): Soraya Cezar Sanglard Costa

Manhuaçu/MG
2024

Adriano José Pereira

Ana Lívia Oliveira de Freitas

Deivid Sebastian Souza Dornelas

O USO DE TECNOLOGIAS DE RECONHECIMENTO FACIAL E SEGURANÇA PÚBLICA: intertextualidade entre a criminologia e direitos constitucionais de proteção de dados

Trabalho de Conclusão apresentado ao como requisito parcial para a obtenção do título de Bacharel em Direito.Curso de Direito da Rede de Ensino Doctum, Unidade de Manhuaçu/MG,

Aprovado em ___/___ / 2024.

BANCA EXAMINADORA

Soraya Cezar Sanglard Costa

Professor(a) Supervisor(a)

Examinador(a)

Examinador(a)

RESUMO

O presente artigo pretende contribuir para a construção de um debate acerca da legitimidade da inserção das tecnologias de reconhecimento facial na Segurança Pública, para combater a criminalidade e seus reflexos na esfera dos direitos fundamentais, transpassando pelo controle estatal, proteção de dados e a necessidade regulamentação legislativa, tendo em vista Emenda Constitucional 115/2022 e a Lei 13.709/2018. Nesse sentido, partindo do conceito de panóptico de Bentham, a vigilância estabelece como um mecanismo de controle estatal, que com os avanços tecnológicos de reconhecimento facial e monitoramento de dados em um mundo digital ampliou seu alcance. Entretanto, essa nova tecnologia, que usa inteligência artificial, apresenta vieses antigos de preconceito racial, reforçando a problemática em torno de sua implementação. No Brasil, ao lado da ausência de regulamento específico sobre o tema, há um presente crescimento das TRF's, com mais de 195 projetos, espalhado por todos os estados da Federação, segundo a Agência Brasil (2024). Diante disso, abrir o debate sobre o uso das TRF's possibilita uma melhor análise acerca da regulamentação no setor público eficiência ou eventual banimento.

Palavras chaves: reconhecimento facial; proteção de dados; vigilância; segurança pública.

SUMÁRIO

1 INTRODUÇÃO **6**

2 DO PANÓPTICO AO MONITORAMENTO FACIAL **9**

2.1 Vigilância entre a Distopia e a Realidade 9

2.2 Conceituação e análise no âmbito do direito comparado. 13

3 DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS E À PRIVACIDADE **16**

3.1 Velhos problemas, novas abordagens 16

4 SEGURANÇA PÚBLICA **20**

4.1 Regulamentação de medidas de policiamento 20

5 CONSIDERAÇÕES FINAIS **23**

REFERÊNCIAS BIBLIOGRÁFICAS **25**

1 INTRODUÇÃO

Estamos imersos em um novo mundo de tecnologias digitais, este artigo, provavelmente, está sendo lido através de um aparelho digital e foi escrito por meio de um. O impacto de novas tecnologias na sociedade é ineludível, não se restringindo a certas áreas da vida privada do cidadão, mas ressignificando toda noção da sociedade e do Estado Democrático de Direito.

Como mais atual expoente dessa nova era, o uso de tecnologias de reconhecimento facial (TRFs) por inteligência artificial (IA) no setor de Segurança Pública assume o centro da discussão acerca das transformações no Estado e na indústria, pela incorporação de mecanismos de monitoramento biométrico e controle de dados. Por trás da aparente melhora da prestação de serviços e informatização, há um universo ainda obscuro sobre a efetividade e consequências dessas tecnologias de monitoramento, como aprofundamento da desigualdade social, perda da privacidade e instauração de mecanismos de controle permanentes (Duarte; Ceia, 2022).

A crescente busca por sistemas de segurança de reconhecimento facial fez esse mercado global sair de 4,35 bilhões de dólares em 2019 para uma estimativa de 12,97 bilhões de dólares em 2027, isso representa um aumento de 297%, segundo dados relatório da empresa de pesquisa e inteligência Fortune Business Insights (2019). O constante avanço do uso dessas técnicas no Brasil, com mais de 195 projetos ativos em todos os estados da federação, segundo a Agência Brasil (2024), mas ainda sem regulamentação, aumenta a preocupação acerca do tema. Isto porque, não há transparência nos tratamentos dos dados coletados ou sobre a efetividade dessas medidas, que custam caro aos cofres públicos. Não muito além, os direitos constitucionais de proteção de dados e privacidade continuam sendo potencialmente violados.

Segundo Duarte e Ceia (2023), a necessidade de identificação dos indivíduos por meio do reconhecimento de características faciais não surgiu com as TRFs, mas remonta do século XIX com as técnicas médicas de Alphonse Bertillon e os retratos compostos de tipos criminosos de Francis Galton, afirmam, contudo, que foi a partir desta década que as TRFs, como o uso de "*redes neurais convolucionai*s", usando o conceito do professor David Leslie, se difundiram. O sistema de monitoramento funciona a partir da captura da imagem do rosto, que será subordinada a um algoritmo especializado em identificar pontos e características faciais únicas, como a distância entre os elementos do nosso rosto (nariz, boca, olhos etc.), o formato do rosto, traços e cicatrizes, cor de pele, cabelo, sobrancelhas. Esses aspectos são

armazenados em um banco de dados e montados como um quebra cabeça por meio de cálculos.

Nesta noção mais integralizada e digital, a ideia de uma “sociedade em rede” proposta pelo sociólogo espanhol Manuel Castells (2005), propõe como um prisma analítico para entender a atual estrutura social. Para Castells (2005), a interconexão global da virada do século XX para o XXI alterou a forma organizacional de poder, influenciando enfraquecimento dos estados nacionais e estruturação de novas formas de organização social, assim “nossas sociedades estão cada vez mais estruturadas em uma oposição bipolar entre a Rede e o Ser", (Castells, 2005, p. 41). Nesse sentido, essa nova forma organizacional condiciona o capitalismo de vigilância e novas formas de monitoramento estatal.

Desse modo, este estudo pretende contribuir para a construção de um debate acerca da legitimidade da inserção dessas novas medidas na Segurança Pública, para combater a criminalidade e seus reflexos na esfera dos direitos fundamentais, transpassando pelo controle estatal, proteção de dados e a necessidade regulamentação legislativa, tendo em vista Emenda Constitucional 115/2022 e a Lei 13.709/2018. Para tanto, utilizou-se de revisional bibliográfico sobre o tema, bem como sobre questões tangentes ao assunto, na tentativa de abordar questões pertinentes para essa que aponta ser uma das principais problemáticas do setor de Segurança Pública no Brasil e no mundo.

Nesse sentido, sem o objetivo de esgotar o tema, foram abordados em um primeiro os conceitos filosóficos que permeiam a vigilância e o poder, valendo-se da contribuição do filósofo Jeremy Bentham, que propôs o “panóptico”, uma espécie de modelo ideal para se adotar em prisões, hospícios e até mesmo em escolas, passando por Foucault, que analisa o mesmo objeto como instrumento disciplinar que projeta a vigilância no indivíduo e, ao mesmo tempo, cria uma relação de autodomínio ético nas relações de poder. Contribuindo ainda para o tema, em “The electronic eye: The rise of surveillance society”, David Lyon (1994), analisa a vigilância a partir de um panóptico eletrônico ou “olho eletrônico”, na qual emerge-se uma nova noção de vigilância, onipresente e voluntária.

