AMON: Controle de acesso do jurisdicionado no TJDFT a partir de técnicas de reconhecimento facial

Jairo Simão Santana Melo
Thiago Arruda Neves
Celso oliveira Neto

Resumo: O Tribunal de Justiça do Distrito Federal e dos Territórios (TJDFT), por meio de suas áreas técnicas, está buscando a constante modernização dos seus sistemas, processos e atividades. Um dos meios para alcançar esse objetivo tem sido o estudo e desenvolvimento de sistemas de automação e inteligência artificial. Um exemplo dessas iniciativas é o projeto Ámon. O Ámon surgiu de uma parceria do Serviço de Ciência de Dados (SERCID) com a Assessoria de Segurança Institucional (ASI) do TJDFT. A demanda da ASI possuía como objetivo a implementação de um sistema de reconhecimento facial, a partir de fotografias, para trazer mais segurança ao jurisdicionado no TJDFT. O sistema a ser desenvolvido deveria integrar-se integrado ao SidenWeb, software do Tribunal que gerencia o controle integrado de acesso às suas dependências. O sistema Ámon encontra-se operacional desde junho de 2020, nas portarias do TJDFT (Fórum Desembargador Milton Sebastião Barbosa). A checagem de segurança dos visitantes do Tribunal foi enriquecida com esse sistema. Agora, além da verificação a partir de metadados, como CPF, é possível realizar uma conferência de cada pessoa a partir do reconhecimento facial, trazendo maior controle sobre quem entra na Casa. Com isso, buscamos trazer mais segurança aos jurisdicionados no TJDFT, mantendo um controle maior sobre quem transita em suas dependências.

Palavras-chave: Reconhecimento facial. Inteligência Artificial. Aprendizagem de máquina. Segurança.

Abstract: The Tribunal de Justiça do Distrito Federal e dos Territórios (TJDFT), through its technical areas, is seeking constant modernization of its systems, processes and activities. One of the means to achieve this goal has been the study and development of automation and artificial intelligence systems. An example of these initiatives is the Amon project. Amon arose from a partnership between the Serviço de Ciência de Dados (SERCID) and the Assessoria de Segurança Institucional (ASI) of TJDFT. ASIS's demand aimed to implement a facial recognition system, based on photographs, to bring more security to the TJDFT jurisdiction. The system to be developed should be integrated with SidenWeb, Court's software that manages the integrated access control to its facilities. The Amon system has been operational since June 2020, at TJDFT's ordinances (Desembargador Milton Sebastião Barbosa Forum). The security check of the Court's visitors was enriched with Amon. Now, in addition to verification using metadata, such as CPF, it is possible to check each person based on facial recognition, bringing greater control over who enters the Court. With that, we seek to bring more security to the jurisdictions in the TJDFT, maintaining greater control over who transits on its premises.

Keywords: Facial recognition. Artificial Intelligence. *Machine learning*. Security.

1 Introdução

Vivemos em uma era em que os avanços tecnológicos têm ocorrido mais rápido do que nunca. Com um ritmo constante de atualizações, diversas tecnologias se popularizaram e foram integradas à rotina das pessoas, como a inteligência artificial e os sistemas em nuvem. Apesar de serem bastante utilizadas, ainda é comum ter dúvidas sobre conceitos relacionados ao *Big Data* e às aplicações de *machine learning* e até mesmo sobre como funciona o reconhecimento facial (IMPACTA, 2020).

O reconhecimento facial não é mais uma tecnologia vista apenas em filmes de ficção científica. Atualmente, dispositivos e sistemas de segurança contam com esse recurso, que promete facilitar rotinas em diversos cenários. Essa tecnologia é uma maneira de identificar rostos humanos em imagens por meio de técnicas digitais. É um recurso baseado em sistemas de Inteligência Artificial que são responsáveis pelo cruzamento de dados e detecção de padrões para garantir que o rosto detectado é de determinada pessoa.

O processamento de imagens da face existe há alguns anos, mas somente agora começou a ganhar espaço e a ser implementada em bancos e outros serviços que demandem reforço na segurança ou, simplesmente, busquem facilitar o acesso do usuário. Hoje, já usamos a biometria para a identificação das pessoas pelas suas digitais, seja para desbloquear o celular, fazer operações bancárias, entrar no país, seja para votar nas eleições. O reconhecimento facial também é baseado em uma técnica biométrica em que os *softwares* "codificam" nosso rosto.

Para fazer esse mapeamento, os sistemas utilizam as características do rosto de uma pessoa, como o tamanho do queixo e a distância entre os olhos. Elas são chamadas de pontos nodais (a face humana possui cerca de 80 pontos). A extração de cada ponto vai formando a assinatura facial e é armazenada em um banco de dados. Ao fim do processo, é necessário comparar as características extraídas com as do banco para encontrar o dono do rosto. Alguns *smartphones* já utilizam a tecnologia para

que o aparelho seja desbloqueado somente pelo proprietário. Segundo pesquisa do *Counterpoint Research*, até 2020, 64% de todos os celulares vão contar com a inovação (RUNRUN, 2020).

Como se trata de uma tecnologia nova, as leis ainda não foram adaptadas para ela. No Brasil, já foi aprovada a Lei Geral de Proteção de Dados Pessoais (LGPDP), que entrou em vigor em agosto de 2020; o artigo 4º, no entanto, exclui o tratamento de dados para fins de segurança pública (OLHAR DIGITAL, 2019).

A preocupação dos especialistas é que os dados não sejam usados apenas para essa finalidade — como o que acontece hoje na China para a definição do crédito social. E a polêmica aumentou com a criação da Autoridade Nacional de Proteção de Dados (ANPD) por medida provisória. Isso porque, além de tornar o poder fiscalizatório sobre o tratamento de dados pelo Estado mais flexível, ela permite o compartilhamento de informações públicas com empresas desde que haja supervisão de uma autoridade (OLHAR DIGITAL, 2019).

O Brasil tem 37 iniciativas em cidades adotando, de alguma maneira, tecnologias de reconhecimento facial. Mais da metade, 19, foram lançadas no período de 2018 a 2019. Essas soluções, em geral, são empregadas nas áreas de segurança pública, transporte e controle de fronteiras (AGÊNCIA BRASIL, 2019).

