



Laboratório de Pesquisa e Desenvolvimento
do Registro Civil do Brasil

*em parceria com o Laboratório de Segurança em Computação
(LabSEC/UFSC)*

ANAIS DO I WORKSHOP ACADÊMICO DO
REGISTRO CIVIL (WARC 2025-1)

Aplicações de Inteligência Artificial
no Registro Civil



PDF Anais do WARC 2025



Vídeo do Workshop

Operador Nacional do Registro Civil do Brasil (ON-RCPN)

Florianópolis, Santa Catarina
Julho de 2025

Dados Internacionais de Catalogação na Publicação (CIP)

W926a Workshop Acadêmico do Registro Civil (1. : 2025 : Florianópolis, SC)

Anais do I Workshop Acadêmico do Registro Civil : Inteligência Artificial e Segurança da Computação [recurso eletrônico] / Workshop Acadêmico do Registro Civil (WARC) ; coordenação acadêmica Ricardo Custódio ; organização Operador Nacional do Registro Civil do Brasil (ON-RCPN), Laboratório de Pesquisa e Desenvolvimento do Registro Civil do Brasil (LabREC), Laboratório de Segurança em Computação (LabSEC/UFSC). – Florianópolis : UFSC, 2025.

XXX p. : il., color.

Inclui bibliografia.

ISBN 978-XX-XXXX-XXX-X

1. Inteligência artificial. 2. Segurança da computação. 3. Registro civil. 4. Proteção de dados. 5. Aprendizado de máquina. 6. Criptografia. 7. Reconhecimento óptico de caracteres. 8. Digitalização de documentos. 9. Preservação digital. I. Custódio, Ricardo. II. Operador Nacional do Registro Civil de Pessoas Naturais. III. Universidade Federal de Santa Catarina. Laboratório de Pesquisa e Desenvolvimento do Registro Civil do Brasil. IV. Universidade Federal de Santa Catarina. Laboratório de Segurança em Computação. V. Título.

CDD: 004.6

CDU: 004.056

Ficha catalográfica elaborada pela Biblioteca Universitária
da Universidade Federal de Santa Catarina

Organização

OPERADOR NACIONAL DO REGISTRO CIVIL DE PESSOAS NATURAIS - ON-RCPN

Presidente

Luis Carlos Vendramin Junior

Vice-presidente

Gustavo Renato Fiscarelli

COORDENAÇÃO ACADÊMICA

Ricardo Custódio

TUTORES

Gustavo de Castro Biage

Gustavo Zambonin

Matheus Saldanha

Wellington Fernandes Silvano

REVISÃO

Ricardo Custódio

Wellington Fernandes Silvano

Mensagem do Operador Nacional do Registro Civil de Pessoas Naturais

É com imensa satisfação e orgulho que o Operador Nacional do Registro Civil de Pessoas Naturais (ON-RCPN) parabeniza a realização do I Workshop Acadêmico do Registro Civil: Inteligência Artificial e Segurança (WARC 2025) e a publicação destes anais, que materializam o espírito inovador e a excelência técnica que devem nortear a modernização dos serviços registrais brasileiros.

A parceria estratégica estabelecida com o Laboratório de Pesquisa e Desenvolvimento do Registro Civil do Brasil (LabREC) e o Laboratório de Segurança em Computação (LabSEC) da Universidade Federal de Santa Catarina representa um marco na história do registro civil brasileiro. Esta colaboração exemplifica nosso compromisso com a inovação responsável, a pesquisa aplicada e o desenvolvimento de soluções tecnológicas que atendam às crescentes demandas da sociedade digital, sem jamais comprometer os direitos fundamentais dos cidadãos.

Os trabalhos aqui apresentados demonstram, de forma inequívoca, que a nova geração de profissionais da computação compreende não apenas os desafios técnicos da modernização registral, mas também suas implicações éticas, sociais e jurídicas. Cada prova de conceito desenvolvida pelos estudantes representa uma resposta criativa e tecnicamente sólida aos problemas reais enfrentados diariamente pelas serventias de registro civil em todo o território nacional.

Destacamos, com particular apreço, a maturidade com que foram abordadas questões sensíveis como a proteção de dados pessoais, a preservação da privacidade e a garantia da segurança da informação. Estes aspectos, fundamentais para a confiança pública no sistema registral, foram tratados não como obstáculos ao desenvolvimento tecnológico, mas como pilares estruturantes de soluções verdadeiramente sustentáveis e socialmente responsáveis.

A diversidade temática dos projetos abrangendo desde sistemas de autenticação biométrica até a digitalização de acervos históricos, passando por assistentes virtuais e plataformas de validação documental reflete a amplitude dos desafios que o registro civil enfrenta na era digital. Mais importante ainda, demonstra que existe uma geração de pesquisadores comprometida em encontrar soluções que conciliem eficiência operacional, segurança jurídica e proteção de direitos.

O ON-RCPN reconhece que iniciativas como o WARC 2025 são fundamentais para o desenvolvimento de um ecossistema de inovação robusto no setor registral. A pesquisa acadêmica de qualidade, quando alinhada às necessidades práticas das serventias, constitui o alicerce sobre o qual construiremos o futuro do registro civil brasileiro um futuro digital,

inclusivo, seguro e eficiente.

Agradecemos profundamente aos organizadores do workshop, aos professores e tutores envolvidos, e especialmente aos estudantes que dedicaram seu talento e energia a este projeto transformador. Agradecemos também ao LabREC, cuja visão estratégica e competência técnica tornaram possível esta parceria frutífera, e ao LabSEC, pela excelência acadêmica e pelo compromisso com a formação de profissionais qualificados.

Estes anais não representam apenas um registro das atividades desenvolvidas, mas constituem um verdadeiro mapa das possibilidades que se abrem para o registro civil brasileiro. Cada página documenta não apenas soluções técnicas, mas também o potencial transformador da colaboração entre academia, setor público e sociedade civil.

O ON-RCPN reafirma seu compromisso com a inovação responsável e com o apoio a iniciativas que promovam a excelência dos serviços registrais. Temos a convicção de que parcerias como esta são essenciais para garantir que o registro civil brasileiro continue sendo referência mundial em qualidade, segurança e acessibilidade.

Que este primeiro workshop seja o início de uma jornada longa e frutífera, na qual a pesquisa acadêmica e a prática registral caminhem juntas na construção de um sistema cada vez mais moderno, confiável e próximo dos cidadãos.

Luis Carlos Vendramin Junior

Presidente

Operador Nacional do Registro Civil de Pessoas Naturais

Gustavo Renato Fiscarelli

Vice-presidente

Operador Nacional do Registro Civil de Pessoas Naturais

Brasília, julho de 2025

Prefácio

É com grande satisfação que apresentamos os anais do I Workshop Acadêmico do Registro Civil: Inteligência Artificial e Segurança (WARC 2025). Este volume representa um marco na convergência entre pesquisa acadêmica de excelência e as demandas práticas do registro civil brasileiro, consolidando uma parceria estratégica que promete transformar profundamente a prestação de serviços registrais no país.

A iniciativa surge em um momento histórico no qual a digitalização dos serviços públicos deixou de ser uma aspiração para se tornar uma necessidade imperativa. O registro civil, como guardião dos dados mais fundamentais da cidadania, encontra-se no epicentro dessa transformação, enfrentando o duplo desafio de modernizar seus processos sem comprometer a segurança, a privacidade e a confiabilidade que caracterizam sua missão institucional.

Os trabalhos aqui reunidos transcendem o exercício acadêmico tradicional. Cada contribuição representa uma resposta tecnicamente fundamentada aos problemas reais enfrentados pelas serventias de registro civil, desde a proteção de dados sensíveis até a digitalização de acervos históricos, passando pela validação automatizada de documentos e pela implementação de sistemas de autenticação robustos. O que torna estas propostas particularmente valiosas é a maturidade com que abordam não apenas os aspectos técnicos, mas também as dimensões éticas, jurídicas e sociais inerentes à modernização do setor registral.

A diversidade temática dos projetos desenvolvidos reflete a amplitude dos desafios contemporâneos do registro civil. A interseção entre Inteligência Artificial e Segurança da Computação, fio condutor da disciplina que originou este workshop, revelou-se um campo fértil para a concepção de soluções inovadoras que conciliam eficiência operacional e proteção de direitos fundamentais. Esta abordagem holística é fundamental para assegurar que a transformação digital do registro civil seja verdadeiramente sustentável e socialmente responsável.

Cabe destacar o papel catalisador do Operador Nacional do Registro Civil de Pessoas Naturais (ON-RCPN) na consolidação desta iniciativa. Sua visão estratégica e seu compromisso com a inovação responsável não apenas viabilizaram a realização do WARC 2025, mas também estabeleceram as bases para uma colaboração duradoura entre academia e setor registral. O convênio estratégico mantido com o Laboratório de Pesquisa e Desenvolvimento do Registro Civil Brasileiro (LabREC) exemplifica como parcerias bem estruturadas podem gerar resultados que beneficiam tanto o avanço do conhecimento quanto a melhoria dos serviços prestados à sociedade.

A metodologia adotada na disciplina, centrada no desenvolvimento de Provas de Conceito (PoCs), demonstrou ser particularmente eficaz para formar profissionais capazes de

pensar criticamente sobre os impactos sociais da tecnologia. Os estudantes não apenas dominaram ferramentas técnicas avançadas, mas desenvolveram uma compreensão aguçada sobre a responsabilidade social inerente ao desenvolvimento de sistemas que lidam com dados pessoais e processos críticos para a cidadania.

Os resultados apresentados nestes anais evidenciam que é possível conceber soluções tecnológicas que sejam simultaneamente inovadoras e éticas, eficientes e seguras, modernas e respeitosas aos direitos fundamentais. Esta síntese, longe de ser trivial, representa o desafio central da transformação digital responsável no setor público.

Agradecemos profundamente ao ON-RCPN pela confiança depositada nesta iniciativa e pelo apoio incondicional ao desenvolvimento de pesquisas que visam ao aprimoramento do registro civil brasileiro. Estendemos nosso reconhecimento aos estudantes, cuja dedicação e criatividade tornaram possível este conjunto notável de contribuições, e aos tutores, cujo acompanhamento técnico e orientação metodológica foram fundamentais para a qualidade dos resultados alcançados.

Esperamos que esta compilação sirva como fonte de inspiração para futuras pesquisas e como referência para a implementação de soluções que modernizem, protejam e democratizem o registro civil brasileiro. Mais que um registro de atividades acadêmicas, estes anais constituem um convite à reflexão sobre o papel da tecnologia na construção de uma sociedade mais justa, inclusiva e transparente.

A Comissão Organizadora

Sumário

Lista de Figuras	xiii
Lista de Tabelas	xiv
Lista de Códigos	xv
Lista de Símbolos e Acrônimos	xvi
Parte I - Privacidade e Segurança da Informação no Contexto do Registro Civil	1
1 Da Proteção de Dados Sensíveis à Inteligência Operacional: Automação Segura no Registro Civil com IA	2
1.1 Introdução	2
1.2 Modelos <i>Transformers</i>	3
1.3 Princípios	5
1.4 Desenvolvimento do Sistema	5
1.4.1 Modelo Base	7
1.4.2 Framework de Desenvolvimento	8
1.4.3 Bibliotecas Principais	9
1.4.4 Componentes Principais	9
1.4.5 Sistema de Treinamento (<i>trainer.py</i>)	10
1.4.6 Sistema Criptográfico (<i>crypto_redaction.py</i>)	10
1.4.7 Interface de Usuário	12
1.4.8 Sistema de Treinamento	13
1.5 Potenciais Usos do Classificador Proposto no Registro Civil	14
1.6 Considerações Finais	15
2 Autenticação Biométrica por Impressão Palmar com Redes Neurais Profundas	17
2.1 Introdução	17
2.2 Metodologia	18
2.2.1 Etapas de Treinamento do Modelo	19
2.3 Extração da Região de Interesse	19
2.4 Extração de Características e Autenticação	20
2.4.1 Arquitetura do Modelo	20
2.4.2 Função de Perda	21

2.4.3	Processo de Autenticação	21
2.5	Bases de Dados	22
2.5.1	Treinamento do Modelo de Extração de Características	22
2.5.2	Treinamento dos Modelos de Aquisição da ROI	22
2.6	Resultados e Discussão	22
2.6.1	Desempenho da Extração da ROI	23
2.6.2	Desempenho do Modelo de Reconhecimento	23
2.7	Conclusão	24
3	Assistente Virtual Jurídico com Mecanismos Avançados de Garantia de Privacidade	26
3.1	Introdução	26
3.2	Objetivos do Projeto	27
3.3	Solução	27
3.4	Camada de Apresentação	29
3.5	Camada de Orquestração	29
3.6	Módulo de Processamento de Dados	30
3.7	Módulo de Geração da Resposta	30
3.8	Fluxo	31
3.9	Conclusão	31
4	Proteção de Registros Cíveis com Criptografia Pós-Quântica e Otimização Baseada em IA	33
4.1	Introdução	33
4.1.1	Justificativa do tema	34
4.1.2	Motivação	34
4.2	Revisão de artigos e ferramentas	34
4.3	Relato da disciplina e provas de conceito propostas	35
4.4	Prova de Conceito	37
4.5	Componentes utilizados	37
4.6	Aplicação e relevância	38
4.7	Conclusão	38
5	Autenticação Biométrica Segura com Provas de Conhecimento Zero	40
5.1	Introdução	40
5.2	Fundamentação Teórica	41
5.3	Proposta do Sistema	42
5.4	Componentes do Sistema	43
5.5	Funcionamento do Sistema	44
5.6	Fase de Registro	45
5.7	Fase de Autenticação	46
6	Classificação da Irredutibilidade de Pentanômios com Técnicas de Inteligência Artificial	48
6.1	Introdução	48

6.2	Revisão da literatura e estado da arte	48
6.2.1	Definição e relevância dos pentanômios irreduzíveis	49
6.2.2	Métodos clássicos de verificação de irreduzibilidade	49
6.2.3	Abordagens recentes e novos formatos de pentanômios	49
6.2.4	Métodos clássicos de verificação de irreduzibilidade	50
6.2.5	Engenharia reversa de polinômios em GF de hardware	50
6.2.6	Comparativo entre métodos tradicionais e abordagem via IA	50
6.2.7	Impacto prático em sistemas sensíveis	50
6.3	Desenvolvimento da Prova de Conceito (POC)	50
6.3.1	Tecnologias Utilizadas	51
6.3.2	Criação do Dataset	51
6.3.3	Organização do Dataset	51
6.3.4	Implementação do Classificador	52
6.3.5	Análise dos Resultados	52
6.4	Conclusão	52

Parte II - Qualidade, Integridade e Confiabilidade dos Dados no Registro Civil **54**

7	Verificação de Integridade e Autenticidade de Certidões de Nascimento	55
7.1	Introdução	55
7.2	Revisão da Literatura e Estado da Arte	56
7.3	Escopo do Projeto	56
7.4	Componentes do Sistema	57
7.5	Aquisição Textual de Documentos	58
7.5.1	Análise de Qualidade Visual com CLIP	58
7.5.2	Extração Óptica de Caracteres com EasyOCR e CRAFT	59
7.6	Extração e Organização de Dados Sensíveis	59
7.7	Verificação de Inconsistências para Emissão de Certidão de Nascimento	60
7.8	Conclusão	61
8	Sistema de Estatísticas Vitais com Integração de Inteligência Artificial	63
8.1	Introdução	63
8.2	Objetivos	64
8.2.1	Objetivo Geral	64
8.2.2	Objetivos Específicos	64
8.3	Metodologia	64
8.3.1	Etapas Metodológicas	65
8.3.2	Visão Geral do Fluxo de Processamento	65
8.4	Tecnologias Disponíveis	66
8.4.1	Frameworks de Inteligência Artificial	66
8.4.2	Tecnologias de Segurança	66
8.4.3	Tecnologias de Visualização e Interoperabilidade	66
8.5	Aspectos Legais e Éticos	67

8.5.1	Legislação Brasileira	67
8.5.2	Considerações Éticas	67
8.5.3	Diretrizes Internacionais Relevantes	68
8.6	Escopo e Delimitação do Projeto	68
8.7	Componentes do Sistema	69
8.7.1	Módulo de Processamento de Dados	70
8.7.2	Módulo de Integração com IA	70
8.7.3	Módulo de <i>Dashboard</i> e Visualização	70
8.7.4	Módulo de Banco de Dados	71
8.8	Arquitetura do Sistema	71
8.9	Conclusões	72
9	Verificação Automatizada de Documentos Utilizando Inteligência Artificial	74
9.1	Introdução	74
9.2	Prova de Conceito	75
9.3	Limitações	76
9.4	Conclusão	77
10	Aprendizado Federado Aplicado a Dados Vitais: Estudo de Caso em Santa Catarina	79
10.1	Introdução	79
10.2	Fundamentação Teórica	80
10.2.1	Análise Preditiva com Dados Vitais	80
10.2.2	Aprendizado Federado: Um Paradigma para a Privacidade	80
10.2.3	Arquitetura e Algoritmos do Aprendizado Federado	81
10.2.4	Vantagens e Desafios	81
10.3	Trabalhos Relacionados	82
10.4	Desenvolvimento da Prova de Conceito	83
10.4.1	Da Coleta ao Tratamento dos Dados	84
10.4.2	Arquitetura da Análise Comparativa	84
10.4.3	A Aplicação Web como Ferramenta de Demonstração	84
10.5	Resultados e Discussões	85
10.6	Aprendizados e Evolução Adquirida	85
10.7	Conclusão	86
Parte III - Preservação Digital e Gestão de Acervos Históricos do Registro Civil		88
11	Reconhecimento de Escrita Manuscrita em Documentos Históricos	89
11.1	Introdução	89
11.2	Trabalhos Relacionados	90
11.3	Metodologia	90
11.3.1	Construção do Conjunto de Dados	90

11.3.2	Modelo de HTR e Ambiente Experimental	91
11.4	Resultados e Discussão	91
11.5	Conclusão	92
12	Do Tinteiro ao Silício: Transcrição de Manuscritos Cursivos com Inteligência Artificial	94
12.1	Introdução	94
12.2	Fundamentos Teóricos	95
12.3	Resultados	96
12.4	Considerações Finais	97
13	Identificação de Estruturas Gráficas em Documentos Históricos com Aprendizado Federado	98
13.1	Introdução	98
13.2	Ferramentas Utilizadas	99
13.2.1	<i>Framework</i> Ultralytics	99
13.2.2	<i>Framework</i> Flower	99
13.2.3	UltraFlwr	99
13.2.4	COCO Annotator	99
13.3	Desenvolvimento da Prova de Conceito	100
13.3.1	Preparação do <i>Dataset</i>	100
13.3.2	Treinamento	101
13.4	Aplicação Web	102
13.5	Repositório do Projeto	103
13.6	Resultados Gerais	104
13.6.1	Métricas de Avaliação para Detecção de Objetos	104
13.6.2	Análise Quantitativa do Desempenho do Modelo	104
13.7	Discussão, Limitações e Aprendizados	105
13.8	Trabalhos Futuros	106

Lista de Figuras

1.1	Fluxograma geral do sistema de classificação e cifragem de informações sensíveis.	6
1.2	Interface de carregamento de <i>dataset</i> para o <i>fine-tuning</i> de modelos <i>Transformer</i>	11
1.3	Configuração de parâmetros para o treinamento de modelos de classificação.	12
1.4	Interface para envio de documentos e seleção do modelo de classificação.	13
2.1	Fluxo do sistema de autenticação por palma	18
2.2	Método para aquisição da ROI, adaptado de Su et al. (95).	20
2.3	Fluxograma do processo de extração da ROI, desde a imagem bruta até a obtenção da área de interesse para autenticação.	21
2.4	Exemplo de falha na extração da ROI devido a poses e oclusões.	23
2.5	Curva de desempenho do sistema, mostrando a relação entre FAR e FRR.	24
3.1	Arquitetura modular do assistente virtual com preservação de privacidade.	28
5.1	Processamento de uma zk-SNARK (9)	43
5.2	Arquitetura do projeto de autenticação biométrica com Provas de Conhecimento Zero na fase de registro.	45
5.3	Arquitetura do projeto de autenticação biométrica com Provas de Conhecimento Zero na fase de autenticação.	47
7.1	Fluxo operacional proposto para o MVP de verificação de integridade de certidões de nascimento.	57
7.2	Arquitetura do sistema de verificação de integridade de certidões de nascimento.	58
8.1	Arquitetura do Sistema de Estatísticas Vitais.	71
9.1	Cliente do Fabric que recebe <i>requests</i> e executa <i>smart contracts</i>	76
9.2	Exemplo de dados extraídos de um documento via OCR.	77
9.3	Trecho do <i>output</i> da execução da PoC.	77
9.4	<i>Shell script</i> responsável pela execução completa da PoC.	78
9.5	Trecho do <i>smart contract</i> desenvolvido para o Hyperledger Fabric.	78
10.1	Fluxo simplificado do algoritmo <i>Federated Averaging</i> (FedAvg).	81
12.1	Exemplo de amostra utilizada contendo trecho de documento manuscrito do século XIX.	96
13.1	Processo de anotação de um assento de nascimento.	101
13.2	Diagrama do ciclo de treinamento federado.	102

13.3 Interface gráfica antes do envio da imagem.	103
13.4 Interface gráfica após o envio da imagem.	103

Lista de Tabelas

8.1	Escopo e delimitação do projeto	69
10.1	Resumo de trabalhos relacionados sobre Aprendizado Federado aplicado a LLMs.	83
10.2	Comparativo de desempenho dos modelos no cenário de teste para Florianópolis.	85
12.1	Resultados qualitativos da transcrição automática.	96
13.1	Métricas de validação do modelo final.	104

Lista de Códigos

1.1	Estrutura simplificada do classificador de texto sensível	9
1.2	Função de treinamento com etapas canonizadas de <i>fine-tuning</i>	10
1.3	Estrutura do sistema de redação criptográfica	11

Lista de Símbolos e Acrônimos

Acrônimos

AES	<i>Advanced Encryption Standard</i>
API	<i>Application Programming Interface</i>
BERT	<i>Bidirectional Encoder Representations from Transformers</i>
CLIP	<i>Contrastive LanguageImage Pre-training</i>
CNH	Carteira Nacional de Habilitação
CNJ	Conselho Nacional de Justiça
CRAFT	<i>Character Region Awareness for Text Detection</i>
CSS	<i>Cascading Style Sheets</i>
CSV	<i>Comma-Separated Values</i>
DLT	<i>Distributed Ledger Technology</i>
ECA	Estatuto da Criança e do Adolescente
ECC	<i>Elliptic Curve Cryptography</i>
ETL	<i>Extract, Transform, Load</i>
FAR	<i>False Acceptance Rate</i>
FL	<i>Federated Learning</i>
FRR	<i>False Rejection Rate</i>
GCM	<i>Galois/Counter Mode</i>
GDPR	<i>General Data Protection Regulation</i>
GPU	<i>Graphics Processing Unit</i>
HTML	<i>HyperText Markup Language</i>
HTR	<i>Handwritten Text Recognition</i>
HTTP	<i>HyperText Transfer Protocol</i>
IA	Inteligência Artificial

ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
ID	Identificador
IoU	<i>Intersection over Union</i>
JSON	<i>JavaScript Object Notation</i>
JWS	<i>JSON Web Signature</i>
LabREC	Laboratório de Pesquisa e Desenvolvimento do Registro Civil do Brasil
LabSEC	Laboratório de Segurança em Computação
LGPD	Lei Geral de Proteção de Dados Pessoais
LLM	<i>Large Language Model</i>
mAP	<i>mean Average Precision</i>
MLM	<i>Masked Language Modeling</i>
MVP	<i>Minimum Viable Product</i>
NER	<i>Named Entity Recognition</i>
NIST	<i>National Institute of Standards and Technology</i>
NLP	<i>Natural Language Processing</i>
NSP	<i>Next Sentence Prediction</i>
OCR	<i>Optical Character Recognition</i>
OCDE	Organização para a Cooperação e Desenvolvimento Econômico
OMS	Organização Mundial da Saúde
ON-RCPN	Operador Nacional do Registro Civil de Pessoas Naturais
ONU	Organização das Nações Unidas
ORM	<i>Object-Relational Mapping</i>
PCZ	Prova de Conhecimento Zero
PDF	<i>Portable Document Format</i>
PII	<i>Personally Identifiable Information</i>
PLN	Processamento de Linguagem Natural
PoC	<i>Proof of Concept</i>
PQC	<i>Post-Quantum Cryptography</i>
RAG	<i>Retrieval-Augmented Generation</i>
RBAC	<i>Role-Based Access Control</i>
RC	Registro Civil
REST	<i>Representational State Transfer</i>

RG	Registro Geral
ROI	<i>Region of Interest</i>
SIDRA	Sistema IBGE de Recuperação Automática
SQL	<i>Structured Query Language</i>
SVM	<i>Support Vector Machine</i>
TFF	<i>TensorFlow Federated</i>
TMI	Taxa de Mortalidade Infantil
TrOCR	<i>Transformer-based OCR</i>
UFSC	Universidade Federal de Santa Catarina
UNESCO	<i>United Nations Educational, Scientific and Cultural Organization</i>
UUID	<i>Universally Unique Identifier</i>
ViT	<i>Vision Transformer</i>
WARC	Workshop Acadêmico do Registro Civil
XAI	<i>Explainable AI</i>
XML	<i>eXtensible Markup Language</i>
ZKP	<i>Zero-Knowledge Proof</i>
zk-SNARK	<i>Zero-Knowledge Succinct Non-Interactive Argument of Knowledge</i>

Símbolos Matemáticos

τ	Limiar de similaridade
\vec{A}	Vetor de características (embedding) da amostra atual
\vec{B}	Vetor de características (embedding) de referência
s	Similaridade de cossenos
x	Parâmetros públicos em circuitos aritméticos
w	Testemunha em provas de conhecimento zero
f	Campo finito
S_p	Chave de prova
S_v	Chave de verificação
π	Prova criptográfica
m	Grau de um polinômio
$GF(2^m)$	Corpo finito de característica 2
P	Precisão
R	Recall (Revocação)

Notações Especiais

$\gcd(a, b)$	Máximo divisor comum entre a e b
$x \equiv y \pmod{p}$	x é congruente a y módulo p
$ AB $	Distância euclidiana entre os pontos A e B
$TMI_{\text{ano_anterior}}$	Taxa de Mortalidade Infantil do ano anterior
[CLS]	Token de classificação em modelos BERT
[MASK]	Token mascarado em modelos de linguagem

Apresentação

Os *Anais do I Workshop Acadêmico do Registro Civil (WARC 2025)* são fruto da colaboração estratégica entre o Laboratório de Pesquisa e Desenvolvimento do Registro Civil do Brasil (LabREC), o Operador Nacional do Registro Civil de Pessoas Naturais (ON-RCPN) e o Laboratório de Segurança em Computação (LabSEC) da Universidade Federal de Santa Catarina (UFSC). Este volume materializa o esforço conjunto e o talento de estudantes dos cursos de Ciência da Computação e Sistemas de Informação que, no primeiro semestre de 2025, participaram da disciplina *Tópicos Especiais em Aplicações Tecnológicas I (Segurança & Inteligência Artificial)*.

Ministrada pelo Prof. Dr. Ricardo Custódio, com a tutoria de Wellington Fernandes Silvano, Gustavo Zambonin, Gustavo Biage e Matheus Saldanha, a disciplina foi concebida para ir além da teoria, desafiando os alunos a explorar a complexa e instigante interseção entre Inteligência Artificial e Segurança da Computação, áreas que compõem a vanguarda tecnológica contemporânea. A metodologia adotada, centrada no desenvolvimento de uma Prova de Conceito (PoC), fomentou autonomia, pensamento crítico e aplicação prática do conhecimento para resolver problemas concretos e de relevância social.

Os trabalhos aqui reunidos apresentam soluções concebidas e implementadas para enfrentar desafios atuais e antecipar demandas futuras do Registro Civil brasileiro. Todas as propostas foram desenvolvidas, documentadas e apresentadas publicamente durante o WARC 2025, realizado em 2 de julho de 2025.

