REVISTA
TRANSGRESSÕES
CIÊNCIAS CRIMINAIS EM DEBATE
v. 8, n. 1, julho de 2020

UTILIZAÇÃO DO RECONHECIMENTO FACIAL ELETRÔNICO POR EMPRESAS PARA IDENTIFICAÇÃO DE SUSPEITOS: SEGURANÇA OU VIOLAÇÃO DO ESTADO DEMOCRÁTICO DE DIREITO?

Isabela Maria Pereira Paes de Barros

Graduanda em Direito pela Universidade Federal de Pernambuco (UFPE).

Isabela Inês Bernardino de Souza Silva

Graduanda em Direito pela Universidade Federal de Pernambuco (UFPE) e estagiária do Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.REC).

RESUMO

O presente artigo busca analisar o uso do reconhecimento facial eletrônico por empresas públicas e privadas como uma ferramenta violadora de direitos humanos, especialmente quando utilizado para identificação de suspeitos de infrações e contravenções penais. Nesse sentido, é comum que esses sistemas de monitoramento estejam passíveis às situações de falsos positivos, identificando, erroneamente, pessoas que têm características físicas semelhantes, e fazendo com que os operadores de segurança acreditem que essas pessoas são culpadas por ações de terceiros. Muitos países estão reduzindo ou limitando o uso dessas tecnologias, mas o Brasil se encontra no caminho oposto a essa tendência. A metodologia de pesquisa deste trabalho é bibliográfica, com consultas a matérias de jornal, artigos científicos e documentos nacionais e internacionais. O resultado obtido é o de que o reconhecimento facial eletrônico, ainda que pareça benéfico, potencializa situações de preconceito e desigualdade que põe em risco parcelas historicamente marginalizadas da população.

Palavras-chave: Reconhecimento facial. Criminologia. Empresas. Direitos humanos.

1 INTRODUÇÃO

A vigilância em empresas públicas e privadas, especialmente como uma forma de aprimoramento da segurança populacional, está sendo um aspecto cada vez mais debatido ao redor do globo terrestre. Muitos eventos de grande magnitude – como Copas do Mundo,

Olimpíadas ou Conferências –, em que grandes aglomerados populacionais são previstos, vêm sendo palco de teste e treinamento de novas tecnologias de vigilância, de modo a se buscar um aprimoramento desses mecanismos, conforme será visto ao longo do trabalho.

Nessa seara crescente, o reconhecimento facial surge como um dos principais instrumentos de vigilância, sob o manto da segurança social. Instalam-se câmeras em cada vez mais lugares e criam-se inteligências artificiais de análise, caracterização e identificação de rostos, ambas as medidas tomadas sob o discurso da necessidade de proteger os cidadãos de possíveis violações de direitos, infrações ou contravenções penais.

Porém, não se percebe que a vigilância e, mais precisamente, o reconhecimento facial, cria um paradoxo. O monitoramento constante de rostos e corpos em ruas, praças, avenidas, empresas públicas, e até privadas, gera uma incerteza e insegurança na vida das pessoas que são submetidas a esse tratamento. Os dados armazenados – sobre lugares frequentados, formato de rosto, características físicas, etc. – criam uma possibilidade de uso de tais informações de maneira indevida; especialmente quando "hackeados" por pessoas mal intencionadas.

Mesmo sem tal exposição aos *hackers*, o reconhecimento facial tem um problema: como se sentir seguro quando o governo ou a empresa por trás daquela câmera sabe sua rotina e seus costumes? Esse sistema, sob a desculpa de sua utilização para identificação de pessoas suspeitas de cometimento de atitudes ilícitas, é mesmo uma forma válida de segurança, ou é uma violação dos corpos, das subjetividades e da intimidade, ou seja, uma violação ao Estado Democrático de Direito em sua essência? São, pois, esses questionamentos que o presente artigo procura discutir.

Assim, a metodologia utilizada é qualitativa, por meio de análise bibliográfica e documental. Utilizou-se da pesquisa em artigos científicos, matérias de jornal e ensaios sobre a temática do reconhecimento facial e do uso dessa ferramenta por empresas públicas e privadas, além de analisar resoluções e documentos da Organização das Nações Unidas acerca do assunto, para avaliar o comprometimento internacional do Brasil frente ao tema.

2 SOCIEDADE DA VIGILÂNCIA

Com o decorrer de duas Guerras Mundiais e da Guerra Fria, além de outros conflitos localizados, e com o desenvolvimento de novas tecnologias de informação, o mundo globalizado passou a procurar maneiras de aumentar a segurança nacional e internacional, em paralelo ao aprimoramento de uma tecnologia que servisse também ao comércio global. Nesse sentido, houve uma melhora nas formas de recolhimento de informações pessoais, para além de "meras" coletas de DNA e impressões digitais, e foi inaugurada a obtenção de informações por meio de dados telefônicos, provedores de internet e do discurso de segurança internacional, até se chegar a um dos métodos de coleta de informações mais desenvolvidos da atualidade: a vigilância por reconhecimento facial.

Surgido em 1964 através de um trabalho de Woodrow Wilson, Chan Wolf e Charles Bisson (VIANA; CONCEIÇÃO; ROCHA, 2019), o reconhecimento facial é um método através do qual se faz uso de *softwares* computacionais a fim de identificar pessoas com base em características de seus rostos. Assim, o programa parte da identificação de "pontos nodais" – como a localização dos olhos ou o alongamento do nariz –, de uma foto pré-identificada, ou de uma série de fotos, para reconhecer um rosto individual por meio do *cross-checking* (isto é, da validação cruzada) de informações, ou seja, através da verificação, em outras fotos ou filmagens, da presença do mesmo padrão de pontos nodais nos rostos identificáveis (PROJECT ON GOVERNMENT OVERSIGHT, 2019; BONFÁ, 2013). É importante frisar, entretanto, que se utilizam distâncias entre pontos para calcular uma probabilidade de combinação do rosto identificado com outro previamente cadastrado no banco de dados, ou seja, não se analisa a face por completo (NUNES, 2019) – o que pode gerar situações de identificação de padrões entre pessoas diversas.

Dessa forma, os sistemas de reconhecimento facial procuram converter as fotos existentes em sistemas de armazenamento de dados para que esses sejam usados de modo a facilitar a identificação de um grande número de indivíduos. Em tal aspecto, essa tecnologia permite que, por meio de imagens captadas por câmeras situadas em diversos pontos da cidade, governos possam cruzar informações em seus bancos de dados acerca de biótipos e formatos do rosto, de modo a obter outras informações da pessoa que está sendo analisada, como impressões digitais e endereços. (PROJECT ON GOVERNMENT OVERSIGHT, 2019).

