INSTITUTO
UNIVERSITÁRIO
DE LISBOA

Impactos sociais do reconhecimento facial: Privacidade e vigilância

Caio César Galdino Sales

Mestrado em Antropologia

Orientador(a):
Doutora Catarina Lopes Oliveira Frois
Professora Auxiliar com Agregação
ISCTE

Novembro, 2021

CIÊNCIAS SOCIAIS
E HUMANAS

Departamento de Antropologia

Impactos sociais do reconhecimento facial: Privacidade e vigilância

Caio César Galdino Sales

Mestrado em Antropologia

Orientador(a):
Doutora Catarina Lopes Oliveira Frois
Professora Auxiliar com Agregação
ISCTE

Novembro, 2021

Agradecimentos

Agradeço primeiramente ao meu esposo, David, que foi a pessoa que me acompanhou por todo este processo e me deu o suporte para a realização desta investigação de maneira que me faltam palavras para descrever o quão importante sua presença foi, e sempre será em minha vida. Também agradeço ao apoio da minha família e amigos que igualmente foram essenciais durante este percurso.

Um agradecimento especial à minha orientadora, Professora Catarina Frois, que me motivou e ajudou a tornar este sonho realidade.

Resumo

A integração de dispositivos tecnológicos promovida pela Cibercultura transformou o espectro cotidiano e incluiu a esfera digital no universo das interações sociais, tornando os contextos *on* e *off-line* quase indiferenciados. O desenvolvimento de tecnologias da informação representa um avanço do ponto de vista técnico, contudo o uso de técnicas de Reconhecimento Facial sob lógicas comerciais impacta o contexto social, pois conflita com as estruturas tradicionais de privacidade e mecanismos que regulamentam o processamento de informações biométricas baseados no consentimento emitido pelo utilizador no universo digital. Paralelamente, o uso de técnicas de vigilância sofisticadas inerentes às sociedades modernas torna o Reconhecimento Facial um aliado para as forças de segurança que viabiliza práticas de vigilância intrusivas, cuja influência do viés algorítmico e da automatização de processos criminais revela preocupações que atingem os diferentes grupos sociais de forma desproporcional. Diante deste enquadramento, propõe-se uma reflexão crítica sobre a mediação tecnológica associada aos contextos da privacidade e segurança, abordando a multiplicidade de danos decorrentes do processamento de informações pessoais de forma descontextualizada, e os desdobramentos deste processo na criação de subjetividades na esfera digital. Este enquadramento sugere a influência de questões raciais ligadas a processos históricos que moldam as práticas de vigilância permeadas por estereótipos hierarquizantes, que por seu turno são transferidos para a lógica sistêmica das decisões algorítmicas destacando a responsabilidade das empresas de tecnologia e das autoridades de segurança, além de questões éticas associadas ao universo da Inteligência Artificial.

Palavras chave: Privacidade, vigilância, Cibercultura, viés algorítmico, inteligência artificial, Reconhecimento Facial, Machine learning

Abstract

The integration of technological devices promoted by Cyberculture transformed the everyday spectrum and included the digital sphere in the universe of social interactions, making the online and offline contexts almost undifferentiated. The development of information technologies represents an advance from a technical point of view however the use of Face Recognition techniques under commercial logic impacts the social context as it conflicts with traditional privacy structures and mechanisms that regulate the processing of biometric information based on consent issued by the user in the digital universe. At the same time, the use of sophisticated surveillance techniques inherent in modern societies makes Face Recognition an ally for the security forces that enables intrusive surveillance practices, whose influence of algorithmic bias and the automation of criminal processes reveals concerns that affect different social groups disproportionately. Given this framework, it is proposed a critical reflection on technological mediation associated with the contexts of privacy and security, addressing the multiplicity of damage resulting from the processing of personal information in a decontextualized way, and the consequences of this process in the creation of subjectivities in the digital sphere. This framework suggests the influence of racial issues linked to historical processes that shape surveillance practices permeated by hierarchical stereotypes, which in turn are transferred to the systemic logic of algorithmic decisions highlighting the responsibility of technology companies and security authorities, in addition of ethical issues associated with the universe of Artificial Intelligence.

Keywords: Privacy, Surveillance, Cyberculture, Algorithmic Bias, Artificial Intelligence, Facial Recognition, Machine learning

Introdução

A proposta da presente investigação se inspira na área da Antropologia dedicada aos *Science and Technology Studies (STS)* e centra-se na utilização de dispositivos de Reconhecimento Facial (RF), nomeadamente os impactos sociais que surgem a partir da relação que o ser humano estabelece com a inovação tecnológica na sociedade contemporânea, relação permeada pelo entrelaçamento de universos aparentemente distintos num mundo caracterizado pela constante coleta e processamento de informações realizadas no domínio digital. Para alcançar este objetivo, faz-se necessário analisar criticamente os mecanismos que regulamentam as práticas ligadas ao processamento de informações pessoais no âmbito digital com especial ênfase nas seguintes dinâmicas: 1) O *processamento de imagens* decorrente do uso de redes sociais onde indivíduos voluntariamente publicam imagens que se conectam com informações pessoais (e.g. dados de contato, local de morada); e 2) O *processamento de informações* decorrente da captura imagens através de sistemas de vídeo vigilância em ambientes públicos e semi-públicos. Ambas as dimensões estão intersectadas com a temática da privacidade em ambiente digital, bem como com questões que incluem o uso de tecnologias da informação ligadas à segurança pública.

O estudo do uso de tecnologias da informação nestas duas dimensões permite-nos discutir o custo social envolvido nas dinâmicas que posicionam a tecnologia como um mediador de relações sociais, e apresentam riscos que merecem especial atenção do ponto de vista antropológico. Por um lado, exploramos as lógicas do consentimento enquanto problemática ligada à forma como se negociam os termos de privacidade no ambiente digital, observando os impactos em termos de ordem individual e coletiva. Por outro lado, discutimos em que medida é que o uso do reconhecimento facial em sistemas de vigilância massiva (tradicionalmente utilizado como forma de controle social caracterizado por violações de direitos e de liberdades civis e marcado pela ausência de regulamentações claras quanto ao tratamento de informações biométricas) põe em evidência que o desenvolvimento tecnológico e a dimensão ética subjacente seguem percursos e velocidades distintas no âmbito do *Global North*[1].

O uso de tecnologias de Reconhecimento Facial para fins de vigilância faz referência direta à temática da privacidade nos debates sobre os impactos dos avanços da Inteligência Artificial (IA), uma vez que a identificação automatizada de indivíduos em ambientes públicos e semi-públicos pode alterar significativamente a realidade social dos que são submetidos a esse tipo monitorização (Lynch 2018; Ringrose 2019). Estes dispositivos tecnológicos classificam as subjetividades individuais como potencialmente pacíficas ou criminosas, reforçando estereótipos negativos a grupos socialmente estigmatizados que ampliam a discriminação racializada sob o *slogan* "combate à criminalidade", por vezes associando a ideia de modernização e atualização do aparato policial para justificar estas

[1] Embora este seja um assunto que abrange um domínio territorial extremamente vasto, o domínio geográfico que esta investigação pretende se concentrar se refere maioritariamente aos contextos específicos da Europa Ocidental e da América do Norte.

práticas (Frois 2011), envolvendo uma multiplicidade de agentes com diferentes níveis de poder e de interesses que movimenta cifras consideráveis no mercado global.

Segundo dados do *Artificial Intelligence Report* de 2019[2], a indústria das *Big tech companies* foi avaliada em 2018 valendo aproximadamente 12 bilhões de dólares, e a projeção de crescimento do setor até ao ano de 2024 foi estimada em até 90 bilhões de dólares (Crawford *et al*, 2019: 50), valores significativos num mercado recente e em plena ascensão. Analisar os desdobramentos sociais ligados ao uso de tecnologias de Reconhecimento Facial remete-nos assim para um estudo crítico do desenvolvimento destes sistemas a partir do ambiente reflexivo das ciências sociais, tendo em conta a influência de perspectivas cognitivistas que influenciam a rotina dos laboratórios de Visão Computacional. É nestes lugares que se torna possível o reconhecimento e a "interpretação" automatizada de imagens a partir de lógicas sistêmicas que se concretizam em interações com diferentes níveis desempenho a partir da óptica do utilizador.

O material empírico utilizado nesta investigação centra-se maioritariamente no contexto norte-americano e europeu com o intuito de explorar como as diferentes regiões lidam com questões relativas ao desenvolvimento tecnológico contemporâneo, e analisar em que termos se constituem a noção de privacidade que influencia os mecanismos de governança do uso de tecnologias de Reconhecimento Facial. O avanço do campo da Inteligência Artificial que aperfeiçoa sistemas de Reconhecimento Facial apresenta-se na figura de benefícios em torno da luta contra o crime organizado e pretende criar uma sensação de segurança coletiva. Em contrapartida, potencia comportamentos discriminatórios que remetem ao racismo estrutural subjacente a processos históricos que ocorrem em simultâneo com o desenvolvimento destes sistemas, o que nos permite questionar o discurso de neutralidade do uso de tecnologias da informação em contextos sociais.

É importante contextualizar o leitor a respeito de terminologias utilizadas no decorrer da argumentação a fim de facilitar o entendimento do ponto de vista prático. Neste sentido, pretende-se evocar a ideia de "modelo facial" (*Facial template*), termo técnico designado para referir o conjunto de dados que possibilitam a identificação de pessoas de forma automatizada através da imagem facial. Este termo se inspira na ideia de *visual personal data* referido na publicação do portal IEEE[3] que discute a temática da vídeovigilância a partir do *General Data Protection Regulation* (GDPR) (Asghar *et al* 2019). O objetivo desta proposta é ampliar a noção de *personal data*[4] do GDPR incluindo a informação visual facial como parte do conjunto de informações pessoais que possibilitam a

[2]Ver *AI report* 2019, publicação do *AI Now Institute*, instituto de pesquisas interdisciplinares da Universidade de Nova Iorque dedicado ao estudo das implicações sociais sobre o uso da Inteligência Artificial.

[3]*Institute of Electrical and Electronical Engineers* que se dedica a analisar o avanço da inovação tecnológica para a humanidade. Ver https://www.ieee.org/ Acedido em: 20/10/2021.

[4] Dados pessoais fazem referência a qualquer informação relativa a uma pessoa física identificada ou identificável ("titular dos dados" "data subject"); uma pessoa física identificável é aquela que pode ser identificada, direta ou indiretamente, em particular por referência a um identificador, como um nome, um número de identificação, dados de localização, um identificador online ou um ou mais fatores específicos para o físico, fisiológico, identidade genética, mental, econômica, cultural ou social dessa pessoa natural. (GDPR, 2016 Artigo 4).

identificação de indivíduos, reforçando a lógica da privacidade visual, não obstante o GDPR ser um mecanismo importante no que se refere à regulamentação da privacidade no espaço digital que valoriza a autonomia do indivíduo em relação às suas informações pessoais. A maneira como o GDPR aborda a definição de dados pessoais permite-nos sugerir a ampliação desta noção com o objetivo de evitar interpretações ambíguas sobre a temática do processamento de dados pessoais (visuais), em que o reconhecimento facial tem ganhado destaque no contexto das tecnologias de informação.

É do interesse desta investigação abordar a inovação tecnológica concordando com as formulações que não tratam a tecnologia como um elemento neutro, ou totalmente dissociado de questões sociopolíticas (Sanmartin e Lujan, 1992 apud Escobar, 1994:212), sobretudo tendo em conta questões relacionadas com o viés algorítmico[5] inscrito no desenvolvimento de sistemas computacionais de reconhecimento facial. Assim, ciência e tecnologia traduzem-se em forças que possibilitam criar ou reformular realidades, isto é, são fatores fundamentais para as manifestações do "Ser no mundo" [6], abordagem antropológica pautada pela noção de Cibercultura[7] tal como pensada por Arturo Escobar (1994) sobre a área de atuação da Antropologia dedicada ao estudo da inovação tecnológica nos contextos culturais em que estes processos se desenvolvem, bem como os que ajudam a criar. Trata-se de um conceito que considera os dispositivos tecnológicos como inventos culturais desenhados a partir de condições específicas que, por seu turno, possibilitam a criação de novas visões de mundo à medida que são incorporados à realidade social.

Dito por outras palavras, a tecnologia apresenta-se como um mediador entre utilizadores e máquinas (e sistemas) possibilitando a interação num espaço que promove o estabelecimento de interações sociais *online*, normalizando o uso da imagem e a exposição da intimidade, ainda que nem sempre seja evidente de que forma as empresas de tecnologia utilizam essas informações. Por outro lado, o uso de recursos de Reconhecimento Facial que dependem de processamentos complexos e contínuos de informação pessoal, acompanhado da existência de vastos bancos de dados, posiciona a

[5]O viés algorítmico refere-se à problemática ligada ao treinamento de modelos de *Machine learning* que desenvolvem limitações sistémicas que influenciam o funcionamento destes modelos em virtude constituição dos bancos de dados utilizados no desenvolvimento desta tecnologia. O treinamento destes modelos a partir de bancos de dados homogêneos (e influenciados por preconceitos sociais) cria lógicas que revelam diferentes níveis de desempenho quando se deparam com dados que fogem ao padrão que o sistema consegue reconhecer, resultando em desempenhos restritos na medida em que este tipo de tecnologia ganha alcance massivo (Tsamados et al 2021). Esta questão será discutida no Capítulo 4 onde abordaremos os custos sociais associados ao viés algorítmico da tecnologia de Reconhecimento Facial.

[6] Escobar inspira-se na obra de Heidegger e na perspectiva ontológica do Ser, o que elucida a discussão de Dasein (Ser-no-mundo) a partir de perspectivas existencialistas, discussão que não será levada a cabo nesta investigação uma vez que foco desta reflexão se limita a abordar os impactos sociais da Inteligência Artificial na sociedade. "Ser no mundo", neste sentido, faz referência às interações que atravessam o indivíduo e integram os contextos *online* e *off-line* de forma interdependentes. No plano da segurança, estas interações se relacionam com a ideia de "Cultura de vigilância", tendo como pressuposto a participação ativa da sociedade que favorece a vigilância através do uso de tecnologias da informação internalizadas nas reflexões e práticas diárias dos cidadãos comuns (Bricalli 2020).

[7]Para Arturo Escobar o termo Cibercultura (1994:214) abrange dois domínios tecnológicos: o primeiro se refere às tecnologias computacionais de informação (Inteligência Artificial), e o segundo a temática da Biotecnologia. Por motivos de precisão esta investigação utiliza este termo fazendo referência ao primeiro destes domínios.

tecnologia como um elemento decisivo em questões de segurança pública. Neste enquadramento, a tecnologia instrumentaliza o Estado, pois aumenta a sua presença e alcance de forma ubíqua, entrando em conflito com questões de privacidade e com os fluxos de informações pessoais que necessitam consentimento explícito, resultando num emaranhado de interesses individuais, de segurança e comerciais que ressaltam a importância de reflexões críticas sobre o processamento de informações biométricas nos contextos de vigilância.

Estes são alguns dos temas que norteiam esta investigação cujo objetivo não pretende fornecer respostas definitivas, mas sim refletir criticamente em torno dos aspectos que aproximam a tecnologia ao cotidiano mais íntimo, tendo em mente que esta aproximação por vezes implica uma relação pouco transparente pela parte dos utilizadores, embora se revele proveitosa para as empresa de tecnologia. O que está por trás de funcionalidades comuns no ambiente das redes sociais que utilizam modelos faciais para fomentar interações no universo virtual? De que forma o uso destas tecnologias pode influenciar rotinas de vigilância e quais são os desdobramentos que estes recursos causam ao serem utilizados de forma massiva a partir de diferentes regulamentações nos diferentes contextos estudados?

Diante das problemáticas relacionadas com a questão da privacidade digital e dos aspectos que associam esta temática com problemas de vigilância, o uso de recursos de Reconhecimento Facial tem provocado respostas de diversas comunidades que se opõem ao uso deste tipo de tecnologia. Tendo em conta os potenciais danos que a imprecisão destes sistemas causa no tecido social, grupos organizados em diversas cidades[8] na América do norte propuseram o banimento momentâneo desta tecnologia em locais públicos até que se compreendam as reais implicações do seu uso (Crawford *et al*, 2019: 25). No mesmo sentido, publicações que discutem os impactos do uso de novas tecnologias abordam os riscos associados ao uso destes sistemas comparando-o com o plutónio (Stark, 2019), material radioativo utilizado na confecção de armamento nuclear altamente controlado.

Esta comparação pretende aludir aos riscos envolvidos nas etapas de categorização de indivíduos realizadas por algoritmos que transformam modelos faciais em unidades de dados quantificáveis ao tentar "interpretar" imagens, procurando reconhecer padrões geometricamente similares dentro de gigantescos bancos de dados criados para treinar redes neurais a reconhecer imagens de forma automatizada. Este processo, de acordo com Stark, pode ter desdobramentos "socialmente tóxicos" diante de princípios hierarquizantes que provocam danos a grupos sistematicamente estigmatizados (Stark, 2019:52-53). O uso do reconhecimento facial suscita debates importantes na atualidade, pois põe em destaque o papel da tecnologia sob uma perspectiva singular que discute a relação que se estabelece entre o ser humano e os produtos da inovação tecnológica, permitindo questionar a velocidade deste avanço que, dia após dia, adentra a realidade social através de novas aplicações e redes sociais pautadas pelo processamento de informações biométricas.

[8] São Francisco, Oakland, Sommerville e Detroit nos Estados Unidos, e Montreal no Canadá são algumas das cidades listadas no *AI Report* como exemplos de locais que conseguiram refrear o uso de Reconhecimento Facial em virtude dos danos inerentes ao uso deste tipo de tecnologia.

As reflexões que esta investigação propõe sobre Inteligência Artificial e Reconhecimento Facial partem de uma perspectiva crítica relacionada aos estudos *decolonials*, que retratam as características do processo colonial a partir da apropriação e expropriação de indivíduos e territórios, e do controlo de estruturas sociais que reproduzem o racismo estrutural. Tais características se assemelham as estruturas que utilizam dados pessoais de forma exploratória na atualidade, que quando projetadas para o plano digital, preveem a comodificação das relações humanas reduzidas a dados indiferenciados que "recriam o poder colonial[9]" e transferem preconceitos sociais para as práticas digitais, mesmo que de forma inconsciente. Dito de outra forma, pretendemos explorar questões implicadas na discriminação racial como um tipo de dano adicional que impacta as comunidades sistematicamente marginalizadas a partir de mecanismos de poder, econômicos e políticos que formataram os aspectos culturais da vida contemporânea num momento pós-colonial (Mohamed *et al* 2020).

Esta perspectiva é relevante, pois através dela é possível compreender impactos sociais da tecnologia da informação a partir da perspectiva dos agentes que vivenciam a exclusão social, a limitação de oportunidades laborais no setor tecnológico e os efeitos de uma vigilância de tipo racializada com implicações nas subjetividades codificadas a partir de estereotipos, sugerindo uma análise criteriosa sobre como se interpreta a ideia de raça culturalmente.

Enquanto recurso tecnológico o Reconhecimento Facial representa um relativo avanço das ciências tecnológicas em termos técnicos. Porém, como veremos nos próximos capítulos fatores ligados às indeterminações dos processos algorítmicos tornam a aplicação deste tipo de tecnologia no contexto social um processo delicado, pois o uso delas, nestes termos, pode viabilizar processos intrusivos e até mesmo autoritários que perturbam liberdades e os direitos individuais.

Metodologia:

A abordagem da temática do Reconhecimento Facial foi realizada através da revisão bibliográfica de artigos científicos e manuais que descrevem o universo da Visão Computacional do ponto de vista do desenvolvimento destes sistemas, bem como de relatórios desenvolvidos por institutos de pesquisas dedicados a avaliar as implicações das técnicas de Inteligência Artificial no âmbito social. Em paralelo, utilizo publicações de suporte que discutem as questões da Cibercultura e dos *STS*, bem como a complexidade de processos como o da interpretação, partindo de inspirações fenomenológicas em torno das perspectivas cognitivistas do setor computacional quanto à reprodução do comportamento humano em ambientes artificiais, além de *insights* da antropologia visual sobre a relação estabelecida com a imagem. Partindo de relatos que exploram a temática da representatividade digital, e da revisão de publicações que retratam as tensões raciais conectadas a processos históricos, inicio a argumentação abordando a flexibilidade da noção de segurança tendo como base teórica a perspectiva crítica da antropologia da segurança, e a análise de artigos publicados em revistas e

[9]Mejias apud Mohamed et al, 2020: 664

periódicos sobre os *Surveillance studies*, relacionando-os a temática da privacidade à luz dos regulamentos de proteção de dados digitais no contexto estudado. Os aspectos ligados a leitura facial geométrica são abordados a partir da crítica quanto ao uso de práticas que remetem a antropometria, e, de forma complementar, articulado aos riscos das tecnologias de Reconhecimento Facial indicados no relatório *Face off* da organização sem fins lucrativos *Electronic frontier foundation*[10] sobre o uso deste recurso por parte do FBI, bem como diversas publicações que discutem os estereótipos associados a grupos historicamente marginalizados, com especial foco na comunidade negra no contexto norte americano.

Do ponto de vista da regulamentação dos dados digitais, utilizo como base o GDPR e regulamentações de âmbito local nos Estados Unidos, contrastando as noções tradicionais de privacidade e as questões éticas ligadas à dinâmica da privacidade no âmbito digital face aos tipos de danos que surgem destas interações, e a influência do ambiente comercial neste processo quando comparado com outras áreas do conhecimento. O argumento sobre o custo social se desenvolve a partir da revisão bibliográfica de argumentações que criticam o uso de técnicas de *Machine learning* em contextos sociais, bem como das perspectivas *decolonials* sobre o colonialismo digital e os desdobramentos que este conceito projeta sobre as comunidades historicamente discriminadas. Por um lado, a análise de publicações e experimentos que retratam os diferentes desempenhos dos sistemas de Reconhecimento Facial tradicionais revela uma multiplicidade de questões inerentes ao uso destes sistemas, cujos impactos nem sempre são evidentes por conta da maneira como eles funcionam. Por outro, a análise de casos que ilustram violações de privacidade no universo digital constituem o enquadramento para uma argumentação critica sobre a utilização de técnicas de vigilância intrusivas associadas ao uso de tecnologias da informação por conta da construção de subjetividades que partem de indeterminações sistêmicas, bem como de visões racializadas sobre determinados grupos sociais. Partindo de indicadores sobre os efeitos do uso do Reconhecimento Facial na literatura que retrata a temática da segurança e da vigilância, elaboro uma perspectiva antropológica multidimensional sobre os desequilíbrios que a automatização de processos causa no contexto social contemporâneo, destacando a esfera discursiva que promove o estado de suspeita constante, tema em que a crítica dos *Surveillance studies* é fundamental para esta investigação, e proponho uma reflexão que pondera o uso deste tipo de tecnologia em contextos específicos, e não de forma generalizada no tecido social.

[10] [10] A *Electronic frontier foundation* é uma organização sem fins lucrativos que atua em defesa das liberdades e direitos civis na esfera digital. Acedido em 20/10/2021 disponível em: https://www.eff.org/.

Capítulo 1: Reconhecimento Facial e Inteligência Artifical: Sistemas de Machine Learning

Abordar a temática do Reconhecimento Facial como um fenômeno implica um trabalho de imersão sobre o domínio informático da Visão Computacional *(Computer Vision)* que nos ajude a perceber como este processo opera do ponto de vista técnico, que passa pelo desenvolvimento de competências essencialmente humanas ligadas ao ato do reconhecimento e da interpretação de imagens em ambientes artificiais. O entendimento desta fase elementar de criação contribui para elucidar questões importantes referentes à maneira como os produtos de inovação tecnológica são desenvolvidos a partir de perspectivas que limitam o desempenho destes sistemas, mas não impede que esta tecnologia seja disponibilizada para utilização massiva, traduzindo-se em processos que envolvem uma linguagem computacional técnica obscura que dificulta a sua compreensão, bem como os eventuais riscos associados a eles.

O Reconhecimento Facial automatizado toca em questões complexas uma vez que envolve a necessidade de consentimento individual quanto ao processamento de dados biométricos digitais que permitem ou restringem o acesso a níveis de informações consideradas sensíveis: por exemplo, no caso de sistemas de Reconhecimento Facial que operacionalizam a autenticação ou verificação de modelos faciais com o intuito de limitar o acesso a informações confidenciais (e.g. informações bancárias), ou confirmar o acesso a informações que correspondam ao *ID* registado na fase de cadastro para o uso de uma determinada aplicação (e.g. mecanismos de desbloqueio de *smartphones*). Estas são algumas das utilizações comuns onde observamos a aplicação de sistemas de Reconhecimento Facial no cotidiano, e que de maneira intuitiva se assemelha ao uso de senhas que protegem informações pessoais. Porém, à medida que as tecnologias da informação se tornaram mais sofisticadas e associaram novos recursos a serviços existentes, criaram-se novas possibilidades que ampliam o escopo destas ferramentas.

No caso do Reconhecimento Facial, entre os possíveis usos destes sistemas, interessa abordar a funcionalidade que consiste na atribuição automatizada de nomes (informações pessoais) a modelos faciais detectados em fotos ou vídeos a partir do cruzamento de informações biométricas em bancos de imagens, o que tecnicamente se refere como identificação e reconhecimento facial. Estes processos, quando combinados com o uso de redes neurais e algoritmos de aprendizagem profunda (*deep learning*[11]*)* tendem a aperfeiçoar e automatizar a realização destas operações. Do ponto de vista

[11] Podemos pensar em *Deep learning* como técnicas utilizadas pela área da Ciência de dados que advém de uma ramificação do campo da Inteligência Artificial, o Aprendizado de Máquina *(Machine learning)*, que utilizam algoritmos para realizar análises de dados que treinam modelos de *Machine Learning* a desempenhar tarefas específicas, por exemplo, reconhecer modelos faciais de forma automatizada. Estas técnicas diferem de práticas computacionais tradicionais da Inteligência Artificial baseadas na programação prévia de representações que deveriam guiar o comportamento inteligente de um sistema, e têm sido amplamente utilizadas por empresas que trabalham com previsões baseadas na análise de dados (Hurwitz e Kirsch, 2018:04).

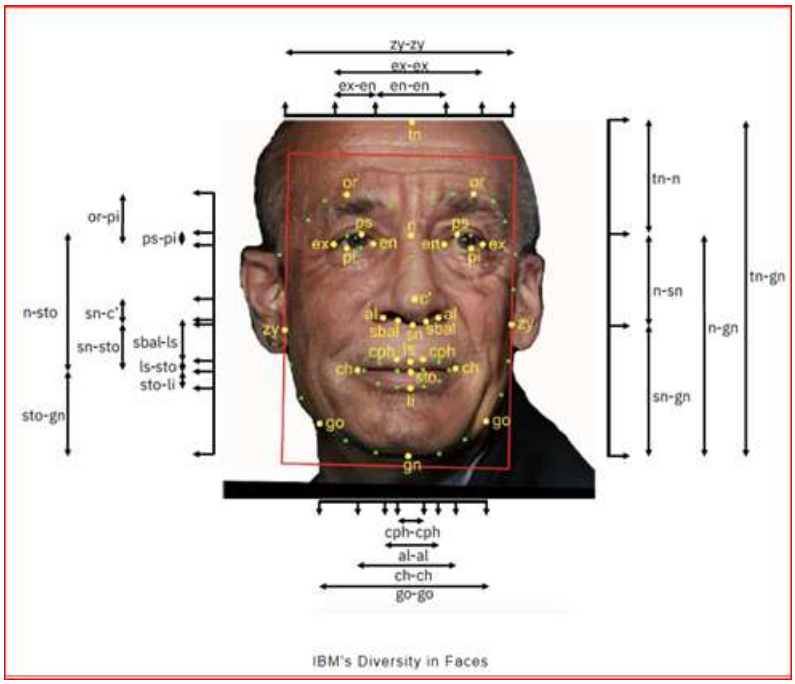
técnico, o Reconhecimento Facial é um "problema" a ser resolvido por algoritmos que levam em consideração as seguintes operações, segundo Jason Brownlee[12]:

1) Detecção de rosto: A identificação de um ou mais rostos numa imagem ou vídeo, e a inclusão de uma moldura digital no rosto de cada indivíduo;

2) Alinhamento Facial: A análise geométrica dos rostos detectados identificando a estrutura detalhada do(s) rosto(s) analisando o formato além de outras características como olhos e nariz;

3) Extração de características individuais: Processo que extrai características individuais que serão utilizadas na comparação com informações disponíveis no banco de dados de imagens utilizado;

4) Reconhecimento facial (*matching)*: O resultado da operação com sucesso das etapas anteriores faz com que um indivíduo seja reconhecido se as características extraídas correspondem a alguma das imagens disponíveis no banco de dados utilizado.



Fonte: Crawford e Paglen, 2019. IBM Diversity in faces. *Excavating AI.*

A execução destas etapas ocorre num ambiente artificial (*training set)* e depende da disponibilidade de um banco de imagens que possibilite que algoritmos analisem modelos faciais de forma constante, o que em tese cria uma dinâmica que aperfeiçoa o desempenho dos modelos de *Machine Learning* na tarefa do reconhecimento facial. Dito por outras palavras, o funcionamento eficiente destes sistemas de Visão Computacional, no caso do Reconhecimento Facial, depende em grande parte do quão variado é o banco de imagens utilizado na fase de treinamento.

[12]Ver *A gentle introduction to deep learning for Face recognition,* de Jason Brownlee no portal *Machine learning mastery*.

Vejamos algumas etapas fundamentais para a criação de um ambiente artificial que "interpreta" imagens: a primeira refere-se à coleta de modelos faciais que constitui o banco de dados onde é desejável que o programador obtenha a maior quantidade de imagens disponíveis para treinar os algoritmos, ou seja, aperfeiçoar a leitura feita pelos modelos de *Machine Learning* para distinguir e reconhecer diferentes padrões geométricos e estatísticos de um determinado objeto a partir das variantes possíveis detectadas. A seguir, inicia-se a fase em que cabe ao programador etiquetar e classificar todas as imagens coletadas consoante ao objetivo de identificação. A partir deste momento entra em ação a atividade computacional das redes neurais onde algoritmos executam incontáveis análises estatísticas que resultam em modelos de *Machine Learning* capazes de "interpretar" imagens de forma automatizada, a partir de limites epistêmicos que determinam o funcionamento do sistema em situações específicas de ambiente controlado. Ou seja, o reconhecimento e a tarefa de "interpretar" modelos faciais decorrem das escolhas feitas durante a supervisão e o desenvolvimento dos bancos de dados e dos processos de treinamento destes algoritmos (Crawford e Paglen, 2019), e é a partir destas escolhas que os modelos de *Machine Learning* procuram as características individuais num banco de imagens para reconhecer um determinado modelo facial, que pode ou não estar associado a outros níveis de informação pessoal dependendo dos critérios utilizados para etiquetar e classificar estas informações.

Depois de estabelecido o banco de dados onde a análise algorítmica cria um modelo de *Machine Learning*, este sistema "interpreta" imagens de maneira automatizada e reconhece os indivíduos que fazem parte do banco de dados, cuja procedência das imagens destaca questões éticas relacionadas com violações da privacidade digital e de consentimento. A publicação *Excavating AI: The Politics of Images in Machine Learning Training Sets*[13] explora aspectos importantes onde é possível observar a influência de assunções que, dependendo do objetivo para o qual um sistema é desenvolvido, (no caso de sistemas de vigilância massiva), as escolhas feitas durante o seu desenvolvimento podem ganhar contornos políticos que põem em evidência a problemática do viés algorítmico embutido nestes processos, com implicações nocivas como a hierarquização social e o aprofundamento da discriminação com fundo racial.

A publicação destaca três níveis onde sucessivas assunções são usualmente feitas durante o desenvolvimento de sistemas de Visão Computacional relacionadas com as etapas de classificação de imagens. A primeira trata dos conjuntos de imagens agregadas que determinam classificações mais gerais, como por exemplo, Homens, Mulheres, Transgêneros e pessoas Não-Binárias, na etapa das taxonomias[14]. A segunda consiste em classificações individualizadas, ou seja, uma espécie de

[13] Publicação do *AI Now institute* de Setembro de 2019 cuja pesquisa se intitula como a "Arqueologia dos *datasets*".

[14] Importante referir que a noção de taxonomia remete aos trabalhos do botânico Sueco Carl Linnaeus, o "pai da taxonomia", figura responsável por criar o sistema de classificação nas ciências naturais no século XVIII amplamente conhecido (Nomenclatura Binomial), e cujo trabalho influenciou o discurso de pseudociências que promoveram o Racismo Científico partindo da noção de Raça como um fator biológico e não um constructo

tipificação (por exemplo, cor de cabelo) e finalmente a terceira etapa procede a etiquetagem das imagens a que são atribuídas às classificações definidas a cada tipo de imagem coletada (Crawford e Paglen, 2019).

Importa mencionar que a relação estabelecida com a imagem tem origem nos trabalhos da antropologia visual através de técnicas de representação do outro com o objetivo inicial de documentar acontecimentos observáveis. O registo destes acontecimentos e a representação do outro funcionou como um processo de recolha de evidências que documentava a expansão colonial e o conhecimento antropológico da época. Ao mesmo tempo que estes registos denotavam o perfil expansionista de grupos dominantes, eles serviam para representar o histórico de culturas e povos em "estado natural[15]". Posteriormente, os registos fotográficos (e cinematográficos) ganharam notoriedade e passaram a representar indivíduos nos contextos industriais, chegando ao momento atual onde a representação digital ocupa centralidade no que se refere à representação visual contemporânea (Ribeiro 2005). A antropologia física e a antropometria também trazem questões importantes para a discussão da imagem, sobretudo num contexto relativo a questões criminais, tema discutido mais adiante por conta da influência da geometria facial utilizada para desenvolver tecnologias de Reconhecimento Facial.

Numa primeira observação, as fases de assunção de sistemas de Visão Computacional não se destacam se pensarmos nelas como parte de uma lógica que identifica objetos. Contudo, quando aplicamos esta mesma lógica a um modelo de *Machine Learning* que automatiza o reconhecimento de pessoas, e que este sistema pode aperfeiçoar técnicas que ampliam formas de vigilância intrusivas que ferem liberdades civis, fica evidente que o desenvolvimento técnico-científico assume um caráter estratégico na contemporaneidade. A partir de princípios estabelecidos no interior de laboratórios de Visão Computacional são definidas diretrizes para identificar indivíduos em ambientes vigiados por meio da análise de aspectos físicos ou comportamentais. Este contexto de transformação das práticas de vigilância e de privacidade faz com que uma análise inspirada no conceito de Cibercultura posicione a Antropologia como estando apta para adentrar este terreno, e elaborar um diagnóstico cultural que impulsione a reflexão sobre as transformações relacionadas com o crescente desenvolvimento técnico científico (Escobar, 1994: 216), que intersecta relações complexas de poder

---

social. Linnaeus foi influenciado por ideias como a da *Scala Naturae,* e suas publicações classificavam os habitantes dos diferentes continentes de acordo com aspectos biológicos como a cor da pele. Em sua 1ª edição do *Systema Naturae* (1735), os habitantes do continente Europeu constavam no topo da escala, lugar este que foi sendo substituídos pelos habitantes dos continentes Asiático e Americano nas edições seguintes.Porém, é importante destacar que os habitantes do continente africano sempre figuraram nos últimos lugares nesta escala hierárquica, acompanhados de descrições negativas como "preguiçosos e negligentes". Ver "*How Scientific Taxonomy Constructed the myth of race*" de Brittany Kenyon-Flatt na revista de antropologia Sapiens.

[15]A expressão "estados naturais" refere-se à documentação de povos e culturas que não detinham o domínio de técnicas de escrita nem de hábitos culturais consoantes aos modelos europeus, normalmente situados no domínio territorial do *Global South* e/ou do Oriente (Ribeiro 2005). Esta designação remete-nos também a representação da dicotomia entre selvagens civilizados, algo observável nos trabalhos de Jean-Baptiste Debret do século XIX que reflete uma interpretação do Brasil colonial a partir da perspectiva da mestiçagem (Almeida, 2009). Dito de doutra forma, perspectivas eurocêntricas.

entre as esferas públicas e privadas que impactam diretamente no futuro dos indivíduos submetidos a este tipo de tecnologia.

As três fases brevemente descritas são relativamente comuns quando pensamos nas etapas que desenvolvem modelos de *Machine Learning,* e o exemplo a seguir ilustra como nasce os primeiros sistemas de Reconhecimento Facial pautados por assunções relacionadas a estados emocionais que evidenciam o quão influente era a perspectiva cognitivista no ambiente tecnológico da época, ainda que, nesta altura, o cognitivismo e o paradigma representacional da Inteligência Artificial já tivessem sido fonte de críticas por Hubert Dreyfus (1971) [16].

Em 1998 foi desenvolvido um banco de dados no Japão por Michael Lyons, Miyuki Kamachi e Jiro Gyoba chamado JAFFE *(Japanese female facial expression)*, cujo objetivo principal era o de ensinar um modelo de *Machine Learning* a reconhecer e etiquetar estados emocionais em modelos faciais de dez mulheres diferentes através da análise de expressões faciais:

Samples from the Japanese females facial expression image set.