Estrutura dos Anais

Os anais estão organizados em três eixos temáticos que refletem as principais frentes de inovação tecnológica no contexto do Registro Civil brasileiro:

A **Parte I: Privacidade e Segurança da Informação no Contexto do Registro Civil** aborda os desafios fundamentais da proteção de dados sensíveis em um ambiente cada vez mais digitalizado. Esta seção explora soluções computacionais avançadas que buscam conciliar a necessidade de processamento de dados em larga escala com os imperativos de segurança e privacidade da informação. Os trabalhos investigam desde modelos de Processamento de Linguagem Natural para classificação e redação criptográfica automatizada até sistemas de autenticação biométrica que empregam provas de conhecimento zero para dissociar o ato de autenticação da exposição do dado biométrico.

O **Capítulo 1** *Da Proteção de Dados Sensíveis à Inteligência Operacional: Automação Segura no Registro Civil com IA*, de Maurício Konrath sob orientação de Wellington Fernandes Silvano, apresenta um sistema completo de classificação automática de informa-

ções sensíveis, utilizando modelos *Transformer* de última geração e um sistema inovador de redação criptográfica que protege informações sem comprometer sua integridade estrutural.

O **Capítulo 2** *Autenticação Biométrica por Impressão Palmar com Redes Neurais Profundas*, de Enzo da Rosa Brum com orientação de Gustavo Biage, explora o desenvolvimento de um sistema de autenticação biométrica robusto, utilizando aprendizado profundo e redes neurais convolucionais para verificação de identidade.

O **Capítulo 3** *Assistente Virtual Jurídico com Mecanismos Avançados de Garantia de Privacidade*, de Lucas Coelho Pini de Sousa sob tutoria de Wellington Fernandes Silvano, desenvolve um assistente virtual para orientação jurídica, integrando arquitetura de *Retrieval-Augmented Generation* (RAG) com mecanismos robustos de preservação da privacidade.

O **Capítulo 4** *Proteção de Registros Cíveis com Criptografia Pós-Quântica e Otimização Baseada em IA*, de Davi Ludvig Longen Machado com orientação de Matheus Saldanha, investiga algoritmos de criptografia pós-quântica combinados com inteligência artificial para otimizar segurança e desempenho.

O **Capítulo 5** *Autenticação Biométrica Segura com Provas de Conhecimento Zero*, de Alex Davis Neuwiem da Silva sob tutoria de Gustavo Zambonin, propõe uma arquitetura de autenticação biométrica que dissocia a verificação de identidade da exposição de dados biométricos.

O **Capítulo 6** *Classificação da Irreducibilidade de Pentanômios com Técnicas de Inteligência Artificial*, de Luiz Maurício do Valle Pereira com orientação de Matheus Saldanha, aplica técnicas de IA a problemas matemáticos complexos com impacto na criptografia moderna.

A **Parte II: Qualidade, Integridade e Confiabilidade dos Dados no Registro Civil** concentra-se nos desafios relacionados à manutenção da fidedignidade e consistência das informações registrais. Esta seção apresenta metodologias computacionais para a validação e verificação contínua de dados, promovendo a transição de uma abordagem reativa para uma estratégia proativa de garantia da qualidade informacional.

O **Capítulo 7** *Verificação de Integridade e Autenticidade de Certidões de Nascimento*, de Ismael Coral Hoepers Heinzelmann sob orientação de Gustavo Zambonin, desenvolve um sistema automatizado para detecção de inconsistências e adulterações em certidões de nascimento.

O **Capítulo 8** *Sistema de Estatísticas Vitais com Integração de Inteligência Artificial*, de Marcelo Dutra Mendonça com orientação de Gustavo Biage, apresenta uma plataforma inteligente para padronização, validação e análise de dados vitais.

O **Capítulo 9** *Verificação Automatizada de Documentos Utilizando Inteligência Artificial*, de Luan Diniz Moraes com tutoria de Wellington Fernandes Silvano, propõe integração de OCR, análise semântica e blockchain para validação documental.

O **Capítulo 10** *Aprendizado Federado Aplicado a Dados Vitais: Estudo de Caso em Santa Catarina*, de Matheus Paulon Novais sob orientação de Gustavo Zambonin, demonstra como múltiplas instituições podem treinar modelos preditivos robustos sem comprometer a privacidade.

A **Parte III: Preservação Digital e Gestão de Acervos Históricos do Re-**

gistro Civil aborda os desafios da conversão de acervos analógicos em recursos digitais pesquisáveis. Os trabalhos aplicam aprendizado profundo para automatizar e escalar a compreensão e transcrição de documentos históricos manuscritos.

O **Capítulo 11** *Reconhecimento de Escrita Manuscrita em Documentos Históricos*, de Gibram Goulart Farias com orientação de Matheus Saldanha, apresenta um dataset customizado para OCR em documentos brasileiros dos séculos XIX e XX.

O **Capítulo 12** *Do Tinteiro ao Silício: Transcrição de Manuscritos Cursivos com Inteligência Artificial*, de Murillo Cordeiro Guindani sob tutoria de Wellington Fernandes Silvano, avalia o uso do modelo TrOCR para escrita cursiva do século XIX.

O **Capítulo 13** *Identificação de Estruturas Gráficas em Documentos Históricos com Aprendizado Federado*, de Lucas Castro Truppel Machado com orientação de Gustavo Biage, propõe um método para detecção colaborativa de elementos gráficos preservando a privacidade.

Estes anais registram os resultados técnicos obtidos, valorizam a produção intelectual de nossos estudantes e contribuem para a visibilidade de uma nova geração de profissionais comprometidos com a inovação ética, a proteção de dados sensíveis e a construção de um futuro digital mais seguro, inclusivo e eficiente para todos os cidadãos brasileiros.

Parte I - Privacidade e Segurança da Informação no Contexto do Registro Civil

A digitalização de infraestruturas críticas, como o Registro Civil, impõe um desafio central: equilibrar a necessidade de processamento de dados em larga escala com os imperativos de segurança e privacidade da informação. Este eixo temático examina soluções computacionais de última geração para enfrentar esse dilema, posicionando-se na confluência entre a Inteligência Artificial e a Criptografia. Os trabalhos reunidos transcendem a aplicação de protocolos convencionais, explorando paradigmas inovadores para a proteção de dados sensíveis, em estrita conformidade com o arcabouço legal vigente.

As contribuições aqui apresentadas abordam o problema sob múltiplas perspectivas. Investigam-se modelos de *Processamento de Linguagem Natural* voltados à classificação e à redação criptográfica automatizada de informações críticas. São explorados sistemas de autenticação biométrica que, simultaneamente, utilizam redes neurais profundas para alcançar elevada acurácia e implementam provas de conhecimento zero (*Zero-Knowledge Proofs* – ZKP) para dissociar o ato de autenticação da exposição do dado biométrico. Ademais, o eixo contempla a prospecção de ameaças emergentes por meio da análise de esquemas de criptografia pós-quântica e o desenvolvimento de assistentes conversacionais que integram a privacidade como elemento arquitetural intrínseco (*Privacy by Design*).

Em conjunto, esses estudos consolidam um corpo de conhecimento voltado à concepção de sistemas que aliam inteligência funcional e robustez em garantias de segurança, contribuindo para a construção de soluções resilientes, éticas e sustentáveis no contexto do Registro Civil.

1 Da Proteção de Dados Sensíveis à Inteligência Operacional: Automação Segura no Registro Civil com IA

Autor: Maurício Konrath

Tutor: Wellington Fernandes Silvano

1.1 Introdução

A transformação digital impõe um duplo desafio ao Registro Civil brasileiro: proteger com rigor um volume crescente de dados sensíveis não estruturados, em conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD) (14), e, simultaneamente, transformar esses dados em ativos estratégicos para a modernização e eficiência dos serviços. Essa encruzilhada estratégica, que equilibra segurança e agilidade, foi recentemente abordada na Cartilha de Boas Práticas em IA do Operador Nacional do Registro Civil de Pessoas Naturais (ON-RCPN) (87), a qual reconhece a Inteligência Artificial (IA) como uma oportunidade histórica desde que sua aplicação garanta a segurança dos dados e o respeito integral aos direitos dos cidadãos. O desafio se intensifica ao considerarmos que tais dados incluem informações de altíssima confidencialidade, como filiação por adoção, reconhecimento de paternidade e retificações de nome ou gênero (11, 12, 22), cuja exposição indevida pode acarretar graves riscos de discriminação.

Processos manuais não apenas são onerosos e propensos a erros críticos (46), como também incapazes de extrair valor operacional dos acervos. Embora a IA, em particular as arquiteturas *Transformer* (102), ofereça soluções promissoras, uma lacuna crítica persiste: a ausência de sistemas práticos, seguros e flexíveis que permitam às próprias serventias aplicar essa tecnologia de forma autônoma e alinhada às suas realidades específicas.

Este trabalho busca preencher essa lacuna por meio do desenvolvimento de uma plataforma ponta-a-ponta que vai do dado sensível à inteligência operacional. O sistema não se limita a classificar informações sensíveis; ele foi concebido como um motor de transformação digital para o Registro Civil. Para o desafio do dado sensível, a plataforma emprega modelos de vanguarda e introduz um sistema de redação criptográfica, que protege a informação sem comprometer sua integridade estrutural. Para o desafio da inteligência operacional, a mesma tecnologia de classificação serve de base para automatizar rotinas

hoje predominantemente manuais, como o roteamento automático de solicitações para os setores competentes e a geração assistida de minutas de respostas ao cidadão, demonstrando um caminho claro que vai além da mera segurança dos acervos.

As contribuições deste trabalho são múltiplas. Primeiramente, apresentamos a engenharia de um sistema robusto e funcional que materializa o princípio de *Privacy by Design*, garantindo o processamento local e a soberania dos dados. Em segundo lugar, propomos um método inovador de redação criptográfica como implementação prática do princípio de sigilo condicional (39), viabilizando acesso controlado à informação original e identificação de pontos de maior fragilidade. Por fim, o sistema estabelece uma ponte entre a complexidade dos modelos de IA e sua aplicação segura por não especialistas, por meio de uma interface que viabiliza supervisão humana eficaz, elemento essencial para a gestão dos riscos residuais de classificação (62). Em conjunto, tais contribuições formam um *blueprint* para a adoção responsável e estratégica da IA, capacitando as serventias a cumprir sua missão com mais segurança e eficiência na era digital.

Diante desse contexto, este trabalho tem como objetivo o desenvolvimento de um sistema completo de classificação automática de informações, que atenda aos seguintes requisitos:

- Utilização de modelos *state-of-the-art* baseados em *Transformers*;
- Operação totalmente local, sem exposição de dados sensíveis;
- Possibilidade de treinamento com dados específicos da instituição;
- Interface web intuitiva, com recursos integrados para redação de documentos;
- Incorporação de mecanismos criptográficos para proteção adicional.

1.2 Modelos *Transformers*

A arquitetura *Transformer*, introduzida por Vaswani et al. (102), revolucionou o uso de modelos de Inteligência Artificial (IA) no Processamento de Linguagem Natural (PLN). Essa revolução decorreu da substituição de unidades recorrentes e convolucionais por mecanismos de atenção, possibilitando o processamento simultâneo de sequências inteiras e a captura eficiente de dependências de longo alcance. O BERT (*Bidirectional Encoder Representations from Transformers*), proposto por Devlin et al. (30), constitui um marco nessa evolução, utilizando exclusivamente a parte codificadora (*encoder*) da arquitetura *Transformer* para proporcionar compreensão contextual bidirecional profunda.

Segundo Rogers; Kovaleva e Rumshisky (89), o BERT apresenta as seguintes características distintivas:

1. **Atenção bidirecional:** Ao contrário de modelos unidirecionais, o BERT contextualiza cada *token* na entrada considerando todos os demais *tokens* da sequência, tanto à esquerda quanto à direita, conferindo ao modelo uma capacidade sem precedentes de inferência contextual semanticamente rica;

2. **Pré-treinamento:** Baseia-se em tarefas inovadoras aplicadas a extensos *corpora* de texto não rotulado, permitindo ao modelo aprender representações linguísticas ricas e generalizáveis. Entre as principais estratégias, destacam-se o *Masked Language Modeling* (MLM), em que o modelo prevê palavras mascaradas com base no contexto bidirecional, e o *Next Sentence Prediction* (NSP), que o capacita a compreender relações entre sentenças;
3. **Fine-tuning:** Ajuste fino de modelos pré-treinados, como o BERT, em tarefas específicas com dados rotulados, aproveitando o conhecimento linguístico e contextual adquirido no pré-treinamento;
4. **Transfer learning:** O *fine-tuning* é uma forma de aprendizado por transferência, em que o conhecimento adquirido em um domínio geral é reutilizado para resolver tarefas especializadas. Essa abordagem é particularmente relevante para a classificação de documentos sensíveis, pois permite rápida adaptação às nuances semânticas e padrões específicos de um domínio.

O *fine-tuning* é especialmente crítico para a tarefa de classificação de informações sensíveis e envolve as seguintes etapas:

1. **Preparação dos dados:** Curadoria e pré-processamento de exemplos de documentos sensíveis e não sensíveis, assegurando formatação padronizada e compatível com o modelo. Inclui identificação automática de colunas de texto e rótulos, análise estatística para balanceamento de classes e mapeamento de rótulos textuais para valores numéricos;
2. **Tokenização:** Conversão do texto pré-processado em *tokens* (subpalavras) por meio de tokenizadores *WordPiece* pré-treinados específicos de cada modelo, com aplicação de *padding* e *truncation* para uniformizar o comprimento das sequências;
3. **Adaptação da arquitetura:** Durante o pré-processamento, insere-se um *token* sintético especial denominado [CLS] (*Classification*) na primeira posição da sequência de entrada. Esse *token* funciona como agregador de informações, após o processamento pelo *encoder* BERT, o vetor oculto correspondente ao [CLS] concentra as informações contextuais de toda a sentença, aproveitando o mecanismo de atenção bidirecional. Para a classificação final, conecta-se especificamente a esse vetor uma camada linear simples seguida de *softmax*, que transforma o vetor em probabilidades finais para cada classe da tarefa (30);
4. **Treinamento:** Ajuste de todos os parâmetros do modelo (incluindo o *Transformer* e as novas camadas de saída) por retropropagação nos dados rotulados da tarefa-alvo, geralmente com taxas de aprendizado reduzidas e poucas épocas de treino, de modo a preservar o conhecimento linguístico geral;
5. **Validação:** Avaliação do desempenho em conjunto de validação independente, utilizando métricas como acurácia, precisão, *recall* e *F1-score*. Aplicam-se técnicas de regularização, como *dropout*, *weight decay* e *early stopping*, para evitar sobreajuste e promover boa capacidade de generalização.

1.3 Princípios

A implementação do sistema foi guiada por princípios fundamentais de segurança da informação e de privacidade, com o objetivo de assegurar a confidencialidade, integridade e disponibilidade dos dados sensíveis ao longo de todo o seu ciclo de vida. A proteção eficaz vai além da mera conformidade regulatória, configurando-se como requisito essencial para a manutenção da confiança e da sustentabilidade institucional. Foram considerados os seguintes princípios:

- **Privacy by Design:** Integrado desde a concepção da arquitetura, este princípio assegura que a privacidade seja tratada como requisito essencial, e não como funcionalidade acessória. Diretrizes normativas, como a Lei Geral de Proteção de Dados Pessoais (LGPD) (14) e o Regulamento Geral sobre a Proteção de Dados (GDPR) (100), determinam a adoção de mecanismos eficazes para a identificação, categorização e proteção de dados pessoais e sensíveis;
- **Processamento local:** Para maximizar a segurança e o controle, os dados não deixam a infraestrutura da instituição. Essa abordagem reduz significativamente os riscos associados à transmissão ou armazenamento em ambientes externos e reforça a política interna de segurança da informação;
- **Criptografia:** Após a identificação e classificação das informações sensíveis, a criptografia é aplicada como camada de defesa fundamental. O sistema utiliza algoritmos de cifragem simétrica, como o *Advanced Encryption Standard* (AES) (67), para proteger seletivamente os trechos classificados como sensíveis. Essa abordagem garante que apenas os dados críticos sejam convertidos para *ciphertext*, preservando a legibilidade e a utilidade do restante do documento;
- **Auditabilidade:** Com o objetivo de assegurar conformidade regulatória e responsabilização, todas as operações executadas pelo sistema são registradas em *logs* detalhados, constituindo um rastro completo das etapas de classificação e de redação. Isso possibilita auditorias abrangentes e a verificação da integridade dos documentos protegidos por entidades autorizadas.

1.4 Desenvolvimento do Sistema

O sistema proposto tem como objetivo identificar automaticamente informações sensíveis em documentos heterogêneos e protegê-las por meio de redação criptográfica, preservando tanto a legibilidade do conteúdo remanescente quanto a governança sobre o acesso futuro. A Figura 1.1 apresenta o fluxo completo, desde a ingestão de arquivos até a geração do documento protegido.

O fluxograma sintetiza duas macrofases do sistema:

- o *ciclo de treinamento*, localizado na área retangular à direita, que parte do conjunto de dados (*dataset*) fornecido pelas serventias e resulta em um modelo BERT ajustado;

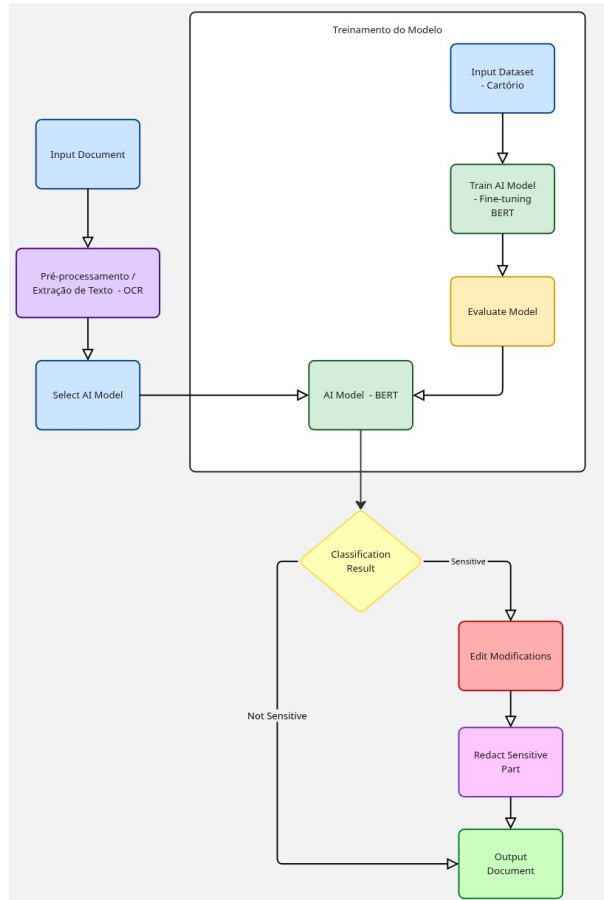


Figura 1.1: Fluxograma geral do sistema de classificação e cifragem de informações sensíveis.

- o *pipeline* de inferência e redação, ilustrado à esquerda, que recebe documentos brutos, classifica cada trecho quanto à sensibilidade e aplica a redação criptográfica sempre que necessário.

Essa representação evidencia como os módulos se integram de forma coesa e funcional.

Para a implementação, recomenda-se o desenvolvimento de uma aplicação web utilizando o *framework* Flask (40) no *backend* e o Bootstrap 5 (81) no *frontend*. A arquitetura geral deve ser modular e escalável, otimizando o fluxo de dados desde a ingestão e pré-processamento até a proteção (cifragem) e a recuperação segura das informações. Os módulos principais que a compõem são:

Interface Web. *Frontend* responsivo, desenvolvido com Bootstrap 5 e JavaScript nativo, que possibilita o envio (*upload*) de documentos, a configuração de parâmetros de treinamento e a visualização dos resultados de classificação por usuários não técnicos. Implementa *design* responsivo, proporcionando experiência de uso consistente em diferentes dispositivos.

Motor de Classificação. Núcleo do sistema de detecção, baseado em modelos com arquiteturas *Transformer* (BERT (30) ou ELECTRA (21)), previamente pré-treinados e ajustados (*fine-tuned*) para identificação de entidades sensíveis ou classificação textual

em nível de sentença/*token*. Utiliza o pacote *Transformers* da Hugging Face (105) como *framework* principal.

Sistema de Treinamento. Módulo dedicado ao *fine-tuning* de modelos *Transformer*, abrangendo preparação de dados, configuração de hiperparâmetros (taxa de aprendizado, tamanho do lote, número de épocas) e otimizações algorítmicas, incluindo *warmup steps* e *early stopping*.

Processador de Documentos. Responsável pela ingestão de documentos em múltiplos formatos (PDF, DOCX, TXT, imagens) e pela extração de texto bruto. Para arquivos não textuais ou digitalizados, emprega-se Reconhecimento Óptico de Caracteres (OCR) via Tesseract-OCR (94), integrado por meio da biblioteca *pytesseract* em Python.

Gerador de Relatórios. Produz nova versão do documento com trechos sensíveis substituídos por contrapartes cifradas, resultando em um artefato final seguro para armazenamento ou transmissão.

Sistema de Redação. Implementa a ocultação ou substituição criptográfica de informações sensíveis identificadas, preservando a legibilidade do restante do documento.

Módulo Criptográfico. Aplica algoritmos de cifragem, como o *Advanced Encryption Standard* (AES), aos trechos classificados como sensíveis, além de gerenciar de forma segura as chaves criptográficas necessárias para as operações de cifragem e decifragem.

1.4.1 Modelo Base

Embora o *fine-tuning* permita a adaptação a uma ampla gama de modelos, este estudo concentrou-se na utilização de arquiteturas *Transformer*, cuja superioridade em compreensão contextual e desempenho em tarefas de classificação já se encontra amplamente documentada (102).

O modelo **ModernBERT** foi selecionado como base devido às suas características otimizadas, que visam eficiência e robustez. Trata-se de uma arquitetura aprimorada, incorporando atualizações estruturais e escaláveis, tais como:

- *Rotary Positional Embeddings* (RoPE) para codificação posicional eficiente;
- alternância de camadas com atenção global e local, equilibrando alcance contextual e custo computacional;
- ativações *Gated Linear Unit with Gating* (GeGLU), que aumentam a expressividade da rede;
- remoção de preenchimentos desnecessários (*unpadding*) para otimizar o processamento;

- normalização pré-camada (*pre-layer normalization*), favorecendo estabilidade no treinamento.

Essas melhorias têm por finalidade aumentar a eficiência computacional, otimizar o consumo de memória e aprimorar a capacidade do modelo para lidar com contextos mais extensos, mantendo ou superando o desempenho em tarefas padrão de *Natural Language Processing* (NLP).

A adaptabilidade da arquitetura *Transformer* possibilita sua aplicação em diferentes idiomas, aproveitando modelos previamente pré-treinados na língua-alvo. As otimizações do ModernBERT foram projetadas para tornar tanto o *fine-tuning* quanto a inferência mais rápidos e menos onerosos em termos de recursos computacionais.

Com essa base consolidada, a próxima subseção apresenta o *framework* de desenvolvimento adotado, detalhando como os componentes de software e as bibliotecas especializadas foram integrados para viabilizar a implementação prática do sistema.

1.4.2 Framework de Desenvolvimento

Para viabilizar a implementação prática do sistema, foi selecionado o *framework* Flask como base para o desenvolvimento da aplicação web. Essa escolha se justifica por oferecer uma plataforma leve e flexível, adequada à integração com bibliotecas de aprendizado de máquina e à construção de interfaces responsivas. Entre os fatores determinantes, destacam-se:

Simplicidade e flexibilidade. O Flask proporciona facilidade na implementação de APIs *RESTful* e flexibilidade na estruturação de rotas e *middleware*, permitindo que o desenvolvedor mantenha controle total sobre a arquitetura do sistema.

Integração com bibliotecas de *machine learning*. A natureza leve do Flask facilita a incorporação de bibliotecas voltadas ao aprendizado de máquina e ao aprendizado profundo, como o *Transformers* da Hugging Face e o PyTorch, promovendo eficiência no fluxo de dados e na comunicação entre módulos.

Controle granular da aplicação. O *framework* possibilita gerenciar de forma detalhada os componentes internos, o que é particularmente vantajoso para sistemas que demandam otimizações específicas e personalizadas, tanto na camada de *machine learning* quanto na de segurança da informação.

Adequação para prototipagem rápida. A combinação de simplicidade, flexibilidade e ampla documentação torna o Flask especialmente indicado para ciclos de desenvolvimento ágeis, permitindo testar, iterar e refinar soluções inovadoras com rapidez.

1.4.3 Bibliotecas Principais

A arquitetura tecnológica do sistema fundamenta-se em um conjunto integrado de *frameworks* e bibliotecas especializadas, cada uma selecionada para atender a aspectos específicos dos requisitos funcionais e não funcionais identificados. As principais bibliotecas empregadas incluem:

PyTorch. Atua como *backend* para operações de aprendizado profundo, oferecendo flexibilidade na implementação de arquiteturas customizadas e otimizações específicas. Sua integração nativa com CUDA possibilita o aproveitamento eficiente de recursos de GPU disponíveis (82).

PyMuPDF (fitz). Utilizada para o processamento de documentos PDF, disponibiliza funcionalidades avançadas para extração de texto, preservação de formatação e manipulação de conteúdo estruturado (4).

Tesseract. Integrado por meio da interface Python **pytesseract** (44), viabiliza o Reconhecimento Óptico de Caracteres (OCR) para extração de texto a partir de documentos digitalizados e imagens, com suporte otimizado para o idioma português.

Cryptography. Essencial para a implementação de funcionalidades de redação criptográfica, provê implementações seguras de algoritmos criptográficos simétricos e assimétricos, em conformidade com padrões amplamente reconhecidos (84).

1.4.4 Componentes Principais

O módulo central do sistema é responsável pela lógica de classificação, implementada no arquivo `classifier.py`. Essa unidade concentra as rotinas essenciais para o carregamento do modelo, a tokenização do texto e a classificação de trechos com base no grau de sensibilidade identificado.

O código 1.1 apresenta a estrutura simplificada da classe `SensitiveTextClassifier`, que encapsula as principais funcionalidades do processo de classificação.

```
1 class SensitiveTextClassifier:
2     def __init__(self, model_path: str):
3         self.model_path = model_path
4         self.model = None
5         self.tokenizer = None
6         self.load_model()
7
8     def classify_text(self, text: str) -> Dict[str, Any]:
9         # Implementação da classificação
10        pass
11
12    def classify_text_chunks(self, text: str) -> List[Dict]:
13        # Classificação por segmentos
14        pass
```

Código 1.1: Estrutura simplificada do classificador de texto sensível

O método `__init__` inicializa a classe, definindo o caminho do modelo, instanciando o objeto de modelo e o *tokenizer*, e invocando o carregamento do modelo treinado. O método `classify_text` recebe um texto integral e retorna a classificação geral quanto à sensibilidade, enquanto o método `classify_text_chunks` processa o texto em segmentos menores, permitindo identificar e classificar partes específicas de forma independente. Essa abordagem segmentada é particularmente útil para documentos extensos ou com seções heterogêneas em termos de conteúdo sensível.

1.4.5 Sistema de Treinamento (*trainer.py*)

Este módulo é responsável pelo *fine-tuning* de modelos baseados em *Transformer* para a classificação de textos sensíveis, conforme proposto por Vaswani et al. (102) e aplicado a tarefas de classificação textual em Devlin et al. (30).

A interface para envio (*upload*) do *dataset* e a tela de configuração de hiperparâmetros são apresentadas, respectivamente, nas Figuras 1.2 e 1.3. Essas interfaces permitem ao usuário carregar dados de treinamento, ajustar parâmetros críticos e iniciar o processo de aprendizado de forma intuitiva.