Juntamente com a disseminação desse recurso, vem também a preocupação das autoridades. O levantamento identificou dois projetos de lei no Congresso Nacional e 21 em assembleias legislativas sobre o tema, sendo oito no Rio de Janeiro e dois em São Paulo. “O reconhecimento facial é colocado como uma espécie de bala de prata para segurança pública”, observou a pesquisadora Marie Hurel (AGÊNCIA BRASIL, 2019).

O Projeto de Lei n. 9.736, de 2018, do Deputado Júlio Lopes (PP/RS), por exemplo, obriga o reconhecimento facial em presídios. O PL n. 11.140, de 2018, do líder do PSL, Delegado Waldir (GO), vai além e determina registros não somente aos detidos, mas também a funcionários e até mesmo advogados que ingressam na unidades de internação (AGÊNCIA BRASIL, 2019).

O TJDFT tem atuação em 19 circunscrições em todo o Distrito Federal com movimentação diária de milhares de pessoas em seus cartórios, fóruns e secretarias. Em cada portaria das unidades do tribunal existe uma estrutura de controle de acesso físico composto de *scanners*, portas giratórias, segurança e atendentes contratadas e servidores responsáveis pelo acesso. Todo acesso é registrado por um sistema de cadastro denominado Siden, em que são registrados os dados do jurisdicionado que adentra as dependências do órgão. Durante esse cadastro no sistema são solicitadas algumas documentações de identificação, tais como RG, CPF ou habilitação, assim como o destino desejado dentro do fórum.

Em 2019, passou-se a exigir uma foto tirada pelos equipamentos do TJDFT e armazenadas em ambiente seguro dentro do Siden, possibilitando que futuramente algum mecanismo de processamento de imagens pudesse auxiliar e contribuir com a segurança interna do tribunal.

2 Estado da arte

a biometria é uma técnica utilizada na identificação de indivíduos a partir do uso de características mensuráveis, como medidas fisiológicas ou comportamentais, que permitem diferenciar de forma confiável um indivíduo dos demais (GUIMARÃES, 2015).

Segundo Santos (2007), a biometria é um conceito associado ao uso eficiente de técnicas de identificação, sendo utilizada há muito tempo pelos povos egípcios no tratamento de extração de características de um indivíduo, com base no uso de métodos e técnicas primordiais relacionadas à existência de marcas de cicatrizes e até mesmo de aparências pessoais para auxiliar no processo de identificação.

Nos sistemas atuais, inicialmente é aplicado à captura de um sinal digital ou analógico das características de uma pessoa. Posteriormente, a atividade responsável pelo processamento e classificação dos padrões é aplicada. Por último, é o processo de decisão que retorna o resultado com muita precisão, e, na maioria dos casos, acontece em tempo real (INTERNATIONAL BIOMETRIC GROUP, 2014 *apud* BOECHAT, 2008). A precisão biométrica é entendida como o maior objetivo e o maior desafio da biometria, sendo necessária a aplicação de vários testes sem amostras heterogêneas de análise e validação do sistema biométrico. A precisão biométrica é medida por situações nas quais sua aplicação alcance resultados satisfatórios, proporcionando casos sem fal-

sos negativos, quando a aplicação não reconhece o indivíduo mesmo este estando devidamente cadastrado na base de dados do sistema, e sem falsos positivos, quando o sistema reconhece um indivíduo como sendo outro (GUIMARÃES, 2015).

A maioria dos sistemas biométricos também possui vários fatores externos ao sistema que podem atrapalhar a sua utilização, como a iluminação, no caso de utilização de imagens, ou da qualidade da digital, que é a característica mais estudada e difundida e, em alguns casos, até considerada sinônimo de biometria (TEIXEIRA, 2011).

Os sistemas biométricos se dividem em dois grandes grupos: 1) os invasivos, que necessitam da colaboração do sujeito para a sua identificação; e 2) os não invasivos, que podem ser utilizados até mesmo sem o conhecimento do identificado. Entre os métodos invasivos, encontram-se os mais conhecidos de biometria, como a biometria pela digital, pela face, pela íris, pela assinatura, entre outros. No que se refere aos métodos invasivos, há métodos biométricos que possuem grande distinguibilidade, ou seja, métodos que conseguem diferenciar dois indivíduos, identificando-os corretamente. Tais métodos desempenham com eficiência o objetivo comum da biometria, que é a identificação de um indivíduo (TEIXEIRA, 2011). Devido a essa característica, eles costumam ser muito utilizados para a identificação, como, por exemplo, na criação de documentos ou cadastro de funcionários. Porém, esses métodos necessitam da colaboração do sujeito que está a ser identificado, o que nem sempre é o caso.

O reconhecimento facial é uma área da visão computacional que se apresenta em constante evolução, tornando-se um importante referencial para o desenvolvimento de aplicações na área de segurança e gestão administrativa. Na área de segurança, mais precisamente na área de segurança pública, o reconhecimento facial é utilizado como ferramenta de apoio na identificação de suspeitos que já praticaram algum tipo de ato ilícito, ou que possuem ficha policial, cujas características da face se encontram armazenadas em uma base de imagens da polícia. O reconhecimento facial é também utilizado por empresas no controle de acesso a lugares restritos (PRODOSSIMO; CHIDAMBARAM; LOPES, 2011).

Em 2012, o TJDFT implantou um projeto estratégico que utilizava os modernos recursos da biometria para fazer o reconhecimento, de forma precisa, da imagem de pessoas. Instalado inicialmente na Vara de Execução das Penas e Medidas Alternativas – Vepema, o Projeto de Controle Biométrico para Benefícios de Penas (Probio) é pioneiro no Judiciário e tinha como objetivo conferir maior segurança e agilidade à identificação de apenados que precisam comparecer bimestralmente em Juízo. Em 2019, o TJDFT instituiu o projeto Ámon, a fim de iniciar os estudos de técnicas de reconhecimento facial, contribuindo com a segurança e modernização do tribunal.

