UNIVERSIDADE DO SUL DE SANTA CATARINA
ISRAEL SARAIVA ALVES

RECONHECIMENTO FACIAL NO AUXÍLIO À SEGURANÇA PÚBLICA NA CIDADE DE FLORIANÓPOLIS

Florianópolis
2020

ISRAEL SARAIVA ALVES

RECONHECIMENTO FACIAL NO AUXÍLIO À SEGURANÇA PÚBLICA NA CIDADE DE FLORIANÓPOLIS

Trabalho de Conclusão de Curso apresentado ao Curso de Especialização em Inteligência de Segurança da Universidade do Sul de Santa Catarina como requisito à obtenção do título de Especialista em Inteligência de Segurança.

Orientador: Prof. Camel André de Godoy Farah, Dr.

Florianópolis

2020

ISRAEL SARAIVA ALVES

RECONHECIMENTO FACIAL NO AUXÍLIO À SEGURANÇA PÚBLICA NA CIDADE DE FLORIANÓPOLIS

Este Trabalho de Conclusão de Curso foi julgado adequado à obtenção do título de Especialista em Inteligência de Segurança e aprovada em sua forma final pelo Curso de Especialização em Inteligência de Segurança da Universidade do Sul de Santa Catarina.

Florianópolis, 19 de junho de 2020

_____

Professor e orientador Camel André de Godoy Farah, Dr.
Universidade do Sul de Santa Catarina

_____

Professor José Luiz Gonçalves da Silveira, Dr.
Universidade do Sul de Santa Catarina

A todos os Soldados do silêncio.

AGRADECIMENTOS

Ao grande Arquiteto do Universo que permitiu mais uma etapa na evolução continuada através de Docentes colocados à disposição dos que se permitem aprender. Aos Professores e a Instituição que conduzem o aluno ao aperfeiçoamento.

“A verdadeira viagem de descobrimento não consiste em procurar novas paisagens, mas de ter novos olhos.” (Marcel Proust, 1913).

RESUMO

A cidade de Florianópolis possui estruturado centro de videomonitoramento apoiando a Segurança Pública. Implantar um software de biometria facial ao atual sistema, subsidiado com informações a partir de um Banco de Dados, pode auxiliar a Segurança Pública na detecção de foragidos e desaparecidos. A pesquisa teve como objetivo principal demonstrar o auxílio do reconhecimento facial à Segurança Pública em Florianópolis, uma vez que, implantado em outras cidades apresenta eficiência com bons resultados alcançados. Nos objetivos específicos foram abordados os temas legais no que diz respeito à Lei Geral de Proteção de Dados Pessoais bem como a compilação de Banco de Dados e critérios para local de monitoramento. Informações atualizadas até junho de 2019 pelo Conselho Nacional de Justiça demonstram que até a citada data havia mais de 300 mil mandados de prisão em aberto no Brasil, e que tais pessoas deambulam pelos centros urbanos no anonimato. A utilização da tecnologia de reconhecimento em tais casos viria a colaborar na detecção e intervenção pontual por parte do Agente de Segurança. O uso deve harmonizar com a Lei Geral de proteção do Dado Pessoal ainda que, no texto, haja previsão legal para o emprego nas questões de segurança. A pesquisa foi realizada utilizando o método quantitativo, pois apresenta números e dados concretos. No tocante a Legislação referente a Dados Pessoais, a SSP/SC promoveu o conhecimento e disseminação da mesma através de palestra e seminário promovendo um ambiente de uso responsável. A implantação definitiva de software com biometria facial deve necessariamente ser testada no local de operação, pois a miscigenação da população é fator determinante nos resultados. O sistema de reconhecimento necessita de um Banco de Dados a ser consultado e que pode ser compilado a partir de informações da carteira nacional de habilitação ou identidade, conforme outras cidades já utilizam. Florianópolis possui os requisitos para operar a biometria em auxilio à Segurança Pública.

Palavras-chave: Segurança Pública. Reconhecimento facial. Tecnologia para monitoramento eletrônico. Inteligência de imagens.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS

ABIN - Agência Brasileira de Inteligência

ADABOOST - Algoritmo clássico de aprendizagem

AFIS - Automated Fingerprint Identification System

ANDP - Autoridade Nacional de Proteção de Dados

BNMP - Banco Nacional de Monitoramento de Prisões

CNJ - Conselho Nacional de Justiça

DTIC - Diretoria de Tecnologia da Informação e Comunicações

EUA - Estados Unidos da América

FBI - Federal Bureau of Investigation

FUVEST - Fundação Universitária para o Vestibular

ICE - Serviço de Imigração e Alfândega

IDEC - Instituto de Defesa do Consumidor

LGPD - Lei Geral de Proteção de Dados

OVERFACE - Biblioteca de aprendizagem de máquina – sobre o rosto

PCA - Análise de Componentes Principais

RGPD - Regulamento Geral de Proteção de Dados

RNAs - Redes Neurais Artificiais

RNC - Rede neural cerebral

SNC - Sistema nervoso central

SSP - Secretaria de Segurança Pública

SSP/SC - Secretaria de Segurança Pública do Estado de Santa Catarina

SUMÁRIO

1 INTRODUÇÃO

Reconhecer uma forma através da visão associando a um nome é o que se aprende desde tenra infância, assim se dá nome a objetos e pessoas.

Reconhecer pessoas e autenticá-las como pai, mãe, irmãos é um processo de aprendizado. Tal autenticação nasce de uma forma natural, assim pessoas interagem se reconhecendo mutuamente sem esforço em total normalidade de ação no cotidiano.

Ao caminhar por uma movimentada alameda o indivíduo inserido na multidão passa a situação de anonimato social. Várias fisionomias e rostos com diversas características singulares cruzam uns pelos outros sem que haja autenticação, afinal não estão no banco de dados pessoal.

Através dos olhos as imagens são captadas, mas o reconhecimento se dá somente quando, através da sinapse, o dado é levado ao cérebro, processado e autenticado com informação já gravada. Neste caso, o banco de dados foi consultado e sinalizou positivo, fez o reconhecimento encontrando um conhecido em meio a várias outras pessoas que não apresentavam as características armazenadas.

Assim como um rosto conhecido é encontrado deambulando no anônimo social, pessoas que não querem ser reconhecidas utilizam do anonimato da multidão como uma ferramenta útil para não serem identificadas. Os motivos são pessoais, mas algumas possuem algum tipo de pendência junto à sociedade.

No Brasil há vários mandados de prisão em aberto, pessoas com pendências judiciais, pessoas com restrições ao convívio social ou que simplesmente fazem parte do rol de pessoas desaparecidas. Estas caminham por centros urbanos sem que sejam identificadas como tal, utilizando o anonimato social.

Uma ferramenta de auxílio para que fossem autenticadas pela Segurança Pública é a utilização de software de reconhecimento facial. Este pode ser adicionado a uma existente rede de câmeras de monitoramento já instaladas nos diversos centros urbanos e áreas de circulação.

O presente trabalho tem como objetivo principal trazer à luz o tema do reconhecimento facial no auxílio à segurança pública na cidade de Florianópolis, que pode ser viável. Para atingir o objetivo a pesquisa foi realizada utilizando o método quantitativo.

Os objetivos específicos abordarão a respeito da legalidade do uso de dado pessoal, qual a regulamentação jurídica, bem como o indicativo para que uma área seja monitorada pela Secretaria de Segurança Pública. Será abordado, ainda, como pode ser alimentado um Banco de Dados para o melhor desempenho do software testado para tal finalidade.

No primeiro momento são apresentados sistemas e seus algoritmos, do reconhecimento de padrão passando pelo aprendizado de máquina, inteligência artificial, seguindo para exemplos do uso da tecnologia em alguns países e findando no monitoramento em Florianópolis.

Na segunda parte do trabalho é apresentada qual a origem da informação do Banco de Dados bem como a importância da qualidade das imagens para o reconhecimento, tanto a detectada como a arquivada para consulta.

No terceiro momento é abordado sobre a consolidação de um único Banco de Dados na intenção de potencializar a utilização da tecnologia.

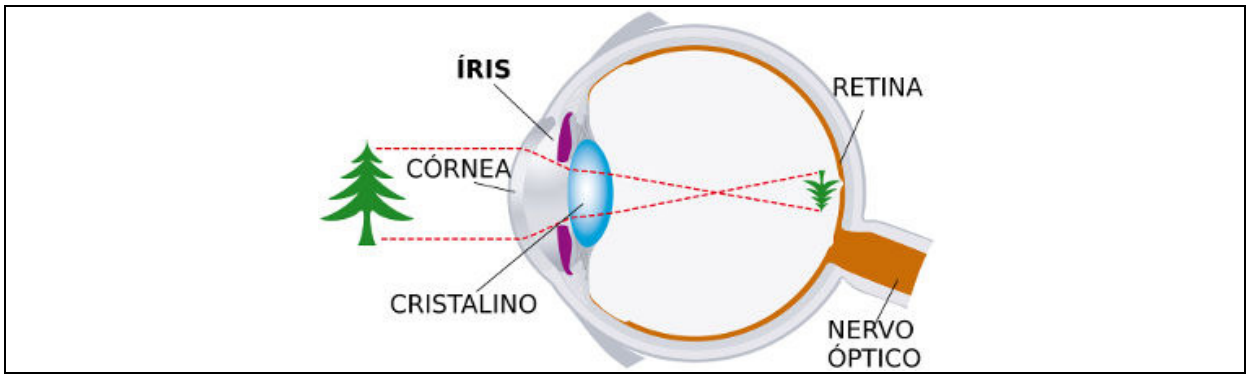
Na quarta parte será tratado sobre como a legislação Internacional pondera o assunto da Proteção de Dados Pessoais, bem como qual o posicionamento do Brasil e alguns Órgãos internos em relação à questão da regulamentação.

A quinta parte versa sobre o videomonitoramento em Santa Catarina com a utilização do Sistema Bem-Te-Vi. Também foi abordado sobre os Centros Integrados de Comando e Controle e as benesses da implantação do sistema de reconhecimento facial à Segurança Pública.

2 SISTEMA DE RECONHECIMENTO DE PADRÕES

O sistema de reconhecimento faz parte do cotidiano e o olho humano é a ferramenta que possibilita captar imagens. A visão é utilizada com pouco esforço por se tratar de uma percepção natural e é através dela que a representação chega ao cérebro, transmitida pelo nervo óptico, para processamento e decisão. Abaixo, esquema representativo do olho humano.

Figura 1 – Anatomia do olho



Fonte: Santos, 2020.

Reconhecer o que é uma árvore se dá a partir de um padrão ensinado de objeto ao qual se denomina árvore. Assim é feito o reconhecimento de coisas e pessoas que naturalmente se reconhece após vinculo do objeto ao nome.

Na imitação do corpo humano e por uma necessidade criada a partir da evolução da sociedade como um todo, na década de 1970 foi criado o primeiro sistema de reconhecimento facial, segundo (PONTES, 2013 *apud* KANADE 1973, p. 5).

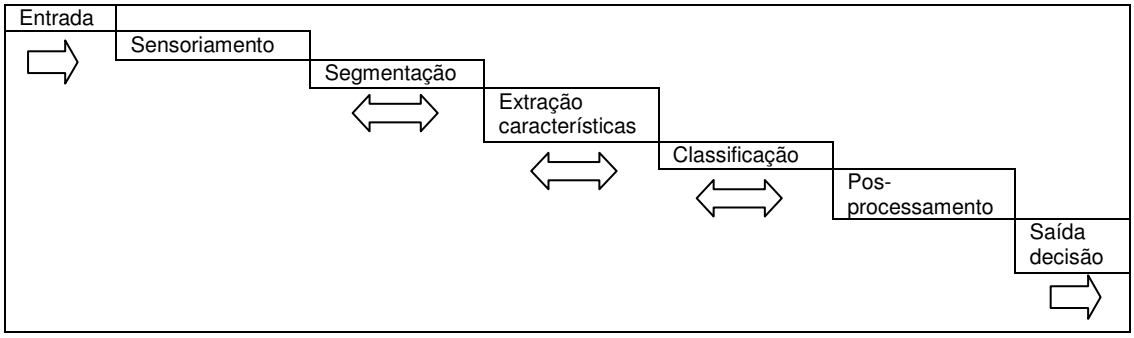
Tal qual o corpo humano necessita de aprender a partir de padrões predeterminados, os sistemas de reconhecimento também evoluíram a partir de princípios semelhantes. Conforme (ARAUJO, 2010 *apud* DUDA, 2000, p. 4).