Fonte: Lyons *et al*, 1999. Exemplos de imagens de expressões faciais do banco de dados JAFFE. *The Japanese Female Facial Expression (JAFFE) Dataset.*

No plano das taxonomias, o banco de dados JAFFE foi concebido para identificar modelos faciais que expressavam estados emocionais, e no plano das classificações individualizadas foram definidos os seguintes estados emocionais *(affect recognition)*: felicidade, tristeza, surpresa, nojo, medo, raiva e neutra. A partir desta estrutura, o sistema deveria identificar e ordenar as imagens que exibissem um dos estados emocionais mencionados, e etiquetá-las de acordo com a leitura visual[17], o que segundo Crawford e Paglen (2019), remete ao primeiro nível de assunção do processo que presume que estados

[16]Ver "*What Computers can't do: The Limits of Artificial Intelligence".*

[17] Neste sentido importa destacar a complexidade que surge do ato de observar que torna este um fator ambíguo, complexo e difícil de ser reproduzido de forma artificial. Partindo de noções exploradas pelas teorias das visualidades e visibilidades, Andrea Mubi argumenta sobre as limitações relativas ao ato da observação como um processo uniforme "Existem tantas maneiras e estilos de perceber, ver, olhar, divisar, captar, vislumbrar, localizar, observar, inspecionar, detectar (...). Tais variações correspondem a uma incrível variedade de tarefas, e sugere que o ato de olhar se prolonga em todos os tipos de direções diferentes para diferentes atividades envolvendo pensamento, consciência, compreensão, apreciação, reconhecimento, fala, manipulação e controle" (Brighenti, 2010: 2-3).

emocionais simulados em laboratório são elementos legítimos para orientar um sistema de identificação facial.

Outro fator destacado pelos investigadores sobre as assunções que compunham o sistema JAFFE refere-se à categoria de imagens "neutras", ou seja, modelos faciais com expressões que não se encaixavam com as classes de emoções previstas no plano taxônomico. Contudo, se pensarmos na gama de estados emocionais que um ser humano é capaz de exibir, fica evidente a limitação da experiência uma vez que a probabilidade do sistema não identificar um estado emocional de forma coerente – ou seja, "interpretar" uma imagem que mostre um estado de confusão, de interesse ou de dor como estados neutros – compromete a consistência do sistema visto que estes são estados emocionais diferentes, e dificilmente seriam interpretadas por seres humanos como "neutros". Neste sentido, a limitação apresentada pelas escolhas tomadas nos níveis taxonômicos influencia diretamente a eficiência do desempenho deste sistema e indica que o processo de identificar modelos faciais de forma automatizada não se trata de um assunto restrito ao universo da engenharia computacional, este processo implica articulações de grande complexidade sensorial que pouco se relacionam com rotinas extremamente técnicas, sugerindo que a participação de outras áreas científicas seja um imperativo no desenvolvimento de tecnologias de Reconhecimento Facial de alcance massivo.

Experiências como a do banco de dados JAFFE pecam por simplificar aspectos importantes nas fases de desenvolvimento sob a justificativa de que estes sistemas foram desenhados para desempenhar tarefas específicas. Esta simplificação verifica-se na assunção de que sete estados emocionais representam a totalidade de emoções possíveis ou, de forma implícita, sugere que estes são os mais relevantes deixando de fora uma infinidade de estados emocionais que passam a ser erroneamente identificados por meio de "interpretações" imprecisas e pouco realistas. Estas lacunas reforçam a crítica ao paradigma representacional da Inteligência Artifical e a impossibilidade de prever e reproduzir todos os aspectos do mundo sensível em ambientes artificiais devido à limitação em torno do conhecimento humano. Neste sentido, o campo da Visão Computacional se mostra reduzido no que se refere à aproximação com reflexões como a da "finitude do conhecimento" [18] discutida pela Filosofia Hermenêutica, que propõe que o conhecimento humano depende de condições que não são possíveis prever na totalidade. Dito por outras palavras, propor que um sistema "interprete" modelos faciais e identifique estados emocionais que não podemos quantificar de forma determinista torna-se uma tarefa demasiado ambiciosa, sobretudo se pensamos no ato da interpretação inspirado no princípio do círculo hermenêutico, e no exercício da interpretação vinculado a fluxos contínuos de perguntas e respostas constantemente renovadas na medida em que o ser humano

[18]Brice Wachterhauser faz referência à Hermenêutica de Gadamer ao pontuar que o conhecimento humano é finito, pois ele depende de condições que o ser humano não pode conhecer na sua totalidade, por exemplo, a linguagem e a história. Esta formulação também é influenciada pela concepção de Habermas sobre a linguagem e a história como elementos fluidos que atuam dentro de um espaço de liberdade humana cuja extensão não nos é possível perceber integralmente, e ambas remontam um passado que igualmente não podemos recuperar na sua totalidade (2002:56-57).

percorre o trajeto interpretativo (Verde, 2009:84). Assim, o resultado desta operação num plano altamente racionalizado difere-se da noção de interpretação sob a óptica da hermenêutica pelo fato de que este processo, quando representado de forma artificial, procura invariavelmente classificar as imagens de forma determinista desconsiderando a perspectiva de constante renovação do trajeto interpretativo[19], além das variadas interpretações relativas ao ato da observação.

Perspectivas cognitivistas e a Visão Computacional

À medida que aprofundamos a temática da Inteligência Artificial e do Reconhecimento Facial, fica evidente que os processos técnicos ramificam-se em sub-operações que envolvem alta complexidade computacional; as várias etapas aqui mencionadas servem para ilustrar as principais fases relativas à criação destes sistemas e dar a conhecer a perspectiva da Visão Computacional como uma área da Inteligência Artificial focada em produzir máquinas ou sistemas aptos a "interpretar" imagens de forma semelhante à visão e interpretação humana. A proposta do Programa *Summer Vision* realizado no MIT em 1966 pretendia viabilizar um sistema capaz de reconhecer padrões a partir da leitura de imagens captadas durante o verão, e posteriormente classificar os objetos identificados a partir de taxonomias previamente determinadas (Seymour, 1966) [20]. Esta lógica de acumulação de modelos representacionais também esteve presente no então recém formado campo da Inteligência Artificial em 1957, quando Allen Newel, Herbet Simon e J.C. Shawn dão a conhecer o projeto *GPS (General Problem Solver)* dedicado à resolução de problemas lógicos a partir de regras e fatos pré-definidos na fase de programação com o objetivo de reproduzir comportamentos inteligentes na solução de problemas específicos, por exemplo, um jogo de xadrez.

Os fundamentos baseados em esquemas representacionais[21] criados para simular comportamentos inteligentes foram objeto de críticas que contestavam a Inteligência Artificial no século XX por defender a premissa de uma suposta semelhança entre processos de cognição e processos computacionais. Esta crítica está presente no argumento de Hubert Dreyfus e na recusa das lógicas essencialmente cartesianas quanto à reprodução de comportamentos inteligentes: "O comportamento do homem não pode ser explicado em termos de um mecanismo de processamento de informações que recebe e processa um conjunto de *inputs*" (1971:100).

Vale a pena explicar que a tentativa de reproduzir comportamentos inteligentes desde meados de 1950 foi orientada pela perspectiva cognitivista e por assunções de cunho biológico e psicológico

[19] Este raciocínio explica a razão pela qual o termo interpretação tem sido utilizado entre aspas em certas ocasiões, pois a "interpretação" em ambiente artificial é normalmente concebida por processos racionais cuja finitude do conhecimento humano impede de representá-la de maneira artificial.

[20] O projeto *Summer Vision* foi idealizado por Marvin Minsky, que na altura concebia a ideia de que a interpretação de imagens representava uma função fundamental para a simulação de comportamentos inteligentes. O projeto foi realizado por Gerald Sussman e pode-se dizer que foi um dos primeiros experimentos da área da Visão Computacional (Crawford e Paglen, 2019).

[21] Ou seja, a ideia de programar um sistema a partir de representações previamente desenhadas para atingir um objetivo específico, e não de propor que um sistema "aprenda" a partir da análise de dados.

sobre a inteligência humana, e serviu como pano de fundo para a formulação de teorias sobre a similaridade do processo de cognição humana ao comportamento artificialmente produzido, como se o primeiro se originasse a partir de esquemas racionais de caráter sequencial passíveis de serem representados num laboratório de forma integral. Neste sentido, a abordagem fenomenológica inspirada pela crítica Heideggeriana de Dreyfus torna-se uma ferramenta teórica importante para propor uma visão crítica quanto ao desenvolvimento destas tecnologias. A partir dela, é possível desmistificar assunções inerentes ao desenvolvimento tecnológico e o intuito de codificar todos os aspectos da vida cotidiana no interior de sistemas computacionais, colocando-nos em contato com perspectivas transcendentais relativas ao ser humano e seu entorno.

Pensar no Ser no sentido Heideggeriano significa pensar no "ser-no-mundo" de forma relacional, e não *o ser e o mundo* como entidades separadas, onde os sujeitos utilizam os objetos do mundo de forma unicamente exploratória. Aplicar este raciocínio ao analisar a Inteligência Artificial e o Reconhecimento Facial ajuda-nos a perceber que representar o mundo através de regras e códigos pré-determinados pode não ser o método mais eficiente para atingir a precisão operativa da cognição humana, pois o ambiente e os objetos que nos rodeiam não se resumem a meros conjuntos de regras e fatos sistematicamente ordenados e exteriores a nós; são elementos que fazem parte do mundo que vivemos que compreende seres humanos, animais e objetos que coabitam em uma mesma temporalidade em constante interação (Dreyfus, 2007: 249 apud Gomes, 2019: 168). Pensar criticamente sobre as fases de desenvolvimento destes sistemas a partir de inspirações fenomenológicas torna-se uma mais valia para esta reflexão, pois revela que a simulação de processos cognitivos que dependem da descrição precisa de regras é algo que compromete o desempenho eficiente destes sistemas por conta de limitações que extrapolam o domínio computacional.

O exemplo do banco de dados JAFFE dá-nos o contexto para perceber como se concebiam modelos de *Machine Learning* projetados para a interpretação de imagens na viragem do século XX para o século XXI, período em que a disponibilidade de imagens no domínio digital e o uso das redes sociais não tinham tanto apelo como atualmente. Porém, as transformações impulsionadas pelas tecnologias da informação alteraram este cenário num curto espaço de tempo, e em pouco mais de 20 anos o uso de *Smartphones* foi incorporado na rotina cotidiana, reformulando a relação que estabelecemos com os produtos da inovação tecnológica, provocando uma profunda alteração na forma como lidamos com a imagem e a privacidade, sobretudo no ambiente das redes sociais.

Este contexto de transformação tem relevância nas análises que envolvem o Reconhecimento Facial, sobretudo se levarmos em consideração o fluxo de imagens disponibilizado diariamente na internet[22]. Esta mudança permite inferir que o papel exercido pelas empresas de tecnologia possui uma relevância nunca antes alcançada do ponto de vista social, pois de forma voluntária os usuários das

[22] Em 2013 o Facebook deu a conhecer que, naquela altura, a plataforma contava com uma média de 350 milhões fotos publicadas por dia. Ver *Facebook users have uploaded a quarter trillion photos since the site's launch* no portal *The Verge*.

redes sociais fornecem informações detalhadas sobre aspectos íntimos da vida cotidiana como gostos pessoais, relações familiares e de amizade. O acesso a este nível de informação permite que as empresas perpetuem práticas como à vigilância corporativa a partir de mecanismos pouco transparentes aos usuários.

A utilização de ferramentas de *Dataveillance*[23] facilita a prática de vigilância corporativa em que a acumulação e análise de dados têm como finalidade principal construir estratégias de *marketing* que visam maximizar lucros através da análise de históricos de busca e da forma como os usuários navegam pela *internet*. O objetivo é sugerir produtos e serviços que se relacionem com o perfil de cada usuário, ou seja, trata-se de uma ferramenta utilizada para atender interesses puramente comerciais, que se dedica a rastrear a atividade digital com implicações que criam tensões no campo da privacidade. Para além disso, e de forma bastante subtil, este processo atua no sentido de moldar o comportamento dos utilizadores (Esposti, 2014:222), dando às empresas maior visibilidade sobre como, quando, e para quem certos anúncios são mais ou menos relevantes.

Diante da problemática do cognitivismo e das sucessivas transformações que os campos da Inteligência Artificial sofreram nas ultimas décadas com o surgimento das técnicas de *Machine Learning*, que em princípio não operam sob a lógica da programação prévia de representações do mundo, fica a impressão de uma aparente superação do paradigma representacional em virtude da substituição dele pelo uso de redes neurais, o que solucionaria os problemas conceptuais da área da Visão Computacional. Importa, contudo, não nos deixarmos conduzir erroneamente por esta impressão.

Se nos primórdios da Inteligência Artificial a perspectiva cognitivista já dava sinais que o funcionamento destes sistemas tinha um caráter limitado por não conseguir representar integralmente o ambiente necessário para simular comportamentos inteligentes, de forma semelhante podemos inferir que esta limitação, no caso do Reconhecimento Facial com *Machine Learning,* ganha uma nova roupagem na medida em que desloca a limitação prévia de criar representações para a necessidade de compor bancos de dados integralmente diversos. Ou seja, em ambos os casos pretende-se criar sistemas que funcionem a partir da identificação de padrões que dependem de orientação humana, orientação esta sujeita às escolhas de quem determina os tipos de modelos faciais mais relevantes para que um sistema possa identificar indivíduos em imagens de forma satisfatória. Este procedimento permite-nos inferir que a problemática do paradigma representacional não foi de facto superada; ganhou apenas uma nova configuração deixando claro que o projeto de ensinar máquinas a interpretar imagens de maneira automatizada não é apenas um projeto que requer recursos técnicos. A maneira como este projeto afeta o contexto social torna-o um projeto social e político que envolve decisões pautadas pela leitura automatizada de informações biométricas (modelos faciais), que influenciam as tensões sociais ligadas ao desequilíbrio de poderes entre os agentes que desenvolvem e os que utilizam

[23] Conceito cunhado por Roger Clarke (1988) que se refere à monitorização constante de pessoas ou grupos que pretende regular o comportamento destes através de sistemas de dados pessoais (apud Esposti, 2014)

estas tecnologias, reforçando estereótipos sobre grupos específicos que demandam esforços interdisciplinares, algo que possibilita que o histórico das ciências sociais seja um aliado importante nestes debates (Crawford *et al*, 2019: 56).

A representatividade digital e o contexto social

Quando pensamos sobre a verificação ou identificação facial é importante ter em conta que estes são processos que um ser humano executa de forma natural, mas cuja descrição determinista constitui-se numa tarefa difícil de ser realizada por máquinas. Codificar estas características com o objetivo de reproduzi-las artificialmente, num primeiro momento leva-nos a crer que a redução de processos tão complexos a conjuntos de procedimentos não totalmente compreendidos podem levar a simplificações de caráter limitado. No caso do Reconhecimento Facial, estas simplificações tendem a assumir um viés discriminatório que resulta no aprofundamento de desigualdades sociais materializadas na composição do banco de imagens[24]. É neste enquadramento que se insere a problemática do viés algorítmico, nomeadamente quando em 2015, a *Google* teve de se desculpar publicamente por classificar usuários da aplicação "Fotos" como gorilas por conta de problemas com os mecanismos de Reconhecimento Facial utilizado na altura que apresentavam dificuldades ao analisar imagens de usuários de pele negra[25].

Seja por questões técnicas quanto ao banco de dados, ou pelo viés atribuído de forma inconsciente a um sistema *(unconscious bias)*, a problemática do viés algorítmico manifesta-se principalmente em grupos historicamente estigmatizados em virtude de aspectos físicos, e expõe limitações que precisam ser endereçadas no universo da tecnologia para fomentar práticas pautadas por princípios éticos e anti-discriminatórios por parte dos responsáveis por operar as redes neurais que "interpretam" imagens. Dito de outra forma, a identificação de falhas técnicas neste processo não implica encontrar soluções puramente racionais por meio de comandos técnicos; trata-se de uma questão bastante mais profunda relacionada com a transparência envolvida nestes processos, e com a maneira como estes são operacionalizados.

Diante desta problemática, a cientista da computação Joy Buolamwini, ativista norte-americana, fundou a Liga da Justiça Algorítmica em 2016 *(The Algorithmic Justice League - AJL)*, sediada em Cambridge, Massachussetts, com o compromisso de promover uma tomada de consciência quanto às implicações da Inteligência Artifical em contextos sociais. A figura de Joy se tornou relevante no debate que aborda os impactos sociais do uso da Inteligência Artificial após seu projeto *(The Aspire*

[24]A quantidade de imagens de pessoas de tons de pele negra muitas vezes é inferior a quantidade de pessoas de pele branca em bancos de dados de sistemas de Reconhecimento Facial. Ver *Facial Recognition Is Accurate If You're A White Guy*. The New York Times.

[25] Episódio racista envolvendo o Google e a tecnologia de reconhecimento facial "*Google Apologises for Photosapp's racist blunder*". BBC news.

mirror[26]*),* onde Joy detectou a ineficiência de um sistema de Reconhecimento Facial em detectar a imagem de indivíduos de pele negra, algo que se tornou um problema prático visto que na altura o projeto em que trabalhava como estudante de ciências da computação previa que os testes fossem feitos com o seu próprio rosto. Esta limitação lhe chamou a atenção, e após inúmeras tentativas sem sucesso, conclui-se que a detecção do seu rosto se tornou uma tarefa que o sistema não conseguia "resolver", e a única forma de fazer o sistema detectar seu rosto seria caso ela pusesse uma máscara branca[27].

Fonte: The Index Project, 2021. *Algorithmic Justice League. AI's threats to civil rights and democracy"*

Este problema prático demonstra a importância do viés algorítmico no interior de sistemas de Visão Computacional; porém, este é um fato que nos fornece alguns elementos conflitantes que esta investigação pretende trazer à discussão nas próximas secções. O primeiro centra-se na falta de representatividade de indivíduos de pele negra nos bancos de dados que ensinam os sistemas de Reconhecimento Facial a identificar imagens, criando um cenário de desempenho limitado do ponto de vista técnico que nos impõe a seguinte pergunta: Um trabalho de recolha de imagens mais diversificado poderia sanar esta dificuldade sistêmica? Em segundo lugar, se deslocarmos esta questão sob a perspectiva da segurança pública e da eventual vigilância massiva utilizando recursos de Reconhecimento Facial, aumentar este banco de dados para melhorar o desempenho destes sistemas

[26]"O *Aspire Mirror* é um dispositivo que permite que você olhe para si mesmo e veja um reflexo em seu rosto com base no que o inspira ou no que você espera ter empatia" Joy Buolamwini. Acedido em 20/10/2021. Disponível em: http://www.aspiremirror.com/

[27]Ver *"How I am fighting bias in algorithms"*, TEDX Beaconstreet de 2016.

poderia criar um ambiente propício a tornar esta mesma população num alvo da polícia por conta dos estigmas sociais associados a questões discriminatórias?

Estas questões introdutórias ilustram como diferentes níveis de desigualdades se sobrepõem às populações submetidas à lógica do racismo, e evidencia que a problemática do viés algorítmico não é apenas um problema específico do ambiente digital, também pode ser problematizado a partir de perspectivas que excluem indivíduos ao lançar sistemas que apresentam baixo desempenho em populações específicas. Para além disso, a inclusão destes grupos se torna um fator problemático em virtude de estigmas sociais que persistem na contemporaneidade, e que podem se agravar dependendo da utilização feita por razões de vigilância e segurança. Neste sentido, não é o objetivo desta investigação propor argumentos que polarizem a discussão sobre o racismo estrutural existente nas relações sociais, mas sim analisar a influência de aspectos culturalmente construídos a partir de processos históricos em torno de estereótipos raciais que tentaram minimizar indivíduos através da exaltação de grupos supostamente superiores.

Partindo deste enquadramento, a análise do uso de tecnologias criadas em torno de preconceitos raciais, e a aparente presença do viés algorítmico na interpretação de modelos faciais de indivíduos brancos e não brancos cria a hipótese que ilustra a continuidade de uma mentalidade racializada da população negra, que na atualidade se depara com representações da sua imagem através de comparações inapropriadas, como no caso da Google "Fotos" já destacado.

Convocar a discussão da representatividade e do viés algorítmico também suscita preocupações relativas à representatividade da população negra nos bancos de dados das forças de segurança em virtude de eventos históricos que retratam a comunidade negra como alvo tradicional da polícia. Neste sentido, promover a inclusão deste grupo no contexto digital é algo que deve ser tratado de forma cuidadosa para que a solução de um problema não se torne a raiz de outro de forma não intencional. É importante perceber que a razão de sublinhar esta discussão tem como objetivo destacar a desigualdade de projeção de vidas quando comparada aos pares brancos (Chagas, A.M e Santos, L. S. 2020). Os históricos culturais, sociais e políticos convertem-se num instrumento ideológico que, mesmo de forma não propositada, permite com que a simples composição de bancos de imagens se realize a partir de amostras de imagens de grupos homogêneos. O uso do Reconhecimento Facial para a temática da vigilância representa um problema social que atinge as comunidades vigiadas de forma integral, porém a inclusão digital de grupos marginalizados possibilita diferentes projeções de vida para estes grupos em virtude de questões culturais que se concretizam em danos adicionais a estas populações.

As tensões raciais e o racismo estrutural

Problematizar as questões raciais que influenciam a esfera social implica pensarmos no conceito de raça como um conceito que não é fixo (tal como no racismo científico). Silvio Almeida (2018)

argumenta sobre as diferentes facetas do racismo utilizando o termo raça como um elemento conectado aos momentos históricos em que a noção de diferentes raças constituía um espectro que classificava indivíduos em função da aparência física, diferenciando-os dos povos europeus a partir do século XVI. Neste sentido, a construção da noção de "homem universal" [28] e o desenrolar posterior do iluminismo no século XVIII são centrais para a abordagem da questão racial, pois o projeto iluminista concebia o homem "ideal" como um ser racional inserido em diferentes contextos (econômico e cultural), dotado de distintas habilidades intelectuais, dentre elas a comparação e a diferenciação. Assim sendo, aqueles que não seguiam este modelo de homem estariam fadados a classificações a partir de escalas inferiores, ou não "ideais". Trata-se de um momento que evidencia uma relação paradoxal, pois ao mesmo tempo em que se superam questões dogmáticas que permitem ao homem se ver apto para desenvolver suas capacidades intrínsecas, este desenvolvimento é relegado a grupos considerados "ideais". É neste momento que surgem terminologias comparativas associadas à raça como "seres civilizados e seres primitivos e/ou selvagens" (Levi-Strauss, 1970), bem como se desenvolve a ideia de que era necessário levar a civilização aos territórios colonizados durante a expansão mercantilista.

Tendo em conta que a noção de raça se conecta com momentos históricos anteriores a modernidade, Almeida (2018:19) argumenta que abordar criticamente o termo raça implica que "Por trás da raça sempre há contingência, conflito, poder e decisão, de tal sorte que se trata de um conceito relacional e histórico".

Situando as questões raciais em torno das problemáticas de conflito e poder, as práticas utilizadas, por exemplo, no transporte da população escravizada[29] nos regimes coloniais surgem a partir de um tipo de controle social que se ocupava com processos identificação, ou seja, de marcação a ferro dos corpos escravizados o que, por um lado tinha o objetivo de identificá-los e comercializá-los como mercadorias e, por outro lado, cumpria a função disciplinar de punir comportamentos desobedientes. Registos de abolicionistas como Thomas Clarkson do século XVIII recuperam a maneira como as populações escravizadas foram submetidas a técnicas de identificação nas viagens transatlânticas onde a marcação a ferro ocorria tanto nos portos de embarque, como antes do desembarque nos portos de destino. A marcação dos corpos era realizada utilizando tachos de ferro com rum para produzir brasas suficientemente quentes para aquecer os moldes de ferro com diferentes inscrições que indicavam aos proprietários que escravo pertencia a qual comprador. Este relato revela como inúmeros povos sofreram, na pele (e por causa da pele), os efeitos desumanizadores influenciados pela hierarquização

[28] O autor faz referência ao Renascentismo e o momento em que a influência dogmática da Europa medieval se enfraquece, fazendo com que a figura do homem se tornasse um elemento central para a reflexão filosófica da época. Trata-se de um período de valorização da ciência e da racionalidade que alterou profundamente as sociedades europeias entre os séculos XIV e XVI.

[29] A maneira como as informações biométricas são processadas para a identificação de indivíduos pelas empresas de tecnologia pode ser interpretada tal como o transporte dos povos escravizados, pois em ambos os casos, a importância da identificação e da comodificação representam uma espécie de domínio sobre o que se entendia/entende como mercadoria.

racial promovido pela *Middelburg Trade Company* holandesa no desembarque de escravos no território de Curaçao, um processo que orientava os capitães das embarcações a marcar-los para efeitos de identificação, bem como para demonstrar o domínio exercido sobre populações designadas como inferiores na altura (Browne, 2015: 99-100).

Ainda que o passado escravocrata seja um exemplo que ilustra o olhar racializado como um elemento central associado à discriminação racial, Almeida (2018) observa que este esquema baseado na diferenciação de indivíduos em função de características biológicas e étnico-culturais estendeu-se, de forma menos evidente, até o século XX. A ascensão do regime nazista e o genocídio dos povos judeus é outra evidência histórica de que raça é um conceito permeado por um espectro político com desdobramentos que naturalizaram a desigualdade de grupos marginalizados por meio de múltiplas facetas de racismo. Um deles é o racismo institucional, mecanismo que operacionaliza (ainda que de forma inconsciente) um sistema de práticas institucionais destinado a promover uma estabilidade social que orienta a atividade de sujeitos inseridos em estruturas que determinam, direta ou indiretamente, desvantagens e privilégios orientados por estereótipos raciais. Trata-se de um mecanismo associado à distribuição e a disputa do poder, que dependendo da forma como ele se expressa na sociedade garante a hegemonia de grupos raciais em posições de poder que invariavelmente suscitam conflitos ligados a aspectos como a estratificação social.

Por outro lado, Almeida (2018) argumenta sobre a expressão do racismo estrutural como um fenômeno que se desenvolve a partir de práticas discriminatórias (individuais e institucionais) associadas à disputa do poder e a ordenamento social derivado destes conflitos. Dito de outra forma, as expressões institucionais que promovem o controle social do poder por parte de grupos raciais existem porque elas fazem parte de uma estrutura que as permite atuar desta forma. A mera existência de comportamentos individuais e institucionais baseados na diferenciação racial como norma constitui o cenário que nos permite inferir que o racismo não é apenas uma característica localizada observada no contexto social, ele faz parte da estrutura social ampla que se manifesta de diferentes formas. As microagressões[30] (Sue, 2010) que afetam as comunidades marginalizadas ilustram como comportamentos individuais ligados a discriminação racial são socialmente normalizados, por exemplo, quando uma pessoa demonstra sentir-se ameaçada ao partilhar um ambiente com indivíduos negros ou latinos, ou quando estes mesmos indivíduos se tornam alvos de anedotas que fazem associações pejorativas como comparações com animais, ou com trabalhos de qualidade inferior. Estas interações exibem a forma como a raça persiste ligada a um determinismo biológico (ou étnico), e que através das microagressões, envia mensagens negativas aos que se tornam objeto de uma estrutura social racista.

[30] Derald Wing Sue (2010), professor de Psicologia explora a idéia das microagressões e a maneira como estes comportamentos impactam negativamente comunidades alvo deste tipo de agressão que partem do comportamento individual na sociedade norte americana.

Assim sendo, a combinação de processos institucionais e comportamentos individuais que partem da noção de raça com premissas deterministas compõe o cenário através do qual o racismo estrutural se torna um fenômeno que deve ser ponderado nos debates que suscitam a questão racial como fonte de conflitos também no ambiente tecnlógico, pois a dimensão relacional e histórica ligada a interpretação da raça evidencia que o exercício do poder baseado na hierarquização racial resulta em desdobramentos "socialmente tóxicos" para certos grupos, e a constatação destes desdobramentos reforça a necessidade de se fomentar reflexões centradas em promover práticas antiracistas que busquem minimizar os impactos negativos do racismo estrutural nas sociedades contemporâneas.

Uma vez que o contexto relacionado ao desenvolvimento e a aplicação de tecnologias da informação toca em aspectos que intersectam múltiplos agentes do ponto de vista social (utilizadores, empresas e instituições), passaremos para a análise das dinâmicas de vigilância ligadas ao tema do Reconhecimento Facial, onde veremos que os impactos sociais ligados ao uso destas tecnologias expõem as sociedades vigiadas a questões de privacidade e segurança de forma diversa, e a continuidade de processos que ainda interpretam as questões ligadas à raça transposta ao universo tecnológico criam níveis de danos adicionais às populações impactadas pelo racismo estrutural, como veremos nos seguintes capítulos.

Capítulo 2: Segurança e vigilância – A mediação da tecnologia na temática da segurança

O uso de tecnologias preditivas com respeito à temática da vigilância em vídeo é um elemento essencial nos debates sobre os impactos da Inteligência Artificial em contextos sociais, sobretudo porque os recursos de Reconhecimento Facial acoplados a estes sistemas são mecanismos que ampliam e sofisticam a vigilância de ambientes classificados como suspeitos. No entanto, como argumenta Woodrow Hartzog[31], é necessário ter cautela com a temática do Reconhecimento Facial uma vez que a lógica subjacente torna indivíduos antes tidos como "inocentes a priori" em indivíduos "ainda não culpados por um crime", impondo uma lógica de desconfiança constante relativamente à segurança de ambientes vigiados e, moldando (de forma consciente ou não) uma espécie de desconfiança seletiva sobre determinados grupos. Tobias Matzner (2016:200) alerta para a maneira como sistemas de vigilância beneficiam de informações pessoais sistematicamente coletadas e agregadas no cotidiano através do uso, por exemplo, de *smartphones*. O autor chama ainda a atenção para questões envolvidas no que designa como "Vigilância como Suspeita", ideia em que se sublinha o caráter performativo que os dados digitais ganham sob a influência do *Big Data*[32], que critica a

[31] Ver *Facial Recognition is the perfect tool for oppression.* Portal Medium.

[32] *Big data* no contexto dos estudos de vigilância pode ser compreendido como a articulação de três fatores principais: A tecnologia e o uso de algoritmos para coletar, analisar e classificar grandes quantidades de dados; o processamento que trata das análises que identificam padrões de acordo com a finalidade para qual um determinado algoritmo será utilizado; a crença no discurso de que a análise de grandes quantidades de dados

maneira como são criadas subjetividades pacíficas e suspeitas a partir de técnicas de análise e classificação de dados de forma hierarquizante. Antes de entrarmos neste terreno torna-se necessário pensar criticamente sobre a noção de segurança e as diversas formas como o conceito se apresenta nos estudos de vigilância.

O monitoramento por câmeras de vídeo é uma questão amplamente estudada pelas ciências sociais por meio dos *Surveillance Studies,* sobretudo por abordar a temática da segurança e do uso de tecnologias de monitoramento para o combate a ameaças que coloquem em risco membros de uma sociedade ou mesmo de todo um Estado (Marx, 1988 e Lyon, 1994). Eventos como os atentados terroristas de 11 de setembro de 2001 nos Estados Unidos potencializaram esta discussão num plano internacional, por um lado, em virtude dos traumas causados por conta da violência como o país foi surpreendido, e por outro lado, devido aos desdobramentos que surgiram em torno da resposta do então presidente George W. Bush com "A guerra ao terror". Esta data ficou marcada na história por demonstrar a vulnerabilidade do país quanto a eventuais ataques com grande poder destrutivo na altura, e deu novas interpretações ao conceito de segurança num plano internacional. Porém, como podemos definir o conceito de "segurança"?

Ou melhor, será que segurança é um conceito passível de se enquadrar num conjunto de formulações fixas e imutáveis, ou será esta uma noção de caráter flexível, que varia de acordo com os arranjos culturais e políticos de um determinado local, e cuja influência de discursos e práticas e experiências pode criar diferentes interpretações?

A segunda opção enquadra-se na perspectiva desta investigação por fazer referência ao que Daniel Goldstein chama de uma "Antropologia Crítica da Segurança", ou seja, uma abordagem que procura reconhecer a influência de discursos e práticas articuladas com a temática da segurança em âmbito global e local, por contraponto com a noção de segurança como algo estritamente ligado à defesa do Estado, ou relegada a assuntos militares. Pensar no conceito de segurança seguindo a perspectiva de Goldstein (2010:490) remete-nos a revisitar formulações de pensadores da antiguidade como Thomas Hobbes (1651) e a visão de que era papel do soberano garantir a segurança do Estado diante das ameaças motivadas pela "guerra de todos contra todos" fundada na concepção de estado de natureza Hobbesiano, e na ausência de estruturas sociais formalizadas no século XVII (sociedade civil), que faziam com que a noção de segurança se baseasse na centralização do poder do soberano e no medo quanto às eventuais ameaças provenientes de instabilidade, mesmo que isto estivesse condicionada à renúncia de certas liberdades.

De forma similar, porém pensando sob uma perspectiva com inclinação liberal, segundo Corey Robbin[33] (2004), as proposições de Montesquieu relativas ao governo e à proteção do Estado pautavam-se pela presença de instituições e indivíduos que competiam entre si para estabelecer um

resulta numa forma avançada de inteligência até então desconhecida (Boyd, 2012: 2 apud , Lott e Cianconi, 2018).

[33] Apud Goldstein, 2010:490.

equilíbrio de poderes, e evitar os abusos cometidos pelas monarquias absolutistas do século XVII. Neste sentido, o medo também se torna um elemento em destaque quanto à segurança do Estado, ainda que desta vez se trate de um medo relativo à ameaça despótica de um Estado centralizador, e do eventual poder absoluto conferido ao soberano. Situando a discussão no contexto das sociedades industriais, Karl Marx (1967) defendia que o medo e os conflitos sociais derivavam da lógica do espírito do capitalismo, e do processo que transformou os indivíduos em sociedade em seres que priorizam uma interminável competição pela produção de riqueza individual. De acordo com James Der Derian (2009), esta alienação produzida pela lógica capitalista tem influência direta na concepção de segurança neste contexto, sobretudo diante da postura adotada pelas sociedades industriais no que se refere a garantir a proteção de riquezas e propriedades (apud Goldstein, 2010: 491).

Recuperar estas formulações nos ajuda a notar, por um lado, a relação histórica entre medo, segurança e governança, e os diferentes arranjos que fez da proteção do Estado e das sociedades uma temática estratégica para o crescimento do Estado. Para além disso, as diferentes articulações da noção de segurança evidenciam a flexibilidade do conceito, permitindo-nos pensar em nela sem associá-la diretamente a conflitos armados ou ameaças bélicas, expandindo o debate sobre o tema para além da esfera militar. Neste sentido, expandir o conceito de segurança remete-nos para o surgimento de políticas liberais no século XX, tendo em conta o surgimento de organizações internacionais que trabalham com uma proposta de segurança ampliada, com base no princípio do esforço conjunto de nações parceiras cuja união se justifica por propor um compromisso coletivo assumido pelos países membros da Organização das Nações Unidas para combater ameaças de cunho totalitário, e evitar calamidades políticas e sociais similares às da II Guerra Mundial. Esta estratégia alterou os parâmetros estabelecidos sobre segurança, pois incluiu a participação de instituições supranacionais, dando-lhes poder de agência na eventualidade de conflitos. Porém, a real expansão do conceito de segurança ocorre na medida em que políticas econômicas neoliberais se tornam mais abrangentes, fazendo com que segurança também se refira ao estado de "segurança humana" definido pela ONU (UN, 1994 apud Goldstein 2010), relacionando-a com níveis de governança, por exemplo, ao nível de segurança de emprego, de saúde e de educação nos limites de uma nação.

Com esta flexibilidade conceitual, e pensando na proposição de uma antropologia crítica da segurança, esta investigação adota uma abordagem reflexiva que analisa criticamente a esfera discursiva com influência na temática da segurança no interior do Estado, incluindo a voz ativa de indivíduos e grupos que reconhecem as inúmeras possibilidades que o debate proporciona do ponto de vista social (Goldstein, 2010:491-2), com especial foco nos aspectos que relacionem os impactos da vigilância mediada por tecnologias de monitoramento em espaços públicos que implicam em processos de hierarquização social, e que envolvem a problemática do viés algorítmico inerentes aos sistemas de Inteligência Artificial e Reconhecimento Facial. Esta mesma flexibilidade do conceito de segurança nos permite destacar o crescente uso de tecnologias que se converteram em práticas de vigilância normalizadas nos contextos sociais a partir dos ataques terroristas de 2001, bem como as

revelações feitas por Edward Snowden[34] em 2013 a respeito do uso de informações pessoais feita por agências governamentais que ampliou significativamente o monitoramento de populações.

A vigilância tradicional de caráter externo, ligada a noção de estratégias geopolíticas e militares passa a ter como aliada práticas que pretendem administrar conflitos internos pautados pela constante coleta de dados, sobretudo a partir do fim do século XX quando as agências estaduais nos Estados Unidos e Canadá ampliam as relações com empresas de tecnologia que permitem o monitoramento constante de populações, algo frequentemente forjado na ideia de governança e pacificação da população (Lyon 2019). Este cenário de vigilância interna se amplia e torna-se mais complexo na medida em que novas tecnologias da informação são desenvolvidas tornando a vida social (e privada) cada vez mais transparente aos olhos das forças de segurança, um cenário que apresenta desafios ligados as questões de privacidade na medida em que a vigilância de locais públicos e semi-públicos (e.g. através de câmeras de vídeo) ganha recursos que processam dados biométricos com o objetivo de identificar indivíduos[35].

O uso de técnicas de vídeo vigilância *(CCTV)* se tornou um instrumento comum nos centros urbanos, em parte motivado por discursos que promovem esta prática para conter o aumento da criminalidade e promover uma maior sensação de segurança, porém o uso deste recurso nem sempre representa um avanço no que se refere à melhoria da segurança pública, sobretudo em locais onde a idéia de insegurança está associada a questões relativas a conjunturas políticas e econômicas, e não necessariamente a presença comprovada de ameaças ou de dados sobre a criminalidade[36]· Contextos específicos requerem soluções e instrumentos que estejam conectados com a realidade local, e o uso de câmeras de *CCTV* como alternativa padrão pode não ser a única resposta viável a todos os contextos.