O fluxo de execução do treinamento segue a função apresentada no Código 1.2, que organiza as etapas de preparação de dados, configuração do modelo, treinamento, validação e armazenamento dos artefatos gerados. O desenvolvimento faz uso de bibliotecas amplamente reconhecidas, como *Transformers* (105), para gerenciamento de modelos e rotinas de *fine-tuning*.

```
1 def train_model(base_model_id, dataset_path, epochs,
2                 batch_size, learning_rate, output_dir):
3     # 1. Pre-processamento do dataset
4     # 2. Configuracao do modelo
5     # 3. Treinamento com Trainer
6     # 4. Validacao e metricas
7     # 5. Salvamento do modelo
```

Código 1.2: Função de treinamento com etapas canonizadas de *fine-tuning*

As etapas implementadas no Código 1.2 podem ser descritas da seguinte forma:

- Preparação do *dataset* com balanceamento de classes e divisão treino-validação;
- Configuração do modelo *Transformer* e do *tokenizer*;
- Treinamento com *Trainer*, incluindo técnicas de regularização como *early stopping* e *weight decay*;
- Validação utilizando métricas como acurácia, precisão, *recall* e F1-score;
- Salvamento dos artefatos finais e dos *logs* de execução.

1.4.6 Sistema Criptográfico (*crypto_redaction.py*)

Este módulo provê as funções centrais para a redação criptográfica seletiva de trechos identificados como sensíveis, bem como para a gestão de chaves e credenciais de acesso

Figura 1.2: Interface de carregamento de *dataset* para o *fine-tuning* de modelos *Transformer*.

temporárias. Sua implementação está em conformidade com padrões internacionais de segurança, como o *Advanced Encryption Standard* (AES) (67) e os modos autenticados Galois/Counter Mode (GCM) (68).

A estrutura básica é apresentada na Listagem 1.3.

```
1 class CryptoRedactionSystem:
2     def encrypt_text(self, text: str) -> str:
3         # Criptografia de informações sensíveis
4
5     def generate_access_key(self, duration_hours: int) -> str:
6         # Emissão de chaves de acesso temporárias
7
8     def generate_qr_code(self, access_key: str) -> BytesIO:
9         # Geração de QR Code para acesso rápido
```

Código 1.3: Estrutura do sistema de redação criptográfica

O módulo criptográfico integra-se ao *pipeline* de inferência do classificador para substituir dinamicamente os segmentos sensíveis por suas contrapartes cifradas, preservando a legibilidade do restante do documento. Além disso, viabiliza auditoria e acesso contro-

The image shows a web interface for configuring model training. It is divided into two main sections: 'Model Configuration' and 'Training Parameters'.
Model Configuration:
- **Base Model ***: A dropdown menu with 'answerdotai/ModernBERT-base' selected. Below it, a note says 'Choose the pre-trained model to fine-tune'.
- **Model Name ***: A text input field containing 'my_sensitive_classifier'. Below it, a note says 'Name for your trained model (letters, numbers, underscore, dash only)'.
- **Training Type**: A dropdown menu with 'Fine-tuning (Recommended)' selected. Below it, a note says 'Fine-tuning is faster and usually gives better results'.
Training Parameters:
- **Epochs**: A text input field with '3'. Below it, a note says 'Number of training iterations'.
- **Batch Size**: A dropdown menu with '16 (Recommended)' selected. Below it, a note says 'Adjust based on available memory'.
- **Learning Rate**: A dropdown menu with '2e-5 (Recommended)' selected. Below it, a note says 'Controls how quickly the model learns'.
At the bottom of the configuration section, there is a 'Show Advanced Options' button and a 'Start Training' button. Below the configuration section, there are three navigation buttons: 'View Models', 'Dashboard', and 'Home'.

Figura 1.3: Configuração de parâmetros para o treinamento de modelos de classificação.

lado às informações protegidas, em conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD).

O método `encrypt_text` realiza a cifragem seletiva do conteúdo sensível utilizando chaves simétricas, garantindo que apenas os trechos classificados como críticos sejam protegidos. O método `generate_access_key` emite credenciais temporárias com prazo de validade definido, assegurando que o acesso ao conteúdo original seja controlado e auditável. Por fim, o método `generate_qr_code` converte a chave de acesso em um código QR, permitindo a recuperação rápida e segura das informações por meio de dispositivos autorizados. Essa integração garante não apenas a proteção criptográfica, mas também a usabilidade e a rastreabilidade necessárias em ambientes de alta sensibilidade, como o Registro Civil.

1.4.7 Interface de Usuário

A interface web foi concebida para maximizar a eficiência e a clareza na interação entre o usuário e o sistema, oferecendo recursos que possibilitam tanto a operação por usuários não técnicos quanto o controle avançado por administradores. Entre as principais funcionalidades implementadas, destacam-se:

- **Upload de documentos:** suporte à ingestão e processamento de arquivos em múltiplos formatos, incluindo PDF, TXT, JSON e imagens (PNG, JPEG), com extração automática de conteúdo textual;
- **Seleção de modelo de classificação:** permite ao usuário escolher o modelo de análise (por exemplo, ModernBERT, BERT Base ou ELECTRA) mais adequado ao contexto ou domínio de aplicação;
- **Visualização de resultados com destaque das áreas sensíveis:** apresenta os documentos processados com os trechos identificados como sensíveis devidamente realçados, facilitando a validação visual e a conferência manual;
- **Download de relatórios em PDF:** gera uma nova versão do documento em que os trechos sensíveis são substituídos por contrapartes cifradas ou tarjadas, mantendo a legibilidade do conteúdo restante;
- **Acesso ao painel administrativo:** possibilita o gerenciamento completo do sistema, incluindo o treinamento de novos modelos, a configuração de parâmetros e a administração de permissões.

A Figura 1.4 ilustra a tela principal da interface, destacando o módulo de envio (*upload*) de documentos e a seleção de modelos de classificação, que representam o ponto de partida do fluxo operacional do sistema.

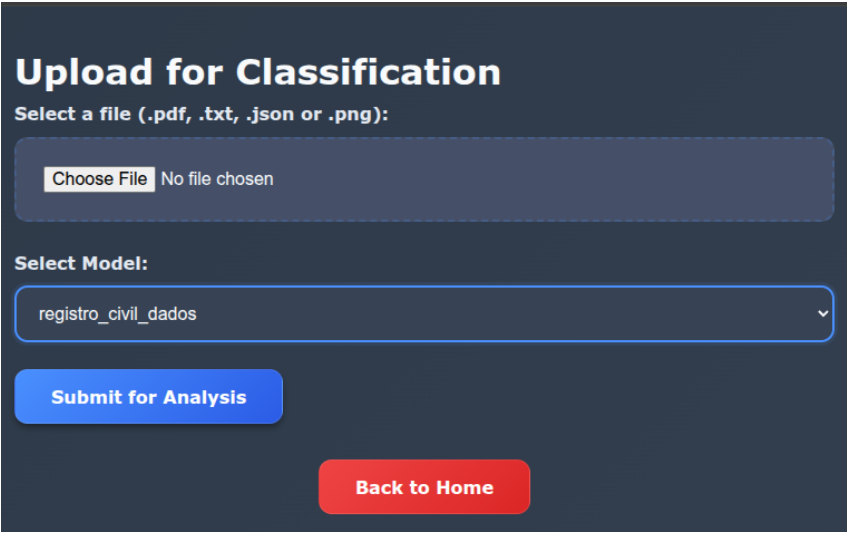


Figura 1.4: Interface para envio de documentos e seleção do modelo de classificação.

Essa interface atua como elo entre o usuário e os módulos internos do sistema, encaminhando os documentos submetidos ao *pipeline* de classificação e redação criptográfica. As escolhas feitas nesta etapa, como o modelo selecionado ou os parâmetros definidos, influenciam diretamente o processamento subsequente, garantindo que a operação final esteja alinhada às necessidades específicas de cada caso de uso.

1.4.8 Sistema de Treinamento

O painel administrativo foi projetado para gerenciar, de forma abrangente, o ciclo de vida dos modelos de *aprendizado de máquina*, fornecendo recursos que possibilitam

tanto a atualização contínua quanto a manutenção operacional do sistema. Entre as funcionalidades oferecidas, destacam-se:

- **Upload de *datasets* de treinamento:** possibilita a ingestão de novos conjuntos de dados para o *fine-tuning* dos modelos, adaptando-os a diferentes domínios ou necessidades específicas;
- **Configuração de hiperparâmetros:** disponibiliza uma interface intuitiva para o ajuste de parâmetros críticos, como taxa de aprendizado, dimensão do lote e número de épocas, otimizando o processo de treinamento e reduzindo riscos de sobreajuste;
- **Monitoramento do treinamento:** permite o acompanhamento em tempo real do progresso do treinamento, incluindo métricas de desempenho, *logs* de convergência e alertas para possíveis anomalias;
- **Validação de modelos:** executa avaliações automáticas sobre conjuntos de validação, assegurando que o modelo mantenha desempenho satisfatório antes de ser promovido para uso em produção;
- **Gestão de modelos treinados:** implementa um sistema de gerenciamento de *ModelPool* que mantém múltiplos modelos carregados em memória, eliminando re-carregamentos custosos e reduzindo o tempo de resposta.

Ao integrar-se ao fluxo geral do sistema, o painel administrativo atua como um centro de controle estratégico, permitindo que ajustes nos modelos sejam rapidamente refletidos no *pipeline* de classificação e redação criptográfica. Dessa forma, garante-se que o desempenho do sistema seja continuamente otimizado, mantendo sua aderência às exigências técnicas, regulatórias e operacionais do Registro Civil.

1.5 Potenciais Usos do Classificador Proposto no Registro Civil

A principal inovação deste trabalho reside no desenvolvimento de um sistema de redação criptográfica que não apenas protege as informações sensíveis, mas também preserva sua integridade e possibilita controle de acesso autorizado. Essa proposta se materializa nas seguintes contribuições:

Preservação da estrutura: ao substituir o texto sensível por uma contraparte cifrada de formato compatível, o sistema mantém o *layout* original do documento, garantindo que o restante do conteúdo permaneça legível e que o contexto seja preservado;

Múltiplos níveis de acesso: possibilita a implementação de políticas de acesso granular, utilizando tanto senhas permanentes quanto chaves temporárias para a decifragem dos dados, alinhando-se a princípios de segredo condicional e boas práticas de controle de acesso.

O sistema proposto transcende seu propósito inicial de proteção de acervos, tornando-se um ativo estratégico para a modernização e otimização das operações do Registro Civil. Uma vez integrado, pode atuar como motor de transformação digital, gerando valor em múltiplas frentes:

Triagem e roteamento automático de solicitações. O Registro Civil do Brasil recebe diariamente um grande volume de solicitações por e-mail, portais online e outros canais. O classificador pode analisar automaticamente cada solicitação e categorizá-la (por exemplo, “Pedido de 2ª via”, “Dúvida sobre prazo de emissão de certidão”). Com base nessa classificação, o sistema encaminha a demanda ao departamento ou atendente especializado adequado, eliminando a triagem manual e reduzindo significativamente o tempo de primeira resposta.

Geração de respostas assistida por IA. Após a classificação da solicitação, o sistema pode consultar uma base de conhecimento interna e, utilizando um modelo de linguagem, gerar um rascunho de resposta para o atendente. Por exemplo, para um pedido classificado como “Dúvida sobre documentos para casamento”, a IA pode redigir um texto contendo a lista completa de documentos necessários, links relevantes e instruções sobre os próximos passos. O atendente revisa, ajusta e envia, resultando em ganhos expressivos de produtividade e padronização das respostas.

Indexação inteligente de acervos históricos. A partir da detecção automática de metadados e categorias, o classificador pode apoiar a organização e a catalogação de registros históricos digitalizados, facilitando a busca e a recuperação de informações por pesquisadores, órgãos públicos e pela própria serventia.

Extração automática de estatísticas vitais. Ao identificar e classificar eventos como nascimentos, casamentos, óbitos e reconhecimentos de paternidade, o sistema pode gerar, em tempo quase real, estatísticas vitais consolidadas, alimentando bases de dados governamentais e apoiando políticas públicas.

Suporte a auditorias de conformidade. O classificador pode auxiliar processos de auditoria interna ou externa ao identificar rapidamente documentos que contenham dados sujeitos a regulamentações específicas, como a LGPD, agilizando verificações e reduzindo riscos de não conformidade.

1.6 Considerações Finais

A jornada de digitalização do Registro Civil, impulsionada pela busca por eficiência e pelas exigências da Lei Geral de Proteção de Dados Pessoais (LGPD) (14), apresenta um desafio duplo: proteger um volume massivo de dados não estruturados e, simultaneamente, capacitar as serventias para operar com agilidade na era digital. Este trabalho buscou enfrentar esse desafio de forma prática, indo além de uma proposta conceitual, por meio do desenvolvimento de um sistema ponta a ponta, funcional e seguro. A trajetória, desde

a fundamentação em modelos *Transformer* até a implementação de uma aplicação web com interfaces para treinamento e classificação, demonstrou, na prática, como a lacuna entre a pesquisa em Inteligência Artificial (IA) e sua aplicação em setores críticos pode ser superada.

O sistema desenvolvido atende integralmente aos objetivos traçados, entregando uma solução precisa, segura, flexível e de aplicação imediata. Sua principal inovação não está em um módulo isolado, mas na sinergia entre a classificação contextual de alta performance e uma arquitetura de segurança concebida sob o princípio de *Privacy by Design*. Ao garantir o processamento 100% local e introduzir um mecanismo de redação criptográfica reversível, a solução oferece uma resposta robusta à ameaça de vazamentos de dados. Diferentemente da redação convencional, a abordagem proposta não destrói a informação, mas a protege, preservando a integridade estrutural do documento e assegurando que o acesso controlado e auditável ao dado original seja possível para entidades autorizadas.

A análise do potencial da ferramenta revelou que seu valor vai muito além da segurança de acervos. Como discutido anteriormente, o motor de classificação constitui a base para uma plataforma de inteligência operacional. As mesmas capacidades de compreensão textual podem ser aplicadas para otimizar o atendimento ao cidadão, seja por meio da triagem automática de solicitações, seja pela geração de respostas assistidas por IA. Essa perspectiva transforma o sistema de uma ferramenta puramente defensiva em um ativo estratégico, capaz de gerar eficiência e modernizar processos em toda a serventia.

Em síntese, este trabalho evidencia que a aplicação responsável da IA, ancorada em práticas sólidas de segurança da informação, representa um caminho viável e poderoso para a transformação digital do Registro Civil. A solução apresentada configura-se como um *blueprint* para capacitar essas instituições essenciais, garantindo que possam cumprir sua missão com máxima eficiência e, ao mesmo tempo, reforçar seu papel como guardiãs da privacidade e dos dados mais fundamentais de cada cidadão. O futuro do registro é digital, e a inteligência artificial, quando bem aplicada, será uma aliada central na construção de um ambiente mais seguro, eficiente e confiável.

Como desenvolvimento futuro prioritário, destaca-se a construção de uma *API* pública e segura para expor as funcionalidades do sistema, viabilizando sua integração com outros fluxos de trabalho e sistemas já utilizados pelas serventias e plataformas do Registro Civil brasileiro. Tal evolução permitirá o uso em larga escala e a interoperabilidade com ecossistemas tecnológicos heterogêneos, ampliando ainda mais o impacto positivo da solução.

Por fim, cabe observar que a proposta está alinhada às diretrizes internacionais de interoperabilidade, transparência e governança de dados no setor público, como recomendado pela Organização para a Cooperação e Desenvolvimento Econômico (OCDE) em seu relatório sobre *Digital Government* (77). Ao adotar práticas que combinam segurança, eficiência e inovação, o Registro Civil brasileiro se posiciona em sintonia com as melhores práticas globais, reforçando seu compromisso com a proteção de dados e a prestação de serviços públicos modernos e confiáveis.

2 Autenticação Biométrica por Impressão Palmar com Redes Neurais Profundas

Autor: Enzo da Rosa Brum

Tutor: Gustavo Biage

2.1 Introdução

A biometria da palma da mão apresenta-se como uma alternativa promissora para autenticação de indivíduos, devido à sua alta unicidade, estabilidade ao longo do tempo e dificuldade de falsificação. A complexa estrutura de linhas, rugas e padrões presentes na palma fornece uma rica fonte de dados para identificação precisa.

O objetivo principal deste trabalho é desenvolver e avaliar um sistema de autenticação biométrica utilizando a palma da mão, empregando técnicas e modelos de *aprendizado profundo*. Para a implementação do sistema, foram exploradas metodologias modernas de visão computacional, aliadas a arquiteturas de redes neurais profundas.

A motivação para este estudo advém do interesse do autor na área de *aprendizado de máquina* e da intenção de compreender, de forma prática, as etapas envolvidas no treinamento de modelos para execução de tarefas específicas. Ao longo da disciplina, houve contato com diversas bibliotecas de *machine learning* e visão computacional, além da oportunidade de constatar o caráter iterativo e experimental do processo de treinamento.

O desenvolvimento do sistema proposto seguiu um fluxo estruturado que abrangeu:

- pré-processamento das imagens, incluindo normalização e alinhamento da palma da mão;
- extração de características discriminativas por meio de redes neurais convolucionais;
- treinamento supervisionado do modelo em conjuntos de dados específicos;
- e avaliação quantitativa utilizando métricas de desempenho apropriadas, visando validar a eficácia do sistema.

O fluxo completo do sistema é apresentado na Figura 2.1.

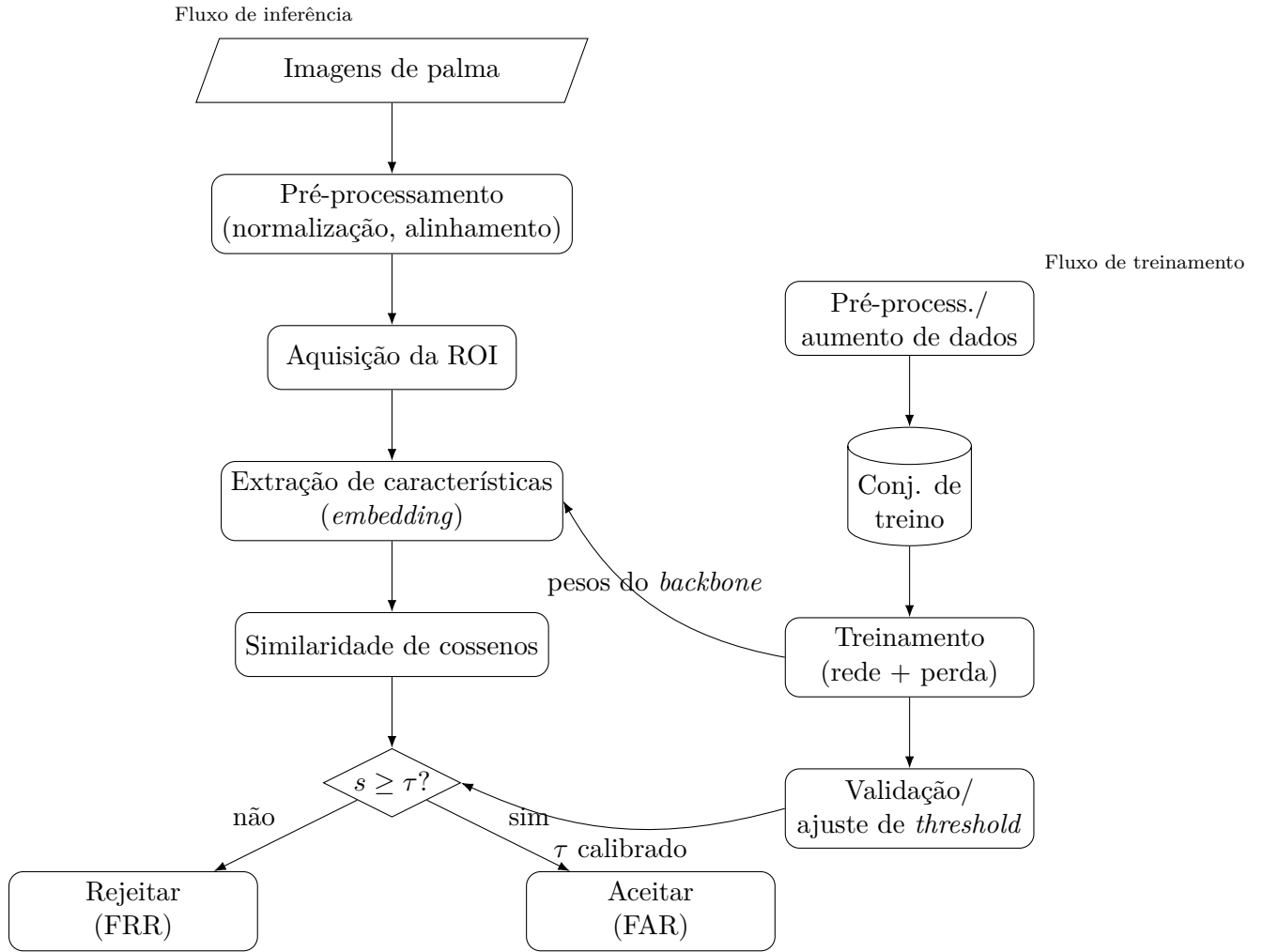


Figura 2.1: Fluxo do sistema de autenticação por palma: da aquisição e pré-processamento à decisão baseada na similaridade de cossenos, com treinamento supervisionado alimentando os pesos do extrator de características e a calibração do limiar τ .

2.2 Metodologia

A metodologia adotada neste trabalho é fundamentada em um *pipeline* de *aprendizado profundo* voltado à autenticação biométrica por meio da palma da mão. O processo é estruturado em duas fases principais:

- **Extração da Região de Interesse (ROI):** etapa responsável por localizar e isolar, a partir da imagem bruta, a porção da palma da mão relevante para a autenticação. Este processo inclui pré-processamento, alinhamento e normalização da imagem, visando reduzir variações relacionadas a posicionamento, escala e iluminação;
- **Extração de características e comparação:** fase em que são gerados vetores de representação (*embeddings*) a partir da ROI, utilizando redes neurais convolucionais. Esses vetores são então comparados por meio de métricas de similaridade, como a similaridade de cossenos, para determinar a correspondência entre a amostra de entrada e os registros existentes.

O fluxo completo, abrangendo as etapas de pré-processamento, extração de características, treinamento supervisionado e avaliação do modelo, é apresentado na Figura 2.1.

2.2.1 Etapas de Treinamento do Modelo

O treinamento do modelo foi conduzido de forma sistemática, seguindo as seguintes etapas:

1. **Preparação do conjunto de dados:** as imagens de palma foram divididas em conjuntos de treino, validação e teste, preservando a proporção de amostras por indivíduo para garantir a representatividade de cada classe;
2. **Aumento de dados (*data augmentation*):** aplicaram-se técnicas de rotação, translação, alteração de brilho e adição de ruído para aumentar a variabilidade e robustez do modelo, mitigando o risco de sobreajuste;
3. **Configuração de hiperparâmetros:** definiu-se taxa de aprendizado inicial, tamanho do lote e número de épocas, buscando um equilíbrio entre velocidade de convergência e desempenho final;
4. **Função de perda e otimizador:** empregou-se a função de perda de entropia cruzada categórica, combinada com o otimizador Adam, devido à sua boa adaptação em problemas de classificação;
5. **Treinamento supervisionado:** as imagens de entrada foram processadas pela rede neural convolucional para extração das características discriminativas, sendo a perda calculada e retropropagada para atualização dos pesos;
6. **Validação e ajuste de parâmetros:** ao final de cada época, o modelo foi avaliado no conjunto de validação, ajustando-se hiperparâmetros e aplicando *early stopping* quando necessário;
7. **Avaliação final:** o desempenho do modelo foi mensurado no conjunto de teste utilizando métricas como acurácia, precisão, *recall* e F1-score, permitindo uma análise equilibrada de desempenho.

2.3 Extração da Região de Interesse

O primeiro passo para um reconhecimento robusto consiste na normalização da entrada, isolando a área da palma que contém as características biométricas mais relevantes. Para isso, foi implementado o método proposto por Su et al. (95). O processo, ilustrado na Figura 2.2, é composto pelas seguintes etapas:

1. **Detecção de pontos-chave:** identificar dois pontos de referência (A e B) na imagem, localizados nos vales entre os dedos;
2. **Alinhamento:** rotacionar a imagem de forma que a linha que conecta os pontos A e B fique perfeitamente alinhada ao eixo horizontal;

3. **Recorte (*crop*)**: definir uma área quadrada centrada na palma, cujo lado mede $1,2 \times |AB|$, onde $|AB|$ representa a distância euclidiana entre os pontos A e B. Esta área constitui a Região de Interesse (ROI).

Para automatizar esta etapa, foi adotado um sistema composto por dois modelos: inicialmente, uma rede YOLOv5-lite [Chen e Gong \(19\)](#) é utilizada para a detecção da mão; em seguida, uma HRNet, baseada na implementação do MMPose [\(79\)](#), processa a imagem detectada a fim de extrair as coordenadas precisas dos pontos-chave. Os dados de treinamento para estes modelos foram preparados utilizando a ferramenta de anotação COCO Annotator [\(16\)](#).

A Figura 2.2 apresenta uma ilustração adaptada do método de aquisição da ROI, enquanto a Figura 2.3 detalha, em formato de fluxograma, o processo completo desde a imagem bruta até a obtenção da área de interesse.

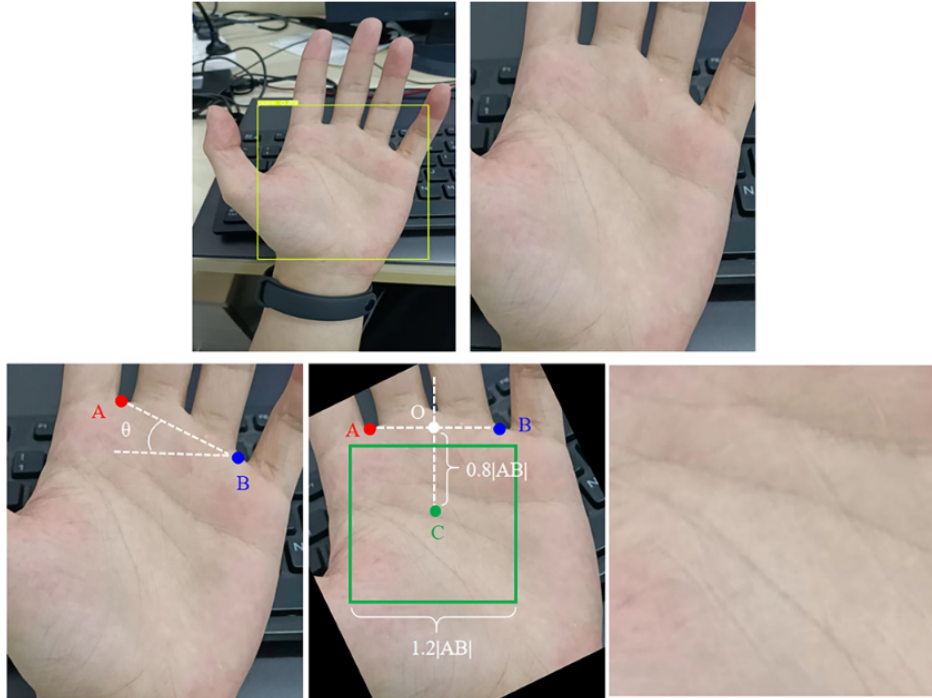


Figura 2.2: Método para aquisição da ROI, adaptado de [Su et al. \(95\)](#).

2.4 Extração de Características e Autenticação

Após a obtenção da *Região de Interesse* (ROI), procede-se à sua análise por um modelo de extração de características treinado para gerar um descritor único e discriminativo.

2.4.1 Arquitetura do Modelo

O modelo adota como *backbone* a EfficientNet [\(104\)](#), previamente treinada na base de dados ImageNet. A camada de classificação final da rede foi removida e substituída por camadas customizadas responsáveis por transformar o vetor de características original, com 1280 dimensões, em um *embedding* final de 512 dimensões.