3 Sistema Ámon

Nesta seção, descrevemos em mais detalhes o sistema Ámon. Na primeira parte, há uma breve explanação sobre a motivação em construí-lo. Em seguida, detalhamos o funcionamento e as particularidades, dando destaque também à integração com o sistema SidenWeb, sistema de controle de acesso do TJDFT.

3.1 Motivação

Partindo de uma visão ampla, o TJDFT, por meio de suas áreas técnicas, tem buscado o estudo e desenvolvimento de projetos de automação e inteligência artificial para cada vez mais modernizar os processos da Casa.

Um exemplo dessas iniciativas é o sistema Hórus (MELO; NEVES; CAVALCANTE, 2019), desenvolvido pelo Serviço de Ciência de Dados (SERCID). O Hórus auxilia nas atividades de identificação, classificação, correção, assinatura, carga e registro de novos processos da Vara de Execução Fiscal do DF, que passam a tramitar de modo digital. Tudo isso de forma automatizada

O Ámon surgiu de uma parceria do SERCID com a Assessoria de Segurança Institucional (ASI) do TJDFT. A demanda da ASI possuía como objetivo a implementação de um sistema de reconhecimento facial, a partir de fotografias, para trazer mais segurança ao TJDFT. O sistema a ser desenvolvido deveria integrar-se ao SidenWeb (https://sidenweb.tjdft.jus.br/), software do Tribunal que gerencia o controle integrado de acesso às suas dependências.

Nas próximas seções, serão detalhadas as características do Ámon, assim como seu modo de funcionamento. Também será descrito de que forma ocorre a integração com o SidenWeb.

3.2 Características e funcionamento

Uma das principais características do sistema Ámon é ter sido desenvolvido sem nenhum custo para o Tribunal de Justiça do DF. Foi utilizada para sua construção a linguagem de programação *Python* (PYTHON, 2020), assim como várias de suas bibliotecas (módulos) de apoio, sendo a principal a biblioteca *face recognition* (FACE RECOGNITION LIBRARY, 2020).

O *Python* é uma linguagem de programação de alto nível, multiparadigma, que possui um modelo de desenvolvimento aberto, comunitário, gerenciado pela *Python Software Foundation* (*Python Software Foundation*, 2020), uma organização sem fins lucrativos, cuja missão é "promover, proteger e evoluir a linguagem de programação *Python*, suportar e facilitar o crescimento de uma comunidade de programadores *Python* diversificada e internacional."[1].

Outra característica importante do Ámon é ser um sistema *RESTful*, ou seja, que segue os princípios da arquitetura REST (*Representational State Transfer*) (COSTA; PIRES; DELICATO; MERSON, 2014) (FENG; SHEN; FAN, 2009) (FIELDING, 2000). O REST é um estilo de arquitetura da web que define regras e restrições para sua utilização como serviço independente.

O Ámon fornece interfaces bem definidas para que outras aplicações possam se comunicar com ele, utilizando seus serviços, ou seja, fornece interoperabilidade entre sistemas na internet, a partir de métodos do protocolo HTTP (*Hypertext Transfer Protocol*) (BERNERS-LEE *et al*, 1996). No caso do Ámon, seus serviços são acessados pelos métodos *Get* (reconhecimento) e *Post* (vetorização). Esses serviços serão detalhados mais adiante.

O que vale adiantar neste momento são as restrições do serviço de reconhecimento facial. O Ámon aceita que seja enviada apenas uma foto por vez para que seja reconhecida, e esse arquivo da foto deve ter um tamanho de no máximo 2 megabytes.

3.2.1 Representação das fotos

De forma bem resumida e objetiva, a principal funcionalidade do Ámon é tentar reconhecer facialmente uma pessoa a partir de uma foto. Vamos detalhar de que forma isso acontece.

Primeiramente, para que possa haver uma tentativa de reconhecimento facial a partir de uma foto de entrada, é necessário que existam outras fotos para serem buscadas e comparadas. A comparação entre fotografias não ocorre com as imagens em si, mas sim com representações numéricas destas. Portanto, uma premissa básica do reconhecimento facial no Ámon é que as fotos sejam traduzidas para uma representação numérica.

Essa representação numérica é uma codificação das características da face de uma pessoa, como, por exemplo a distância entre as orelhas, entre os olhos, a distância do queixo até a ponta do nariz, etc.

Não são as fotos completas que são traduzidas, mas sim as faces localizadas nessas fotos. A ordem para que as fotos estejam prontas para serem utilizadas pelo Ámon está ilustrada na Figura 1. O Ámon trabalha internamente com as representações numéricas.

Figura 1 – Fluxo ilustrativo de transformação de imagem do Ámon

Fonte: elaborada pelos autores.

Nesse ponto, trabalhamos com o módulo *face recognition* do *Python*. Num primeiro momento utilizamos um de seus métodos, o qual nos retorna a localização da face humana em uma imagem. Na sequência, interagimos com outro método da biblioteca, que recebe uma imagem e a localização da face e nos retorna um vetor numérico representativo da face de 128 dimensões. Esse vetor é chamado de *encoding* da face, e o processo completo nós chamamos de vetorização da imagem.

Como informamos anteriormente, devem existir outras fotos para comparação e reconhecimento de uma imagem de entrada. O processo de vetorização da imagem finaliza com o armazenamento do *encoding* em um arquivo central. Esse arquivo central é a base de fotos do Ámon, composta por representações numéricas (vetores) de faces.

3.2.2 Parâmetros de configuração

Antes de descrevermos a lógica dos serviços do Ámon, vamos abordar nesta seção quais parâmetros são necessários para configuração do sistema. Tais parâmetros

1 Traduzido livremente de: https://www.python.org/psf/. Acesso em: 7 ago. 2020.

possuem influência na maneira como o reconhecimento facial é executado.

O primeiro parâmetro é a forma como as faces devem ser localizadas numa foto, e é necessário ser informado no método correspondente da biblioteca *face recognition*. Esse método recebe como entrada uma imagem e o modo de detecção de faces. São dois os possíveis modos: HOG (*Histogram of Oriented Gradients*/Histograma de Gradientes Orientados) (DALAL; TRIGGS, 2005) (EBRAHIMZADEH; JAMPOUR, 2014) (NEWELL; GRIFFIN, 2011) (RYBSKI; HUBER; MORRIS; HOFFMAN, 2010) ou CNN (*Convolutional Neural Network*/Rede Neural Convolucional) (FARFADE; SABERIAN.; LI, 2015) (GUO; WANG; YAN; ZHENG; LI, 2020) (LI *et al*., 2015) (MATSUGU; MORI; MITARI; KANEDA, 2003) (RANJAN; SANKARANARAYANAN, 2017). O valor desse parâmetro é configurado na aplicação.