[34]David Lyon (2014) aborda o impacto das revelações feitas por Snowden quanto a maneira como a National Security Agency (NSA) norte americana obteve acesso a metadados de utilizadores de serviços de telecomunicação, bem como de redes sociais como Facebook e Google para ampliar a capacidade de vigilância nacional. O acesso a dados pessoais combinado com técnicas de Big data de analisar, classificar e estabelecer correlações a partir do cruzamento de dados possibilita as agências de segurança a rastrear indivíduos de forma intrusiva, e evidencia como as tecnologias da informação se mostram eficientes aliados em matéria de vigilância, ainda que nem sempre esta relação esteja evidente aos utilizadores.

[35] Importa ressaltar a definição de dados biométricos presente no artigo 4º, ponto 14 do GDPR qunto a imagem facial como *uma* das possíveis formas de identificar indivíduos *"*Dados biométricos são dados pessoais resultantes do processamento técnico específico relacionado às características físicas, fisiológicas ou comportamentais de uma pessoa física, que permitem ou confirmam a identificação única dessa pessoa física, como imagens faciais ou dados dactiloscópicos"

[36] A instalação temporária de câmaras de CCTV em Portugal, proposta inicialmente em 2005 é um caso que ilustra a presença de fatores ideológicos que influenciaram o espectro político para atender demandas relativas à insegurança de setores específicos, mesmo sem a presença de indicadores estatísticos suficientes que justificassem este projeto. A ausência de indicadores de criminalidade foi sobreposta por reivindicações de insegurança feitas por um setor (associação comercial) que influenciou a conjuntura política em 2007 a instalar câmeras de vigilância no centro histórico da cidade do Porto, impactando a rotina de vigilância e a relação da polícia com a comunidade local. O projeto causou desacordo entre os diversos setores impactados direta e indiretamente, e em 2011 teve a renovação vetada pela Autoridade de proteção de dados diante da evidência de que, para além das câmeras não ajudarem as tarefas das forças policiais, a operação e a manutenção delas representava um custo significativo para a cidade, assim sendo, elas foram desativadas (Frois, 2014: 45-61).

Evidentemente o objetivo desta investigação não é propor que a vídeo vigilância seja uma prática descartável, uma vez que ela se justifica em contextos sociais influenciados pela presença de organizações criminosas que de facto exigem a presença das forças policiais de forma intensa, servindo como um recurso estratégico para mapear localidades que a presença física da polícia não alcança. Porém, é importante ter em conta que a utilização deste recurso sob a influência de contextos que não representam a realidade local, ou que promovem discursos que acentuam o medo excessivo sobre crimes não detectados pode legitimar o uso de práticas de vigilância de forma desnecessária (e custosa), por conta de fatores ideológicos quanto à securitização de ambientes externos que invertem pressupostos básicos legais quanto à inocência dos indivíduos, impactando a realidade social local (Frois, C. 2014: 50).

Ainda que utilização da vídeovigilância tenha como pressuposto a idéia de consentimento tácito, o processamento de informações biométricas feito por empresas privadas para as autoridades policiais é algo que deve ser problematizado nos debates públicos, sobretudo diante da existência de mecanismos de proteção de dados digitais específicos, como é o caso do GDPR (*General Data Protection Regulation)* na Europa, que controla as práticas relacionadas à proteção de dados na região, uma vez que o processamento de informações biométricas realizado sob o slogan da segurança pode converter-se em uma prática que fere os direitos de privacidade individual e impactar valores democráticos.

Vídeo vigilância, Reconhecimento Facial e processamento de dados biométricos

A importância de um debate inclusivo sobre a prática do Reconhecimento Facial como um recurso de vigilância reforça as recomendações[37] do *AI Report 2019* em torno dos impactos do uso desta tecnologia em contextos sociais, e sugere que empresas e governos que vislumbrem trabalhar com este recurso em contextos sociais interrompam ou adiem tal projeto até que existam mecanismos de regulamentação dedicados à temática da vigilância, ou até que os riscos inerentes ao seu uso sejam estudados de forma exaustiva (Crawford *et al*, 2019:06). O uso do Reconhecimento Facial em rotinas de vigilância tende a criar violações de privacidade, sobretudo porque o processamento de informações biométricas não conta com o consentimento explícito decorrentes das imagens capturadas, por exemplo, em filmagens de ruas ou de estabelecimentos comerciais. Ou seja, nestes contextos, o processamento e o armazenamento compulsório destas informações convertem-se num processo autoritário que visa promover a segurança de ambientes, e, ao contrário de outras tecnologias

[37] Dentre as recomendações do relatório sobre o uso de tecnologias de Inteligência Artificial e Reconhecimento Facial em contextos sociais cabe-nos destacar as seguintes: Promover mudanças estruturais na indústria da Inteligência Artificial incluindo o combate ao racismo sistêmico, e promover um ambiente diverso nos setores que desenvolvem estas tecnologias; Reconhecer que a problemática da Inteligência Artificial aplicada em contextos sociais requer ir além da busca por respostas para questões técnicas; Promover ambientes que permitam que os desenvolvedores conheçam a finalidade para qual uma determinada tecnologia foi criada; A regulamentação das questões de vigilância que articulam a utilização de sistemas privados em ambientes públicos, e a devida responsabilização às empresas que causam danos a comunidades submetidas ao uso desta tecnologia de forma compulsória e pouco transparente (Crawford *et al*, 2019:06-09)

de identificação biométrica como a análise da íris, palma da mão e impressão digital – processos que dependem da ação voluntária do individuo (Mingtsung e Lu Cai, 2020: 23) – o uso de câmeras que possibilitam o Reconhecimento Facial compulsório operado por dispositivos de segurança não oferece ao indivíduo a possibilidade de consentir as atividades posteriores à recolhade imagens. O exemplo do contexto europeu ilustra a maneira como este tipo vigilância deve atender requisitos específicos na região para ser colocada em prática.

O artigo 35º do GDPR prevê que o monitoramento sistemático de locais públicos se entende como uma "operação de alto risco" sempre que ele envolva o processamento de informações pessoais que resultem em eventuais riscos aos direitos e às liberdades individuais. Para além disto, o artigo prevê o estabelecimento de avaliações de impacto da proteção de dados como uma prática que visa controlar a conformidade de atividades de alto risco que devem detalhar os tipos de processamento de dados utilizados, bem como o tipo de consentimento que fundamenta esta atividade do ponto de vista legal[38], e estas avaliações devem ser realizadas mesmo quando há duvidas quanto a evidência de risco às liberdades e direitos individuais (Barnoviciu *et al* 2019)

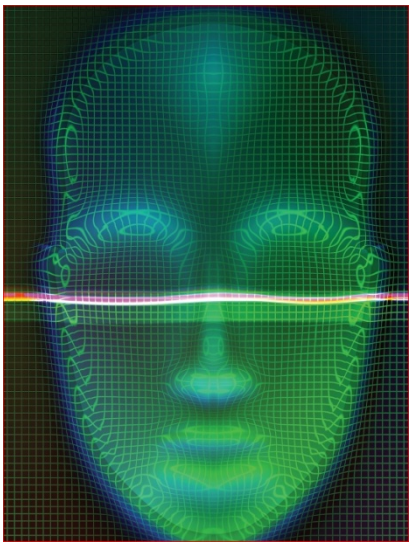
Além da problemática quanto ao consentimento, outro tema que levanta preocupação referente ao uso do Reconhecimento Facial para fins de vigilância reside no fato destes sistemas utilizarem recursos estatísticos para extrair as características individuais no processo de detecção e reconhecimento de indivíduos, pressupondo o mapeamento de modelos faciais na busca por traços faciais únicos que o sistema orienta para reconhecer indivíduos. Este processo assemelha-se com uma tradição científica familiar à antropologia desde os fins do século XIX, a Antropometria[39], campo que nasce a partir de concepções quanto a um determinismo biológico interligado a questões comportamentais que utilizava técnicas que pretendiam explicar as diferenças entre homens, mulheres, pessoas de pele branca e negra a partir de características biológicas para atribuir comportamentos natos a cada um desses indivíduos. Um âmbito onde esta tradição se desenvolveu consideravelmente na altura foi o da identificação criminal, tendo como base a ideia de que aspectos físicos e fisiológicos poderiam ter influência na conduta criminosa de indivíduos considerados perigosos (Madureira, 2003:287-288).

O estudo de aspectos físicos com o objetivo de identificar comportamentos delinquentes compromete o eventual uso de Reconhecimento Facial no que se refere à vigilância, pois evidencia um aspecto ligado a históricos problemáticos do ponto de vista ético tais como a eugenia e a hierarquização do homem a partir de características físicas, que fazem referência a publicações como a de Cesare Lombroso *L'uomo delinqüente* (1876) e suas afirmações biodeterminantes, por exemplo, ao

[38] O GDPR lista os tipos de consentimento previstos que regulamentam estas atividades, são eles: 1) consentimento explícito e específico, 2) consentimento contratual, 3) consentimento para cumprir com obrigações legais, 4) consentimento necessário para proteger interesses vitais, 5) consentimento necessário para questões de interesse público e 6) consentimento necessário para propósitos de interesses legítimos (GDPR, 2016, Artigo 6º: ponto 1).

[39] "A Antropometria é a designação atribuída à estatística do corpo" (Madureira, 2003: 284)

comparar o cérebro de criminosos com o cérebro de homens "primitivos", ou mesmo nas afirmações de que "frontais desenvolvidos, orelhas largas, caninos proeminentes e maxilares protuberantes tornam-se características físicas identificadoras da predisposição para a delinquência" (Madureira, 2003:288). O posicionamento atual da Antropologia contemporânea e das ciências sociais rejeita estas dinâmicas hierarquizantes, e critica este tipo de práticas discriminatórias, bem como o uso de dispositivos de segurança opressivos por parte do Estado (Maguire *et al* 2014). Contudo, se pensarmos nesta dinâmica mediada pela tecnologia da informação, onde empresas privadas disponibilizam sistemas que traçam um mapeamento estatístico facial automatizado capaz de identificar indivíduos em ambientes externos, e que estes sistemas podem ser utilizados para maximizar o desempenho das autoridades de segurança a partir de premissas pouco éticas sobre a estatística do corpo, e pouco precisas do ponto de vista técnico, cria-se o enquadramento que nos permite questionar o papel da tecnologia enquanto ferramenta que instrumentaliza o Estado, sobretudo quando estes dispositivos tendem a ser desenvolvidos e comercializados para fins militares[40] (Crawford *et al*, 2019: 42-43).



Fonte: Stark, 2019

A Vigilância fora do escopo do GDPR

As condições sobre as quais ocorre o entrelaçamento entre tecnologia da informação, vigilância e relações de poder expõem um aspecto da inovação tecnológica que toca em questões éticas relativas ao desenvolvimento de modelos de *Machine Learning*. Esta intersecção promove, de forma consciente ou não, práticas que produzem danos de natureza individual e coletiva adicionais a grupos específicos, nomeadamente grupos de afrodescendentes, latinos ou comunidades socialmente estigmatizadas. No

[40] O *AI report* chama atenção sobre a corrida armamentista da Iinteligência Artificial entre EUA, China e Rússia que criou uma competição entre estes países quanto ao desenvolvimento de tecnologias de Iinteligência Artificial para usos militares, bem como sinaliza possíveis parcerias entre as empresas de *Silicon Valley* e as autoridades militares norte-americanas, parcerias que envolvem interesses comerciais e militares relacionando diversas estruturas de poder ligadas ao desenvolvimento técnico-científico, permitindo-nos confirmar que a tecnologia neste contexto não é um elemento neutro neste debate.

caso específico de afrodescendentes, Simone Browne (2015) explora a idéia de Epidermalização[41] como um mecanismo que impõe um olhar racializado nos corpos destes indivíduos, e cria um processo de vigilância que dá forma ao que a autora chama de "vigilância racializada", ou seja, uma técnica de controle social pautada por práticas que hierarquizam indivíduos a partir do tom de pele, tal como ocorria na altura em que os regimes coloniais eram socialmente aceites e posicionavam a classe detentora de poder político e econômico no topo de uma suposta escala racial. Assim, a vigilância racializada, além de ter em conta a cor de pele de quem observa (e de quem é observado), também considera(va) outros aspectos como classe, sexo e etnia (Browne, 2015:16-17) para criar um sistema desumanizado e opressor que favorecia exclusivamente o interesse das classes dominantes, em detrimento da objetificação de grupos inferiorizados com consequências que se prolongam nas interações sociais (discriminação racial e étnica) ainda hoje.

Situando a discussão num plano mais atual, o fato de que interesses políticos, económicos e militares se articulam com fatores que impulsionam a inovação tecnológica em nome de uma corrida armamentista toca diretamente nas questões de segurança e, para além disso, a homogeneidade racial dos profissionais responsáveis pela ética nestes ambientes[42] torna-se problemática uma vez que a busca por valores éticos globais envolve o trabalho conjunto de indivíduos que não experimentam as injustiças promovidas pelos impactos causados pelas tecnologias mais recentes. Isto significa que aqueles que detêm o poder técnico e financeiro de elaborar premissas éticas - ao não experimentarem o mundo de forma diversa - criam provisões incapazes de perceber os danos que afetam grupos pouco representados neste ambiente, o que possivelmente constrói premissas sistêmicas insensíveis a demandas mais específicas em sistemas que serão comercializados para monitorar populações de forma generalizada.

Neste sentido, abordar o fenómeno do Reconhecimento Facial como um objeto de estudo para discutir criticamente a temática da segurança e da vigilância na contemporaneidade tem um valor singular, pois recuperar aspectos hierarquizantes que no passado foram responsáveis por submeter milhares de indivíduos as mais diversas atrocidades durante séculos permite-nos argumentar de forma criteriosa sobre o avanço tecnológico baseado em continuidades históricas, que e em nome de discursos que promovem a segurança pública mediada por dispositivos tecnológicos, propõe o estabelecimento de um estado de monitorização permanente que atinge diferentes grupos sociais de forma desproporcional. Ainda que a relação entre o passado colonial e o uso das tecnologias da informação pode não ser evidente, a maneira como os desenvolvimentos do setor fazem uso de

[41] *Epidermalization* é um termo utilizado por Frantz Fanon (1952) na obra *Black skin, White mask* e faz referência à dinâmica discriminatória imposta pela maneira como indivíduos afrodescendentes eram (e continuam a ser) objetificados de forma pejorativa pelo olhar pautado pelas dinâmicas discriminatórias do colonialismo (apud Browne, 2015: 7)

[42] A questão da pouca diversidade nos ambientes laborais (maioria de indivíduos brancos) quanto ao desenvolvimento de princípios éticos é mencionada na publicação que trabalha a idéia dos *Ethic owners,* profissionais responsáveis por elaborar práticas organizacionais que promovam valores éticos no interior das empresas de tecnologia. Ver *Ethic owners A new model of organizational responsibility in data-driven technology companies* (Moss e Metcalf 2020).

técnicas como a leitura facial geométrica, e a forma como as informações pessoais são utilizadas de forma exploratória nos permite estabelecer uma semelhança entre ambos os processos.

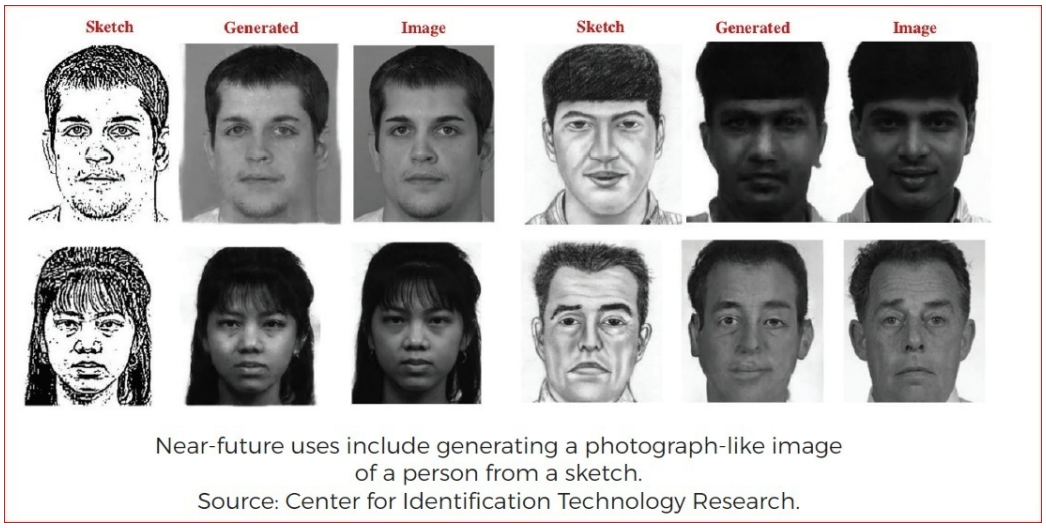
Observemos alguns indicadores obtidos do relatório *Face off* (Lynch, 2018:19) que ilustram um rápido avanço quanto ao uso de dispositivos de Reconhecimento Facial por parte das autoridades policiais norte-americanas, e evidenciam o desejo de vigilância constante na sociedade contemporânea com grande presença de dispositivos tecnológicos. O relatório aponta para o eventual acesso do *FBI* [43] a imagens publicadas em redes sociais bem como de gravações de câmeras *CCTV* na busca por suspeitos. Esta possibilidade amplia substancialmente a visibilidade da polícia sobre indivíduos de forma não consentida, e pode aumentar o banco de imagens desta entidade[44] de maneira indiscriminada, pois um indivíduo que aceita os termos de privacidade de uma rede social, ou que caminha por uma rua sem saber que está a ser gravado, não conta com a possibilidade de que suas informações pessoais sejam utilizadas para fins de segurança nacional.

Outro indicador sinalizado pelo relatório que reforça este estado de vigia constante refere-se a projetos ainda mais ambiciosos que pretendem incorporar vestimentas dotadas de câmeras utilizadas por oficiais nas rotinas de patrulhamento *(Body worn cameras)* que permitem gravar operações policiais e reconhecer modelos faciais em tempo real, e desenvolver sistemas que permitem o Reconhecimento Facial em condições extremas como filmagens noturnas e com pouca visibilidade. O relatório chama também a atenção para projetos que propõem a utilização de sistemas capazes de "interpretar" imagens de pessoas em idade infantil ou a partir de retratos falados policiais, e em seguida traçar o seu retrato em idade adulta, além de sistemas de identificação orientados por questões de gênero, posicionamento político e eventual predisposição a crimes a partir do histórico de atividades suspeitas (Lynch, 2018: 21-22). Estas capacidades permitem-nos inferir que a tecnologia, quando proposta nestes contextos, atinge um grau de intrusão excessivo se pensada sob a perspectiva da normalização da vigilância integrada[45] como uma forma de monitorar a segurança de populações.

[43] *Federal Bureau ofinvestigation*, a principal agência de investigação criminal do departamento de justiça nos Estados Unidos.

[44] O *Next Generation Identification (NGI)* é o banco de dados biométricos utilizado pelo FBI operado por algoritmos que realizam o Reconhecimento Facial a partir de uma base de aproximadamente 30 milhões de fotos, e o FBI intitula como o maior e mais eficiente repositório de informações biométricas do mundo. Acedido em 20/10/2021. Disponível em: https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi

[45] O termo vigilância integrada será utilizado para fazer referência às técnicas de vídeovigilância dotadas do recurso de Reconhecimento Facial, ou seja, o processo de vigiar e reconhecer de forma automatizada.



Fonte: Lynch, 2018: 22. Os usos em um futuro próximo incluem a geração de uma imagem semelhante a uma fotografia de uma pessoa a partir de um esboço. *Face off Law enforcement use of face recognition technology*.

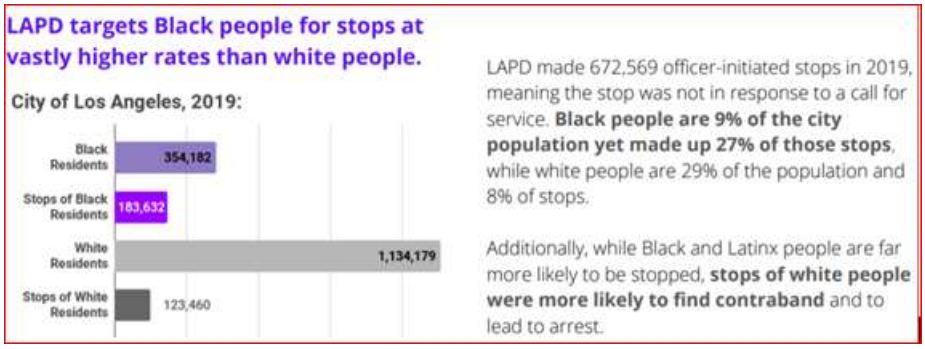
A análise dos indicadores que exploram o uso de técnicas de Reconhecimento Facial por parte das forças de segurança transporta-nos para um nível de instrumentalização policial antes pensado em filmes de ficção científica futurista, e que dia após dia torna cada vez mais próximo um estado de vigilância integrada. O uso deste tipo de vigilância sem a devida regulamentação em termos de privacidade, combinada com a problemática dos efeitos negativos do viés algorítmico e da vigilância racializada, funcionam como combustível para promover uma reflexão crítica sobre a maneira como as empresas de tecnologias e as autoridades policiais articulam os seus interesses sem equacionar os contextos em que estes dispositivos serão incorporados, ou os eventuais danos que estes processos ocasionam.

Simone Browne (2015) elucida as tensões relativas à vigilância nos momentos em que a comunidade afro-americana é desproporcionalmente abordada por oficiais de patrulha ao serem parados, por exemplo, ao conduzir, ou as frequentes abordagens feitas pela polícia de Nova Iorque *(stop-and-frisk)* que ocorrem em maior número com indivíduos de pele negra em virtude da visão estereotipada das forças policiais sobre esta comunidade, cujo olhar costuma interpretar a presença destes indivíduos como potenciais criminosos (2015:13) [46]. Este olhar que estereotipa afroamericanos como alvos de vigilância também se observa no contexto canadiano, quando em meados de 1970, as forças de segurança de Montreal (RCMP[47]) decidem infiltrar o agente Warren Hart nos protestos que promoviam o empoderamento da comunidade negra e a luta por igualdade, o que para as forças de segurança na altura serviu de justificativa para estabelecer estratégias de vigilância sobre indivíduos considerados radicais, ou potenciais transgressores dos ideais da sociedade canadiana, ainda que na altura as políticas de multiculturalismo no país defendiam a igualdade de tratamento a todos os

[46] De forma similar, Didier Fassin (2013) analisa este cenário relativamente à vigilância de grupos marginalizados na periferia de Paris. Ver *Enforcing order: An ethnography of urban policing.*

[47] Royal Canadian Mounted Police.

cidadãos, pelo menos do ponto de vista institucional (Tecle *et al*, 2017). A ideia de vigilância racializada também se observa na menção feita pelo *AI report* (Crawford *et al*, 2019:25) ao destacar a suspensão do sistema de policiamento preditivo *LASER*[48] como resultado movimentos comunitários da região de Los Angeles que detectaram uma tendência discriminatória relativamente a interação da policia com a comunidade afro-americana em comparação com as abordagens feitas a indivíduos brancos. Segundo dados do ano de 2019[49], a população negra que representava 9% do total de residentes figurou em 27% das abordagens feitas, enquanto a população de pele branca, que representava 29% do total de residentes teve um índice de abordagens de apenas 8%:



Fonte: Stop LAPD spying Coalition, 2019. O LAPD tem como alvo os negros em taxas muito mais altas do que os brancos. *LAPD confirma criminalização contínua e assédio à comunidade negra.*

Estas questões podem não ser evidentes para quem não as experimenta diariamente, porém causam impactos e traumas a nível social e psicológico nesta população, pois limita os direitos civis de indivíduos que experimentam o racismo de forma sistemática. Neste sentido, pensar na instrumentalização do patrulhamento policial por via do uso de sistemas de policiamento preditivos implantados em contextos socialmente diversos implica, a priori, identificar questões que afetam negativamente o cotidiano das diferentes populações, primando para que visões racializadas não interfiram nas liberdades dos indivíduos de forma injusta e intrusiva, evitando cometer erros de um passado ainda não totalmente reparado. Para tal é importante que se criem mecanismos que regulamentem o uso destas tecnologias, em particular as que fazem uso do processamento de dados biométricos como o Reconhecimento Facial. Porém, ao contrário da realidade europeia que conta com a presença ampla do *GDPR*, a temática da privacidade digital no contexto norte-americano tem especificidades em virtude da autonomia conferida a cada Estado federal em regular internamente as suas questões, e esta particularidade, como veremos nas próximas secções, dificulta o debate que procura construir premissas que visem regular a privacidade digital no país.

[48] O *LASER (Los Angeles Strategic Extraction and Restoration)* é um sistema de policiamento preditivo cuja operação foi suspensa após uma série de reivindicações feitas por comunidades locais que denunciaram a forma desproporcional como os afro-americanos e latinos são discriminados. The Los Angeles Times.

[49] Dados obtidos da pesquisa realizada em 2019 pelo *Stop LAPD Spying Coalition*, um grupo organizado de Los Angeles que luta pela descriminalização e pelos direitos civis da população afro-americana.

O uso de sistemas preditivos no patrulhamento

A utilização de recursos de policiamento preditivo nos Estados Unidos é uma prática que vem sendo incorporada como alternativa para sofisticar as rotinas de patrulhamento policial sob o discurso de que o uso desta tecnologia ajuda a prever e evitar atividades criminosas ou suspeitas de forma eficiente devido ao caráter automatizado em que as informações são analisadas, o que em tese possibilita uma resposta mais rápida da corporação na incidência destes eventos, criando uma dinâmica menos tendenciosa nos processos decisórios uma vez que o que antes era operado pela atividade humana passa a ser gerenciado de forma "neutra" por sistemas eletrônicos. No entanto, a maneira como a tecnologia da informação adentra o terreno da vigilância altera substancialmente a dinâmica operacional de patrulhamento. Aquilo que antes pertencia ao domínio da estratégia policial pensada para situações específicas passa a ser desenvolvido por setores privados orientados pela lógica do livre mercado, e pela suposição de que qualquer indivíduo é um potencial suspeito. Esta relação que envolve o setor privado nas decisões automatizadas em função de algoritmos se intensifica quando projetada para a temática da vigilância, pois através de técnicas sofisticadas de classificação de dados, oferecem-se soluções que, por um lado agregam e classificam dados agregados para mapear sequencias de factos, e por outro, utiliza tais técnicas para prever certos comportamentos, ou até intervir, ou antecipar a ocorrência de distúrbios. Todo este enquadramento se torna um fator problemático que impacta liberdades democráticas e redefine as relações de privacidade, sobretudo tendo em mente a forma como estas informações são obtidas pelas forças de segurança (Lyon, 2014: 4).

Assim sendo, determinar o quão suspeito cada indivíduo pode ser baseia-se no processamento de dados computadorizados relativamente, por exemplo, à localização de indivíduos, e se esta localização for categorizada como de "alto risco" para a segurança pública, é provável que a sugestão feita por este recurso resulte numa vigilância mais intensa desta localidade, porém o que torna este facto uma inquietação não é meramente a lógica sistêmica por trás disto, e sim, quem e como se definem graus de risco que determinam práticas de vigilância.

Se levarmos em conta a forma como os estereótipos raciais são impostos às comunidades marginalizadas, descarta-se qualquer caráter "neutro" em relação a esta alternativa para o patrulhamento, uma vez que a classificação destas informações, mesmo que automatizada, invariavelmente passará pela interferência humana no momento em que o histórico de atividades suspeitas indique uma localidade como um *hot spot*[50]. Para além disso, a maneira como as estruturas de vigilância se diversificam na atualidade onde a auto-vigilância se torna possível mediante ao uso de

[50] Refletindo comparativamente sobre a criação de identidades produzida no contexto da vídeovigilância, convém mencionar que "Um dos maiores riscos da vigilância contemporânea é deixar-se levar a pensar que é possível ter controle absoluto sobre os usos dados às informações que coletamos (às objetivações que produzimos). Na ausência de evidências que comprovem o contrário, nunca se pode presumir que não haverá corrupção, ineficácia, fraqueza humana, ganância ou atrevimento" (Pina Cabral 2008: 25 apud Frois, 2013:44).

smartphones cria a sensação de uma sociedade de segurança máxima, uma vez que recursos tecnológicos rotineiros permitem superar barreiras quanto ao acesso a informações de forma rápida e barata, algo como uma "sociedade transparente" (Marx, apud Browne, 2015:15).

Ainda que as estruturas de vigilância atuais assumam diferentes formas, o uso de técnicas de policiamento preditivo mediada por tecnologias da informação ganhou relevância na contemporaneidade, e neste sentido vale a pena fazer referência à publicação de Aaron Shapiro (2019) [51] que discute a maneira como o sistema de policiamento preditivo *Hunchlab* foi elaborado para criar previsões orientadas por históricos criminais no Estado da Filadélfia de forma automatizada.

Por norma, situamos a ideia de patrulhamento como uma tecnologia policial que racionaliza a função preventiva da polícia com o objetivo de prevenir atividades suspeitas, estabelecendo o controle policial logístico sobre áreas de potencial risco identificadas a partir da análise de históricos criminais, cujo desdobramento se verifica na organização espacial dos oficiais de patrulhamento no terreno, indo ao encontro de uma das principais funções estabelecidas para a polícia quanto à prevenção ao crime e a desordem[52]· Trata-se de uma técnica de segurança de caráter preventivo que desempenha a ação de vigilância que ao mesmo tempo em que observa, é observada; adicionalmente ela opera através de cartografias definidas que identificam padrões de comportamento e movimento de indivíduos (suspeitos ou não) que circulam nos espaços e tempos (horários) destacados, criando uma presença ubíqua da autoridade policial em pontos estratégicos para a manutenção da segurança pública urbana (Nail, 2015 apud Shapiro, 2019: 458-459).

Dado o estreitamento de relações entre as empresas de tecnologia e o setor militar nos EUA, o uso de tecnologias preditivas que visem tornar mais eficiente o desempenho policial no combate ao crime deixa de ser uma hipótese para se converter num facto, ou melhor, numa demanda que motiva as empresas a produzir tecnologias que pretendem reformular a lógica de patrulhamento através de análises algorítmicas. Porém, quando submetemos este cenário a uma análise crítica, esta proposição apresenta inconsistências que podem resultar em comportamentos discriminatórios por parte das forças policiais e aprofundar as conhecidas disparidades raciais e socioeconômicas.

Pensar no desenvolvimento de sistemas de policiamento preditivo significa pensar na transformação da maneira como as informações são manuseadas pelas forças policiais (através de empresas), e na conversão de históricos criminais em dados interpretáveis por algoritmos *(Big data)* que resultam em sistemas concebidos para calcular a probabilidade de crimes ocorrerem em localidades que apresentem potencial risco. Este processo, para além de identificar localidades potencialmente críticas, identifica também horários em que se verifica uma maior incidência de

[51] Artigo publicado em *Surveillance & Society* que aborda criticamente o discurso que apoia a reforma das rotinas de patrulhamento através do uso de sistemas de policiamento preditivo. Esta análise torna-se necessária visto que neste contexto o Reconhecimento Facial atua como um recurso acessório aos sistemas preditivos, que operam a partir de assunções similares as das tecnologias de Visão Computacional abordadas anteriormente.

[52] "O primeiro de nove princípios estabelecidos por Robert Peel em 1829 que diz: A missão básica para qual a polícia existe é de prevenir o crime e a desordem" (apud Shapiro, 2019: 458).

atividade suspeita de forma semelhante ao método de patrulhamento tradicional, exceto que, neste caso, todo o processo ganha um caráter automatizado e opera-se a uma velocidade bastante superior à capacidade humana de realizar esta tarefa (mais valia financeira). Esta dinâmica, na eventualidade de combinar recursos de Reconhecimento Facial, aproxima-se à noção de vigilância integrada e estabelece níveis de controle social que expõem certos grupos a vigilância intensa por conta de imaginários socialmente construídos em torno de determinadas localidades.

A análise de Shapiro consiste num trabalho etnográfico conduzido entre outubro de 2015 e maio de 2016 sobre o uso do sistema de policiamento preditivo *Hunchlab* durante a rotina de patrulhamento policial, um produto de uma empresa com base em Filadélfia[53] e desenvolvido para prever a ocorrência de crimes com o objetivo de tornar a resposta das forças policiais na ocorrência destes eventos mais rápida e efetiva. Na perspectiva do autor, esta utilização traduz-se em um discurso que visa racionalizar as técnicas de patrulhamento através de previsões pouco fundamentadas que impõem a reforma algorítmica como uma alternativa viável para o processo de patrulhamento policial. No entanto, este processo possui uma dinâmica ambivalente, pois ao mesmo tempo em que se codificam locais e comportamentos como suspeitos ou de risco, implicitamente estabelecem-se os locais e comportamentos normalizados e aceitáveis, ou seja, trata-se de uma dinâmica dialética que exclui e inclui, ou que distribui segurança e danos aos contextos sociais onde ela é utilizada por meio de práticas sociotécnicas de patrulhamento (Shapiro, 2019: 457) [54]. Assim, incorporar uma estrutura automatizada nestes contextos requer identificar os tipos de subjetividades que emergem dessas práticas, por exemplo, na construção de subjetividades pacíficas e criminosas dos espaços patrulhados, e reconhecer a limitação do trabalho executado no terreno pelos oficiais de patrulha nos moldes tradicionais, cuja solução viável passa por remediar tais práticas através de tecnologias que propõem um nível de eficiência e de justiça que nem sempre são comprovados antes de serem colocados em prática.

A atmosfera de dúvida sobre a real efetividade do sistema manifesta-se pela forma como se opera a previsibilidade proposta por ele. Basicamente o *Hunchlab* foi desenhado para ser operado pelo algoritmo *Predictive mission,* inicialmente financiado pelo governo norte-americano através do NSF *(National Science Foundation),* com o propósito de criar um modelo de *Machine Learning* capaz de prever as localidades potencialmente suspeitas na região, e conduzir as atividades de patrulhamento do departamento de polícia da Filadélfia a partir da análise de registros criminais anteriores, bem como de dados de caráter mais geral como censos, calendários escolares e eventos de lazer. Cria-se assim uma

[53] A Azavea é a empresa que planeou e desenvolveu o sistema Hunchlab, que posteriormente foi vendido para a empresa Shotspotter, uma empresa que trabalha em softwares direcionados a ajudar comunidades carentes e departamentos de polícia a combater a violência. Para maiores informações ver: https://www.azavea.com/blog/2019/01/23/why-we-sold-hunchlab/ Acedido em 20/10/2021.

[54] Podemos expandir esta análise utilizando a forma como a vigilância é interpretada no campo da visibilidade social. Neste contexto a vigilância age como uma prática que estabelece os limites daquilo que deve ou não se tornar visível através de práticas que moldam e transformam o contexto social, criando regimes de visibilidade que normatizam a atividade de vigilância (Brighenti, 2010: 151)

lógica sistêmica repleta de variáveis que se adequam ao objetivo central do contratante; um sistema sensível a variações espaciais e temporais (Shapiro, 2019: 462) que, no caso de um departamento de polícia, sugere antecipar a resposta das forças policiais para impedir a ocorrência de atividades criminosas por um lado, e por outro lado, codificar a presença de indivíduos nos locais considerados críticos como potenciais suspeitos, sobretudo se esta for uma prática que viabilize materializar o desejo de uma sociedade que normaliza a vigilância massiva em busca da sensação de segurança máxima (Norris, Clive e Gary Armstrong 1999).

A ocorrência de atividades suspeitas e de crimes vai auto-ajustando cada uma das variáveis do sistema que passa a identificar um local, ou um horário (ou ambos combinados) como mais ou menos propício à ocorrência de perturbações, algo que gradativamente desenha o mapa do patrulhamento e a forma como os oficiais são divididos em campo. Porém, ainda que este procedimento pareça ser extremamente sofisticado do ponto de vista tático, é preciso ter em conta que o que o sistema pretende devolver a partir das análises algorítmicas de dados anteriores são apenas *previsões*, ou seja, aproximações ou estimativas criadas a partir de informações criminais similares que sugerem eventos que podem vir a ocorrer ou não. Este regime, em si mesmo, cria uma lógica de incertezas sobre a incidência destes eventos que imputa ao sistema *Hunchlab* um fator de indeterminação que compromete o resultado proposto pela reforma das rotinas de patrulhamento (Shapiro, 2019:462-463).