Ato contínuo, foram abordadas como outros países têm lidado com essa nova tecnologia. Em um terceiro momento buscou-se estabelecer um paralelo com o Direito Constitucional de proteção aos dados e à privacidade, bem como o papel da Lei de Proteção aos Dados nesses cenários. Por fim, o trabalho debruçou-se na ausência de regulamentação dessas TRF’s e seu uso indiscriminado e avulso pelo setor público de segurança.

Dentro desse escopo, evidenciou-se que a vigilância sempre foi uma ferramenta de poder do Estado, justificada pela busca pela segurança do bem comum. Entretanto, dentro do

Estado Democrático de Direito, essas questões ganham novos contornos com o uso das tecnologias de reconhecimento facial. Isto porque, essas novas tecnologias parecem ser o caminho natural desta "sociedade em rede", encontram-se com direitos fundamentais, que são a principal costura do estado democrático. Diante disso, a criação de normas que regulamentem de forma clara e efetiva essa implementação, abordando desde que a forma de funcionamento, à transparência sobre a efetividade, tratamento de dados, bem como estudos e consultas públicas para verificar aplicabilidades das TRF's no contexto brasileiro, parece o ponto de vista mais inequivocamente reconhecido.

2 DO PANÓPTICO AO MONITORAMENTO FACIAL

2.1 Vigilância entre a Distopia e a Realidade

A discussão sobre a vigilância, direitos e regimes políticos não é apenas da filosofia ou da sociologia, permeando enredos de obras de ficções científicas. Um exemplo a ser mencionado é a distópica série Black Mirror em sua primeira temporada (2011), que trata em diversos episódios como as tecnologias têm controlado a vida das pessoas através da vigilância. Outra ficção que aborda essa temática é a obra de George Orwell intitulada 1984, em que a sociedade de Londres é constantemente vigiada por uma entidade denominada "Big Brother". Os habitantes da civilização da fictícia Oceânia não sabem quando estão ou não sendo vigiados, conforme o seguinte trecho "você era obrigado a viver - e vivia, em decorrência do hábito transformado em instinto - acreditando que todo som que fizesse seria ouvido e, se a escuridão não fosse completa, todo movimento examinado meticulosamente" (Orwell, 2009, p. 51).

Na ficção a vigilância se dava através das "teletelas" que captavam tudo o que estava ao seu redor. Para ter um maior alcance, esse aparelho era instalado em todos os lugares públicos e até mesmo dentro das casas. Ademais, como forma de controle e alienação, havia cartazes por toda a cidade com o seguinte a frase: "O Grande Irmão está de olho em você". O regime totalitário vivido por essa sociedade fazia uma inversão de valores ao afirmar que "Guerra é paz", "Liberdade é escravidão" e "Ignorância é força".

Semelhante ao totalitarismo imaginado por Orwell, o livro Admirável mundo novo de Aldous Huxley (2014), apresenta uma sociedade completamente modificada, na qual todos os seres humanos são criados em laboratórios e alienados durante toda a infância para amarem e obedecerem ao estilo de vida que os espera. Nessa civilização a vigilância não ocorre por meio de câmeras ou aparelhos, mas sim através da docilização de seus próprios corpos. Os indivíduos se encontram tão dominados e inseridos no sistema que quando uma outra pessoa começava a pensar diferente e a questionar aquele modo de vida, os mais inseridos reportavam essas condutas aos superiores ou estimulam seus companheiros a tomarem uma droga chamada "soma".

Essa substância era capaz de inibir esses questionamentos e, principalmente, a tristeza, proporcionando felicidade instantânea ao indivíduo. Quando a droga não conseguia "consertar" o indivíduo, ele era enviado para outra civilização, o que para muitos seria uma espécie de castigo. Para além disso, havia um intenso controle dos dados, já que os

fundadores dessa civilização apagaram ao máximo todos os vestígios das sociedades passadas, como livros e fatos históricos.

Embora pareça obra de ficção, a redução generalizada da privacidade e a vigilância em larga escala da população é uma realidade possível e processualmente desenvolvida em vários países. Os avanços tecnológicos podem ser usados como ferramentas de controle e docilização dos corpos, legitimados pela suposta manutenção da segurança e pelos interesses econômicos do grande mercado financeiro.o

Nessa senda, a vigilância para além das ficções vem sendo justificada a partir da ideia de construção e manutenção da segurança das pessoas e dos locais. Em virtude disso, o filósofo Jeremy Bentham propôs o "panóptico", que seria um modelo ideal para se adotar em prisões, hospícios e até mesmo em escolas, analisado por Michel Foucault na obra "vigiar e punir". O projeto de Bentham sugere a construção de um edifício circular, no qual as celas dos prisioneiros estariam lado a lado, impedindo a comunicação entre eles. Por conseguinte, bem ao meio haveria uma construção para os vigilantes, que pela localização poderiam observar todas celas, inclusive o interior de cada uma. Conforme a descrição, as janelas, que chamou de "alojamento do inspetor", deveriam ter venezianas, porque dessa forma, os prisioneiros não conseguiriam saber quantos funcionários estariam os observando. Pela incerteza se estariam ou não sendo vigiados, os encarcerados não desviariam suas condutas, portanto, esse seria um dos principais objetivos do modelo proposto por Bentham: a interiorização da dúvida e, consequentemente, da autovigilância (Foucault, 1999).

A partir disso, com a teoria do filósofo francês Michel Foucault, afirma Candiotto (2012) que o pensamento pós-moderno experimenta uma transformação quanto a visão analítica do poder e suas atribuições entre Estado e sociedade: sob uma nova ótica, Foucault defende que o poder não é um objeto atribuído a um grupo ou instituição, mas um conjunto estratégico de ações plurais em situações complexas no âmbito da sociedade, manifestando assim, o real sentido do poder "[...]O poder se exerce em rede e, nessa rede, não só os indivíduos circulam, mas estão sempre em posição de serem submetidos a esse poder e também de exercê-lo." (Foucault, 1997, p. 26 *apud* Candiotto, 2012, p. 97) .

Dessa forma, o poder deve ser entendido como produto deslocado de um eixo fixo da estrutura monárquica situada no século XVII (Candiotto, 2012). Na lógica foucaultiana, a operacionalidade do poder intrínseca nas relações humanas, foi instrumentalizada na modernidade a partir de uma técnica que massifica os indivíduos a um padrão, recodificando-os a um quadro disciplinar. O conceito de panóptico de Bentham é analisado

por Foucault como instrumento disciplinar que projeta a vigilância no indivíduo e, ao mesmo tempo, cria uma relação de autodomínio ético nas relações de poder (Foucault, 1999).