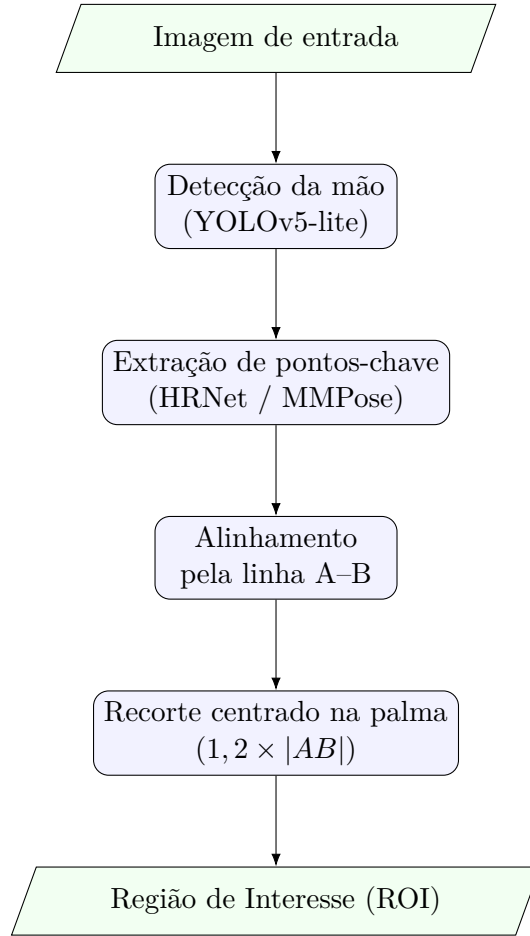


Figura 2.3: Fluxograma do processo de extração da ROI, desde a imagem bruta até a obtenção da área de interesse para autenticação.

2.4.2 Função de Perda

O treinamento foi otimizado por meio da função de perda *SubCenter ArcFace* (28), utilizando a implementação descrita em (66). Essa técnica ajusta o espaço de características de modo a maximizar a distância entre *embeddings* de identidades distintas e minimizar a distância entre *embeddings* da mesma identidade. A abordagem de *sub-centro* permite ao modelo aprender representações mais ricas ao definir múltiplos vetores centrais para cada classe (identidade).

2.4.3 Processo de Autenticação

A autenticação consiste na comparação entre os *embeddings* extraídos de duas imagens de palma. A similaridade é calculada pelo cosseno do ângulo entre os vetores correspondentes, sendo que um valor acima de um limiar pré-definido caracteriza uma correspondência positiva, autenticando o usuário.

2.5 Bases de Dados

O treinamento dos modelos descritos na metodologia demandou o uso de bases de dados distintas para cada tarefa específica. A seguir, são detalhadas as bases utilizadas tanto no treinamento do modelo de extração de características quanto nos modelos de aquisição da *Região de Interesse* (ROI).

2.5.1 Treinamento do Modelo de Extração de Características

Para o treinamento do modelo de reconhecimento da palma da mão, baseado na EfficientNet, foi construída uma base de dados agregada a partir de múltiplos conjuntos públicos. As bases empregadas foram:

- 11k Hands (3);
- SMPD (47);
- MPD (111);
- Tongji (110);
- REST (18).

O conjunto combinado totalizou aproximadamente 40.000 imagens, correspondentes a cerca de 1.000 identidades distintas.

Neste trabalho, foram utilizadas apenas as ROIs já extraídas e normalizadas desses conjuntos. As imagens foram organizadas em uma estrutura de diretórios, em que cada pasta corresponde a uma identidade única.

2.5.2 Treinamento dos Modelos de Aquisição da ROI

O treinamento dos modelos responsáveis pela aquisição da ROI – YOLOv5-lite para detecção da mão e HRNet para extração de pontos-chave – utilizou uma base distinta, composta por imagens com anotações de *bounding boxes* e *keypoints*. As bases empregadas foram:

- MPD (111): 966 imagens anotadas manualmente para esta tarefa;
- RPG1K (59): 971 imagens anotadas manualmente para esta tarefa;
- REST (18): 48 imagens anotadas manualmente;
- 11k Hands (3): 16 imagens anotadas manualmente.

2.6 Resultados e Discussão

Nesta seção, são apresentados os resultados obtidos em cada etapa da *pipeline*, seguidos de uma análise crítica sobre o desempenho observado.

2.6.1 Desempenho da Extração da ROI

O primeiro passo da avaliação consistiu em verificar a eficácia do sistema de aquisição da *Região de Interesse* (ROI). Do conjunto total de aproximadamente 40.000 imagens disponíveis, o sistema de detecção conseguiu extrair a ROI com sucesso em cerca de 35.000 imagens.

O critério para considerar uma extração bem-sucedida foi a obtenção de uma pontuação de confiança maior ou igual a 0,3 para todos os pontos-chave necessários. Isso representa uma taxa de sucesso de aproximadamente 87,5%.

Apesar da elevada taxa de acerto, o método não é imune a poses incomuns ou à oclusão dos dedos. A Figura 2.4 apresenta um exemplo típico em que a inclinação da mão impede a detecção confiável dos pontos A e B, resultando na perda da ROI.

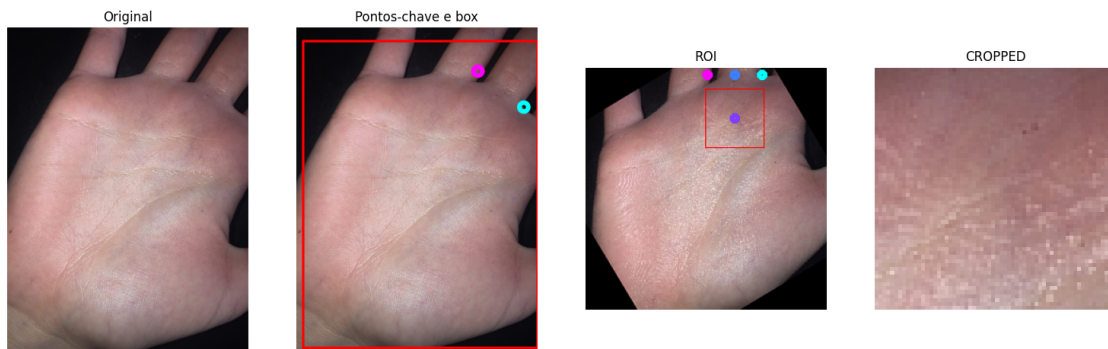


Figura 2.4: Exemplo de falha na extração da ROI devido a poses e oclusões.

2.6.2 Desempenho do Modelo de Reconhecimento

O modelo de extração de características foi treinado utilizando as 35.000 ROIs obtidas com sucesso. Sua performance foi avaliada com base em duas métricas amplamente utilizadas em sistemas biométricos:

- **Taxa de Falsa Aceitação** (*False Acceptance Rate* – FAR): frequência com que o sistema autentica indevidamente um indivíduo não autorizado (considera duas pessoas distintas como sendo a mesma);
- **Taxa de Falsa Rejeição** (*False Rejection Rate* – FRR): frequência com que o sistema rejeita indevidamente um indivíduo autorizado (considera a mesma pessoa como sendo duas diferentes).

Com um limiar de similaridade de cossenos definido em 0,3, o sistema alcançou um FAR de 0,2% e um FRR de 2,26%.

Em termos práticos:

- a cada 1.000 tentativas de autenticação por impostores, aproximadamente 2 seriam aceitas indevidamente;
- a cada 100 tentativas de autenticação de usuários legítimos, cerca de 2 seriam rejeitadas indevidamente.

A relação completa entre FAR e FRR para diferentes valores de limiar é apresentada na Figura 2.5.

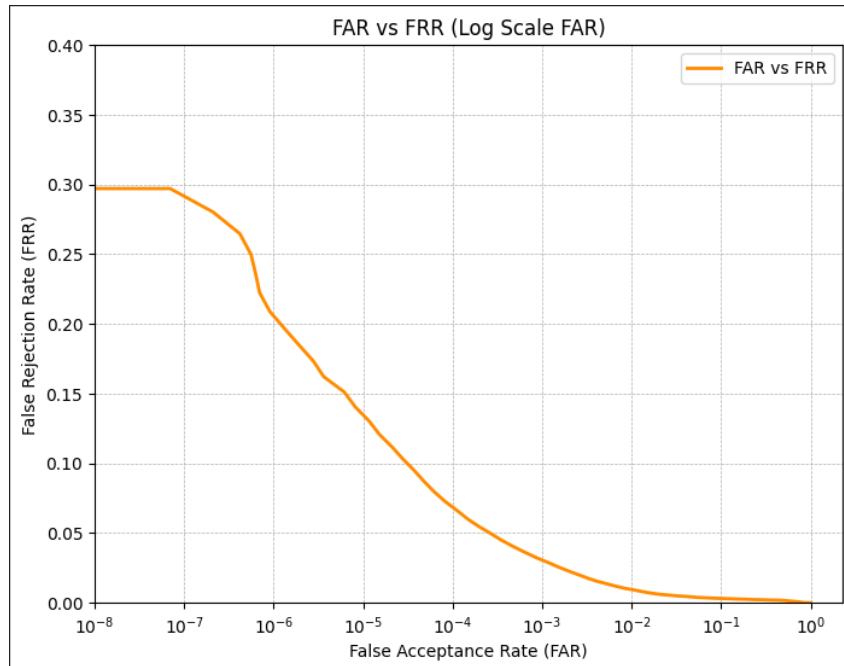


Figura 2.5: Curva de desempenho do sistema, mostrando a relação entre FAR e FRR.

2.7 Conclusão

Os resultados obtidos suscitaram a hipótese de um possível vazamento de dados, isto é, a utilização, nos testes, de informações já presentes no treinamento do modelo. Essa possibilidade, contudo, foi descartada, uma vez que se garantiu que nenhuma identidade presente no conjunto de treino foi utilizada nos conjuntos de validação ou de teste.

A explicação mais plausível para o elevado desempenho reside no fato de que, embora as imagens pertençam a indivíduos distintos, todas foram obtidas a partir das mesmas bases públicas. Assim, compartilham características semelhantes de iluminação, qualidade e tipo de câmera. Esse fator pode levar a uma superestimação do desempenho do modelo, o qual tende a se apresentar superior ao que se verificaria em condições reais, nas quais há muito mais variabilidade.

Durante testes exploratórios do *proof of concept* (PoC) disponível em <https://enzobrum.github.io/visao-computacional/>, observou-se que o modelo é particularmente sensível às condições de iluminação, apresentando, por exemplo, classificações divergentes para duas imagens da mesma mão capturadas sob luz amarela e luz branca. Tal comportamento aponta para um potencial eixo de aprimoramento futuro.

Para uma validação mais robusta da capacidade do sistema, seria recomendável a realização de testes utilizando uma base de dados completamente nova e previamente desconhecida pelo modelo. No entanto, tal abordagem não pôde ser implementada no presente trabalho devido a limitações de tempo.

3 Assistente Virtual Jurídico com Mecanismos Avançados de Garantia de Privacidade

Autor: Lucas Coelho Pini de Sousa

Tutor: Wellington Fernandes Silvano

3.1 Introdução

Nas primeiras semanas do projeto, foram realizadas extensas sessões de pesquisa, leitura e estudo, com o objetivo de compreender as ferramentas disponíveis, identificar os principais problemas e dificuldades a serem enfrentados e definir a estrutura e a arquitetura da solução proposta. Desde o início, a identificação de dados sensíveis apresentou-se como uma das principais preocupações, dada a complexidade inerente a essa tarefa.

O planejamento inicial previa a implementação e utilização de algoritmos de *Named Entity Recognition* (NER) para lidar com esse desafio. Entretanto, durante a análise de fóruns especializados sobre o tema, observou-se a recorrente recomendação do uso de inferência baseada em modelos de linguagem para essa finalidade.

A constatação de que essa abordagem se apresenta, atualmente, como uma alternativa viável e eficiente motivou sua adoção no projeto. Essa escolha também foi impulsionada por uma motivação pessoal: a curiosidade em explorar os limites e as capacidades das ferramentas de *Inteligência Artificial* (IA) generativa, que têm recebido grande destaque, tanto no contexto acadêmico quanto no mercado.

Ao longo do desenvolvimento, foram realizadas reuniões pontuais com o orientador designado, Wellington Fernandes Silvano, as quais se mostraram fundamentais para o avanço do projeto e para o aprofundamento em aspectos específicos da disciplina e da solução proposta. As principais discussões concentraram-se no escopo do trabalho, bem como nas ferramentas e técnicas passíveis de aplicação na solução final.

Entre os pontos de destaque desses encontros, incluem-se:

- a definição do conjunto de documentos que comporia a base teórica utilizada pelo assistente;
- a escolha do *framework* para a geração da interface gráfica;
- a discussão sobre parâmetros e modelos de linguagem;

- uma visão geral sobre o contexto do registro civil;
- sugestões para a apresentação da prova de conceito.

Adicionalmente, merecem destaque as reuniões realizadas com a comitiva da Corregedoria do Foro Extrajudicial do TJ-SC e o *Workshop* que contou com a presença de Luis Carlos Vendramin Júnior, presidente do Operador Nacional do Registro Civil de Pessoas Naturais (ON-RCPN). Ambos os encontros contribuíram para a divulgação do trabalho e trouxeram comentários e preocupações pertinentes aos respectivos contextos, resultando em aprimoramentos na proposta desenvolvida.

3.2 Objetivos do Projeto

O objetivo geral deste projeto é desenvolver um assistente virtual capaz de fornecer orientação jurídica básica no contexto do registro civil, assegurando a proteção da privacidade dos dados sensíveis tratados durante as interações com o usuário.

De forma específica, o projeto busca:

- implementar mecanismos eficientes para detecção e anonimização automática de dados sensíveis em documentos e consultas textuais;
- integrar modelos de linguagem de última geração para compreensão e resposta a perguntas jurídicas em linguagem natural;
- criar uma interface gráfica interativa e intuitiva, que permita ao usuário acessar informações jurídicas de forma prática e segura;
- adotar práticas e tecnologias que garantam conformidade com a *Lei Geral de Proteção de Dados Pessoais* (LGPD) e demais normativas aplicáveis;
- validar a solução por meio de uma prova de conceito funcional, utilizando um conjunto de documentos e consultas representativas do contexto real.

3.3 Solução

O sistema desenvolvido neste projeto consiste em um assistente conversacional interativo, implementado sobre uma arquitetura de *Retrieval-Augmented Generation* (RAG) aliada a um robusto componente de preservação da privacidade. Seu objetivo central é fornecer respostas contextualmente relevantes, extraídas de uma base de conhecimentos previamente estruturada, assegurando que quaisquer dados sensíveis fornecidos pelo usuário sejam identificados e anonimizados antes de qualquer processamento ou geração de resposta.

A arquitetura adotada é modular e organiza-se em quatro camadas principais, que operam de forma sequencial:

1. **Camada de Apresentação:** interface responsável pela interação com o usuário, recebendo entradas textuais e exibindo as respostas geradas;

2. **Camada de Orquestração:** coordena o fluxo de dados entre os diferentes módulos, garantindo a execução ordenada das etapas de processamento;
3. **Módulo de Processamento de Dados:** responsável por detectar e anonimizar dados sensíveis, aplicando técnicas de *Named Entity Recognition* (NER) e filtros de privacidade;
4. **Módulo de Geração da Resposta:** utiliza modelos de linguagem aliados à arquitetura RAG para formular respostas precisas, considerando tanto o contexto fornecido pelo usuário quanto a base de conhecimentos.

A Figura 3.1 apresenta uma visão esquemática da arquitetura proposta, destacando a sequência de operações desde a entrada do usuário até a entrega da resposta final.

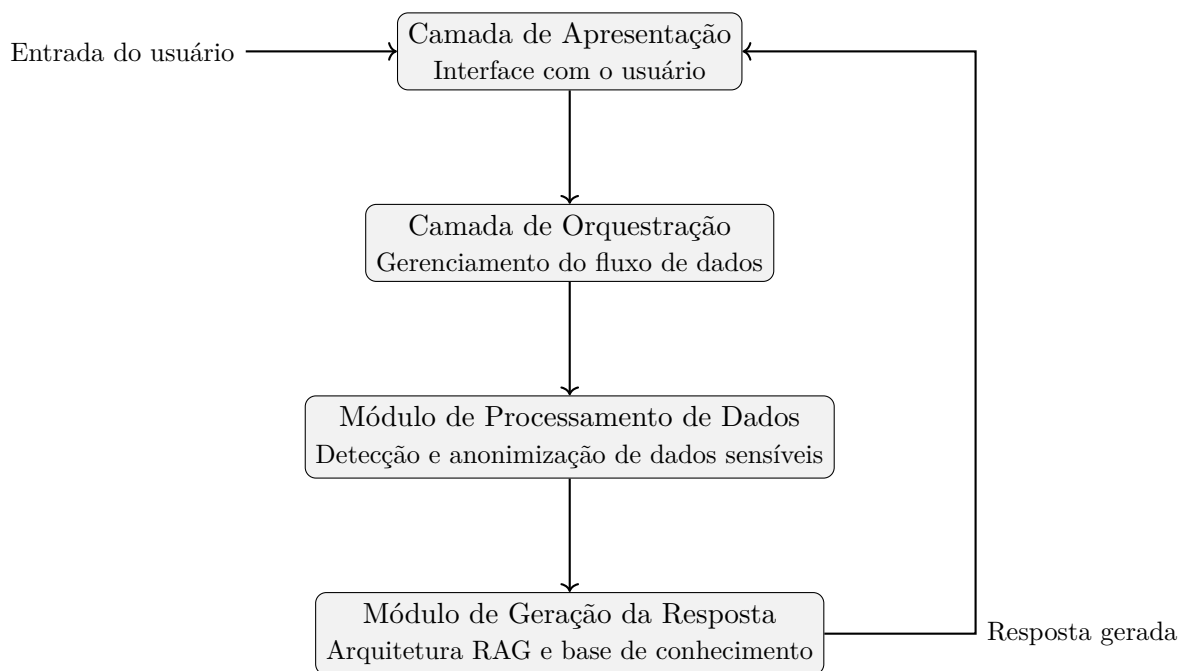


Figura 3.1: Arquitetura modular do assistente virtual com preservação de privacidade.

O fluxo representado na Figura 3.1 pode ser descrito da seguinte forma:

1. O usuário envia uma consulta textual por meio da **Camada de Apresentação**;
2. A **Camada de Orquestração** recebe a solicitação e direciona o conteúdo para os módulos apropriados, garantindo que as etapas sejam processadas na ordem correta;
3. O **Módulo de Processamento de Dados** analisa a entrada, detecta entidades sensíveis e realiza a anonimização necessária, de forma a proteger a privacidade antes de qualquer uso do conteúdo;
4. O **Módulo de Geração da Resposta**, utilizando a arquitetura RAG, busca informações relevantes na base de conhecimentos e produz uma resposta personalizada;
5. A resposta é enviada de volta à **Camada de Apresentação**, que a exibe ao usuário, completando o ciclo de interação.

Essa arquitetura modular apresenta vantagens significativas, como a possibilidade de substituição ou atualização independente de cada camada, facilitando a evolução tecnológica do sistema. Além disso, a separação clara entre o processamento de dados e a geração de respostas contribui para a conformidade com a *Lei Geral de Proteção de Dados Pessoais* (LGPD), permitindo que a privacidade seja tratada como um requisito fundamental e transversal. A abordagem também favorece a escalabilidade, permitindo que novas fontes de dados ou modelos de linguagem mais avançados sejam integrados sem a necessidade de reestruturar toda a solução.

3.4 Camada de Apresentação

A interface com o usuário consiste em uma aplicação *web* interativa, cuja função primária é possibilitar a comunicação entre o usuário e o sistema, delegando todo o processamento complexo às camadas inferiores. Foi projetada para simular uma conversa em tempo real no formato de *chat*.

Esta camada desempenha as seguintes funções principais:

- apresentar o histórico da conversa de forma sequencial e organizada;
- capturar novas perguntas ou solicitações do usuário por meio de um campo de entrada de texto;
- exibir as respostas finais geradas pelo sistema, incluindo, quando necessário, elementos visuais complementares para detalhamento do processo.

Do ponto de vista tecnológico, a camada foi implementada utilizando *frameworks* modernos de desenvolvimento *web*, como *React.js* para a construção de interfaces dinâmicas e responsivas, e bibliotecas de estilização como *Tailwind CSS* para padronização visual e adaptação a diferentes dispositivos. A comunicação com a *Camada de Orquestração* é realizada por meio de requisições HTTP assíncronas (*AJAX* ou *fetch API*), permitindo que o fluxo de mensagens seja atualizado em tempo real sem recarregamento da página. Além disso, foram incorporadas boas práticas de *UX design* para garantir acessibilidade, clareza na apresentação das respostas e uma experiência de uso intuitiva.

3.5 Camada de Orquestração

Esta camada representa o elemento central da arquitetura, responsável por interligar e sincronizar os módulos funcionais do sistema. Atua como ponto de controle e tomada de decisão, garantindo que o fluxo de dados ocorra de maneira eficiente, coerente e segura. Além de assegurar a correta sequência de execução das tarefas, a Camada de Orquestração também é responsável por manter a integridade das informações trocadas entre os componentes, viabilizando a execução coordenada de operações complexas e a adaptação dinâmica a diferentes contextos de interação.

O núcleo desta camada consiste em um controlador encarregado de:

- Receber a solicitação enviada pelo usuário por meio da Camada de Apresentação;

- Gerenciar o estado da conversa, preservando o histórico de interações para utilização contextual pelo assistente;
- Coordenar, de forma sequencial e/ou paralela, as chamadas aos diferentes subsistemas, incluindo anonimização, busca na base de conhecimento e geração da resposta;
- Formatar a resposta final, assegurando sua conformidade com os requisitos funcionais e linguísticos, antes de encaminhá-la novamente à Camada de Apresentação.

3.6 Módulo de Processamento de Dados

Este módulo concentra as funcionalidades essenciais para a manipulação e preparação dos dados utilizados pelo sistema, englobando tanto o tratamento de informações sensíveis quanto a gestão da base de conhecimento. É composto por dois componentes principais:

- **Componente de Tratamento de Dados Sensíveis:** módulo especializado que emprega um modelo de linguagem treinado (*Mistral 7B*) para identificar e extrair *Personally Identifiable Information* (PII) presentes no texto de entrada. As informações extraídas são temporariamente armazenadas e substituídas por marcadores genéricos (*placeholders*) a fim de preservar a privacidade durante o processamento. Ao final do fluxo, este componente realiza a reidentificação, reinserindo os dados originais na resposta final de forma controlada;
- **Componente de Gerenciamento da Base de Conhecimento:** responsável pela persistência e recuperação de informações oriundas de documentos relevantes ao contexto do registro civil (corpus de conhecimento). Os documentos são processados e segmentados em unidades menores (*chunks*), que são posteriormente convertidas em vetores numéricos por meio de um modelo de *embedding* de texto (*Nomic Embed Text*). Estes vetores são armazenados e indexados em um banco de dados vetorial (*ChromaDB*), possibilitando buscas por similaridade semântica com alta eficiência.

3.7 Módulo de Geração da Resposta

O Módulo de Geração da Resposta constitui a etapa final do fluxo de processamento, sendo responsável por elaborar a resposta a ser enviada ao usuário. Sua principal função é sintetizar uma resposta coerente e contextualizada a partir de um *prompt* estruturado que integra três elementos-chave:

- A solicitação do usuário previamente anonimizada;
- Os trechos de informação semanticamente mais relevantes, recuperados da base de conhecimento;
- O histórico da conversa, utilizado para manter a continuidade e coerência do diálogo.

Para a construção da resposta, este módulo emprega um modelo de linguagem (*Gemma 3 1B*) capaz de interpretar o conjunto de informações fornecidas e formular uma saída textual precisa, mantendo conformidade com o contexto e as diretrizes de comunicação definidas para o sistema.

3.8 Fluxo

Quando o usuário envia uma solicitação, os dados percorrem um fluxo operacional claramente definido, no qual cada etapa é responsável por uma função específica dentro da arquitetura do sistema:

1. **Entrada:** a solicitação é recebida pela Camada de Apresentação e encaminhada aos módulos de processamento;
2. **Anonimização:** o Componente de Tratamento de Dados Sensíveis é acionado para identificar informações pessoais (*Personally Identifiable Information* - PII), substituí-las por marcadores genéricos (*placeholders*) e armazená-las temporariamente para uso posterior;
3. **Busca por Similaridade:** a solicitação anonimizada é convertida em um vetor e utilizada para consultar o banco de dados vetorial. São então recuperados os trechos de texto mais relevantes da base de conhecimento, com base em similaridade semântica;
4. **Composição do Contexto:** os trechos recuperados (contexto) são combinados com a solicitação anonimizada e o histórico da conversa, formando um *prompt* estruturado que servirá como entrada para o assistente;
5. **Síntese da Resposta:** o *prompt* completo é processado pelo Módulo de Geração da Resposta, que elabora uma saída textual coerente e contextualizada;
6. **Reidentificação:** a resposta gerada, que pode conter marcadores genéricos, é novamente processada pelo Componente de Tratamento de Dados Sensíveis para restaurar as informações pessoais originais do usuário;
7. **Saída:** a resposta final, agora completa e personalizada, é encaminhada à Camada de Apresentação para exibição ao usuário.

3.9 Conclusão

Este trabalho resultou no desenvolvimento bem-sucedido de um assistente virtual para orientação jurídica, demonstrando a viabilidade de integrar a arquitetura de *Retrieval-Augmented Generation* (RAG) a um mecanismo robusto de preservação da privacidade.

A principal inovação consiste na implementação de um fluxo integrado de anonimização e reidentificação, apoiado em um modelo de linguagem especializado para a proteção de dados sensíveis, possibilitando que o usuário interaja de forma segura e confidencial. A arquitetura modular proposta, capaz de orquestrar diferentes modelos de Inteligência

Artificial para tarefas especializadas, como detecção de entidades, busca semântica e síntese de respostas, mostrou-se uma abordagem eficaz e contemporânea para solucionar um problema de alta complexidade e relevância social.

O projeto ultrapassa o caráter de prova de conceito técnica, posicionando-se como uma solução de aplicabilidade prática, evidenciada pelo interesse e *feedback* positivo de entidades como o Foro Extrajudicial do TJ-SC. Ao atender simultaneamente à necessidade de democratizar o acesso à informação jurídica e resguardar o direito fundamental à privacidade, a solução proposta estabelece bases sólidas para futuras implementações tanto no setor público quanto no privado.

Como trabalhos futuros, recomenda-se a ampliação do corpus de conhecimento, o aperfeiçoamento contínuo dos modelos empregados e a condução de avaliações sistemáticas de desempenho, a fim de consolidar a ferramenta como um recurso confiável e de referência para o cidadão.

Em síntese, este estudo reafirma que é possível aliar inovação tecnológica e responsabilidade ética, pavimentando o caminho para um ecossistema de inteligência artificial verdadeiramente centrado no ser humano.

4 Proteção de Registros Civis com Criptografia Pós-Quântica e Otimização Baseada em IA

Autor: Davi Ludvig Longen Machado

Tutor: Matheus Saldanha

4.1 Introdução

Este capítulo apresenta as experiências do autor durante a disciplina INE 5448 – Inteligência Artificial e Segurança, ministrada pelo professor Ricardo Custódio.

Na primeira fase da disciplina Tópicos Especiais em Aplicações Tecnológicas I (Segurança e Inteligência Artificial), foi disponibilizado um guia com as diretrizes da chamada “Fase Exploratória”. Esse documento estabelecia os objetivos iniciais para o desenvolvimento de um projeto com escopo definido, inserido no contexto da aplicação de Segurança e IA no Registro Civil Brasileiro.

Como ponto de partida, o professor apresentou uma lista com aproximadamente vinte propostas de temas, abrangendo desde verificação biométrica robusta até a aplicação de algoritmos de criptografia pós-quântica. Cada aluno deveria escolher um desses temas (ou propor uma variação), realizar uma revisão de literatura e definir um escopo factível para o desenvolvimento de um *Minimum Viable Product* (MVP) ao longo do semestre.

Conforme descrito no documento orientador da disciplina, essa fase inicial teve duração de duas semanas e seus principais objetivos foram:

- Escolher um tema dentro do escopo da disciplina;
- Levantar o estado da arte técnico e científico relacionado ao tema;
- Delimitar um escopo concreto para o projeto;
- Definir métricas claras e mensuráveis para avaliação do MVP.