> O Reconhecimento de Padrões faz parte da área de Aprendizado de Máquina, e seu objetivo é separar objetos (ou padrões) em categorias (ou classes). Os objetos podem ser qualquer conjunto de medidas que necessite ser classificado, como por exemplo, os pixeis de uma imagem[1].

[1] (ARAUJO, 2010 *apud* Duda, 2000 p. 4). Algoritmo para reconhecimento de características faciais baseado em filtros de correlação. 2010. Tese (Mestrado em Engenharia Elétrica) – Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2010.

Um reconhecimento de padrões se norteia nas etapas abaixo, conforme figura, sendo que não é um ciclo unidirecional, exceto pela entrada e saída, podendo sofrer a retroalimentação do dado.

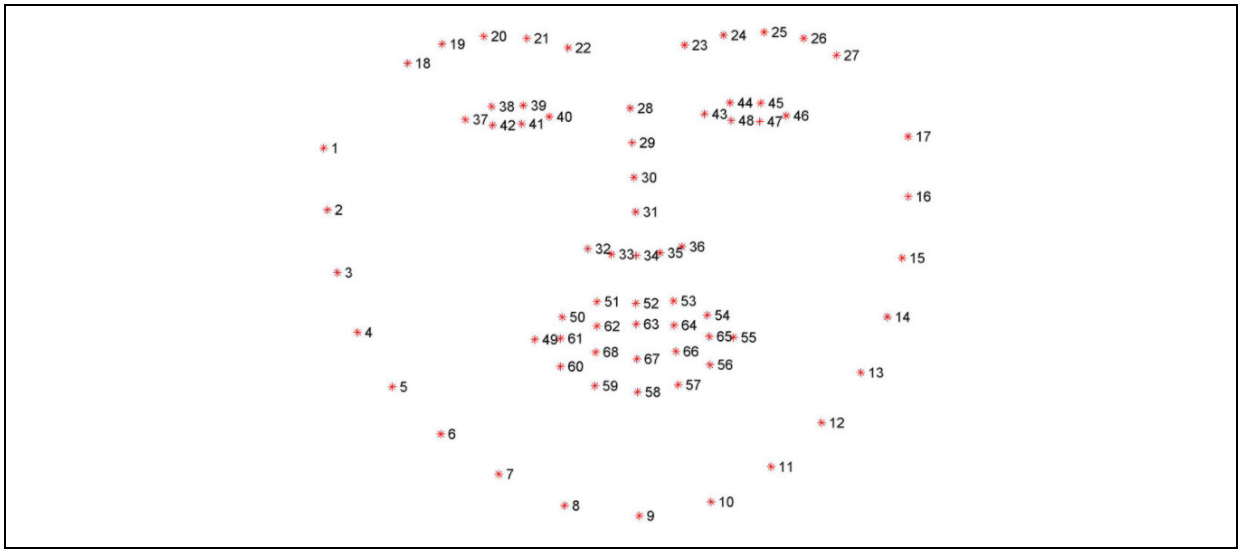
Figura 2 – Etapas de um reconhecimento de padrão



Fonte: Elaborado pelo autor, 2020.

O reconhecimento de padrão leva em conta o número de pontos fiduciais, que são pontos de controle sobre um objeto que definem regiões e características necessárias a detecção, sendo diretamente proporcional o acerto ao número de pontos determinados e inversamente proporcionais ao tempo resposta de máquina.

Figura 3 – Pontos fiduciais



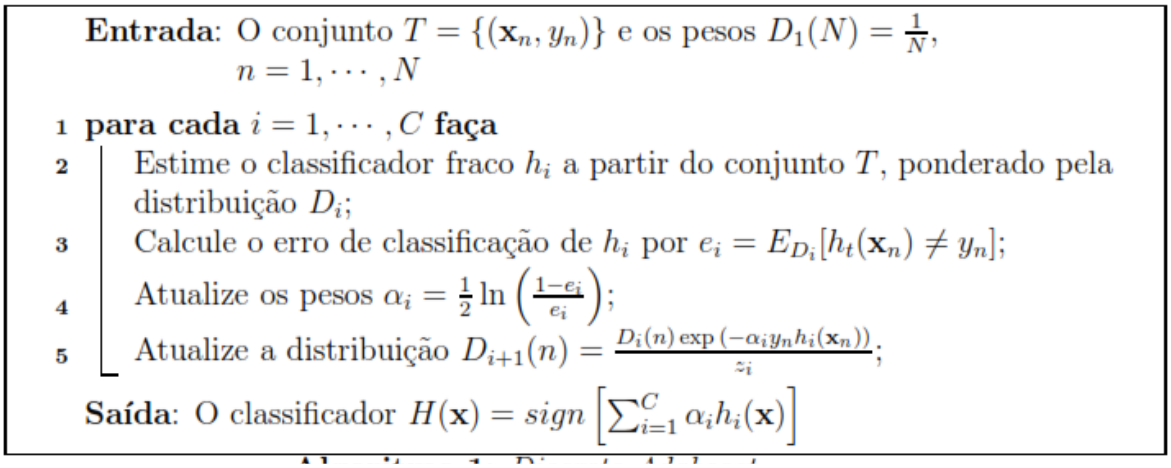
Fonte: TERUEL, imagem adaptada de Sagonas, 2013.

2.1 MÉTODO CLÁSSICO DE APRENDIZAGEM DA MÁQUINA ADABOOST

Existem diversos métodos de classificação de padrões, tais como Linear Fisher, Support Vectors e outros. Aqui será apresentado um dos métodos de aprendizagem de classificadores clássicos, o AdaBoost.

Cada método de aprendizagem de máquina proporciona suas particularidades, mas todos apresentam o mesmo objetivo final que é ensinar a máquina a pensar, considerando variantes distintas. Para elucidar o trabalho das diversas variações de Boosting que em linguagem de máquina tem função de impulsionar um algoritmo de aprendizado de máquina convertendo vários fracos em um resultado forte, a mais utilizada é o AdaBoost. Afirma Araujo (2010 *apud* FREUND, 1995, p.11) tendo sua forma original também conhecida como Discrete AdaBoost ou Adaptive Boosting, conforme abaixo:

Figura 4 – Algoritmo Discrete Adaboost



Fonte: Araujo, 2010.

O Adaptive Boosting também conhecido como Discrete AdaBoost tem por base a ideia principal de criar um classificador forte a partir de vários classificadores fracos, conforme (ARAUJO, 2010 *apud* FREUND, Y., SCHAPIRE, R. R,1997, p. 9).

> Algumas técnicas de combinação de classificadores utilizam versões reamostradas do conjunto de treino no aprendizado dos classificadores constituintes. Uma técnica bastante utilizada e com muitas variações é o *Boosting*. A ideia é que é possível gerar um classificador forte (*Strong Learner* ou *S-*

> *trong Classifier*), a partir de um conjunto de classificadores fracos (*Weak Learners* ou *Weak Classifiers*)[2].

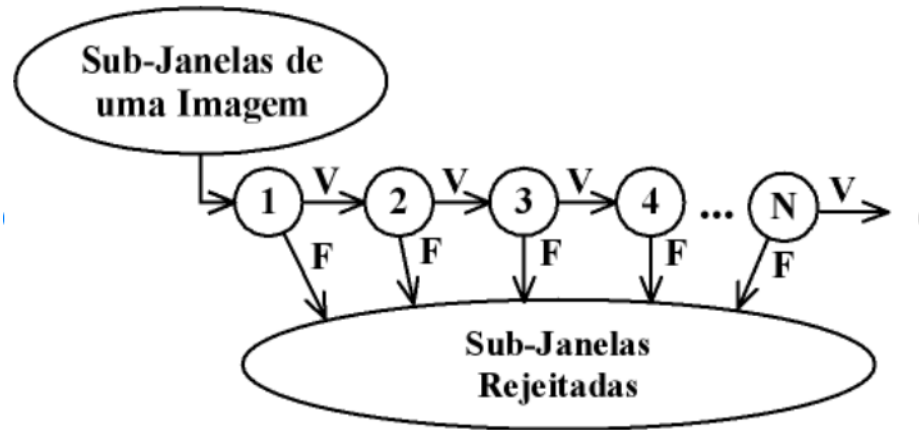
Para potencializar a leitura de um classificador como algoritmo final a utilização de subgrupos de classificadores deu origem aos sistemas baseados em cascata de classificadores. Cada algoritmo classificador faz determinada tarefa não encerrando o processo, mas sim encaminhando para um próximo algoritmo variante que terá outra tarefa específica. Em efeito cascata se chega a um algoritmo forte.

2.2 SISTEMAS E ALGORITMOS ATUALMENTE UTILIZADOS

Detecção é uma etapa inicial em muitos sistemas incluindo os de reconhecimento de características faciais. Existem diversos métodos acoplados a sistemas para empregar para tal tarefa, mas basicamente subdividem em dois grandes grupos: Sistemas baseados em modelos ativos e os Sistemas baseados em cascata de classificadores. A pesquisa focou no Sistema baseado em cascata.

Abaixo, segue representação esquemática do Sistema baseado em cascada de classificadores:

Figura 5 – Cascata de classificadores



-Cascata de Classificadores O algoritmo consiste na construção de uma cascata de classificadores. O bloco 1 representa o classificador mais simples. A complexidade dos classificadores vai aumentando até ao classificador final (bloco N), onde é confirmada a presença de uma face numa sub-janela da imagem a avaliar. Cada etapa da cascata é constituída por um classificador treinado pelo algoritmo AdaBoost (Adaptive Boosting). O treino do algoritmo de aprendizagem é acelerado pela acção do AdaBoost,

Fonte: Jesus, 2018.

[2] (ARAUJO, 2010 *apud* FREUND, Y., SCHAPIRE, R. R,1997, p. 9).

Seguindo a linha de cascata de classificadores, utilizando uma versão do AdaBoost chamada de Gentle AdaBoost se chega ao algoritmo Viola-Jones, que face sua precisão e plasticidade vêm sendo muito empregado nos sistemas de reconhecimento. O Viola-Jones, conforme Rouhani (2019) vem sendo empregado por apresentar alta precisão na leitura de faces e baixa taxa de falsos positivos, ademais com baixo custo computacional.

Segundo Rouhani (2019), o algoritmo é composto de três partes distintas utilizando classificadores Boosting garantindo o bom desempenho e velocidade de processamento.

A tecnologia do reconhecimento facial está sendo utilizado de várias formas e em diversos segmentos da sociedade, impulsionado pelo aprimoramento dos sistemas operacionais e novos algoritmos que apresentam resultados fidedignos. O exemplo é o uso da tecnologia em aparelhos celulares, ou como senhas pessoais de bancos, ainda, como chave de acesso à residência. A popularização do uso se dá pela simples facilidade de aplicação e segurança proporcionada.

Segundo o artigo sobre reconhecimento facial, publicado por Silveira (2018), onde foi utilizado um software que utiliza o algoritmo de reconhecimento facial Eigenface em um aplicativo Android e recursos da biblioteca OpenCV:

> Para a implementação do software, a linguagem JAVA foi utilizada com a distribuição Android API 21 do pacote Software Development Kit (SDK), usando o Integrated Development Environment (IDE). Foram realizados testes de desempenho, relatando o potencial da biblioteca OpenCV para o reconhecimento facial, de modo auxiliar toda a comunidade científica no uso desse algoritmo no campo da biometria[3].

Demonstrado o potencial para o reconhecimento facial de tal algoritmo, ele é aberto a toda comunidade científica gratuitamente a título de auxílio comum, o que facilita a popularização e avanço da tecnologia.

Atrás dos resultados obtidos, da simplicidade de uso, a construção de sistemas automáticos de reconhecimento facial é uma tarefa complexa e com problemas reais, sendo o mais específico a segmentação, que segundo Marengoni (2009) em visão computacional é o processo de dividir uma imagem digital em múltiplas regiões. O objetivo é a simplificação da imagem para facilitar a análise.