A incerteza epistémica no funcionamento de sistemas de policiamento preditivo oferece-nos outra questão importante para esta investigação. A ideia da monitorização territorial faz referência à presença das estruturas mais amplas de poder que utilizam a tecnologia da informação para controlar a atividade de indivíduos em um determinado espaço e tempo. O controle territorial de localidades convoca a reflexão de que, por um lado trata-se de um sistema de controlo que opera em dois níveis: o primeiro é o controlo exercido no ambiente físico fazendo com que as forças policiais se desloquem efetivamente para conter, ou impedir eventuais distúrbios. O segundo é o controle digital que se estabelece a partir da posse de informações capturadas que podem ser utilizadas pelas empresas que gerenciam estes dados a qualquer momento. Uma vez que a relação entre o espaço físico e digital torna-se cada vez menos indiferenciada, e que o desejo de vigilância se torna um fator normalizado, podemos inferir a partir de uma perspectiva *decolonial*, que o controlo social que advém de práticas que exploram as informações pessoais faz referência a uma assimetria de poderes comparada a ideia de colonialidade estrutral[55]. Ao passo em que o uso de tecnologias da informação cria uma esfera digital interconectada, e que a maneira como fazemos uso dela habilita mecanismos de controle intrusivos, abre-se a possibilidade de que este controle se expanda de forma contínua tal como os regimes coloniais o fizeram. Desta forma, projetar este esquema para as relações digitais representa a

[55] O termo colonialidade será utilizado tendo em conta a noção de continuidade de um colonialismo forjado na maneira desproporcional como as relações de poder se manifestavam entre colonizadores e colonizados. Nesta abordagem, o histórico da expropriação de recursos e de indivíduos percebe-se como peça fundamental para os desdobramentos do mundo moderno "A colonialidade é aquilo que sobrevive ao colonialismo" (Ndlovu-Gatsheni, 2015 e Bhambra, 2018 apud Mohamed et al, 2020: 663)

continuidade de um sistema de práticas e valores ligados ao controlo social (e financeiro) que resiste até os dias de hoje. Dito de outra forma, a expansão territorialista evoca o que se define como "colonialidade algorítmica", termo utilizado para referir à presença de valores culturalmente cristalizados que influenciam as interações sócio-culturais e políticas modernas possibilitada pela continuidade de processos que advém do histórico colonial ocidental (Mohamed *et al*, 2019: 665-666).

Diante desta reflexão sobre a territorialidade, e a questionável previsibilidade de sistemas preditivos baseados em incertezas e indeterminações, a eficiência dos resultados apresentados por estes sistemas é colocada em causa, portanto pensar em incluir recursos de Reconhecimento Facial que incrementem este tipo de patrulhamento representa um risco ainda maior às comunidades submetidas a estas práticas, sobretudo se o histórico das operações policiais se constitui a partir de práticas que evidenciam a desproporcionalidade com a qual comunidades específicas são abordadas pela polícia. Neste sentido, pensar criticamente sobre a utilização de sistemas de policiamento preditivo como o *Hunchlab* revela que o uso de dispositivos pouco precisos em assuntos relativos à segurança assume um caráter que extrapola a esfera de interesses comerciais e técnicos das empresas de tecnologias, além dos interesses militares que permeiam o domínio das forças policiais.

Pensar na articulação entre segurança e tecnologia da informação significa ter em conta, num primeiro momento, o contexto em que os indivíduos estão inseridos de forma individual e coletiva, e a maneira como as subjetividades são desenhadas a partir de esquemas que hierarquizam os indivíduos socialmente por aspectos como etnia, tom de pele e classe social. Representa ainda, num segundo momento, pensar que o discurso que defende uma sociedade de segurança máxima pode ser compreendido de forma distinta para os diferentes grupos: para aqueles que têm suas subjetividades codificadas como pacíficas, esta reforma pode ser positiva e aumentar a sensação de segurança; para o grupo cuja subjetividade é codificada como suspeita e criminosa, esta reforma traduz-se em desdobramentos que remontam mecanismos de controle social e de hierarquização racial que evidenciam a prática da vigilância racializada como um subproduto da colonialidade com consequências discriminatórias que se acumulam aos múltiplos fatores impulsionados pela mediação tecnológica em matéria de segurança, portanto a lógica de patrulhamento e da vigilância integrada deve ser problematizada ponderando as questões raciais envolvidas para que ela ocorra de forma equilibrada no contexto social.

Capítulo 3 - Regulamentação de proteção de dados digitais

Diante de um contexto que, por um lado é influenciado por perspectivas cognitivistas e por assunções sobre realidades distantes dos laboratórios de visão computadorizada – seja pela dimensão técnico-científica racional que quer codificar atos como o da interpretação de forma imprecisa ou pela pouca diversidade que caracteriza estes ambientes – e, por outro lado, pela combinação de técnicas de processamento de informações biométricas que resultam em desdobramentos que aprofundam desigualdades – configura-se um enquadramento que convoca a discussão sobre as questões éticas envolvidas no desenvolvimento e uso de tecnologias como o Reconhecimento Facial em contextos sociais.

Partindo da reflexão sobre a ética, é possível identificar aspectos relativos às responsabilidades dos agentes que comercializam e introduzem tecnologias de uso massivo responsável por impactos de caráter individual e coletivo que interessam a perspectiva antropológica inspirada nos estudos *STS*. Refletir criticamente sobre os impactos que estes processos causam socialmente implica situarmos a classe de danos a dois níveis. Um deles é ao nível individual, aquele que atinge o espectro da privacidade devido ao processamento de modelos faciais provenientes do uso de redes sociais, que partem de processos voluntários ligados as novas formas de socialização. Este tipo de dano se amplifica no contexto do uso de técnicas *Big data* criando a classe de danos coletivos, aqueles que surgem em função de processos que classificam informações em escala, e adjetivam indivíduos e subjetividades a partir de análises fundadas em incertezas epistêmicas que criam desdobramentos potencialmente perigosos do ponto de vista social em domínios como o da vídeovigilância, cuja influência de estereótipos raciais é um dado observado antes mesmo da utilização de técnicas de Reconhecimento Facial[56]. Desta forma, a classe de danos coletivos representa um fator onde a ética no desenvolvimento de sistemas deve ser avaliada de forma criteriosa.

Os debates sobre os impactos da tecnologia como mediador das temáticas da privacidade e segurança ganharam expressão na atualidade, sobretudo depois da criação de mecanismos de proteção de dados digitais voltadas a minimizar os impactos negativos que resultam de processos de tomada de decisões automatizadas facilitados por algoritmos de *Machine Learning*. A existência de regulamentos como o GDPR, que lança mão de princípios que procuram regulamentar as atividades que exigem o processamento de dados pessoais é positiva uma vez que revela o interesse de comunidade internacional em regular estas atividades. Porém, é importante observar que estes princípios traduzem-se em formulações que tornam os processos de interpretação, aplicação e supervisão (governança) das atividades um fator sujeito a interpretação de diferentes agências de autoridade de proteção de dados

[56] A vigilância realizada por câmeras na Itália ilustra o contexto em que indivíduos provenientes do leste europeu e do norte da África se converteram em objetos de observação dos agentes que operavam câmeras de CCTV. Fatores como idade e vestimenta, além da aparência física feminina representavam as características que mais chamavam a atenção dos agentes de segurança, provocando o efeito *reality-show* como resultado da observação mediada pela tecnologia (Fonio, 2007 apud Frois, 2013:44).

que operam no espaço europeu. Tomemos como exemplo os princípios básicos do GDPR com relação ao processamento de dados pessoais no espaço europeu que impõe à figura do *data controller*[57] as seguintes premissas de acordo com o Artigo 5º (2016):

1. O processamento de dados pessoais deve ser operado de forma transparente, justa e de acordo com os princípios legais vigentes;
2. A coleta de dados se limita a atender objetivos explícitos e legítimos, e não deve ser utilizada para atender a propósitos que não tenham sido previamente comunicados;
3. Somente coletar dados necessários às finalidades informadas, evitando o manuseio de informações sensíveis sem finalidade explicita;
4. Garantir que dados processados sejam atualizados, e em caso de negativo, removê-los das bases de dados;
5. Limitar o armazenamento de dados que permitem a identificação individual somente para atender finalidades específicas;
6. Garantir que o processamento de dados sensíveis ocorra de forma segura, e sem causar riscos a privacidade ou a integridade dos titulares dos dados *(data subjects).*

A partir destes princípios básicos, o *Data controller* deve adequar o processamento de dados pessoais tendo em conta questões como transparência, propósito explícito, imprecisão, limite de armazenamento, garantias de privacidade. Do ponto de vista macro da gestão de dados digitais, pode-se criar uma sensação de amplitude ilimitada para o escopo destes princípios, mas, de uma perspectiva de governança e da aplicabilidade local, as múltiplas interpretações podem gerar diferentes práticas em diferentes regiões.

O escopo de abrangência do GDPR atende aos interesses de privacidade e proteção de dados dos cidadãos e residentes na comunidade européia, e abrange as empresas que processem dados pessoais de cidadãos europeus, ainda que fora do seu limite territorial. Por outras palavras, o Espaço Econômico Europeu *(European Economic Area)* regulamentado pelo GDPR conta com a figura do *data subject* como elemento fundamental que possui o poder de controlo sobre dados pessoais, e cujo processamento automatizado fica sujeito ao seu consentimento expresso e claro (Asghar *et al,* 2019). A importância que o regulamento dá ao *data subject* verifica-se na formulação que aborda os direitos básicos previstos no capítulo 3º do GDPR (2016), que garante autonomia individual no que se refere ao processamento de informações pessoais por parte de empresas.

Para as questões de privacidade vale a pena ressaltar os seguintes pontos: Direito ao acesso a dados coletados por empresas (Artigo 15º); Direito a retificação (Artigo 16º) e de exclusão de dados pessoais (Artigo 17º); Direito a restringir o processamento de dados (Artigo 18º); Direito de ser

[57] O *Data controller* é aquele que determina o propósito e o meio através do qual o processamento de dados pessoais ocorrerá. Esta figura pode se apresentar na forma de uma pessoa, uma instituição ou uma autoridade pública (GDPR, 2016, Artigo 4º: ponto 7).

informado sobre a coleta de dados antes que ela ocorra (Artigo 19º), e de ser informado até 72 horas em caso de vazamento de dados (Artigo 34º). Estes direitos garantem à figura do *data subject* a autonomia de controlar o processamento de informações de forma transparente e consentida entre as partes implicadas no processamento de *visual personal data*, posicionando a temática da privacidade digital na região como um elemento passível de controlo individual, o que atesta ao GDPR a reputação de uma das mais completas regulamentações de proteção de dados do mundo da atualidade, que serviu de inspiração para criar regulamentações similares em diversos países de acordo com o AI Report (Crawford *et al*, 2019: 31)[58].

Além dos princípios básicos quanto ao processamento ético de dados pessoais e dos direitos do *data subject*, o consentimento claro e inequívoco é o fator essencial para a execução legal deste tipo de atividade, evitando formulações demasiado complexas e permitindo que o *data controller* demonstre de forma simples que a recolha e o processamento de dados pessoais não ocorreu de forma irregular. No caso de uma pessoa desejar retirar o consentimento dado a uma determinada atividade, a remoção deverá ocorrer de forma igualmente simples de acordo com o artigo 7º do GDPR (2016), evitando penalidades previstas no regulamento que podem variar entre 4% do volume de negócios anual do ano fiscal anterior, ou um máximo de 20 milhões de euros (aquilo que for maior) dependendo da severidade da infração cometida[59]. No entanto, é importante recordar que mesmo o regulamento europeu tendo um escopo e uma abrangência bastante ampla, o Reconhecimento Facial não é um tema abordado de forma específica nas diretrizes que orientam o processamento de dados, pois de acordo com o artigo 4º, ponto 14 das provisões gerais do regulamento, a imagem facial é considerada apenas *parte* de um conjunto de dados biométricos tratados como informações sensíveis em virtude do potencial de identificação individual inscrito nela.

Ainda que o GDPR seja pioneiro em disponibilizar um conjunto de regras que regulam o tratamento de informações pessoais (e biométricas) em diferentes países - e que tenha sido notada ausência de mecanismos específicos que abordem o fenómeno do Reconhecimento Facial no contexto das transformações técnico-científicas - é preciso reconhecer a importância de alguns conceitos presentes no regulamento que suscitam perspectivas positivas que possibilitam, por exemplo, processos de vigilância que não dependem exclusivamente do processamento de informações biométricas, e que complementam as disposições do regulamento. As noções de proteção de dados como padrão, e a proteção de dados no desenvolvimento[60].

A proteção de dados como padrão faz referência ao estabelecimento dos limites em torno da recolha, armazenamento e processamento de dados limitados a finalidades específicas, e prevê que estas informações não sejam acessadas por aqueles que não têm autorização para tal, o que reforça a

[58] Em 2019 o número de países que contava com algum regulamento de proteção de dados era de 130 países, e o *AI Report* sinaliza que as regulamentações no Brasil (Lei Geral de Proteção de Dados) e no Quênia *(Data protectionact 2019)* se inspiraram na estrutura do GDPR.

[59] Conforme artigo 83 do GDPR.

[60] *Data protection by default* e *data protection by design*, respetivamente.

premissa da privacidade individual discutida. Já a proteção de dados no desenvolvimento refere-se ao desenvolvimento das práticas organizacionais imputadas ao *data controller* que possibilitem a compatibilidade do processamento de informações consoante aos direitos do *data subject*, bem como aos princípios que regulamentam o processamento de informações pessoais (biométricas). Este tipo de proteção faz uso das noções de *"pseudonymization"* e "minimização" na recolha de dados como práticas que devem ser incorporados por empresas cujos serviços possam vir a utilizar o processamento de informações pessoais sem o devido consentimento, evitando não conformidades com o regulamento (GDPR, 2016, artigo 25). Estas noções, no caso da vídeovigilância, podem se tornar alternativas viáveis para excluir o Reconhecimento Facial dos contextos de segurança.

A noção de *pseudonymization* associada à proteção de dados no desenvolvimento de práticas de vigilância é um elemento importante nesta investigação, pois partindo dela desenvolve-se a hipótese de que, tendo em conta que a vídeovigilância é algo socialmente normalizado nos contextos estudados (e tratada como uma operação de alto risco pelo regulamento), importa promover reflexões que explorem maneiras de torná-la menos invasiva, não apenas para cumprir com responsabilidades regulamentares, mas para resguardar o direito de privacidade visual e fomentar relações sociais justas e simétricas. A proposta da *pseudonymization*, ainda que expressa de forma vaga no regulamento[61] cria a oportunidade de subverter a lógica de que a tecnologia instrumentaliza o estado no caso do Reconhecimento Facial, pois permite com que a comunidade técnico-científica desenvolva ferramentas que protegem a privacidade individual, e suavizem seu potencial intrusivo. Partindo deste enquadramento, e do domínio de habilidades específicas do mundo da Visão Computacional, Asghar *et al*, (2019) discutem a perspectiva tecnológica a luz do GDPR e propõem alternativas como a aplicação de filtros em imagens capturadas que impedem o reconhecimento e a identificação de indivíduos nas imagens capturadas por câmeras de vigilância. Tais técnicas são conhecidas como *video redaction*, e propõe o uso de recursos que fornecem pelo menos onze formas de impedir o processamento de informações pessoais de forma desautorizada:

[61] "A aplicação da *pseudonymization* aos dados pessoais pode reduzir os riscos para os *data subjects* em causa e ajudar o *data controller* a cumprir as suas obrigações de proteção de dados" (GDPR, 2016, recital 28).

Fonte: Asghar *et al* 2019. *Técnicas de vídeo redaction protegidas pela privacidade no processamento de imagens.*

Uma vez que o processamento de informações biométricas depende da estrutura de consentimento clara segundo o GDPR, pensar no desenvolvimento de tecnologias que auxiliem a proteção da privacidade se converte em uma mais valia ética para as empresas, além de um benefício social que dificulta a ocorrência de processamento de informações pessoais de forma indevida. Esta proposição minimiza as consequencias negativas relativamente ao viés algorítmico por excluir a hipótese do processamento de modelos faciais, e reduz a possibilidade de que as imagens provenientes de câmeras de vigilância sejam utilizadas para finalidades que não tenham sido consentidas pelo *data subject*.

De forma praticamente oposta, o contexto norte-americano dispõe de uma estrutura altamente fragmentada no que se refere à política de proteção de dados e de privacidade, e conta com diversos mecanismos de abrangência estadual, que tornam complexas a compreensão e aplicabilidade de práticas similares ao alcance do GDPR. A diversidade de regulamentações no país remete para a multiplicidade de interpretações que se traduzem em diferentes práticas no território norte-americano, e a intervenção de abrangência nacional para regular o manuseio de dados pessoais é uma demanda constantemente mencionada nos debates que abordam a influência da IA no cotidiano (Crawford *et al*, 2019: 31). No que se refere à regulamentação de dados digitais, os atos de privacidade vigentes nos Estados de Illinois e da Califórnia são os atos mais relevantes para o contexto desta investigação uma vez que possuem um escopo e um caráter abrangente, ainda que circunscritos a localidades específicas.

O *Biometric Information Privacy Act*[62] (BIPA) surge em 2008, e é o primeiro dos atos de privacidade que procura regular a recolha e o armazenamento de dados biométricos que ocorra de forma não consensual, além de permitir que indivíduos interponham ações judiciais contra empresas em casos de eventuais violações de privacidade. Trata-se de uma iniciativa da *American Civil Liberties Union (*ACLU) que prevê que empresas recolham e armazenem dados pessoais mediante a informação prévia quanto à coleta e a finalidade desta atividade, e requer o consentimento explícito individual para realizar qualquer tipo de processamento de dados biométricos. No mesmo sentido, o *California Consumer Privacy Act* (CCPA) foi aprovado em 2018 e visa proteger a privacidade dos residentes no Estado da Califórnia, exigindo que as empresas informem que tipo de dados serão coletados e qual a finalidade, além de informar se há intenção de que estes dados sejam vendidos ou divulgados a terceiros. O CCPA[63] garante aos residentes do Estado a opção de não permitir a venda de dados pessoais, e faculta o acesso e a exclusão de informações pessoais dos bancos de dados empresariais sem que haja qualquer tipo de retaliação quanto ao exercício do direito à privacidade, o que representa um avanço significativo, sobretudo porque o Estado compreende a área de *Silicon Valley*, berço de grandes empresas de tecnologia norte-americanas como o Facebook, Google e Apple.

É indiscutível que tanto o BIPA como o CCPA são mecanismos que regulamentam o processamento de dados digitais permitindo um maior controlo por parte da população sobre a forma como as informações pessoais são manuseadas pelas empresas tecnológicas. Contudo, dado que a abrangência destas estruturas está limitada a um alcance ao nível estadual, e que o alcance das tecnologias de Reconhecimento Facial podem atingir patamares nacionais (e até mesmo transnacionais), é preciso reconhecer a existência de uma assimetria entre a distribuição das tecnologias da informação e os mecanismos que regulamentam o seu uso no contexto norte-americano. Esta relação assimétrica provoca um desequilíbrio nas interações sociais mediadas pelas tecnologias da informação, cujos prejuízos se projetam nos utilizadores que podem vir a autorizar o processamento de informações pessoais por não se atentarem aos detalhes dos longos e complexos termos de condições fornecidos pelas empresas.

Os contextos norte-americanos mencionados dispõem de mecanismos similares ao GDPR em autonomia e poder de agência, porém a forma como a temática se constitui no país cria regulamentações díspares a nível nacional, dificultando o desenvolvimento de estratégias que regulem o processamento de dados pessoais de forma equilibrada, o que faz com que a perspectiva ética seja interpretada de diferentes maneiras. Em ambos os cenários, as empresas tecnológicas desenvolvem e disponibilizam dispositivos/sistemas de Reconhecimento Facial de alcance massivo, o que em si impõe questões éticas e, no caso europeu, estas questões podem ser exploradas a partir das noções de proteção de dados padrão e no desenvolvimento, além é claro da utilização da tecnologia em favor da

[62] Para maiores informações sobre o BIPA, ver https://www.aclu-il.org/en/campaigns/biometric-information-privacy-act-bipa Acedido em 20/10/2021.
[63] Para maiores informações sobre o CCP/A, ver https://oag.ca.gov/privacy/ccpa Acedido em 20/10/2021.

proteção da privacidade. Refletindo comparativamente sobre ambos cenários, resta-nos propor um questionamento: a ausência de uma estrutura robusta como o GDPR faz com que a temática do Reconhecimento Facial nos Estados Unidos busque outras soluções para tratar do tema no país. A ideia de regulamentar o processamento de dados digitais, e o desenvolvimento de sistemas e práticas nas ciências tecnológicas com base em princípios éticos seria suficiente para minimizar os impactos sociais das tecnologias da informação em contextos sociais?

Princípios éticos e proteção de dados

Para além das preocupações corporativas ligadas à melhoria da competitividade comercial dos produtos desenvolvidos, ou das estratégias de *marketing* amparadas na disseminação irrestrita de anúncios nas plataformas digitais, as empresas de tecnologia atualmente enfrentam desafios éticos quanto à diversidade de indivíduos impactados pelos produtos e serviços disponibilizados em escala global, que dia após dia redesenham o papel da tecnologia nas interações sociais e incorporam novas e diferentes dinâmicas na realidade social. O teor transformativo adquirido pela tecnologia da informação nas últimas décadas destacou o papel da cultura digital e criou um mercado pouco diverso no que se refere à elaboração de premissas éticas.

Este cenário provoca debates relacionados à questão da representatividade da diversidade cultural em posições estratégicas, normalmente ocupadas por grupos homogêneos, bem como toca nas questões éticas da Inteligência Artificial e dos princípios que orientam as atividades no setor. A Organização para a Cooperação e desenvolvimento econômico (OECD) e o grupo de especialistas em Inteligência Artificial da União Européia (HLEG) propõem a aplicação de princípios que orientem a indústria da Inteligência Artificial de forma similar a campos tradicionais da ciência como a Medicina. Esta proposição se resume em quatro princípios fundamentais para guiar o desenvolvimento da Inteligência Artificial e que se aplicam igualmente ao Reconhecimento Facial: respeito pela autonomia humana, prevenção de danos, justiça e clareza dos processos que englobam o uso de Inteligência Artificial. Estes princípios certamente parecem positivos em discursos que expõem análises de macrogestão, mas na prática não deixam claras as formas de governança nem planos de ação concretos sobre como atingi-los. Torna-se assim necessário refletir com cautela sobre esta proposição de relacionar campos do conhecimento com históricos tão distintos, pois o sucesso da estrutura ética da Medicina pode não ter a mesma efetividade no universo da tecnologia e da Inteligência Artificial se pensarmos criticamente sobre as diferenças (conceituais e históricas) de ambas as áreas do conhecimento[64]. Vejamos alguns princípios da Medicina e qual a relação deles com o campo das ciências tecnológicas.

[64]Artigo de Brent Mittelstadt (2019) que aborda a problemática da governança relacionada à comparação de princípios éticos da Medicina e da Inteligência Artificial. Ver *Principles alone cannot guarantee ethical Artificial Intelligence*.

O primeiro dos princípios utilizados na Medicina refere-se aos objetivos comuns e deveres fiduciários, ou seja, os objetivos estabelecidos para promover a saúde e o bem-estar do paciente. Por outras palavras, o compromisso estabelecido por profissionais de saúde de garantir que os interesses dos pacientes tenham prioridade sobre qualquer interesse de ordem particular ou institucional, e a relação de confiança que advém destas práticas. Trata-se de uma série de códigos e valores morais que guiam a ética na tomada de decisões assumindo um espírito de cooperação por parte dos profissionais de saúde para construir uma relação de confiança entre o paciente e os serviços prestados, tanto no ambiente público como no privado. A ausência da figura do "paciente" na dinâmica da Inteligência Artificial, além do fato de que o universo tecnológico se respalda em ambientes de extrema pressão para a diminuição de custos e o aumento do lucro não permitem o estabelecimento de objetivos comuns entre os profissionais da Inteligência Artificial, tampouco cria laços de confiança dos utilizadores sobre os serviços disponibilizados. Outro aspecto que difere ambas as áreas do conhecimento é o fato de que não há uma regulamentação oficial que determine valores éticos e universais aos desenvolvedores de Inteligência Artificial ou de Reconhecimento Facial, de forma que as relações éticas constituídas nestes ambientes não possuem qualquer compromisso com interesses públicos. Se observarmos a lógica mercantil implícita no desenvolvimento e na distribuição destes serviços, fica claro que o compromisso principal que se estabelece é o de beneficiar financeiramente os acionistas das empresas (Mittelstadt, 2019: 2-3). Desta forma, esta é uma comparação que não se sustenta, pois o espírito de cooperação da Medicina em nada se parece com a noção de competitividade presente nas empresas privadas.

O segundo princípio abordado pelo autor refere-se ao histórico profissional e normativo que guia a tomada de decisões dos profissionais de Medicina, cuja transposição para o campo da Inteligência Artificial e do Reconhecimento Facial se torna uma tarefa difícil em virtude dos diferentes históricos entre ambas, sendo a primeira pautada por um longo e variado histórico de pesquisa e de práticas comprovadamente demonstradas nas sociedades ocidentais. A presença deste histórico de códigos e práticas que conhecem a figura de um "bom médico" não impediu a presença de negligência médica, ou mesmo de práticas condenáveis como as cometidas pelo regime Nazi durante a II Guerra Mundial quanto à esterilização involuntária de judeus, ou experiências orientadas pela figura do sigilo médico. Eventos deste tipo motivaram o desenvolvimento de princípios éticos como o Tratado de Nuremberga de 1947, que demonstra a predisposição das ciências médicas em reformular as suas práticas tendo como objetivo o respeito pela autonomia do paciente.

O histórico recente quanto ao desenvolvimento de técnicas de Inteligência Artificial e Reconhecimento Facial não nos permite relacioná-las com a história da Medicina, seja porque o campo não passou por significativas transformações conceituais no que se refere à prática, seja pela natureza diversa que compõe a formação dos profissionais que atuam no universo da tecnologia, que muitas vezes possuem equipas de múltiplas localidades trabalhando no desenvolvimento de um único sistema. Este cenário torna-se ainda mais complexo na medida em que os danos que advêm do

ambiente tecnológico muitas vezes não são imediatamente visíveis, portanto a utilização dos princípios da Medicina nos contextos da Inteligência Artificial e do Reconhecimento Facial se converte num desafio conceptual uma vez que o universo da tecnologia ainda não está devidamente equipado para permitir esta comparação (Mittelstadti, 2019: 4-6). A falta de preparação das empresas de tecnologia em lidar com questões éticas de forma transparente e igualitária é sublinhada por Jacob Metcalf [65] quando afirma que "as empresas de tecnologias não estão organizadas para fazer as perguntas certas sobre os impactos prejudiciais de seus produtos, especialmente sobre as comunidades afrodescendentes e indígenas". Se as empresas de tecnologia não estão formatadas para fazer as perguntas certas para tratar de questões éticas internas, pensar na ética das decisões automatizadas realizadas por sistemas que apresentam limitações epistêmicas parece-nos um complicador que torna este desafio ainda mais dificil.

O terceiro princípio que orienta as decisões na área médica refere-se à tradução de princípios em práticas através de métodos comprovados, o que novamente apresenta limitações conceituais para efeito de comparação. O surgimento relativamente recente da Inteligência Artificial e das tecnologias da informação é um fator que dificulta o estabelecimento de objetivos comuns entre os profissionais, bem como a criação de normas que orientem atividades específicas no âmbito privado. Adicionalmente, Mittelstadti argumenta que a diferença temporal entre os diferentes ramos de atuação não permite uma reflexão amadurecida sobre métodos comprovadamente equitativos e eficientes para orientar práticas éticas no desenvolvimento deste tipo de tecnologia, pelo contrário: este fator converte-se num *objetivo* relativamente ao caminho a ser trilhado pelo setor, e não algo que possa ser utilizado com base na experiência e numa reflexão crítica comprovada. A combinação de códigos de conduta e práticas que são constantemente testadas e revistas pelas autoridades médicas garante que este sistema de princípios se adeque aos desafios éticos decorrentes do ambiente médico, que através de instituições fortes desenvolve políticas específicas que orientam a tomada de decisão de forma coerente, respeitando a autonomia do paciente. O mesmo não ocorre no ambiente multifacetado e ainda em construção da Inteligência Artificial, e na medida em que o setor tente se orientar a partir de princípios que não se relacionam com o setor específico da tecnologia, criar-se-ão diretrizes conflituosas quanto a questões éticas neste setor cujas prioridades se relacionam com a lógica do mercado, e não com o bem estar dos utilizadores (Mittelstadti, 2019: 7).

A ausência de clareza quanto ao desenvolvimento de premissas éticas relativas ao campo da Inteligência Artificial tem suscitado debates com opiniões divergentes sobre as razões pelas quais a demanda pelo uso de sistemas de Reconhecimento Facial aumenta exponencialmente. A presença de mecanismos que regulamentam as práticas de processamento de dados é um fator que fortalece a agenda da privacidade e fomenta o desenvolvimento de tecnologias que atuam de forma positiva no contexto social, por exemplo, para o gerenciamento do contexto pandémico da COVID-19. Iniciativas

[65]Publicação online no portal *Points Data & Society*. Ver *Looking for Race in Tech companies Ethics. Identifying tensions where race and tech ethics intersect.*

como a da empresa Pangea[66] sediada em Israel, que desenvolveu tecnologia de Reconhecimento Facial para auxiliar as autoridades nacionais a identificar indivíduos vacinados, e coibir o uso de passaportes sanitários de pessoas que utilizavam *QR codes* de amigos ou familiares para burlar o controlo sanitário em ambientes controlados. Em março de 2021, com aproximadamente 50% da população vacinada, as medidas de segurança para o controlo pandémico local contavam com a apresentação do passaporte sanitário para a verificação de *QR codes* que indicavam o nível de imunidade individual, tal como ocorre em diversas localidades. Na medida em que foram detectadas tentativas de burlar o controlo sanitário, a empresa sugeriu o uso do Reconhecimento Facial como um recurso que impede o uso de credenciais por outrem uma vez que a confirmação da imunidade contra o vírus se baseia na verificação de modelos faciais[67]. Vale ressaltar que Israel dispõe de uma regulamentação de proteção de dados fundada na proteção da privacidade e do processamento de dados pessoais *(Protection of Privacy Law, 5741-1981)* com abrangência nacional, o que difere conceitualmente dos mecanismos de proteção de dados norte-americanos.

O quarto e último princípio da Medicina refere-se à existência de mecanismos de responsabilização legal e profissional, que somado aos três princípios já abordados cria uma estrutura sólida que guia os objetivos, as normas e os métodos que regulam a atividade médica, que conta com mecanismos legais que responsabilizam os profissionais em casos de negligência ou de práticas questionáveis. Os comitês éticos e as instituições certificadoras têm assim possibilidade de avaliar e enquadrar práticas que estejam em desacordo com princípios fundamentais, que podem resultar em sanções como punições disciplinares ou mesmo a perda da licença para exercer a atividade em casos extremos (Mittelstadti, 2019: 8). De forma oposta, as atividades exercidas no âmbito da Inteligência Artificial e do Reconhecimento Facial, sobretudo no contexto norte-americano, dispõem de mecanismos com limitações territoriais no que se refere à responsabilidade quanto aos danos individuais e coletivos causados pelo uso destes sistemas, e este arranjo dificulta as analises que buscam equacionar os tipos de danos causados, bem como as soluções que possam fortalecer a agenda da proteção de dados no país de forma integrada.

Os princípios da medicina, na melhor das hipóteses podem servir como inspiração para criar as estruturas que irão regulamentar as práticas da Inteligência Artificial e do Reconhecimento Facial no futuro, e não como padrões comparativos entre setores que não se relacionam. Adicionalmente, é preciso ter em mente que noções como autonomia humana, prevenção de danos, justiça e clareza devem contar com proposições concretas que possam minimizar os impactos negativos do ponto de vista social, sobretudo em localidades que não contam com regulamentações abrangentes. Enquanto estes princípios não se traduzem em políticas específicas, populações de diversas localidades são

[66] Para maiores informações sobre a empresa, ver https://pangea-it.com/about-us/ Acedido em 20/10/2021

[67] Ainda que este caso extrapole os limites territoriais propostos por esta investigação, ele serve-nos como exemplo de localidades que não utilizam a estrutura do GDPR, e que ainda assim conseguem articular o uso do Reconhecimento Facial de forma positiva. Ver "*Tech firms launches facial recognition to catch Israelis using fake vaccine passports*". Mashable Middle East.

submetidas a tecnologias que não capturam a complexidade da diversidade humana, e que inclusivamente podem tornar-se mecanismos que criam desigualdades estruturais, que por conta de uma estrutura de regulamentação difusa, dificultam a atribuição de responsabilidade aos agentes que concebem e operacionalizam estes sistemas.

É importante reforçar que o objetivo desta investigação não é o de fornecer respostas sobre as questões éticas abordadas, mas sim suscitar a reflexão crítica sobre processos sistémicos que envolvem múltiplos agentes e estruturas (públicas e privadas), que estabelecem uma lógica de danos difícil de rastrear em virtude de linguagens pouco acessíveis ao grande público, além de lógicas sistémicas igualmente complexas onde a ausência de premissas regulatórias robustas amplia desigualdades sociais e comportamentos discriminatórios. Esta é uma dimensão essencial a ter-se em conta quando pensamos sobre a ética envolvida no desenvolvimento das tecnologias da Visão computacional, que de forma indireta evidencia um desequilíbrio aparentemente vantajoso às empresas de tecnologia.

A assimetria de poderes, neste contexto, toca em questões que são projetadas no ambiente virtual, mas que nascem de práticas e valores culturais que se tornam fonte de conflito por conta da forma como valores éticos são desenvolvidos no ambiente técnico-científico, e a secção a seguir ilustra este ponto a partir da temática do viés algorítmico na criação de bancos de imagens que treinam modelos de *Machine Learning*. Neste sentido, vale a pena refletir antecipadamente sobre a formulação que aborda o racismo sistémico presente nas esferas no domínio tecnológico de Ruha Benjamin (2019, apud Mohamed *et al*, 2020:662) "Considerando que em uma época anterior a intenção de aprofundar as desigualdades raciais era mais explícita, hoje a desigualdade codificada é perpetuada precisamente porque aqueles que projetam e adotam tais ferramentas não estão pensando cuidadosamente sobre o racismo sistémico".

Tendo em vista as indicações de que o mercado das empresas de tecnologia é composto por grupos homogêneos, e que este pode ser um dos elementos que denotam a desigualdade codificada e o racismo sistémico, importa pensar criticamente sobre os custos sociais relacionados a estes processos, bem como explorar quais alternativas se apresentam atualmente para minimizar este cenário no âmbito do Reconhecimento Facial.

Capítulo 4: Os custos sociais da Inteligência Artificial e do Reconhecimento Facial: O viés algorítmico e o impacto na privacidade.

Os custos sociais associados aos impactos do uso de sistemas algorítmicos tendem a ter um amplo alcance nas diferentes comunidades globais em virtude do cruzamento de processos que envolvem o processamento de quantidades massivas de dados para alimentar bancos de dados digitais, que classificam dados heterogêneos influenciados por lógicas sistémicas não totalmente compreendidas

pelas ciências tecnológicas[68]. Neste sentido, se pensarmos sob a perspectiva do Reconhecimento Facial e da diversidade de modelos faciais que compreende diferentes formatos do rosto e tipos de pele, é desejável que a construção de bancos de imagens que treinam algoritmos de Reconhecimento Facial seja feita baseada numa ampla diversidade de amostras, e não numa quantidade massiva de dados homogêneos na tentativa de equilibrar eventuais incoerências sistêmicas, de outra forma estes sistemas sujeitam parte da comunidade de utilizadores à discriminação algorítmica, e os expõem a situações que impactam sua experiência virtual e sua realidade social diante de visões de mundo específicas projetadas em sistemas utilizados em contextos socialmente heterogêneos. A presença de indeterminações que influenciam os resultados apresentados pelo desempenho destes sistemas, somada às sucessivas assunções feitas nos ambientes da Inteligência Artificial e da Visão Computacional, neste contexto, são denominadas como viés algorítmico, ou seja, o resultado obtido a partir de processos mais ou menos precisos ligados à fase de desenvolvimento de tecnologias de Inteligência Artificial, no caso do Reconhecimento Facial, dos bancos de imagens que criam desempenhos desiguais nas comunidades globais.

O viés *(bias)* inscrito na lógica sistémica que orienta a atividade algorítmica é constantemente abordado na crítica quanto ao impacto das tecnologias algorítmicas e a maneira como se promovem as decisões automatizadas como inquestionáveis (Cathy O'Neil, 2017) [69]. De forma consciente ou não, o desenvolvimento das fases taxonômicas e a busca pelo reconhecimento de padrões entre dados constantemente processados e recombinados estabelecem padrões algorítmicos que refletem visões de mundo de caráter sistémico limitadas, e estas limitações, como constantemente sublinhado, criam vivências digitais e sociais distintas dependendo do contexto em que um modelo de *Machine Learning* opera. Partindo de um exemplo hipotético, modelos de *Machine Learning* criados a partir de bancos de fotos com maior quantidade de imagens de homens do que de mulheres tendem a efetuar o processamento de imagens de homens de forma mais eficiente do que das mulheres: a presença de quantidades superiores de imagens masculinas que treina o algoritmo o torna mais sensível a identificar diferentes padrões de imagens de homens do que de mulheres. Na medida em que o banco

[68]O uso de análises algorítmicas produz "evidencias inconclusivas e ações (automatizadas) injustificadas" por conta da forma como o sistema de análises é estruturado. A lógica epistêmica baseada na busca por associações e correlações com múltiplas variáveis cria a dinâmica de *apophenia*, ou seja, o sistema identifica padrões de forma mecânicapor deparar-se com imensas quantidades de dados que oferecem conexões que irradiam para qualquer direção (boyd and Craford, 2012 apud Tsamados, 2021). Dito de outra forma, as conexões estabelecidas por modelos de *Machine Learning* nem sempre refletem resultados válidos, ou que necessariamente façam sentido. Uma vez que haja dados disponíveis, o modelo realiza as análises comparativas que desencadeiam decisões automatizadas a partir de lógicas mecânicas moldadas pela maneira como ele foi treinado para estabelecer conexões, desta forma, a incidência de evidências inconclusivas ou de ações injustificadas serve-nos como indicador de que este tipo de tecnologia não apresenta resultados totalmente precisos.