Essa identificação rápida de qualquer pessoa é utilizada para legitimar o uso do reconhecimento facial como uma ferramenta para combater o terrorismo e o crime (PROJECT

ON GOVERNMENT OVERSIGHT, 2019), como será melhor visto adiante. Nesse sentido, deve-se ter parcimônia com a utilização do reconhecimento facial e dos demais mecanismos de vigilância, buscando-se não impedir o anonimato e violar as subjetividades individuais, especialmente tendo em vista que as ferramentas de reconhecimento facial são utilizadas de forma controversa para reprimir protestos e imputar condutas criminosas aos protestantes.

Todavia, em muitos lugares, não se vê o comedimento. Na China, por exemplo, a tecnologia vem começando a moldar a sociedade em uma versão futurista dos livros orwellianos "Oceania" e "1984"; enquanto nos Estados Unidos, o reconhecimento facial vem tomando conta cada vez mais das agências públicas e privadas, sem que existam leis suficientes que regulem essa tecnologia invasiva (PROJECT ON GOVERNMENT OVERSIGHT, 2019).

3 O RECONHECIMENTO FACIAL COMO UM ASPECTO DA VIGILÂNCIA FACE AOS DIREITOS HUMANOS E A FALÁCIA DA SEGURANÇA PÚBLICA

É fato que o reconhecimento facial, na contemporaneidade, é usado para o combate do terrorismo e das demais condutas socialmente indesejáveis e passíveis de punição estatal, de modo a facilitar a execução da pena e evitar a prescrição da pretensão punitiva do Estado (SPANHOL; LUNARDI; SOUZA, 2016; BONFÁ, 2013). Contudo, seu uso não pode ser feito de maneira indiscriminada, devendo ser balanceado com um imperativo categórico que proteja os direitos humanos e os valores de cada sociedade, incluindo-se, especialmente, o direito ao anonimato e à liberdade de expressão e associação, além de atender à exigência de transparência governamental (PROJECT ON GOVERNMENT OVERSIGHT, 2019). Isso porque, a partir do momento que o indivíduo sabe que pode ser reconhecido de forma remota e catalogado como participante de uma manifestação pública, sua liberdade de expressão e seu direito de se posicionar sobre o que quiser são comprometidos (ABRAMOVAY, 2019).

Nesse sentido, os erros do reconhecimento facial podem gerar situações de constrangimento, prisões arbitrárias e violações de direitos humanos mais graves (NUNES, 2019). Ademais, muito se questiona sobre a mitigação da privacidade e da proteção de dados dos cidadãos, por parte do aparato estatal, ao se valer de *softwares* de reconhecimento facial (CANTO, 2019). A situação é agravada com o fato de que essa tecnologia não necessita de

uma natureza militar para que consiga impactar em questões estatais de segurança e defesa (BUZAN; HANSEN, 2009).

O fato é que o algoritmo necessita de um grande volume de dados para poder tomar suas próprias decisões. Estes são retirados de toda a população continuamente, o que pode gerar consequências futuras nas questões de direitos fundamentais e, por isso, precisam ser jurídica e eticamente regulados.

Porém, as previsões internacionais sobre o tema são escassas. Ainda assim, em 2013, o Brasil mostrou suas preocupações quanto a isso – sobretudo, após a descoberta de que a então presidenta Dilma Rousseff estava sendo espionada por um esquema de vigilância internacional da Agência de Segurança Nacional Norte-Americana (NSA) (CANTO, 2019). Dessa forma, a representação brasileira na Assembleia Geral das Nações Unidas (AGNU) e a chanceler alemã Angela Merkel apresentaram a Resolução n. 68/167 sobre o direito à privacidade na era digital, um dos primeiros documentos internacionais sobre o tema – ainda que de caráter recomendatório (UNITED NATIONS GENERAL ASSEMBLY, 2013).

No ano seguinte, em 2014, a AGNU adotou outra resolução sobre o tema, a Resolução n. 69/166, que adicionou ao documento anterior outras recomendações em matéria de direitos humanos, como "o reconhecimento da necessidade de discutir e analisar, com base na legislação internacional de direitos humanos, questões relacionadas com a promoção e proteção do direito na era digital" (CANTO, 2019, p. 9). Além disso, a mencionada resolução destacou que existem riscos relacionados à coleta de metadados, tais como a revelação de informações pessoais e características como hábitos, relações sociais e preferências privadas, e que devem ser tomadas medidas para proporcionar reparações em casos de violação à privacidade de indivíduos ou em casos de condutas de vigilância arbitrárias (UNITED NATIONS GENERAL ASSEMBLY, 2014).

Tendo em vista essas resoluções, surgem, então, questionamentos. Como permitir o reconhecimento facial por meio de sistemas eletrônicos quando esses podem ser usados de maneira arbitrária pelas instâncias governamentais, configurando uma verdadeira violação ao Estado Democrático de Direito – compreendido como cumprimento das normas e dispositivos legislativos os quais são adotados em território nacional por todos os jurisdicionados, entes públicos ou privados –, ao qual o próprio governo também está submetido?

É importante, ainda, pontuar que essa situação é agravada pelas falhas do reconhecimento facial, que demonstram como esse instrumento eletrônico pode vir a

discriminar pessoas e privá-las de direitos básicos, como o de ir e vir a qualquer momento. Um exemplo disso é o chamado "racismo algorítmico": distorções nas bases de dados de algoritmos que geram distorções nos resultados obtidos, sendo mais comuns os resultados de falso positivo em desfavor de pessoas negras que de pessoas brancas, criando situações de constrangimento e discriminação contra essa parcela da população que já é vítima de um racismo estrutural (AMPARO, 2020). Ademais, há, ainda, os dados que demonstram que 90,5% das pessoas presas através da utilização de monitoramento facial, no Brasil, são negros (NUNES, 2019), o que agrava tal panorama.

Isso incide diretamente nas questões de racismo estrutural do Brasil. Nesse aspecto, é importante frisar que o debate sobre vigilância e direito penal sempre perpassa pela ótica estatal de punir seus sujeitos "delinquentes" de acordo com critérios raciais (SILVA; SILVA, 2019), nos quais negros e negras são as maiores vítimas. A seletividade do sistema repercute diretamente nos dados que são usados para alimentar a inteligência artificial do reconhecimento facial, o que acaba por gerar mais constrangimento e violência para a população negra.