[3] SILVEIRA, Jheime ,Santos da., SÁ Abreu, Angela de. Reconhecimento Facial Usando o algoritmo Autenticação da biblioteca Open CV.

A grande quantidade de informação que o software recorre para que aconteça o reconhecimento facial pela máquina foi amenizado utilizando imagens captadas em ambientes controlados. Persistiu o problema para a captação em ambientes não controlados e a solução apontada foi utilização de filtros de abstração que constitu-em uma forma moderna de simplificação da imagem e permite remover informação desnecessária do objetivo.

Um estudo feito por Pontes (2013, p. 70), tese de mestrado, utilizando as bi-bliotecas de imagens Labelled Faces in the Wild, Closed-set identification e Image Retrieval, com utilização de nove cadeias de pré-processamento de imagens conclu-iu que:

> As avaliações efetuadas permitem concluir que a etapa de pré-processamento que permite um maior aumento no número de indivíduos corretamente reconhecidos é a deteção e segmentação das faces presentes numa imagem. Através da comparação do desempenho das galerias Original, Cropped e Masked é ainda possível concluir que a segmentação produz um maior impacto no algoritmo LBPH, seguido pelo algoritmo Fisherfaces e em último lugar pelo algoritmo Eigenfaces[4].

Face ao exposto, a fase de pré-processamento utilizando a segmentação por parte do algoritmo é a melhor fórmula para a obtenção de resultados positivos.

Conforme análise em um estudo na Universidade Federal do Semi-Árido, pu-blicado na revista brasileira de computação aplicada em 2012, a utilização do algo-ritmo de Análise de Componentes Principais (PCA) apresentou o melhor resultado de desempenho.

> Embora diferentes todas as faces possuam características como, por exem-plo, uma boca, dois olhos e um nariz. No presente trabalho é proposto um sistema de reconhecimento facial desenvolvido em duas fases. Inicialmente utilizam-se as técnicas de Análise de Componentes Principais (PCA) e Ei-genfaces (autofaces) para a extração de características da face. Na segun-da fase foram aplicados os classificadores K-Nearest Neighbors (K-NN), Random Forest (Floresta Aleatória) e K-Star (K-estrela) no processo de re-conhecimento da face. A validação dos algoritmos foi realizada numa base de dados contendo 1280 imagens de 64 classes distintas. Finalmente, foi mostrado que o desempenho dos algoritmos testados para sistemas de re-conhecimentos de face baseado em PCA foram muito satisfatórios, atingin-do as melhores taxas de reconhecimento, acima de 90% em todos os classi-ficadores[5].

[4] PONTES, Pedro Tiago Carvalho da Silva. Visage - Impacto dos Filtros de Abstração no Reconhe cento Facial em Imagens. 2013.

[5] UFERSA. REDFACE: um sistema de reconhecimento facial baseado em técnicas de análise de-componentes principais e autofaces.

No tocante a análise conforme o tamanho da imagem e número de pixel baseado na técnica Eigenfaces e K-Nearest Neighbors, evidenciaram que imagens em dimensões de 12x9 pixels produzem a melhor taxa de precisão. Para tal, deve combinar a medida de distância euclidiana normalizada utilizando medidas de similaridade para valores contínuos e um número de Eigenfaces que é o nome dado a um conjunto de vetores próprios quando usado no problema de visão computacional do reconhecimento de rosto humano, igual a vinte.

Figura 6 – Distância Euclidiana

$$d = \sqrt{\sum_{k=1}^{n} (p_{ik} - p_{jk})^2}$$

Fonte: Jason, 2012.

Enfim, dos vários motores de reconhecimento facial, o que a maioria deles faz é medir as várias distâncias entre os vários pontos de um rosto; entre os olhos, do nariz ao queixo, canto do olho à ponta da orelha e outros mais. Todos esses dados são transformados em um código numérico de identificação e tais códigos são trafegados pela rede, armazenados em bancos de dados e efetivamente comparados pelos softwares. A quantidade de pontos analisados é variável. Vale ressaltar que tal quantidade de pontos implica na velocidade e precisão da resposta requerendo um sistema operacional com maior robustez para processar.

Cada sistema tem sua especificidade quanto ao método e leitura da captação dos pontos fiduciais, necessitando de mais ou menos dados para um bom resultado, gerando um código para cada face, ou seja, chave de leitura. Há sistema aberto à comunidade científica canalizando esforços e interesses na disseminação do conhecimento da área. Conforme parágrafo anterior, todos perseguem o objetivo a partir de um padrão conhecido como rosto humano, mas cada qual gera reconhecimento a partir de um código gerado que é reconhecido neste ou naquele sistema.

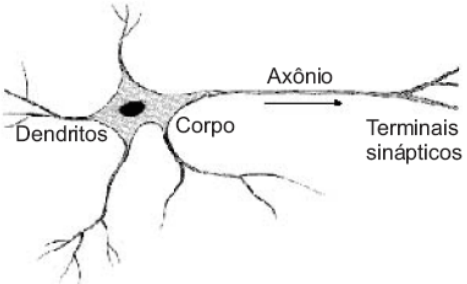
Uma vez que a expansão e utilização do reconhecimento através de biometria facial vêm sendo progressiva em face de simplicidade e segurança, acolher um sistema de algoritmos, que faça leituras de outros sistemas classificatórios, que possibi-

lite ler classificação de outros sistemas de algoritmos pode ser uma solução para compartilhar Banco de Dados.

2.3 REDES NEURAIS ARTIFICIAIS - VELOCIDADE DE RECONHECIMENTO.

As redes neurais artificiais (RNA) são inspiradas nas redes neurais cerebrais (RNC) do sistema nervoso central (SNC), sendo representadas através de códigos, modelos matemáticos. Abaixo a representação de um neurônio humano.

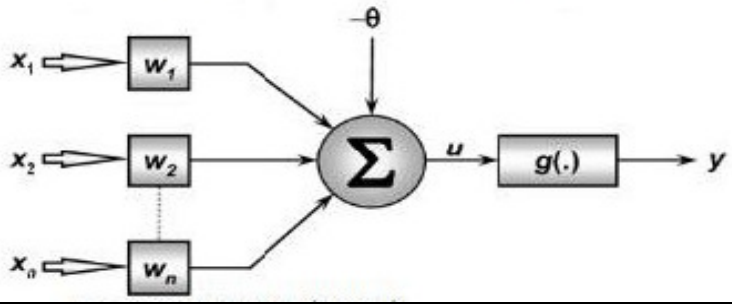
Figura 7 – Representação de um neurônio



Fonte: Ferneda, 2006.

Os neurônios se ligam uns aos outros formando uma rede de transmissão. A informação segue até ao orgão central, cérebro, onde são processados. Assim o neurônio artificial, tal qual o humano, se liga a outros para que ocorra a transmissão para então o processamento do dado fornecido ou captado. Segue esquema representativo de um neurônio artificial.

Figura 8 – Representação de um neurônio artificial



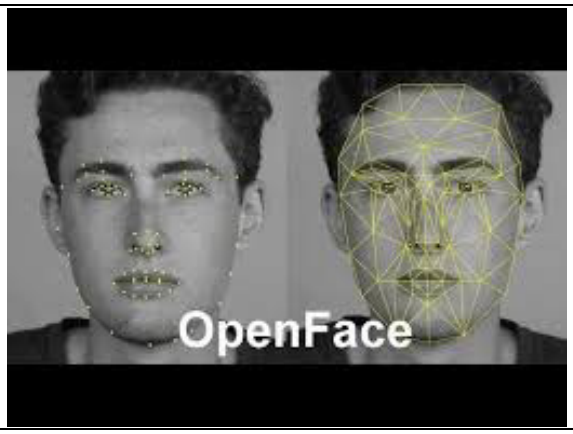
Fonte: Rouhani, 2019.

Assim como o ser humano passa pelo aprendizado, as RNAs necessitam do aprendizado de máquina, conforme o item 2.1, e em 2015 a Time Google Brain criou o TensorFlow que é uma biblioteca de aprendizado de máquina com código aberto sob a licença Apache 2.0.

O TensorFlow foi elaborado para o aprendizado de máquina, mas diferentemente de outros sistemas, este permanece com código aberto de extremidade a outra, permitindo o uso e o desenvolvimento para ser implantado em aplicativos. Trata-se de um Framework de redes neurais de aprendizado profundo, Deep Learning, e pode ser associado ao OpenFace ou seja, ao Banco de Dados para reconhecimento de faces. Ele tem aplicação na regularização do treinamento de uma rede neural artificial forçando o modelo algorítmico aprender previsões. Uma técnica genérica podendo ser utilizada em redes neurais como NNs de feed-forward, NNs convolucionais e NNs recorrentes.

Abaixo figura representativa do Open Face. Os pontos marcados ou pontos fiduciais são as marcas responsáveis para que se tenham distâncias determinantes possibilitando a geração de uma chave de leitura e a diferenciação de um indivíduo para outro.

Figura 9 – OpenFace



Fonte: Facial recognition, 2018.

A detecção de uma imagem, onde a captação é tomada a partir de ambiente não controlado, se torna fator de grande importância para o reconhecimento facial, pois a demanda, a velocidade de processamento pode ser maior ou menor em fun-

ção da qualidade. Imagens de ambientes não controlados aumentam a margem de erro gerando falsos positivos ou falsos negativos.

2.3.1 Videomonitoramento e o reconhecimento facial em alguns Países

Vários países estão utilizando a tecnologia visando melhor administração de seus centros urbanos e suas fronteiras em face de situações crescentes de violência e ações terroristas. Existem óbices a serem superados pela tecnologia do reconhecimento facial para que o uso remeta melhores resultados.

Abaixo, informações de como alguns países estão fazendo uso da tecnologia de biometria facial promovendo a autenticação, ou seja, reconhecimento, publicado no Portal brasileiro sobre identificação digital (2020).

> O Governo português quer criar um sistema de reconhecimento facial para usar a chave móvel digital, ferramenta que já permite aceder a vários serviços online do Estado, como o Portal das Finanças, a Segurança Social, e serviços do Sistema Nacional de Saúde. A tecnologia de reconhecimento facial vai muito além de ser uma alternativa à palavra-passe.
> Na China**,** os usos incluem autorizar o acesso a metros em Xangai e Pequim, e projetar imagens de peões a desrespeitar os sinais de trânsito em Shenzhen em ecrãs gigantes (juntamente com o nome e uma multa via SMS). Já os alunos de uma escola secundária em Hangzhou são filmados e avaliados quanto ao comportamento e estado emocional: a cada 30 segundos o programa registra se estão a escrever, ler, fazer perguntas ou a dormir e se parecem felizes, zangados, confundidos, aborrecidos ou com medo. O Japão usa a tecnologia para registrar o número de vezes que alguém entra em cassinos e casas de apostas.
> Emirados Árabes Unidos, um espaço rodeado de câmaras de reconhecimento facial no aeroporto do Dubai identifica as pessoas que passam – o sistema pode autorizá-las a entrar no país ou, alternativamente, alertar o pessoal de segurança.
> Singapura utiliza a tecnologia para encontrar pessoas idosas que podem estar perdidas. Reino Unido, a polícia londrina vai começar a testar um sistema de reconhecimento facial em lugares chave na cidade para encontrar criminosos[6].

A seu turno, os Estados Unidos utilizam o sistema panóptico como uma ferramenta nos aeroportos, indo do controle de vistos à detecção de ilegais passando pela seção de procurados.

Algumas cidades nos EUA utilizam o reconhecimento facial no auxílio à segurança pública, mas cabe ressaltar que pelos menos quatro delas proibiram o uso por parte da polícia local. A título de exemplo da medida, São Francisco, por meio da

[6] Cryptoid.com.br/identidade-digital-destaques/como-os-paises-usam-o-reconhecimento-facial.

Câmara Legislativa chegou ao entendimento que o reconhecimento através de biometria facial instalado na cidade não estava pronto para o uso devido ao grande número de falsos positivos. Ademais, foi alegado que as pessoas de tal centro urbano tampouco estão prontas para lidar com a tecnologia.

2.3.2 Videomonitoramento e o reconhecimento facial no Brasil

A pluralidade étnica da população brasileira, pela miscigenação, apresenta dificuldade particular em relação a outros países no quesito qual o sistema algorítmico a ser utilizado para biometria facial. Para minimizar o problema, antes da implantação do sistema de reconhecimento, a exemplo de Florianópolis, os sistemas estão sendo testados no local de aplicação até que as respostas que se esperam sejam atendidas.