[69]Cathy O'Neil descreve os processos algorítmicos como "Armas de destruição matemática *(weapons of math destruction)"* e argumenta sobre a autoridade das ciências tecnológicas quanto aos veredictos resultantes de decisões automatizadas: "muitos desses modelos (de *Machine Learning*) codificavam preconceitos humanos e mal-entendidos nos sistemas de *software* que cada vez mais gerenciavam nossas vidas (...). Seus veredictos, mesmo quando errados ou prejudiciais, estavam fora de discussão ou apelação. E eles tendiam a punir os pobres e oprimidos em nossa sociedade, enquanto tornavam os ricos mais ricos" (O'Neil., 2017 introdução).

de dados segue recebendo maiores quantidades de imagens de homens, cria-se uma disparidade entre o desempenho das diferentes classes de reconhecimento, que neste exemplo variam consoante ao gênero atribuído na classificação destes dados.

O reconhecimento automatizado de imagens opera-se através da recolha, classificação e processamento de modelos faciais cujas análises são orientadas por aspectos físicos como tom de pele e olhos, cor de cabelo e expressões faciais, bem como por aspectos comportamentais como estilo de roupa, forma de caminhar e gesticular (Asghar *et al*, 2019). Assim, a constante produção de dados que emerge das interações digitais contemporâneas molda o ambiente para que as empresas de tecnologia tenham à sua disposição quantidades massivas de informações para treinar os seus modelos de *Machine Learning* e ampliar os seus bancos de dados em proporções incalculáveis, expandindo seu domínio no território digital. Isto significa que se estabelece uma relação assimétrica de poder entre as empresas e os utilizadores, que ao utilizarem os serviços em plataformas digitais de forma gratuita, fornecem informações detalhadas sobre a sua intimidade que posteriormente serão utilizadas para outras finalidades (e.g vigilância), ou seja, uma relação de caráter exploratório que subjaz deste contexto, a saber, a ideia de "colonialismo digital" [70].

Historicamente a representação cultural dos povos afrodescendentes foi construída por meio de processos e discursos que legitimaram a violência e a subordinação destes indivíduos baseada em práticas discriminatórias e excludentes. Contudo, é importante perceber que na mesma medida em que a dinâmica de dominação foi exercida para desfavorecer um grupo específico, ela também construiu uma centralidade que exaltou uma classe dominante como normativa, promovendo uma cultura de adoração deste grupo que foi incorporada nas relações culturais no decorrer dos séculos. Esta dinâmica se observa nas formulações que abordam o racismo estrutural como um sistema de privilégios baseados na significação racial das diferentes tonalidades de pele que influenciou o desenvolvimento de tecnologias de reprodução visual de tal forma que reproduz a ideia da "Brancura prototípica" [71].

Um exemplo que ilustra a continuidade da interpretação da ideia de raça partindo de determinismos biológicos se relaciona com o setor da fotografia, que desde meados do século XVIII teve a influência de princípios racializados no que se refere à representação visual da população afrodescendente. Estudos apontam que a tecnologia utilizada pelas empresas Kodak e Fuji na elaboração de filmes fotográficos até meados de 1990 tinham como base normativa os tons de pele

[70] O AI Report destaca que o uso do termo colonialismo digital deve ser feito com cautela para que não se torne uma metáfora superficial na abordagem crítica de práticas abstratas sem a devida atenção os contextos históricos, políticos e culturais relativos aos regimes coloniais, pois a forma como funcionam as estruturas econômicas, políticas e culturais que conhecemos na atualidade possuem laços íntimos com a história dos regimes coloniais do Ocidente (Crawford *et al*,2019:43-44)

[71] Lewis Gordon (2006), inspirado na trajetória de ativistas negros como Frantz Fanon e William Edward Burghart DuBois, problematiza a ideia de negação de subjetividade da comunidade afrodescendente como um tipo de violência estrutural que normatiza a cor da pele branca ("Brancura prototípica"), e nega a subjetividade a aqueles que não se encaixem dentro desta norma. Aos indivíduos "desviantes" restava a lógica do "tudo é permitido", por exemplo, o processo de marcação / identificação dos corpos escravizados. (apud Browne. 2015: 110)

caucasianos, o que tornava estes filmes pouco sensíveis à identificação de características e contornos de indivíduos com tons de pele negra. Este dado evidencia como ideais construídos a partir de noções excludentes de raça, e moldadas por questões estruturais ligadas à influência do histórico colonial estiveram presentes numa realidade social não tão distante, que privilegiou o tom de pele caucasiano em detrimento dos impactos causados às comunidades não brancas (Leslie, 2020: 13). De forma similar, Lorna Roth (2009) abordou este episódio retratando não apenas o evidente viés racial presente na indústria fotográfica, como também as queixas de setores industriais (produtores de chocolate) datadas desde meados da década de 1960 em torno da qualidade das fotografias de seus produtos [72].

Mesmo após a mudança de paradigma que substituiu os filmes fotográficos por câmeras digitais, relatos de usuários de computadores portáteis comercializados pela Hewlett Packard apontam o viés da "brancura prototípica" influenciando também o funcionamento de mecanismos de Reconhecimento Facial destes equipamentos de forma semelhante à dos filmes fotográficos. Um vídeo publicado no Youtube[73] em 2009 mostrou como o sistema de Reconhecimento Facial reconhece, sem dificuldades, modelos faciais de indivíduos com tons de pele branca ou clara, porém, no momento em que o sistema se depara com um modelo facial de um indivíduo não caucasiano, o sistema deixava de reconhecer um rosto na imagem.

Este episódio gerou repercussões negativas e a empresa foi acusada de racismo sistémico, pois o fato de um sistema de Reconhecimento Facial possuir maior eficiência ao analisar certos tons de pele ilustra pelo menos dois aspectos relativos ao viés algorítmico de acordo com o relatório do Instituto Alain Turing: o primeiro é de que a escolha feita por quem programou e desenvolveu este sistema privilegiava o Reconhecimento Facial a partir de fatores como iluminação e contraste que possibilitavam o reconhecimento de tons de pele específicos, desconsiderando a diversidade de utilizadores. O segundo aspecto relaciona-se com questões culturais em torno da ética destes processos e de uma relativa apatia por parte das indústrias de tecnologia em priorizar práticas que promovam a equidade de desempenho através da realização de testes em diferentes tonalidades de pele antes do lançamento do sistema, o que poderia evitar ou minimizar o impacto negativo às comunidades mais afetadas pelo viés algorítmico (Leslie, 2020: 14-15).

Para além da questão do viés algorítmico, este enquadramento nos permite inferir sobre a desigualdade ao nível da empregabilidade nas empresas de tecnologia conforme apontado por Moss e Metcalf a partir das entrevistas realizadas em *Sillicon Valley*. Segundo observações dos autores, as relações laborais no setor se baseiam na noção de meritocracia, como se todos os indivíduos tivessem as mesmas condições de ascensão profissional, algo que a discussão sobre o racismo institucional nos permite inferir que esta não é uma realidade que todos os grupos possam dizer que partilham. Desta maneira, a reflexão sobre a ideia de meritocracia se apresenta muito mais como um mecanismo ideológico que pretende racionalizar as desigualdades sociais atribuindo o sucesso de um grupo em

[72] Ver *Looking at Shirley, the ultimate norm: Colour balance, image technologies, and cognitive equity*.
[73] Ver *HP Investigates Claims of 'Racist' Computers.* Wired, Dezembro 2009.

detrimento de "diferenças naturais" de outro[74]. Adicionalmente, "Durante décadas, o poder econômico e o prestígio cultural que a meritocracia detém foi expresso pela ideia de que aqueles que trabalham lá são os *melhores e os mais brilhantes*, ao mesmo tempo descartando a sub-representação de negros e latinos em posições de poder com alegações de que apenas o talento bruto é recompensado sem respeito à raça ou gênero" (Moss e Metcalf, 2020:41).

O custo social associado à mediação da tecnologia da informação abrange as relações laborais, e consequentemente se projeta nos produtos e serviços presentes na sociedade por conta da forma abstrata como o viés algorítmico opera, e este cenário revela a influência de valores culturais no interior das empresas de tecnologia que evidenciam a desigualdade presente num setor que reformulou as interações sociais; desta maneira a reflexão critica sobre a maneira como ele se estrutura é fundamental para a contemporaneidade. A seguir será discutida outra faceta relativamente ao custo social inerentes ao uso de tecnologias da informação, e a forma como estas práticas afetam as determinadas comunidades de um ponto de vista interseccional.

Viés algorítmico e a dimensão interseccional

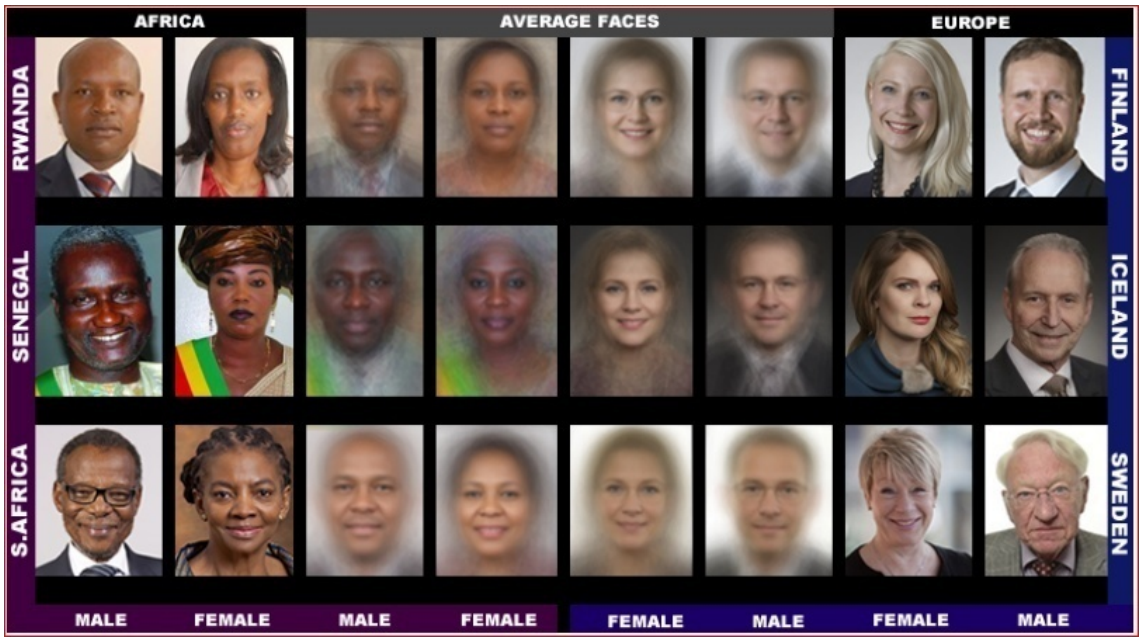
Um estudo realizado por Joy Buolamwini e Timnit Gebru em 2018[75] aborda o impacto de fatores interseccionais presentes no desempenho de sistemas comerciais de Reconhecimento Facial, e revela aspectos importantes para esta investigação, nomeadamente a disparidade de desempenho de sistemas que, por um lado, não apresentam dificuldades em reconhecer de forma precisa modelos faciais de homens com tonalidade de pele branca/clara *(Lighter Males)*, apresentando taxas de imprecisão inferiores a 1% de probabilidade de erros, mas, por outro lado, quando se trata de operar o Reconhecimento Facial em modelos faciais de mulheres com tonalidades de pele negra *(Darker Females)*, os mesmos sistemas apresentam taxas de imprecisão que variam de 20% a 34%[76].

A observação comparativa do desempenho destes sistemas teve em conta a formulação de um banco de dados criado pelos investigadores, o *Pilot Parliament Benchmark – PPB* que parte de critérios de classificação de gênero limitada ao binarismo (masculino e feminino), uma vez que os sistemas comparados foram programados para classificar imagens a partir de assunções que reduzem a noção de gênero a categorias fixas. Neste sentido, e por razões de precisão na análise, a designação de gênero elegida para o PPB baseou-se na indicação dos investigadores sobre como indivíduos são percebidos como homens e mulheres. Para além disso, o PPB utilizou o critério de tipos de pele de

[74] Mouk, 2017; Castilla e Benard, 2010; Subramanian, 2019 apud Moss e Metcalf, 2021:41.
[75] Ver *Gender Shades: Intersectional Accuracy disparities in commercial gender classification*.
[76] Resultados obtidos através da análise de sistemas de Reconhecimento Facial capazes de classificar modelos faciais a partir de categorias de gênero comercializados por empresas como a Microsoft, IBM e Face++ (Buolamwini e Gebru, 2018:9)

acordo com a escala dermatológica Fitzpatrick[77] utilizada pela comunidade médica para classificar e determinar o risco de doenças dermatológicas em pacientes com variadas tonalidades de pele.

A escolha da escala Fitzpatrick para determinar o tipo de pele atribuído a cada indivíduo justifica-se com o objetivo de evitar uma leitura étnico-racial de indivíduos por parte dos algoritmos na tentativa de subverter a dinâmica, também binária, do Reconhecimento Facial de indivíduos brancos e não brancos. Ou seja, a proposta de formulação do PPB se revela inovadora para os moldes do processamento e reconhecimento de imagens, pois procurou reduzir os aspectos inscritos nas escolhas racializadas realizadas nos níveis taxonômicos que afetam o desempenho de sistemas através do viés algorítmico tendo em conta a variação de tipos de pele, bem como questões relacionadas aos processos migratórios que desenharam contextos socialmente diversos na realidade social global. Neste contexto, a escala Fitzpatrick dispõe de seis níveis de classificação sendo os níveis I, II e III associados à tonalidade de pele branca e clara, e IV, V e VI associados à tonalidade de pele negra. Importante destacar que este banco de dados se constitui de imagens de Parlamentares de seis países africanos e europeus, isto é, figuras públicas, e a escolha destes indivíduos têm como objetivo criar um ambiente balanceado no quesito "tipos de pele", para que os processos algorítmicos não sejam impactados de forma parcial, eventualmente privilegiando determinado tipo de pele nas análises (Buolamwini e Gebru, 2015:6-7):



Fonte: Buolamwini, e Gebru, 2015: 4. *Imagens de exemplo e rostos do novo Pilot Parliaments Benchmark (PPB)*

77 Trata-se de um método desenvolvido por Thomas B. Fitzpatrick utilizado pela área da Dermatologia que classifica numericamente os tipos de pele com base na exposição à luz solar. Ver *The validity and practicality of sun-reactive skin types I through VI. Archives of Dermatology.*

Depois de realizados os procedimentos de classificação das imagens no PPB em termos de gênero e tipos de pele, os autores propõem uma análise comparativa do PPB com dois bancos de dados utilizados para operar o Reconhecimento Facial nos Estados Unidos, o *IJB-A*, um banco de dados composto à época por imagens de 500 figuras publicas utilizado pelo *National Institute of Standards and Technology (NIST)* considerado pelas autoridades locais como geograficamente diverso. O outro banco de dados é o *Adience*, um banco de dados comercial composto por imagens de 2,194 indivíduos indiferenciados. Para efeito de comparação, as imagens destes dois bancos de dados foram categorizadas individualmente seguindo as premissas da escala Fitzpatrick, e os resultados obtidos dão-nos pistas que traçam de forma preliminar a maneira como o viés algorítmico se constitui no interior dos sistemas, evidenciando não apenas a pouca representação da população de pele não branca no ambiente digital, mas também a forma como uma parcela específica desta população (nomeadamente a das mulheres negras) tende a ser mais impactada pela dinâmica do Reconhecimento Facial.

Ao verificarmos o percentual de imagens a partir das classificações de gênero e tipo de pele, os bancos de dados *IJB-A* e *Adiance* apresentam quantidades desproporcionais de imagens que representam mulheres negras com resultados de 4,4% e 7,4% respetivamente. De forma oposta, a representação de homens brancos atinge números 59.4% e 41.6% respectivamente, o que demonstra o nível de sobrerepresentação de uma parcela da população masculina, e o evidente desequilíbrio através do qual os processos algoritmos operam nestes bancos de dados, possivelmente moldando um viés sistêmico que permite o pleno funcionamento de técnicas de Reconhecimento Facial numa população, e o consequente baixo desempenho noutra. Esta configuração ilustra a influência de questões interseccionais implícitas na lógica que estabelece a predominância de homens de tonalidade de pele branca como fator normativo para treinar os modelos de *Machine Learning* para efeitos de Reconhecimento Facial (similar ao caso da calibração dos filmes fotográficos). Demonstra ainda que a construção dos dois bancos de dados comerciais foi realizada a partir de premissas pouco criteriosas quanto à diversidade de tipos de pele, ainda que a utilização posterior destes sistemas ocorra de forma indiscriminada, mesmo sem haver qualquer recomendação por parte dos desenvolvedores sobre a eficácia reduzida em determinadas populações.

Desta forma, a leitura facial do grupo de mulheres negras apresenta uma disparidade de desempenho se comparada à leitura de seus pares de pele branca, por exemplo, no caso do banco de dados *Adience* que conta com 44.6% de representação de *lighter females*. Ao observar a distribuição de imagens orientada pela escolha dos indivíduos e do critério de diferentes tipos de pele na composição da base de dados PPB, nota-se um maior equilíbrio neste banco de imagens bem como na estrutura utilizada na sua elaboração:

Fonte: Buolamwini, e Gebru, 2015:7. *A porcentagem de mulheres mais escuras, mulheres mais claras, homens mais escuros e homens mais claros no PPB, IJB-A e Adience.*

A partir da análise dos bancos de dados *IJB-A* e *Adience* é evidente que a parcela de mulheres negras representadas em ambos é bastante inferior do que a de homens e mulheres brancas, o que nos possibilita afirmar que a possibilidade de incoerências sistémicas ocorrerem no grupo de mulheres negras é significativa. Uma vez que a Cibercultura e a interação com dispositivos tecnológicos seja um imperativo cada dia mais presente na realidade social, e que estas tecnologias passem a servir, por exemplo, para identificar indivíduos em locais como escolas, hospitais, bancos ou órgãos governamentais, a forma como estes bancos de dados é feita, e a maneira como os sistemas de Reconhecimento Facial são treinados criará empecilhos a esta população de forma desproporcional fazendo com que a exclusão digital se transfira para a esfera social.

Tendo em conta que estes sistemas também são utilizados para instrumentalizar as forças de segurança, a possibilidade de identificação incorreta (ou até mesmo a não identificação) suscita preocupações do ponto de vista social, pois a identificação incorreta pode causar transtornos desnecessários que invariavelmente terão como fonte de conflito a questão racial. Por um lado a "não identificação" pode resultar na exclusão social em ambientes públicos controlados, porém, por outro lado ela pode ser um fator positivo para conter as práticas relativas a vigilância racializada conforme aponta Nabil Hassein[78], pois o acesso a informações pessoais de populações culturalmente estigmatizadas em bases de dados calibradas com um viés sistêmico pode ter consequências diretas nos direitos e nas liberdades destes indivíduos por conta da forma como suas subjetividades foram desenhadas a partir de fatores como o racismo estrutural. É importante pontuar que a questão do acesso a informações biométricas por parte das forças de segurança é algo que atinge as sociedades de forma integral, porém, as questões raciais criam um fator interseccional que se acumula na experiência social de comunidades marginalizadas, criando diferentes experiências e projeções de vida de forma desigual.

Se por um lado a subrepresentação destas comunidades se converte num dado que evidencia uma eventual continuidade de processos históricos, sociais e políticos de outrora que resultam na potencial exclusão social destes indivíduos, por outro, a inclusão digital desta população nas estruturas algorítmicas convencionais resultam numa problemática social que nos permite identificar a dimensão

[78] Publicação que apóia a não inclusão de indivíduos afrodescendentes nos bancos de dados de Reconhecimento Facial como uma estratégia de resistência. Ver *Against Black inclusion in Facial Recognition.* Portal Digital Talking Drum.

interseccional dos custos sociais associados à mediação das tecnologias da informação, e esta sobreposição de desigualdades se torna mais intensa no caso das mulheres negras cuja exposição a níveis de exclusão e violência é explorada nos estudos feministas que abordam as questões de identidade, raça e gênero (Crenshaw 1991).

Diante deste enquadramento, a proposta de elaborar um banco de dados à volta de critérios como a escala Fitzpatrick sugere um modelo de banco de imagens equilibrado em termos de representatividade, e atua como uma iniciativa que visa minimizar os efeitos de processos históricos, sociais e políticos que refletem na realidade social contemporânea mesmo que de forma inconsciente. Também é importante ressaltar que para que este cenário se altere de forma significativa, é preciso identificar e reconhecer a influência das questões raciais como um problema social que exige reparação, onde o viés algorítmico como categoria de análise permite-nos observar as diferentes dinâmicas influenciadas pela esfera digital, abrindo-nos horizontes para questionar a interação desta tecnologia com o contexto social.

Neste sentido pode-se afirmar que a iniciativa de Buolamwini e Gebru dialoga com as teorias *decolonials*, pois "A base da Inteligência Artificial *decolonial* repousa em uma abordagem auto-reflexiva para desenvolver e implantar uma Inteligência Artificial que reconhece desequilíbrios de poder e seus sistemas de valores implícitos (Mohamed *et al*, 2020: 672)". A partir do experimento com o banco de dados PPB, fica claro o desequilíbrio entre as partes representadas e excluídas nas dinâmicas relacionadas ao Reconhecimento Facial; por outro lado, o experimento também nos dá pistas sobre possíveis saídas que subvertem a lógica sistêmica que favorece a sobrerepresentação de grupos específicos, sendo assim, promover reflexões que busquem igualar as condições de uso das populações submetidas a estes tipos de tecnologia pode ser um primeiro passo em direção a modelos éticos pensados (e desenvolvidos) por pessoas que de facto experimentam os impactos negativos da Inteligência Artificial na atualidade.

O desgaste da noção de privacidade

A temática da privacidade tem importante destaque nas reflexões que abordam os impactos sociais do Reconhecimento Facial e da Inteligência Artificial, pois o contexto do uso de dispositivos móveis que processam modelos faciais em ambientes públicos de forma compulsória é uma preocupação que chama a atenção não apenas da comunidade científica, mas também de ativistas que criticam o uso de técnicas de vigilância intrusivas por autoridade policiais, e denunciam o benefício do avanço tecnológico utilizado para potencializar práticas intrusivas que conflitam com as noções de privacidade e liberdades civis.

Esta dinâmica é central na análise das transformações sociais motivadas pelo desenvolvimento tecnológico que, neste caso, posiciona a tecnologia da informação como mediadora de tensões que abrangem a esfera da segurança pública ao mesmo tempo em que evidencia a relação assimétrica que

esta dinâmica impõe à ordem social ao utilizar informações privadas como mercadorias indiferenciadas, sobretudo para compor bancos de imagens que são descontextualizadas de seu ambiente/objetivo original, causando danos de ordem individual e coletiva.

Tratando da esfera individual, é importante termos em conta a existência das inúmeras formas de socialização da atualidade que convocam a exposição voluntária da intimidade, e motivam os usuários a publicar imagens e opiniões de forma sistemática, incitando-os a uma espécie de engajamento digital baseado num fluxo de conteúdo que disponibiliza milhões de imagens nas redes sociais, que influenciam a forma como os usuários interagem uns com os outros, criando um verdadeiro espetáculo que nos permite citar Guy Debord (2003: 17) "O espetáculo apresenta-se como algo grandioso, positivo, indiscutível e inacessível. Sua única mensagem é o que aparece é bom, o que é bom aparece". A concepção de "espetáculo" discutida por Debord é uma crítica social importante que aborda um fenómeno associado à lógica capitalista, permitindo-nos refletir de forma crítica sobre a relação estabelecida pelas empresas de tecnologia e os utilizadores. Para além dos apelos visuais do âmbito digital, este processo também sugere uma reconfiguração da noção de privacidade, que atualmente é desenhada a partir da emissão de consentimento individual exigido pelas empresas de tecnologia quanto à utilização de serviços negociados por meio de termos e condições que normatizam os aspectos da privacidade de acordo com regras estabelecidas por mecanismos de proteção de dados.

Tratando da esfera coletiva, importa abordar como dados individuais se convertem em blocos de dados coletivos, que geram análises automatizadas que orientam as práticas de vigilância preditiva, e até mesmo a gravação de operações policiais em tempo real. É inevitável pensar sobre os aspectos da privacidade sem fazer referência à declaração dos direitos humanos que prevê o direito à privacidade no artigo 12º, e garante de forma ampla que ninguém deve sofrer intromissões arbitrárias na sua vida privada (UN, 1948): "Artigo 12.º Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei."

Situando o direito à privacidade no âmbito do espaço europeu, os artigos sétimo e oitavo[79] da Carta dos Direitos Fundamentais da União Europeia (2000) também abordam a proteção de dados pessoais como um direito conferido a todos os cidadãos, um direito inalienável e garantido sob a proteção da lei, que combinado com estrutura do GDPR torna o espaço Europeu um ambiente ativo na elaboração de políticas que incentivaram a valorização da privacidade como um direito humano baseado no controle individual de informações privadas. Podemos observar a ideia de privacidade no Ocidente também desenvolvida nos Estados Unidos, com o "O direito à privacidade" de Samuel D.

[79]Artigo 7º: Respeito pela vida privada e familiar. Todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações; Artigo 8º: Proteção de dados pessoais: 1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito; 2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respetiva retificação. 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.

Warren e Louis D. Brandeis, na publicação da *Harvard Law Review*no final do século XIX que pretendia estabelecer "O direito de ser deixado em paz", inspirado no caso do juiz Thomas Cooley e o contexto do surgimento de novas tecnologias que poderiam violar o até então pouco conhecido reino da privacidade[80] (1890:195).

A possibilidade do registo fotográfico e da manipulação deste tipo de informação é importante para a discussão da privacidade por evocar a oposição entre o público e o privado, e estabelecer em que situação tais informações podem ou não ser manuseadas, dependendo do contexto. Cintia Dal Bello (2011:141) problematiza a relação entre privacidade inspirada em conceitos como a individualidade e a identidade, e a forma como estas noções evoluíram nas sociedades modernas. Desde a concepção do espaço privado como sendo o quarto privativo burguês – que permitia ao indivíduo acessar seu íntimo através do silêncio das paredes solitárias para se expressar em diários e cartas, bem como conduzir reflexões que constituíam sujeitos, ou indivíduos únicos com identidades em constante evolução (Sennet, 1977) – até ao momento em que a racionalidade técnico-científica invade a vida moderna, estabelecendo mecanismos complexos de privacidade que atravessam o tecido social e combinam a interação da privacidade com o universo digital através do uso de redes sociais, onde a intimidade se apresenta de forma espetacularizada.

Dal Bello explora a ideia de *evasão da privacidade*[81] que, apesar de resultar numa divergência quanto à noção de privacidade burguesa, também constitui sujeitos e identidades que socializam num ambiente dinâmico controlado por um emaranhado burocrático digital que, em poucas palavras, permite que as empresas de tecnologia comercializem e manuseiem informações privadas como mercadorias. Ainda no contexto norte-americano, outro elemento importante a respeito da privacidade é o "Ato de privacidade de 1974" [82], iniciativa que surgiu com o intuito de regular a recolha, uso e a disseminação de informações pessoais realizada por agentes federais e prevenir técnicas de vigilância ilegais após o escândalo Watergate, que entre outros aspectos ligados a atos de corrupção, resultou no pedido de renúncia do então Presidente Richard Nixon[83]. A criação do ato de privacidade de 1974 procurava restabelecer a confiança na democracia norte-americana e impor limites sobre o manuseio de informações privadas, que atualmente se soma a mecanismos específicos de âmbito estadual que ressaltam o caráter poroso da noção de privacidade no país, e explica as demandas que promovem a criação de mecanismos de âmbito federal que regulamentem o campo da privacidade na era digital, tornando transparente a compreensão sobre o uso de informações privadas para o público em geral.

[80] "Fotografias instantâneas e empresas jornalísticas invadiram os recintos sagrados da vida privada e doméstica; e inúmeros dispositivos mecânicos ameaçam cumprir a previsão de que "o que é sussurrado no armário será proclamado do alto das casas" (Warren, S., & Brandeis, L. 1890:195).

[81]Dal Bello discute a concepção de Paula Sibilia (2008) sobre evasão da privacidade, e a influência da cultura mediática inscrita no uso das redes sociais, e na dinâmica de partilha constante da vida pessoal que questiona a aplicabilidade da invasão da privacidade quando confrontada com a lógica de funcionamento do Facebook, bem como com o comportamento da geração Y que procura expandir os limites da privacidade tradicional em busca de um mundo "mais aberto" (Dal Bello, 2011: 144-146).

[82]Ver *Privacy act 1974.*

[83] Ver Enciclopedia Britannica. Richard Nixon.

À medida que a tecnologia da informação é incorporada nas distintas áreas da vida social cotidiana, mais se apresentam sinais de desgaste de noções tradicionalmente constituídas como no caso da privacidade, o que reflete na relação que os usuários de redes sociais estabelecem com a imagem de forma efêmera e utilitária. Paula Sibilia e Ligia Diogo (2011) discutem as "vitrines da intimidade" e a forma como a imagem, neste caso o retrato fotográfico, deixou de ser um elemento que permitia o indivíduo ligar-se ao seu passado e recordar lembranças de experiências que alcançavam o território da intimidade (e até do sagrado) através dos registos fotográficos de familiares. Segundo as autoras, esta dimensão contrasta com a lógica das redes sociais que alterou esta relação e substituiu a dinâmica da elaboração e preservação do álbum de fotografias pelo uso de dispositivos que se articulam rapidamente às redes sociais, alimentando fluxos incessantes de publicações em busca de interações superficiais cujo objetivo é criar regularidade de conteúdo que literalmente expõe a rotina dos utilizadores no espaço digital de forma voluntária. A constância na renovação do conteúdo sugere a desvalorização da imagem e da privacidade nos ambientes virtuais, uma vez que a sua efemeridade faz com que rapidamente caiam no esquecimento; o conteúdo das redes sociais tende a ser ordenado dando prioridade de visualização às publicações recentes, criando de forma implícita uma constante necessidade de manutenção das vitrines da intimidade. Esta característica enfatiza o caráter transformador que a tecnologia da informação assume ao remodelar hábitos culturais, transformando a forma como nos relacionamos com a imagem, e afetando o imaginário coletivo a partir de fatores econômicos e políticos inscritos no funcionamento das redes sociais.

A privacidade condicionada ao consentimento

Na medida em que cresceu a utilização das plataformas digitais, cresceram também as estratégias que buscam tratar das questões da privacidade, bem como proteger os interesses das partes envolvidas. Paralelamente, desenvolveram-se regulamentos como o GDPR, que ambicionam implantar mecanismos de proteção de dados digitais capazes de abranger os países membros da União Europeia através do controlo individual da informação ligado ao consentimento prévio; no contexto norte-americano, desenvolvem-se diversos mecanismos de abrangência local que regulamentam em diferentes níveis a proteção de dados no país, e dificultam tanto o entendimento dos utilizadores, como a aplicação de políticas em âmbito nacional. Este cenário revela que, seja de forma ampla e unificada, ou de forma fragmentada, a abordagem sobre a proteção de dados no Ocidente tem em comum a premissa do consentimento como fator essencial para permitir ou restringir o processamento de dados pessoais.

Esta premissa pode ser positiva do ponto de vista comercial se pensarmos no espaço virtual como um ambiente comercial que exige a aceitação de condições específicas para seu uso. No entanto, esta lógica deixa de lado os serviços que não se apresentam aos utilizadores enquanto relações comerciais, como no caso das redes sociais, que mesmo sem demonstrar explicitamente seu caráter comercial,

trabalham baseadas na lógica do aceite aos termos e condições dos utilizadores. Como fizemos já referência, estes "termos e condições" muitas vezes são longos, vagos e complexos, o que possivelmente faz com que muitos utilizadores os aceitem sem a devida análise crítica das reais utilizações dos seus dados pessoais, tornando este mecanismo de privacidade uma mais-valia positiva somente para a proteção das empresas envolvidas nesta relação. Em último caso, o utilizador forneceu o consentimento para o processamento de dados pessoais deixando a empresa em uma posição conveniente, restando pouca ou nenhuma ação em relação aos efeitos que estas atividades podem lhe causar.

Partindo deste enquadramento, importa propor uma reflexão que questione o fato das empresas tecnológicas fornecerem estes termos e condições disponibilizados de forma burocrática, pois ainda que elas tenham o consentimento individual, isto não lhes garante o direito de realizar o processamento de dados pessoais que possam causar danos aos utilizadores; no mesmo sentido, indivíduos que emitem o consentimento (de forma consciente ou não) não devem tornar-se responsáveis por fiscalizar as ações das empresas, por exemplo, ao optarem por fazer parte de uma rede de interações *online*.

Mais do que fornecer condições extensas de utilização dos serviços digitais, é necessário que se construam estruturas independentes que disponham de políticas claras quanto ao uso de informações privadas que estabeleçam uma relação de confiança entre utilizadores e empresas[84]. Da mesma forma, é necessário que se consciencialize a comunidade digital sobre a utilização que as empresas fazem dos dados pessoais, principalmente tendo em conta a sua responsabilização quanto aos possíveis danos às diferentes comunidades por parte dos produtos disponibilizados no mercado, sobretudo se estas informações são partilhadas com as forças de segurança.

Antes de explorarmos um caso de violação de privacidade relativo ao ambiente das redes sociais, importa destacar um fator relevante sobre a discussão da temática da privacidade e os seus desdobramentos na contemporaneidade. Ao pensarmos criticamente sobre o Reconhecimento Facial e os riscos que o uso desregulado desta tecnologia pode provocar no domínio da privacidade, recordamo-nos dos atos e tratados de privacidade de natureza individual mencionados, porém é necessário termos em conta que algumas destas formulações desenvolveram-se a partir de contextos totalmente diferentes do que vivemos atualmente.

A influência das tecnologias da informação, da Inteligência Artificial e da lógica *Big Data* tinham pouco ou nenhum espaço na vida privada há algumas décadas, portanto não representavam reais riscos individuais ou coletivos na esfera social. Discutir a problemática da privacidade nesta investigação tem como base analisar o cruzamento de informações pessoais no âmbito digital destacando o desgaste do conceito de privacidade por um lado, e por outro lado, refletir sobre as transformações e os desafios

[84]Woodrow Hartzog aborda a temática da privacidade baseada na lógica da "notificação e escolha" desde a década de 1990, e argumenta "Até hoje, esses acordos existem em grande parte para proteger legalmente as empresas e não para informar totalmente os usuários de forma inteligível". Ver One Zero *User agreement are betraying you.*

atrelados às novas estruturas de privacidade que surgem a partir do desenvolvimento tecnológico. Uma vez que a noção de privacidade ganha novos contornos, a análise deste contexto convoca abordagens renovadas que interpretem esta realidade tendo em conta os limites da noção de privacidade tradicional, e da sistemática da "notificação e escolha" onde o consentimento atua como elemento chave desta equação. Visto que a natureza analítica *Big data* impõe análises de dados individuais agrupados (ou seja, dados coletivos) classificados por algoritmos de forma automatizada, criam-se blocos de dados coletivos que utilizam algoritmos que buscam associar, por exemplo, informações biométricas com outras classes de dados (e.g. dados pessoais de contato, morada) de forma infinitamente variada para a tomada de decisões, e a influencia das indeterminações epistêmicas e o caráter hierarquizante e interseccional dos sistemas de identificação facial tende a expor os indivíduos por trás destes dados de maneira prejudicial.

Esta dinâmica de classificação de dados coletivos não está prevista pelos mecanismos de privacidade uma vez que este cenário refere-se às questões ligadas aos direitos coletivos. Ou seja, o processamento desta classe de dados sugere a hipótese da categoria de *danos coletivos* que os mecanismos de privacidade individual e a lógica do consentimento individualizado nem sempre são eficazes, pois o consentimento emitido num contexto pode não ter a mesma validade quando processado de forma descontextualizada; por outro lado, negar o consentimento tampouco garante que um indivíduo não se torne alvo de algoritmos que busquem, por exemplo, associar modelos faciais capturados em imagens de outros usuários, pois "A era do *machine learning* efetivamente torna a negação individual do consentimento sem sentido. Mesmo se eu me recusar a usar o Facebook ou Twitter ou Amazon - o fato de que todos ao meu redor aderiram significa que há tantos pontos de dados sobre mim para atingir-me[85]". Dito por outras palavras, a sistemática de associação algorítmica constante grava as informações capturadas em imagens e busca associá-las com potenciais usuários, mesmo que estes tenham negado o consentimento para uma rede social digital, ou seja, o contexto das interações *off-line* o insere de volta ao fluxo digital, ainda que de forma involuntária. Deste modo, refletir sobre a real efetividade destes mecanismos torna-se um uma prioridade para tratar os aspectos da privacidade no mundo digital.

A lógica da obtenção de consentimento para processar dados pessoais é efetiva para mediar relações explicitamente comerciais entre utilizadores e empresas, em que o consumidor procura um determinado serviço, e ao compreender os termos de uso pode optar por permitir ou não que este processamento aconteça. Trata-se de uma relação que envolve a venda de serviços condicionada a detalhes contratuais que oferecem liberdade de escolha aos utilizadores de aceitá-las ou não, e esta é uma prática compreensível uma vez que o espaço virtual seja utilizado para tal. No entanto, no caso das redes sociais, onde não existe uma relação comercial explicitamente estabelecida entre as partes, o

[85] A publicação do Centro de políticas Cibernéticas da universidade de Standford *Freeman Spogli Institute* aborda este aparente descompasso entre os sistemas que regulamentam a privacidade do ponto de vista individual, e a forma como o processamento de dados eleva a categoria para um dano de nível coletivo. Ver *The data Delusion: Protecting Individual data isn't enough when the harm is collective*.

vínculo estabelecido depende da confiança que o utilizador deposita na rede social como um mecanismo de socialização. Na medida em que as interações sociais e digitais se confundem, e que as práticas organizacionais sofisticam a intrusão a partir da análise de dados coletivos, resta-nos propor um questionamento: até que ponto é oferecido aos indivíduos a opção de não utilizar estes serviços?