A sociedade disciplinar aqui avaliada se assenta na ênfase punitiva da alma do indivíduo, transferindo os suplícios corporais para uma nova forma correcional de vigilância e controle. Nesta lógica, outras áreas passam a atuar com métodos de doutrinação, valendo-se de "punições panópticas" – engendrando o que Foucault denomina como "corpos dóceis". Com isso, o disciplinamento aconteceria na individualização, por meio do poder de coerção em todas estas instituições disciplinares; aperfeiçoando e eventualmente penalizando os corpos "[...] a disciplina define cada uma das relações que o corpo deve manter com o objeto que manipula. Ela estabelece cuidadosa engrenagem entre um e outro" (Foucault, 1999, p.156).

Contudo, a concepção de disciplinamento abre espaço para uma nova tecnologia do poder: o biopoder, que por sua vez, não elimina o poder anteriormente elucidado, mas o integra através da noção coletiva de controle. Como o próprio nome sugere, esta classificação do poder refere-se à vida, mais especificamente sobre a relação de poder na vida populacional. Esse conceito é comumente exemplificado em dissociação a outra análise de poder foucaultiana: o poder soberano (Diniz; Oliveira, 2014).

Para Diniz e Oliveira (2014), enquanto o poder soberano consistia na lógica de "deixar viver" ou "fazer morrer", o biopoder alicerça-se na racionalização de "fazer viver" ou "deixar morrer", preconizado na noção de bem estar populacional. Surge, então, a concepção de uma política que se vale dessa tecnologia de controle para a manutenção da vida da população; a biopolítica. Sendo assim, legitimam-se mecanismos para o controle e vigilância em massa para eliminar o que possivelmente limitaria a vida do coletivo. O biopoder utiliza os corpos já docilizados por meio da individualização no poder disciplinar para uma conjuntura coletiva, legitimada no bem estar populacional.

Dessa forma, a perpetuação do formato disciplinar ganha várias escalas e interfaces, com a ramificação das relações, o poder intrínseco a elas se torna molecular, dificilmente objetificado – o que amplia a capacidade de docilização bem como a introjeção da vigilância, tornado o indivíduo controlável à submissão biopolítica por meio do biopoder (Diniz; Oliveira, 2014). A governamentalidade, outro conceito que constrói Foucault, pelo que analisa Candiotto (2010), tangencia todas as tecnologias de poder aqui exemplificadas, haja vista o seu caráter integracionista e relacional com o que antes era entendido como os precursores do poder; a guerra e a luta, e correlaciona-os com a forma interpretativa institucionalizada do poder jurídico-liberal do século XVIII.

Dessa maneira, para Candiotto (2010) o conceito de governamentalidade de Foucault incita um paradigma o qual não está restrito à noção de dominação da guerra, nem a de contrato consensual do modelo jurídico clássico, mas uma conjuntura desses dois modelos reconfigurados dentro de um novo universo de relações de poder, criando assim uma "superfície de contato" entre a forma de governo de si para consigo com aquele que manuseiam o governo dos outros, permitindo assim, através da análise das relações de poder como fluidas e mutáveis dentro do quadro social, um afastamento da técnicas violentas da dominação.

Contudo, dentro da governamentalidade, objetiva-se o governo da mente do indivíduo através de práticas discursivas e técnicas legitimadas pelo próprio poder que as utiliza, assim limitando as liberdades individuais e neutralizando as forças de resistência haja vista a docilização e os próprios mecanismo da biopolítica que introduzem a noção de ser da população os seus validadores.

A teoria foucaultiana da vigilância foi repensada por David Lyon, sob o aspecto que a normalização nem sempre é violenta ou coercitiva por natureza. Segundo Lyon (1994), Foucault deu continuidade à vigilância como um instrumento de punição, enquanto a análise da vigilância não deve ser somente de natureza negativa ou pessimista. Por outro lado, não se pode tolerar atitudes ou que dispositivos de vigilância invadam a privacidade ou coloquem a democracia em risco. A vigilância é intrinsecamente ambígua. Pode implicar cuidado e segurança dos vigiados (por exemplo, o salva-vidas na praia) ou pode envolver um esforço para controlar aqueles cuja conduta está sob suspeita (por exemplo, policiais em uma vigilância de bairro) e permitir práticas discriminatórias.

O surgimento do computador e da internet são articulados por Lyon para inquirir o "panóptico eletrônico" – uma releitura contemporânea dos estudos de Bentham, Orwell e Foucault. Conforme Lyon, "novas tecnologias de vigilância usadas no policiamento americano podem pressagiar o máximo sociedades de vigilância" (Lyon, 1994, p. 108, google translate)[1], bem como informação e vigilância constituem processos de retroalimentação. Todavia, o sociólogo adverte contra os pressupostos teóricos do tipo de determinismo tecnológico inscrito na distopia de George Orwell.

Para Lyon, a vigilância é definida como "a atenção focada, sistemática e rotineira de informações pessoais para fins de influência, gerenciamento, proteção ou direção" (Lyon,

[1] No original: new surveillance technologies used in American policing could portend ultimate surveillance societies.

2010, p.1, google translate)[2].Contudo, é preciso diferenciar a fiscalização do governo e do mercado, enfatizando a importância de distinguir entre o uso da vigilância nos dois domínios (Lyon, 1994).

2.2 Conceituação e análise no âmbito do direito comparado.

A prática da vigilância é anterior à criação das tecnologias digitais, do computador e da internet, mas os adventos do pós-Segunda Guerra Mundial modificam a intensidade e o modo de operação da vigilância para permear a vida cotidiana e as relações com os regimes políticos (Lyon, 2010). Um exemplo de aplicação da tecnologia à segurança pública é o sistema de monitoramento ou reconhecimento facial, implantado em diversos lugares do mundo, inclusive no Brasil.

O funcionamento do sistema de monitoramento parte da captura da imagem do rosto, que será subordinada à análise de um algoritmo especializado em identificar pontos e características faciais, como explica Duarte e Ceia (2022):

> As TRFs atuais funcionam a partir de alguns passos específicos. Inicialmente, imagens são capturadas por instituições públicas ou privadas (i.e., forças policiais, departamentos de trânsito, agências de identificação civil, empresas privadas de segurança, bancos etc.). Em seguida, essas imagens são convertidas em códigos alfanuméricos que conferem unicidade aos dados, que passam então a integrar as bases com as quais serão feitas as análises. Na fase operacional, uma nova imagem é capturada e comparada com o arquivo para verificação de identidade (i.e., para acessar a conta do banco o aplicativo pede que o cliente tire uma nova foto do rosto que será cruzada com a base de dados). O resultado do sistema algorítmico não é uma resposta definitiva (sim ou não), mas um cálculo de probabilidade que afere a chance de que a nova imagem seja da pessoa cujo dado biométrico estava no arquivo (Duarte; Ceia, 2022, p.18).

De acordo com pesquisa publicada na revista científica Science, a inteligência artificial, mesmo mecanismo utilizado na leitura e captação de dados faciais, pode ser tendenciosa e segregacionista, não operando de modo simétrico para todos os tipos de face ou características de gênero, raciais, etárias etc.(Caliskan; Bryson; Narayanan, 2017). Assim como a identificação com base nos atributos faciais do século XIX feita por técnicas médicas de Alphonse Bertillon e os retratos compostos de tipos criminosos de Francis Galton, os novos avanços das TRF's não conseguiram esconder a face do preconceito dos marcadores raciais.