Atenta às novas tecnologias e seu emprego, a Secretaria de Segurança Pública de Santa Catarina (SSP/SC) promoveu seminário elucidativo no tocante ao uso de informação pessoal em consonância com a Lei de proteção de dados, visto que a imagem é considerada dado pessoal de acordo com o já vigente Regulamento Geral de proteção de Dados, em seu Art. 9º, 1, da União Européia[7], e com o Art. 5º, II, da Lei Geral de Proteção de Dados[8], que entrará em vigor em agosto de 2020 no Brasil.

A utilização da tecnologia de reconhecimento facial no Brasil vem sendo empregada em várias cidades e situações. A título de situação, ela foi usada durante a Copa América ocorrida no país em 2019 com a principal finalidade de identificar e vetar a entrada de torcedores estrangeiros envolvidos em episódios de violência. Os resultados foram satisfatórios e demonstrou efetividade no uso.

No quesito centros urbanos, a cidade do Rio de Janeiro utiliza o reconhecimento facial em auxílio à Segurança Pública. As pessoas detidas para averiguação após reconhecimento facial são por vários motivos, partindo do não pagamento de pensão alimentícia até traficantes e homicidas foragidos. Segundo Porta Voz da Polícia Militar do Rio de Janeiro, coronel Mauro: “se esse sistema puder ser adotado em larga escala na cidade ou no estado do Rio de Janeiro, será um aparato tecnológico de grande valia para diminuir a criminalidade”.

[7] Ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_pt
[8] Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709/2018.

A eficiência do sistema de reconhecimento possibilita ações pontuais e direcionamento do Agente Público. Além do Rio de Janeiro, Salvador, Paraíba e São Paulo são outros exemplos que estão fazendo uso da tecnologia.

No Estado da Paraíba, durante as festas de São João no centro da cidade de Campina Grande, o reconhecimento facial resultou na prisão de onze foragidos, ademais, as ocorrências costumeiras tiveram redução de 90% em relação ao ano anterior no mesmo evento. Bons resultados para a Segurança Pública do Estado.

Em São Paulo a tecnologia provida pela Thales Gemalto é utilizada nas investigações da Polícia Civil, comparando imagens do Banco de Dados de documentos de identidade com aqueles capturados nas cenas dos crimes. A confiabilidade no sistema calha ser o mesmo utilizado pela Federal Bureau of Investigation (FBI).

Na Bahia a aplicação da tecnologia de reconhecimento facial da Secretaria de Segurança Pública daquele Estado foi inaugurada em dezembro de 2018, não a título de teste, mas sim efetivamente incorporada em auxílio à Segurança Pública.

Conforme a SSP/BA divulgou, até o mês de novembro de 2019 foram capturados 80 foragidos através do sistema implantado. Segundo o Secretário de Segurança Pública Teles Barbosa: “a Segurança Pública segue atuando de forma precisa e discreta, avançando com a tecnologia para outros pontos da capital baiana”.

A tecnologia de reconhecimento facial no auxílio à Segurança Pública em Salvador demonstra que há um potencial a ser explorado quando da implantação de sistema de reconhecimento. O uso da tecnologia colabora para baixar os índices apresentados pelo IPEA (2019).

> Segundo o IPEA a Bahia, no geral, apresentou uma taxa de homicídio crescente a partir de 2013, partindo de 37,8 pontos e chegando ao número de 48,8 pontos em 2017, diferindo da média nacional que partiu de 28,6 e chegou à 31,6 considerando a mesma janela de datas e amostragem baseada no referencial de 100 mil habitantes[9].

O reconhecimento facial apresenta bons resultados à Segurança Pública dos Estados que as utilizam. Tem contribuído decisivamente nas capturas de foragidos que perambulam pelos centros urbanos utilizando o anonimato social como ferramenta para passarem despercebidos pelos Agentes de Segurança Pública.

---

[9] IPEA- http://www.ipea.gov.br/atlasviolencia/arquivos/downloads/6537-atlas2019.pdf

Em linha paralela de atuação os aeroportos internacionais no Brasil utilizam a biometria facial no controle alfandegário. Fazendo uso do Banco de Dados da Receita Federal, as imagens são captadas e processadas de modo indicar quem deve ou não abrir a bagagem. Segundo a chefe da equipe Jane Kambara (2016): “solução proporciona à Receita Federal precisão e agilidade na identificação de pessoas-alvo para a fiscalização de contrabando, descaminho e apreensão de produtos ilegais”.

Como reflexo da medida, diminuiu o incômodo no fluxo de passageiros facilitando o trabalho aduaneiro. O sistema demonstra ser eficiente e apresenta resultados positivos em conjunto com outras medidas aeroportuárias adotadas.

A abrangência da tecnologia de reconhecimento facial no Brasil se estende inclusive no combate a fraude em vestibulares aplicados pela Fundação Universitária para o Vestibular (Fuvest).

No Brasil a infraestrutura ainda é um problema a ser vencido para que haja ampla implantação de sistemas com reconhecimento facial, mas ainda assim a efetividade dos resultados apresentados pelas Instituições que utilizam o reconhecimento em prol da segurança é satisfatória e minimiza custos orgânicos.

3 BANCO DE DADOS

Estruturar um Banco de Dados robusto e viabilizar a interoperabilidade talvez seja o maior desafio para a Segurança Pública no que diz respeito ao reconhecimento facial, quiçá a compilação de um que atenda situações inerentes à atividade de Segurança Pública da Federação como um todo.

As fontes de dados utilizadas atualmente são variadas. A Polícia Civil de São Paulo, por exemplo, alimenta o Banco de Dados a partir da foto do sistema de identidades expedidas pelo Estado, por sua vez o Estado do Rio de Janeiro compara os rostos dos transeuntes com os procurados pela Justiça, presentes em um Banco de Dados provido pela Polícia Civil. O sistema de reconhecimento facial compara as imagens captadas com os 49 mil rostos de pessoas com mandados de prisão no Estado.

O Banco de Dados utilizado para fins de controle alfandegário em alguns aeroportos internacionais do Brasil tais como do Galeão na cidade do Rio de Janeiro e Guarulhos em São Paulo é fornecido pela Receita Federal para que haja o reconhecimento. Somente fins alfandegários.

Os passageiros oriundos de voos internacionais são submetidos ao reconhecimento facial, sendo a Receita Federal que procede ao processamento dos dados coletados, bem como fornece a informação para o Banco de Dados.

Figura 10 – Reconhecimento Receita Federal

Fonte: Receita Federal do Brasil, 2016.

Nos Estados Unidos (EUA) os dados da carteira de motorista são utilizados pela Federal Bureau of Investigation e também pelo Serviço de Imigração e Alfândega (ICE) para compor o Banco de Dados para reconhecimento facial. Tal prática apresenta solidez no arquivo a ser consultado pelo motivo de que as imagens foram obtidas em ambientes controlados e sofrem revalidações periódicas.

No Brasil, utilizar dados captados para um fim e os destinar para outro, necessariamente deve estar em concordância com a legislação e protocolos. O uso não regulamentado em legislação pertinente acarreta judicialização do fato. Banco de Dados alimentado com informação de documento pessoal emitido pelos Estados ou pela União apresentam características adequadas para utilização em reconhecimento facial em face da qualidade na captação da imagem.

A transparência e legalidade da utilização de dados e informações pessoais no Brasil apresentam adiantado processo regulatório e parâmetros de uso. Em consonância com outros países, foi promulgada a Lei Nº 13.709 de 14 de agosto de 2018. O assunto em tela será discorrido no item 4.2 em Lei Geral de Proteção de Dados no Brasil.

Atualmente cada Instituição brasileira que utiliza o reconhecimento facial trabalha com o seu próprio Banco de Dados e com fonte diversa. Não existe a interoperabilidade interagências no tocante unificação dos dados. Não há um banco de informações que atenda a todas as instituições. Tal prática inviabiliza a eficiência de um sistema de reconhecimento em encontrar um foragido, extraviado ou procurado do Estado de Santa Catarina que esteja circulando no anonimato social em outro Estado. Segundo o Conselho Nacional de Justiça (CNJ), o Brasil tem mais de 300.000 mil mandados de prisão em aberto, dados atualizados até junho de 2019. Outrossim, no que diz respeito a desaparecimentos, somente no Estado de Santa Catarina, considerando o período de 01 janeiro de 2018 à 01 de janeiro de 2020 foram contabilizadas 611 pessoas desaparecidas.

Seguindo um ideal de unificação de dados o Conselho Nacional de Justiça criou em 2018 o Banco Nacional de Monitoramento de Prisões (BNMP), constando os dados cadastrais de todos os presidiários do sistema carcerário brasileiro, uma vez que até então estava mais próximo da estimativa do que realidade. O documento vem sendo utilizado como ferramenta de grande importância no mapeamento geral da população carcerária.

Figura 11 – Banco Nacional de Monitoramento de Prisões

Fonte: Conselho Nacional de Justiça, 2018.

Partir da premissa que seja uma ferramenta a ser disponibilizada no formato de Banco de Dados às outras instituições é precipitado, mas o trabalho apresenta aspectos interessantes à formatação de um Banco de Dados para biometria facial de uso nacional. Em linha similar, o Tribunal Superior Eleitoral envida esforços na consolidação de um Banco de Dados dos eleitores, ainda que biométrico digital, porém apresenta robustez para dados faciais com a utilização do sistema Automated Fingerprint Identification System (AFIS).

3.1 QUALIDADE DAS IMAGENS NO BANCO DE DADOS

O Brasil apresenta grande índice de miscigenação em face de várias migrações que aqui se instalaram, com isso, segundo afirma Abboud da Empresa de Tecnologia Thales Gemalto (2019), a grande diversidade étnica brasileira dificulta a leitura de biometria facial por parte das máquinas, principalmente algoritmos utilizados e ou testados em pequenas diversidades étnicas.

Uma boa imagem do objetivo basta para o reconhecimento facial. Depara-se assim com a qualidade da fotografia no Banco de Dados e a coletada, mas segundo

Torres da Empresa Retina: “Não se pode confiar 100% no software e tampouco ter alguém mal preparado para operar. Não existe solução de reconhecimento facial que funcione sozinho e nem à prova de falha, até porque esta pode ser humana”.

Solução apontada pela citada empresa é ter processos de dupla ou até mesmo tripla checagem, minimizando e até erradicando a falha.

Uma imagem ideal para compor um Banco de Dados para reconhecimento facial deve possuir certas qualidades. Tal qualidade é alcançada quando a captação é feita em ambiente controlado a exemplo de fotos produzidas para documentos diversos expedidos pelos Estados e pela União. A qualidade requerida é alcançada por padronização do ambiente e do fotografado.

Imagem de qualidade captada ao ar livre é aquela que se aproxima da feita em ambiente controlado, isto é, sem sombras, sem óculos escuros, sem fumaça no ambiente, cabeça descoberta, iluminação favorável, ângulo fotográfico, projeção de luz, fundo etc.

A qualidade desejável de uma imagem é possível em ambiente controlado onde todos os itens citados ficam sujeitos aos ajustes para captação o que motiva o uso pelos sistemas de reconhecimento de biometrias faciais. A utilização das informações de Órgãos emissores de identidade ou da carteira nacional de habilitação (CNH) são fontes importantes a serem consideradas para formatar um Banco de Dados para operar o reconhecimento facial.

No que concerne atualização do Banco de Dados para o reconhecimento facial, utilizar informações inerentes à CNH apresenta a vantagem que tal documento é revalidado periodicamente.

3.1.1 Qualidade das imagens captadas

A resposta que um sistema de reconhecimento facial pode proporcionar, minimizando erros de falso positivo ou negativo, é diretamente proporcional a clareza, da imagem captada e da amostra contida no Banco de Dados.

Um banco de dados com imagens feitas a partir de ambientes controlados é uma ponta do sistema e a outra é a captação. Por certo que apenas uma boa imagem já é suficiente para proporcionar o reconhecimento, mas alguns locais de captação estão sujeitos ao ambiente, ademais, em se tratando de Segurança Pública

por vezes os equipamentos não são modernizados diminuindo a qualidade na captação ou no momento da transmissão.