O desgaste da noção de privacidade alterou a forma como nos relacionamos com a imagem no universo digital, incluindo a privacidade num universo virtual ainda em construção. Diante deste contexto, a teoria da integridade contextual de Helen Nissenbaum (2004) ajuda-nos a refletir sobre a privacidade a partir de diferentes contextos com diferentes fluxos de informação. A partir dela observa-se uma estrutura de proteção à privacidade pautada pela premissa de que todos os setores da vida social são permeados por diferentes normas informacionais que desenham os arranjos de privacidade consoantes ao contexto situacional, e a partir de expectativas específicas. Vejamos como podemos utilizar esta ferramenta teórica para analisar o contexto específico da privacidade digital e a forma como o consentimento operacionaliza os aspectos da privacidade num ambiente maioritariamente comercial.

A privacidade na esfera digital

Uma vez que a sociedade utiliza o espaço digital para realizar diferentes tarefas, seja com finalidades de pesquisas, compras, socialização, ou atividades ligadas ao funcionamento da burocracia estatal, percebemos que conceber este espaço como um ambiente exclusivamente comercial representa uma limitação conceptual, pois neste enquadramento os aspectos da privacidade são orientados a partir de premissas similares às de transação de valores, o que supõe que o tratamento de informações pessoais e biométricas ocorra tal como o gerenciamento de bens de consumo ou serviços.

Nissenbaum (2011) propõe que o espaço digital seja tratado como uma arena pública que permite inúmeras formas de interação, incluindo cenários que não se apresentam ao público na forma de operações comerciais. Esta proposta baseia-se na integração de processos econômicos, sociopolíticos e culturais no ambiente digital em virtude do desenvolvimento tecnológico nos séculos XX e XXI que transformou os hábitos da população, e ampliou o escopo de serviços de forma inédita, sobretudo após os desdobramentos da pandemia da COVID-19 que impôs medidas de distanciamento social por questões de saúde pública, algo que intensificou ainda mais a transição de serviços para modelos digitais. É importante ter em conta que esta proposta não pretende considerar a noção de privacidade digital (*online)* como algo totalmente distinto da privacidade tradicional (*off-line)*, pois muitas das atividades que realizamos digitalmente eram antes realizadas de forma presencial a partir de normas específicas de tratamento de informações pessoais, ou seja, na medida em que prestadores de serviços como bancos e instituições incorporam a internet como uma ferramenta para mediar operações, não se cria um novo tipo de privacidade, mas sim um processo de transição de estruturas sociais complexas

que denotam a integração e a relação complementar das esferas *online* e *off-line*, e não uma relação de oposição conceitual (Nissenbaum, 2011:33).

Tendo em conta natureza diversa que o espaço virtual apresenta e disponibiliza praticamente todo tipo de serviço operado por meio de uma sequência de *clicks*, uma pessoa que opta por não fornecer o consentimento aos termos de privacidade de um *website,* ou que decide não participar de uma rede social como o Facebook, opta deliberadamente por não ter acesso a determinadas informações e deixa de participar de parte da vida social que foi assimilada pela plataforma numa relação que entrelaça as esferas *online* e *off-line,* onde a privacidade é negociadas a partir da lógica do "pegar ou largar". A rejeição dos termos disponibilizados por fatores como a incompreensão transforma-se num impeditivo que afeta a socialização de indivíduos, e não em uma possibilidade de escolha real. "Largar", neste contexto, não significa uma escolha livre fundamentada na plena compreensão do funcionamento de mecanismos difusos, mas sim numa escolha que assenta a responsabilidade do isolamento digital voluntário no utilizador e limita as interações digitais a partir de termos generalistas que por vezes não deixam claro o que é feito com as informações pessoais, nem quem terá acesso a tais informações, ou sob quais condições estas transações ocorrerão. A dificuldade de compreensão destes termos, na sua maioria elaborados com linguagem técnica pouco comum aos não familiarizados com o domínio computacional; ou vagos quanto aos possíveis usos dados a estas informações torna difícil a compreensão sobre o tratamento das informações pessoais após dado o consentimento, e cria o risco de que usuários sejam induzidos a aceitá-los somente pela ânsia de estar inserido na dinâmica das redes sociais, configurando um cenário que afeta não apenas a livre escolha, mas também a relação de transparência estabelecida entre as empresas e os usuários das redes sociais (Nissenbaum 2011: 34-35).

Tomando como exemplo a política de uso de informações pessoais disponibilizada pelo Facebook, antes mesmo de uma pessoa criar uma conta a página coloca questões sobre o uso de *cookies*[86] para personalizar os conteúdos e serviços oferecidos pela plataforma, e mostrar anúncios supostamente mais relevantes ao utilizador. A pessoa que escolhe "gerir definições de dados" depara-se com uma caixa de diálogo com uma série de informações sobre o uso de *cookies* com mais de 4,600 caracteres que pretende resumir a política de cookies[87] com pelo menos 18 hiperligações. Estas hiperligações conduzem a diversos outros sítios *online* que, por seu turno, disponibilizam uma infinidade de possibilidades sobre as definições de publicidade e controlo de dados de atividades fora

[86] *Cookies* em linguagem simples são ficheiros utilizados para identificar um computador (ou dispositivos móveis) ou usuário no domínio da Internet. Estes ficheiros podem conter dados individuais como os nomes de usuários ou senhas de acesso a um *website,* e normalmente são rastreados pelas empresas de tecnologia sob o discurso de melhorar a experiência de navegação dos usuários.

[87] A política resumida de cookies pode ser consultada na página inicial do Facebook. Ver https://pt-pt.facebook.com/ Acedido em 20/05/2021. O anexo 1 apresenta as caixas de diálogo disponibilizadas pelo Facebook no que se refere a política de *cookies,* que se constitui de aproximadamente 12 mil caracteres com 25 hiperlinks que conduzem o usuário a um verdadeiro oceano de informações de difícil compreensão.

da plataforma, cuja leitura integral pressupõe que o utilizador compreenda este universo de informações para tomar uma decisão consciente sobre a utilização dos serviços da plataforma.

É importante observar que o resumo da política que procura esclarecer as questões relativas ao uso de *cookies* destaca o botão em azul, sugerindo ao utilizador a decisão de simplesmente "Aceitar tudo" e dar seguimento à experiência na plataforma. Esta opção é seguramente tentadora quando uma pessoa se depara com tamanha quantidade de informações a serem analisadas antes de utilizar uma plataforma de socialização *online*, por um lado, e por outro lado, implica uma tomada de decisão induzida que torna esta forma de gerir a privacidade uma mera alegoria jurídica cuja efetividade burocrática sobrepõe a figura da plena compreensão e da livre decisão de uso da plataforma:

Fonte: Facebook, inc (Página inicial)

Assim sendo, fica evidente que o uso da plataforma está condicionado ao constante rastreio de informações pessoais justificado pela aceitação das condições que implicam fazer parte de uma complexa rede de anúncios personalizados consoante o comportamento individual dos utilizadores dentro e fora do Facebook. Esta dinâmica, que prevê a compreensão de políticas apresentadas em linguagem técnica sobre o domínio computacional demonstra o que Nissenbaum discute quanto ao "paradoxo da transparência" inerente ao processo de aviso e consentimento (notificação e escolha) (2011: 35-36).

O facto de o Facebook fornecer um imenso conjunto de informações técnicas ao solicitar o consentimento individual, não significa que estas informações serão totalmente compreendidas quando o utilizador emite o consentimento, tornando a transparência sobre o processo de escolha um aspecto frágil. Não se estabelece transparência apenas por disponibilizar um conjunto de informações de forma burocrática; este processo deve procurar transmitir informações concretas que auxiliem a decisão do utilizador informando as consequências ligadas ao processamento de informações pessoais de forma inteligível. Por outro lado, esta é uma questão desafiadora, pois resumir demasiado estas informações pode resultar em interpretações superficiais que não conseguem traduzir todos os aspectos importantes para a tomada de decisão diante da ausência de práticas comprovadas de um ramo recente; Adicionalmente, este processo pode relacionar questões que dependem do interesse comercial de revelar detalhes sobre o comércio de dados digitais, além de estratégias comerciais que o núcleo executivo empresarial pode não ter interesse em torná-las pública. Assim, é importante refletir que a

concepção destas políticas não é pensada para apresentar todas as possibilidades de uso dos dados pessoais em virtude de aspectos que, ao serem públicos, revelam aquilo que garante destaque e competitividade comercial no mercado, sendo assim, a arena da privacidade é invadida pela lógica comercial através de uma estrutura pouco transparente quanto à comercialização e o processamento de informações pessoais como bens de troca.

Um caso de 2015 que ilustra a questão da violação de direitos de privacidade digital ocorreu no Estado de Illinois, EUA, onde mecanismos de leitura e Reconhecimento Facial utilizados pelo Facebook tornaram-se objeto de ação judicial por não seguirem os parâmetros adotados sobre a privacidade estabelecidos pelo BIPA no Estado de Illinois. Trata-se de um processo em que utilizadores da plataforma denunciaram violações estatutárias de privacidade quando identificaram o processamento de informações biométricas feito por mecanismos de Reconhecimento Facial associados à função de etiquetagem de usuários da plataforma em fotografias. Neste processamento, o sistema fez uma leitura de imagens em que extraiu características únicas dos rostos identificados, criando uma "assinatura facial". Uma vez que esta assinatura facial possua um modelo facial correspondente no banco de imagens da empresa, o sistema estabelece a conexão das informações de forma automatizada e sugere etiquetar os usuários identificados. Porém, a ausência de consentimento expresso por parte dos utilizadores para este tipo de processamento fere as secções 15(a) e 15(b)[88] que abordam o tratamento de informações biométricas bem como as obrigações estatutárias específicas a serem seguidas na região.

Uma vez que o Estado de Illinois baseia-se nas premissas específicas do BIPA quanto ao tratamento de informações biométricas, o processamento destas informações fica condicionado ao consentimento expresso dos envolvidos que previa a apresentação de cronogramas de destruição de dados biométricos sempre que já tenha sido alcançado o objetivo inicial relacionado à coleta destas informações, ou após três anos da ultima interação do indivíduo com a entidade privada. No caso Patel vs. Facebook[89] estas condicionantes não se verificaram. O caso ganhou grande repercussão após o recurso interposto pela defesa do Facebook ter apresentado argumentos sobre a inexistência de danos concretos aos interesses pessoais da acusação, porém visto que o propósito regulamentar do BIPA tem como foco regular a privacidade e o processamento de informações biométricas, e que o uso da tecnologia de Reconhecimento Facial de forma não consentida resulta em potenciais riscos materiais à privacidade dos envolvidos, a simples violação estatutária constitui-se como elemento suficiente para permitir a acusação de fundamentar sua queixa. O processo tramitou nos tribunais norte-americanos, e

[88] A seção 15 do BIPA dedica-se a regulamentar a dinâmica da coleta e processamento de informações biométricas estabelecendo diretrizes que prevêem a divulgação de prazos de retenção destas informações, e o não cumprimento destas normas configura-se na violação estatutária de interesses concretos na privacidade por representar um risco material aos envolvidos. Ver BIPA.

[89] Adam Pezen, Carlo Licata e Nimesh Patel, residentes em Illinois na ocasião são as partes representadas na acusação que se baseou na secção 20 do BIPA que prevê que qualquer pessoa prejudicada pela violação desta lei tem o direito de acionar judicialmente a empresa nos tribunais federais em busca de reparação. Ver: *Patel vs. Facebook, Inc.*, 932 F.3d 1264 (9th Cir. 2019)

em fevereiro de 2021 as partes concordaram em encerrá-lo, indenizando os impactados pelos danos causados à privacidade visual e gerando um prejuízo inicial em torno de 650 milhões de dólares, o que abriu precedentes para que outros utilizadores reclamassem o seu direito à privacidade acionando a empresa judicialmente[90].

O caso Patel vs. Facebook aborda aspectos importantes sobre a privacidade e evidencia a importância de se estabelecerem regras claras voltadas para a finalidade específica do processamento de dados biométricos, bem como dos conflitos com a realidade das empresas de tecnologia que por vezes processam informações pessoais em escala, tratando-as como *coisas* dissociadas de suas identidades, e negligenciando estatutos que regulam o tratamento deste tipo de informações. Esta interação revela uma relação problemática em matérias de ética corporativa da Inteligência Artificial que desestabiliza a confiança dos utilizadores na medida em que se torna pública a prática do processamento de informações de forma não consentida, algo legalmente condenável a partir da regulamentação BIPA diante das incertezas sobre os desdobramentos das decisões automatizadas[91]. Seja por conta do volume de dados biométricos que a plataforma recebe e processa diariamente através da exposição das vitrines da intimidade, ou pela influência comercial do universo digital, o processamento destas informações de forma descontextualizada não obedece às diretrizes estabelecidas pelo ato de privacidade BIPA[92].

Este caso representa uma vitória importante para a proteção da privacidade, no entanto limita-se apenas ao Estado do Illinois, e considerando a presença do Facebook a nível transnacional ainda há um longo caminho pela frente, porém ele inspira uma reflexão crítica sobre a privacidade na esfera digital e representa um passo em busca de perspectivas que defendem a regulamentação da privacidade *online* em parâmetros nacionais. A maneira como o estatuto BIPA regulamenta o processamento de informações biométricas assemelha-se ao modo como este tipo de informação é tratado no mundo *off-line*, ou seja, obedece a normativas específicas que zelam pelo tratamento destas informações dentro dos contextos específicos. Esta prática está de acordo com a proposta inicial de Nissembaum sobre a importância de não diferenciar a privacidade digital da privacidade *off-line*, mas sim de incorporar este domínio na já construída arena da privacidade, adaptando-a a realidade da vida social que compreende ambos os universos a partir normas previamente estabelecidas, em vez de pensar nela de forma distinta a partir de novos termos.

A proposta da integridade contextual da privacidade promove a reflexão de parte do espaço virtual como um ambiente público, sujeito a regras estritas ligadas ao contexto em que as informações

[90] A tribuna de Chicago noticiou em abril de 2021 a possibilidade de o Facebook ter de indenizar aproximadamente 1,6 milhões de usuários residentes em Illinois diante de violações estatutárias de privacidade que o caso Patel vs. Facebook trouxe à tona. Ver *Waiting for your $345 from the Illinois Facebook privacy settlement? Here it's why it's delayed.*

[91] A secção 5 (f) do BIPA prevê a regulamentação estrita de dados biométricos visto que a ramificação do campo das tecnologias biométricas ainda não é totalmente compreendida.

[92] A secção 10 do BIPA prevê a identificação biométrica de forma específica: "Identificador biométrico é o processo que faz a leitura da retina, íris, impressão digital e de voz e a leitura da geometria das mãos e do rosto".

foram obtidas, sobretudo em matéria de identificação biométrica, pois a maneira como determinadas práticas comerciais podem perturbar os diferentes fluxos informacionais não é apresentada de forma clara na lógica burocrática do consentimento, e esta forma de conceitualizar a privacidade preserva o caráter individual e único das informações, além de sustentar a confiança nas instituições que se encarregam delas (Nissenbaum, 2011:39-40; 43).

A privacidade é certamente um aspecto impactado pela Cibercultura através das múltiplas mediações que as tecnologias da informação operacionalizam na vida social. Este impacto revela-se nas estruturas associadas ao controlo de informações biométricas criando a categoria de danos coletivos ainda pouco explorada pela literatura contemporânea. Isto impõe desafios que procurem integrar e ajustar os aspectos da privacidade de acordo com o contexto em que estas informações são fornecidas, partindo de normas claras que não depositem o ônus do processamento de informações biométricas somente nos usuários de forma burocrática ou induzida. Esta reflexão propõe conceber parte do universo digital como um ambiente que trabalhe a favor da privacidade, valorizando a ética e a responsabilização das empresas quanto aos danos provenientes destas atividades como um ponto central para orientar o tratamento de informações biométricas. Perspectivas como a da integridade contextual e casos como a vitória estatutária do BIPA em Illinois começam a traçar este caminho. Este é um caminho que deve ser trilhado de forma justa e transparente para que o espaço virtual se torne um ambiente seguro tanto para as empresas de tecnologia como para os utilizadores, que devem estar informados sobre o processamento de informações biométricas para tomarem decisões conscientes sobre as escolhas conectadas aos meios de interação social, e sem temer que as empresas utilizem estas informações de forma descontextualizada e irregular.

Questões de privacidade e vigilância

Conceber parte do espaço digital como domínio público é um fator importante para a proteção de informações biométricas visuais, pois permite classificar estas informações em níveis de confidencialidade que estruturam o acesso aos diferentes fluxos informacionais, evitando o uso indevido de informações privadas por parte de empresas que vêem no processamento contínuo de dados uma fonte de expansão comercial disfarçada pela dinâmica do engajamento social. No entanto, importa compreender que da mesma forma que o processamento de informações biométricas sob a lógica comercial cria perturbações dos fluxos informacionais, o mesmo ocorre se o agente responsável por estes processamentos na esfera do Estado o faz a partir de perspectivas que colocam em causa o direito a privacidade.

O tratamento de informações biométricas que associam o uso do Reconhecimento Facial a práticas de vigilância é um dos fatores que convoca a discussão sobre a privacidade em locais públicos, pois além do viés sistémico impregnado no funcionamento dos sistemas de Reconhecimento Facial que atinge comunidades específicas em termos de representatividade e desempenho, os

comportamentos discriminatórios e as práticas de vigilância racializada podem influenciar a tomada de decisão em contextos de segurança, representando um perigo real para a subjetividade dos indivíduos submetidos à vigilância massiva e intrusiva. Como vimos, a privacidade pensada em espaços privados suscita a mudança das estruturas que a regulam, pois a inclusão da tecnologia da informação mediando aspectos triviais da vida social abre discussões relacionadas à emissão de consentimento, e a transparência das fases de processamento de dados biométricos, sobretudo na criação de bancos de dados que treinam algoritmos de Reconhecimento Facial.

Porém, quando pensamos sobre violações de privacidade em ambientes externos, a natureza do ambiente público pode confundir a aplicação da lógica da privacidade perante o discurso de que não se deve haver expectativa de privacidade nestes tipos de espaços. Nissenbaum discute esta formulação elucidando falhas conceptuais nas abordagens sobre a privacidade tradicionalmente baseadas em três princípios básicos: limitar a vigilância de cidadãos e evitar o uso destas informações contra a população; restringir o acesso a informações sensíveis e privadas; conter a intrusão em locais determinados privados ou pessoais (2004: 125-130), neste sentido, nota-se uma lacuna que limita o debate da privacidade no caso de ambientes externos e invalida a estrutura da privacidade individual em locais públicos. Dito por outras palavras, uma concepção de privacidade estática que não captura uma releitura do conceito de forma flexível e ajustável conforme se alteram os hábitos culturais e sociais.

Novamente recorreremos à estrutura da integridade contextual e a valorização do contexto como um elemento central para determinar as normas e práticas específicas que orientam os fluxos de informações nas diferentes esferas da vida social, evitando limitar o argumento apenas na dicotomia entre público e privado, pois ela não nos parece suficientemente ampla para abordar a complexidade que a mediação tecnológica apresenta na atualidade. Partindo desta hipótese, a natureza do lugar é apenas um dos fatores a ter-se em conta nesta equação. O *contexto* onde se disponibilizam certas informações pessoais faz parte do espectro culturalmente convencionado que estabelece a confiança da população em fornecer informações num ambiente específico e seguro, onde se supõe que estas informações jamais serão utilizadas contra quem as forneceu, muito menos que sejam compartilhadas de forma irrefletida. Portanto, incluir o contexto como fator que orienta a regulamentação da privacidade implica em levarmos em consideração que diferentes contextos implicam em distintas normas para os múltiplos fluxos informacionais cotidianos.

Traduzindo esta formulação para o caso das informações pessoais biométricas, a autora destaca aspectos que orientam a privacidade a partir da "integridade contextual" que preveem duas normas básicas quanto à regulamentação dos fluxos de informações: "As normas de adequação e de distribuição de informações pessoais" (2004: 138). As normas de adequação são aquelas em que se estabelece o quão apropriado é revelar informações pessoais de outrem em diferentes contextos e, neste sentido, o exemplo da medicina ilustra o funcionamento deste fluxo informacional. Um paciente que revela informações pessoais médicas a um profissional da saúde o faz para atender objetivos

específicos[93] ligados à busca de informações ou tratamentos. Mediante consentimento do paciente, é expectável que estes profissionais compartilhem estas informações com os seus pares em contextos profissionais, sempre que o objetivo desta partilha se justifique para atender as expectativas do paciente. Porém, considera-se inapropriado que um médico exponha essas informações em contextos informais como conversas com amigos e familiares, pois esta prática apropria-se de informações obtidas num contexto e transfere-as para outro prejudicando a integridade contextual, e perturbando o fluxo informacional das informações recolhidas em procedimentos que seguem normas éticas estritas quanto à confidencialidade dos dados dos pacientes.

As normas de distribuição são aquelas que regulam e mantém os fluxos informacionais em pleno funcionamento, ou seja, estabelecem os limites sobre o acesso a informações privadas sob condições específicas que variam consoante o contexto. No caso da Medicina, a distribuição de informações pessoais de pacientes nos Estados Unidos requer o consentimento destes em diferentes práticas que abrangem desde a procura por tratamentos, até a esfera comercial da indústria farmacêutica. Cada uma destas práticas dispõe de mecanismos específicos que garantam a proteção adequada destas informações (Nissenbaum, 2004: 138-143). Um exemplo deste tipo de situação mais próximo do universo do Reconhecimento Facial apresenta-se na utilização de imagens publicadas nas redes sociais, que repentinamente se transformam em dados que alimentam bancos de imagens para treinar algoritmos utilizados pelas forças de segurança para identificar indivíduos em gravações de câmeras de segurança, independente se estes são suspeitos ou não.

O relatório *Face off* destaca a maneira como o FBI trabalhou com o repositório *NGI-IPS* (banco de dados biométricos utilizado pelo FBI) para viabilizar o processamento de diferentes informações pessoais e biométricas utilizando técnicas de Reconhecimento Facial em imagens provenientes de bancos de dados de âmbito civil e criminal, o que ilustra o cruzamento de distintos fluxos informacionais mencionado, e em 2016, pelo menos 51 milhões de fotografias obtidas nestes termos já estavam sujeitas a tecnologia de Reconhecimento Facial. O repositório de informações biométricas *NGI* dispõe de informações como impressão digital, registros de íris e da palma da mão ligadas às rotinas burocráticas de verificação de históricos criminais *(Background check)*, ou de obtenção de licenças de condução. O *IPS*, por seu turno, é a secção responsável pelo gerenciamento das imagens obtidas nestas rotinas, permitindo-nos concluir que a combinação destas informações para finalidades terceiras cria conflitos que interferem no objetivo inicial para o qual estas informações foram coletadas, e realçam o aspecto intrusivo e autoritário por meio do qual as forças de segurança norte-americanas fazem uso de tecnologias de Reconhecimento Facial (Lynch, 2018: 14).

[93] A confiança *(supporting assurances)* estabelecida em procedimentos médicos como cirurgias advêm das garantias associadas às práticas médicas no decorrer dos séculos, que contam com sistemas rigorosos de aprendizagem e treinamento, bem como diversos códigos de conduta profissional e instituições que consolidaram a Medicina como uma área especializada na saúde e no bem estar das pessoas, seja em ambientes privados ou públicos, o caráter assistencial da medicina deve sempre prezar pelo bem estar do paciente (Nissenbaum, 2011: 36)

Ainda no que se refere à utilização de imagens de fontes externas, o GAO em 2016 *(Government Accountability Office),* reportou números ainda mais expressivos quanto à utilização de recursos de Reconhecimento Facial por parte do FBI através do sistema FACE *(Facial analysis, comparison and evaluation system),* que teve acesso a aproximadamente 411 milhões de fotos, oriundas de registos obtidos do repositório *NGI*, além de registos ligados a aplicação de vistos de pelo menos 16 dos Estados norte-americanos (Lynch, 2018: 15).

Table 4: Number of Photos Available to Facial Analysis, Comparison, and Evaluation (FACE) Services by Repository as of December 2015

Searchable Repository	Description of photos in the repository	Number of photos[a] (millions)
Federal Repositories		
Department of Defense's Automated Biometric Identification System	Individuals detained by U.S. forces abroad, among others	6.7
Next Generation Identification - Interstate Photo System (NGI-IPS)	Criminal and civil mug shots[b]	29.7
Department of State's Consular Consolidated Database	Visa application[c]	140
State Repositories		
North Dakota	Driver's license, criminal mugshots, correction photos	1.2
Vermont	Driver's license	1.8
New Mexico	Driver's license	2.9
Delaware	Driver's license	4
Utah	Driver's license, criminal mugshots, correction photos	5.2
Alabama	Driver's license	6.5
Nebraska	Driver's license	8
South Carolina	Driver's license, criminal mugshots, probation photos	8
Tennessee	Driver's license	12.5
Iowa	Driver's license	13
Arkansas	Driver's license	15.4
Kentucky	Driver's license	18.4
Texas	Driver's license	24
Michigan	Driver's license, criminal mugshots, correction photos	35.6
North Carolina	Driver's license	36
Illinois	Driver's license	43
Total		**411.9**

Fonte Imagem: GAO Report, 2016: 48. *Número de fotos disponíveis para análise facial, comparação e Serviços de avaliação (FACE) por repositório em dezembro de 2015.*

Outro aspecto sublinhado no relatório *Face off* refere-se ao cumprimento dos protocolos federais que impõem que o FBI torne explícita as razões pelas quais a agência empreende a recolha e o processamento de dados biométricos (de variadas fontes), para atestar a conformidade com as diretrizes de privacidade presentes no Ato de privacidade de 1974 e no *E-government act* de 2002. Por um lado o ato de privacidade prevê que as agências governamentais notifiquem formalmente o Registo Federal sobre todo e qualquer sistema que colete e utilize informações pessoais de cidadãos norte-americanos por meio do Sistema de notificação e registos[94], e esta notificação deve especificar o tipo de informação coletada, bem como o uso e a proteção dada a esta informação. Por outro lado, o *E-government Act* prevê que as agências conduzam avaliações de impacto de privacidade[95] similares em nível de detalhe sobre a razão da coleta e do uso das informações privadas; exceto que no caso destas avaliações de impacto, as agências também devem informar com quem tais informações poderão ser compartilhadas. Segundo o relatório *Face off*, o FBI cumpriu com os protocolos de avaliação de impacto da privacidade em 2008, porém deixou de apresentar estas avaliações nos anos seguintes, voltando a apresentá-la novamente apenas no ano de 2015, após ter efetuado pelo menos 100 mil buscas utilizando técnicas de Reconhecimento Facial nos bancos de dados *NGI* e *IPS* (Lynch, 2018: 17-18).

Partindo do princípio que o funcionamento dos sistemas de Reconhecimento Facial apresenta limitações técnicas ao processar imagens de grupos específicos, é necessário refletir sobre a

[94] *System of Records Notice (SORN)*
[95] *Privacy impact assessment (PIA)*

probabilidade de que estes grupos sejam desproporcionalmente enquadrados em eventos relacionados ao problema dos falsos positivos. O FBI reconheceu este ponto como uma limitação dos sistemas que operavam o Reconhecimento Facial na altura, no entanto isto não se traduziu numa preocupação em termos de privacidade para a agência uma vez que a lógica do sistema baseia-se na criação de uma lista de possíveis suspeitos, e não na identificação positiva destes[96], o que demonstra ser um argumento inconsistente uma vez que o próprio repositório de informações biométricas do FBI possui uma estrutura (o *IPS*) dedicada a reunir fotos com o objetivo de aplicar técnicas de Reconhecimento Facial.

As questões de privacidade e do contexto em que as informações são disponibilizadas são relevantes tendo em conta a forma fragmentada como as informações biométricas são reguladas no país, e a assimetria de poder estabelecida quando a figura do Estado (neste caso, das agências de segurança) entra nesta equação é evidente. Por outro lado, a noção do consentimento emitido em contextos específicos se torna frágil quando estas informações passam a ser utilizadas de forma descontextualizada, sobretudo se pensarmos na perspectiva de que um julgamento criminal tradicional (não automatizado) prevê a necessidade da figura de um suspeito para iniciar uma investigação, que pode ou não incorrer em um julgamento criminal. Ainda que as forças de segurança façam uso de estruturas de específicas de poder que lhes permite adentrar a privacidade de indivíduos suspeitos para a manutenção da ordem pública, é desejável que isto ocorra com base nos mecanismos legais que autorizem uma determinada investigação (Marks *et al*, 2015:3).

Mesmo que a utilização do Reconhecimento Facial seja justificada para acelerar o processo de identificação de suspeitos, a imprecisão destes sistemas torna este processo momentaneamente ineficaz, e potencialmente injusto na medida em que indivíduos inocentes de determinados grupos são erroneamente identificados como suspeitos de crimes de forma automatizada por conta da ocorrência de falhas sistêmicas como no caso dos falsos positivos[97].

O cruzamento dos fluxos de informações pessoais e a automatização de processos criminais são elementos que, ao serem combinados como recurso nas funções de vigilância, posa riscos de violação de privacidade e limita os direitos e o exercício da democracia de forma coerente. O uso de dispositivos que gravam, identificam e julgam criminalmente indivíduos em tempo real a partir de indeterminações sistêmicas que nem os próprios cientistas conseguem explicar é uma hipótese

[96] Uma narrativa que tentou explicar que a criação de uma lista de suspeitos não se configura como uma identificação positiva de indivíduos. O FBI argumenta que a lógica desenhada para o sistema prevê que uma pessoa codificada como suspeita apareça em 85% das vezes na lista dos 50 prováveis suspeitos, sempre que o verdadeiro suspeito faça parte do banco de dados utilizado, o que não deixa clara a hipótese sobre o que ocorre quando o verdadeiro suspeito não faz parte do banco de dados utilizado, e expõe a falta de transparência sobre esta questão (Lynch: 2018:16).

[97] Robert Julian-Borchak Willians, residente do Estado de Michigan foi preso após ser erroneamente implicado como suspeito de furto numa loja na cidade de Detroit em 2020. O caso ganhou repercussão após se tornar público que a polícia utilizou um software de Reconhecimento Facial que "interpretou" a gravação de má qualidade dos arquivos de vigilância interna da loja que concluiu, após "interpretar" a foto antiga da licença de condução de Willians, levando-o a ficar sob custódia por 30 horas por engano. The Washignton Post.

importante para tornar o estabelecimento desta prática um tema central nos debates que abordam a ética das decisões automatizadas. Na medida em que estes recursos passam a ser utilizados pelas forças de segurança sem que sejam analisados os riscos associados ao uso, ou mesmo sem que o tema tenha sido debatido de forma aberta, a presença das forças de segurança passa a ser interpretadas como uma ameaça, e não como um fator que garante a segurança pública.

A presença de tecnologias de Reconhecimento Facial em contextos, por exemplo, de manifestação pública cria a possibilidade de limitar a participação de indivíduos frequentemente considerados alvos da policia, o que o relatório *Face off* denomina como *chilling speech*. Por outras palavras, este é o efeito do uso do Reconhecimento Facial no espaço público que limitam o direito de indivíduos de se expressarem livremente, desestablizando pilares da democracia norte-americana como a Primeira Emenda constitucional (Lynch, 2018:22). Ainda que esta prática tenha efeitos "socialmente tóxicos" do ponto de vista social, este tipo de situação já tornou indivíduos que defendem a causa *Black Lives Matter* alvo de perseguição policial na cidade de Nova Iorque[98].

Capítulo 5: Perspectiva Antropológica sobre a vigilância: Reflexão crítica a propósito da utilização de tecnologias de informação.

Partindo das experiências relatadas sobre o uso de tecnologias da informação em assuntos ligados à segurança, é possível inferir que este é um tema cuja reflexão crítica tem como imperativo a integração da diversidade de vozes que compõem a sociedade civil no que respeita o desenvolvimento, aplicação e supervisão destas técnicas em ambientes externos. Esta reflexão tem como objetivo evitar o cruzamento indevido de fluxos de informações privadas, e propor o cumprimento de princípios democráticos que tratem todos os diferentes indivíduos submetidos ao uso destes sistemas de forma igual.

A influência de lógicas sistêmicas pouco precisas no funcionamento de sistemas preditivos compromete o resultado proposto pelos seus *designers* como vimos no caso do sistema *Hunchlab*, pois o grau de indeterminação emanado por este sistema pode ter efeitos negativos na construção de estereótipos, criando técnicas de vigilância orientadas por *Big data* que reforçam preconceitos socioeconômicos sobre locais e grupos, além de evidenciar a performatividade que os dados numa estrutura que orienta a atividade das autoridades de segurança no contexto do patrulhamento.

[98]Derrick Ingram, co-fundador da organização *Warriors in thegarden* cuja demanda por justiça social critica a forma violenta e opressiva como a comunidade afro-americana é abordada pela polícia foi vitima de uma tentativa de prisão orientada pela leitura de modelos faciais de imagens publicadas na rede social Instagram. O motivo da perseguição teve como justificativa o fato de Derrick "gritar com um oficial de segurança utilizando um megafone", e nas palavras de Derrick "Estamos sendo especificamente visados com essa tecnologia por causa do que estamos protestando, e porque estamos tentando desconstruir um sistema do qual a polícia faz parte". Ver *Ban dangerous facial recognition technology that amplifies racist policing*. Amnestia International website.

Este processo permite-nos relacionar o que Tobias Matzner denomina como "visão representacional", uma visão que se potencializa durante a comercialização destes sistemas através da promoção de uma mais-valia que cria um imaginário de que a utilização desta tecnologia captura um fragmento preciso do mundo na forma de arquivos computacionais, supostamente possibilitando uma compreensão do mundo a um nível de detalhe jamais visto antes (Matzner, 2016:202). Tendo em conta as violações da privacidade contextual evidenciada pelo processamento de modelos faciais de forma não consentida, e a hipótese da continuidade de aspectos culturais que hierarquizam a interpretação da raça, o uso de técnicas de vigilância que tornam a presença policial ubíqua reproduzem o processo de vigilância integrada sistemática em situações onde esta estratégia tática nem sempre é necessária, impactando a relação estabelecida entre as forças de segurança e a sociedade civil. Na medida em que se verifica a tentativa do uso massivo do recurso de Reconhecimento Facial que geram efeitos negativos e que ganham grande repercussão mediática, isto pode criar um desconforto na sociedade e fazer com que o uso desta tecnologia não seja interpretado como um recurso eficiente, mesmo em casos onde existam riscos reais ao Estado, sendo assim, é necessário refletir quando, e em que situações as forças de segurança devem recorrer a este nível de controle.

Diferente do escopo da polícia na Europa do século XVIII que consistia em coordenar as atividades produtivas do homem e inculcar uma espécie de disciplina (poder disciplinar) eficiente o bastante para torná-lo uma ferramenta útil para o crescimento do Estado, os processos históricos responsáveis por gerir as populações globais complexificaram-se, e o que antes era de responsabilidade da polícia passou a ser controlado por ramificações do Estado repletas de especialistas em economia e política, além dos níveis de poder executivo, legislativo e judiciário num ambiente urbanizado bastante distinto da conjuntura pré-moderna. Estas mudanças alteraram o papel das forças policiais para uma figura mais recente em que ela se converte num mecanismo de segurança repressivo cuja função principal é conter situações de desordem, e garantir a segurança da sociedade contra ameaças que coloquem em causa a ordem social (Foucault, 2009). Neste sentido, o patrulhamento e a vigilância de ambientes externos fazem parte da função policial, e ao mesmo tempo em que permite o pleno funcionamento das engrenagens sociais dentro de parâmetros aceitáveis, posiciona a ideia de uma sociedade segura como uma condição e um meio para alcançar esta ordem (Foucault, 2006 apud Schwell, 2014: 85).

A ideia de vigilância construída a partir de previsões, ou cálculos de risco, e não da evidência efetiva de suspeitos, relaciona-se com a transformação do sistema criminal de justiça tradicional para um sistema de justiça atuarial (Freeley e Simon, 1994 apud Marks *et al*, 2015: 5) que trabalha mediante a potenciais riscos a segurança pública com a intenção de conter atividades que ainda não ocorreram, porém, uma vez que a lógica epistêmica das previsões apresenta indeterminações conceituais, a probabilidade de que uma previsão incorreta oriente a decisão algorítmica é um fator que coloca em causa a base desta transformação. Durante a era moderna, a influência do Panóptico de Foucault (1987) auxiliou a conceptualizar a vigilância como uma técnica que previa o exercício do

poder disciplinar a partir da observação constante, onde a disciplina se tornou uma política de Estado espalhada pelos setores públicos e privados de forma vertical. A partir da integração das tecnologias da informação nas tratativas de vigilância, esta configuração ampliou o alcance da vigilância, convocando a ideia de *Surveillant assemblage* trabalhada por Haggerty e Ericson (2000:608 apud Marks *et al*, 2015: 7) onde a coleta de dados pessoais de diferentes fontes e dispositivos passa a influenciar a forma como as técnicas de vigilância são colocadas em prática. Diferentemente de um poder central, que através da vigilância coerciva pretendia exercer o controlo populacional, este modelo de vigilância emana das relações estabelecidas com os dispositivos conectados às tecnologias da informação, tornando possível que qualquer pessoa seja vigiada a partir de dispositivos de geolocalização. Desta forma, à realidade dos contextos sociais atuais extrapolam a ideia do panóptico das sociedades disciplinares, pois os arranjos técnico-científicos ligados ao manuseio de grandes quantidades de dados, e a utilização de sistemas de policiamento preditivo desenhados para identificar indivíduos potencialmente suspeitos impõem uma realidade distinta da analisada por Foucault.