> Com efeito, uma vez que o racismo faz parte da estrutura do Estado brasileiro, o que ocorre é que a sua reprodução no seio da internet acaba sendo feita da mesma forma: com discrição. Assim, o que se tem é o enraizamento tecnológico de preconceitos, ainda mais porque se tem a vaga crença de que, por se tratar de operações basicamente matemáticas, não haveria como reproduzir discursos racistas e preconceituosos através do seu emprego (SILVA; SILVA, 2019, p. 14).

Nesse sentido, é importante pontuar como os sistemas de reconhecimento facial são menos precisos e mais errôneos ao captar rostos de pessoas negras (BUOLAMWINI; GEBRU, 2018). Ademais, existem problemas no algoritmo de busca de sites como Google, como é possível ver no exemplo da busca por termos como "garotas negras" que, até pouco tempo, resultava em conteúdo pornográfico, além da problemática do Google Photos, que rotulava pessoas negras como "gorilas". Em outra faceta do racismo estrutural, há, ainda, os casos de câmeras da Nikon que não captavam rostos de pessoas asiáticas, além das *startups* que afirmavam poder identificar terroristas apenas com os traços faciais das pessoas (SILVA, 2019), demonstrando os riscos da perpetuação de mecanismos de "estereotipação" e exclusão de grupos sociais (DREYER; SCHULZ, 2018).

Todas essas situações acabam gerando desconforto e mal estar em pessoas que não se encontram nos padrões desenhados por esses *softwares.* Além disso, há ainda a possibilidade

de que tais falsos positivos, ou identificações errôneas, criem casos em que pessoas acabem sendo identificadas como criminosos quando não o são, podendo, inclusive, escalonar para casos mais sérios de perseguição policial e morte (METZ, 2019).

O uso de algoritmos de reconhecimento demonstra, portanto, como essas tecnologias são manipuladas e utilizadas de forma que, embora pareçam neutras, têm como objetivo prever comportamentos, reduzir o tempo livre ou influenciar opções políticas. Assim, os instrumentos de reconhecimento facial, além de violadores de direitos humanos básicos, refletem e reforçam preconceitos de gênero, raça e classe existentes no imaginário social (COALIZÃO DIREITOS NA REDE, 2019).

4 A VIGILÂNCIA E O RECONHECIMENTO FACIAL NAS PERSPECTIVAS MUNDIAL E BRASILEIRA

O movimento contrário ao uso do reconhecimento facial, percebendo as nuances prejudiciais destes, vem sendo uma tendência em crescimento ao redor do mundo (NUNES, 2019). Cidades como São Francisco, Somerville e Oakland, nos Estados Unidos, baniram, em 2019, o uso de tecnologias de reconhecimento facial nas instâncias governamentais, inclusive em âmbito policial (METZ, 2019). Ademais, a Microsoft, empresa do ramo de *softwares* e *hardwares*, recentemente recusou um pedido de uma agência de policiamento do estado da Califórnia, Estados Unidos, para fornecimento de tecnologia de reconhecimento facial sob o argumento de preocupação com os direitos humanos. Nesse sentido,

> A recusa se deu pela possibilidade de aumentar a discriminação para com mulheres e pessoas de pele negra, haja vista que tecnologias de reconhecimento facial são majoritariamente treinadas em homens brancos, o que poderia levar a erros de interpretação e, consequentemente, prisões abusivas e incoerentes. (ARBULU, 2019a)

Na mesma esteira, a própria Amazon, empresa do ramo, sofreu críticas por motivos semelhantes: no estado do Oregon, também nos Estados Unidos, o *software* “Rekognition”, utilizado pela polícia, foi alvo de pedidos de paralisação de seu uso e banimento por existirem testes comprovando que ele apresenta falhas de reconhecimento (ARBULU, 2019a).

Na Inglaterra, apesar de não haver tal tipo de banimento, o governo decidiu permitir o uso de sistemas de reconhecimento facial apenas por meio de autorização governamental,

em que se mostre ser necessário e proporcional ao uso específico do sistema de policiamento. Em tal viés, o governo ainda dispôs que os funcionários que forem lidar com esses sistemas de reconhecimento devem ser treinados para a compreensão dos riscos associados ao uso do *software*, gerando uma aura de conscientização necessária, demonstrando uma forma de lidar com a implementação do reconhecimento facial que ainda considera princípios como transparência e democracia (MAIA, 2019).

Cidades como Londres, entretanto, ainda têm uma quantidade exacerbada de dispositivos de reconhecimento facial por habitante – mais que Pequim, por exemplo. Já a China, onde há cerca de 176 milhões de câmeras de segurança, detém 46% do faturamento sobre dispositivos de reconhecimento facial no mundo (ABRAMOVAY, 2019), demonstrando, ainda, o poder social desses sistemas.

Já na perspectiva brasileira, a utilização do reconhecimento facial vem aumentando de maneira exponencial, indo na contramão de outros países (NUNES, 2019), sob o argumento de que esta tecnologia seria essencial para garantir a segurança da população. Equipando-se câmeras ao redor da cidade, as pessoas, em tese, tendem a se sentir mais protegidas e assistidas pelo Estado. Contudo, como foi visto anteriormente, isso é uma falácia, já que há uma grande margem de erro para essas câmeras.

Com o objetivo primordial de fiscalizar e garantir a segurança, o Brasil vem se tornando "um dos principais e mais atraentes laboratórios a céu aberto para as tecnologias de vigilância estrangeiras durante a última década" (CANTO, 2019, p. 2). Seu uso já foi feito na Rio+20, em 2012, na Copa do Mundo de 2014, nos Jogos Olímpicos e Paraolímpicos de 2016 e na Copa América de 2019 (CANTO, 2019).

A justificativa para o seu uso é sempre a mesma: com o reconhecimento facial, os agentes de segurança prometem diminuir substancialmente a violência e criar perímetros de segurança, onde qualquer pessoa foragida da polícia, mesmo disfarçada, possa ser encontrada.

Nesse cenário, o Instituto Igarapé do Rio de Janeiro vem fazendo uma metragem acerca do aumento do número de câmeras que vêm sendo instaladas por todo o Brasil e constatou que foram reportados 48 casos do uso de reconhecimento facial por autoridades públicas e seus parceiros do setor privado desde 2011, dentre os quais 13 foram utilizados para segurança pública (INSTITUTO IGARAPÉ, 2020). Segundo eles:

> [...] bases de dados públicas e privadas (algumas contendo informações detalhadas sobre as vidas civil e penal das pessoas) já coletavam registros faciais e biométricos

> mesmo antes do país aprovar a sua lei de proteção de dados pessoais. Essas bases são fundamentais para alimentar o sistema de reconhecimento facial com informações que possam apontar quando uma pessoa tem pendências com as autoridades públicas, registro criminal ou quando não é quem diz ser.