O modelo HOG é um descritor de características, ou seja, simplifica uma imagem extraindo dela informações úteis para uma aplicação. É utilizado em processamento de imagens para detecção de objetos. Na nossa realidade, o HOG, portanto, é utilizado para detectar faces em uma foto.

O modelo CNN é uma classe de rede neural que vem sendo aplicada de forma bem sucedida na análise e processamento de imagens. Enquanto o HOG possui uma boa *performance* para detecção de faces frontais em fotos, o CNN é capaz de localizar faces em ângulos variados.

A grande diferença entre os dois modelos, para o sistema Ámon, é a seguinte:

- HOG: Menos preciso, mais limitado, mais rápido;
- CNN: Mais preciso, mais robusto, mais lento.

O segundo e último parâmetro necessário para o funcionamento do Ámon é a tolerância do reconhecimento facial ou acurácia desejada. A utilização desse parâmetro será melhor compreendida na próxima seção.

Esse parâmetro é um número entre 0 e 1 (inclusive), o qual é configurado na aplicação e utilizado por padrão nos processos de reconhecimento. Porém, há também a possibilidade de o usuário informar esse valor pontualmente para uma busca facial específica. Caso o usuário opte por informar esse valor, este terá preferência na execução, ou seja, será utilizado no procedimento de reconhecimento facial em vez do valor configurado na aplicação.

3.2.3 Lógica do reconhecimento facial

Nesta seção explicaremos como funciona o reconhecimento facial no Ámon. Revisando o que comentamos anteriormente, os serviços do Ámon são fornecidos por meio de métodos HTTP. O reconhecimento facial é acessado a partir do método *Get*. Esse serviço recebe um parâmetro obrigatório (uma foto) e um parâmetro opcional (valor da acurácia). A foto deve possuir no máximo 2MB, e deve ser enviada uma foto por requisição.

O serviço de reconhecimento facial do Ámon inicia com essas checagens (quantidade de fotos e tamanho do arquivo). Após isso, é validada a qualidade da foto enviada. O Ámon retorna um erro para o usuário se:

- O arquivo da foto estiver corrompido;
- Não for possível detectar uma face na foto:
  - qualidade baixa da imagem;
  - foto sem pessoa;
  - face em um ângulo/posição de difícil detecção, etc.

Caso nesse ponto nenhum erro seja retornado, a foto é considerada válida, sendo portanto possível detectar uma face. Com a face detectada, é gerada a sua representação numérica. É com essa representação que a busca na base de fotos é realizada.

Utilizando novamente a biblioteca *face recognition* do *Python*, conseguimos calcular a distância entre as faces, ou seja, a distância entre os vetores de *encoding*. Esse método de distância recebe dois parâmetros: a representação numérica de uma face (nossa imagem de entrada) e um conjunto de vetores numéricos para busca e comparação (nossa base de fotos).

O retorno desse método é um conjunto de números, que são as distâncias da nossa imagem de entrada para cada imagem da base de dados. O valor da distância é um número entre 0 e 1, inclusive. Quanto menor esse valor mais similar uma face é de outra. Portanto, de todas as distâncias retornadas, interessa-nos recuperar a menor distância.

Recuperar a menor distância significa recuperar a face da base de dados mais similar à nossa face de entrada. Isso não significa (ainda) que o reconhecimento facial retornou uma pessoa. Nesse momento o

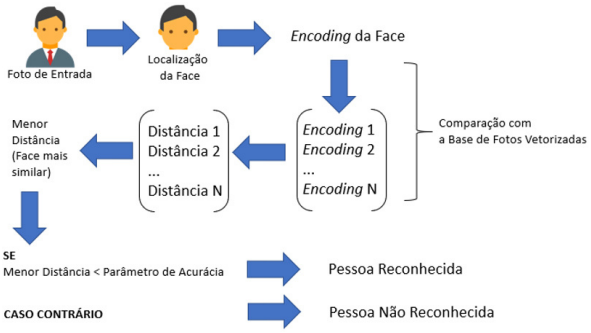
Ámon realiza uma comparação, a da menor distância recuperada com o parâmetro de acurácia (seja o da aplicação, seja o informado pelo usuário).

Caso o valor recuperado da menor distância seja menor ou igual ao parâmetro da acurácia, consideramos que o reconhecimento facial encontrou uma pessoa para a imagem fornecida como entrada. Caso contrário, informamos que o reconhecimento facial não encontrou ninguém para a foto fornecida.

Assim, podemos notar a importância do parâmetro de tolerância. Baseado em experimentos, podemos definir um valor padrão de calibragem e confiabilidade do Ámon (mais detalhes na seção de resultados). Um valor de distância sempre é retornado na comparação da foto com a base, porém nosso parâmetro de tolerância certifica-se de que a foto localizada é ou não uma ocorrência verdadeira de reconhecimento facial.

Por exemplo, se ao enviarmos uma foto para reconhecimento, a face que mais se aproxima da nossa tem uma distância de 0.45, essa distância ainda é razoavelmente longe de 0, portanto há uma grande chance de que nossa foto não foi reconhecida na base. Ao compararmos essa distância com nosso parâmetro, digamos, de 0.35, o Ámon informa ao usuário que a sua imagem não foi reconhecida. O processo de reconhecimento facial está ilustrado na Figura 2.

Figura 2 – Fluxo do Reconhecimento Facial do Ámon



Fonte: elaborada pelos autores.

3.2.4 Serviço de vetorização

além do reconhecimento facial, o Ámon disponibiliza outro serviço, acessado a partir do método *Post*. É o serviço de vetorização de imagens. Deve ser enviada uma imagem por requisição.

Assim como o serviço de reconhecimento facial, a vetorização também afere a qualidade da foto, ou seja, se o arquivo estiver corrompido ou não for possível detectar uma face na foto, é retornada uma mensagem de erro ao usuário.