Segundo este estudo desenvolvido na área, ao submeterem nomes variados à análise semântica dos programas, incorporava-se vieses preconceituosas, semelhante à linguagem

[2] No original: surveillance is understood as any focused attention to personal details for the purposes of influence management, or control.

humana. Relacionando os termos segundo o gênero, as combinações apresentavam nomes femininos ligados ao casamento e à família e os nomes masculinos à profissão e salário, bem como falha na tradução de artigos de gêneros neutros, presente em línguas como diversos idiomas e culturas.

Outro grande problema que vem sendo questionado é a atuação dos softwares de reconhecimento facial de grandes corporações como Amazon, IBM, Google, Microsoft e Facebook, Face ++, vinculado às redes sociais e aos aplicativos de smartphone. Os programas de reconhecimento dessas empresas, usados pela polícia americana para identificar e prender suspeitos de crimes, apresentavam falhas graves ao analisar diferentes traços de pessoas negras. Segundo o estudo desenvolvido pela pesquisadora do Instituto de Tecnologia de Massachusetts (MIT), Joy Buolamwini, Gender Shades, os softwares da IBM, Microsoft e Face ++ são ótimos no reconhecimento de homens de pele clara, com apenas 0,3% de erro, mas quanto a homens negros esse erro pode chegar em até 12% dentro do mesmo software. O resultado das mulheres negras é ainda mais alarmante, com a taxa de erro chegando em até 34.7% no programa da IBM.

A Organização não governamental (ONG) *Fight for the Future* em uma experiência com a comunidade universitária testou o *software Rekognition* com 400 pessoas, programa de reconhecimento facial da Amazon, em um comparativo com um banco de dados faciais de criminosos. O resultado foram 58 identificados na comunidade universitária, todos falsos positivos. A maior parte era de pessoas não-brancas, conforme informação no jornal "Época Negócios". O mesmo software também apresentou dificuldades de analisar diferentes gêneros, classificando erroneamente 31% de mulheres de pele preta como homens, segundo o *New York Times*. Na Inglaterra, o programa de reconhecimento facial utilizado pela polícia metropolitana em Londres, apesar de inicialmente anunciado com uma baixa taxa de erro, falhou 81% das vezes na análise de perfis em cruzamento com rostos criminosos, é o que diz o estudo independente da Universidade de Essex, que abre o discurso para um racismo algorítmico, conceito

Para além dos vieses das TRF’s, outros fatores podem influenciar no reconhecimento como luz, sombra, chuva, neblina, sujeitas na câmera

As TRF’s vêm ganhando espaço no Brasil, ancoradas em um dos principais desafios nacionais: a sensação e falta de segurança (Mello, 2024). As tecnologias são tratadas como o mecanismo capaz de reduzir o índice de crimes e da violência através do controle intermitente. Por exemplo, o governo do Distrito Federal instalou câmeras de reconhecimento facial em todo o seu território em 2020, ademais, outras metrópoles brasileiras vêm dando

sinais de maior interesse quanto à adesão desses programas de monitoramento. No carnaval de 2020 em Salvador, estado da Bahia, a polícia fez o uso do reconhecimento facial para capturar foragidos; o Metrô de São Paulo adotou esse método para aprimorar seu sistema de monitoramento sob a justificativa de ampliação da segurança (G1, 2022).

No entanto, a Defensoria Pública do Estado de São Paulo, a Defensoria Pública da União, o Coletivo de Advocacia em Direitos Humanos (CADHu), o Instituto Brasileiro de Defesa do Consumidor (Idec), o Intervozes e a Artigo 19 abriram uma ação judicial exigindo documentos que possam confirmar que os dados coletados dos usuários do Metrô não serão utilizados impropriamente. Ao serem apresentados esses documentos, as entidades mencionadas concluíram que o sistema que será adotado pelo Metrô de São Paulo é inseguro e não é capaz de garantir a segurança das informações dos frequentadores daquele lugar (MIGALHAS, 2022). Outro problema ocorrido foi no Rio de Janeiro, onde uma mulher foi confundida com uma foragida da polícia. O equívoco foi desfeito na delegacia após a conferência de documentos (G1, 2024). Esses equívocos vêm se tornando cada vez mais frequentes, ao passo da implementação dessa nova tecnologia.

Contudo, há vários alertas e variantes pouco discutidos sobre o uso descontrolado do reconhecimento facial e suas consequências sociais, que para o pesquisador de pós-doutorado na Microsoft Research Montreal Luke Stark (STARK, 2019), deve ser tratado com o mesmo rigor que resíduos nucleares, isso graças a sua falta de regulamentação e controle, o que abre precedentes para usos ilegítimos da tecnologia, classificada como o “plutônio da IA”.

Com o objetivo de discutir a relação entre as práticas e técnicas de monitoramento facial, as tecnologias de produção de dados e as grandes corporações e o controle social, utiliza-se os conceitos desenvolvidos na disciplina de estudos da vigilância, especificamente as contribuições teóricas de Jeremy Bentham sobre o panoptismo; a teoria da microfísica e da docilização dos corpos de Michel Foucault (1999), o monitoramento eletrônico através da internet e monopolização dos dados digitais face a democracia como pensou o sociólogo David Lyon (1994) e panóptico digital.

3 DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS E À PRIVACIDADE

3.1 Velhos problemas, novas abordagens

A segurança pública é um tema relevante no âmbito internacional, e no Brasil, um direito fundamental garantido pela Constituição de 1988. Nesse sentido, é certo que o surgimento e avanço de novas tecnologias podem revolucionar a segurança pública, disponibilizando ao Estado ferramentas com poder de potencializar o combate ao crime em suas diferentes espécies.

Entretanto, nesse cenário, surge a preocupação quanto à privacidade dos indivíduos e à possível vigilância descontrolada por parte do Estado e a forma com que podem impactar na persecução penal e nos direitos constitucionais à intimidade e à privacidade. Para lidar com essas questões, governos ao redor do mundo têm implementado leis de proteção de dados, buscando assegurar que as informações pessoais sejam tratadas com responsabilidade.

Durante o julgamento da no julgamento da Medida Cautelar nas Ações Diretas de Inconstitucionalidade (ADI) nº 6388, correlacionada ao direito à privacidade e intimidade, tendo em vista o teor da Medida Provisória 954/2020, o Ministro Ricardo Lewandowski, em seu voto estabeleceu uma cronologia normativa acerca do tema. Segundo Lewandowski, no âmbito internacional, previamente ao emblemático julgamento da Lei do Censo (Volkszählungsgesetz), de 1983, pelo Tribunal Constitucional Alemão, já em 1981, o Conselho Europeu atento à Proteção de Dados promulgou a Convenção 108, de Strasbourg. Ademais, o Ministro afirma que, tal diploma, em seu art. 2º, "a" e “b”, destaca a importância do controle sobre o tratamento automatizado de dados.