Este relatório apresenta, nas seções seguintes, a justificativa da escolha do tema, a revisão bibliográfica, a definição detalhada do escopo e da arquitetura da solução, bem como as métricas de sucesso que orientarão as próximas etapas do projeto.

O tema selecionado foi “Proteção Quanticamente Segura com Otimização por IA para Registros Civis”, cuja proposta envolve o uso de algoritmos de criptografia pós-quântica (*Post-Quantum Cryptography* – PQC) combinados com técnicas de inteligência artificial para otimizar o desempenho e a segurança na proteção de dados sensíveis do registro civil.

4.1.1 Justificativa do tema

A escolha do tema “Proteção Quanticamente Segura com Otimização por IA para Registros Civis” foi motivada por um forte interesse pessoal na área de criptografia pós-quântica (*Post-Quantum Cryptography* – PQC), amplamente explorada no contexto das atividades desenvolvidas no Laboratório de Segurança em Computação (LabSEC) e em projetos vinculados à Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), como o projeto Hawa.

A experiência prévia com algoritmos como o *CRYSTALS-Dilithium* possibilitou que a proposta surgisse de forma natural, configurando-se como uma oportunidade de aplicar e aprofundar conhecimentos adquiridos, além de explorar uma fronteira tecnológica de elevada relevância para a segurança da informação.

4.1.2 Motivação

A motivação técnica decorre do cenário atual: com a padronização dos algoritmos pós-quânticos pelo Instituto Nacional de Padrões e Tecnologia dos Estados Unidos (*National Institute of Standards and Technology* – NIST), torna-se cada vez mais urgente considerar sua integração a sistemas críticos, como os de registro civil. Nesse contexto, o projeto propõe não apenas a aplicação desses algoritmos em um *Minimum Viable Product* (MVP) funcional, mas também a incorporação de técnicas de inteligência artificial para otimização, com o objetivo de reduzir tempos de processamento e aprimorar a robustez das operações criptográficas em cenários reais de uso.

4.2 Revisão de artigos e ferramentas

A revisão da literatura identificou quatro trabalhos principais que fundamentam o desenvolvimento do projeto:

- [Dash e Ullah \(27\)](#) discutem o impacto conjunto da computação quântica e da inteligência artificial na cibersegurança, ressaltando a necessidade de soluções híbridas que combinem criptografia pós-quântica (*Post-Quantum Cryptography* – PQC) e técnicas de *machine learning*;
- [Kumar e Weaver \(54\)](#) abordam o uso de inteligência artificial para otimização de algoritmos criptográficos, enfatizando a relevância de *frameworks* colaborativos entre governo e setor privado para viabilizar a transição para padrões pós-quânticos;
- [Blackledge e Mosola \(10\)](#) apresentam aplicações de IA, como redes neurais e computação evolutiva, no desenvolvimento de cifras mais robustas e na análise de entropia – técnicas com potencial para aprimorar esquemas de criptografia pós-quântica;

- Yusuf et al. (108) analisam a viabilidade de soluções criptográficas otimizadas por IA em ambientes com recursos limitados, como pequenas empresas, fornecendo subsídios relevantes para o contexto do registro civil brasileiro.

No levantamento de iniciativas e ferramentas, destacam-se o projeto *Open Quantum Safe*, as bibliotecas *liboqs* e *Bouncy Castle*, e os *frameworks* de IA *TensorFlow* e *PyTorch*, todos adequados para a experimentação prática do *Minimum Viable Product* (MVP). Tecnologias complementares, como o *Optuna* (para otimização de hiperparâmetros) e o *Qiskit* (para simulação quântica), também foram mapeadas.

No campo legal e ético, foram consideradas diretrizes como a Lei Geral de Proteção de Dados Pessoais (LGPD) (14) e o Marco Civil da Internet (13), que impõem obrigações rigorosas relativas à proteção de dados e à privacidade. A conformidade com essas legislações será parte integrante do projeto, assegurando que as soluções propostas atendam tanto a requisitos técnicos quanto a normativos.

4.3 Relato da disciplina e provas de conceito propostas

A base conceitual desenvolvida durante a disciplina permitiu avançar com clareza na definição do escopo técnico do *Minimum Viable Product* (MVP), arquitetado como um sistema baseado em microsserviços, composto por módulos dedicados à criptografia, otimização com IA, gerenciamento de registros e *API Gateway*. Essa estrutura modular foi concebida para facilitar testes, experimentações e futuras integrações.

A continuidade do projeto foi planejada com foco no desenvolvimento dos componentes definidos e na validação das métricas de sucesso previamente estabelecidas, como tempo de assinatura, consumo de recursos e resiliência criptográfica frente a simulações de ataque.

A proposta original, intitulada “Proteção Quanticamente Segura com Otimização por IA para Registros Civis”, avançou até a etapa de integração com banco de dados. Foi desenvolvido um sistema que expõe uma *REST API* para geração de chaves pós-quânticas no padrão *CRYSTALS-Dilithium*, com armazenamento seguro dessas chaves utilizando criptografia baseada no *CRYSTALS-Kyber*. Essa arquitetura preserva a modularidade do MVP, mantendo a base em microsserviços e prevendo suporte para testes de otimização futura com IA, conforme planejado inicialmente.

Todo o sistema foi orquestrado com *Docker*, permitindo a composição e gerenciamento dos microsserviços. A aplicação, na versão atual, possibilita que agentes externos (por exemplo, sistemas de registro civil simulados) solicitem a criação e o armazenamento seguro de chaves criptográficas resistentes a ataques quânticos, cumprindo integralmente os objetivos da primeira metade do projeto.

A etapa seguinte, envolvendo a camada de inteligência artificial para otimização dinâmica dos algoritmos e do fluxo de assinaturas, está prevista para a fase de refinamento. Nessa fase, um agente poderá solicitar a criação de novas chaves ou a recuperação de chaves previamente geradas, encapsuladas de forma segura no banco de dados.

Paralelamente, foi desenvolvido um sistema denominado “Resumo Automático de Legislações ou Normas”, que consiste em um agente de IA para sumarização de textos ju-

rídicos complexos, como provimentos da Corregedoria Nacional de Justiça. Esse sistema utiliza modelos como o *LLaMA 3*, integrados via *ChatGroq*, oferecendo uma interface em formato de chat, suporte a entradas em PDF e HTML, armazenamento cifrado das interações (via *Fernet*) e formatação dos resumos em *Markdown*, com possibilidade de exportação para PDF. Apesar das limitações decorrentes do uso de um modelo gratuito, a solução demonstrou utilidade prática para operadores do registro civil que necessitam compreender rapidamente legislações extensas.

Durante a apresentação do primeiro projeto, o professor responsável sugeriu um redirecionamento do trabalho para um caso de uso mais específico, com foco em IA aplicada. A nova proposta envolve a construção de um sistema capaz de extrair automaticamente dados do signatário (nome e data) a partir de uma assinatura manuscrita em documento escaneado, normalmente no formato de rubrica – funcionalidade de alta relevância para validações posteriores em contextos forenses, notariais ou pós-morte.

O desenvolvimento desse novo MVP, descrito no relatório “OCR Signature PMSS”, utiliza:

- Um modelo YOLOv8 (96) treinado para detecção de assinaturas;
- *PyTesseract* (44) para OCR básico, combinado com mecanismos de verificação;
- Um modelo de Reconhecimento de Entidades Nomeadas (*Named Entity Recognition* – NER), especificamente *Ifcc/bert-portuguese-ner*, para extração de nomes;
- Um *pipeline* de reconstrução textual para corrigir saídas incorretas do OCR.

Em reunião com o tutor da disciplina, Matheus Saldanha, foram discutidos o estado atual e os próximos passos do projeto de OCR de assinaturas manuscritas. Na ocasião, apresentou-se a integração parcial das tecnologias de OCR (incluindo *PyTesseract*, *PaddleOCR* e modelos NER da Hugging Face) em um fluxo coeso. O tutor validou a abordagem, ressaltando que, embora ainda em desenvolvimento, o sistema já representa uma prova de conceito (*Proof of Concept* – POC) viável e promissora, com maturidade suficiente para ser apresentada em eventos como o LabSEC Day e o WARC.

Para aumentar a eficácia do OCR em manuscritos, foram definidos padrões de entrada para os testes iniciais:

- Documentos escaneados com conteúdo alinhado verticalmente;
- Texto próximo à assinatura digitado em fonte digital;
- Nome do signatário e data posicionados próximos à rubrica.

Esses padrões visam reduzir a variabilidade dos dados de entrada e melhorar a precisão das etapas de extração.

Na fase intermediária do projeto, o sistema de OCR foi apresentado a membros do Tribunal de Justiça de Santa Catarina (TJSC), já integrando:

- Detecção automática de rubricas por meio de modelos YOLOv8;

- Extração de nomes e datas utilizando OCR combinado com NER;
- Um fluxo funcional para processamento de documentos escaneados e identificação automática de elementos de assinatura.

A apresentação no TJSC gerou questionamentos construtivos e serviu como teste realista de aplicabilidade em ambiente institucional. O sistema demonstrado é essencialmente o mesmo que será apresentado no LabSEC Day e no WARC, com nível de maturidade superior ao típico MVP acadêmico, reforçando seu potencial para aplicação prática no ecossistema do Registro Civil brasileiro.

4.4 Prova de Conceito

Na etapa final do desenvolvimento, o projeto atingiu um marco relevante ao concluir a integração de todos os módulos em uma prova de conceito (*Proof of Concept* – POC) funcional e demonstrável, conectada a uma *branch* personalizada do sistema ADES, mantida por um aluno de Trabalho de Conclusão de Curso (TCC) sob orientação do professor Ricardo Custódio.

Essa versão final do sistema foi projetada com o objetivo de automatizar a conversão de documentos contendo assinaturas manuscritas (rubricas) em versões eletrônicas assinadas digitalmente, preservando validade jurídica.

A solução representa um avanço expressivo para o uso de esquemas de assinatura digital *post mortem* (*Post Mortem Signature Scheme*), especialmente aplicáveis em contextos como inventários e partilhas, preservação histórica e digitalização de acervos documentais sensíveis.

4.5 Componentes utilizados

O desenvolvimento da solução envolveu a integração de diversos componentes de software e modelos de inteligência artificial, conforme descrito a seguir:

- YOLOv8 (96) para detecção precisa da região contendo a assinatura manuscrita;
- *PaddleOCR* (24) e *PyTesseract* para extração textual, abrangendo tanto conteúdo manuscrito quanto impresso;
- Modelo *BERT NER* (26) para identificação de nomes e datas nas áreas adjacentes à rubrica;
- Integração com o assinador ADES, adaptado para possibilitar:
 - Assinaturas digitais retroativas e de uso único;
 - Geração de certificados únicos por documento, com chave privada descartável;
 - Assinatura testemunhal secundária para validação institucional.

Essa integração permitiu que o sistema automatizasse completamente o ciclo de processamento, contemplando as seguintes etapas:

1. Recepção do documento escaneado;
2. Aplicação de OCR combinado com modelos de IA;
3. Extração automática dos dados do signatário;
4. Assinatura digital com certificado temporário;
5. Geração de documento validado digitalmente.

4.6 Aplicação e relevância

A prova de conceito (*Proof of Concept* – POC) foi concebida com foco em aplicabilidade prática no ecossistema jurídico brasileiro, apresentando especial relevância para órgãos de Registro Civil (RC). A tecnologia possibilita:

- Digitalização segura de documentos históricos com valor legal;
- Emissão de assinaturas digitais válidas a partir de documentos físicos contendo rubrica;
- Redução de risco jurídico por meio de validação institucional automatizada e testemunhada.

Além disso, o sistema demonstrou ser escalável e adaptável a contextos mais amplos, como:

- Assinatura de documentos com múltiplas páginas ou múltiplas rubricas;
- Disponibilização de interface gráfica amigável com links diretos para acesso e validação;
- Potencial de evolução para gestão de acervos públicos e integração a iniciativas de transformação digital em âmbito nacional.

4.7 Conclusão

O desenvolvimento deste projeto permitiu percorrer um ciclo completo de concepção, pesquisa, implementação e validação de uma solução de alto valor técnico e social. A experiência destacou-se por oferecer uma exploração prática da interseção entre segurança da informação, inteligência artificial e desafios concretos enfrentados pelo Registro Civil brasileiro.

Inicialmente voltado à proteção quanticamente segura de dados com apoio de IA, o projeto evoluiu ao longo do semestre para atender a uma demanda mais específica: a automatização da extração e assinatura digital de documentos contendo rubricas manuscritas, especialmente no contexto de assinaturas *post mortem*. Essa mudança de direcionamento foi essencial para alinhar os interesses técnicos do autor às necessidades reais discutidas em sala de aula e com o professor responsável, resultando em um sistema mais focado, tangível e aplicável.

As diversas etapas, desde o estudo do estado da arte, passando por provas de conceito parciais, até a integração final com uma *branch* personalizada do sistema ADES, possibilitaram aprendizado significativo sobre arquitetura de microserviços, processamento de linguagem natural, reconhecimento óptico de caracteres (OCR), criptografia pós-quântica e validações jurídicas digitais.

Além dos resultados técnicos, destaca-se o amadurecimento comunicacional e a capacidade de apresentar e defender o projeto para diferentes públicos, incluindo membros do Tribunal de Justiça de Santa Catarina (TJSC), pesquisadores e professores do LabSEC, e participantes do WARC 2025. A apresentação neste último evento foi particularmente marcante, com boa recepção e interação qualificada, permitindo ao autor expor de forma clara os desafios e soluções propostos.

Essas experiências foram valiosas não apenas para o amadurecimento técnico, mas também para a formação profissional do autor como engenheiro da computação, com sólida base em segurança da informação, inovação e pensamento crítico voltado à aplicabilidade social da tecnologia.

O projeto deixa um legado viável para continuidade futura, seja na forma de aprimoramentos técnicos, discussões normativas e jurídicas, integrações institucionais ou como ponto de partida para novas iniciativas de pesquisa e extensão universitária.

Agradecimentos: O autor expressa sua profunda gratidão a todos os envolvidos na realização desta disciplina. Em especial, agradece ao professor Ricardo Custódio, cujo empenho e visão tornaram a disciplina possível. Agradece também aos tutores, profissionais brilhantes e pessoas inspiradoras, cuja orientação e paciência foram fundamentais. Foi um privilégio poder aprender com todos, deixando aqui um sincero abraço e o desejo de reencontros em futuras oportunidades igualmente enriquecedoras.

O sistema desenvolvido abre novos horizontes de pesquisa, incluindo:

- Investigação normativa e legal sobre assinaturas *post mortem*;
- Definição de entidades legitimadas a assinar em nome de falecidos;
- Análise ética e jurídica sobre representação de vontade;
- Aprimoramento contínuo com novas técnicas de OCR e modelos avançados de reconstrução textual;
- Adoção em ambientes com alto volume documental, integrando-se a políticas públicas de digitalização.

5 Autenticação Biométrica Segura com Provas de Conhecimento Zero

Autor: Alex Davis Neuwiem da Silva

Tutor: Gustavo Zambonin

5.1 Introdução

Este capítulo apresenta o projeto intitulado “Autenticação Biométrica com Provas de Conhecimento Zero”, cujo objetivo é desenvolver um sistema de autenticação que combina um modelo de Inteligência Artificial (IA) para reconhecimento biométrico com um protocolo de segurança baseado em Provas de Conhecimento Zero (PCZs).

A proposta visa garantir um método de verificação de identidade seguro e que preserve a privacidade dos usuários, eliminando a necessidade de armazenar ou transmitir dados biométricos completos. Para tal, propõe-se um sistema em que os dados biométricos sejam armazenados de forma criptografada e distribuída, reduzindo significativamente o risco de comprometimento em caso de ataques. Com o uso de PCZs, a validação da identidade do usuário ocorre sem a exposição dos dados biométricos, elevando o nível de privacidade.

Ao contrário das senhas, dados biométricos constituem identificadores únicos e irreversíveis, de modo que sua proteção é essencial. O método proposto acrescenta uma camada adicional de segurança, tornando o processo mais resiliente frente a tentativas de ataque no contexto de autenticação biométrica.

O repositório com o código-fonte do sistema desenvolvido está disponível em:

<https://github.com/AlexDavisNeuwiem/INE5448>

A demonstração prática em vídeo do projeto pode ser acessada no link:

<https://youtu.be/NZuAtn9qfy4>

O desenvolvimento deste trabalho buscou explorar a segurança e a eficiência das PCZs em um cenário real de autenticação, contribuindo para um estudo mais aprofundado e alinhado com os desafios atuais da área.

5.2 Fundamentação Teórica

As Provas de Conhecimento Zero (*Zero-Knowledge Proofs* – ZKPs) são protocolos criptográficos que permitem a um *providor* convencer um *verificador* de que uma determinada afirmação é verdadeira, sem revelar qualquer informação adicional além da veracidade da afirmação Goldreich (38) e Fiat e Shamir (35). Esses protocolos devem atender a três propriedades fundamentais:

- **Completeness:** se a afirmação for verdadeira, o verificador será convencido pelo provedor;
- **Solidez** (*soundness*): se a afirmação for falsa, um provedor mal-intencionado dificilmente conseguirá convencer o verificador;
- **Conhecimento Zero:** o verificador não obtém nenhuma informação adicional além do fato de que a afirmação é verdadeira.

As ZKPs podem ser *iterativas*, exigindo múltiplas trocas de mensagens entre provedor e verificador, ou *não iterativas*, como nos esquemas baseados na heurística de Fiat-Shamir (35).

No contexto de autenticação biométrica, a integração com ZKPs surge como uma solução promissora para reforçar a privacidade e a segurança (80). Essa abordagem permite que um usuário comprove sua identidade sem expor os dados biométricos completos, mitigando riscos de interceptação ou vazamento. Trabalhos recentes têm proposto protocolos que associam classificadores biométricos, como *Support Vector Machines* (SVMs), a esquemas de ZKP, como no modelo BioAu-SVM+ZKP, que preserva a privacidade e mantém alta acurácia de autenticação (29).

Outra linha de pesquisa explora a integração de ZKPs com *blockchain* e computação homomórfica para autenticação biométrica descentralizada, como no protocolo BioZero, que combina compromissos de Pedersen e *zk-SNARKs* para garantir verificações eficientes sem expor dados sensíveis (60). Em ambientes comerciais, tecnologias como *Zero-Knowledge Biometrics* empregam computação multipartidária segura para transformar e verificar dados biométricos diretamente no dispositivo do usuário, eliminando a necessidade de armazenamento centralizado (51).

Essa combinação de autenticação biométrica e ZKPs oferece vantagens significativas:

- **Privacidade elevada:** os dados biométricos nunca são expostos ou armazenados em forma bruta;
- **Segurança reforçada:** a prova de identidade é realizada sem transmissão de dados sensíveis;
- **Conformidade regulatória:** alinhamento com legislações de proteção de dados, como a LGPD e o GDPR.

Entretanto, a implementação dessas soluções envolve desafios técnicos relevantes, como a complexidade de integração entre módulos de IA biométrica e protocolos criptográficos avançados, além da necessidade de conscientização e aceitação por parte dos usuários finais.

5.3 Proposta do Sistema

No contexto de reconhecimento facial, cada rosto pode ser representado por um vetor de características, também denominado *embedding*. Conforme demonstrado por [Schroff; Kalenichenko e Philbin \(92\)](#), esses vetores são gerados por redes neurais previamente treinadas com o objetivo de capturar traços faciais distintivos. A comparação entre vetores de *embeddings* é geralmente realizada por meio da métrica de similaridade de cossenos, que calcula o cosseno do ângulo entre dois vetores em um espaço vetorial.

O valor resultante dessa métrica varia entre -1 (vetores opostos) e 1 (vetores idênticos). Valores próximos de 1 indicam alta similaridade, sugerindo que os rostos correspondentes são da mesma pessoa.

Em um sistema tradicional de autenticação facial baseado em similaridade de cossenos, a imagem capturada no momento da autenticação é convertida em um vetor \vec{A} , o qual é comparado com um vetor \vec{B} previamente armazenado durante o cadastro do usuário. A autenticação é considerada bem-sucedida quando a similaridade de cossenos entre \vec{A} e \vec{B} excede um limiar τ , previamente definido com base nas características do modelo de IA utilizado.

Contudo, o armazenamento direto desses vetores representa um risco substancial à segurança e privacidade dos usuários. Como os *embeddings* são representações vetoriais únicas da biometria facial, sua exposição pode permitir reconstrução de imagens ou fraudes por simulação de identidade. Ademais, ao contrário de senhas, os dados biométricos são permanentes e não podem ser substituídos em caso de vazamento.

Para mitigar esses riscos, este projeto propõe a incorporação da verificação de similaridade de cossenos em um circuito de Prova de Conhecimento Zero (PCZ). Especificamente, a verificação da condição $\text{similaridade_de_cossenos}(\vec{A}, \vec{B}) > \tau$ é encapsulada como uma operação dentro de um circuito aritmético. Nesse arranjo, o limiar τ é um parâmetro público, enquanto os vetores \vec{A} e \vec{B} são mantidos como entradas privadas conhecidas apenas pelo provador.

Com isso, torna-se possível realizar a autenticação sem revelar as *embeddings* faciais ao verificador, preservando integralmente a privacidade do usuário. O verificador apenas recebe a prova criptográfica de que a similaridade foi verificada corretamente, sem qualquer exposição dos dados sensíveis.

Essa arquitetura apresenta as seguintes vantagens:

- **Privacidade completa:** os vetores biométricos não são revelados nem armazenados em formato acessível;
- **Segurança elevada:** a prova criptográfica é resistente a engenharia reversa e ataques de reidentificação;
- **Conformidade regulatória:** a solução alinha-se às exigências da LGPD e de regulamentações internacionais sobre proteção de dados biométricos.

A Figura 5.1 ilustra o funcionamento de um esquema do tipo zk-SNARK (*Zero-Knowledge Succinct Non-Interactive Argument of Knowledge*), conforme descrito por [Bitansky et al. \(9\)](#). O circuito aritmético é representado como $C(x, w) \rightarrow f$, onde:

- x : parâmetros públicos, conhecidos por provador e verificador;
- w : testemunha, conhecida apenas pelo provador;
- f : campo finito sobre o qual o circuito é definido.

Durante o pré-processamento, executa-se um algoritmo confiável S , responsável por gerar os parâmetros públicos do circuito: $S(C) \rightarrow (S_p, S_v)$, sendo S_p a chave de prova utilizada pelo provador e S_v a chave de verificação usada pelo verificador.

O provador, de posse de (S_p, x, w) , gera uma prova criptográfica π :

$$\pi \leftarrow \text{Prove}(S_p, x, w)$$

Essa prova é então transmitida ao verificador, que aplica a função:

$$\text{Verify}(S_v, x, \pi)$$

para confirmar a validade da computação encapsulada sem acesso à testemunha w .

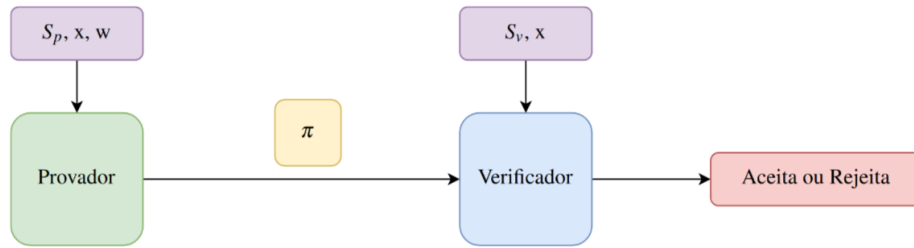


Figura 5.1: Processamento de uma zk-SNARK (9)

A Figura 5.1 resume visualmente o fluxo de geração e verificação de uma prova zk-SNARK, destacando como a computação privada é encapsulada de forma criptograficamente segura, permitindo ao verificador atestar a validade da autenticação sem jamais ter acesso direto aos dados biométricos ou à lógica interna da computação.

5.4 Componentes do Sistema

O protocolo proposto envolve a interação coordenada entre três entidades principais: o usuário, o modelo de Inteligência Artificial (IA) e o servidor. Cada uma dessas entidades desempenha um conjunto distinto de funções, visando assegurar a autenticação com preservação de privacidade por meio de Provas de Conhecimento Zero (PCZs).

O **modelo de IA** é responsável por gerar a representação vetorial da identidade do usuário, denominada *embedding*. Suas funções incluem:

- Gerar a *embedding* a partir dos dados biométricos ou de identidade fornecidos pelo usuário;
- Produzir a PCZ que comprove a similaridade entre duas *embeddings* sem revelar o conteúdo original.

O **usuário** é a entidade que deseja registrar-se e autenticar-se no sistema. Suas responsabilidades abrangem:

- Solicitar o registro e a autenticação;
- Proteger sua chave criptográfica pessoal;
- Armazenar seu identificador único (ID);
- Executar a criptografia da *embedding* antes do envio ao servidor.

O **servidor** atua como ponto central de armazenamento e validação, sem acesso direto às *embeddings* originais nem capacidade de descriptografá-las. Entre suas responsabilidades, destacam-se:

- Conduzir a cerimônia de confiança inicial;
- Armazenar a *embedding* criptografada;
- Fornecer, quando solicitado, a *embedding* criptografada e a chave de prova;
- Verificar a PCZ enviada pelo usuário, validando a autenticidade da identidade.

5.5 Funcionamento do Sistema

Antes do início do protocolo, duas etapas preparatórias são fundamentais para assegurar o correto funcionamento do sistema: o treinamento do modelo de Inteligência Artificial (IA) para reconhecimento facial e a realização da cerimônia de confiança pelo servidor.

O **treinamento do modelo de IA** tem como objetivo capacitar o sistema a identificar e verificar rostos com elevado nível de precisão, utilizando técnicas de aprendizado profundo e extração de características discriminantes.

A **cerimônia de confiança** estabelece os parâmetros criptográficos iniciais necessários para a execução das Provas de Conhecimento Zero (PCZs), incluindo:

- Geração de pares de chaves criptográficas;
- Definição e publicação de parâmetros públicos;
- Configuração de políticas de segurança associadas ao protocolo.

Uma vez concluídas essas etapas, o sistema passa a operar em duas fases principais:

- **Fase de registro** – em que o usuário submete seus dados para criação da *embedding* e armazenamento seguro no servidor;
- **Fase de autenticação** – em que a identidade do usuário é verificada por meio de PCZs, sem exposição das *embeddings* originais.

5.6 Fase de Registro

Na fase de registro, o sistema realiza a conversão segura dos dados biométricos do usuário em uma representação vetorial (*embedding*) e seu armazenamento protegido no servidor. O processo ocorre da seguinte forma:

Primeiramente, o modelo de Inteligência Artificial (IA) extrai a *embedding* do usuário, convertendo dados biométricos em representações vetoriais de alta dimensionalidade. Em seguida, o usuário criptografa sua *embedding* utilizando um algoritmo de criptografia simétrica, como o Advanced Encryption Standard (AES). Essa *embedding* criptografada é então transmitida ao servidor, que a armazena de forma segura e atribui ao usuário um identificador único (ID). Por fim, o usuário mantém sob sua posse tanto a chave criptográfica quanto o ID recebido.