O procedimento segue o mesmo raciocínio da preparação da foto para o reconhecimento facial. Utilizando a biblioteca *face recognition*, a face é localizada na foto, e então é gerada uma representação numérica.

A grande diferença é o objetivo final. Após a geração do *encoding* da imagem, este é armazenado no nosso arquivo central de fotos, ou seja, é realizado um incremento da base. Isso é muito importante para aumentar a qualidade e precisão do Ámon, pois com o passar do tempo a base de fotos está sendo enriquecida com mais imagens.

Temos então os seguintes cenários a partir do serviço de vetorização:

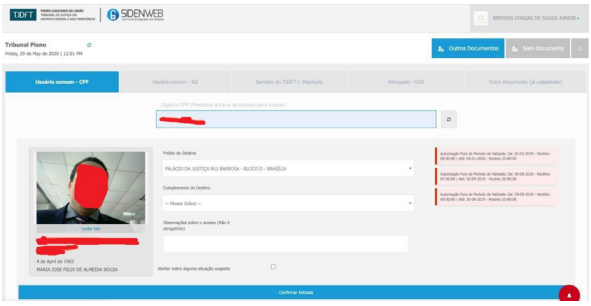
1) Mais fotos de pessoas diferentes, o que aumenta o universo de pessoas que podem ser reconhecidas pelo Ámon;
2) Mais fotos diferentes da mesma pessoa, o que aumenta a chance de essa pessoa ser reconhecida pelo Ámon, pois a similaridade de uma foto dela qualquer será calculada com diversas candidatas, possivelmente em diferentes ângulos.

3.2.5 Integração com o sidenweb

O Ámon foi desenvolvido pelo Serviço de Ciência de Dados do TJDFT, numa parceria com a Assessoria de Segurança Institucional. Essa demanda tinha como objetivo principal trazer mais segurança à integridade física dos membros do TJDFT.

Desde junho de 2020 o Ámon está em operação no Tribunal de Justiça do DF (https://www.tjdft.jus.br/institucional/imprensa/noticias/2020/junho/tjdft-aprimora-seguranca-com-implantacao-de-sistema-de-reconhecimento-facial-para-controle-de-acesso-de-visitantes). O sistema está funcionando de forma integrada com o SidenWeb, software da segurança do Tribunal que gerencia o controle integrado de acesso às suas dependências. A tela de informações de visitante do SidenWeb está ilustrada na Figura 3.

Figura 3 – Tela de informações de visitante do SidenWeb



Fonte: elaborada pelos autores.

O SidenWeb funciona nas portarias do Tribunal. Quando uma pessoa chega às dependências do TJDFT, ela se identifica na portaria com sua documentação e informa seus dados, como nome e CPF, para a criação de um novo cadastro, caso ainda não o possua. A pessoa também é solicitada a tirar uma foto.

A cada nova visita da pessoa ao Tribunal, a sua foto deve ser atualizada. O histórico das fotos é mantido numa base de dados própria do SidenWeb. A sua documentação sempre é conferida com o cadastro existente. Portanto, para conferência e detecção de possíveis fraudes, o SidenWeb baseia-se nos metadados da pessoa, como o CPF ou número da identidade. Por exemplo, uma fraude é apontada caso alguém apresente um documento pertencente a outra pessoa.

A integração do Ámon com o SidenWeb funciona conforme ilustrado na Figura 4.

Figura 4 – Fluxograma de integração SidenWeb/Ámon

Fonte: elaborada pelos autores.

A integração funciona da seguinte forma: quando a foto de uma pessoa é tirada na portaria, será realizado o seu reconhecimento facial, e sua foto será vetorizada e adicionada na base de fotos do Ámon.

Para o reconhecimento positivo ou não, são utilizadas duas medidas de acurácia. A primeira é o parâmetro que já discutimos, definido no próprio sistema Ámon. A medida de similaridade/distância entre as fotos deve estar abaixo desse parâmetro para ser considerado um possível reconhecimento positivo.

Como estratégia da integração, há outra medida de tolerância definida no SidenWeb, com valor abaixo da que está definida no Ámon. Podemos entender que a primeira medida, do Ámon, funciona como uma triagem, e a segunda medida, do SidenWeb, confirma a veracidade do reconhecimento facial, para dar mais segurança ao resultado.

Caso a menor medida de similaridade entre a foto de uma pessoa e a base de fotos esteja abaixo das duas métricas, é considerado automaticamente que há um reconhecimento positivo. Caso essa menor medida esteja acima da acurácia do SidenWeb, esse reconhecimento é separado para uma confirmação manual.

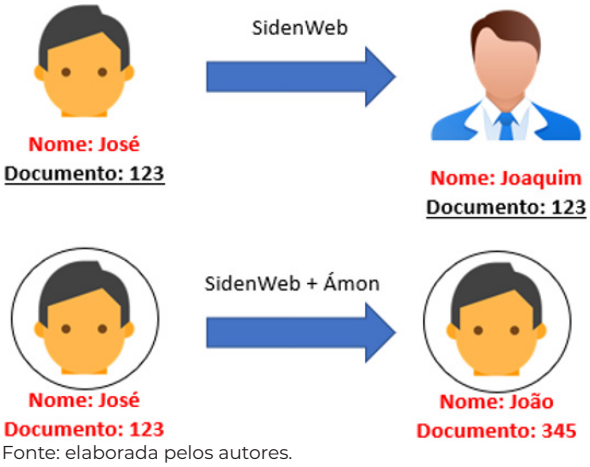
Em ambos os casos, caso se trate da mesma pessoa, a foto é adicionada tanto na

base do SidenWeb como vetorizada na base do Ámon. Caso não se trate da mesma pessoa, há um possível indício de fraude detectado. Com isso, temos como detectar fraudes além da conferência dos dados de uma pessoa.

Com o SidenWeb, a partir de dados documentais, tentava-se conferir se aqueles dados realmente eram daquela pessoa a partir de uma conferência na base de dados do sistema. Com o Ámon integrado, é possível detectar problemas a partir da foto da pessoa. Se a foto reconhecida do sistema juntamente com os registros recuperados exibirem dados de documentos diferentes dos apresentados, temos um indício de fraude, ou seja, aquela mesma pessoa já visitou o Tribunal antes portando documentos diferentes.