Um fato importante é que, além de violar os direitos fundamentais da população, esse sistema, quando colocado em locais muito específicos, como estádios, após o evento, fica sem uso. Ou seja, investimentos milionários são feitos, mas não há nenhuma perspectiva de como aquela tecnologia possa ser usada no futuro. Na Copa América de 2019, quando questionado, Hilário Medeiros, gerente de Segurança do Comitê Organizador Local (COL), respondeu que: "como vai ser em termos de legado, isso nós não estamos tratando. Estamos tratando agora do momento da operação" (DOLZAN, 2019).

Já no caso de tecnologias colocadas no ambiente público da cidade, estas sim viram um problema para a população, uma vez que, depois de vigiar os torcedores, começam a fiscalizar o restante da sociedade de forma diária. Segundo Kayyali:

> Legisladores usaram a série de megaeventos esportivos no país para justificar os altos investimentos em tecnologia de segurança. Mas as ferramentas que a polícia e o exército agora têm em mãos não são temporárias. São legados duradouros. E a combinação dessa tecnologia, um novo governo conflituoso e abusos contínuos a direitos humanos por parte de policiais no Brasil formam, para muitos, o desenho de um desastre (KAYYALI, 2016).

Mais preocupante ainda é o fato de toda essa vigilância estar nas mãos de uma empresa privada, a International Business Machines (IBM), empresa norte-americana. Ela possui um arsenal gigantesco de *data centers* e integra mais de 30 agências do Centro de Operações do Rio (THE NEW YORK TIMES, 2012). Ele é o

> Primeiro Centro do planeta na linha mundial de Cidades Inteligentes, que irá integrar todas as etapas de um gerenciamento de crise: desde a antecipação, mitigação e preparação, até a resposta imediata aos eventos e realimentação do sistema com novas informações que podem ser usadas em futuros casos (PREFEITURA DO RIO DE JANEIRO, 2010).

Além do mais, obviamente, esse sistema pode gerar lucros multimilionários (THE NEW YORK TIMES, 2012) para a empresa, uma vez que tal ramo vem crescendo de maneira exponencial e sendo utilizado por diversos países e cidades ao redor do mundo.

Além dos grandes eventos esportivos, a tecnologia de vigilância e reconhecimento facial vem sendo aplicada também no Carnaval brasileiro. Em 2019, o reconhecimento facial foi utilizado na praia de Copacabana, no Rio de Janeiro, com o objetivo de "reconhecer carros

roubados e pessoas que estivessem com mandados de prisão expedidos" (INTERVOZES, 2019). O *software*, de propriedade da empresa Oi, comparava os rostos das pessoas filmadas com fotos de procurados e, caso houvesse compatibilidade, alertava às autoridades. Tudo isso ocorreu no Centro Integrado de Comando e Controle (CICC) da cidade. Ao total, quatro pessoas foram reconhecidas e presas, um adolescente foi apreendido e um carro roubado foi recuperado. No Carnaval de Salvador um sistema semelhante foi utilizado, pertencente à empresa chinesa Huawei (INTERVOZES, 2019; DO BRASIL, 2019).

> Celebradas pelo governador Wilson Witzel e por autoridades policiais do Estado, as tecnologias de reconhecimento facial acumulam controvérsias, erros e fortes contestações nos países que as utilizam como ferramenta de segurança pública. O primeiro aspecto diz respeito ao caráter intrusivo e o perigo que representam a direitos civis, sobretudo em governos autoritários e que podem empregar o recurso para vigilância estatal em massa (INTERVOZES, 2019).

Além disso, o objetivo futuro é expandir essas câmeras, conforme coronel Mauro Fliess (DO BRASIL, 2019):

> O coronel acrescentou que a intenção da secretaria é estender o projeto a outros bairros, embora ainda não tenha um calendário para isso. De acordo com o porta-voz, o custo inicial do projeto é zero, uma vez que a operadora de telefonia já tem contrato com os órgãos de segurança na instalação de programas de comunicação nos veículos das polícias.
> 'A Oi já é uma parceira do estado. Hoje, dá todo o suporte à telefonia 190 e toda a rede de dados da corporação. Esse custo já está agregado ao serviço que a Oi presta ao estado. Isso na realidade é o tráfego de dados', completou.

Todavia, o reconhecimento já apresentou erros ao prender erroneamente pessoas no Brasil. Um exemplo é o caso de uma mulher em Copacabana, a qual fora confundida com uma pessoa procurada pela polícia que já há havia sido detida em 2015 e já se encontrava recolhida em um presídio (BIANCHI, 2020). Segundo Fliess, no país, "assim que o sistema aponta 70% de possibilidade de a pessoa ser a procurada, uma viatura é direcionada ao local" (apud ARBULU, 2019b). Em outras palavras, o sistema nunca possui 100% de certeza quando aponta um suspeito. Isso é um grande risco para a população em geral, uma vez que viola a própria liberdade dos cidadãos, que podem ser confundidos.

Outro exemplo importante a ser citado é a utilização de tais câmeras dentro de ônibus e metrôs. Em Pernambuco, no ano de 2018, foi anunciada pelo Sindicato das Empresas de Transporte de Passageiros do estado (Urbana-PE) a aquisição de um novo sistema de validação do acesso ao ônibus no Grande Recife, o bilhete eletrônico (Vale Eletrônico Metropolitano – VEM) passou a ter sua validade a partir de reconhecimento facial. A pessoa é

fotografada seis vezes no momento que adentra no ônibus e, mesmo que não use o bilhete eletrônico, é igualmente monitorada (AMORIM; RAMIRO, 2018).

5 A ENTRADA DE EMPRESAS NA ÁREA DE VIGILÂNCIA: POSSÍVEIS CONSEQUÊNCIAS

Tudo isso leva ao questionamento da forma como o Estado está se propondo a resolver as questões de criminalidade no país. Será que seria a maneira mais adequada para resolução dessas questões deixar que os dados da sua população fiquem nas mãos e sob julgamento de tecnologias de empresas privadas? Já foi visto, anteriormente, que os dados são apontamentos vitais sobre a realidade da população. Seu conteúdo, bastante pessoal, pode gerar grandes controvérsias na vida de uma pessoa. Isso se multiplica exponencialmente quando se vê que tais dados podem incriminar e restringir a liberdade de alguém.