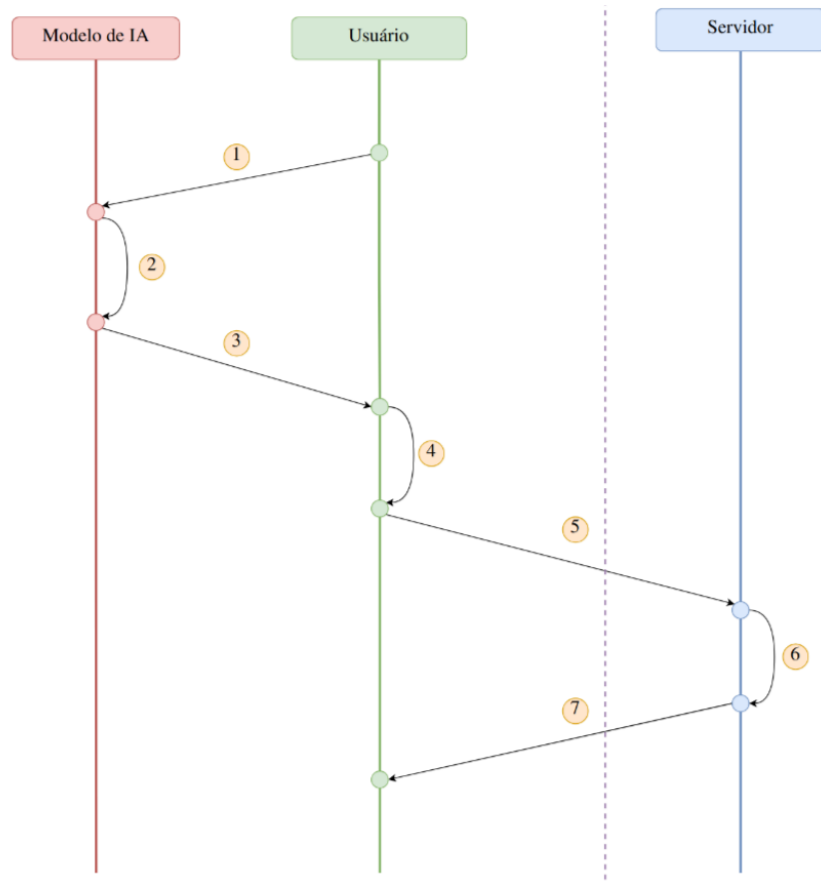


Figura 5.2: Arquitetura do projeto de autenticação biométrica com Provas de Conhecimento Zero na fase de registro. **Legenda:** (1) O usuário solicita o registro ao modelo de IA, enviando sua imagem facial; (2) O modelo de IA extrai a *embedding* do usuário; (3) O modelo de IA envia a *embedding* gerada para o usuário; (4) O usuário criptografa sua *embedding*; (5) O usuário envia a *embedding* criptografada para o servidor; (6) O servidor armazena a *embedding* criptografada no banco de dados; (7) O servidor envia um identificador único (ID) para o usuário.

A Figura 5.2 apresenta o diagrama de fluxo do processo de registro descrito nesta seção.

5.7 Fase de Autenticação

Na fase de autenticação, o processo inicia-se com o envio, por parte do usuário, de seu identificador único (ID) ao servidor. O servidor, então, disponibiliza uma cópia da *embedding* criptografada correspondente a esse ID, juntamente com a chave de prova.

O usuário, de posse desses dados, realiza localmente a descriptografia da *embedding* utilizando sua chave simétrica pessoal. Em seguida, solicita ao modelo de Inteligência Artificial (IA) a geração de uma Prova de Conhecimento Zero (PCZ), utilizando um protocolo como *zk-SNARK*, para verificar se a similaridade entre a *embedding* recém extraída e a *embedding* registrada anteriormente excede um limiar pré-definido. A verificação de similaridade pode ser expressa pela seguinte condição:

$$\text{similaridade_de_cosseno}(\text{embedding_atual}, \text{embedding_antiga}) > \text{limiar_de_similaridade}$$

A prova resultante é enviada ao servidor, que realiza sua verificação. Se a prova for considerada válida, o usuário é autenticado com sucesso. A Figura 5.3 apresenta o diagrama de fluxo deste processo.

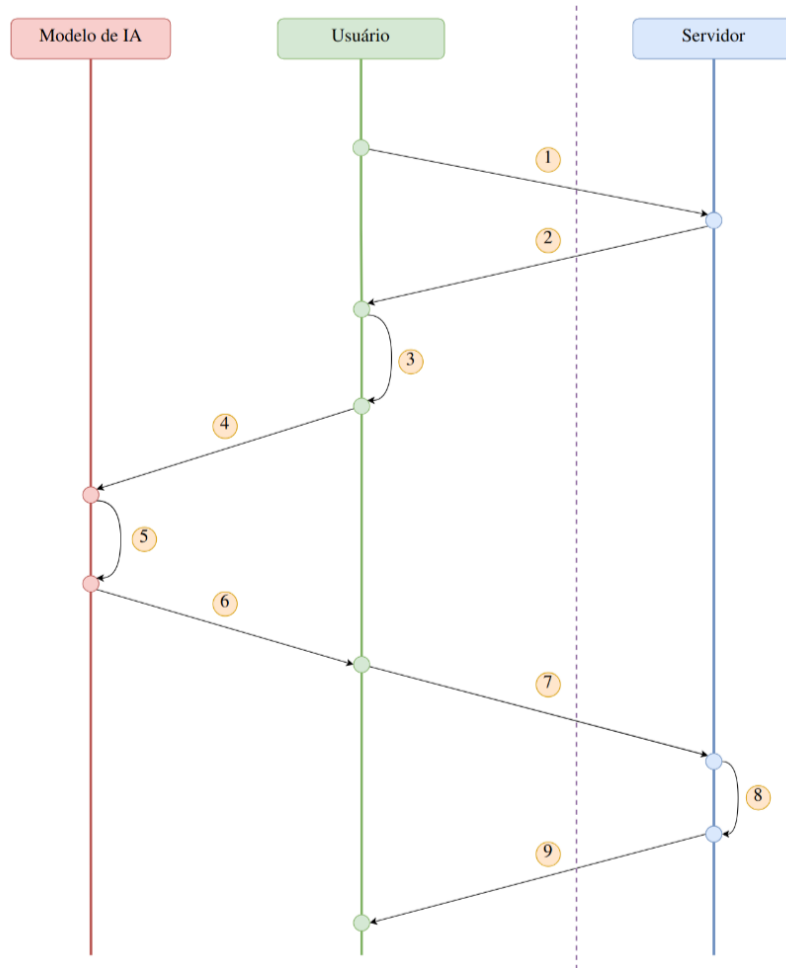


Figura 5.3: Arquitetura do projeto de autenticação biométrica com Provas de Conhecimento Zero na fase de autenticação. Legenda: (1) O usuário solicita a autenticação, enviando seu ID ao servidor; (2) O servidor retorna a chave de prova e uma cópia da *embedding* criptografada correspondente ao ID informado; (3) O usuário descriptografa a *embedding* recebida; (4) O usuário solicita ao modelo de IA a geração da prova PCZ, enviando sua imagem atual, a *embedding* recém-descriptografada e a chave de prova; (5) O modelo de IA extrai a *embedding* da imagem atual e gera a prova; (6) O modelo de IA envia a prova ao usuário; (7) O usuário envia a prova ao servidor; (8) O servidor verifica a validade da prova; (9) O servidor informa ao usuário o resultado da autenticação.

6 Classificação da Irredutibilidade de Pentanômios com Técnicas de Inteligência Artificial

Autor: Luiz Maurício do Valle Pereira

Tutor: Matheus Saldanha

6.1 Introdução

Este trabalho aborda a aplicação de Inteligência Artificial (IA) no contexto da dissertação de mestrado de [Banegas](#) (6), intitulada “*Pentanômios irredutíveis sobre $GF(2^m)$ para redução modular eficiente*”.

A escolha do tema se justifica pelo elevado interesse da comunidade científica nas aplicações de pentanômios irredutíveis em criptografia de curva elíptica (*Elliptic Curve Cryptography* – ECC). A seleção criteriosa de pentanômios adequados é essencial para garantir algoritmos criptográficos eficientes e robustos. Trata-se de um campo com significativo potencial de pesquisa e contribuição acadêmica, no qual este trabalho se propõe a ser um ponto de partida para investigações futuras que possam refinar os métodos aqui apresentados.

A busca por pentanômios irredutíveis é especialmente relevante para a implementação de estruturas algébricas capazes de melhorar o desempenho de algoritmos criptográficos. Tais algoritmos são fundamentais para assegurar a confidencialidade e o sigilo de dados sensíveis, inclusive no contexto do registro civil, onde a proteção da informação é requisito legal e técnico essencial.

Para alcançar esse objetivo, foi desenvolvido um classificador baseado em redes neurais artificiais, capaz de avaliar a irredutibilidade de pentanômios e classificá-los como redutíveis ou irredutíveis. O escopo deste estudo se restringe à criação e avaliação do classificador, não abrangendo testes com o algoritmo de *conta-XOR* descrito por [Banegas](#) (6).

6.2 Revisão da literatura e estado da arte

A classificação de pentanômios irredutíveis sobre $GF(2^m)$ é um tema central em aplicações criptográficas modernas, particularmente na criptografia de curva elíptica (*Elliptic*

Curve Cryptography – ECC). A escolha do polinômio gerador adequado impacta diretamente a eficiência das operações de multiplicação e redução modular no corpo finito, influenciando o desempenho de algoritmos críticos como geração de chaves, assinatura digital e protocolos de troca segura de informações.

6.2.1 Definição e relevância dos pentanômios irredutíveis

Um pentanômio sobre $GF(2)$ pode ser expresso genericamente como:

$$f(x) = x^m + x^a + x^b + x^c + 1, \quad 0 < c < b < a < m.$$

Um polinômio é dito irredutível se não pode ser fatorado em polinômios de grau inferior sobre o mesmo corpo. Essa propriedade garante que o corpo $GF(2^m)$ gerado tenha estrutura algébrica adequada para suportar operações criptográficas eficientes e seguras.

Segundo Banegas (6), os pentanômios irredutíveis constituem uma alternativa eficiente aos trinômios, especialmente quando estes não existem ou apresentam desempenho subótimo em determinada arquitetura de hardware ou software.

6.2.2 Métodos clássicos de verificação de irredutibilidade

A verificação tradicional da irredutibilidade de polinômios sobre $GF(2)$ emprega testes baseados no pequeno teorema de Fermat para polinômios. O critério clássico estabelece que $p(x)$ é irredutível se e somente se:

$$x^{2^m} \equiv x \pmod{p(x)}$$

e, adicionalmente, $\gcd(x^{2^{m/q}} - x, p(x)) = 1$ para todo divisor primo q de m .

Para pentanômios, algoritmos especializados como o *conta-XOR* (6) exploram a esparsidade do polinômio para acelerar o processo de verificação, reduzindo significativamente o número de operações lógicas necessárias.

6.2.3 Abordagens recentes e novos formatos de pentanômios

Trabalhos como Brent e Zimmermann (15) e Gao e Panario (37) exploram propriedades estruturais de polinômios esparsos para filtrar rapidamente candidatos redutíveis. Banegas; Custódio e Panario (7) propuseram uma classe específica de pentanômios da forma:

$$f(x) = x^{2b+c} + x^{b+c} + x^b + x^c + 1, \quad m = 2b + c,$$

otimizada para multiplicadores baseados no algoritmo de Karatsuba, reduzindo o custo de operações XOR e AND sem comprometer a latência de execução.

Além disso, surgiram métodos de engenharia reversa que permitem extrair o polinômio irredutível de implementações em hardware, analisando expressões algébricas resultantes da lógica de multiplicação em $GF(2^m)$.

6.2.4 Métodos clássicos de verificação de irredutibilidade

A abordagem tradicional envolve verificar se:

$$x^{2^m} \equiv x \pmod{p(x)},$$

com verificações adicionais de $\gcd(x^{2^{m/q}} - x, p(x)) = 1$ para cada divisor primo q de m . Métodos especializados, como o algoritmo "conta-XOR", exploram a esparsidade dos pentanômios para acelerar significativamente a verificação formal.

6.2.5 Engenharia reversa de polinômios em GF de hardware

Yu; Holcomb e Ciesielski (107) propuseram uma técnica poderosa baseada em álgebra computacional para extrair o polinômio irreduzível $P(x)$ usado em multiplicadores GF implementados em hardware, incluindo estruturas Mastrovito e Montgomery, a partir do netlist a nível de portas. O método opera em paralelo, analisa a expressão algébrica de cada bit de saída e consegue identificar $P(x)$ de forma eficiente, inclusive para multiplicadores com largura de até 571 bits.

6.2.6 Comparativo entre métodos tradicionais e abordagem via IA

- **Métodos clássicos:** garantem verificação exata, porém apresentam custo computacional elevado para graus altos de m ou grande espaço de candidatos.
- **Classificador por IA:** funciona como um filtro inicial, aprendendo padrões estruturais que permitem reduzir drasticamente o número de candidatos que precisam de verificação formal, sem comprometer o rigor matemático.

A combinação de ambos permite aliar desempenho e robustez à busca de pentanômios irredutíveis de alto grau.

6.2.7 Impacto prático em sistemas sensíveis

Pentanômios irredutíveis moldam as regras aritméticas dentro de corpos finitos, influenciando diretamente multiplicações e reduções modulares, operações centrais em criptografia aplicada, como em sistemas de registro civil, onde agilidade e segurança são exigências legais e técnicas fundamentais.

6.3 Desenvolvimento da Prova de Conceito (POC)

Esta seção descreve o processo de desenvolvimento do classificador, a construção do conjunto de dados (dataset) e os resultados obtidos nos testes da aplicação. Todo o código-fonte desenvolvido para esta POC está disponível no repositório público: <https://github.com/Luiz276/POC-pentanomios>.

6.3.1 Tecnologias Utilizadas

As principais tecnologias empregadas no desenvolvimento foram:

- Python 3.10;
- Biblioteca PyTorch, para construção e treinamento do modelo de aprendizado de máquina;
- Biblioteca Pandas, para manipulação e tratamento dos dados.

6.3.2 Criação do Dataset

Foi criado um dataset específico para a validação da POC, estruturado em um arquivo `.csv` contendo quatro colunas com valores inteiros representando os graus dos polinômios e uma coluna adicional com o rótulo (*label*) indicando se o pentanômio é redutível (0) ou irredutível (1).

6.3.3 Organização do Dataset

O dataset final encontra-se na pasta `dataset` do repositório e é composto por três arquivos `.csv`:

- `dataset.csv`: conjunto final utilizado no treinamento, obtido pela união dos dois arquivos seguintes;
- `clean_pentanomials.csv`: lista de pentanômios irredutíveis extraídos de [Banegas \(6\)](#);
- `random_pentanomials.csv`: lista de pentanômios redutíveis gerados aleatoriamente por script.

Cada um desses arquivos foi gerado por scripts específicos:

- `generate_random_pentanomials.py`: gera pentanômios aleatórios e produz o arquivo `random_pentanomials.csv`;
- `parse_known_pentanomials.py`: processa o arquivo `raw_known_pentanomials.txt` com dados extraídos de [Banegas \(6\)](#), produzindo o arquivo `clean_pentanomials.csv`;
- `create_dataset.py`: combina os dois conjuntos anteriores, resultando no arquivo `dataset.csv`.

O conjunto final foi particionado em 80% para treinamento e 20% para validação.

6.3.4 Implementação do Classificador

O classificador, implementado no arquivo `classifier.py`, é composto por três camadas lineares. As duas primeiras utilizam a função de ativação ReLU, e a última, a função Sigmoid. O treinamento foi realizado por 500 épocas (*epochs*), com *learning rate* de 0.001.

Durante o treinamento, observou-se redução contínua da função de perda (*loss*), atingindo valor final de 0.2191. Na etapa de validação, o modelo obteve acurácia de 0.92, demonstrando desempenho satisfatório para o problema proposto.

6.3.5 Análise dos Resultados

O desempenho do classificador foi avaliado a partir de dois indicadores principais: a função de perda (*loss*) e a acurácia (*accuracy*) sobre o conjunto de validação. O valor final da *loss* obtido no treinamento foi de 0.2191, indicando que o modelo conseguiu minimizar de forma consistente os erros de predição ao longo das épocas. A convergência suave e estável da *loss* sugere que a escolha dos hiperparâmetros, como *learning rate* e número de épocas, foi adequada para a complexidade do problema.

A acurácia final de 0.92 no conjunto de validação revela que o modelo foi capaz de generalizar bem para exemplos não vistos durante o treinamento, distinguindo com alta precisão pentanômios redutíveis e irredutíveis. Esse resultado é particularmente relevante, considerando que o dataset foi construído a partir de fontes heterogêneas, combinando dados extraídos de [Banegas \(6\)](#) e amostras geradas aleatoriamente.

Embora o desempenho seja satisfatório, é importante destacar que a avaliação foi feita sobre um conjunto relativamente pequeno e controlado. Para validações futuras, recomenda-se a ampliação do dataset, incluindo pentanômios de diferentes graus e características, a fim de verificar a robustez e a escalabilidade do modelo em contextos mais variados. Além disso, experimentos com arquiteturas mais profundas ou técnicas de regularização poderiam ser conduzidos para investigar possíveis ganhos adicionais de desempenho.

6.4 Conclusão

O presente trabalho demonstrou que é viável desenvolver um classificador de pentanômios com base em sua irredutibilidade, embora o processo apresente desafios significativos. Os resultados indicaram a ocorrência de *overfitting*, o que limita a capacidade de generalização do modelo. Dentre os fatores que contribuíram para essa limitação, destacam-se:

- **Tamanho e diversidade insuficientes do dataset:** O conjunto de dados construído para esta POC conta com menos de mil pentanômios, número insuficiente para representar de modo abrangente o espaço de busca. Ademais, as amostras consideradas irredutíveis foram extraídas exclusivamente da família descrita por [Banegas \(6\)](#), restringindo a abrangência do classificador.
- **Tuning de hiperparâmetros realizado de forma empírica:** A escolha dos hiperparâmetros foi feita por meio de avaliações repetidas, sem o uso de procedi-

mentos sistemáticos de otimização, o que compromete a assertividade dos valores selecionados.

Trabalhos Futuros

Frente às limitações identificadas, sugere-se avançar nas seguintes frentes:

- **Expansão e diversificação do dataset**, ampliando o número de amostras e incluindo múltiplas famílias de pentanômios irredutíveis, com vistas a fortalecer a representatividade e a robustez do modelo.
- **Otimização sistemática de hiperparâmetros** com o uso de ferramentas como *Optuna* ou *Ray Tune*, visando encontrar configurações mais adequadas à complexidade do problema.
- **Aplicação do algoritmo Conta-XOR** sobre os pentanômios irredutíveis detectados, avaliando possíveis impactos e melhorias nos processos de classificação dentro da teoria de polinômios.

Embora restrito em escopo, este trabalho representa um ponto de partida promissor para o emprego de técnicas de aprendizado de máquina na classificação de polinômios irredutíveis, com ênfase nos pentanômios. Os resultados obtidos indicam que, com conjuntos de dados mais amplos e diversos, tais modelos podem não apenas aprimorar a acurácia na identificação de irredutibilidade, mas também servir como ferramentas heurísticas na descoberta de novas famílias ainda não catalogadas. Dessa forma, contribuem de forma significativa e inovadora para os campos de álgebra computacional e teoria de polinômios.

Parte II - Qualidade, Integridade e Confiabilidade dos Dados no Registro Civil

A fidedignidade dos registros vitais é um requisito indispensável para a eficácia da administração pública e para a garantia plena dos direitos civis. Entretanto, assegurar a integridade e a qualidade dos dados em sistemas distribuídos e heterogêneos configura um desafio computacional de elevada complexidade. Este eixo temático reúne pesquisas que aplicam técnicas de Inteligência Artificial (IA) para enfrentar esse problema de forma sistemática, promovendo a transição de uma abordagem predominantemente reativa, centrada na correção de erros, para uma estratégia proativa de validação e verificação contínua.

Os trabalhos apresentados exploram metodologias computacionais diversificadas para assegurar a consistência e a precisão das informações. Entre elas, destacam-se *pipelines* de validação que integram visão computacional e modelos de linguagem para a verificação cruzada de documentos; plataformas voltadas à normalização e ao tratamento automatizado de inconsistências em grandes volumes de dados estatísticos; e, de forma inovadora, o uso de tecnologias de registro distribuído (*Distributed Ledger Technology* – DLT) para a criação de trilhas de auditoria imutáveis no processo de verificação de consistência.

Além disso, este eixo apresenta o paradigma do *Aprendizado Federado* como alternativa ao duplo desafio de treinar modelos preditivos robustos a partir de dados provenientes de múltiplas serventias, preservando a privacidade e evitando a centralização de informações sensíveis. Essa abordagem mantém a autonomia administrativa e a independência operacional dos cartórios de Registro Civil.

As contribuições reunidas nesta parte representam avanços significativos no desenvolvimento de sistemas capazes de garantir confiabilidade, auditabilidade e rastreabilidade das informações, atributos essenciais para a construção de uma governança pública baseada em evidências.

7 Verificação de Integridade e Autenticidade de Certidões de Nascimento

Autor: Ismael Coral Hoepers Heinzelmann

Tutor: Gustavo Zambonin

7.1 Introdução

A certidão de nascimento, no contexto brasileiro, transcende a condição de mera formalidade burocrática: ela constitui o primeiro e mais fundamental ato jurídico na vida de um indivíduo. Este documento essencial é a porta de entrada para o ordenamento jurídico, conferindo identidade, nacionalidade, nome e ascendência familiar. Sem a certidão de nascimento, o acesso a direitos e serviços básicos torna-se inviável, consolidando-a como a base para a obtenção de todos os demais documentos civis e para o pleno exercício da cidadania.

A ausência ou a imprecisão deste registro pode, na prática, negar o direito a uma identidade oficial reconhecida, restringindo o acesso a serviços e à proteção estatal. Assim, a integridade do registro civil não se limita a uma questão administrativa, mas configura um problema fundamental de direitos humanos e de acesso à justiça.

Para o Estado, a precisão dos registros civis é igualmente crucial, pois eles constituem insumos vitais para o controle e o planejamento populacional, fundamentando a formulação e a avaliação de políticas públicas em áreas como saúde, educação e segurança. A confiabilidade desses dados também fornece a segurança jurídica necessária para a realização de transações civis e comerciais, contribuindo para a eficiência da administração pública.

Apesar de sua importância incontestável, o sistema de registro civil brasileiro enfrenta desafios significativos relacionados à qualidade dos dados e à ocorrência de inconsistências. Essas falhas, que variam desde erros de digitação a omissões críticas e duplicações de registros, comprometem a fidedignidade das informações, gerando problemas práticos e legais para os cidadãos e dificultando a gestão pública eficaz. Um registro incorreto ou inconsistente pode tornar o documento inválido ou problemático, levando a consequências análogas à inexistência formal do registro, como exclusão social e perpetuação da vulnerabilidade.

Este projeto propõe o desenvolvimento de um validador de inconsistências para cer-

tidões de nascimento, uma ferramenta destinada a assegurar a precisão desses registros essenciais. Ao garantir a integridade das certidões, contribui-se para a efetividade das políticas públicas e para que todos possam exercer plenamente sua cidadania.

O sistema proposto utilizará técnicas de Inteligência Artificial (IA) para analisar a certidão de nascimento de uma criança em conjunto com os documentos de seus pais, identificando eventuais erros ou alterações. Para tal, serão empregados o *Contrastive LanguageImage Pre-training* (CLIP) (85) para o processamento das imagens, o *EasyOCR* (48) para a extração precisa do texto e Modelos de Linguagem de Grande Escala (*Large Language Models* LLMs) para a verificação inteligente dos dados extraídos, aumentando, assim, a confiabilidade no processo de registro de novos cidadãos no país.

7.2 Revisão da Literatura e Estado da Arte

Análise de sistemas internacionais como Adobe Scan (2) e DocuSign (32) revelou funcionalidades básicas de verificação, porém sem emprego de aprendizado profundo. No Brasil, o sistema e-Notariado oferece digitalização mas não detecção automática de fraudes.

O projeto considera a LGPD (14) para tratamento de dados sensíveis e a Resolução CNJ nº 332/2020 (23) que regulamenta a digitalização de documentos cartoriais, enfatizando a necessidade de manter integridade e autenticidade.

7.3 Escopo do Projeto

O objetivo central deste trabalho é desenvolver um *Produto Mínimo Viável* (MVP) de um sistema capaz de detectar automaticamente inconsistências e indícios de adulteração em certidões de nascimento. A abordagem proposta consiste na comparação estruturada dos dados constantes na certidão da criança com as informações extraídas dos documentos de seus pais, empregando técnicas avançadas de *machine learning* para assegurar a integridade e a confiabilidade desses registros.

O escopo contempla a implementação de métodos de processamento de imagens, extração automática de texto e verificação semântica de dados, de forma a construir um mecanismo que possa ser incorporado a fluxos operacionais do registro civil. Assim, busca-se criar uma ferramenta que não apenas identifique problemas potenciais, mas que também sirva como suporte técnico para a validação preventiva de documentos, contribuindo para a redução de erros e fraudes no sistema registral.

A Figura 7.1 apresenta, de forma esquemática, o fluxo operacional proposto para o MVP, desde a entrada dos documentos até a geração do relatório de inconsistências.

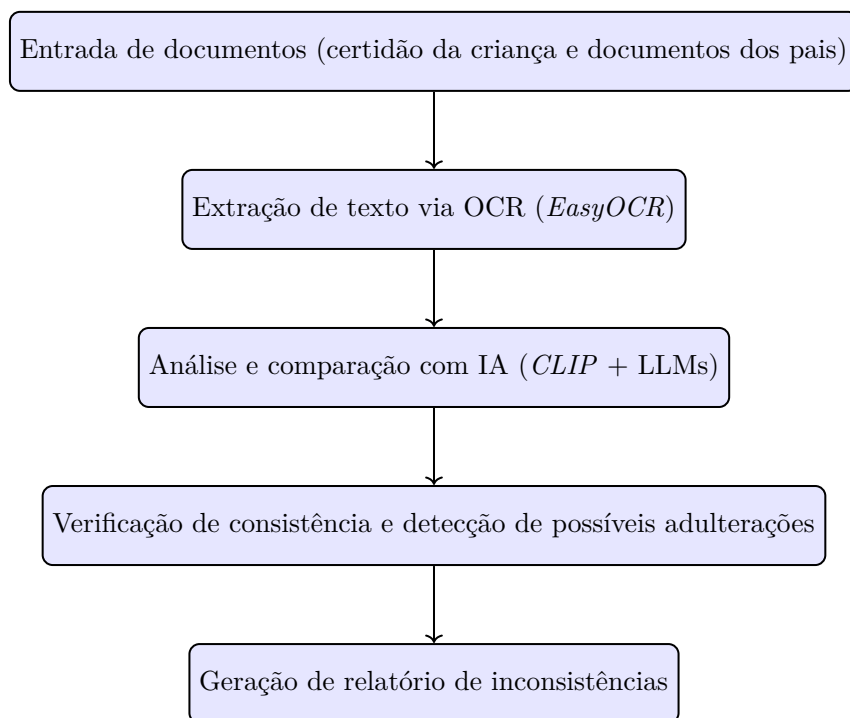


Figura 7.1: Fluxo operacional proposto para o MVP de verificação de integridade de certidões de nascimento.

7.4 Componentes do Sistema

A Figura 7.2 ilustra os principais componentes do sistema, descritos a seguir:

- **Pré-processamento de imagens:** conjunto de ferramentas para normalização, remoção de ruídos e preparação das imagens dos documentos (certidões e documentos dos pais) para análise subsequente;
- **Extração de características visuais (*CLIP*):** módulo que utiliza o *Contrastive LanguageImage Pre-training* (CLIP) para extrair atributos visuais relevantes dos documentos, auxiliando na detecção de padrões e possíveis alterações;
- **Reconhecimento Óptico de Caracteres (*EasyOCR* com *CRAFT*):** componente responsável por extrair com precisão o texto dos documentos, convertendo imagens em dados legíveis para o sistema;
- **Verificação inteligente de dados (LLMs):** uso de Modelos de Linguagem de Grande Escala (*Large Language Models* - LLMs) para analisar e cruzar os dados extraídos, identificando inconsistências, padrões suspeitos e possíveis adulterações entre a certidão da criança e os documentos dos pais;
- **Interface de usuário:** interface intuitiva para o envio dos documentos e apresentação dos resultados da análise, com destaque visual para as inconsistências encontradas.