Diante deste contexto, o caráter performativo dos dados e os tipos de subjetividades que emergem desta lógica sistêmica nas etapas posteriores a recolha e processamento de informações se tornam uma preocupação para a análise dos contextos de vigilância atuais. A utilização das análises *Big data* em contextos de segurança reforçam o que Matzner discute à luz do pensamento de Deleuze (1992 apud Matzner, 2016: 203) quanto às formas de controlo social que utilizam as tecnologias da informação na produção de "Dividuos", ou seja, micro entidades (perfis) criadas a partir de interações no ambiente virtual que impõem aspectos específicos extraídos da atividade digital aos indivíduos na esfera real, o que no contexto da construção das subjetividades digitais, reproduz as figuras de indivíduos potencialmente pacíficos ou suspeitos.

A construção destas subjetividades a partir do fator da indeterminação fica sujeita à análise de comportamentos feita em escalas que determinam padrões de subjetividades ordeiras e suspeitas, e estes padrões criam perfis individualizados que orientam as decisões algorítmicas a criar representações que orientam a ação policial, o que significa que os "dividuos" gerados pelas análises de dados de indivíduos codificados de forma positiva (pacífica) e negativa (suspeita), constituem o ambiente que molda a decisão sobre as subjetividades a partir de padrões de comportamento mais ou menos delimitados por um lado, e probabilidades mais ou menos corretas por outro (Matzner 2016:203-204). Na medida em que as autoridades policiais diversificam as fontes que possibilitam a identificação de pessoas de forma automatizada, quer seja tendo acesso a banco de dados governamentais, ou a imagens provenientes de redes sociais, esta prática engendra um processo que confere aos dados um caráter performativo, reforçando estruturas de poder e de autoridade estabelecidas por meio de enunciados inscritos na esfera discursiva que aludem à noção de "citações" e do poder dos atos performativos (Derrida, 1977: 17; Butler, 1993: 227 apud Matzner 2016: 205).

O autor argumenta que um ato performativo é bem-sucedido porque "acumula a força de autoridade por meio da repetição ou citação de um conjunto de práticas autoritárias anteriores"

(Butler, 1993:226 apud Matzner 2016: 206). Esta proposição nos permite inferir que na medida em que um grupo específico é constantemente considerado suspeito, e, na mesma medida, outro grupo é constantemente considerado pacífico, o peso que estas repetições ganham na esfera social constrói diferentes tipos de subjetividades que prevêem diferentes tipos de tratamentos. Desta forma, as repetidas interpelações que surgem por parte das forças de segurança sobre potenciais suspeitos frequentemente apontarem para grupos marginalizados pode não ser uma mera coincidência, e sim representar atos performativos ligados a subjetividade de grupos que foram sistematicamente codificadas como suspeita. Ainda que esta proposta tenha em conta que este processo não ocorra de forma consciente, ela evidencia a forma como se estabelecem relações de poder orientadas pelas questões culturalmente enraizadas, que naturalmente são transferidas para o ambiente digital para reproduzir a mesma lógica.

Este enquadramento permite-nos refletir criticamente sobre o conceito de segurança a partir de uma perspectiva antropológica, isto é, enquanto uma categoria analítica cuja observação do desenvolvimento e do uso de tecnologias da informação evidencia práticas que impactam a sociedade como um todo, desfavorecendo indivíduos a partir de uma multiplicidade de danos provenientes da utilização de informações biométricas em matéria de segurança, e que, adicionalmente, impõe uma dimensão interseccional que afeta de forma mais intensa as populações marginalizadas. Assim sendo, o custo social relativo ao uso de tecnologias da informação sugerem que a vigilância integrada na temática da segurança pública pode potencializar os comportamentos discriminatórios e acentuar as desigualdades sistêmicas, portanto, provocando desdobramentos "socialmente tóxicos" nas dinâmicas sociais.

O viés algorítmico é um elemento presente na realidade digital por conta da maneira como processos históricos, culturais e políticos construíram práticas discriminatórias contra os grupos inferiorizados antes mesmo da invenção dos computadores, e na medida em que o domínio das ciências tecnológicas não demonstra beneficiar-se da multiplicidade da diversidade cultural, nota-se que este é um problema que não se inicia por conta da atividade digital; ele é apenas um reflexo da forma como as relações racializadas sempre impactaram as comunidades marginalizadas, exceto que, neste contexto, é possível identificá-lo a partir de uma análise crítica da Cibercultura.

A vigilância integrada em campo – Tensões sobre Reconhecimento Facial e os discursos de securitização

A análise de estudos que denunciam os efeitos sociais causados pelo uso pouco regulado de tecnologias de Reconhecimento Facial em determinadas regiões demonstra a existência de lacunas éticas que exigem atenção ao desenvolvimento e aplicação de tecnologias da informação em matéria de segurança. Fatores como a justiça atuarial e o caráter performativo de dados, atrelados a sistemática de decisões automatizadas desenham um modelo de justiça criminal automatizada que gradativamente

exclui a ação humana, e comprime os processos criminais transpassando elementos que protegem os indivíduos de eventuais abusos de poder do sistema criminal tradicional [99].

As novas formas de vigilância que classificam informações individuais em blocos e as processa de forma descontextualizada criam as bases que suscitam o processo de "suspeita categórica" uma vez que a utilização de sistemas que localizam, identificam, classificam e tornam indivíduos suspeitos de forma automatizada, transforma o processo tradicional de busca por suspeitos específicos para uma constante busca por indivíduos potencialmente suspeitos (Marx, 2004 e Marx 2011 apud Marks *et al*, 2020: 12), um processo que além de acelerar a lógica do julgamento criminal, seguramente é vendido com a intenção de minimizar custos operacionais. Adicionalmente, o contexto inerente às novas formas de vigilância sugere a perspectiva do Banóptico proposto por Didier Bigo (*apud* Browne, 2015: 38-39) como sendo adequada para compor esta análise, uma vez que os processos que hierarquizam e categorizam a subjetividade de indivíduos a partir de categorias de risco pouco precisas sugere que a atividade policial é orientada a partir de assunções sobre o comportamento de potenciais suspeitos, e pelo temor de prováveis riscos associados a estes indivíduos; uma espécie de paranóia social cuja motivação se dá por meio de previsões superficiais, e não por análises contextuais aprofundadas[100]

Por outro lado, a análise das novas técnicas de vigilância revela-se um tema complexo, pois ao utilizarmos o conceito de segurança como categoria analítica, inúmeros outros elementos juntam-se à equação para a reflexão sobre os custos sociais causados pela mediação das tecnologias da informação nos contextos de segurança pública. Um destes elementos refere-se ao papel dos discursos que influenciam o desenvolvimento e o uso destes mecanismos em matéria de segurança, mesmo que sua regulamentação ocorra nas fases posteriores da sua aplicação.

Alexandra Schwell (2014) analisa o impacto da esfera discursiva em torno do processo de securitização de ambientes e a forma como estes discursos moldam a opinião pública nos contextos de segurança através de elementos que normalizam a ideia de um estado de emergência constante, bem como dos processos que naturalizam o uso de técnicas de segurança intrusivas. Esta análise faz referência aos estudos da Escola de Copenhaga e os atos discursivos que classificam determinados assuntos como "tópicos de segurança" que tem o poder de suspender a aplicação de regras na presença de ameaças a segurança (apud Buzan *et al*, 1998).

Esta dimensão discursiva prevê que aquele que identifica a ameaça à segurança e sugere possíveis soluções, adquire um capital simbólico e a legitimidade necessária para convencer o público a aceitar o discurso de securitização e a aplicação de regimes especiais em situações extraordinárias

[99] "As salvaguardas presentes no modelo tradicional de justiça criminal têm três objetivos gerais: (i) a minimização da intrusão do estado nas vidas dos cidadãos, (ii) a proteção da dignidade humana e (iii) defender a legitimidade da coerção do estado e exatidão factual" (Marks *et al*, 2020: 4)

[100] A inversão da lógica disciplinar no ambiente das redes sociais é um elemento que destaca a relevância do Banóptico como ferramenta teórica, pois a sobre-exposição presente na dinâmica das redes sociais cria a dinâmica onde o próprio usuário se autodisciplina com respeito à exposição da intimidade com receio de não ser observado (Gilliom, 2012, apud Browne: 2015: 39)

independente da comprovação da eficácia das técnicas sugeridas (Schwell, 2014: 87). Por outras palavras, a excepcionalidade inerente às temáticas relacionadas com a segurança justifica o uso de técnicas de vigilância, que diante de contextos como os de sociedade de segurança máxima, suspeita categórica e a criação de subjetividades pacíficas e suspeitas (automatizada), criam ansiedades na opinião pública que classificam todo e qualquer distúrbio da ordem social como um elemento que justifica o uso de medidas extraordinárias, desde pequenos delitos com importância localizada até eventos de maior gravidade. O grau de intensidade de cada um destes distúrbios não é relevante numa sociedade onde o medo e a suspeita são sentimentos comuns e moldam a expectativa coletiva sobre a segurança pública, e este é um resultado que garante que o discurso da securitização teve suficiente adesão quanto à adoção de técnicas de vigilância ubíquas, seja qual for o contexto e o nível de ameaça que as autoridades policiais tenham que lidar.

Outro aspecto essencial para criar a adesão necessária para justificar o uso de técnicas de vigilância intrusiva torna-se evidente na forma como esta temática é abordada por parte dos meios de comunicação, e o tom sensacionalista com que são tratados os assuntos relacionados com a segurança e imigração[101]. A forma como o jornalismo tende a representar ocorrências policiais muitas vezes acompanha um tom dramático digno de filmes de ficção policial, transformando eventos de influência localizada em assuntos de interesse e importância singular, criando uma sensação de que as técnicas utilizadas pelas forças de segurança para o combate à criminalidade uma espécie de ato heróico[102].

A combinação de uma conjuntura que inclui elementos como a presença de forças policiais de caráter repressivo, bem como a influência de discursos que promovem a segurança pública através do uso de tecnologias da informação, promovem a ideia da vigilância integrada, e este enquadramento torna-se apropriado para refletir sobre o posicionamento adotado pelo FBI nos Estados Unidos quanto ao uso de câmeras acopladas ao uniforme policial *(Body worn cameras – BWC),* como parte das iniciativas de inteligência policial (*Smart Police Initiative – SPI)* [103] promovidas pelo Departamento de Justiça norte-americano a partir de 2012.

Estas iniciativas implicam na utilização de recursos de pesquisa das áreas de segurança e de processamento eficiente de dados com o objetivo de elaborar táticas baseadas em evidências que possibilitem a aplicação da lei no país de forma eficiente, efetiva e econômica, o que em tese coloca a atividade policial em pé de igualdade com a complexidade dos novos arranjos sociais atuais que mesclam as identidades individuais e digitais. Estas iniciativas, segundo publicação da Universidade

[101] "Os tablóides austríacos foram muito claros sobre as ondas de imigração e roubos que se esperavam após o alargamento do espaço Schengen em 2007. A impressão foi dada em relatos dos media, e cartas aos editores de jornais de que a população austríaca estava apavorada com a perspectiva de enchentes de criminosos 'gangues do leste' esperando para invadir seu país" (Schwell 2010)

[102] A publicação *The truth about crime. Sovereignty, Knowledge, Socialorder* de Jean e John Comaroff (2016) dispõe de relatos similares relativamente a forma como os media retrataram o trabalho da polícia na África do Sul, comparado-os com heróis.

[103] Para mais informações sobre a *Smart Police Initiative*, ver https://bja.ojp.gov/program/smart-policing-initiative-spi/overview Acedido em 20/10/2021

da Virginia, tiveram um orçamento de cerca de 20 milhões de dólares (Ringrose, 2019:57) [104], e incluíam o uso de Reconhecimento Facial nas *body worn cameras* utilizadas pelos oficiais de polícia em âmbito nacional, suscitando diversas preocupações sobre violações nos campos da privacidade e dos direitos humanos.

O caso do uso de *body worn cameras* nos Estados Unidos ilustra como certos discursos influenciam as diversas esferas envolvidas neste processo, desde as empresas interessadas em desenvolver e fornecer estas tecnologias em favor da instrumentalização policial, até a esfera política em que este assunto pode ganhar relevância em virtude da sensibilidade inerente à temática da segurança para a opinião pública. O tribunal federal distrital no Estado de Nova Iorque *(Southern districtof New York - S.D.N.Y)* estabeleceu, em 2013[105], o uso de *body worn cameras* dotadas de recursos de Reconhecimento Facial nas rotinas de patrulhamento depois de suspeitas de repetidas abordagens policiais conduzidas a cidadãos afro-americanos por motivações de cunho racial, sugerindo que a utilização destes dispositivos permite a monitorização objetiva e a efetiva validação destas abordagens.

O parecer dado pelo tribunal para justificar o uso de recursos de gravação nestas operações prevê que esta prática favorece a criação de um ambiente de respeito mútuo entre os agentes de patrulhamento e a população, pois a consciência sobre a interação gravada promove uma melhoria na interação entre as partes, resultando em abordagens justas e justificadas, algo que na prática também funcionaria como uma resposta à perda de confiança da população desproporcionalmente afetada pelas abordagens motivadas por questões raciais (Ringrose, 2019:59-60). Esta pode parecer uma justificação coerente para um discurso de caráter político, porém, é necessário ter em conta a perspectiva da população submetida a este tipo de vigilância; ter o conhecimento de que uma operação será gravada e de que as informações biométricas capturadas farão parte de um banco de dados não implica que haja consentimento para este tipo de prática, pelo contrário, revela o caráter arbitrário que molda esta relação.

Neste sentido, este parecer forjado na promoção de boas práticas policiais serve como um véu que encobre o objetivo manifestado pelo FBI de adotar o uso de tecnologias de Reconhecimento Facial como um tema central para a agência, e este contexto movimenta o mercado de empresas que fornece soluções que pretendem aperfeiçoar as práticas de segurança e de vigilância onde o benefício palpável se materializa na redução de custos operacionais, e no lucro decorrente da comercialização e operação destes sistemas.

Ringrose destaca que em 2018, a Axon, uma das maiores empresas envolvidas no desenvolvimento de *body worn cameras* nos Estados Unidos adquiriu a patente de um *software* que possibilita o Reconhecimento Facial neste tipo de filmagens. Ao identificar um modelo facial, o

[104] Ver *Law enforcement's pairing of facial recognition with body-worn cameras escalates privacy concerns* do *Virginia Law Review online*.
[105] Floyd v. City of New York, 959 F. Supp. 2d 668, 685 (S.D.N.Y. 2013) apud Ringrose, 2019.

programa processa a informação num banco de dados que pesquisa informações privadas como o nome do indivíduo reconhecido e envia a análise para um dispositivo manual de forma automatizada, algo que ressalta as preocupações sobre o eventual uso indevido deste tipo de tecnologia por parte da polícia. Porém, esta não parece ser uma preocupação partilhada por Rick Smith, CEO da empresa, que alega que o risco de uso indevido por parte da polícia não deve ser motivo para rejeitar este recurso, pois para além de compreender os riscos, é preciso compreender os benefícios que este sistema de vigilância pode trazer para a sociedade (2019:61).

Uma observação atenta ao discurso do CEO da Axel, e o contexto em que se adota o uso de Reconhecimento Facial nas *body worn cameras* permite-nos compreender que os objetivos comerciais e políticos deste projeto sobrepõem qualquer demanda por direitos constitucionais onde discurso do risco ganha um caráter dual na dinâmica que promove as novas técnicas de vigilância. Por um lado, o risco relacionado com comportamentos suspeitos atua como um elemento codificado em modelos de *Machine Learning* que orientam a atividade policial que, somada ao teor ideológico das práticas de vigilância racializada, cria interações desproporcionais aos diferentes grupos submetidos a este sistema de vigilância. Já o risco quanto ao uso indevido desta tecnologia por parte das autoridades policiais é interpretado apenas como um fator que não desencadeia maiores complicações sociais; de forma antagônica, este discurso pretende silenciar a hipótese do uso indevido em troca de benefícios que não podem ser medidos de forma objetiva pela sociedade. A dualidade de discurso que aborda o risco como estratégia política não está relacionada com os impactos que a indeterminação causa a grupos específicos, mas sim com quem está autorizado a gerir estes riscos a favor de objetivos específicos quanto à aplicação de técnicas de vigilância disseminadas em contextos socialmente heterogêneos.

A complexidade envolvida no rastreamento destes processos por vezes dificulta a identificação da responsabilidade dos agentes envolvidos nesta cadeia de processos, e esta dificuldade se obscurece através de discursos que promovem a securitização como estratégia política em nome da segurança publica. O sensacionalismo utilizado pelos veículos de informações na ânsia de obter a máxima audiência faz uso de terminologias genéricas como gangs, imigração ilegal, tráfico de drogas (Schwell, 2014: 96) com o objetivo de maximizar o risco de suspeita bem como a necessidade de segurança para proteger os cidadãos, no entanto a utilização genérica destes termos pode criar imaginários coletivos que tendem a resultar em práticas como a da vigilância racializada, trazendo consequências que desfavorecem indíviduos quer seja por conta do tom de pele ou pelos locais onde estes vivem.

Simone Browne discute a proposta de uma tomada de consciência biométrica ligadas aos conflitos raciais impostos à comunidade afro-americana, e ressalta esta proposta como um imperativo central ao sugerir debates públicos sobre a utilização de técnicas de Reconhecimento Facial, tendo em conta a responsabilidade compartilhada entre o Estado e as empresas envolvidas em contextos onde as informações geradas a partir da leitura de características físicas sejam fundamentalmente entendidas a partir da óptica dos direitos humanos, uma vez que a maneira como estas características são culturalmente significadas no interior dos laboratórios de Visão Computacional tende a ser

influenciada por um teor ideológico implícito no desenvolvimento destes sistemas, causando impactos mais intensos na rotina da comunidade afrodescendente na medida em que esta se depara com as novas formas de vigilância mediadas pelas tecnologias da informação (Browne, 2015:114-116). No mesmo sentido, Ringrose (2019: 66) oferece uma série de recomendações em torno do uso de *body worn cameras* dotadas de mecanismos de Reconhecimento Facial por parte das autoridades policiais, que se alinham com a ideia de tomada de consciência biométrica no sentido de limitar a forma como informações privadas são manuseadas em nome da segurança. Estas recomendações sugerem: limitação da recolha de informações biométricas obtidas a partir do uso de *body worn cameras,* e o cumprimento de protocolos que possibilitem manter as comunidades sujeitas a este tipo de vigilância informada sobre os processos de coleta, armazenamento e processamento desta classe de informação; o armazenamento de informações obtidas nestes termos deve ser limitado, e a sua partilha deve seguir padrões que limitem essa troca, sempre informando a finalidade por traz da coleta; a importância de se criar mecanismos independentes de avaliação do uso destas informações no contexto norte-americano com o intuito de mitigar técnicas de vigilância pautadas por um viés racializado, e garantir a responsabilização dos atores envolvidos nas tomadas de decisão automatizadas em casos de falsos positivos, algo que tornaria este processo mais transparente e justo do ponto de vista social.

A regulamentação do tratamento de informações biométricas no contexto norte-americano torna as práticas de vigilância de ambientes externos (e o uso de *body worn cameras* a nível nacional) um problema que evoca distintas interpretações. Aspectos ligados ao histórico de vigilância racializada, além do uso de análises algorítmicas criam processos de interpelação das subjetividades de comunidades marginalizadas que reforçam a afirmação de que o uso destas tecnologias de forma desregulada favorece para ampliar os conflitos de ordem racial. A realidade europeia do GDPR, ainda que pautada por orientações amplas dirigidas a diferentes contextos culturais, recorre a ferramentas de proteção da privacidade que possibilitam a exclusão de técnicas de Reconhecimento Facial em matéria de vigilância que minimizam os riscos associados ao processamento de informações sem o devido consentimento. Por outro lado, a emissão de consentimento individual nem sempre é um fator determinante no que se refere ao processamento de dados agrupados na lógica *Big data* que cria categorias de danos coletivos que necessitam reflexões amadurecidas sobre o tema. Sendo assim, a representatividade de comunidades excluídas do ambiente técnico-científico surge como um elemento que possivelmente favorece a agenda da tomada de consciência biométrica, pois traz às fases elementares do desenvolvimento destes sistemas aqueles que são mais impactados pelo custo social ligados ao uso das tecnologias da informação, e permite com que a automatização dos processos criminais seja abordada por perspectivas que diferem dos discursos de securitização tradicionais.

Estas propostas permitem com que os impactos da continuidade de processos históricos, sociais e políticos sejam minimizados, tornando a dinâmica da privacidade e do Reconhecimento Facial em matéria de segurança mais equilibradas; permite também que estas tecnologias não exponham apenas os efeitos negativos quando utilizadas em contextos sociais, o que faz dos avanços do campo técnico-

científico uma maios valia integral, onde todos os indivíduos podem ser "interpretados" de forma igualitária e justa.

Conclusão

Analisar o fenómeno do Reconhecimento Facial permite-nos explorar o domínio da Visão Computacional e perceber os cenários implicados na utilização de tecnologias da informação em contextos sociais que convocam abordagens interdisciplinares na medida em que as consequências da sua utilização extrapolam o universo computacional. A maneira como se desenvolvem as dinâmicas no interior de laboratórios computacionais influencia no comportamento dos sistemas de Inteligência Artificial e Reconhecimento facial utilizados em contextos sociais, e impacta a vivência *online* e *off-line* em múltiplas dimensões, o que revela que as transformações ligadas a Cibercultura impõem desafios práticos que as empresas de tecnologia ainda não estão devidamente preparadas para gerir. O paradigma representacional da Inteligência Artificial se renovou com a integração das técnicas algorítmicas a partir do século XXI, e o que aparantava estar solucionado se transformou em uma dinâmica com poderosos sistemas de análise de dados coletivos, que combinado com práticas de *dataveillance* e com a crescente integração de dispositivos eletrônicos que mediam interações sociais, sobretudo depois da pandemia da COVID-19, disponibiliza grandes quantidades de dados pessoais onde modelos faciais são utilizados para o treinamento sistemas de Reconhecimento Facial de forma ainda não totalmente clara ao grande público.

Partindo da observação d os desdobramentos do avanço tecnológico relatado por institutos de pesquisa interdisciplinares, e instituições não governamentais que atuam em defesa dos direitos civis na era digital, além de diversas publicações que abordaram a temática do Reconhecimento Facial, tornou-se possível constituir o material empírico que fundamentou esta investigação a estabelecer os contextos em que o uso destes recursos oferece potenciais riscos as liberdades e direitos nos contextos da privacidade visual e da segurança. A interpretação de imagens é um processo complexo que depende de funções cognitivas que o ser humano pode não estar apto a explicar de forma integral, o que faz com que a reprodução desta habilidade em ambiente artificial ocorra a partir de assunções que impactam diretamente a comunidade de utilizadores, e com maior intensidade os grupos menos representados nos ambientes digitais. Este enquadramento permite-nos concluir que a maneira como a tecnologia da informação se apresenta aos utilizadores convoca reflexões sobre as questões éticas, políticas e sociais cuja presença de fatores culturais ligados a exclusão social e a discriminação se transferem para as lógicas sistémicas de forma involuntária, criando impactos que dificultam rastrear a responsabilidade dos agentes que desenvolvem e utilizam tais tecnologias em contextos heterogêneos.

O histórico de práticas que ilustra os diferentes desempenhos destes sistemas nos contextos estudados evidencia resquícios de uma mentalidade colonial ligada à interpretação da ideia de raça que hierarquiza diferentes grupos em função de questões fenotípicas, criando um ideal racializador que reflete no imaginário coletivo das sociedades contemporâneas até os dias de hoje, mesmo que de

forma menos explícita. A distinta perspectiva de projeção de vida das populações (brancas e não brancas) é um fator que se torna evidente neste contexto, sobretudo quando pensamos a partir da temática da segurança e dos estereotipos negativos impostos aos grupos não brancos. No que se refere ao universo digital, a sobrerepresentação das populações brancas nos processos que calibram os modelos de *Machine Learning* demonstrou a influência inconsciente de fatores culturalmente naturalizados que fazem do racismo uma realidade que ao contrário de diminuir, se reproduz no interior dos processos computacionais.

Por outro lado, a forma como a Cibercultura transformou o espectro da segurança ampliou a visibilidade das forças policiais possibilitando técnicas de vigilância que dificilmente serão revertidas. Partindo da perspectiva da antropologia crítica da segurança e da flexibilidade do conceito, bem como do posicionamento dos *surveillance studies* quanto ao uso de técnicas de vigilância que coletam informações pessoais de maneira sistemática, identificou-se uma relação assimétrica estabelecida pelas forças de segurança em parceria com as empresas tecnológicas que viabilizam o processamento de informações pessoais de forma descontextualizada que reforça um estado de suspeita constante, o que para além de provocar preocupações ligadas à esfera da privacidade, fere liberdades e direitos em contextos em que a regulamentação de dados digitais apresenta-se de forma pouco integrada. Neste sentido, a abordagem comparativa do GDPR em relação à vigilância de espaços externos nos mostrou alternativas que propõem mecanismos conceituais que favorecem as prerrogativas do regulamento em relação à emissão de consentimento do ponto de vista individual, restando ao regulamento propor mecanismos que possam conter os danos coletivos no campo da privacidade, que podem passar pelo alargamento da noção de dados pessoais e pela abordagem do tema do Reconhecimento Facial de forma específica no futuro.

Os contextos em que o Reconhecimento Facial surge nesta investigação são permeados por aspectos que nos permitem concluir que esta tecnologia não é utilizada de forma neutra, pelo contrário, os contextos analisados denotam que a utilização deste recurso quase sempre está associada a questões estratégicas, seja por questões de vigilância ou por interesses comerciais (ou pela combinação de ambos). Na medida que a tecnologia passa a instrumentalizar a atividade das forças de segurança maximizando seu alcançe, e, ao mesmo tempo, automatizando rotinas através do uso de sistemas preditivos caracterizados por indeterminações epistêmicas, a reflexão crítica sobre a utilização destas técnicas torna-se um fator positivo para propor um equilibrio social, pois estabelecer um estado de vigilância integrada a partir dos custos sociais discutidos implicará em relações dialéticas desproporcionais em virtude do uso de sistemas de patrulhamento preditivo, o que invariavelmente suscita conflitos de ordem socioeconômica e racial. Neste sentido, esta investigação sugere uma interpretação critica sobre a automatização das técnicas de patrulhamento orientadas por análises algorítmicas, tendo em conta um alinhamento que tenha como premissa a avaliação das multiplas esferas associadas à segurança de ambientes externos, com especial destaque às questões

ligadas aos conflitos orientados pela vigilância racializada no patrulhamento tradicional, e o impacto nas subjetividades decorrentes dos desdobramentos do uso de sistemas de policiamento preditivo.

A presença de mecanismos que regulamentem a proteção de dados digitais surge como um forte aliado para normatizar o processamento de informações biométricas visuais inerentes ao uso de tecnologias de informação. A presença de instituições independentes que supervisionem o processamento destas informações é proposta como um elemento fundamental para determinar os limites e as responsabilidades daqueles que desenvolvem e utilizam estes sistemas. O GDPR propõe mecanismos que minimizam o potencial de identificação individual que instrumentaliza as forças de segurança, suscitando iniciativas que tornam a videovigilância menos invasiva, e independente do processamento de informações biométricas. Comparativamente, o aspecto fragmentado dos mecanismos de regulamentação de dados nos Estados Unidos dificulta uma análise de contexto em termos amplos, impactando negativamente esta demanda de setores da sociedade civil local, permitindo-nos concluir que a agenda da privacidade visual no país é uma área que possibilita reflexões propositivas em torno de avanços nas estruturas da privacidade que criam oportunidades às ciências sociais de se posicionar nos estudos sobre as tecnologias da informação.

As tecnologias de Inteligência Artificial e Reconhecimento Facial de uso massivo são técnicas recentes e na sua maioria desenvolvidas em ambientes laborais pouco diversos, ainda que paradoxalmente seu uso ocorra de forma disseminada, assim, os desafios éticos ligados que o setor da Visão Computacional tem pela frente envolve a integração da diversidade cultural nos debates que determinam as questões éticas, e a elaboração de práticas que compreendam a complexidade e a diversidade de utilizadores submetidos a estas técnicas. Integrar as comunidades menos representadas no ambiente laboral tecnológico é um aspecto fundamental para fomentar práticas éticas no setor, e pode ser um passo inicial em direção ao estabelecimento de objetivos coletivos equitativos para alterar o caráter homogêneo do universo tecnológico, e projetar novas perspectivas quanto aos mecanismos associados à tomada de decisões automatizadas, representando um ganho social no combate a discriminação.

Esta investigação procurou relacionar relatos e experiências que partem da realidade social para ilustrar a maneira como mediação tecnológica interfere nas questões de segurança e privacidade, porém é preciso ter em conta que estes mecanismos, em si, representam um avanço do universo técnico-científico importante, assim, o foco principal desta análise centrou-se em explorar a utilização destes dispositivos e os efeitos decorrentes do viés algorítmico. A estrutura epistêmica destes sistemas e a influencia de fatores como a *apophenia* nos permitem concluir, que ainda que a Visão Computacional tenha conseguido desenvolver sistemas altamente sofisticados, estes sistemas ainda estão sujeitos a limitações técnicas não totalmente compreendidas por quem os desenvolve, portanto, questionar a aplicação comercial destes sistemas torna-se uma mais valia essencial que fundamenta a hipótese dos custos sociais inerentes discutidos.

Iniciativas como as de Joy Buolamwini e Timnit Gebru que partem de experimentos práticos que identificam incongruências sistémicas das tecnologias de Reconhecimento Facial tradicionais, mostram-nos a disparidade de desempenho destes sistemas que se acentua na medida em que a leitura facial é realizada no grupo de mulheres negras, revelando o caráter interseccional do viés algorítmico em sistemas calibrados com imagens de indivíduos brancos. Em contrapartida, a utilização de critérios relacionados ao tipo de pele e a recolha de modelos faciais de forma criteriosa permite um equilíbrio sistêmico no que se refere à representatividade, e possívelmente no desempenho destes sistemas. *Insights* como este reforçam o argumento da representatividade de grupos historicamente marginalizados na construção de premissas éticas durante o desenvolvimento de tecnologias de Reconhecimento facial, pois subverte as técnicas tradicionais do domínio da Visão computacional possibilitando novos horizontes para o setor, o que consecutivamente tende a minimizar aspectos resultantes de processos mais amplos ligadas ao racismo estrutural nas relações sociais contemporâneas.

Os custos sociais ligados aos danos individuais e coletivos denotam que integrar a tecnologia da informação nos processos de socialização exige uma alteração das estruturas de privacidade tradicionais em virtude dos danos coletivos relacionados às analises *Big data*. Por um lado a influência da cultura digital e fatores como a evasão da privacidade e a exposição da intimidade evidenciam o caráter transformativo que integra os contextos *on* e *off-line* de forma indiferenciada, trazendo benefícios práticos onde a mediação tecnológica é vista de forma cômoda e positiva em relações comerciais explícitas. Por outro lado, a negociação da privacidade baseada no consentimento cria uma relação cuja vantagem se observa apenas do lado das empresas de tecnologia, pois a responsabilidade por aceitar e fiscalizar as atividades previstas nestes termos repousa na emissão de um consentimento que por vezes é obtido de forma induzida, seja pela complexidade da linguagem utilizada, ou pela ânsia de participar em ambientes virtuais. A privacidade pautada somente por premissas comerciais põe em evidência a problemática da transparência, sobretudo no ambiente das redes sociais onde a confiança entre o utilizador e a empresa se torna moeda de troca; na medida em que esta confiança é ameaçada por interesses associados às questões de segurança que oferecem riscos aos direitos constitucionais, refletir sobre alternativas que possam garantir que não haja distúrbios nos fluxos informacionais individuais e valorizar o contexto onde as informações foram obtidas representam um potencial avanço no universo da privacidade visual.

Nesse sentido, um dos objetivos desta investigação foi propôr uma reflexão que colocou em destaque a importância dos regulamentos de proteção de privacidade na esfera digital como uma resposta institucional que limita as práticas invasivas ligadas ao processamento de informações biométricas em nome da segurança, porém, tendo em conta que a lógica da emissão de consentimento apareceu-nos como um ponto em comum nos contextos estudados, a teoria da privacidade contextual se apresenta como um elemento complementar na proposta de composição de uma estrutura da privacidade no ambiente digital que pode minimizar os efeitos negativos das análises *Big data* onde a

figura do consentimento não garante a privacidade de facto. A experiência da violação de privacidade em Illinois ilustrou a forma como ocorrem processamentos de dados biométricos de forma indevida, e o cruzamento de fluxos informacionais onde as empresas de tecnologia cada vez mais se apropriam de informações sensíveis para viabilizar interesses comerciais, sendo assim, a reflexão quanto ao caráter mercantil das informações pessoais se posiciona nesta investigação com a função de conciencializar a comunidade de utilizadores sobre os desdobramentos que uma simples sequência de *clicks* produz, bem como expor a responsabilidade que subjaz deste processo na esfera comercial.

A conciencialização coletiva sobre os efeitos na área da privacidade se alargam quando observamos a tendência que o uso de *body worn câmeras* representa no contexto norte americano, sobretudo tendo como base a maneira como o FBI se articulou para incrementar as técnicas de processamento de modelos faciais obtidos de fontes terceiras, o que da perspectiva dos grupos estruturalmente marginalizados, denota violações de privacidade bem como danos subseqüentes que se sobrepõem aos fatores discriminatórios que não são compartilhados de forma coletiva no âmbito social, desta forma, a elaboração de políticas éticas claras e específicas que regulamentem a temática do Reconhecimento Facial pode equacionar os interesses de todos os setores sociais envolvidos na utilização deles, e ponderar o uso de técnicas de vigilância intrusiva em situações que não justificam o uso deste recurso. A automatização de processos criminais lança mão de processos que constroem padrões de subjetividades de forma desigual que reforçam comportamentos discriminatórios, e negligencia salvaguardas importantes ligadas ao julgamento criminal tradicional. Parte deste processo nasce da demanda pela redução de custos operacionais que se converte numa mais valia comercial para o setor tecnológico durante a oferta destes recursos para as forças de segurança, porém importa que sejam discutidas também as questões da eficácia destas ferramentas, e dos tipos danos que elas causam em contextos heterogêneos como um contra-argumento nos contextos em que estas ferramentas são promovidas como aliadas neutras nas dinâmicas da segurança pública.

A análise da dimensão discursiva que promove o uso do Reconhecimento Facial nas rotinas de vigilância é um elemento fundamental a ter-se em conta, pois a partir dela identificamos os interesses subjacentes à instrumentalização policial. Ainda que o avanço tecnológico seja positivo da perspectiva técnia, é importante perceber que o desejo de automatização de processos não deve ser usado para sobrepor os direitos ou as responsabilidades advindas destas proposições, sobretudo quando a ideia de risco é distorcida por parte das empresas tecnológicas. As estratégias sócio-políticas criadas a partir do risco eminente despertam sentimentos conflitantes na sociedade em virtude da forma como a subjetividades são codificadas e noticiadas, portanto as demandas que sugerem a utilização de dispositivos tecnológicos que possibilitam o processo de vigilância integrada devem orientar-se por uma visão abrangente das demandas sociais, e não apenas por fatores ligados a custos operacionais ou estratégias comerciais. Por outro lado, a difusão de discursos sensasionalistas que divulgam acontecimentos que potenciam sentimentos de insegurança coletiva por parte dos meios de comunicação atua como um fator adicional nesta equação, resultando em estados de alerta constante

que normalizam medidas extraordinárias para situações rotineiras, portanto, concluímos que a vigilância integrada é um tema que deve ser explorado de maneira particularmente atenta, e dirigida a situações que apresentem riscos comprovados para os Estados soberanos, e não constituir uma regra para o cotidiano social. Como vimos, a utilização deste recurso de forma generalizada e sem regulamentação adequada pode instaurar um regime de controle social que limita as interações sociais e colocar em risco valores democráticos.

Propostas como a da tomada de consciência biométrica e a inclusão das informações visuais na estrutura que protege os direitos humanos representam uma transformação deste panorama do ponto de vista da manutenção dos direitos e das liberdades, e esta iniciativa conjugada com mecanismos que regulamentem o processamento de informações digitais, bem como com políticas claras que estabeleçam normas específicas para a privacidade podem equilibrar os conflitos ligados aos impactos das tecnologias da informação e tornar a integração desta mediação mais equitativa numa perspectiva coletiva. Uma vez que a tecnologia da informação se torna (e se tornará) cada vez mais presente nos contextos sociais, refletir criticamente sobre a forma como estes processos se desenvolvem e são utilizados de forma massiva representa um movimento que cria a oportunidade à Antropologia de inserir-se em domínios pouco convencionais para o conhecimento antropológico, contudo o universo que se abre a partir da análise de desdobramentos técnico-científicos representa um campo em potencial para o futuro da ciência.