Para que a máquina efetue o reconhecimento, conforme afirma Rouhani (2019), os softwares de reconhecimento facial necessitam que você diga quem é uma determinada pessoa para que seja reconhecida em outras fotos. A imagem captada deve possuir qualidade suficiente para que seja possível o algoritmo efetuar clara leitura dos pontos fiduciais, evitando assim falsos positivos e negativos.

O software de biometria facial é instalado em rede de monitoramento que, por vezes, já se encontra em funcionamento há muitos anos. Bastantes câmeras de um sistema de videomonitoramento são substituídas apenas quando deixam de funcionar e não quando obsoletas o que pode ter uma qualidade diminuída no tocante aos pixels na captação.

3.1.2 Falso positivo ou falso negativo

Para que um algoritmo classificador atinja nível desejável de operação deve necessariamente ter o menor índice de falsos positivos ou negativos sob a pena de cair em descrédito no uso.

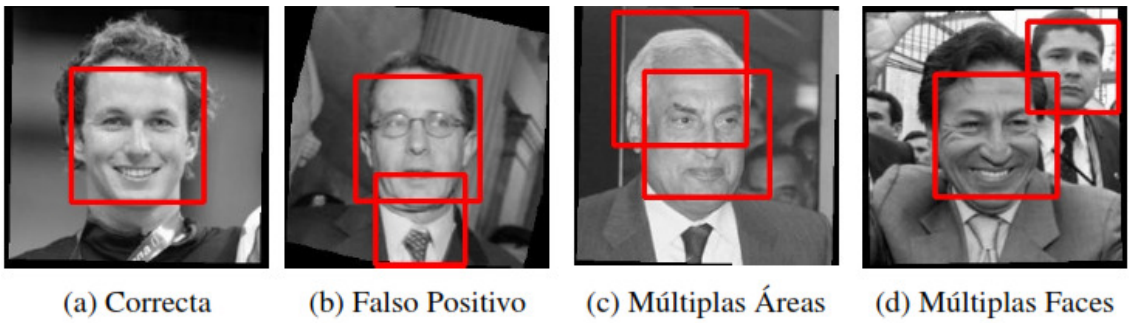
O falso positivo é justamente quando há diferença entre o detectado e o que se quer detectar, mas a máquina aponta como sendo coincidentes. As imagens não coincidem e o sistema de reconhecimento acusa como sendo o objetivo procurado. A falha pode estar na leitura que a máquina fez de forma equivocada, um algoritmo que não supra a necessidade daquele público, pode ser também a imagem no Banco de Dados que não apresenta clareza ou a imagem captada.

Quando ocorre um falso positivo, havendo intervenção do Agente de Segurança Pública na condução ou repressão, pode vir a gerar desconforto bilateral. Ressalta-se aqui a importância do preparo do Operador do sistema e dos Agentes de Segurança em labutar com a nova tecnologia, evitando judicialização.

O falso negativo vem justamente ao contrário, quando o objetivo não é reconhecido e são coincidentes. As falhas são as mesmas apontadas no falso positivo.

Para minimizar os falsos positivos e negativos, através da inteligência artificial é utilizado o aprendizado de máquina que depois de analisar algumas centenas de imagens passa a mapear o processo com aumento da eficácia de resposta no reconhecimento.

Figura 12 – Imagens submetidas ao aprendizado de máquina



Fonte: Rouhani, 2019.

Atualmente existe uma gama de algoritmos para os mais variados perfis e objetivos. Dentre os utilizados, conforme já citado, o Viola-Jones apresenta resultado satisfatório em relação a minimizar falhas de falsos positivos e negativos utilizando o método de cascata de classificadores.

Os erros ou enganos advindos do software ou do despreparo do Operador e do Agente de intervenção podem gerar simples desconfortos a situações que serão judicializadas, assim, o aprendizado de máquina, a capacitação do operador e dos agentes de intervenção são fatores determinantes ao sucesso de um sistema em operação.

4 PROTEÇÃO DE DADOS PESSOAIS

A partir de uma legislação pertinente que normatize, com elaboração de protocolos e procedimentos de utilização, atendendo a correta manipulação do uso do dado pessoal, com Órgão fiscalizador atuante, os dados pessoais estarão protegidos por Lei com as garantias conforme previsão legal.

A proteção legal do Dado Pessoal é uma ferramenta imprescindível para tornar realidade à construção de um Banco de Dados Nacional que possibilite a interoperabilidade no uso interagências, imputando responsabilidades pelo uso indevido da informação pessoal.

Ações não atendendo o parágrafo anterior, acabam por resultar em situações tais como ocorreu nos Estados Unidos da América. Os EUA através das polícias locais iniciaram o reconhecimento facial em centros urbanos sem que houvesse amparo por parte da legislação, isto somado aos falsos positivos resultou na proibição do uso dos sistemas de biometria facial em algumas cidades.

No Brasil a Lei de Proteção de Dados prevê entrar em vigor em agosto de 2020. A legislação favorece possível criação de um repositório de dados pessoais nacional, uma vez que atualmente cada Instituição trabalha com Banco de Dados restrito ao próprio círculo.

4.1 REGULAMENTO GERAL DE PROTEÇÃO DE DADOS

O Regulamento Geral de Proteção de Dados (RGPD) foi criado pela União Européia (UE) nº 2016/679[10] através do Parlamento Europeu e Conselho da mesma.

Com a demanda da utilização do uso de dados pessoais no gerenciamento migratório, nas ações antiterrorismo e outras, os países da UE, no intuito de proteção da individualidade do cidadão coibindo abusos, regulamentou o tratamento e o uso de informações pessoais, sendo vedada a utilização indiscriminada.

Concomitantemente, os países da União Européia criaram Organismos responsáveis pela proteção, utilização e pela fiscalização do uso do dado.

A restrição do uso procurou não fragilizar as ações relacionadas à segurança interna européia, ao contrário, de forma regulamentada prevê o uso enfatizando a

[10] https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_pt.

legalidade no tratamento e uso quando a questão é relacionada à segurança do Bloco Europeu.

4.2 LEI GERAL DE PROTEÇÃO DE DADOS NO BRASIL

O Brasil em consonância com a UE no tocante ao tratamento de dados pessoais promulgou a Lei Geral de Proteção de Dados (LGPD) em 2018.

Com a necessidade de regulamentação do assunto, através da Casa Civil, o Planalto dispôs a Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais que versa sobre o assunto e o regulamenta. A Lei prevê entrada em vigor em agosto de 2020, conforme abaixo:

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios[11].

A Lei promulgada delimita tipificando o uso das imagens e dados pessoais sensíveis, mas que podem ser utilizadas sem que para isso o usuário fique a margem da legalidade, conforme o Art. 4º da Lei 13.709:

> Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:
> I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;
> II - realizado para fins exclusivamente:
> a) jornalístico e artísticos; ou
> b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;
> III - realizado para fins exclusivos de:
> a) segurança pública;
> b) defesa nacional;
> c) segurança do Estado; ou
> d) atividades de investigação e repressão de infrações penais; ou
> § 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei[12].

[11] Lei Geral de Proteção de Dados Pessoais.
[12] Opus citatum.

O Art. 4º da Lei, acima, faz os apontamentos básicos e necessários para num segundo momento o Art. 5º da LGPD trazer à luz alguns conceitos de forma a colaborar na hermenêutica de valor ao entendimento mútuo. De modo simplificado, o extrato da citada Lei por definição, versa que dados pessoais são àqueles cujas informações dizem respeito às opções individuais das pessoas no que se referem às questões religiosas, sexuais, políticas, filosóficas bem como dados da genética, biométrica e de saúde.

São dados que envolvem a privacidade das pessoas e que a exploração indevida pode gerar discriminação ou qualquer tipo de exclusão ou preterimento, resultando prejuízos pessoais e profissionais ao titular.

Para efeito da LGPD, conforme o Art. 11, o tratamento de dados pessoais sensíveis somente poderá ocorrer quando houver consentimento por parte do titular ou responsável e a esse for dada a extensão específica do uso.

A Lei, no entanto, homologa o tratamento do dado pessoal sensível com exclusão do consentimento e sem que haja agravo legal ao usuário, na aplicação da hipótese em que haja o conluio com a situação de indispensável. Situações tais como: ocorrendo necessidade do cumprimento de obrigação legal ou regulatória, tratamento compartilhado de dados necessários à execução por parte da administração pública, realização de estudos por órgão de pesquisa, exercício regular do direito, proteção à vida, da incolumidade de si ou de outrem, tratamento de saúde com extensão a procedimentos a serem realizados por profissionais de saúde e garantia da prevenção à fraude e segurança do titular do dado.

Em decorrência do uso indevido ou não autorizado de dados pessoais, ao usuário cabe a implicação prevista no Art. 31 da referida Lei: quando houver infração em decorrência do tratamento de dados pessoais por Órgãos Públicos, a autoridade nacional poderá enviar informe com medidas cabíveis para fazer cessar a violação.

Para que o cumprimento da Lei atenda a demanda para a qual foi promulgada, alguns mecanismos foram implantados convergindo no alinhamento com a Lei nº 13.709, tal como a figura da Autoridade Nacional de Proteção de Dados e também de um Conselho Nacional de Proteção de Dados Pessoais e da Privacidade.

Cabe aos mecanismos a tarefa de dar solidez e garantias do correto cumprimento no uso do dado pessoal.

4.2.1 Lei de Proteção de Dados e a Agência Brasileira de Inteligência

A utilização do reconhecimento facial pela Segurança Pública foi tema de debate em audiência pública na Câmara dos Deputados e contou com a presença de representante da Agência Brasileira de Inteligência (ABIN) junto a Comissão de Ciência, Tecnologia, Comunicação e Informática em 03 de abril de 2019.

A ABIN defendeu que: “o uso da tecnologia de reconhecimento facial pode suprir necessidades táticas para melhorar a segurança pública do Brasil e apontou a necessidade do Congresso construir uma regulamentação sobre o tema”. Abaixo imagem feita na audiência.

Figura 13 – Audiência Pública na Câmara dos Deputados

Fonte: ABIN, 2019.

Segundo o representante da ABIN o reconhecimento facial pode ser utilizado para rastrear fugitivos, identificar agressores, localizar desaparecidos e acompanhar suspeitos de terrorismo. O Agente representante da ABIN declarou em plenário que:

> Há uma necessidade do Estado de localizar pessoas em determinadas situações. O reconhecimento facial poderia ser uma técnica muito importante para a segurança pública.
> O oficial de Inteligência da ABIN atentou para a necessidade de o país ter uma legislação adequada para regulamentar à vigilância estatal por meio do reconhecimento facial. De acordo com o integrante da Agência, é preciso diferenciar vigilância pública e privada e traçar requisitos legais com limites para a atuação do Estado[13].

[13] http://www.abin.gov.br/abin-apoia-regulacao-de-reconhecimento-facial.

De forma consensual, na audiência, ficou definido que deve existir delimitação legal ademais, que é importante minimizar ou erradicar excessos, principalmente àqueles praticados institucionalmente, por se tornam mais desastrosos para a administração pública.

A ABIN defendeu a diferenciação do privado do público, enfatizando a importância da clara fronteira de onde cada qual atua, não imputando a responsabilidade legal de um para outro no uso do dado pessoal.

5 VIDEOMONITORAMENTO EM SANTA CATARINA

Vários Estados brasileiros ao longo do tempo aderiram à tecnologia de videomonitoramento, cada Ente da Federação há seu tempo fez a implantação objetivando o aprimoramento da Segurança Pública no âmbito de suas jurisdições.

A implantação no Estado de Santa Catarina se deu entre final de 1999 e início do ano 2000, obedecendo a critérios determinados pela SSP/SC. A rede de monitoramento foi gradualmente expandida às cidades do Estado. Conforme Memorial do Projeto Bem-Te-Vi:

> O Projeto Bem-Te-Vi de videomonitoramento investiu mais de R$ 14 milhões em 115 cidades de Santa Catarina. O Estado é monitorado por 2.450 câmeras, espalhadas em 115 municípios. São 139 salas de monitoramento e 12 Centrais Regionais de Emergência, ou seja, 151 Centrais de Videomonitoramento. O sistema está em processo de implantação em 21 novos municípios catarinenses, os quais receberão um total de 188 pontos de videomonitoramento[14].