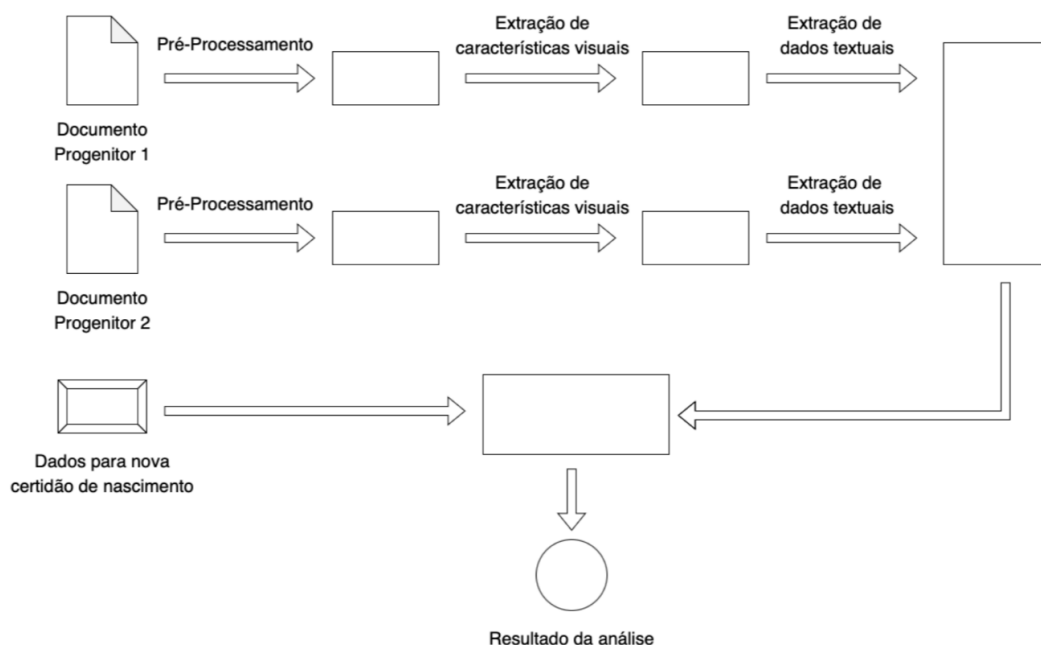


Figura 7.2: Arquitetura do sistema de verificação de integridade de certidões de nascimento.

7.5 Aquisição Textual de Documentos

Esta seção descreve o módulo de **aquisição textual** do sistema, responsável por transformar imagens de documentos em texto estruturado para as etapas posteriores. O fluxo ocorre em duas fases complementares: (i) **análise de qualidade visual**, para rejeitar imagens inadequadas e reduzir erros nas etapas subsequentes; e (ii) **extração óptica de caracteres**, para converter o conteúdo textual presente nas imagens em dados legíveis por máquina.

7.5.1 Análise de Qualidade Visual com CLIP

O *Contrastive LanguageImage Pre-training* (CLIP) é um modelo de rede neural treinado para compreender e relacionar imagens e texto, a partir de grandes conjuntos de dados compostos por pares de imagens e descrições textuais. Essa arquitetura permite estabelecer correlações semânticas robustas entre diferentes modalidades de dados, possibilitando que o sistema entenda o conteúdo visual de um documento a partir de sua descrição textual e vice-versa.

No presente projeto, o CLIP é utilizado para classificar diversas propriedades visuais dos documentos, atribuindo notas de 0 a 10 para cada categoria. Documentos com pontuação inferior a 6 em critérios essenciais são rejeitados automaticamente, garantindo um padrão mínimo de qualidade para o processamento posterior.

As classificações de qualidade avaliadas incluem:

- **Resolução:** baixa, média ou alta;

- **Foco:** borrado, bem focado ou nítido;
- **Ruído:** com muito ruído, com algum ruído ou sem ruído visível;
- **Iluminação:** mal iluminado, adequadamente iluminado ou bem iluminado;
- **Reflexos:** reflexos que obscurecem o texto, reflexos visíveis ou ausência de reflexos;
- **Enquadramento:** documento parcialmente cortado, levemente cortado nos cantos ou perfeitamente enquadrado;
- **Fundo:** poluído, neutro ou limpo;
- **Alinhamento:** inclinado, levemente desalinhado ou perfeitamente alinhado;
- **Clareza do texto:** ilegível, borrado ou legível;
- **Condição física:** danificado, com desgaste ou em perfeito estado;
- **Fidelidade de cores:** cores desbotadas, precisão média ou cores fiéis à realidade.

Este passo inicial é fundamental para reduzir a propagação de erros e otimizar a análise posterior. A detecção precoce de problemas visuais permite alertar um agente de registro civil sobre a necessidade de inspeção manual, reforçando a integridade e a confiabilidade do processo.

7.5.2 Extração Óptica de Caracteres com EasyOCR e CRAFT

Para a conversão das informações visuais em dados textuais, será empregada a biblioteca *EasyOCR* (48), reconhecida por sua robustez e eficiência. O *EasyOCR* integra o algoritmo *Character Region Awareness for Text Detection* (CRAFT), que possibilita a identificação e isolamento preciso das regiões de texto em imagens de certidões e documentos de identidade.

Uma vez detectadas as áreas de texto, o sistema realiza a conversão dessas regiões em dados legíveis por máquina, preservando o conteúdo para análise semântica posterior. Essa etapa é essencial para que módulos subsequentes, como os Modelos de Linguagem de Grande Escala (*Large Language Models* LLMs), possam processar e verificar as informações extraídas.

A escolha do *EasyOCR* justifica-se por sua capacidade de lidar com variações de fonte, tamanho e qualidade de imagem, assegurando resultados consistentes mesmo em documentos com desgaste físico ou digitalizações de baixa resolução.

7.6 Extração e Organização de Dados Sensíveis

Após a validação da qualidade visual dos documentos, a etapa subsequente consiste na extração e organização das informações neles contidas. Considerando a natureza sensível desses dados, optou-se por empregar modelos executados localmente, de modo a garantir a segurança e a privacidade do processo.

Para o Reconhecimento Óptico de Caracteres (OCR), foi utilizado o modelo *Character Region Awareness for Text Detection* (CRAFT), responsável por identificar e extrair o texto dos documentos com elevada precisão, convertendo imagens em dados textuais legíveis por máquina.

Os dados extraídos pelo CRAFT, entretanto, apresentaram ruído significativo, demandando um processo adicional de organização e padronização. Para essa tarefa, foram avaliados Modelos de Linguagem de Grande Escala (*Large Language Models* LLMs) com capacidades avançadas de raciocínio (*thinking*). Três modelos foram analisados: Mistral (49), Qwen3 (106) e Deepseek (42).

- **Mistral** (24 bilhões de parâmetros) apresentou falhas frequentes na organização satisfatória dos dados, comprometendo a consistência dos resultados;
- **Qwen3** apresentou variação significativa de precisão, obtendo acertos ocasionais, porém com elevada taxa de falhas;
- **Deepseek** foi testado nas versões R1 (*thinking*) e V2 (*chat*). O modelo Deepseek-R1, com 14 bilhões de parâmetros, destacou-se por sua alta eficácia na organização e análise dos dados.

Em virtude de sua performance superior, o Deepseek-R1 foi selecionado para atuar tanto na organização quanto na análise dos dados extraídos, assegurando um processamento robusto, consistente e confiável.

7.7 Verificação de Inconsistências para Emissão de Certidão de Nascimento

Com os dados extraídos e organizados, o sistema prossegue para a verificação de inconsistências entre as informações contidas nos documentos dos pais (RG) e os dados destinados à emissão da certidão de nascimento simplificada. O objetivo é permitir que a Inteligência Artificial (IA) auxilie no processo de validação, prevenindo fraudes e erros de entrada, mesmo quando validações básicas já tenham sido realizadas no momento da inserção dos dados.

As inconsistências são verificadas com base nos seguintes critérios:

1. **Verificação de erros gerais:** análise de todos os campos para identificar possíveis erros de digitação, como troca de letras em nomes próprios ou sobrenomes (ex.: “Souza” vs “SouSa”);
2. **Análise do nome do registrado (filho) e filiação:**
 - **Consistência dos nomes dos pais:** os nomes dos progenitores no campo “Filiação” da certidão devem ser idênticos aos nomes completos presentes em seus respectivos documentos de RG;

- **Validade dos sobrenomes do filho:** cada sobrenome individual presente no nome completo do filho deve constar no conjunto de sobrenomes dos pais e dos avós. A ordem dos sobrenomes é livre e a ausência de um sobrenome do pai ou da mãe não é considerada inconsistência. Essa verificação assegura que nenhum sobrenome inexistente seja adicionado;
 - **Consistência dos nomes dos avós:** quando disponíveis nos documentos dos pais, os nomes dos avós devem corresponder aos nomes listados na certidão de nascimento.
3. **Unicidade dos progenitores:** os números de CPF do Parente 1 e do Parente 2 devem ser distintos, garantindo que os documentos pertençam a pessoas diferentes;
4. **Coerência temporal (datas):**
- a data de nascimento do registrado na certidão não pode ser posterior à data atual;
 - as datas de nascimento de ambos os pais (constantes nos RGs) devem ser anteriores à data de nascimento do filho;
 - as datas de expedição de cada RG devem ser posteriores à data de nascimento do respectivo titular.
5. **Validade do local de nascimento (naturalidade):** o local de nascimento do filho na certidão deve corresponder a uma cidade e a um estado válidos no território brasileiro;
6. **Integridade e formato dos documentos:** verificação se os números de CPF contêm 11 dígitos numéricos, se os números de RG apresentam um formato plausível e se todas as datas (nascimento e expedição) são válidas no calendário (ex.: inexistência de 30 de fevereiro).

O sistema retorna, então, uma lista de potenciais inconsistências, permitindo que o usuário revise e modifique os dados quando a análise da IA estiver correta.

7.8 Conclusão

Os experimentos foram conduzidos utilizando documentos pessoais do autor e de sua parceira, a fim de gerar dados para a emissão simulada de uma certidão de nascimento de um filho hipotético. Em função da minimização proposital das validações de entrada, os resultados apresentaram certa volatilidade; contudo, em média, a abordagem mostrou-se promissora.

Um caso ilustrativo ocorreu quando o local de nascimento do filho foi informado como São Paulo - SP, enquanto o pai possuía naturalidade em Florianópolis - SC e a mãe em Petrolina - PE. Nessa situação, o sistema emitiu uma recomendação de revalidação, acompanhada de um alerta classificado como erro de nível baixo, com a observação: Pai nasceu em SC, mãe nasceu em PE, o filho pode nascer em qualquer local, mas esta combinação pode indicar uma possível inconsistência.

Esse resultado demonstra que a abordagem proposta, quando integrada a outras validações, pode atuar como um recurso valioso para reduzir erros operacionais e mitigar o risco de fraudes no processo de emissão de certidões de nascimento.

Como perspectiva de evolução, propõe-se o aprimoramento dos modelos de análise para contemplar um conjunto mais amplo de regras de consistência, incorporando dados provenientes de bases oficiais de referência e explorando técnicas avançadas de *machine learning* para detecção de padrões anômalos. Além disso, a integração do sistema a plataformas nacionais de registro civil permitiria validações em tempo real, elevando significativamente a robustez, a escalabilidade e o impacto prático da solução. Tais avanços deverão ser acompanhados pela implementação rigorosa de mecanismos de segurança e privacidade, em conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD), garantindo a proteção das informações sensíveis e a preservação dos direitos dos cidadãos.

8 Sistema de Estatísticas Vitais com Integração de Inteligência Artificial

Autor: Marcelo Dutra Mendonça

Tutor: Gustavo Biage

8.1 Introdução

O presente trabalho propõe o desenvolvimento de um Sistema de Estatísticas Vitais com Integração de Inteligência Artificial (IA), concebido como uma plataforma voltada à modernização e à otimização do processamento de dados demográficos brasileiros. O sistema foi idealizado para atender às demandas crescentes de digitalização dos serviços públicos, especialmente no contexto dos registros civis e das estatísticas vitais, empregando técnicas avançadas de IA para automatizar processos tradicionalmente manuais.

Os sistemas tradicionais de registro ainda dependem, em grande medida, de procedimentos manuais e de sistemas legados, o que resulta em inconsistências, duplicações e baixa qualidade dos dados. A heterogeneidade de formatos de entrada, como PDF, Excel, Word e diferentes padrões de data, cria um cenário complexo que exige soluções inteligentes para unificação e validação. É nesse contexto que a aplicação de técnicas de IA, em especial modelos de linguagem natural executados via *Ollama*, revela-se promissora.

Esses modelos possuem o potencial de identificar automaticamente inconsistências, padronizar dados e gerar *insights* estatísticos em tempo real. Trata-se de uma capacidade transformadora, considerando que dados vitais de qualidade são fundamentais para o planejamento de políticas públicas, a alocação de recursos e a tomada de decisões estratégicas. Assim, a automatização desses processos resulta não apenas em economia de recursos, mas, sobretudo, na elevação da qualidade e da eficiência dos serviços prestados à população.

No âmbito do Registro Civil, as estatísticas vitais desempenham um papel central na produção de informações confiáveis sobre nascimentos, óbitos, casamentos e outros eventos demográficos, constituindo um insumo essencial para políticas sociais, sanitárias e econômicas. A integração de IA nesse contexto pode ampliar significativamente a interoperabilidade entre diferentes bases de dados, nacionais e internacionais, ao promover a harmonização de formatos, a correspondência automática de registros e a detecção de inconsistências em múltiplas fontes. Essa capacidade contribui para alinhar o sistema

brasileiro a padrões e recomendações de organismos internacionais, como as Nações Unidas (101) e a Organização Mundial da Saúde (103), fortalecendo a qualidade, a comparabilidade e a utilidade das informações produzidas.

Diante desse cenário, a presente proposta busca traduzir essas diretrizes e padrões globais em uma solução prática e escalável, capaz de integrar tecnologias de inteligência artificial a fluxos de trabalho reais do Registro Civil, assegurando que os ganhos de qualidade e interoperabilidade se convertam em benefícios concretos para a gestão pública e para a sociedade.

8.2 Objetivos

8.2.1 Objetivo Geral

Desenvolver um sistema integrado de estatísticas vitais, com suporte de técnicas de Inteligência Artificial, capaz de automatizar a padronização, validação e análise de dados provenientes do Registro Civil, assegurando qualidade, interoperabilidade e alinhamento com padrões e recomendações internacionais (101, 103).

8.2.2 Objetivos Específicos

- Implementar mecanismos de extração, transformação e padronização de dados oriundos de múltiplos formatos (PDF, Excel, Word, entre outros);
- Empregar modelos de linguagem natural para detecção automática de inconsistências, erros de preenchimento e duplicidades nos registros;
- Integrar recursos de análise estatística em tempo real, permitindo o monitoramento contínuo de indicadores vitais;
- Garantir a interoperabilidade com bases nacionais e internacionais, por meio de mapeamentos de dados compatíveis com padrões da ONU e da OMS;
- Assegurar a conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD) e com boas práticas de segurança da informação, preservando a privacidade dos titulares;
- Disponibilizar uma interface intuitiva para operadores do Registro Civil e gestores públicos, facilitando o uso e a interpretação dos resultados;
- Criar mecanismos de exportação e compartilhamento seguro de dados, de forma a apoiar a formulação de políticas públicas e a tomada de decisão estratégica.

8.3 Metodologia

A metodologia adotada para o desenvolvimento do Sistema de Estatísticas Vitais com Integração de Inteligência Artificial foi organizada em etapas sequenciais e iterativas, contemplando desde a coleta e pré-processamento dos dados até a validação final

dos resultados. Essa abordagem permite o desenvolvimento incremental do sistema, com possibilidade de ajustes conforme a análise dos resultados parciais.

8.3.1 Etapas Metodológicas

1. **Levantamento de requisitos e análise do domínio:** identificação das necessidades específicas do Registro Civil e das estatísticas vitais, incluindo formatos de entrada, padrões de qualidade e requisitos de interoperabilidade com outras bases de dados;
2. **Coleta e integração de dados:** agregação de registros oriundos de múltiplos formatos (PDF, Excel, Word, CSV, entre outros), simulando cenários reais de heterogeneidade de fontes e padrões;
3. **Pré-processamento e padronização:** aplicação de técnicas de extração de texto, normalização de formatos de data, unificação de codificação de caracteres e remoção de inconsistências estruturais;
4. **Implementação de validações automatizadas:** utilização de modelos de linguagem natural via *Ollama* para identificação de inconsistências semânticas, duplicidades e erros de preenchimento;
5. **Integração de análises estatísticas:** desenvolvimento de módulos para cálculo e atualização em tempo real de indicadores vitais (nascimentos, óbitos, casamentos, entre outros), conforme metodologias recomendadas pela ONU (101) e pela OMS (103);
6. **Garantia de segurança e privacidade:** implementação de mecanismos de proteção de dados em conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD), incluindo controle de acesso, criptografia e registro de auditoria;
7. **Desenvolvimento da interface de usuário:** criação de um ambiente interativo e responsivo, destinado a operadores do Registro Civil e gestores públicos, para visualização de relatórios, gráficos e alertas de inconsistências;
8. **Validação e testes:** execução de testes unitários e integrados, avaliação da acurácia dos modelos de IA e verificação da conformidade com padrões internacionais;
9. **Documentação e treinamento:** produção de guias técnicos e materiais de capacitação para garantir a adoção eficaz do sistema pelas equipes envolvidas.

8.3.2 Visão Geral do Fluxo de Processamento

O fluxo geral do sistema pode ser resumido nas seguintes fases:

- Entrada de dados heterogêneos;
- Padronização e normalização;
- Validação semântica e estrutural com IA;

- Cálculo e atualização de estatísticas vitais;
- Geração de relatórios e exportação segura de dados.

8.4 Tecnologias Disponíveis

A materialização deste projeto depende da seleção criteriosa de um conjunto de tecnologias que, operando de forma integrada, garantem simultaneamente a capacidade analítica e a segurança robusta da plataforma. A arquitetura de software foi concebida sobre *frameworks* e bibliotecas de código aberto, amplamente validados pela comunidade técnica, abrangendo desde o processamento de dados e a execução de modelos de Inteligência Artificial (IA) até a proteção das informações em todas as camadas da aplicação.

8.4.1 Frameworks de Inteligência Artificial

- **Ollama:** *framework* local para execução de modelos de linguagem, permitindo o processamento de dados sensíveis sem necessidade de envio para serviços externos, assegurando privacidade e controle total sobre as informações;
- **Scikit-learn:** biblioteca consolidada para *machine learning* clássico, adequada para tarefas de classificação, regressão e detecção de anomalias;
- **Pandas/NumPy:** ferramentas essenciais para processamento e análise de dados, oferecendo alto desempenho na manipulação de grandes volumes de informação e suporte a operações matemáticas vetorizadas.

8.4.2 Tecnologias de Segurança

- **Flask-Security:** *framework* robusto de segurança para aplicações web, oferecendo autenticação, autorização e mecanismos de proteção contra ataques comuns;
- **SQLAlchemy:** *Object-Relational Mapping* (ORM) com recursos avançados de segurança de dados, incluindo sanitização automática de *queries* e prevenção contra *SQL injection*;
- **Cryptography:** biblioteca Python para criptografia, com implementações seguras de algoritmos criptográficos modernos, cobrindo funções simétricas, assimétricas e de assinatura digital.

8.4.3 Tecnologias de Visualização e Interoperabilidade

- **Plotly/Dash:** bibliotecas para criação de visualizações interativas e *dashboards* dinâmicos, permitindo a exploração visual de indicadores vitais e a geração de relatórios analíticos acessíveis a diferentes perfis de usuários;
- **Matplotlib/Seaborn:** ferramentas consolidadas para geração de gráficos estatísticos de alta qualidade, adequadas para relatórios técnicos e apresentações formais;

- **FastAPI:** *framework* moderno para construção de APIs de alto desempenho, facilitando a integração com sistemas externos, bases governamentais e plataformas internacionais de estatísticas vitais;
- **OpenAPI/Swagger:** especificação e documentação padronizada das APIs, garantindo que serviços de diferentes origens possam interoperar de forma consistente;
- **Pydantic:** biblioteca para validação e serialização de dados em conformidade com esquemas definidos, assegurando integridade nas trocas de informações;
- **Parquet/Feather:** formatos de armazenamento de dados otimizados para análise em larga escala, compatíveis com ecossistemas de *big data* e ferramentas analíticas.

8.5 Aspectos Legais e Éticos

A aplicação de Inteligência Artificial (IA) em um domínio de alta criticidade como o Registro Civil transcende os desafios puramente técnicos, exigindo aderência rigorosa a arcabouços legais e a princípios éticos fundamentais. Desde a concepção, o desenvolvimento do sistema foi pautado pela conformidade com a legislação brasileira de proteção de dados e pelas melhores práticas de ética em IA, assegurando que a inovação tecnológica contribua para fortalecer, e não comprometer, os direitos dos cidadãos e a confiança no serviço público.

8.5.1 Legislação Brasileira

- **LGPD (Lei Geral de Proteção de Dados Pessoais):** observância integral dos princípios e obrigações previstos na Lei nº 13.709/2018, incluindo minimização da coleta de dados, transparência no tratamento, base legal adequada e consentimento informado dos titulares;
- **Marco Civil da Internet:** aderência aos princípios de neutralidade de rede, privacidade e proteção de dados, conforme estabelecido na Lei nº 12.965/2014, garantindo que o processamento seja realizado de forma ética e segura;
- **Regulamentações Cartorárias:** conformidade com normas e provimentos do Conselho Nacional de Justiça (CNJ), em especial no que se refere à digitalização, preservação e segurança de documentos, assegurando integridade e autenticidade.

8.5.2 Considerações Éticas

- **Transparência Algorítmica:** adoção de práticas de *IA explicável* (*Explainable AI* - XAI) para decisões automatizadas, possibilitando que operadores e usuários compreendam os critérios e dados utilizados nos processos decisórios;
- **Mitigação de Viés Algorítmico:** implementação de auditorias periódicas, validação cruzada e diversidade no conjunto de dados de treinamento para reduzir riscos de discriminação ou tratamento desigual;

- **Consentimento Informado:** oferta de mecanismos claros, acessíveis e auditáveis para coleta e gestão do consentimento, assegurando que os titulares compreendam o uso e a finalidade de seus dados.

8.5.3 Diretrizes Internacionais Relevantes

A governança ética e legal de sistemas de IA aplicados ao Registro Civil pode ser fortalecida pela adoção de padrões e recomendações de organismos internacionais, que servem como referência para a harmonização de práticas entre países:

- **Nações Unidas (ONU):** as *Principles and Recommendations for a Vital Statistics System* (101) estabelecem diretrizes para a coleta, processamento e disseminação de estatísticas vitais, incluindo aspectos de qualidade, comparabilidade internacional e confidencialidade dos dados;
- **Organização Mundial da Saúde (OMS):** o guia *Improving the Quality and Use of Birth, Death and Cause-of-Death Information* (103) enfatiza a necessidade de padronização e interoperabilidade entre sistemas de registro civil e de saúde, promovendo a utilização segura e efetiva dos dados para políticas públicas;
- **Organização das Nações Unidas para a Educação, a Ciência e a Cultura (UNESCO):** a *Recomendação sobre a Ética da Inteligência Artificial* (99) estabelece princípios globais para o desenvolvimento e uso responsável de IA, incluindo direitos humanos, inclusão, equidade e promoção de sistemas transparentes e auditáveis.

A incorporação dessas diretrizes complementa a legislação nacional, oferecendo um referencial de boas práticas que favorece a interoperabilidade internacional, a confiança pública e a proteção efetiva dos direitos fundamentais no contexto do Registro Civil.

8.6 Escopo e Delimitação do Projeto

O presente trabalho abrange o desenvolvimento de uma plataforma funcional em nível de Produto Mínimo Viável (MVP), concebida para utilizar técnicas de Inteligência Artificial no processamento de dados vitais. O sistema proposto, em sua versão inicial, terá como foco principal:

- Padronização automática de dados de estatísticas vitais provenientes de múltiplas fontes heterogêneas;
- Detecção e resolução inteligente de inconsistências sem intervenção manual direta;
- Geração automatizada de *insights* estatísticos e relatórios demográficos sintéticos;
- Garantia de segurança e conformidade legal no tratamento de dados sensíveis, alinhada à legislação nacional e a diretrizes internacionais.

Com o objetivo de manter o foco e assegurar a viabilidade técnica e operacional do MVP, determinadas funcionalidades, embora relevantes para versões futuras, foram explicitamente excluídas do escopo desta etapa de desenvolvimento:

- Processamento completo e simultâneo de dados de nascimentos, óbitos e casamentos em todas as suas variáveis;
- Integração plena com múltiplas categorias de fontes externas além das três tipologias iniciais previstas;
- Implementação de uma interface web totalmente interativa para monitoramento e administração;
- Detecção automatizada de inconsistências complexas de caráter jurídico ou multirregistro;
- Geração de relatórios estatísticos abrangentes com visualizações dinâmicas e interativas em tempo real.

A Tabela 8.1 resume, de forma comparativa, as funcionalidades incluídas e excluídas nesta fase do projeto, permitindo uma visualização clara das fronteiras estabelecidas para o MVP.

Tabela 8.1: Escopo e delimitação do projeto

Incluído no Escopo (MVP)	Fora do Escopo (Versões Futuras)
Padronização automática de dados de estatísticas vitais provenientes de múltiplas fontes heterogêneas	Processamento completo e simultâneo de dados de nascimentos, óbitos e casamentos
Detecção e resolução inteligente de inconsistências sem intervenção manual direta	Integração plena com múltiplas categorias de fontes externas além das três tipologias iniciais
Geração automatizada de <i>insights</i> estatísticos e relatórios demográficos sintéticos	Implementação de uma interface web totalmente interativa para monitoramento e administração
Garantia de segurança e conformidade legal no tratamento de dados sensíveis	Detecção automatizada de inconsistências complexas de caráter jurídico ou multirregistro
–	Geração de relatórios estatísticos abrangentes com visualizações dinâmicas e interativas em tempo real

8.7 Componentes do Sistema

A arquitetura do sistema foi concebida de forma modular, visando flexibilidade, escalabilidade e manutenibilidade. É composta por quatro componentes principais que operam de forma integrada: um núcleo de processamento de dados para ingestão e padronização;

um motor de integração com IA para análise inteligente; uma camada de visualização e *dashboard* para interação com o usuário; e um módulo robusto de banco de dados para a persistência segura das informações. É fundamental observar que, conforme detalhado a seguir, os princípios de segurança e as considerações éticas não constituem um componente isolado, mas sim um pilar transversal, incorporado desde a concepção de cada um desses módulos.

8.7.1 Módulo de Processamento de Dados

Este módulo constitui o núcleo funcional do sistema, responsável pela extração automática e inteligente de dados de documentos em múltiplos formatos, incluindo PDF, Excel, JSON e DOCX. O sistema implementará normalização e padronização de dados utilizando algoritmos de *machine learning*, permitindo integração *seamless* com múltiplas fontes, como cartórios, sistemas de saúde e funerárias. O processamento contemplará diferentes formatos de data, incluindo ISO, DD/MM/AAAA e MM-DD-AAAA, assegurando versatilidade na ingestão de dados.

No aspecto de segurança, o módulo incorporará criptografia AES-256 para proteção de dados em trânsito e em repouso, validação rigorosa de entradas com sanitização automática, logs de auditoria criptografados para todas as operações e *rate limiting* para prevenção de ataques distribuídos de negação de serviço (DDoS). As considerações éticas incluem a minimização de dados processados, restrição ao uso apenas de informações estritamente necessárias, anonimização automática quando tecnicamente viável e transparência total por meio de logs acessíveis aos usuários autorizados.

8.7.2 Módulo de Integração com IA

Este módulo proporcionará funcionalidades avançadas por meio da detecção automática de inconsistências utilizando modelos de linguagem executados no Ollama, resolução inteligente de conflitos de dados com capacidade de aprendizado contínuo, extração de informações estruturadas de textos não estruturados e reconhecimento de padrões para detecção de anomalias e surtos epidemiológicos.