A primeira análise que precisa ser feita diz respeito ao percentual de acerto que o reconhecimento facial pode ter. Até o presente momento, a maioria dos equipamentos destinados ao reconhecimento facial possui uma alta taxa de imprecisão, a qual pode gerar riscos para pessoas inocentes.

O grande problema é que, caso a foto seja tirada em condições ideais, como as feitas do rosto de prisioneiros, é mais fácil que o reconhecimento facial consiga identificar a pessoa, caso esteja nas mesmas condições. Todavia, a vigilância vem atingindo o dia-a-dia da sociedade e captura fotos de pessoas, geralmente, em movimento. Isso cria uma grande imprecisão, principalmente se houver má iluminação, ângulo ruim, movimento e grandes distâncias. Isso é o que gera os chamados “falsos positivos” e “falsos negativos” (PROJECT OF GOVERNMENT OVERSIGHT, 2019).

> Falsos negativos são o fracasso em associar uma pessoa em duas imagens; eles ocorrem quando a semelhança entre duas fotos é baixa, refletindo alguma alteração na aparência da pessoa ou nas propriedades da imagem. Falsos positivos são a associação errônea de amostras de duas pessoas; elas ocorrem quando os rostos digitalizados de duas pessoas são semelhantes (GROTHER; NGAN; HANAOKA, 2019, p. 5, tradução nossa).

Em outras palavras, o falso positivo ocorre quando o *software* associa duas pessoas diferentes como se fossem a mesma pessoa e o falso negativo quando não consegue associar

duas ou mais fotos da mesma pessoa. Nesse sentido, "os falsos positivos são muito mais perigosos, uma vez que podem identificar incorretamente uma pessoa acusada de um crime, por exemplo. No campo dos negócios, pode facilitar as fraudes, também" (FEITOSA JÚNIOR, 2019).

Quanto maior for o banco de dados, maior a probabilidade de haver falsos positivos, uma vez que haverá uma maior probabilidade de mais pessoas parecidas estarem lá. Segundo o relatório *The Perpetual Line-Up*, os algoritmos cometem vários erros diferentes. Basicamente, ele utiliza a foto e compara com um banco de dados que possui, e responde se há alguém que tem grande compatibilidade com as fotos ou não (GARVIE; BEDOYA; FRANKLE, 2016). É exatamente nesse ponto que é necessária a atenção de seres humanos para identificar se há algum erro dentro dessa verificação e tentar corrigi-lo. Porém, há uma grande crença por parte das autoridades nos resultados entregues por essa tecnologia. Muitas vezes, eles são aceitos sem nenhum tipo de desconfiança, quando, na verdade, deveria haver uma "checagem humana" antes de prosseguir para o cerceamento da liberdade de uma pessoa, para que esta não seja acusada indevidamente de um crime.

Por exemplo, na Polícia Metropolitana do Reino Unido, foi feita uma pesquisa que apontou que o índice de erro do reconhecimento facial foi de 81% no Carnaval de 2016 (MANTHROPE; MARTIN, 2019), uma vez que, dos 42 identificados pela tecnologia, apenas seis estavam certos (ENGLAND, 2019b). Já no Brasil, a situação é bem mais crítica. Com o reconhecimento facial, a Bahia teve 903 alertas durante o Carnaval, mas apenas 33 mandados de prisão foram feitos, ou seja, 4% das pessoas identificadas (PAULUZE, 2020), uma taxa baixíssima de precisão.

Devido a isso, já há autoridades ao redor do mundo que exigem que o reconhecimento facial tenha um percentual de acerto elevado para que a pessoa identificada possa ser considerada uma suspeita. É o caso da Polícia de São Francisco, que exige uma aproximação de 96% entre as fotos comparadas (GARVIE; BEDOYA; FRANKLE, 2016).

Não é sem razão, inclusive, que a Google, a Amazon e a Microsoft já se pronunciaram contra o uso de reconhecimento facial (ENGLAND, 2019a; DENT, 2019; LOCKLEAR, 2018). As imagens capturadas pelas câmeras, na maioria das vezes, não são imagens frontais do rosto. Além disso, as imagens também podem se encontrar com uma baixa qualidade devido à luz, o que distorce ainda mais o rosto filmado. Por isso, é mais comum do que se imagina que a máquina cometa erros de identificação.

Ademais, como é uma tecnologia que lida com direitos fundamentais das pessoas – imagem, privacidade, liberdade –, ela pode tanto ajudar a polícia a identificar algum criminoso, quanto pode ser decisiva para condenar uma pessoa inocente. Adicionando ainda mais problemáticas, se pode observar que, com tamanha baixa taxa de precisão, qual a porcentagem que seria considerada limítrofe na hora de escolher se aquela pessoa corresponde mesmo ou não à imagem? O percentual de 70% pode ser considerado um número favorável ou desfavorável na hora da acusação?

Essas questões ainda não estão sendo debatidas de maneira concreta dentro do cenário criminal. Com a ideia de uma tecnologia que solucionará qualquer problema, a população vem sendo convencida de que, apenas com ela, será possível identificar qualquer criminoso. Muito pelo contrário, a vulnerabilidade das pessoas se mostra como característica ímpar à ojeriza criada por parte dos estudiosos a esse tipo de tecnologia.

Como poder confiar apenas no discernimento de uma máquina que apenas se utiliza de algoritmos para fazer uma decisão? "Infelizmente, a aplicação da lei pode receber informações irrealisticamente otimistas dos fornecedores sobre o quão bem o reconhecimento facial funciona [...] que, na realidade, é limitada em como pode ser efetivamente implantada" (PROJECT OF GOVERNMENT OVERSIGHT, 2019, tradução nossa). Ou seja, obviamente, quando uma empresa privada tenta vender seu produto, ela faz todo um *marketing* em cima das suas boas qualidades, afirmando que dará aos policiais a possibilidade de identificar instantaneamente suspeitos, ou que apenas com foto o policial poderá ver se ele é suspeito ou não, identificar num banco de dados com alto grau de precisão, entre outras justificativas. Todavia, essa descrição sempre será exagerada, irreal, e, ao final, induz a todos, fazendo-os acreditar que estão diante de uma tecnologia revolucionária, com capacidades ilimitadas.

Contudo, sua limitação está cada vez mais aparente, já que os resultados se alteram de acordo com o local e as condições onde tal tecnologia é aplicada. Além disso, o reconhecimento facial é muito menos preciso quando envolve pessoas negras, o que aumenta ainda mais a sua vulnerabilidade e seus riscos (AMPARO, 2019; BARBON, 2019).