O sistema de videomonitoramento em Santa Catarina recebeu o nome de Bem-Te-Vi. Segundo a Secretária de Segurança Pública, atualmente a rede conta com 2.450 câmeras espalhadas em 115 municípios com 151 salas de controle do videomonitoramento.

Figura 14 – Bem-Te-Vi

Fonte: SSP/SC, 2017.

[14] http://www.ssp.sc.gov.br/index.php/programas/bem-te-vi.

A renovação e manutenção para que a rede de videomonitoramento se mantenha operacional no tocante aos equipamentos instalados é da responsabilidade, por competência, da Diretoria de Tecnologia da Informação e Comunicações (D/TIC). Segundo a SSP/SC o Órgão responsável pelo gerenciamento na aquisição dos materiais é o Ministério Público do Estado. O DTIC é quem descreve o material para que a aquisição atenda a demanda técnica necessária no relativo aos modelos de equipamentos.

Conforme a SSP/SC e o Memorial do Programa Bem-Te-Vi os recursos empregados são oriundos do Programa Pacto por Santa Catarina para adquirir e manter o videomonitoramento operacional no Estado:

> O Programa Bem-te-vi, executado pela Secretaria de Estado da Segurança Pública (SSP/SC), emprega recursos provenientes do "Pacto por Santa Catarina" – programa de investimentos promovido pelo Governo do Estado e das Prefeituras Municipais[15].

O Programa Pacto por Santa Catarina fomenta parceria entre o Estado e as Prefeituras, não mandatório, mas por adesão, com celebração de convênio de atendimento mútuo. O Estado provê a Segurança Pública, mas com os convênios, as Prefeituras preparam a infraestrutura necessária à implantação de sistema de videomonitoramento urbano, potencializando a segurança em cada ente conveniado.

O norte do sistema como um todo apresenta caráter preventivo de forma atenuar o repressivo, agindo no triângulo do crime, conforme (RODRIGUES, 2017 *apud* TASCA, 2012, p. 199 e 201):

> O triângulo do crime oferece uma visão dos elementos necessários para a ocorrência de um crime, cuja interação pode ser assim sintetizada: para que um crime ocorra deve haver convergência de tempo e espaço em, pelo menos, três elementos – um provável agressor, uma vítima/alvo adequado, na ausência de um guardião capaz de impedir o crime. [...] A teoria das atividades rotineiras exige mais do que a existência de um agressor (infrator), requer um alvo (vítima) vulnerável e um ambiente propício, ou seja, um ambiente que forneça as condições exatas para que o crime ocorra[16].

O sistema em si não impede uma ação delituosa, mas sim previne, não descartando a possibilidade de intervenção do Agente de Segurança que pode ser acionado para atender a demanda captada pelo videomonitoramento. Primariamente o

[15] www.ssp.sc.gov.br/files/BTV.pdf.
[16] Rodrigues, 2017.

sistema apresenta eficiência desacreditando a prática do ato delinquente. A possibilidade de estar sendo vigiado desacredita a ação do indivíduo, tal situação remonta à ótica panóptica de Foucault (2017), onde um edifício circular com pátio interno ostentava uma torre com vigilante, as pessoas que estavam no prédio em forma de círculo não sabiam ao certo se estavam sendo vigiadas ou não.

Se primariamente o videomonitoramento proporciona tal resultado, sem reconhecer seus atores, se pode considerar pelo menos interessante à Segurança Pública um sistema com reconhecimento facial que reconheça o autor.

A segunda fase proporcionada pelo videomonitoramento é a repressiva por parte dos Agentes de Segurança Pública, que são acionados pelo Operador de forma que a resposta repressiva seja pontual e eficiente.

O planejamento de atendimento ao chamado, bem como o posicionamento de câmeras e Agentes são estratégicos. Estão baseados em estatísticas de ocorrências que são compiladas a partir dos boletins de ocorrências registrados.

Figura 15 – Vídeomonitoramento

Fonte: SSP/SC, 2017.

O sistema de videomonitoramento apresenta então suas faces de eficiência sendo a primeira fase desacreditar o ato e a segunda repressiva com a ação policial.

A fase de desacreditar que um delito seja bem sucedido permite diminuir a presença de Agentes de Segurança Pública em vários locais ao mesmo tempo. O reflexo dessa prevenção incide em um efetivo menor para proteger a mesma área. Por outro lado, se a prevenção não for suficiente, o videomonitoramento permite que as ações sejam pontuais, com resultados mais precisos e deslocamento da força policial para o foco do problema, ademais, as imagens são arquivadas para eventual uso pela justiça e fins de elucidar controvérsias.

O reconhecimento através de biometria facial não é uma realidade na rede de videomonitoramento gerenciada pela SSP/SC, mas conforme experiências citadas no presente trabalho, noutras cidades fora do Estado (SC) os resultados de video-monitoramento com sistema de reconhecimento facial apresentam bons resultados à Segurança Pública.

5.1 CENTRO INTEGRADO DE COMANDO E CONTROLE

Para demonstrar resultados positivos na sua operação, um sistema de videomonitoramento deve apresentar duas pontas conectadas. Um extremo do sistema de monitoramento é a detecção e o outro, no caso da Segurança Pública, é o Centro de Comando e Controle ou as salas de controle da vigilância eletrônica.

Figura 16 – Câmeras de vídeomonitoramento

Fonte: Moreira, 2018.

A detecção é possível através de câmeras instaladas que podem estar isoladas ou comporem uma rede com várias interligadas.

Instaladas em pontos definidos permitem abrangência de cobertura e necessariamente devem estar conectadas a um centro de controle de onde se visualizam as imagens geradas.

Figura 17 – Centro Integrado de Comando e Controle de Canoas/RS.

Fonte: Weissheimer, 2016.

O local de recebimento de imagens de videomonitoramento pode ser dimensionado conforme a demanda do número de imagens captadas simultaneamente.

A título de Segurança Pública em Santa Catarina, o recebimento das imagens se dá por 151 salas destinadas para tal distribuídas pelo Estado.

Para gerenciar as situações originadas nas mais variadas cidades, às Secretarias de Segurança Pública dos Estados criaram seus Centros Integrados de Comando e Controle. A implantação de um Centro Integrado de Comando e Controle varia conforme a infraestrutura fornecida ao Órgão daquele Estado.

No Rio de Janeiro o Centro Integrado de Comando e Controle, opera com reconhecimento facial inserido ao sistema de videomonitoramento. As imagens captadas seguem o mesmo fluxo, enquanto o software destinado a biometria facial faz a varredura comparando faces na multidão com o Banco de Dados provido pela Polícia Civil. Um sistema de alarme avisa em caso de detecção positiva, dispensando a ação humana no processo de apontamento e análise. A partir da detecção positiva o Centro envia, ou não, Agentes para averiguação e, ou, repressão.

A cidade de Florianópolis apresenta extensa malha de cobertura de videomonitoramento, ademais possui estruturado centro de videomonitoramento. Ambas

as características convergem no favorecimento de implantação de biometria facial tal como em algumas outras capitais brasileiras.

Abaixo o exemplo de um Centro Integrado de Comando que foi implantado, em Curitiba, para atender os jogos da Copa do Mundo - FIFA Brasil 2014.

Figura 18: Centro Integrado de Comando e Controle Regional

Fonte: SSP/PR, 2014.

Sob o nome de Centro Integrado de Comando e Controle Regional, foi inaugurado em 2014, sendo operado por profissionais da Polícia Militar, Polícia Civil, Corpo de Bombeiros, Defesa Civil, Departamento Penitenciário e pelas Guardas Municipais do Estado do Paraná. Mesmo com o fim do evento mundial, a infraestrutura permanece ativada, porém não opera com biometria facial.

5.2 RECONHECIMENTO FACIAL NA CIDADE DE FLORIANÓPOLIS

Os avanços tecnológicos no tocante a videomonitoramento acabam por tornar obsoletos equipamentos com tecnologias recentes. Novas tecnologias requerem equipamentos atualizados, modernos, que possuam características que suportem cada vez mais a demanda do fluxo de dados, transmissão e difusão, com qualidade de imagem. Conforme descrito no tópico 3.1.1, a má qualidade de uma detecção gerada ou transmitida por videomonitoramento precário, pode gerar falsos resultados, principalmente quando se opera com biometria facial. Cabe ressaltar que os sistemas de reconhecimento facial, não são novos equipamentos a serem adquiridos, mas sim um software, um programa que é instalado à estrutura que já existen-

te em funcionamento. Os resultados advindos do sistema de reconhecimento possuem relação direta à qualidade da detecção, a requerida pelo software e naturalmente àquela que compõe o Banco de Dados.

A SSP/SC com vistas à necessidade de atualização, expansão e substituição de equipamentos em solução de videomonitoramento vem adquirindo novos materiais através de licitação elaboradas pelo Ministério Público.

No tocante a infraestrutura, em 2015 após a 58ª Reunião Nacional de Secretários da Segurança Pública, o então Secretário a SSP/SC divulgou que Santa Catarina receberia um Centro Integrado de Comando e Controle. A nova estrutura foi construída e entregue, operando com a centralização da Segurança Pública, mas o Centro Integrado de Comando e Controle ainda não é uma realidade.

Conforme anunciado em 2015 pelo Secretário Grubba:

> Santa Catarina receberá ainda este ano investimentos do Governo Federal com a construção do Centro Integrado de Comando e Controle (CICC). O anúncio foi feito na manhã desta quarta-feira, 15, durante reunião do secretário da Segurança Pública, César Augusto Grubba, com dirigentes da Secretaria Nacional de Segurança Pública (Senasp). De acordo com o secretário Grubba, o CICC abrigará o centro integrado das inteligências, sala de crise, call center, vídeomonitoramento e uma central de processamento de dados[17].

O gerenciamento da Segurança Pública através de um Centro Integrado de Comando e Controle gera maior consciência situacional, uma vez que integram dados de Inteligência, Defesa Civil, Bombeiro, Polícia Militar, Polícia Civil e Guarda Municipal.

Conforme delineado em 2015, a nova estrutura passou a agregar também a Central Regional de Emergência da Grande Florianópolis que antes funcionava anexo ao 4º Batalhão da Polícia Militar no centro da capital.

A implantação do CICC em Florianópolis ainda não realizada, não impede a possibilidade da inserção da tecnologia de reconhecimento facial no auxílio à Segurança Pública em Florianópolis, uma vez que a infraestrutura com gerenciamento aproximado das ações de segurança possui sala de videomonitoramento da cidade e do Estado.

---

[17] CENTRO INTEGRADO https://www.sc.gov.br/index.php/noticias/temas/seguranca-publica/santa-catarina-vai-ganhar-centro-integrado-de-comando-e-controle-cicc.

Com a estrutura pronta e recebida pela Secretaria de Segurança Pública do Estado, a mesma promoveu um seminário com o tema abordando a LGPD que entrará em vigor a partir de agosto de 2020. O intuito principal foi desmistificar a Lei, bem como orientar para as adequações necessárias por parte dos Órgãos públicos e privados que tem acesso a dados pessoais por questões funcionais. Na mesma linha de raciocínio, o Tribunal de Contas de Santa Catarina realizou em novembro de 2019, com a presença de integrantes da União Européia um seminário com a finalidade de disseminar e esclarecer aos Servidores e participantes os pormenores da Lei de Proteção de Dados.

A legislação sobre dados pessoais alcança as redes de monitoramento que captam e arquivam imagens de transeuntes, bem como as utilizadas na composição do Banco de Dados para reconhecimento facial.

5.2.1 Áreas monitoradas com reconhecimento facial

Uma área monitorada com reconhecimento facial depende exclusivamente do objetivo em relação ao público monitorado que se quer detectar, podendo ser pessoas desaparecidas, foragidos, traficantes, terroristas etc.

Para a Segurança Pública os locais podem ser os centros urbanos, aeroportos, estádios, locais de visitação, praias, ruas, avenidas etc. A definição dos locais depende do planejamento de cada Órgão de Segurança, atendendo seus objetivos que também podem ser a curto, médio e longo prazo.