> Artigo 2 – Definições Para os efeitos da presente Convenção: a. “dados pessoais” refere-se a qualquer informação relativa a uma pessoa singular identificada ou identificável (“titular dos dados”); b. “tratamento de dados” refere-se a qualquer operação ou conjunto de operações efetuadas sobre dados pessoais, tais como a recolha,armazenamento, preservação, alteração, recuperação, divulgação, disponibilização, supressão, destruição ou execução de operações lógicas e/ou aritméticas sobre esses dados. (UNIÃO EUROPEIA, 1981, p.3)

Para além, ilustra o Ministro Lewandowski, que há também, nos Estados Unidos, o *Freedom of Informatin Act*, de 1974, e sua reforma de 1986, que garantem o acesso às informações, bem como sua retificação ou complementação, permitindo ao titular reivindicar esse direito diretamente perante a agência responsável pela posse dos dados pessoais (BRASIL, 2020).

Mais recentemente, em 27 de abril de 2016 o Parlamento Europeu e o Conselho da União Europeia estabeleceram a Diretiva (UE) 2016/680 com a finalidade de garantir a

proteção dos dados pessoais no contexto de investigações e operações de segurança realizadas pelas autoridades competentes para fins de prevenção, investigação, detecção ou repressão de infrações penais e para a execução de sanções penais. A diretiva elenca os princípios norteadores do tratamento de dados, dentre os quais estão: os princípios da segurança e integridade da informação, da qualidade dos dados, da finalidade, da necessidade e da transparência (art. 4º, nº 1) (Almeida, 2022).

Nessa linha, ainda em relação à proteção constitucional sobre o direito à privacidade e intimidade, Ministra Rosa Weber, relatora da ADI nº 6388, destaca que o uso dos dados pelas empresas e pelo poder público deve ser feito de forma legítima, com os parâmetros enunciados adequadamente para os titulares dos dados, como a finalidade e o modo de utilização dos dados objeto da norma. Enfatiza ainda a Ministra que as condições em que se dá a manipulação de dados pessoais digitalizados, por agentes públicos ou privados, consiste em um dos maiores desafios contemporâneos do direito à privacidade.

Na fundamentação de seu voto, Weber utilizou dos estudos sobre o tema do professor Daniel J. Solove, "*Nothing to hide: The false tradeoff between privacy and security"* (2011), com apontamentos importantes no tocante à privacidade em tempos de crise. Segundo ele, há uma falsa dicotomia entre privacidade e segurança como se ambos os valores fossem mutuamente excludentes. Nesse contexto, tece críticas ao "*argumento do pêndulo*" de acordo com o qual, em tempos de crise, o pêndulo se inclina em direção à segurança, permitindo a restrição de direitos, já em tempos de paz, o pêndulo retorna à valorização da liberdade e à proteção dos direitos. Aduz o professor que tempos de crise não são uma carta em branco para ferir direitos Constitucionais. (Solove, 2011 *apud* BRASIL, 2020)

De fato, não há que se falar em direitos absolutos, sendo assim, eventuais restrições ao direito à privacidade, à proteção de dados e à autodeterminação informativa podem e devem ocorrer, mas devem estar amparadas por parâmetros legais e constitucionais. Como dito por Solove:

> Sacrifícios de direitos e liberdades civis devem ser feitos somente quando o governo justifica adequadamente por que esses sacrifícios são necessários. É preciso submeter tais restrições a um escrutínio meticuloso, especialmente porque, em tempos de crise, o medo distorce nosso julgamento. [...] devemos ser extremamente cautelosos ao fazer sacrifícios desnecessários (Solove, 2011, p.61, *apud,* BRASIL, 2020, p.56)

No âmbito legislativo, foi publicada em 2018 a Lei nº 13.709, tida como a Lei Geral de Proteção de Dados, LGPD, e, em 2022 foi promulgada a EC nº 115 que passou a assegurar o direito à proteção dos dados pessoais na esfera constitucional. A LGPD assim como a Diretiva 2016/680 da UE, abriga em seu texto os princípios limitadores relativos ao trato de

dados pessoais, estipulando que a sua coleta só pode ocorrer estritamente em conformidade com a finalidade para a qual foi destinada, evitando qualquer captação excessiva, conforme estabelecido por seu art. 6º, incisos II e III:

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: […] II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
> III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados

Entretanto, há que se mencionar que a LGPD não regula o tratamento de dados no âmbito da segurança pública, e de atividades de persecução e repressão de infrações penais. Sendo assim, o artigo 4º, caput, III, "a" e "d", c/c §1º, da referida lei, expressa a necessidade da elaboração de "*lei específica que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular*".

Nesse diapasão, o governo brasileiro tem se mobilizado para desenvolver estratégias de regulamentação do uso da tecnologia de monitoramento facial. Em agosto de 2024 a Câmara dos Deputados realizou audiência pública na Comissão de Segurança Pública com a participação de diversos setores da sociedade, promovendo debates sobre a aplicação do reconhecimento facial como ferramenta para a manutenção da segurança pública. De acordo com o deputado Capitão Alden (PL-BA), o objetivo da audiência pública seria encontrar soluções que garantam tanto a eficácia no combate ao crime quanto o respeito aos direitos humanos e às liberdades individuais. (BRASIL, 2024)

Além disso, em obediência a ordem constitucional trazida pela EC nº 115/2022, bem como, ao que preceitua o artigo 4º, caput, III, "a" e "d", c/c §1º da LGPD, foi apresentada à Câmara dos Deputados, em novembro de 2020 como anteprojeto, tornando-se em 2022 Projeto de Lei (PL) da Lei de Proteção de Dados para Segurança Pública e Persecução Penal. Ademais, caso o PL 1515/2022 venha a ser transformado em lei, isto demonstra um avanço significativo no ordenamento jurídico do sistema de justiça criminal brasileiro na busca resguardar os direitos e garantias dos cidadãos diante do poder de vigilância estatal, e ainda, de acordo com sua exposição de motivos, quando ainda era um anteprojeto, suprir "um enorme déficit de proteção dos cidadãos, visto que não há regulamentação geral sobre a licitude, a transparência ou a segurança do tratamento de dados em matéria penal, tampouco

direitos estabelecidos ou requisitos para utilização de novas tecnologias que possibilitam um grau de vigilância e monitoramento impensável há alguns anos" (BRASIL, 2022, p.2).

Cumpre destacar que o Instituto dos Advogados Brasileiros (IAB), aprovou parecer antes do texto tornar-se PL, quando era apenas o anteprojeto de Lei de Proteção de Dados, destacando que "o anteprojeto cumpre a principal função de um estatuto jurídico nesse âmbito: restringir as possibilidades de arbítrio e do uso autoritário e ilegítimo das tecnologias de vigilância por parte de autoridades públicas" (Fernandes; Meggiolaro; Prates, 2020, p. 18). Adiante, o parecer ressalta a importância do anteprojeto, visto que busca garantir a segurança jurídica na utilização de novas tecnologias para a investigação e proteção de crimes, além de aprimorar a segurança pública no país.

É cediço que a segurança pública há muito tempo emprega o uso de tecnologia nas ações das autoridades estatais, como as interceptações telefônicas, o uso de câmeras de vigilância (CCTV3) e a análise estatística para desempenho da atuação policial em locais e horários estratégicos. Além disso, nota-se que é atual a discussão sobre a utilização da tecnologia de Monitoramento Facial e sua validade no âmbito da segurança pública.