O resumo das detecções de fraudes discutidas aqui encontra-se ilustrado na Figura 5.

Figura 5 – Detecção de Fraudes no SidenWeb e Ámon



Fonte: elaborada pelos autores.

4 resultados

Nesta seção, ilustraremos os resultados alcançados com a operacionalização do Ámon no TJDFT. É importante destacar que todo o processo de desenvolvimento e testes da ferramenta foi conduzido pelos autores. Os dados e estatísticas apresentados nesta seção são oriundos desses experimentos.

O sistema Ámon encontra-se operacional desde junho de 2020, nas portarias do TJDFT (Fórum Desembargador Milton Sebastião Barbosa). A homologação e os testes foram realizados pela Assessoria de Segurança Institucional, tanto do Ámon isoladamente quanto da sua integração com o SidenWeb. A Figura 6 ilustra a interface de testes do Ámon.

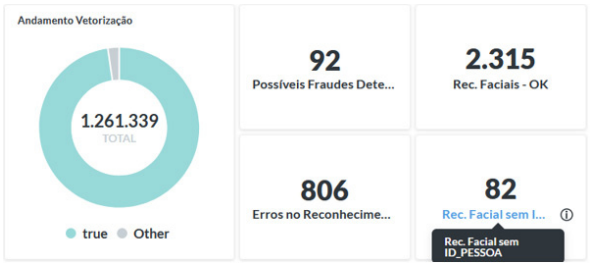
Figura 6 – Interface de Testes do Ámon

Fonte: elaborada pelos autores.

Quando uma foto é encontrada/reconhecida na base, além de a foto correspondente ser retornada, o Ámon também recupera alguns metadados da pessoa encontrada: Identificador da base do SidenWeb, Nome e CPF, conforme ilustrado na Figura 6.

Além dos testes e homologação, para que pudéssemos operacionalizar o Ámon, era necessário montar a sua base de fotos, com imagens de faces vetorizadas. Para isso, utilizamos a própria base de dados do SidenWeb, que possui fotos de visitantes e servidores do TJDFT. No momento da entrega do Ámon, a sua base continha cerca de 1 milhão e 261 mil registros vetorizados de fotos, conforme detalhamento do painel de indicadores[2] descrito na Figura 7.

Figura 7 – Indicadores de processamento do SIDEN



Fonte: elaborada pelos autores.

O tempo médio de processamento dos serviços do Ámon é:

- Reconhecimento Facial: cerca de 10 segundos, sendo que 7 segundos são contabilizados na localização da face na imagem de entrada com o algoritmo CNN. O restante do tempo é utilizado para a busca da face vetorizada pela face mais próxima na base de fotos;
- Vetorização: cerca de 12 segundos, sendo que 7 segundos são contabili-

2 *Dashboard* de indicadores de reconhecimento facial do SIDEN. Disponível em: https://metabase-asi.apps.tjdft.jus.br/public/dashboard/5e87cac9-6894-44c2-8af1-1a3309111dc3.

zados na localização da face na imagem de entrada com o algoritmo CNN. O restante do tempo é utilizado para o incremento e persistência da base atualizada de fotos do Ámon.

Optamos pela utilização do algoritmo CNN, pois apesar de ter o seu processamento mais lento, é mais preciso e robusto do que o algoritmo HOG. Por exemplo, com a utilização do algoritmo CNN para a localização de faces nas fotos para posterior reconhecimento facial, obtivemos sucesso em casos diversos como:

- rosto não totalmente frontal;
- pessoa utilizando máscara;
- pessoa com máscara no queixo;
- pessoa com óculos.

Em geral, nos testes realizados, foram poucas as ocorrências de erros no processamento da foto, ou seja, na impossibilidade de definição da face. Nos experimentos conduzidos pelo SERCID, em maio de 2020, foram detectados alguns erros, entre eles: a) foto sem face e b) foto de baixa qualidade. Nessa condição, é solicitada à pessoa que tire outra foto. Após a implantação do sistema, a taxa de erro[3] está em torno de 25,16% que pode ser computada pela quantidade de erros no reconhecimento dividido pela soma de: a) reconhecimento facial (ok); b) erros no reconhecimento e c) reconhecimento facial sem cadastro. Essas variáveis estão descritas em termos quantitativos na Figura 7.

O valor de tolerância/acurácia também foi definido a partir dos testes realizados. Vale lembrar que esse valor pode ser configurado a qualquer tempo no sistema Ámon bem como podemos informar um valor diferente a cada requisição do serviço de reconhecimento facial. A conclusão que obtivemos sobre esse parâmetro foi o de serem utilizados valores baixos, próximos de 0 (zero), para uma maior confiabilidade na ocorrência de um reconhecimento. C o m o mencionamos na seção 3.2.5, caso o valor de similaridade/distância retornado seja abaixo do valor definido no Ámon, a ocorrência é considerada um potencial reconhecimento verdadeiro, pois ainda trabalhamos com um segundo valor de tolerância definido no SidenWeb, com valor abaixo do definido no Ámon.

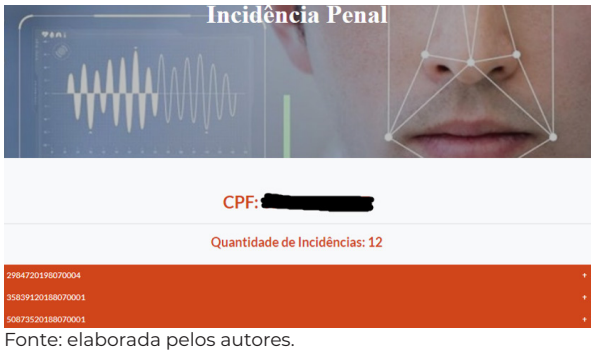
3 *Dashboard* de indicadores de reconhecimento facial do SIDEN. Disponível em: https://metabase-asi.apps.tjdft.jus.br/public/dashboard/5e87cac9-6894-44c2-8af1-1a3309111dc3.