Ainda que não utilize o reconhecimento facial, mas operando largamente com o videomonitoramento, a SSP/SC define as áreas a serem monitoradas em conformidade com os índices de ocorrências no local, bem como àquelas que apresentam sensibilidade pela concentração de comércio e áreas bancárias.

No tocante aos aeroportos, estes apresentam esquemas de videomonitoramento acirrado e vários com reconhecimento facial. Os aeroportos representam a entrada e saída de pessoas das cidades e dos países, com isso o videomonitoramento segue na preservação da segurança do Estado.

6 CONCLUSÃO

A escolha de um sistema de reconhecimento facial para auxiliar a Segurança Pública requer ponderar que existem variedades de programas. Selecionar um que atenda a demanda étnica populacional necessita que o software seja testado no local de operação para que apresente resultados satisfatórios.

A miscigenação do povo representa um fator importante, pois a escolha de um algoritmo testado em poucas amostras populacionais pode não apresentar as respostas que se busca na Segurança Pública. Algoritmos testados em poucas diversidades de amostragem demonstram pouca eficiência quando utilizadas numa população com origens múltiplas.

O aprendizado de máquina, através da inteligência artificial, proporcionado pela família de algoritmos AdaBoost com seus classificadores em cascata, apresentam excelentes resultados de reconhecimento facial. O AdaBoost através de testes e estudos evoluiu resultando o algoritmo Viola-Jones, que apresenta os melhores resultados no reconhecimento facial.

A problemática da grande quantidade de dados captados na imagem em ambientes não controlados visto que, na composição da imagem aparecem dados que não fazem parte do objetivo foi resolvido com a inserção no sistema algorítmico de filtros de abstração, onde através do aprendizado de máquina proporcionado pela inteligência artificial, o sistema seleciona o objetivo desejado descartando dados não interessantes ao reconhecimento.

Em ambientes controlados, imagens em dimensões 12x9 pixels proporcionaram a melhor taxa de precisão, acuidade, sendo possível aplicar as mesmas dimensões ambientes abertos.

Cada sistema de biometria facial apresenta sua especificidade de modo que não é possível um código chave, reconhecimento de um indivíduo, ser gerado em sistema X e ser utilizado por sistema Y, obtendo o mesmo resultado. Descarta-se assim a possibilidade de um Banco de Dados unificado onde constem somente códigos. Existe a necessidade da imagem ou um sistema que leia todos os códigos.

A utilização da tecnologia de biometria facial se mostra progressiva com grandes expectativas de expansão no uso em face de segurança e simplicidade no manuseio, já os sistemas utilizados, seguem cada qual sua lógica na concorrência em detrimento do domínio do mercado consumidor.

Para utilização em nível de Segurança Pública, a efetividade do reconhecimento pela máquina demanda sistemas operacionais com algoritmos que minimizem os falsos positivos e negativos. Uma biometria instalada que apresente muitas falhas acarreta descrença na utilização, controvérsias e demandas jurídicas e, como ocorreu em algumas cidades nos EUA, a proibição do uso da tecnologia.

A utilização de dados pessoais necessita de regulamentação, protocolos, Lei que dê o amparo legal para o uso. A falta de transparência na coleta e uso de dados pessoais gera ações judiciais, assim, utilizar a tecnologia em favor do bem social implica em regulamentar para que o Operador tenha o respaldo legal e segurança jurídica para operar. Atento ao tema, o Brasil promulgou a Lei Geral de Proteção de Dados que entrará em vigor em agosto de 2020. Os locais que operam com biometria facial, atualmente, estão estritamente relacionados à demanda do judiciário.

As cidades brasileiras que operam o reconhecimento facial colhem bons resultados, uma vez que implantaram o software no sistema de videomonitoramento existente, que continua a operar normalmente enquanto a varredura é efetuada pelo algoritmo. Este, por sua vez, aponta uma coincidência detectada com aquela que está no Banco de Dados gerando detecção positiva.

As áreas de monitoramento são fixas, mas os softwares permitem configurar quais os pontos a utilizarem a detecção facial. O Operador do Sistema seleciona conforme o interesse Operacional quais câmeras devem efetuar a detecção, assim viabilizando o reconhecimento facial nas áreas de interesse.

Dados estatísticos apresentam reduções nos índices de violência e aumento de prisões nas cidades que estão utilizando o reconhecimento facial operado por suas respectivas Secretarias de Segurança Pública.

Na cidade do Rio de Janeiro as pessoas captadas pelo sistema de reconhecimento facial compreendem casos desde pensão alimentícia a traficantes e homicidas procurados pela justiça. Em João Pessoa as ocorrências costumeiras tiveram redução de 90% e em Salvador à aplicação da tecnologia em um ano capturou 80 foragidos.

Todos os dias pessoas perambulam pelos centros urbanos em seus objetivos pessoais, são anônimos, são transeuntes que conjugam espaços lado a lado sem que saibam as motivações de outrem ou seus nomes, suas procedências e intenções. O policiamento ostensivo oferece a sensação de segurança enquanto o videomonitoramento busca focos de anormalidade, mas conforme a pesquisa, o reco-

nhecimento facial é uma ferramenta que realiza um trabalho discreto de grande valia à Segurança Pública pinçando àqueles que por algum motivo não deveriam estar no meio social.

Alguns aeroportos internacionais no Brasil operam com reconhecimento facial para fins alfandegários e apresentam bons resultados no combate ao ilícito, seguindo a mesma linha de detecção da Segurança Pública, mas com foco distinto, uma vez que a origem do Banco de Dados é da Receita Federal.

O estudo em questão constatou que cada Instituição Pública provê seu Banco de Dados de forma singular, não existe interoperabilidade e tampouco mesma origem da informação a ser utilizada. A utilização pela Segurança Pública tem por base informações de documentos como da carteira nacional de habilitação, identidade e dados fornecidos pela justiça, já para o controle alfandegário, os elementos são da Receita Federal. A infraestrutura representa um problema tal que, não se viabilizou até o momento a compilação de um Banco de Dados único que atenda a todas as Secretarias de Segurança Pública da União.

A implantação e operação de Centros Integrados de Comando e Controle previstos e determinados por Lei Federal possibilitam a informação transitar de forma dinâmica entre os Agentes de Segurança Pública gerando maior consciência situacional. Também viabiliza de forma mais eficiente a operação de sistema de reconhecimento facial na rede de monitoramento. Com a pesquisa foi constatado que para operar um sistema de biometria facial se faz necessário a capacitação dos usuários, tanto o Operador como àqueles que farão abordagem de um positivado.

Através da SSP/SC em Florianópolis foi elaborado seminário desmistificando, disseminando e capacitando Agentes públicos e privados no tocante a Lei Geral de Proteção de Dados. Tal ação é importante, pois promove um ambiente propício a implantação de um sistema de reconhecimento, uma vez que a Lei 13.709 deve estar clara e solidificada nas Instituições, representando um pilar regulatório.

Florianópolis possui um centro de monitoramento junto a SSP/SC que apresenta robusta capacidade de gerenciamento no videomonitoramento. A rede de câmeras sofre regular manutenção e atualização com aquisição de novos equipamentos o que viabiliza a inserção de sistema de reconhecimento facial.

A particularidade de instalação do sistema é a viabilidade de embarcar o software em uma rede de câmeras em operação. A cidade de Florianópolis possui estratégica malha de videomonitoramento.

A decisão de qual algoritmo instalar, qual software utilizar, deve passar necessariamente pela fase de teste na cidade. Aquele que melhor resultado apresentar em face da população miscigenada pode ser instalado no auxílio à Segurança Pública.

A problemática de um Banco de Dados em comum, que seja integrado a outros Estados da Federação não constitui um problema isolado, mas sim de todas as Secretarias de Segurança Pública.

REFERÊNCIAS

ABIN. **ABIN apóia regulação de reconhecimento facial.** Disponível em: http://www.abin.gov.br/abin-apoia-regulacao-de-reconhecimento-facial/. Acesso em 1 jun. 2020.

ARAUJO (2010 apud FREUND, Y., SCHAPIRE, R. E, p.9). **"A decision-theoretic generalization of online learning and an application to boosting**", Journal of Computer and System Sciences, v. 55, n. 1, pp. 119–139, 1997. Disponível em: https://link.springer.com/chapter/10.1007/3-540-59119-2_166. Acesso em: 07 abr. 2020.

ARAUJO, Gabriel Matos. **Algoritmo para reconhecimento de características faciais baseado em filtros de correlação**. 2010. Tese (Mestrado em Engenharia Elétrica) – Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2010. Disponível em: http://pee.ufrj.br/teses/textocompleto/2010021901.pdf. Acesso em: 07 abr. 2020.

BRASIL . **LEI Nº 13.709, DE 14 DE AGOSTO DE 2018.** Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 07 abr. 2020.

_____. **LEI Nº 12.663, DE 5 DE JUNHO DE 2012.** Dispõe sobre as medidas relativas à Copa das Confederações FIFA 2013, à Copa do Mundo FIFA 2014 e à Jornada Mundial da Juventude - 2013, que serão realizadas no Brasil; altera as Leis nºs 6.815, de 19 de agosto de 1980, e 10.671, de 15 de maio de 2003; e estabelece concessão de prêmio e de auxílio especial mensal aos jogadores das seleções campeãs do mundo em 1958, 1962 e 1970. Presidência da República, 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12663.htm. Acesso em: 10 de maio de 2020.

_____. **LEI Nº 13.853, DE 08 DE JULHO DE 2019.** Esta Lei altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm. Acesso em: 07 de maio 2020.

_____. **LEI Nº 8.666, DE 21 DE JUNHO DE 1993.** Esta Lei estabelece normas gerais sobre licitações e contratos administrativos pertinentes a obras, serviços, inclusive de publicidade, compras, alienações e locações no âmbito dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios. Presidência da República, 1993. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/cons.htm. Acesso em: 07 de abr. 2020.

_____. **LEI Nº 9.307, DE 23 DE SETEMBRO DE 1996.** Lei da Arbitragem. Presidência da República, 1996. Disponível em: http://www.planalto.gov.br/ccivil_03//leis/l9307.htm. Acesso em: 07 de maio 2020.

_____. **Reunião Nacional de Secretários da Segurança Pública.** Florianópolis, 2015. Disponível em: https://www.sc.gov.br/index.php/noticias/temas/seguranca-publica/santa-catarina-vai-ganhar-centro-integrado-de-comando-e-controle-cicc. Acesso em: 20 mar. 2020.

_____. **Secretaria de Segurança Pública.** Memorial Bem-Te-Vi. Florianópolis, 2017. Disponível em: ssp.sc.gov.br/files/BTV.pdf. Acesso em: 05 abr. 2020.

_____. **Segurança Pública.** Florianópolis, 2015. Disponível em: https://www.sc.gov.br/index.php/noticias/temas/seguranca-publica/santa-catarina-vai-ganhar-centro-integrado-de-comando-e-controle-cicc. Acesso em: 20 mar. 2020.

_____. **Serviço Federal de Processamento de Dados - SERPRO**. Disponível em: http://intra.serpro.gov.br/tema/noticias-tema/reconhecimento-facial-intensifica-seguranca. Acesso em 15 abr. 2020.

CARLA PEQUENINO. **Cryptoid, portal brasileiro sobre identificação digital**. 2020 (Notícias eletrônicas). Disponível em: https://cryptoid.com.br/identidade-digital-destaques/como-os-paises-usam-o-reconhecimento-facial/. Acesso em: 27 mar. 2020.

CHAVES, Bruno Butilhão**. Estudo do algoritmo AdaBoost de aprendizagem de máquina aplicado a sensores e sistemas embarcados.** 2012. Tese (Mestrado em Engenharia) – Universidade de São Paulo, São Paulo, 2012. Disponível em: https://teses.usp.br/teses/disponiveis/3/3152/tde-12062012-163740/publico/Bruno_Chaves_Diss_vfrevisada.pdf. Acesso em: 27 mar. 2020.

COMISSÃO EUROPÉIA. **Proteção de dados da EU - RGPD.** 2016. Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_pt. Acesso em: 28 mar. 2020.

CONSELHO NACIONAL DE JUSTIÇA. **Banco Nacional de Monitoramento de Prisões.** Disponível em: https://www.cnj.jus.br/wp-content/uploads/2018/01/57412abdb54eba909b3e1819fc4c3ef4.pdf. Acesso em 15 abr. 2020.