Nesse sentido, ainda diante das incertezas jurídicas, perpetuam-se diversos questionamentos sobre a adequação da tecnologia de monitoramento facial em ambientes democráticos, devido ao risco iminente de violações a direitos fundamentais. Certo é que, com a implementação do monitoramento facial na segurança pública, o debate se volta para a forma de regulamentação, de modo que essa tecnologia seja usada de forma ética e que os algoritmos não perpetuem vieses ou discriminações existentes.

4 SEGURANÇA PÚBLICA

4.1 Regulamentação de medidas de policiamento

A questão da segurança pública no Brasil está inserida em um contexto amplo e complexo, o que torna necessária levar em conta características próprias das políticas criminais e do sistema penitenciário brasileiro. Nesse cenário, segundo Almeida (2022) é clara a distinção de qual grupo o Estado busca proteger e qual busca reprimir com força física, policial ou até mesmo institucional. Nesse ínterim, ao analisar a segurança pública no Brasil, Almeida (2022), utiliza conceitos do professor Alessandro Baratta (2002), para traçar um panorama mais amplo sobre as políticas públicas criminais.

Segundo a autora, na visão de Baratta (2002) há duas classes: subalterna e dominante, o que muito se assemelha à atual estrutura sócio-econômica nacional. Assim, a classe dominante possui constante interesse na manutenção da estrutura econômica-social, de modo que, a funcionalidade do sistema conserve as desigualdades para condicionar as políticas públicas criminais à perseguição da classe subalterna, mantendo o estigma e perseguição a esse grupo. Com efeito, nos dizeres do autor, a classe subalterna é aquela perseguida pelos mecanismos de criminalização. Nestes moldes, descreve um sistema que muito se assemelha ao sistema penal brasileiro, o Brasil possui registros de níveis alarmantes de violência policial, uma das maiores populações carcerárias do mundo e tem registrado mais de 40 mil assassinatos violentos anualmente.

> O sistema das imunidades e da criminalização seletiva incide em medida correspondente sobre o estado das relações de poder entre as classes, de modo a oferecer um salvo-conduto mais ou menos amplo para as práticas ilegais dos grupos dominantes, no ataque aos direitos das classes subalternas. (Baratta, 2002, p. 198 *apud* Almeida, 2022, p. 267).

Nesse diapasão, o projeto de pesquisa coordenado pelo Professor Pablo Nunes,“O Panóptico: Monitor do Reconhecimento Facial no Brasil”, do Centro de Estudos de Segurança e Cidadania aponta que em 2019, 151 pessoas foram presas com uso de reconhecimento facial, sendo que mais de 90% dessas pessoas eram negras. Ademais, para Nunes“o reconhecimento facial tem se mostrado uma atualização high-techpara o velho e conhecido racismo que está na base do sistema de justiça criminal e tem guiado o trabalho policial há décadas” (Nunes, 2019, p. 69-70)

Dessa forma, o uso do reconhecimento facial foi promovido como uma ferramenta eficaz e precisa para localizar indivíduos procurados pela polícia, sendo apresentado como solução para o desafio de identificação de suspeitos por seres humanos. No entanto, erros ocorreram com frequência, resultando em prisões indevidas. Isso acontece porque a precisão

dos sistemas de reconhecimento facial não é garantida em todos os casos, já que os algoritmos podem apresentar falhas, especialmente ao identificar pessoas de diferentes grupos étnicos, aumentando o risco de falsas identificações.

Após passar 3 dias preso, em outubro de 2020, essas foram as palavras ditas por José Domingos Leitão, 52 anos, em depoimento ao portal R7 "*Eu sofri, porque fui julgado pelos vizinhos. Perdi muitos serviços, porque disseram que eu era traficante. Falei que era inocente e a delegada falou para mim para eu pensar no que tinha feito. Pensei muito na família, que eu não ia voltar mais.*" (R7, 2022). Isto porque, José Domingos Leitão foi identificado falsamente como autor de um crime por uma tecnologia de reconhecimento facial. À vista disso, é cediço que o tratamento inadequado de dados físicos de uma pessoa pode ter um impacto significativo, com altos riscos de violação a direitos fundamentais.

No sistema de reconhecimento facial, os modelos são treinados com base em vastos bancos de dados contendo milhões de imagens de rostos, obtidos de redes sociais, sites de compartilhamento de imagens e câmeras, sendo principalmente armazenados por grandes empresas de tecnologia, como o Google. Isso evidencia que dados históricos carregados de preconceitos podem afetar a eficácia desses algoritmos, levando a um aumento de falsas identificações e abordagens policiais desproporcionais em comunidades negras e minoritárias.

Desse modo, Nunes (2019), coordenador do Panóptico, alerta para a postura do poder público de aplicar recursos em algo que notadamente traz prejuízos à população negra e marginalizada, sendo essa uma característica do Estado Brasileiro que há muito tempo aceita tais violações, até mesmo de morte em alguns casos, que ocorre à classe subalterna e é tido como mero efeito colateral. É nesse sentido que a aplicabilidade do reconhecimento facial no Brasil, carente de regulamentação, tem reforçado preconceitos já existentes na sociedade e se mostrado uma atualização high-tech para o velho e conhecido sistema segregacionista que oprime a classe subalterna e está nas bases do sistema de justiça criminal brasileiro.

Toda essa narrativa não pode ignorar o fato de que o sistema opera com dados tendenciosos, camuflando opiniões por números; uma ciência segregacionista dissimulada em matemática algorítmica, capaz de impedir que os indivíduos consigam empregos ou benefícios, confundindo-os com criminosos e restringindo sua liberdade por meio de prisões injustas, além de criar verdadeiros "mapas criminosos". De acordo Tarcízio Silva (2022, p. 15), isso ocorre porque a tecnologia de reconhecimento facial na segurança pública tem sido utilizada como ferramenta de violência estatal inserida em um histórico de construção onde as próprias forças policiais são um instrumento de segregação.

Nesse raciocínio, a falta de regulamentação faz com que o reconhecimento facial passe a ser mais uma ferramenta pela qual o Estado segregacionista se une com a tecnologia para, por meio de processos obsoletos e invisíveis, continuar trilhando um caminho de injustiças e violações. Nesse sentido, a cientista de dados Cathy O'Neil explica em sua obra "Algoritmos de destruição em massa: como o big data aumenta a desigualdade e ameaça a democracia" que os algoritmos na verdade funcionam como reprodutores de padrões de programação, usando as bases de dados com os quais foram alimentados. Assim, ao invés de uma análise desligada de preconceitos, os algoritmos reforçam o estigma e desigualdades, uma vez que os próprios dados trazem em si vieses sociais e raciais.

> A própria polícia gera novos dados, o que justifica mais policiamento. E nossos presídios inundam centenas de milhares de pessoas condenadas por crimes sem vítimas. A maioria deles vem de bairros empobrecidos, e a maioria é negra ou hispânica. Então, mesmo que um modelo não enxergue a cor da pele, o resultado o faz. Em nossas cidades amplamente segregadas, a localização geográfica é um proxy altamente eficaz para raça (O'neil, 2020, p.83).