5 Perspectivas futuras

Com a operacionalização do sistema Ámon para reconhecimento facial a partir de fotos, podemos pensar em outros sistemas e aplicações. Como pode-se observar tendo por base a interface do Ámon (Figura 5), podemos imaginar outras integrações com o sistema, a partir dos metadados retornados do reconhecimento facial.

Por exemplo, a partir do CPF da pessoa localizada, é possível conferirmos se esta pessoa possui alguma incidência penal ou conferir a existência de algum registro no Sistema Eletrônico de Execução Unificado (SEEU)[4]. Os primeiros testes já foram realizados. A Figura 8 mostra o retorno de incidências penais a partir de uma consulta pelo CPF de uma pessoa.

Figura 8 – Consulta de Incidências Penais



Fonte: elaborada pelos autores.

Outra ideia que vem sendo trabalhada é aplicar o reconhecimento facial em vídeos ao vivo de câmeras do Tribunal. Experimentos também já vêm sendo realizados, utilizando-se praticamente as mesmas bibliotecas do *Python* aplicadas no Ámon com fotos. Isso fortalece ainda mais a questão da segurança para todos os frequentadores do TJDFT. Podemos, por exemplo, verificar se alguma pessoa possui ou não permissão para frequentar determinados locais da Casa.

Com o reconhecimento facial a partir de câmeras, a perspectiva é expandir o Ámon para outras localidades, como, por exemplo, as Varas Penais. Na carceragem, poderíamos imaginar o Ámon realizando reconhecimento facial por vídeo nas visitas de advogados, atestando a veracidade da documentação com a pessoa que os apresenta, além da permissão que aquele profissional tenha de realizar as visitas.

A Vara de Execuções das Penas em Regime Aberto – VEPERA jurisdiciona pessoas que cumprem penas privativas de liberdade em prisão domiciliar ou que foram

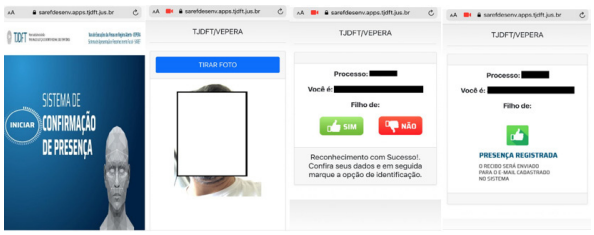
4 Disponível em: https://seeu.pje.jus.br/seeu/.

beneficiadas pela suspensão da pena (*sursis* penal) ou pelo livramento condicional. O contingente jurisdicionado alcança mais de 20 mil pessoas, as quais comparecem regularmente ao Fórum Mirabete para cumprimento das condições impostas no momento da concessão do benefício. Essa situação, que muito ocupa e preocupa a VEPERA, adquiriu maior relevância e urgência com o advento da pandemia da covid-19.

O distanciamento social recomendado em face da Pandemia persistirá por tempo substancial e, provavelmente, exigirá a modificação de muitas das atividades realizadas pela VEPERA. As atividades presenciais na Vara encontram-se suspensas no momento, e isso significa que as condições impostas aos jurisdicionados padecem do acompanhamento e das respostas exigidas ao efetivo cumprimento da reprimenda penal. As atividades impactantes que reclamam atenção imediata, são três: (i) Apresentações Bimestrais; (ii) Fiscalização de Recolhimento Domiciliar; e (iii) Atendimento no Balcão da Vara.

Nesse sentido, a construção de um sistema que possibilite a apresentação de apenados de forma remota já está em curso, como pode ser observado na Figura 9.

Figura 9 – Projeto para apresentação remota de apenados



Fonte: elaborada pelos autores.

(a) tela de inicialização do sistema, (b) console base do fluxo de apresentação com ativação da câmera e localização do dispositivo do apenado, (c) reconhecimento facial baseado no projeto Amon e (d) encaminhamento da presença do apenado.

6 Conclusão

Apesar de implantação recente, o Ámon tem apresentado resultados satisfatórios quanto à aplicação de reconhecimento facial nas dependências do TJDFT, onde a taxa de efetividade[5] está em torno de 72,27%, que pode ser computada pela quantidade de reconhecimento facial (ok) dividido pela soma de: a) reconhecimento facial (ok); b) erros no reconhecimento e c) reconhecimento facial sem cadastro. Essas variáveis estão descritas em termos quantitativos na Figura 7.

5 *Dashboard* de indicadores de reconhecimento facial do SIDEN. Disponível em: https://metabase-asi.apps.tjdft.jus.br/public/dashboard/5e87cac9-6894-44c2-8af1-1a3309111dc3.

A robustez na execução do reconhecimento em vários cenários (máscara, óculos, etc.) nos faz vislumbrar um futuro promissor com relação à melhoria da segurança no Tribunal.

A checagem de segurança dos visitantes do Tribunal foi enriquecida com o Ámon. Além da verificação a partir de metadados, como CPF, agora é possível realizar uma conferência de cada pessoa a partir do reconhecimento facial, trazendo maior controle sobre quem entra na Casa.

Devemos também ressaltar outras vantagens como o fato de a ferramenta ter sido desenvolvida sem custos para o TJDFT, utilizando a linguagem *Python*, cada vez mais empregada pelos profissionais de Ciência de Dados e Inteligência Artificial. Por se tratar de um sistema *RESTful*, o Ámon pode ser integrado a outras ferramentas, além do SidenWeb.

As perspectivas futuras também são animadoras. Foram iniciados estudos e meios de se trabalhar com outras integrações a partir do reconhecimento facial, como a checagem de incidências penais, a aplicação do Ámon em vídeos de câmeras ao vivo.

As parcerias da área de Tecnologia da Informação com outros setores do TJDFT reforçam o objetivo da Casa de melhoria e modernização dos seus sistemas, processos e atividades.

Referências

AGÊNCIA BRASIL. **Tecnologias de Reconhecimento Facial são usadas sem 37 cidades no país**. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2019-09/tecnologias-de-reconhecimento-facial-sao-usadas-em-37-cidades-no-pais/. Acesso em: 9 ago. 2020.