EDUARDO R. HRUSCHKA. **SCC5895 – Análise de Agrupamento de Dados.** Representação de Dados e Medidas de Proximidade. USP, São Paulo. Disponível em: http://wiki.icmc.usp.br/images/5/55/Representacao_Proximidade_2012.pdf. Acesso em: 05 abr. 2020.

FABIO ABRANTES DINIZ, THIAGO REIS DA SILVA, FRANCICO EDUARDO SILVA ALENCAR. **Um estudo empírico de um sistema de reconhecimento facial utilizando o classificador KNN**. Volume 8, número 1. Passo Fundo 2016 (Revista Brasileira de Computação Aplicada). Disponível em: http://seer.upf.br/index.php/rbca/article/view/5227. Acesso em: 05 abr. 2020.

FERNANDO PAIVA. **Mobile time**. 2019 (revista eletrônica). Disponível em: https://www.mobiletime.com.br/noticias/21/11/2019/sorria-voce-esta-sendo-reconhecido/. Acesso em: 05 mar. 2020.

FERNEDA, Edberto. **Redes neurais e sua aplicação em sistemas de recuperação de informação.** Ciência da Informação. Brasília, v. 35, n. 1, jan./abr 2006. Disponível em: https://www.scielo.br/scielo.php?script=sci_arttext&pid=S0100-19652006000100003#fig01: Acesso em: 1 jun. 2020.

FREUND, Y., SCHAPIRE, R. E. **A decision-theoretic generalization of online learning and an application to boosting**. Dezembro 2006. Disponível em: https://pdfs.semanticscholar.org/5fb5/f7b545a5320f2a50b30af599a9d9a92a8216.pdf. Acesso em : 05abr 2020.

GLAUCO ARBIX**. Tecnologia de reconhecimento facial é banida de São Francisco**. (São Paulo, 2019) Jornal da USP. Disponível em: https://jornal.usp.br/atualidades/tecnologia-de-reconhecimento-facial-e-banida-de-sao-francisco/. Acesso em: 28 mar. 2020.

GOVERNO DE SANTA CATARINA. **Centro Integrado de Comando e Controle.** Disponível em: http://www.ssp.sc.gov.br/. Acesso em: 05 abr. 2020.

_____. **Diretoria de tecnologia da informação e comunicações**. Disponível em: http://www.ssp.sc.gov.br/dtic/index.php/coordenadorias/videomonitoramento-e-suporte. Acesso em: 05 abr. 2020.

GOVERNO FEDERAL. **Receita Federal - Migração**. Disponível em: http://www.fazenda.gov.br/noticias/2016/agosto/receita-federal-lanca-sistema-de-reconhecimento-facial. Acesso em 15 abr. 2020.

GUSTAVO ALTMAN. **Justiça impede o uso de câmeras de reconhecimento facial no metrô.** (São Paulo, 2018). Disponível em: https://www.jota.info/justica/mp-cancele-cameras-metro/. Acesso em: 28 mar. 2020. https://www.sul21.com.br/cidades/2016/02/21313canoas-investe-em-video-monitoramento-e-grupos-de-whatsapp-para-combater-violencia/. Acesso em 1 jun. 2020.

INSTITUTO BRASILEIRO DE DEFESA DO CONSUMIDOR. **Metrô de SP já vendeu seu rosto e só agora terá de explicar por quê.** 2020. Disponível em: https://idec.org.br/idec-na-imprensa/metro-de-sao-paulo-ja-vendeu-seu-rosto-e-so-agora-tera-de-explicar-por-que. Acesso em: 05 maio 2020.

INSTITUTO DE PESQUISA ECONÔMICA APLICADA. **Atlas da violência retratos dos municípios brasileiros.** Rio de Janeiro, 2019. Disponível em: http://www.ipea.gov.br/atlasviolencia/arquivos/downloads/6537-atlas2019.pdf. Acesso em: 05 abr. 2020.

JASON, Janderson. **Medidas de Similaridade.** Novembro 2012. Disponível em: http://www.dsc.ufcg.edu.br/~pet/jornal/novembro2012/materias/recapitulando.html: Acesso em: 1 jun. 2020.

JESUS, Rui M. **Cascata de classificadores**. Novembro 2018. Disponível em: https://www.researchgate.net/figure/Cascata-de-Classificadores-O-algoritmo-consiste-na-construcao-de-uma-cascata-de_fig2_337316195: Acesso em: 1 jun. 2020.

MARENGONI, Mauricio., STRINGHINI, Denise. **Introdução à Visão Computacional usando OpenCV.** Volume 16, número 1. Porto Alegre: 2009 (RITA – Revista de Informática Teórica e Aplicada). Disponível em: https://www.seer.ufrgs.br/rita/article/view/rita. Acesso em 28 mar. 2020.

MICHAELIS. **Dicionário Brasileiro da Língua Portuguesa**. Disponível em: http://michaelis.uol.com.br/moderno-portugues. Acesso em: 27 mar. 2020.

MINUTO DA SEGURANÇA. Polícia do Rio prende 63 pessoas com tecnologia de reconhecimento facial. **O blog da segurança da informação,** 20 nov. 2019. Disponível em: https://minutodaseguranca.blog.br/policia-do-rio-prende-63-pessoas-com-reconhecimento-facial/. Acesso em: 4 mar. 2020.

MOREIRA, Eduardo. Target HD. Target HD. **Como serão as câmeras de segurança com inteligência artificial no futuro**. Julho 2018. Disponível em: https://www.targethd.net/como-serao-as-cameras-de-seguranca-com-inteligencia-artificial-no-futuro/. Acesso em 1 jun. 2020.

OPEN FACE. **Top 10 Facial Recognition APIS** (updated for 2018). Disponível em: https://www.liberaldictionary.com/face-recognition/top-10-facial-recognition-apis-updated-for-2018-rapidapi/.: Acesso em: 1 jun. 2020.

PONTES, Pedro Tiago Carvalho da Silva. **Visage - Impacto dos Filtros de Abstração no Reconhecimento Facial em Imagens**. 2013. Tese (Mestrado Integrado em Engenharia Informática e Computação) – Universidade do Porto, Porto, 2013. Disponível em: https://sigarra.up.pt/flup/pt/pub_geral.pub_view?pi_pub_base_id=26248. Acesso em: 4 mar 2020.

PREFEITURA MUNICIPAL DE FLORIANÓPOLIS. **Decreto Municipal Nº 21347.** Edição nº 2647. Florianópolis, 16 de março de 2020 Diário Oficial Eletrônico do Município de Florianópolis. Disponível em: http://www.pmf.sc.gov.br/arquivos/diario/pdf/16_03_2020_18.39.59.bebde7c3e96f781d066b2de22c6c4967.pdf. Acesso em: 28 mar. 2020.

RESEARCHGATE. **Cascata de Classificadores**. Disponível em: https://www.researchgate.net/figure/Cascata-de-Classificadores-O-algoritmo-consiste-na-construcao-de-uma-cascata-de_fig2_337316195 . Acesso em: 05 abr. 2020.

RIOS, CARVALHO, João Pedro, Ana Beatriz. ACADEMIA.EDU **– Seletividade**: o panoptismo midiático e a eficiência do sistema penal. Disponível em: https://www.academia.edu/35286863/seletividade_o_panoptismo_midiático_e_a_eficiência_do_sistema_penal. Acesso em: 04 nov. 2019.

RODRIGUES, DANIEL (2017 *apud* HIPÓLITO; TASCA, 2012. p. 5). **Secretaria de Segurança Pública.** Memorial Bem-Te-Vi. Florianópolis, 2017 Disponível em: http://www.ssp.sc.gov.br/files/BTV.pdf. Acesso em: 05 abr. 2020.

ROLIM VIOTTI & LEITE CAMPOS**. Reconhecimento facial e multas são destaque no tema de proteção de dados**. São Paulo, 2019. Portal internet. https://rolimvlc.com/informes/reconhecimento-facial-protecao-dados/. Acesso em: 27 mar. 2020.

ROUHANI, Sama. **Reconhecimento de face e de "prova de vida" com Tensorflow para criação de um sistema de segurança voltado a residências e a ambientes de acesso restrito**. 2019. Tese (Mestrado Matemática Estatística e Computação Aplicadas à Indústria) – Universidade de São Paulo, São Paulo, 2019. Disponível em: https://www.teses.usp.br/teses/disponiveis/55/55137/tde-21082019-155544/publico/SamaRouhani.pdf. Acesso em 28 mar. 2020.

SANTOS, Marco Aurélio da Silva. **Mundo Educação**. Disponível em: https://mundoeducacao.bol.uol.com.br/fisica/olho-humano-um-instrumento-optico.htm#. Acesso em: 1 jun. 2020.

SCIENCE DIRECT. A decision-Theoric Generalization of On-Line Learning and an Application to Boosting. **Journal of Computer an System Sciences**.Volume 55, Issue 1, Ago/1997. Disponível em: https://www.sciencedirect.com/science/article/pii/S002200009791504X. Acesso em 27 de mar. 2020.

SECRETARIA DE SEGURANÇA PÚBLICA DA BAHIA. **Reconhecimento Facial da SSP alcança a marca de 80 prisoes**. Versão ou edição (se houver).Salvador: 03 de nov. 2019, site da Segurança Pública da Bahia. Disponível em: http://www.ssp.ba.gov.br/2019/11/6733/Reconhecimento-Facial-da-SSP-alcanca-a-marca-de-80-prisoes.html. Acesso em: 28 mar. 2020.

SECRETARIA DE SEGURANÇA PÚBLICA DE SÃO PAULO. Polícia civil do Estado de São Paulo. **Secretaria de Segurança Pública**. São Paulo, 2020. Acesso restrito via login pelo endereço eletrônico: https://www.policiacivil.sp.gov.br/portal/faces/oracle/webcenter/portalapp/pages/login.jspx?_afrLoop=2290142859319765&_afrWindowMode=0&_afrWindowId=null#!%40%40%3F_afrWindowId%3Dnull%26_afrLoop%3D2290142859319765%26_afrWindowMode%3D0%26_adf.ctrl-state%3Dg9xk6xc2m_13.

SECRETARIA DE SEGURANÇA PÚBLICA E ADMINISTRAÇÃO PENITENCIÁRIA. **Centro de Comando e Controle Regional.** Paraná. Site da Segurança Pública do Paraná. Disponível em: http://www.seguranca.pr.gov.br/CICCR/. Acesso em: 26 mar. 2020.

SILVEIRA, Jheime ,Santos da., SÁ Abreu, Angela de. Reconhecimento Facial Usando o algoritmo Autenticação da biblioteca Open CV. **ZENODO – r**evista eletrônica, Uberlândia, re 9, nov, 2018. Disponível em: https://zenodo.org/record/1478919#.XoCtf1VKjIU. Acesso em 28 mar. 2020.

SUPERIOR TRIBUNAL ELEITORAL. **Banco de dados biométrico**. Disponível em: http://www.tse.jus.br/imprensa/noticias-tse/2019/Agosto/biometria-confere-ainda-mais-seguranca-na-identificacao-dos-eleitores. Acesso em 15 de abr. 2020.

TENSORFLOW. **An end-to-end open source machine learning platform.** Disponível em: www.tensorflow.org. Acesso em 27 mar. 2020.

TERUEL, Gilberto Ferreira. **Imagem adaptada de Sagonas 2013**. Disponível em: https://www.researchgate.net/figure/Figura-2-Representacao-dos-68-pontos-fiduciais-marcados-sobre-face-humana-generica_fig2_328658018: Acesso em: 1 jun. 2020.

UFERSA. REDFACE: um sistema de reconhecimento facial baseado em técnicas de análise de componentes principais e autofaces. **DOAJ** – revista brasileira de computação aplicada, Passo Fundo, 2012. Disponível em: https: https://doaj.org/article/1ed1f436dc624ac185d494c96c6836ec. Acesso em 27 mar. 2020.

Weissheimer, Marco. Sul21. **Canoas investe emvídeo-monitoramento e grupos de whatsapp para combater violência**. Fevereiro 2016. Disponível em: https://www.sul21.com.br/cidades/2016/02/21313canoas-investe-em-video-monitoramento-e-grupos-de-whatsapp-para-combater-violencia/. Acesso em: 1 jun 2020.