Considerando a crescente adoção de projetos e investimentos voltados para a ampliação do uso de tecnologias na segurança pública, e apesar das possíveis vantagens do reconhecimento facial, é fundamental não ignorar as consequências de sua implementação em uma estrutura social racializada. Isso é ainda mais relevante na ausência de uma análise de visões, transparência, ética e regras específicas, que visem prevenir e/ou combater práticas discriminatórias e racistas em relação a grupos mais vulneráveis.

5 CONSIDERAÇÕES FINAIS

Os avanços tecnológicos têm empurrado a barreira da ficção e da realidade muito mais rápido do que imaginaria George Orwell quando escreveu sua obra “1984”. Por certo que desde dos tempos de Orwell a vigilância e o poder estatal são vistos com cautela, para não serem subterfúgio de arbitrariedades sob a justificativa de “maior segurança”. Para avaliar tais pontos, passou-se por uma construção histórico-filosófica, das técnicas de controle com o panóptico e as noções de vigilância e poder. Posteriormente, em uma análise comparada e dos vieses das tecnologias de reconhecimento facial, verificou alguns dos riscos práticos dessas implementações e o movimento cidades do norte global em relação as TRF’s.

No Brasil, a Lei de Proteção ao Dados e a Emenda Constitucional 115/202, redimensionaram, a seu modo, as diretrizes na proteção de dados e este como um direito fundamental. Por certo, que os direitos fundamentais não são absolutos, condicionando-se a ponderação para sua aplicabilidade. Do mesmo modo, ao Estado não está permitido absoluto poder de controle e vigilância, sob a justificativa de uma maior segurança.

A análise da tecnologia de reconhecimento facial e sua integração crescente nas políticas de segurança pública revela um cenário desafiador e complexo, embora seu uso possa trazer benefício em termos de eficiência, o uso indiscriminado dessas tecnologias, especialmente em ambientes públicos, põe em xeque questionamentos sobre privacidade, liberdade individual e a perpetuação de desigualdades, sobretudo racial. Necessário salientar alguns aspectos como a alta taxa de falsos positivos, identificados de forma incorreta, bem como a opacidade dos algoritmos, resultando em violações de direitos e discriminação, sobretudo tangenciando grupos marginalizados.

Destarte, urge a necessidade de regulamentação dessas tecnologias, face não apenas no que diz respeito aos benefícios, mas também aos riscos emergentes, a abordagem cautelosa evita o uso excessivo e descontrolado dessas ferramentas. Nesse sentido, a regulamentação específica e estudos sobre o tema apontam ser os caminhos mais seguros entre as opções. Sendo assim, estabelecer diretrizes, avaliar impactos, aperfeiçoar ferramentas e verificar as efetividades das TRF’s, garante efetividade à proteção de dados e à privacidade, ao passo que possibilita entender a melhor forma de utilizar essas tecnologias, sem violar garantias fundamentais.

É crucial que os direitos fundamentais dos cidadãos sejam preservados, dando prioridade e transparência no uso de tais tecnologias a fim de que não ocorram injustiças sociais. A questão central que se coloca é até que ponto a vigilância e o controle, facilitados

pela inteligência artificial, podem ser compatibilizados com a garantia das liberdades e da proteção de dados pessoais, evitando que os avanços tecnológicos se tornem instrumentos de repressão e exclusão.

REFERÊNCIAS BIBLIOGRÁFICAS

ALMEIDA, Eduarda Costa. Os grandes irmãos: o uso de tecnologias de reconhecimento facial para persecução penal. **Revista Brasileira de Segurança Pública**, v. 16, n. 2, p. 264-283, 2022. Disponível em: <https://revista.forumseguranca.org.br/index.php/rbsp/article/view/1377>. Acesso em: 02 de outubro de 2024.

BLACK Mirror: 1º temporada. Direção: Brian Welsh; Euros Lyn; Otto Bathurst. Roteiro: [Charlie Brooker; Konnie Huq; Jesse Armstrong].Produção: [Zeppotron]. Reino Unido, 2011. **Netflix**. Disponivel em: <https://www.netflix.com/br/title/70264888>. Acesso em: 10 de março de 2024.

BRASIL. **Constituição** (1988). Constituição da República Federativa do Brasil. Brasília, DF: Senado Federal: Centro Gráfico, 1988.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2018]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 de set. de 2024.

BRASIL, Senado Federal. **Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal**. Brasília: Senado Federal, 2022. Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/gruposde-trabalho/56alegislatura/comissao-de-juristas-dados-pessoais-segurancapublica /outrosdocumentos/DADOSAnteprojetocomissaoprotecaodadossegurancapersecucaoFINAL.pdf. Acesso em: 18 de setembro de 2024.

BRASIL. Superior Tribunal de Justiça. **Referendo na Medida Cautelar na Ação Direta de Inconstitucionalidade 6.388/DF**. Trata-se de pedido de medida cautelar em ação direta de inconstitucionalidade em face do art. 2º, da Medida Provisória nº 954/2020. Relatora: Min. Rosa Weber, 06 de maio de 2020. Disponível em:https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754357772. Acesso em: 12 de outubro de 2024.

BRASIL, **Projeto de Lei nº 1515/2022**. Lei de Proteção de Dados Pessoais para fins exclusivos de segurança do Estado, de defesa nacional, de segurança pública, e de investigação e repressão de infrações penais. Iniciativa: Coronel Armando. Brasília: Câmara dos Deputados, 2022. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2326300&fichaAmigavel=nao. Acesso em: 20 setembro. 2024.

BRASIL. Congresso. Câmara dos Deputados. Comissão promove debate sobre o uso de ferramentas de reconhecimento facial no combate ao crime**. Agência Câmara de Notícias**, 2024. Disponível em: https://www.camara.leg.br/noticias/1058042-comissao-promove-debate-sobre-o-uso-de-ferramentas-de-reconhecimento-facial-no-combate-ao-crime/ Acesso em: 15 de outubro de 2024.

BUOLAMWINI, Joy; GEBRU, Timnit. Gender shades: Intersectional accuracy disparities in commercial gender classification. In: **Conference on fairness, accountability and**

transparency. PMLR, 2018. p. 77-91. Google Translate. Disponível em: <https://proceedings.mlr.press/v81/buolamwini18a.html?mod=article_inline&ref=akusion-ci-shi-dai-bizinesumedeia> Acesso em: 12 jul. 2024.

CANDIOTTO, Cesar. A governamentalidade política no pensamento de Foucault. Filosofia Unisinos, v. 11, n. 1, 2010. Disponível em:<bit.ly/49fh1P2> Acesso em 23 de maio 2024.

CANDIOTTO, Cesar. A governamentalidade em Foucault: da analítica do poder à ética da subjetivação. O que nos faz pensar, v. 21, n. 31, p. 91-108, 2012. Disponível em: <https://oquenosfazpensar.com.br/oqnfp/article/view/363> Acesso em 21 maio 2024.

CALISKAN, Aylin; BRYSON, Joanna J.; NARAYANAN, Arvind. Semantics derived automatically from language corpora contain human-like biases. **Science**, v. 356, n. 6334, p. 183-186, 2017. Google Translate. Disponível em: https://www.science.org/doi/10.1126/science.aal4230. Acesso em: 08 de setembro de 2024.