Assim, tem-se empresas privadas que detêm um grande número de dados pessoais da população e a capacidade de incriminar pessoas, sendo elas inocentes ou não. Muitas vezes, caso seja identificada uma pessoa, os policiais vão agir como se ela realmente fosse o suspeito. A empresa não vende sua tecnologia afirmando que há a possibilidade de aquela pessoa não ser a que eles estavam procurando. Muito pelo contrário, elas vendem o produto

afirmando que, dentre todas as pessoas que estão no seu banco de dados, aquela é a mais provável (GARVIE; BEDOYA; FRANKLE, 2016). Isso muda muito o modo de agir a partir da identificação.

Dessa forma, a abordagem policial é diversa do modelo "ideal", visto que o agente público não se utiliza da presunção de inocência, mas da "presunção de culpabilidade", ou seja, da ideia de que o sujeito investigado é culpado, já que uma tecnologia de reconhecimento facial lhe deu essa informação. É necessário, todavia, entender que essa é uma forma de prova, mas que também é preciso haver outras para corroborar qualquer decisão legal. O crescimento do reconhecimento facial no âmbito público e privado quebra essa lógica, fazendo com que as pessoas, cada vez mais, queiram usá-lo como o único meio de prova necessário, revestido de uma aparente objetividade.

Por isso, entendendo a problemática e procurando mitigá-la, o projeto *The Perpetual Line-Up*, de 2016, traz algumas recomendações bastante importantes sobre o tema. Primeiramente, as fotos que forem utilizadas no reconhecido facial devem ser retiradas de carteira de motoristas, documentos de identificação e devem ser constantemente renovadas. Além disso, tais fotos só devem ser usadas por meio de uma ordem judicial que as permita, e que seja lastreada por um pedido fundamentado, isto é, plausível. Já caso o reconhecimento facial seja aplicado em vídeos de vigilância ou câmeras usadas pela polícia, recomenda-se fortemente que seja definido pelos órgãos quais são os limites e a natureza do espaço público.

Nesse viés, o governo precisaria fazer relatórios públicos e auditorias internas para sempre checar como estão funcionando tais câmeras, além de financiar testes de precisão, criar testes padronizados e independentes para taxas de erro com tendência racial e criar bancos de dados de fotos que facilitem tais testes. A polícia também precisa ser transparente quanto aos dados e ao modo que eles estão sendo usados, prezando pela sua precisão e inovação. É necessário haver a pressão da população acerca desse tema, para que as políticas sejam em prol da privacidade, liberdade civil e direitos, evitando qualquer tipo de abuso ou uso indevido (GARVIE; BEDOYA; FRANKLE, 2016).

No mesmo viés, pauta-se a Organização das Nações Unidas: o órgão internacional considera essencial uma abordagem multissetorial para a mitigação de riscos, baseada no desenvolvimento de tecnologias de reconhecimento facial e inteligência artificial por meio de uma abordagem alinhada aos direitos humanos (UNITED NATIONS HUMAN RIGHTS OFFICE OF THE HIGH COMMISSIONER, 2018). Assim, a própria ONU já publicou

documentos universais para guiar empresas e órgãos estatais com princípios orientadores de mitigação de riscos no uso de novas tecnologias, sugerindo que as empresas dos mais diversos setores devem ser proativas na defesa aos direitos humanos, fazendo avaliações de impactos de direitos fundamentais, implementando-as para mitigá-los, e acompanhando a eficácia dessas medidas (UNITED NATIONS HUMAN RIGHTS OFFICE OF THE HIGH COMMISSIONER, 2011), para mostrar às partes interessadas e à sociedade civil que existem medidas de redução de impacto em vigor.

6 CONSIDERAÇÕES FINAIS

Portanto, é preciso ponderar acerca do uso do reconhecimento facial para fins de identificação criminal, uma vez que este mitiga direitos fundamentais bastante importantes para a pessoa humana. Tais tecnologias podem ser usadas como um dos meios de prova, mas não pode ser o único. A partir do momento em que há a combinação entre a foto e a pessoa no vídeo, as autoridades, normalmente, tendem a já enquadrá-la como o próprio culpado, não como o suspeito, gerando inúmeras situações de desconforto, principalmente para com pessoas negras, as quais são as principais vítimas de falsos positivos.

É necessário entender que, assim como há provas testemunhais, físicas, biológicas, entre outras, pode haver a prova feita através do reconhecimento facial, mas que esta não pode ser tomada como verdade absoluta. Para tanto, é preciso melhorar as legislações que envolvem o tema.

A população precisa ficar atenta ao caminhar das tecnologias de reconhecimento facial e compreender que não há solução mágica para os problemas sociais que são enfrentados há anos. Essa tecnologia não vem para erradicar qualquer tipo de criminalidade ou prática indevida dentro da sociedade, apesar de ter essa aparente proposta. Muito pelo contrário: se não for bem usada, ela pode gerar conflitos e violações de direitos sociais básicos, prejudicando ainda mais a população e violando o Estado de Direito Constitucional.

REFERÊNCIAS

ABRAMOVAY, Ricardo. Como enfrentar a Era da Vigilância Total**. Outras Palavras**, 17 dez. 2019. Disponível em: https://outraspalavras.net/tecnologiaemdisputa/como-enfrentar-era-da-vigilancia-total/. Acesso em: 18 fev. 2020.

AMPARO, Thiago. Polícia algorítmica**. Folha de São Paulo**, São Paulo, 2020. Disponível em: https://www1.folha.uol.com.br/colunas/thiago-amparo/2020/01/policia-algoritmica.shtml. Acesso em: 17 fev. 2020.

AMORIM, Eduardo; RAMIRO, André. Recife anuncia rastreamento de cidadãos com câmera em ônibus. **Carta Capital**, 8 nov. 2018. Disponível em: https://www.cartacapital.com.br/blogs/intervozes/recife-anuncia-rastreamento-de-cidadaos-com-camera-em-onibus-1/ Acesso em: 03 maio 2020.

ARBULU, Rafael. Microsoft recusou oferta em reconhecimento facial em favor dos direitos humanos. **Canaltech**, 17 abr. 2019. 2019a. Disponível em: https://canaltech.com.br/inteligencia-artificial/microsoft-recusou-oferta-em-reconhecimento-facial-em-favor-dos-direitos-humanos-137385/. Acesso em: 19 fev. 2020.