Referências Bibliograficas:

ALMEIDA, M. R. C. de Junho 2009. Índios mestiços e selvagens civilizados de Debret reflexões sobre relações interétnicas e mestiçagens. In *Varia Historia* (online). Vol. 25, N. 41. 85-106. Acedido em: 20/10/2021 Disponível em: https://doi.org/10.1590/S0104-87752009000100005

ALMEIDA, Silvio., 2019. *Racismo estrutural* (online). São Paulo: Sueli Carneiro, acedido em: 20/10/2021. Disponível em: https://blogs.uninassau.edu.br/sites/blogs.uninassau.edu.br/files/anexo/racismo_estrutural_feminismos_-_silvio_luiz_de_almeida.pdf

AMNESTIA INTERNATIONAL., 2021. Ban dangerous facial recognition technology that amplifies racist policing (online). Acedido em 20/10/2021. Disponível em: https://www.amnesty.org/en/latest/press-release/2021/01/ban-dangerous-facial-recognition-technology-that-amplifies-racist-policing/

ASGHAR *et al*., Agosto 2019. Visual Surveillance within the EU General Data Protection Regulation: A Technology Perspective. In *IEEE Access* (online). Vol. 7. 111709-111726. Acedido em 20/10/2021. Disponível em: DOI:10.1109/ACCESS.2019.2934226

BARNOVICIU *et al*., 2019. *GDPR compliance in Video Surveillance and Video Processing Application* (online). Acedido em: 20/10/2021. Disponível em: doi: 10.1109/SPED.2019.8906553.

BBC News, 2015. *Google Apologises for Photosapp'sracistblunder* (online). Acedido em 20/10/2021. Disponível em https://www.bbc.com/news/technology-33347866

BIPA, 2008. *Biometric Information Privacy Act* (online). Acedido em 20/10/2021. Disponível em: https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57

BRICALLI, I. L. Setembro 2020., A vigilância como cultura. In *Sociologia & Antropologia* (online). Vol. 10, N. 3. 1103-1107. Acedido em 20/10/2021. Disponível em: https://doi.org/10.1590/2238-38752020v10316

BRIGHENTI, Andrea Mubi., 2010. *Visibility in social theory and social research*. 1st edition. London. Palgrave Macmillan.

BROWNE, Simone., 2015. *Dark Matters: On the Surveillance of Blackness* (online). Durham and London: Duke University Press, Acedido em: 20/10/2021. Disponível em: https://doi.org/10.1215/9780822375302

BUOLAMWINI, J. e GEBRU, T., February 2018. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. In *Proceedings of the 1st Conference on Fairness, Accountability and Transparency.* In *Proceedings of Machine Learning Research* (online). Vol. 81. 77-91. Acedido em 20/10/2021. Disponível em: https://proceedings.mlr.press/v81/buolamwini18a.html.

BUOLAMWINI, Joy., 2016 *How I am fighting bias in algorithms* (online). Acedido em 20/10/2021. Disponível em: https://www.ted.com/talks/joy_buolamwini_how_i_m_fighting_bias_in_algorithms

BRITANNICA, The Editors of Encyclopaedia., 2021. *"Richard Nixon"* (online). Encyclopedia Britannica, Acedido em 20/10/2021. Disponível em: https://www.britannica.com/biography/Richard-Nixon.

BROWNLEE, J., 2019. *A gentle introduction to deep learning for Face recognition* (online). Acedido em 20/10/2021. Disponível em: https://machinelearningmastery.com/introduction-to-deep-learning-for-face-recognition/

CDFUE., (2000). Carta dos Direitos Fundamentais da União Europeia (online) . Acedido em 20/10/2021. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A12012P%2FTXT

CHAGAS, A. e SANTOS, L., Novembro 2020. Negros internet e ciência: A representatividade e suas webconexões. In *Educação*, *As provocações atuais da Cibercultura nas redes educativas* (online). Vol. 10. N.2. 179–192. Acedido em: 20/10/2021. Disponível em: https://doi.org/10.17564/2316-3828.2020v10n2p179-192

CHANNICK, Robert., 2021. *Waiting for your $345 from the Illinois Facebook privacy settlement? Here's why it's delayed* (online). Acedido em: 20/10/2021. Disponível em: https://www.chicagotribune.com/business/ct-prem-biz-facebook-privacy-settlement-delay-appeal-20210405-fydkqfwkrfew7jc6koe2rbmndy-story.html

CHEN. Brian X., 2009. HP Investigates Claims of 'Racist' Computers (online). Acedido em 20/10/2021. Disponível em: https://www.wired.com/2009/12/hp-notebooks-racist/

COMAROFF, Jean, e COMAROFF John L., 2017. *The Truth about Crime: Sovereignty, Knowledge, Social Order* (online). Chicago: University of Chicago Press, acedido em: 20/10/2021. Disponível em: https://www.academia.edu/38099555/The_Truth_about_Crime_Soveregnty_Knowledge_Social_Order_Jean_Comaroff_John_Comaroff

CRAWFORD, Kate e PAGLEN, Trevor., 2019. *Excavating AI: The Politics of Training Sets for Machine Learning* (online). Acedido em: 20/10/2021. Disponível em https://excavating.ai

CRAWFORD *et al*., 2019. *AI Now 2019 report* (online). Acedido em 20/10/2021. Disponível em: https://ainowinstitute.org/AI_Now_2019_Report.pdf

CRENSHAW, K. W., 1991. Mapping the Margins: Intersectionality, Identity Politics, and Violence against Women of Color. *In Stanford Law Review*. Vol. 43 N. 6, 1241-1299.

DAL BELLO, C., 1º semestre 2011. Visibilidade, vigilância, identidade e indexação: A questão da privacidade nas redes sociais digitais. *In Logos Comunicação e Universidade* (online). Vol. 18. N. 1. 139-151. ISSN 0104-9933. Acedido em: 20/10/2021. Disponível em: https://www.e-publicacoes.uerj.br/index.php/logos/article/view/1261/1602.

DAWOOD, Ayub., 2021. *Tech firm launches facial recognition to catch Israelis using fake vaccine passports* (online). Acedido em 20/10/2021. Disponível em: https://me.mashable.com/tech/13361/tech-firm-launches-facial-recognition-to-catch-israelis-using-fake-vaccine-passports

DEBORD, Guy., 2003. *A Sociedade do Espetáculo* (online). Rio de Janeiro. Projeto Periferia, acedido em 20/10/2021. Disponível em: https://www.marxists.org/portugues/debord/1967/11/sociedade.pdf

DREYFUS, Hubert L., 1971. *What Computers Can't Do: The Limits of Artificial Intelligence*. 1st edition. Nova Iorque. Harper e Row publishers Inc.

ESCOBAR, A. Junho 1994. Welcome to Cyberia: Notes on the Anthropology of Cyberculture [and Comments and Reply]. In *Current Anthropology* (Online), 35: 3 pp, 211-231. Acedido em: 20/10/2021. Disponível em: https://www.jstor.org/stable/2744194

ESPOSTI, S. D., Maio 2014. When big data meets dataveillance: The hidden side of analytics. In *Surveillance & Society* (online). Vol. 12. N. 2. 209-225. Acedido em: 20/10/2021. Disponível em: https://doi.org/10.24908/ss.v12i2.5113

FACEBOOK, INC. Política de cookies (online). Acedido em 20/05/2021. Disponível em: https://www.facebook.com/policies/cookies/

FASSIN, Didier. 2013. *Enforcing order: An ethnography of urban policing*. 1st edition. Cambridge, UK. Polity.

FITZPATRICK, T. B., 1988. The validity and practicality of sun-reactive skin types I through VI. In *Archives of Dermatology* (online). Vol. 124. N. 6. 869-871. Acedido em 20/10/2021. Disponível em: doi:10.1001/archderm.1988.01670060015008

FOUCAULT, Michel., 1987., *Vigiar e punir. História da violência nas prisões.* Edição 27. Petrópolis. Vozes.

FOUCAULT, Michel., 2009. *Security, Territory, Popoulation* (online). Nova Iorque. Picador

FROIS, C., 2011., *Vigilância e Poder*. Edição 1. Lisboa. Mundos Sociais.

FROIS, C. 2013., *Peripheral Vision: Politics, Technology and Surveillance*. Edição 1. Nova Iorque. Berghahn books.

FROIS, Catarina, 2014. Video Surveillance and the discretionary power in the name of security and defence. In MAGUIRE *et al*. *The Anthropology of security. Perspectives from the frontline of policing counter- terrorism and border control*. Londres. Pluto Press.

GAO REPORT., 2016. *FACE RECOGNITION TECHNOLOGY FBI Should Better Ensure Privacy and Accuracy* (online). Acedido em 20/10/2021. Disponível em: https://www.gao.gov/assets/680/677285.pdf

GOLDSTEIN, Daniel, Agosto 2010. Toward a Critical Anthropology of Security. In *Current Anthropology* (online). Vol. 51. N. 4. 487-517. Acedido em: 20/10/2021. Disponível em: http://www.jstor.org/stable/10.1086/655393

GOMES, R. B. B., Julho 2018. Hubert Dreyfus e Martin Heidegger: Representação e Cognição. *Revista Kinesis.* Vol. 10. N.22. Acedido em: 20/10/2021. Disponível em: https://doi.org/10.36311/1984-8900.2018.v10n22.16.p164

HARTZOG, Woodrow., 2018. *Facial Recognition is the perfect tool for oppression* (online). Acedido em 20/10/2021. Disponível em: https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66

HARTZOG, Woodrow., 2018. *User agreement are betraying you* (online). Acedido em 20/10/2021. Disponível em: https://onezero.medium.com/user-agreements-are-betraying-you-19db7135441f//

HARWELL, Drew., 2021. *Wrongfully arrested man sues Detroit police over false facial recognition match* (online). Acedido em 20/10/2021. Disponível em: https://www.washingtonpost.com/technology/2021/04/13/facial-recognition-false-arrest-lawsuit/

HASSEIN, Nabil., 2017. *Against Black inclusion in Facial Recognition* (online). Acedido em 20/10/2021. Disponível em: https://digitaltalkingdrum.com/2017/08/15/against-black-inclusion-in-facial-recognition/

HURWITZ, Judith e KIRSCH, Daniel., 2018. *Machine learning IBM* (online). Nova Jérsia. IBM limited edition. Acedido em 20/10/2021. Disponível em: https://www.ibm.com/downloads/cas/GB8ZMQZ3

KENYON-FLATT, Bittany., 2021. *How Scientific Taxonomy Constructed the myth of race* (online). Acedido em 20/10/2021. Disponível em: https://www.sapiens.org/biology/race-scientific-taxonomy/

LESLIE, David., 2020., *Understanding bias in facial recognition technologies: an explainer*. The Alan Turing Institute. Acedido em: 20/10/2021. Disponível em: https://doi.org/10.5281/zenodo.4050457

LEVIS-STRAUSS, C., 1970. Raça e história. In *Raça e ciência*. São Paulo. Comas *et al*. 231-269

LOHR, Steve., 2018. *Facial Recognition Is Accurate If You're A White Guy* (online). Acedido em 20/10/2021. Disponível em: https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html

LOTT, Y. M. e CIANCONI, R. de B., 2018. Vigilância e privacidade, no contexto do big data e dados pessoais: análise da produção da Ciência da Informação no Brasil. In *Perspectivas em Ciência da Informação* (online). Vol. 23. N. 4 117-132. Acedido em: 20/10/2021. Disponível em: https://doi.org/10.1590/1981-5344/3313>

LYNCH, J., 2018. *Face off Law enforcement use of face recognition technology* (online). Acedido em: 20/10/2021 Disponível em: https://www.eff.org/files/2018/02/15/face-off-report-1b.pdf

LYONS *et al*., 1998. The Japanese Female Facial Expression (JAFFE) Dataset (online). Acedido em 20/10/2021. Disponível em: https://doi.org/10.5281/zenodo.3451524.

LYON, D., Julho 2014. Surveillance, Snowden, and Big Data: Capacities, consequences, critique. In Big Data & Society (online). Acedido em: 20/10/2021. Disponível em: https://doi.org/10.1177/2053951714541861

LYON, D.., & Centre for International Governance., 2019. *State and Surveillance*. *In Governing Cyberspace during a Crisis in Trust: An essay series on the economic potential — and vulnerability — of transformative technologies and cyber security* (online). Acedido em 20/10/2021. Disponível em: http://www.jstor.org/stable/resrep26129.6

LYON, David., 1994. *The Electronic Eye: The Rise of Surveillance Society*. 1a edição. Minneapolis:

University of Minnesota Press.

MADUREIRA, N., 2003. A Estatística do Corpo: antropologia física e antropometria na alvorada do século XX. In *Etnográfica* (online). Vol. 7, 283-303. Acedido em 20/10/2021. Disponível em: https://www.researchgate.net/publication/251572416

MARKS et-al., 2015. Automatic justice? *Technology, Crime and Social Control*., In *R. Brownsword, E. Scotford and K. Yeung, Queen Mary University of London School of Law Legal*

Studies (online). Research Paper No. 211/2015. 1-34. Acedido em 20/10/2021. Disponível em: https://ssrn.com/abstract=2676154.

MAGUIRE *et al*., 2014. *The Anthropology of Security. Perspectives from the Frontline of Policing, Counter-terrorism and Border Control*. Edição 1. Londres. Pluto Press

MARX, G., 1988. *Undercover: Police Surveillance in America*. 1st edition. Berkeley. University of California Press.

MATZNER, T., Setembro 2016. Beyond data as representation: The performativity of big data in surveillance. In *Surveillance & Society* (online). Vol.14. N. 2. 197–210. Acedido em 20/10/2021. Disponível em: https://doi.org/10.24908/ss.v14i2.5831

METCALF, Jacob., 2020. *Looking for Race in Tech Company Ethics. Identifying tensions where race and tech ethics intersect* (online). Acedido em: 20/10/2021. Disponível em: .https://points.datasociety.net/looking-for-race-in-tech-company-ethics-956919fe48ee

MINGTSUNG, C. e CAI, L., Julho 2020. Research on the application of face recognition system. In *Proceedings of the 2020 5th International Conference on Humanities Science and society development* (online). Vol. 451. 23-29. Acedido em 20/10/2021. Disponível: doi={https://doi.org/10.2991/assehr.k.200727.057}

MITTELSTADT, B., Novembro 2019. Principles alone cannot guarantee ethical AI. In *Nature Machine Intelligence* (online). Vol. 1. N. 10. 1-19. Acedido em 20/10/2021. Disponível em: DOI: 10.1038/s42256-019-0114-4

MOHAMED *et al*., Dezembro 2020. Decolonial AI: Decolonial Theory as Sociotechnical Foresight in Artificial Intelligence. In *Philosophy & Technology* (online). Vol. 33. N.4. Acedido em 20/10/2021. Disponível em: DOI: 10.1007/s13347-020-00405-8

MOSS, Emanuel e Jacob METCALF., 2020. *Ethics Owners: A New Model of Organizational Responsibility in Data-Driven Technology Companies* (online). Acedido em 20/10/2021. Disponível em: https://datasociety.net/pubs/Ethics-Owners.pdf.

NISSENBAUM, H., Fevereiro 2004. Privacy as contextual integrity. In Symposium, Privacy as Contextual Integrity, 79 (online). Washington Law Review. Vol. 79. N.1. 119-158. Acedido em 20/10/2021. Disponível em: https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10/

NISSENBAUM, H., Fall 2011. A contextual approach to Privacy online. In *Daedalus: American Academy of Arts and Sciences*, Fall (online). Acedido em 20/10/2021. Disponível em: https://www.amacad.org/publication/contextual-approach-privacy-online

NORRIS, C. e ARMSTRONG, G., 1999. *The maximum surveillance society: The rise of CCTV* (online). Routledge. Acedido em 20/10/20/2021. Disponível em: https://doi.org/10.4324/9781003136439.

O'NEIL, C., 2017. *Weapons of math destruction*. 1st edition. Londres: Crown.

PATEL v. Facebook, Inc. (online), 932 F.3d 1264 (9th Cir. 2019) Acedido em 20/10/20/2021. Disponível em: https://epic.org/documents/patel-v-facebook/

PAPERT, S., 1966. *The Summer Vision Project* (online). Acedido em 20/10/2021. Disponível em: http://hdl.handle.net/1721.1/6125

PUENTE, Mark., 2019. LAPD ends another data-driven crime program touted to target violent offenders (online). Acedido em 20/10/2021. Disponível em: https://www.latimes.com/local/lanow/la-me-laser-lapd-crime-data-program-20190412-story.html

PRIVACY ACT, 1974. (online). Acedido em 20/10/2021. Disponível em: https://www.justice.gov/opcl/overview-privacy-act-1974-2020-edition/introduction

REGULATION (EU)., 2016/679 Of The European Parliament And of the Council (General Data Protection Regulation) (online). Acedido em 20/10/2021. Disponível em: http://eurlex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

RIBEIRO, J. S., Dezembro 2005. Antropologia visual, práticas antigas e novas perspectivas de investigação. In *Revista de Antropologia* (online). Vol. 48, N. 2. 613-648. Acedido em 20/10/2021. Disponível em: https://doi.org/10.1590/S0034-77012005000200007

RINGROSE, K., Fevereiro 2019. Law enforcement's pairing of facial recognition technology with bodyworn cameras escalates privacy concerns. In *Virginia Law Review Online, volume* Vol. 105. 57-66. Acedido em 20/10/2021. Disponível em: https://www.virginialawreview.org/articles/law-enforcements-pairing-facial-recognition-technology-body-worn-cameras-escalates/

ROBERTSON, Adi., 2013. *Facebook users have uploaded a quarter trillion photos since the site's launch* (online). Acedido em 20/10/2021. Disponível em: https://www.theverge.com/2013/9/17/4741332/facebook-users-have-uploaded-a-quarter/-trillion-photos-since-launch

ROTH, L., Março 2009. Looking at Shirley, the Ultimate Norm: Colour Balance, Image Technologies, and Cognitive Equity. In *Canadian Journal of Communication* (online). Vol. 34. N. 1. Acedido em 20/10/2021. Disponível em: DOI: 10.22230/cjc.2009v34n1a2196

SCHAAKE, Marietje, 2018. *The data Delusion: Protecting Individual data isn't enough when the harm is collective* (online). Acedido em: 20/10/2021. Disponível em: https://cyber.fsi.stanford.edu/publication/data-delusion

SCHWELL, A., Maio 2010. The Iron Curtain revisited: the "Austrian way" of policing the internal Schengen border. In *European Security* (online), Vol. 19, No. 2. 317–336. Acedido em 20/10/2021. Disponível em: https://doi.org/10.1080/09662839.2010.531706

SCHWELL, A., 2014. Compensating (In)security: Anthropological perspectives on internal policy. In Maguire, *et al*. *The Anthropology of security. Perspectives from the frontline of policing counter- terrorism and border control*. Londres: Pluto Press.

SENNET, R., 1978. *The Fall of Public Man*.1st edition. Cambridge: Cambridge University Press.

SHAPIRO, A., Setembro 2019. Predictive Policing for reform? Indeterminacy and intervention in Big data policing. In *Surveillance & Society* (online). Vol. 17. N. 3.4. 456-472 Acedido em 20/10/2021. Diponível em: https://doi.org/10.24908/ss.v17i3/4.10410

SIBILIA, P. e DIOGO, L., 2011. Vitrines da intimidade na internet: imagens para guardar ou para mostrar. In *Estudos De Sociologia* (online). Vol. 16. N. 30127-139. Acedido em 20/0/2021. Disponível em: https://periodicos.fclar.unesp.br/estudos/article/view/3892

STARK, L., Abril 2019. Facial recognition is the Plutonium of AI. In . XRDS Spring (online), Vol. 25. N. 3. Acedido em 20/10/2021. Disponível em: https://doi.org/10.1145/3313129

STOP LAPD SPYING., 2019. *LAPD confirms continued criminalization and harassment of the black community* (online). Acedido em 20/10/2021. Disponível em: https://stoplapdspying.org/wp-content/uploads/2021/03/LAPD-Confirms-Continued-Criminalization-and-Harassment-of-the-Black-Community-2-Pager-Final.pdf

SUE. D. W. (2010)., *Microaggression: More Than Just Race* (online) Acedido em 20/10/2021. Disponível em: . https://www.uua.org/sites/live-new.uua.org/files/microaggressions_by_derald_wing_sue_ph.d._.pdf.

TECLE *et al*., 2017. Castrating Blackness: Surveillance, Profiling and Management in the Canadian Context. In Flynn S. e Mackay A. *Spaces of Surveillance*. Londres. 187-210. Palgrave Macmillan, Cham. Disponível em: https://doi.org/10.1007/978-3-319-49085-4_11

THE INDEX PROJECT , 2021., *Algorithmic Justice League. AI's threats to civil rights and democracy* (online). Acedido em: 20/10/2021. Disponível em: https://theindexproject.org/stories/algorithmic-justice-league

TSAMADOS *et al*., Fevereiro 2021. The ethics of algorithms: key problems and solutions. In *AI & Society* (online). Acedido em 20/10/2021. Disponível em: https://doi.org/10.1007/s00146-021-01154-8

UNITED NATIONS, 1948. *Universal declaration of human rights* (online). Acedido em 20/10/2021. Disponível em: https://dre.pt/declaracao-universal-dos-direitos-humanos

VERDE, F,, 2009. *A Explicação Hermenêutica*. Coimbra: Editora Angelus Novus.

WACHTERHAUSER, B., 2002. Getting it Right: Relativism, Realism, and Truth. In DOSTAL, R. (Ed.) *The Cambridge Companion to Gadamer*. Cambridge: Cambridge University Press, 52-78.

WARREN, S. e LOUIS B., 1890. *The Right to Privacy*. *Harvard Law Review* (online) Acedido em: 20/10/2021. Disponível em:. https://www.jstor.org/stable/1321160?seq=1#metadata_info_tab_contents

Anexos:

Anexo 1: Política de cookies (Completa). Caixas de diálogo que mediam o processo de entendimento de como funciona a dinâmica de Cookies no Facebook:

Cookies e outras tecnologias de armazenamento

Os cookies são pequenas porções de texto utilizadas para armazenar informações em browsers. Os cookies são utilizados para armazenar e receber identificadores e outras informações em computadores, telemóveis e outros dispositivos. Também são utilizadas outras tecnologias para fins semelhantes, incluindo dados que armazenamos no teu browser ou dispositivo, identificadores associados ao teu dispositivo e outros tipos de software. Nesta política, referimo-nos a todas estas tecnologias como "cookies".

Utilizamos cookies se tiveres uma conta do Facebook, se utilizares os Produtos do Facebook (incluindo o nosso site e as nossas apps) ou se acederes a outros sites e apps que utilizam os Produtos do Facebook (incluindo o botão Gosto ou outras Tecnologias do Facebook). Os cookies permitem ao Facebook disponibilizar-te os Produtos do Facebook e compreender as informações que recebemos sobre ti, incluindo informações sobre a tua utilização de outros sites e apps, independentemente de teres ou não efetuado o registo ou de teres sessão iniciada.

Esta política explica como utilizamos os cookies e as opções que tens disponíveis. Salvo se especificado em contrário nesta política, a Política de Dados aplica-se ao nosso tratamento dos dados que recolhemos através de cookies.

Por que motivo utilizamos cookies?

Os cookies ajudam-nos a fornecer, a proteger e a melhorar os Produtos do Facebook através da personalização de conteúdos, da adaptação e medição de anúncios e ao proporcionar uma experiência mais segura. Os cookies que utilizamos incluem cookies de sessão, que são eliminados quando fechas o teu browser, e cookies persistentes, que ficam no teu browser até expirarem ou até os eliminares. Embora os cookies que utilizamos possam ser alterados ocasionalmente à medida que melhoramos e atualizamos os Produtos do Facebook, utilizamo-los para os seguintes fins:

Autenticação

Utilizamos cookies para verificar a tua conta e determinar quando tens sessão iniciada, de forma a facilitar o teu acesso aos Produtos do Facebook e para te fornecermos a experiência e as funcionalidades mais adequadas.

Por exemplo: utilizamos cookies para manter a tua sessão iniciada enquanto navegas entre Páginas do Facebook. Os cookies também nos ajudam a memorizar o teu browser, para não teres de inserir os teus dados de início de sessão no Facebook continuamente e poderes iniciar sessão mais facilmente no Facebook através de apps e sites de terceiros. Por exemplo, utilizamos os cookies "c_user" e "xs", incluindo para este fim, com uma duração de 365 dias.

Segurança e integridade do site e de produtos
Utilizamos cookies para nos ajudar a manter a segurança e proteção da tua conta, dados e dos Produtos do Facebook.

Por exemplo: os cookies ajudam-nos a identificar e a aplicar medidas adicionais de segurança quando alguém tenta aceder a uma conta do Facebook sem autorização (por ex.: ao tentar adivinhar rapidamente várias palavras-passe). Também utilizamos cookies para armazenar informações que nos permitem recuperar a tua conta caso te esqueças da tua palavra-passe ou para solicitar um processo de autenticação adicional quando nos informas que a tua conta foi pirateada. Isto inclui, por exemplo, os nossos cookies "sb" e "dbln", que nos permitem identificar o teu browser de forma segura.

Também utilizamos cookies para combater atividades que desrespeitam as nossas políticas ou que comprometem de qualquer outra forma a nossa capacidade de fornecer os Produtos do Facebook.

Por exemplo: os cookies ajudam-nos a lutar contra o spam e ataques de phishing ao permitir-nos identificar computadores que são utilizados para criar grandes quantidades de contas do Facebook falsas. Também utilizamos cookies para detetar computadores infetados com malware e para tomar medidas de forma a prevenir que os mesmos causem mais danos. O nosso cookie "csrf", por exemplo, ajuda-nos a impedir ataques de falsificação de pedidos entre sites. Os cookies também nos ajudam a prevenir o registo de menores de idade em contas do Facebook.

Publicidade, recomendações, dados analíticos e medição
Utilizamos cookies para nos ajudar a apresentar anúncios e recomendar negócios e outras organizações a pessoas que possam ter interesse nos produtos, serviços ou causas que os mesmos promovem.

Por exemplo: os cookies permitem-nos apresentar anúncios às pessoas que tenham visitado anteriormente o site, comprado produtos ou utilizado as apps de um negócio, bem como recomendar produtos e serviços com base nessa atividade. Os cookies também nos permitem limitar o número de vezes que vês um anúncio, para não teres de ver sempre o mesmo anúncio. Por exemplo, o cookie "fr" é utilizado para mostrar, medir e melhorar a relevância dos anúncios e tem uma duração de 90 dias.

Também utilizamos cookies para nos ajudar a medir o desempenho de campanhas de anúncios dos negócios que utilizam os Produtos do Facebook.

> *Por exemplo:* utilizamos cookies para contar o número de vezes que um anúncio é apresentado e para calcular o custo desses anúncios. Também utilizamos cookies para medir a regularidade com que as pessoas efetuam ações, como efetuar compras após uma impressão de anúncio. Por exemplo, o cookie "_fbp" identifica os browsers com a finalidade de te fornecer anúncios e serviços de análise de sites e tem uma duração de 90 dias.

Os cookies ajudam-nos a apresentar e a medir anúncios nos diferentes browsers e dispositivos utilizados pela mesma pessoa.

> *Por exemplo:* podemos utilizar cookies para evitar que vejas sempre o mesmo anúncio nos vários dispositivos que utilizas.

Os cookies também nos permitem fornecer dados analíticos sobre as pessoas que utilizam os Produtos do Facebook, bem como sobre as pessoas que interagem com os anúncios, sites e apps dos nossos anunciantes e negócios que utilizam os Produtos do Facebook.

> *Por exemplo:* utilizamos cookies para ajudar os negócios a compreender os tipos de pessoas que gostam das respetivas Páginas do Facebook ou que utilizam as respetivas apps, de forma a que os mesmos possam fornecer conteúdos mais relevantes e desenvolver funcionalidades que possam ser interessantes para os seus clientes.

Também utilizamos cookies, como o nosso cookie "oo", que tem uma duração de 5 anos, para te ajudar a deixar de ver anúncios do Facebook com base na tua atividade em sites de terceiros. Sabe mais sobre as informações que recebemos, a forma como escolhemos os anúncios que te apresentamos dentro e fora dos Produtos do Facebook e os controlos que tens à tua disposição.

Serviços e funcionalidades do site
Utilizamos cookies para ativar a funcionalidade que nos ajuda a fornecer os Produtos do Facebook.

Por exemplo: os cookies ajudam-nos a armazenar preferências, a saber em que altura viste ou interagiste com conteúdos dos Produtos do Facebook e a fornecer-te experiências e conteúdos personalizados. Por exemplo, os cookies permitem-nos apresentar sugestões a ti e a outras pessoas e personalizar os conteúdos de sites de terceiros que integram os nossos plug-ins sociais. Se tens o cargo de administrador de uma Página, os cookies permitem-te alternar entre a publicação a partir da tua conta pessoal do Facebook e da Página. Utilizamos cookies como o "presence", baseado na sessão, para dar suporte à tua utilização das janelas de chat do Messenger.

Também utilizamos cookies para nos ajudar a fornecer-te conteúdos relevantes face à tua localização.

Por exemplo: armazenamos informações num cookie instalado no teu browser ou dispositivo para que possas ver o site no teu idioma preferencial.

Desempenho
Utilizamos cookies para te fornecer a melhor experiência possível.

Por exemplo: os cookies ajudam-nos a encaminhar o tráfego entre os servidores e a compreender a velocidade de carregamento dos Produtos do Facebook para cada pessoa. Os cookies também nos ajudam a registar a proporção e as dimensões do teu ecrã e janelas e a saber quando ativas o modo de alto contraste, de forma a apresentarmos os nossos sites e apps corretamente. Por exemplo, definimos os cookies "dpr" e "wd", cada um com uma duração de 7 dias, para fornecer uma experiência ideal para o ecrã do teu dispositivo.

Análise e pesquisa
Utilizamos cookies para compreendermos melhor a forma como as pessoas utilizam os Produtos do Facebook, para que possamos melhorá-los.

Por exemplo: os cookies ajudam-nos a compreender a forma como as pessoas utilizam o serviço do Facebook, a analisar as partes dos Produtos do Facebook que as pessoas consideram mais úteis e apelativas e a identificar funcionalidades que podem ser melhoradas.

Sites e apps de terceiros
Os nossos parceiros de negócio também podem optar por partilhar informações com o Facebook a partir de cookies colocados nos domínios dos seus sites, quer tenhas ou não uma conta do Facebook ou tenhas sessão iniciada. Especificamente, os cookies com os nomes _fbc ou _fbp podem estar colocados no domínio do parceiro de negócio do Facebook cujo site estás a visitar. Ao contrário dos cookies que estão colocados nos domínios do Facebook, estes cookies não são acessíveis pelo Facebook quando estás num site que não seja o site no qual foram colocados, incluindo quando estás num dos nossos domínios. O seu propósito é igual ao dos cookies colocados no domínio do Facebook, cujo objetivo é personalizar conteúdos (incluindo anúncios), medir anúncios, elaborar estatísticas e fornecer uma experiência mais segura, como definido na nossa Política de Cookies.

Voltar ao início

Onde utilizamos cookies?

Podemos guardar cookies no teu computador ou dispositivo e receber informações armazenadas em cookies quando utilizas ou visitas:

- Os Produtos do Facebook;
- Produtos fornecidos por outros membros das Empresas do Facebook; e
- Apps e sites fornecidos por outras empresas que utilizam os Produtos do Facebook, incluindo as empresas que integram as Tecnologias do Facebook nos respetivos sites e apps. O Facebook utiliza cookies e recebe informações quando visitas esses sites e apps, incluindo informações do dispositivo e informações sobre a tua atividade, sem que tenhas de efetuar qualquer outra ação. Isto ocorre independentemente de teres ou não uma conta do Facebook ou de teres sessão iniciada.

Voltar ao início

É possível que outras empresas utilizem cookies em associação aos Produtos do Facebook?

Sim, outras empresas utilizam cookies nos Produtos do Facebook para nos fornecer serviços de publicidade, medição, marketing e análise e para te fornecer determinadas funcionalidades e melhorar os nossos serviços para ti.

Por exemplo, os cookies de outras empresas ajudam a personalizar os anúncios fora do Facebook, a medir o seu desempenho e eficácia e a prestar apoio ao marketing e à análise. Determinadas funcionalidades nos Produtos do Facebook utilizam cookies de outras empresas para funcionar (por exemplo, determinadas funcionalidades de mapas, pagamentos e segurança). Saibe mais sobre as empresas que utilizam cookies nos Produtos do Facebook.

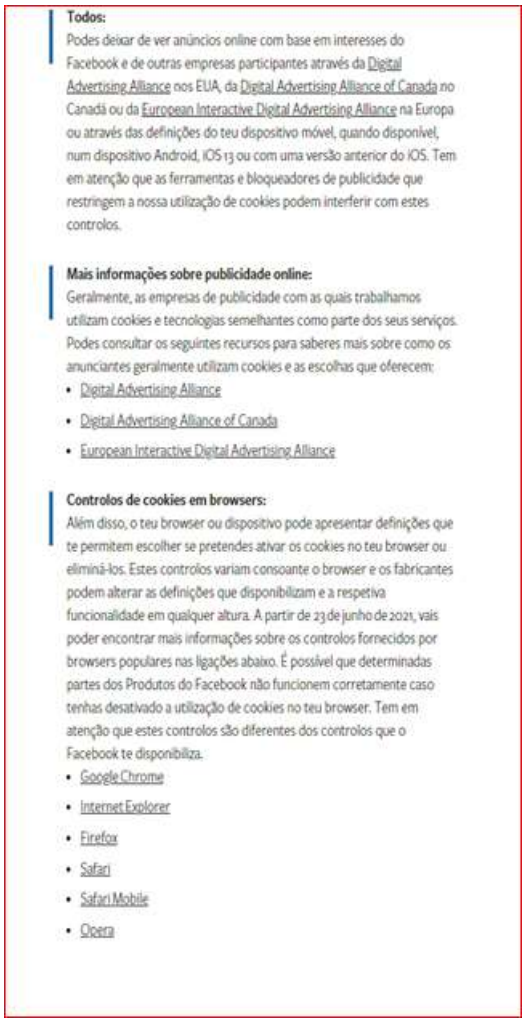
Os cookies também são utilizados por outras empresas nos respetivos sites e apps em associação aos Produtos do Facebook. Para compreenderes como os cookies são utilizados por outras empresas, consulta as respetivas políticas.

Como podes controlar as tuas informações?

Utilizamos cookies para ajudar a personalizar e melhorar conteúdos e serviços, fornecer uma experiência mais segura e mostrar-te anúncios relevantes e úteis dentro e fora do Facebook. Podes controlar a forma como utilizamos dados para te apresentar anúncios e muito mais através das ferramentas descritas abaixo.

Se tiveres uma conta do Facebook:

- Podes utilizar as tuas preferências de publicidade para saberes por que motivo estás a ver um anúncio específico e controlar a forma como utilizamos as informações que recolhemos para te apresentar anúncios.
- Para te apresentar anúncios que sejam mais relevantes para ti, utilizamos os dados que os anunciantes e outros parceiros nos fornecem sobre a tua atividade fora dos Produtos das Empresas do Facebook, incluindo sites e apps. Podes controlar se utilizamos estes dados para te apresentar anúncios nas tuas definições de anúncios.
- A Audience Network do Facebook é uma forma de os anunciantes te apresentarem anúncios em apps e sites fora dos Produtos das Empresas do Facebook. Uma das formas de a Audience Network apresentar anúncios relevantes passa por utilizar as tuas preferências de publicidade para determinar quais os anúncios que podes ter interesse em ver. Podes controlar esta opção nas tuas definições de publicidade.
- Podes rever a tua atividade fora do Facebook, que é um resumo da atividade que os negócios e as organizações partilham connosco sobre as tuas interações com os mesmos, como visitas aos seus sites ou às suas apps. Esses negócios e organizações utilizam as nossas ferramentas de negócios, como o Píxel do Facebook, para partilharem estas informações connosco. Isto ajuda-nos a realizar ações como dar-te uma experiência mais personalizada no Facebook. Sabe mais sobre a atividade fora do Facebook, sobre a forma como a utilizamos e como a podes gerir.



Todos:
Podes deixar de ver anúncios online com base em interesses do Facebook e de outras empresas participantes através da Digital Advertising Alliance nos EUA, da Digital Advertising Alliance of Canada no Canadá ou da European Interactive Digital Advertising Alliance na Europa ou através das definições do teu dispositivo móvel, quando disponível, num dispositivo Android, iOS 13 ou com uma versão anterior do iOS. Tem em atenção que as ferramentas e bloqueadores de publicidade que restringem a nossa utilização de cookies podem interferir com estes controlos.

Mais informações sobre publicidade online:
Geralmente, as empresas de publicidade com as quais trabalhamos utilizam cookies e tecnologias semelhantes como parte dos seus serviços. Podes consultar os seguintes recursos para saberes mais sobre como os anunciantes geralmente utilizam cookies e as escolhas que oferecem:

- Digital Advertising Alliance
- Digital Advertising Alliance of Canada
- European Interactive Digital Advertising Alliance

Controlos de cookies em browsers:
Além disso, o teu browser ou dispositivo pode apresentar definições que te permitem escolher se pretendes ativar os cookies no teu browser ou eliminá-los. Estes controlos variam consoante o browser e os fabricantes podem alterar as definições que disponibilizam e a respetiva funcionalidade em qualquer altura. A partir de 23 de junho de 2021, vais poder encontrar mais informações sobre os controlos fornecidos por browsers populares nas ligações abaixo. É possível que determinadas partes dos Produtos do Facebook não funcionem corretamente caso tenhas desativado a utilização de cookies no teu browser. Tem em atenção que estes controlos são diferentes dos controlos que o Facebook te disponibiliza.

- Google Chrome
- Internet Explorer
- Firefox
- Safari
- Safari Mobile
- Opera

Data da consulta: 20/05/2021