BERNERS-LEE, Tim *et al*. ***Hypertext Transfer Protocol* – HTTP/1.0**. Internet Engineering Task Force. 1996. Disponível em: https://www.ietf.org/rfc/rfc1945. Acesso em: 7 ago. 2020.

BOECHAT, G. C. **Investigação de um modelo de arquitetura biométrica multimodal para identificação pessoal**. Recife, 2008, Dissertação (Mestrado em Ciência da Computação). Universidade Federal de Pernambuco. Recife, 2008.

COSTA, B.; PIRES, P.; DELICATO, F.; MERSON, P. **Evaluating a representational state**

transfer (rest) architecture. What is the impact of rest in my architecture? In Software Architecture (WICSA), 2014 IEEE/IFIP Conference on, pages 105-114, Sydney, NSW.

DALAL, Navneet; TRIGGS, Bill. **Histograms of Oriented Gradients for Human Detection**. In Computer Vision and Pattern Recognition, 2005. CVPR 2005. IEEE Computer Society Conference on, volume 1, p. 886–893. IEEE, 2005.

EBRAHIMZADEH, R.; JAMPOUR, M. **Efficient handwritten digit recognition based on histogram of oriented gradientes and svm**. International Journal of Computer Applications, vol. 104, pp. 10-13, October 2014.

FACE RECOGNITION LIBRARY. **Recognize and manipulate faces from *Python* or from the command line with the world's simplest *face recognition* library**. Disponível em: https://github.com/ageitgey/face_recognition. Acesso em: 7 ago. 2020.

GUIMARÃES, R. M. **Desenvolvimento de um protótipo de software de reconhecimento facial de tempo real para registro eletrônico de ponto em ambientes indoor com utilização do dispositivo *kinect***, Belo Horizonte, 2015. Dissertação (Mestrado profissional em sistemas de informação e gestão do conhecimento).

FARFADE, S. S.; SABERIAN, M. J.; LI, L. J. **Multi-view face detection using deep convolutional neural networks**. ACM Int. Conf. Multimedia Retrieval, pp. 643-650, 2015.

FENG, X.; SHEN J.; FAN Y. **REST: An alternative to RPC for Web services architecture**. Proc. 1st Int. Conf. Future Inf. Netw. (ICFIN), pp. 7-10, Oct. 2009.

FIELDING, Roy Thomas. **Architectural Styles and the Design of Network-based Software Architectures**. PhD Dissertation. Dept. of Information and Computer Science, University of California, Irvine. Chapter 5, p. 76-106, 2000.

GUO, G.; WANG, H.; YAN, Y.; ZHENG, J.; LI, B. **A fast face detection method via convolutional neural network**. In: Neurocomputing, vol. 395, June 2020, pp. 128-137.

IMPACTA. **Você sabe como funciona o Reconhecimento Facial?** Disponível em: https://www.impacta.com.br/blog/voce-sabe-como-funciona-o-reconhecimento-facial/. Acesso em: 8 ago. 2020.

LI, Haoxiang *et al*. **A convolutional neural network cascade for face detection**. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2015, pp. 5325-5334.

MATSUGU, M.; MORI, K.; MITARI, Y.; KANEDA, Y. **Subject independent facial expression recognition with robust face detection using a convolutional neural network.** Neural Netw., vol. 16, no. 56, pp. 555-559, Jun-Jul 2003.

MELO, Jairo; NEVES, Thiago; CAVALCANTE, Weiss. Hórus – processamento inteligente dos dados digitalizados da vara de execução fiscal do Distrito Federal. **Revista Eletrônica do CNJ**, v. 3, n. 1, p. 51-64, 2019.

NEWELL, A. J.; GRIFFIN, L. D. **Multiscale histogram of oriented gradient descriptors for robust character recognition**. In: ICDAR, pages 1085-1089. IEEE, 2011.

PRODOSSIMO, F. C.; CHIDAMBARAM, C.; LOPES, H. S. **Otimização da detecção de olhos em imagens faciais utilizando os algoritmos colônia de abelhas artificiais e *harmony search***. Anais do X Congresso Brasileiro de Inteligência Computacional, Fortaleza, 2011.

OLHAR DIGITAL. **Reconhecimento Facial: o que se pode esperar dele?** Disponível em: https://olhardigital.com.br/2019/03/23/noticias/reconhecimento-facial-o-que-se-pode-esperar-dele/. Acesso em: 9 ago. 2020.

PYTHON. **The official home of the python programming language**. Disponível em: https://www.python.org/. Acesso em: 7 ago. 2020.

Python Software Foundation. **The organization behind *Python***. Disponível em: https://www.python.org/psf/. Acesso em: 7 ago. 2020.

RANJAN, R.; SANKARANARAYANAN, S. **An all-in-one convolutional neural network for face analysis**. In 12th IEEE International Conference on Automatic Face & Gesture Recognition (AFGR), 2017.

RUNRUN. **O Reconhecimento Facial vai afetar a publicidade e a sua vida**. Disponível em: https://blog.runrun.it/reconhecimento-facial/. Acesso em: 8 ago. 2020.

RYBSKI, P.; HUBER, D.; MORRIS, D.; HOFFMAN, R. **Visual classification of coarse vehicle orientation using histogram of oriented gradiente features**. Proc. IEEE IV Symp., pp. 921-928, 2010-Jun.

SANTOS, D. V. **Predição de *links* em redes de coautoria: um estudo utilizando a teoria da evolução espectral em redes complexas.** Dissertação (Mestrado em Sistemas de Informação e Gestão do Conhecimento). Fa-

culdade de Ciências Empresariais (FUMEC). Belo Horizonte, 2014.

TEIXEIRA, R. F. da S. **Transformação multi--escala para segmentação de impressões digitais**. Dissertação (Mestrado em Ciência da Computação). Instituto de Computação, UNICAMP, Campinas, 2011.

Jairo Simão Santana Melo
Doutor em Engenharia Elétrica - Subárea de Automação (PGEA) pela Universidade de Brasília - UNB em (2012), Assessor de Ciência de Dados do TJDFT.

Thiago Arruda Neves
Mestrado em Ciência da Computação pela UFPE. Analista Judiciário no Serviço de Ciência de Dados do TJDFT.

Celso oliveira Neto
Secretário Geral do TJDFT