_____. Mulher é detida por engano após erro em sistema de reconhecimento facial do RJ**. Canaltech**, 10 jul. 2019. 2019b. Disponível em: https://canaltech.com.br/governo/mulher-e-detida-por-engano-apos-erro-em-sistema-de-reconhecimento-facial-no-rj-143761/. Acesso em: 9 fev. 2020.

BARBON, Júlia. 151 pessoas são presas por reconhecimento facial no país; 90% são negras. **Folha de São Paulo**, São Paulo, 22 nov. 2019. Disponível em: https://www1.folha.uol.com.br/cotidiano/2019/11/151-pessoas-sao-presas-por-reconhecimento-facial-no-pais-90-sao-negras.shtml. Acesso em: 17 jan. 2020.

BIANCHI, Paula. Witzel e Gringos Miram a sua Cabecinha**. The Intercept Brasil,** 27 jan. 2020. Disponível em: https://theintercept.com/2020/01/27/witzel-gringos-miram-sua-cabecinha/. Acesso: em 9 fev. 2020.

BONFÁ, Cizenando Morello. **Um sistema de reconhecimento facial em vídeo baseado em uma implantação Multithread do algoritmo TLD**. 2013. 102 f. Dissertação (Mestrado em Engenharia Elétrica) - Pontifícia Universidade Católica do Rio de Janeiro. Rio de Janeiro. 2013. Disponível em: http://www2.dbd.puc-rio.br/pergamum/tesesabertas/1112771_2013_completo.pdf. Acesso em: 01 abr. 2020.

BUOLAMWINI, Joy; GEBRU, Timnit. Transparency Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. **Conference on Fairness, Accountability, and Transparency.** Proceedings of Machine Learning Research 81:1–15, 2018. Disponível em: http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf. Acesso em: 31 maio 2020.

BUZAN, Barry; HANSEN, Lene. **The Evolution of International Security Studies**. Cambridge, Reino Unido: Cambridge University Press, 2009.

CANTO, Mariana. **Made in Surveillance: A regulação da importação e do uso de tecnologias de vigilância estrangeiras e a relativização dos direitos fundamentais e da soberania estatal.** VI Simpósio Internacional LAVITS, 2019. Disponível em: http://lavits.org/wp-content/uploads/2019/12/Canto-2019-LAVITS.pdf. Acesso em: 09 fev. 2020.

COALIZÃO DIREITOS NA REDE. **Alerta! Novas propostas de lei visam aumentar o vigilantismo no Brasil.** 18 nov. 2019. Disponível em: https://direitosnarede.org.br/2019/11/18/novas-propostas-lei-vigilantismo-brasil.html. Acesso em: 18 fev. 2020.

DENT, Steve. Amazon shareholders will vote to ban facial recognition**. Engadget,** 15 abr. 2019. Disponível em: https://www.engadget.com/2019/04/15/amazon-shareholder-vote-facial-recognition/?guccounter=1. Acesso em: 16 jan. 2020.

DO BRASIL, Cristina Indio. Rio: programa de reconhecimento facial entra em operação no carnaval**. Agência Brasil**, 27 jan. 2019. Disponível em: http://agenciabrasil.ebc.com.br/geral/noticia/2019-01/rio-programa-de-reconhecimento-facial-entra-em-operacao-no-carnaval. Acesso em: 20 fev. 2020.

DOLZAN, Marcio. Arenas da Copa América terão reconhecimento facial para identificar torcedores**. Estadão**, 25 abr. 2019. Disponível em: https://esportes.estadao.com.br/noticias/futebol,arenas-da-copa-america-terao-reconhecimento-facial-para-identificar-torcedores,70002803975. Acesso em: 09 fev. 2020.

DREYER, Stephan; SCHULZ, Wolfgang. **Was bringt die Datenschutz-Grundverordnung für automatisierte Entscheidungssysteme?** Potenziale und Grenzen der Absicherung individueller, gruppenbezogener und gesellschaftlicher Interessen. Bertelsmann Stiftung, april 2018. Disponível em: https://www.hans-bredow-institut.de/uploads/media/Publikationen/cms/media/p4ymg73_BSt_DSGVOundADM_dt.pdf. Acesso em: 31 maio 2020.

ENGLAND, Rachel. Microsoft discreetly wiped its massive facial recognition database. **Engadget**, 6 jun. 2019. 2019a. Disponível em: https://www.engadget.com/2019/06/06/microsoft-discreetly-wiped-its-massive-facial-recognition-databa/?guccounter=1. Acesso em: 17 jan. 2020.

_____. UK police's facial recognition system has an 81 percent error rate**. Engadget**, 04 jul. 2019. 2019b. Disponível em: https://www.engadget.com/2019/07/04/uk-met-facial-recognition-failure-rate/. Acesso em: 11 fev. 2020.

FEITOSA JÚNIOR, Alessandro. Algoritmos de reconhecimento facial são enviesados, diz órgão dos EUA. **Gizmodo Brasil,** 20 dez. 2019. Disponível em: https://gizmodo.uol.com.br/reconhecimento-facial-enviesados-estudo-eua/. Acesso em: 11 fev. 2020.

GARVIE, Clare; BEDOYA, Alvaro M.; FRANKLE, Jonathan. **The Perpetual Line-Up:** Unredulated Police Face Recognition in America. 2019. Disponível em:

https://www.perpetuallineup.org/sites/default/files/2016-12/The%20Perpetual%20Line-Up%20-20Center%20on%20Privacy%20and%20Technology%20at%20Georgetown%20Law%20-%20121616.pdf. Acesso em: 10 jan. 2020.

GROTHER, Patrick; NGAN, Mei; HANAOKA, Kayee. **Face Recognition Vendor Test (FRVT):** Part 3: Demographic Effects**.** 2019. Disponível em: https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf. Acesso em: 11 fev. 2020.

INSTITUTO IGARAPÉ. **Videomonitoramento Webreport**. 2019. Disponível em: https://igarape.org.br/videomonitoramento-webreport/. Acesso em: 04 maio 2020.

INTERVOZES. Reconhecimento facial no Carnaval: riscos tecnológicos nada divertidos**. Carta Capital**, 14 mar. 2019. Disponível em: https://www.cartacapital.com.br/blogs/intervozes/reconhecimento-facial-no-carnaval-riscos-tecnologicos-nada-divertidos/. Acesso em: 09 fev. 2020.

KAYYALI, Dia. As Olimpíadas estão transformando o Rio em um Estado de vigilância e repressão. **Vice,** 13 jun. 2016. Disponível em: https://www.vice.com/pt_br/article/ezbj9w/as-olimpiadas-estao-transformando-o-rio-em-um-estado-de-vigilancia. Acesso em: 09 fev. 2020.