CASTELLS, Manuel. A Rede e o Ser. Tecnologia Sociedade e transformação histórica. *In* CASTELLS, Manuel. **A sociedade em Rede.** ed.8. Rio de Janeiro: Editora Paz e Terra, 2005. v.1. p. 39 - 50. Disponível em: <bit.ly/3OBhcL8> Acesso em: 23 de outubro de 2024.

DINIZ, Francisco Rômulo Alves; OLIVEIRA, Almeida Alves de. Foucault: do poder disciplinar ao biopoder. **Scientia**, v. 2, n. 3, p. 143 -157, 2013. Disponível em:<http://www.faculdade.flucianofeijao.com.br/site_novo/scientia/servico/pdfs/VOL2_N3/FRANCISCOROMULOALVESDINIZ.pdf> Acesso em 23 de maio.

DUARTE, D.; CEIA, E. (org.) **Tecnologia, Segurança e Direitos:** os usos e riscos de sistemas de reconhecimento facial no Brasil. — Rio de Janeiro: Konrad Adenauer Stiftung, 2022. Disponivel em: <https://www.kas.de/documents/265553/0/Tecnologia%2C+Seguran%C3%A7a+e+Direitos+VF.pdf/8c70ec5a-1adf-69a8-39fb-f7afb1f76e91?version=1.0&t=1696517977110> Acesso em: 23 de setembro de 2024.

ÉPOCA NEGÓCIOS. Sistemas de I.A. falha em identificar pessoas não brancas e universidade desiste de usar reconhecimento facial, 2020. **Época Negócios.** Disponível em:<https://epocanegocios.globo.com/Tecnologia/noticia/2020/02/racismo-em-i-leva-universidade-desistir-de-reconhecimento-facial-no-campus.html> Acesso em: 18 de setembro de 2024.

FERNANDES, Maíra Costa; MEGGIOLARO, Daniela; PRATES, Fernanda. **Parecer sobre o anteprojeto de lei de proteção de dados para segurança pública e persecução penal: apresentado à câmara dos deputados em novembro de 2020**. Rio de Janeiro: Instituto dos Advogados Brasileiros, 2022. Disponível em: file:///C:/Users/SAMSUNG/Downloads/Parecer_na_Ind_001.2021.pdf. Acesso em: 15 de outubro de 2024

FORTUNE BUSINESS INSIGHTS. **Facial Recognition Market Size, Trends, Share (2030).** Global Report, 2019. Google Translate. Disponível em: https://www.fortunebusinessinsights.com/industry-reports/facial-recognition-market-101061. Acesso em 02 de novembro de 2024.

FOUCAULT, Michel. **Vigiar e Punir**: nascimento da prisão. Tradução de Raquel Ramalhete. Editora Vozes, v.20. Petrópolis: Rio de Janeiro, 1999

G1. Metrô de SP inicia operação de sistema de reconhecimento facial; TJ chegou a impedir instalação. **G1** 2022. Disponível em: <https://g1.globo.com/sp/sao-paulo/noticia/2022/11/21/metro-de-sp-inicia-operacao-de-novo-sistema-de-monitoramento-eletronico-por-meio-de-reconhecimento-facial-tj-chegou-a-impedir-instalacao.ghtmll> Acesso em: 20 de agosto. de 2024.

G1. Servidora pública é confundida com foragida da justiça por sistema de reconhecimento facial da polícia do RJ, 2024. **G1.** Disponível em:<bit.ly/3Vi2IDC> Acesso em: 21 de agosto 2024.

HUXLEY, Aldous. Admirável Mundo Novo. - 1ª ed. - Rio de Janeiro, Biblioteca Azul, 2014.

IG TECNOLOGIAS. Metrô de SP terá reconhecimento facial perigoso à população, acusam entidades. **IG Tecnologia**, 2020. Disponível em: <https://tecnologia.ig.com.br/2020-06-24/metro-de-sp-tera-reconhecimento-facial-perigoso-a-populacao-acusam-entidades.html> Acesso em: 20 de agosto de 2024.

LYON, David. The Surveillance State: From Tabs to Tags. *In*: LYON, D. **The Electronic Eye:** The Rise of Surveillance Society. NED-New edition, University of Minnesota Press, 1994. p. 102–18. Google Translate.

LYON, David. Surveillance, power and everyday life. *In:*LYON, D. **Emerging digital spaces in contemporary society: Properties of technology**. London: Palgrave Macmillan UK, 2010. p. 107-120. Google Translate. Disponível em: <https://www.academia.edu/51762262/Surveillance_power_and_everyday_life> Acesso em: 01 de junho 2024.

MELLO, Daniel. Reconhecimento facial está presente em todos os estados do Brasil. **Agência Brasil,** 2024. Disponível em: https://agencrasil.ebc.com.br/geral/noticia/2023-08/reconhecimento-facial-esta-presente-em-todos-os-estados-do-brasil. Acesso em: 02 de novembro 2024.

MIGALHAS. Ação questiona uso de reconhecimento facial no metrô de SP, 2022. **Migalhas.** Disponível em:<bit.ly/4g4MDJy> Acesso em: 22 de agosto de 2024.

NUNES, Pablo. Novas ferramentas, velhas práticas: reconhecimento facial e policiamento no Brasil. *In:* NUNES, P. **Centro de Estudos de Segurança e Cidadania; Rede de Observatório da Segurança.** Relatos da violência: cinco meses de monitoramento, análises e descobertas. São Paulo: Universidade Candido Mendes, 2019. Disponível em: https://observatorioseguranca.com.br/wordpress/wp-content/uploads/2019/11/1relatoriorede.pdf. Acesso em: 19 setembro. 2024.

O'NEIL, Cathy. Baixas Civis: justiça na era do big data. *In*: O'NEIL, C. **Algoritmos de destruição em massa : como o big data aumenta a desigualdade e ameaça a democracia** / Cathy O'Neil; tradução Rafael Abraham. p. 77 - 93.- 1. ed. - São Paulo. Editora Rua do Sabão. 2020.

ORWELL, George. **1984**. São Paulo: Companhia das Letras, 2009.

R7. Reconhecimento facial erra de novo e acusa inocente**.** *In:* Fábio Bomfim. **R7**. Brasília, 2022. Disponível em: https://noticias.r7.com/brasilia/reconhecimento-facial-erra-de-novo-e-acusa-inocente-21/01/2022. Acesso em: 19 de setembro de 2024.

SILVA, Tarcízio. **Racismo algorítmico: inteligência artificial e discriminação nas redes digitais**. p. 51 -71. Edições Sesc SP, 2022. (Disponível em bit.ly/3YHs3aW) Acesso em 14 de outubro 2024.

STARK, Luke. Facial recognition is the plutonium of AI. **TheACMMagazinefor Students**, 2019. Disponível em: <https://dl.acm.org/doi/10.1145/3313129> Acesso em: 20 de junho de 2024.

UNIÃO EUROPEIA. Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal. **Conselho da Europa.** 1981Disponível em: https://rm.coe.int/cm-convention-108-portuguese-version-2756-1476-7367-1/1680aa72a2. Acesso em: 12 de outubro de 2024.

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: 11 setembro 2024.