LOCKLEAR, Mallory. Google pledges to hold off on selling facial recognition technology**. Engadget,** 13 dez. 2018. Disponível em: https://www.engadget.com/2018/12/13/google-hold-off-selling-facial-recognition-technology/?guccounter=1. Acesso em: 16 jan. 2020.

MAIA, Pedro. The Usage and Dangers of Facial Recognition Technology**. Impakter**, 12 de setembro de 2019. Disponível em: https://impakter.com/the-usage-and-dangers-of-facial-recognition-technology/. Acesso em: 18 fev. 2020.

MANTHROPE, Rowland; MARTIN, Alexander J. 81% of Suspects Flagged by Met's Police Facial Recognition Technology Innocent, Independent Report Says**. Sky news,** 4 jul. 2019. Disponível em: https://news.sky.com/story/met-polices-facial-recognition-tech-has-81-error-rate-independent-report-says-11755941. Acesso em: 11 fev. 2020.

METZ, Rachel. Beyond San Francisco, more cities are saying no to facial recognition**. Cable News Network**, 17 jul. 2019. Disponível em: https://edition.cnn.com/2019/07/17/tech/cities-ban-facial-recognition/index.html. Acesso em: 18 de fev. 2020.

NUNES, Pablo. Exclusivo: levantamento revela que 90,5% dos presos por monitoramento facial no Brasil são negros**. The Intercept Brasil**, 21 nov. 2019. Disponível em: https://theintercept.com/2019/11/21/presos-monitoramento-facial-brasil-negros/. Acesso em: 18 de fev. 2020.

PAULUZE, Thaiza. Carnaval de SP vai ter sistema de reconhecimento facial para identificar suspeitos. **Folha de São Paulo,** São Paulo, jan. 2020. Disponível em: https://www1.folha.uol.com.br/cotidiano/2020/01/carnaval-de-sp-vai-ter-sistema-de-reconhecimento-facial-para-identificar-suspeitos.shtml. Acesso em: 16 jan. 2020.

PREFEITURA DO RIO DE JANEIRO. **Centro de Operações Rio chega para integrar 30 órgãos municipais.** Prefeitura do Rio de Janeiro, Rio de Janeiro, 30 de dezembro de 2010. Disponível em: http://www.rio.rj.gov.br/web/guest/exibeconteudo?article-id=1419835. Acesso em: 09 fev. 2020.

PROJECT OF GOVERNMENT OVERSIGHT. **Facing the Future of Surveillance.** 2019. Disponível em: https://www.pogo.org/report/2019/03/facing-the-future-of-surveillance/. Acesso em: 11 fev. 2020.

SILVA, Rosane Leal da; SILVA, Fernanda dos Santos Rodrigues da. Reconhecimento Facial e Segurança Pública: os perigos do uso da tecnologia no sistema penal seletivo brasileiro. *In:* 5º CONGRESSO INTERNACIONAL DE DIREITO E CONTEMPORANEIDADE, 2019, Santa Maria. **Anais** [...]. Disponível em: https://www.ufsm.br/cursos/pos-graduacao/santa-maria/ppgd/wp-content/uploads/sites/563/2019/09/5.23.pdf&sa=D&ust=1590802537960000&usg=AFQjCNGgQE7Gf9i481NNjB69iHD2S8U9jA. Acesso em: 31 maio 2020.

SILVA, Tarcizio. Linha do Tempo do Racismo Algorítmico. **Blog do Tarcízio Silva**, 2019. Disponível em: https://tarciziosilva.com.br/blog/posts/racismo-algoritmico-linha-do-tempo. Acesso em: 18 fev. 2020.

SPANHOL, Fernando José; LUNARDI, Giovani Mendonça; SOUZA, Márcio Vieira de (Org.). **Tecnologias da informação e comunicação na segurança pública e direitos humanos**. São Paulo: Blucher, 2016. 206 p.

THE NEW YORK TIMES. I.B.M takes “Smart Cities” Concept to Rio de Janeiro**. The New York Times,** Nova York, 03 mar. 2012. Disponível em: https://www.nytimes.com/2012/03/04/business/ibm-takes-smarter-cities-concept-to-rio-de-janeiro.html?_r=0. Acesso em: 9 fev. 2020.

UNITED NATIONS GENERAL ASSEMBLY. **A/RES/68/167. The right to privacy in the digital age**. Resolução adotada pela Assembleia Geral das Nações Unidas em 18 dez. 2013. 2013. Disponível em: https://undocs.org/A/RES/68/167. Acesso em: 20 fev. 2020.

_____. **A/RES/69/166. The right to privacy in the digital age.** Resolução adotada pela Assembleia Geral das Nações Unidas em 18 dez. 2014. 2014. Disponível em: https://undocs.org/en/A/RES/69/166. Acesso em: 20 fev. 2020.

UNITED NATIONS HUMAN RIGHTS OFFICE OF THE HIGH COMMISSIONER. **Making a Difference:** An Introduction to Human Rights. 2018. Disponível em: https://europe.ohchr.org/Documents/Publications/MakeADifference_EN.pdf. Acesso em: 31 maio 2020.

_____. **Guiding principles on business and human rights.** 2011. Disponível em: https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf. Acesso em: 31 maio 2020.

VIANA, Cleiton Correia; CONCEIÇÃO, Valdir Silva da; ROCHA, Angela Machado. Reconhecimento facial e a relativização do direito de imagem. **Revista Ingi,** vol. 3, n. 3**.** 2019. Pp. 436-450. ISSN: 2594-8288.

USE OF FACIAL ELECTRONIC RECOGNITION BY COMPANIES FOR IDENTIFICATION OF SUSPECTS: SECURITY OR VIOLATION OF THE DEMOCRATIC STATE OF LAW?

ABSTRACT

The following article pursuit the analysis of the use of electronic facial recognition by the public and private companies as a human rights violating tool, especially when used to identify suspected and criminal offenses. Therefore, it is common for these monitoring systems to be susceptible to situations of false positives, mistakenly identifying people who have similar physical characteristics, making security operators believe that these people are to blame for others actions. Many countries have been reducing or limiting the use of these technologies, however, Brazil is going on the opposite direction of it. The research methodology of this work is bibliographic, with consultations to newspaper articles, scientific articles, and national and international documents. The result obtained is that electronic facial recognition, even though it seems beneficial, potentiates situations of prejudice and inequality that endangers historically marginalized portions of the population.

Keywords: Facial recognition. Criminology. Companies. Human rights.