A segurança será garantida pela execução exclusivamente local dos modelos de IA, eliminando o envio de dados para serviços externos, validação rigorosa das saídas com múltiplas camadas de verificação, *fallback* automático para métodos tradicionais em caso de falha do modelo e monitoramento contínuo de comportamentos anômalos. As considerações éticas abrangem a implementação de *IA explicável* (*Explainable AI*) com justificativas detalhadas para decisões automatizadas, supervisão humana obrigatória para decisões críticas, prevenção ativa de vies algorítmico mediante validação contínua e auditoria regular dos modelos para assegurar *fairness*.

8.7.3 Módulo de *Dashboard* e Visualização

O módulo de *dashboard* fornecerá uma interface web responsiva e de design moderno para monitoramento em tempo real, visualizações interativas de estatísticas com gráficos dinâmicos, geração de relatórios automatizados e exportação de dados em múltiplos for-

matos. Também incluirá um sistema de alertas para detecção de anomalias e tendências críticas.

No campo da segurança, contará com autenticação multifator obrigatória, controle de acesso baseado em funções (*Role-Based Access Control* RBAC) com granularidade fina, proteção contra ataques web comuns (XSS, CSRF, *SQL injection*) e sessões seguras com *timeout* automático. Do ponto de vista ético, garantirá a apresentação clara e não tendenciosa de dados, respeito absoluto à privacidade na visualização, consentimento explícito para compartilhamento de *insights* e transparência quanto às limitações e incertezas dos dados apresentados.

8.7.4 Módulo de Banco de Dados

Este módulo assegurará o armazenamento seguro e eficiente dos dados vitais, com versionamento completo e histórico de alterações, backup automatizado com múltiplas camadas de redundância e recuperação rápida em caso de falhas. A segurança será reforçada por criptografia em nível de campo, controle de acesso granular com registros detalhados, monitoramento em tempo real de atividades suspeitas e testes periódicos de penetração e vulnerabilidade.

As considerações éticas incluem políticas claras de retenção limitada de dados, implementação do direito ao esquecimento conforme a LGPD, portabilidade integral de dados para os titulares e total transparência sobre uso e compartilhamento das informações.

8.8 Arquitetura do Sistema

A arquitetura do sistema, ilustrada na Figura 8.1, foi projetada em um modelo de múltiplas camadas (*multi-tiered*), que promove a separação de responsabilidades, a escalabilidade e a manutenibilidade.

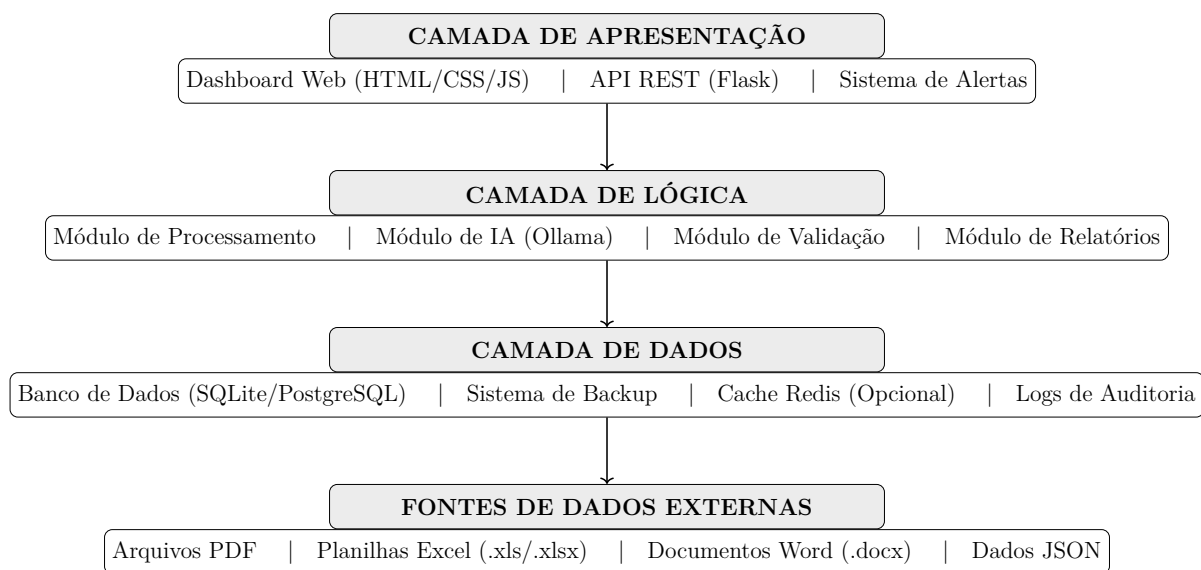


Figura 8.1: Arquitetura do Sistema de Estatísticas Vitais.

O fluxo de dados inicia-se com a ingestão das Fontes de Dados Externas (e.g., PDF, planilhas), que são gerenciadas pela Camada de Dados, responsável pela persistência segura, backups e logs de auditoria.

Em seguida, os dados são processados pela Camada de Lógica, núcleo do sistema, onde os módulos de validação, processamento e o motor de IA (Ollama) executam a padronização, a detecção de inconsistências e a geração de *insights*.

Finalmente, os resultados são entregues ao usuário por meio da Camada de Apresentação, que inclui um *dashboard* web interativo, uma API REST para integrações e um sistema de alertas. Essa estrutura desacoplada garante que cada parte do sistema possa ser desenvolvida, testada e atualizada de forma independente, aumentando a robustez da solução.

Para materializar essa arquitetura, foi selecionado um *stack* tecnológico moderno e robusto, baseado em Python:

- **Backend:** Python 3.11+ com Flask e extensões de segurança;
- **Banco de Dados:** SQLite (desenvolvimento) / PostgreSQL (produção);
- **IA:** Ollama para execução local de modelos de linguagem;
- **Frontend:** HTML5, CSS3, JavaScript ES6+, Bootstrap 5;
- **Processamento:** Pandas, NumPy, PyPDF2, openpyxl, python-docx.

8.9 Conclusões

O desenvolvimento de um Sistema de Estatísticas Vitais com Integração de Inteligência Artificial representa um avanço significativo na modernização dos serviços públicos brasileiros. O estudo demonstrou a viabilidade técnica e o potencial transformador da aplicação de IA em contextos governamentais, respeitando de forma rigorosa os princípios éticos e os requisitos legais vigentes.

A solução proposta incorpora inovações técnicas relevantes. O processamento local de IA por meio do Ollama assegura privacidade total dos dados, enquanto a arquitetura modular proporciona um design flexível, permitindo expansão e manutenção simplificadas. A automatização inteligente reduz de forma drástica a necessidade de trabalho manual, ao mesmo tempo em que a segurança *by design* garante proteção desde a concepção do sistema.

O impacto social esperado é expressivo, com ganhos de eficiência administrativa, redução de custos operacionais e melhoria na qualidade dos serviços prestados. A formulação de políticas públicas será beneficiada por dados mais completos, padronizados e confiáveis, e a transparência dos processos governamentais será fortalecida. Além disso, o sistema pode contribuir para a democratização do acesso às estatísticas vitais, ampliando a acessibilidade e a equidade na prestação dos serviços.

Durante o desenvolvimento, reforçou-se a compreensão de que a integração de considerações éticas deve ocorrer desde as fases iniciais do projeto. Ficou evidente que a

segurança não pode ser tratada como um aspecto secundário, e que a flexibilidade arquitetural é essencial para assegurar a capacidade de evolução tecnológica da solução.

O trabalho estabelece uma base sólida para futuras expansões, incluindo a integração com sistemas legados, a implementação em escala nacional e a adição de recursos avançados de *machine learning*. Também se vislumbra a possibilidade de ampliar a interoperabilidade com outras bases e sistemas governamentais, potencializando de forma significativa o alcance e a utilidade da plataforma.

Por fim, reforça-se que a segurança e a privacidade devem permanecer como prioridades centrais em qualquer evolução do sistema. A proteção robusta dos dados e o respeito contínuo aos direitos dos cidadãos constituem elementos indispensáveis para preservar a confiança pública e garantir a legitimidade das soluções baseadas em IA no Registro Civil e nas estatísticas vitais, em consonância com as diretrizes internacionais para governança responsável de dados estabelecidas pela OCDE (75).

9 Verificação Automatizada de Documentos Utilizando Inteligência Artificial

Autor: Luan Diniz Moraes

Tutor: Wellington Fernandes Silvano

9.1 Introdução

A verificação de identidade, elemento central para a segurança em processos digitais, enfrenta desafios crescentes devido a fraudes cada vez mais sofisticadas. Entre esses desafios, destacam-se a exploração de dados ocultos em documentos (1) e vulnerabilidades inerentes a formatos de arquivo como o PDF (17). No contexto brasileiro, em que a identidade civil é estabelecida pelos Cartórios de Registro Civil e materializada em documentos como Certidões de Nascimento, Registro Geral (RG) e Carteira Nacional de Habilitação (CNH), a integridade deste ecossistema é crucial. Contudo, abordagens tradicionais de validação podem se mostrar insuficientes, seja pela morosidade da verificação manual ou pela incapacidade de sistemas isolados realizarem análises de consistência cruzada eficazes (41, 64). Uma limitação crítica desses métodos é a ausência de uma trilha de auditoria segura e imutável, aspecto fundamental para a confiabilidade e a integridade dos registros.

Para mitigar essas lacunas, este trabalho propõe uma arquitetura de validação de consistência documental, implementada na forma de uma *Proof of Concept* (PoC). A solução integra tecnologias avançadas, utilizando um sistema de Reconhecimento Óptico de Caracteres (OCR) para extração de dados e um Modelo de Linguagem de Grande Porte (*Large Language Model* - LLM) para análise semântica e cruzamento de informações-chave entre documentos. O componente de segurança baseia-se no registro de evidências de verificação em uma rede *blockchain*, assegurando imutabilidade, privacidade e auditabilidade – características amplamente destacadas como benefícios dos livros-razão distribuídos (90).

Este relatório foi desenvolvido no âmbito da disciplina Segurança e Inteligência Artificial (INE5448 – Tópicos Especiais em Aplicações Tecnológicas I), cursada no primeiro semestre de 2025 na Universidade Federal de Santa Catarina. O projeto, intitulado “Prova de Consistência Inteligente: Verificação Automatizada de Documentos com IA”, foi sugerido pelo professor Ricardo Custódio e pelo tutor Wellington Fernandes Silvano.

9.2 Prova de Conceito

Para a construção da prova de conceito (PoC), documentos falsos foram gerados com o uso de inteligência artificial, especificamente Carteira Nacional de Habilitação (CNH), Registro Geral (RG) e comprovante de residência. O fluxo de processamento inicia-se com o pré-processamento das imagens, etapa em que se realiza o aumento do contraste, a inversão binária e a detecção automática da orientação correta do documento.

Na sequência, os documentos são submetidos à leitura por meio de sistemas de Reconhecimento Óptico de Caracteres (OCR), utilizando o TesseractOCR (93) e o EasyOCR (48). A acurácia de ambos é comparada, e o resultado final é composto palavra a palavra, selecionando-se aquele com maior *score* entre os dois sistemas. Scripts desenvolvidos em Python gerenciam esta etapa. Um exemplo dos campos extraídos (como nome, CPF e data de nascimento) é apresentado na Figura 9.2.

Os dados extraídos são então enviados ao modelo Mistral, executado em um contêiner via Ollama. A função principal desse modelo é retornar o nome do titular do documento, permitindo verificar se todos os documentos se referem à mesma pessoa. Adicionalmente, outras informações são cruzadas e validadas, como CPF e data de nascimento, bem como a verificação da validade dos documentos. Nesta etapa, empregaram-se expressões regulares (*regex*) e heurísticas específicas.

Os resultados são armazenados em um arquivo JSON, juntamente com a média aritmética da precisão do OCR, o identificador único (UUID) e o *timestamp*. Em seguida, cria-se uma assinatura no formato JWS (*JSON Web Signature*) sobre esses dados. Por fim, as informações assinadas são registradas na *blockchain* do Hyperledger Fabric, divididas em dois conjuntos: *private data* (UUID e assinatura) e *public data* (UUID, hash da assinatura e *timestamp*). Para isso, é realizado um *request* para um cliente do Fabric, ilustrado na Figura 9.1, que recebe as requisições da aplicação e invoca os *smart contracts* por meio do Fabric Gateway, retornando as respostas ao sistema principal.

O recurso *Private Data* do Hyperledger Fabric é utilizado para armazenar, via *transient data*, os dados privados em um banco de dados local do nó, enquanto os dados públicos são passados como argumento ao *smart contract* e registrados no *ledger*. O script da PoC, além de executar todas as etapas anteriores, também é responsável por recuperar os dados e validar a assinatura. A PoC é orquestrada por meio de um *shell script*, apresentado na Figura 9.4.

O resultado consolidado do fluxo, incluindo *logs*, UUIDs e dados assinados, é parcialmente mostrado na Figura 9.3. Já o principal trecho do *smart contract* proposto encontra-se na Figura 9.5.

A arquitetura proposta demonstra caráter inovador ao integrar, de forma coesa, tecnologias emergentes para resolução de um problema real de verificação documental. A combinação de OCR híbrido, análise semântica com LLM e registro imutável em *blockchain* cria uma solução que não apenas automatiza e acelera o processo de validação, mas também fortalece a auditabilidade, a confiabilidade e a segurança jurídica dos registros, atendendo a requisitos técnicos e regulatórios essenciais para ambientes de alta criticidade.

Além disso, a Organização para a Cooperação e Desenvolvimento Econômico (OCDE) recomenda que, em contextos públicos, tecnologias de *distributed ledger* (como *blockchain*) sejam utilizadas para reduzir custos operacionais, aumentar a transparência e fortalecer a

```
app.get('/api/public-data/:uuid', async (req: Request, res: Response) => {
  const uuid = req.params.uuid;
  console.log(`\n--> Received GET /api/public-data/${uuid}`);

  try {
    // Valida se o UUID foi fornecido na URL
    if (!uuid) {
      return res.status(400).json({
        status: "Error",
        message: "UUID parameter is required."
      });
    }

    // Chama a função que consulta a blockchain para obter os dados públicos
    const publicData = await getPublicData(contractOrg1, uuid);

    // Envia a resposta de sucesso com os dados encontrados
    return res.status(200).json({
      status: "Success",
      data: publicData
    });
  } catch (error: any) {
    console.error(`Error processing request for UUID ${uuid}:`, error);
  }
});
```

Figura 9.1: Cliente do Fabric que recebe *requests* e executa *smart contracts*.

confiança entre governos e cidadãos (71), benefícios que a presente PoC busca concretizar no processo de verificação documental.

9.3 Limitações

Uma primeira limitação foi o tempo reduzido de desenvolvimento, considerando que o tema do projeto final sofreu alteração no início de junho, aproximadamente um mês antes da data de elaboração deste relatório. Ainda assim, parte dos conhecimentos previamente adquiridos, como o estudo sobre o Hyperledger Fabric, pôde ser reaproveitada de forma produtiva.

A principal restrição, entretanto, esteve relacionada aos recursos de hardware disponíveis. A placa de vídeo utilizada (NVIDIA GTX 1650, com 4 GB de memória) não é adequada para a execução de aplicações de inteligência artificial de maior porte. Embora o TesseractOCR tenha apresentado desempenho satisfatório por ser otimizado para uso em CPU, tanto o EasyOCR quanto o modelo Mistral precisaram ser executados exclusivamente em modo CPU, resultando em tempos de processamento elevados. Essa limitação inviabilizou a execução simultânea de múltiplos serviços que se comunicam via API.

Como solução de contorno, foi desenvolvido um *shell script* para orquestrar a execução sequencial das etapas da PoC, registrando os resultados intermediários em arquivos. Essa abordagem, embora não represente uma arquitetura ideal, possibilitou a implementação funcional do protótipo e a validação do conceito proposto.

Para superar essas limitações em trabalhos futuros, recomenda-se a utilização de infraestrutura computacional mais robusta, preferencialmente com unidades de processamento gráfico (GPUs) com maior capacidade de memória e desempenho compatível com modelos de IA de última geração. Adicionalmente, a adoção de uma arquitetura baseada em microsserviços com execução paralela e comunicação assíncrona via API permitiria maior

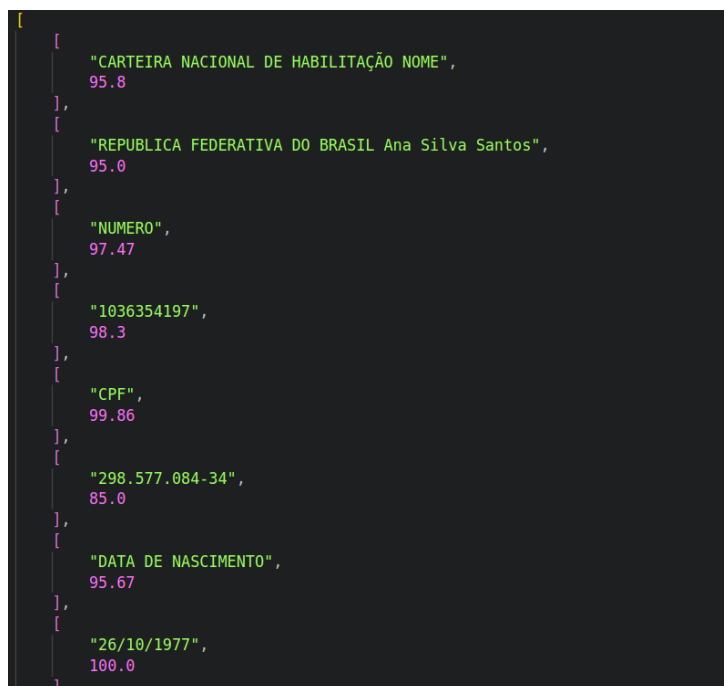


Figura 9.2: Exemplo de dados extraídos de um documento via OCR.



Figura 9.3: Trecho do *output* da execução da PoC.

escalabilidade e melhor aproveitamento de recursos.

9.4 Conclusão

A participação na disciplina mostrou-se extremamente proveitosa, pois possibilitou um aprofundamento nos estudos sobre Inteligência Artificial (IA) e segurança da informação, com ênfase em *blockchain*. A apresentação dos resultados no Workshop sobre Registro Civil representou uma oportunidade relevante de compartilhamento e validação dos conhecimentos adquiridos.

Impressões do aluno. O desenvolvimento desta *Proof of Concept* (PoC) exigiu a utilização de diversas tecnologias, incluindo *TypeScript*, *Go*, *Python*, bibliotecas para *OCR*, *shell script*, *Docker*, *Ollama*, além da comunicação via API com modelos de IA e da implementação de *chaincode* para o *Hyperledger Fabric*.

```
run.sh
1  #!/bin/bash
2  source .env.example
3
4  python3 main.py
5
6  cd Ollama
7  docker compose up -d > /dev/null 2>&1
8  cd ..
9
10 python3 ./Ollama/main.py
11
12 cd Ollama
13 docker compose down > /dev/null 2>&1
14 cd ..
15
16 echo ">>> Starting Fabric ledger..."
17 cd fabric_blockchain_app
18 ./run_network.sh > /dev/null 2>&1 &
19 BLOCKCHAIN_PID=$!
20 cd ..
21
```

Figura 9.4: *Shell script* responsável pela execução completa da PoC.

```
58 type PrivateAsset struct {
59     UUID      string `json:"UUID"`
60     SignedData string `json:"signed_data"`
61 }
62
63 func (s *SmartContract) CreateAsset(ctx contractapi.TransactionContextInterface, uuid string, dataHash string, timestamp string) error {
64     transientMap, err := ctx.GetStub().GetTransient()
65     if err != nil {
66         return fmt.Errorf("error getting transient: %v", err)
67     }
68
69     transientAssetJSON, ok := transientMap["private_data"]
70     if !ok {
71         return fmt.Errorf("asset not found in the transient map input under key 'private_data'")
72     }
73 }
```

Figura 9.5: Trecho do *smart contract* desenvolvido para o Hyperledger Fabric.

A experiência contribuiu para uma mudança significativa de percepção sobre IA. Inicialmente, havia certo ceticismo em relação à tecnologia; entretanto, ao estudar seus fundamentos e observar suas múltiplas aplicações ao longo do semestre, tornou-se claro que a IA é uma ferramenta de elevado potencial, cuja eficácia está diretamente relacionada ao uso ético e à aplicação adequada em contextos relevantes.

10 Aprendizado Federado Aplicado a Dados Vitais: Estudo de Caso em Santa Catarina

Autor: Matheus Paulon Novais

Tutor: Gustavo Zambonin

10.1 Introdução

No cenário tecnológico contemporâneo, a Inteligência Artificial (IA) consolidou-se como uma ferramenta de valor inestimável para a extração de *insights* e para a realização de previsões a partir de vastos conjuntos de dados. Contudo, sua crescente adoção suscita questões críticas no campo da segurança da computação, notadamente quanto à privacidade e à confidencialidade das informações. A metodologia tradicional de treinamento de modelos de *machine learning*, que frequentemente exige a centralização de dados, colide diretamente com regulamentações de proteção de dados, como a Lei Geral de Proteção de Dados Pessoais (LGPD) (14), e com a natureza intrinsecamente distribuída das bases de dados no mundo real.

A proposta deste trabalho, alinhada aos objetivos da disciplina, consistiu em aprofundar-se nesta interseção, consolidando conhecimentos práticos em IA e segurança por meio de uma Prova de Conceito (PoC). O foco não se restringiu à aplicação de algoritmos, mas incluiu a compreensão das motivações, dos desafios e das novas possibilidades arquiteturais que combinam desempenho preditivo e segurança computacional.

A motivação para a escolha do tema decorreu da necessidade de abordar este dilema fundamental. O Aprendizado Federado (*Federated Learning* – FL) apresentou-se como tecnologia promissora, ao propor um paradigma no qual a colaboração para o treinamento de modelos robustos ocorre sem a necessidade de compartilhamento de dados brutos. Para materializar este conceito, foi selecionado um estudo de caso de alta relevância social: a previsão da Taxa de Mortalidade Infantil (TMI) em Santa Catarina. Este cenário ilustra de forma precisa o problema, pois envolve dados de saúde sensíveis, geograficamente distribuídos entre os diversos municípios do estado, que atuam como “clientes” detentores de suas próprias informações.

Este relatório documenta a jornada de desenvolvimento desta PoC, desde a concepção inicial, passando pela coleta e tratamento dos dados, a implementação dos modelos, os desafios enfrentados e, de forma igualmente relevante, os aprendizados consolidados ao

longo do processo.

10.2 Fundamentação Teórica

10.2.1 Análise Preditiva com Dados Vitais

As estatísticas vitais, como os registros de nascimentos e óbitos, constituem a base para a formulação de políticas públicas eficazes e fundamentadas em evidências. A Taxa de Mortalidade Infantil (TMI), calculada como o número de óbitos de crianças com menos de um ano de idade para cada mil nascidos vivos, destaca-se como um dos indicadores mais sensíveis das condições de saúde, saneamento e qualidade de vida de uma população. A capacidade de prever a evolução dessa taxa possibilita que gestores públicos realizem alocação proativa de recursos, direcionando investimentos para áreas de risco antes que crises se intensifiquem, com o objetivo final de reduzir mortes evitáveis.

Para esta Prova de Conceito (PoC), foram utilizados dados públicos do Sistema IBGE de Recuperação Automática (SIDRA) (45). A construção de um *dataset* robusto para a modelagem exigiu a combinação de informações de diferentes fontes, cada qual contribuindo com uma peça do problema. Foram coletados dados anuais de nascidos vivos e óbitos infantis, que constituem a base para o cálculo da TMI, e dados decenais do Censo Demográfico, como renda média e percentual de cobertura de esgotamento sanitário, utilizados como variáveis preditivas (*features*) fundamentais, dada sua forte correlação com a TMI.

10.2.2 Aprendizado Federado: Um Paradigma para a Privacidade

O Aprendizado Federado (*Federated Learning* – FL) é uma abordagem de *machine learning* concebida para treinar modelos de IA em um conjunto de dispositivos ou servidores descentralizados. Sua principal característica, e também seu maior diferencial, é permitir que o treinamento ocorra sem que os dados brutos precisem deixar sua localidade de origem. Em vez de centralizar os dados em um único servidor, o FL centraliza apenas as atualizações de parâmetros resultantes do treinamento local. Trata-se, portanto, de uma mudança de paradigma: o modelo desloca-se até os dados, e não o inverso.

Essa abordagem é sustentada por três princípios centrais:

- **Privacidade por concepção** (*privacy by design*): garante que dados sensíveis de cada participante não sejam expostos ou compartilhados;
- **Colaboração sem centralização**: possibilita que múltiplas organizações, inclusive concorrentes, colaborem para desenvolver modelos mais robustos do que aqueles obtidos isoladamente;
- **Inteligência coletiva**: o modelo global final beneficia-se da diversidade e da escala dos dados de todos os participantes, resultando em maior robustez, precisão e justiça.

10.2.3 Arquitetura e Algoritmos do Aprendizado Federado

A arquitetura típica de um sistema de Aprendizado Federado envolve dois componentes principais: um servidor central (ou agregador) e um conjunto de clientes. Os clientes são detentores dos dados locais (por exemplo, municípios, hospitais ou dispositivos móveis) e responsáveis pelo treinamento local do modelo. O servidor central orquestra o processo, mas nunca acessa diretamente os dados brutos.

O algoritmo mais utilizado no FL é o *Federated Averaging* (FedAvg), proposto originalmente pelo Google, cujo funcionamento ocorre em ciclos de comunicação, conforme ilustrado na Figura 10.1:

1. **Distribuição:** o servidor central seleciona um subconjunto de clientes disponíveis e envia a eles o estado atual do modelo global (parâmetros ou pesos);
2. **Treinamento local:** cada cliente treina o modelo recebido com seus próprios dados, por um número predefinido de épocas ou iterações;
3. **Atualização e retorno:** os clientes enviam de volta apenas as atualizações realizadas (novos pesos ou deltas), e não os dados brutos;
4. **Agregação:** o servidor central calcula uma média ponderada das atualizações (geralmente ponderada pelo número de amostras de cada cliente) para atualizar o modelo global.

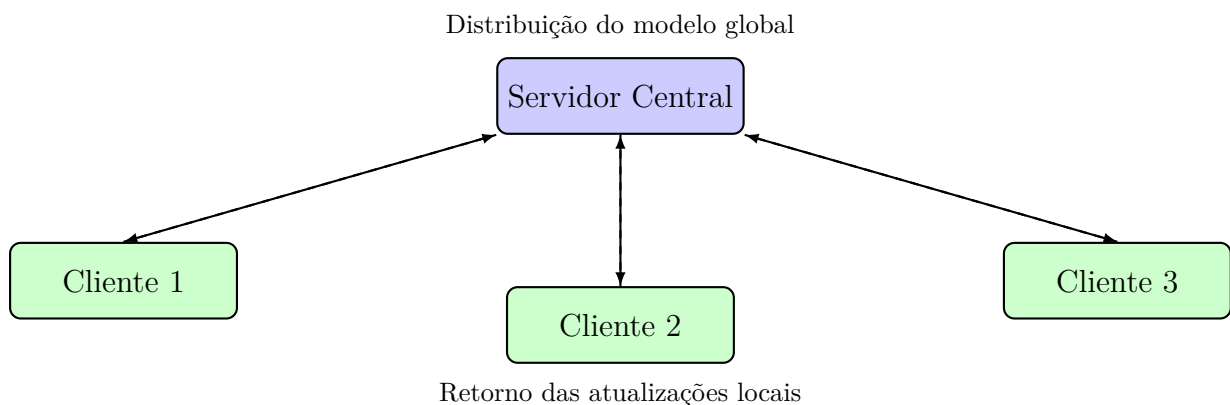


Figura 10.1: Fluxo simplificado do algoritmo *Federated Averaging* (FedAvg). As setas contínuas indicam a distribuição do modelo global para os clientes; as setas tracejadas indicam o retorno das atualizações locais para o servidor central.

10.2.4 Vantagens e Desafios

A principal vantagem do Aprendizado Federado é a preservação da privacidade, aspecto crucial em domínios como saúde, finanças e indústria, onde a manipulação de dados está sujeita a regulamentações rigorosas, como a LGPD (14). Além disso, ao manter os dados em sua origem, o FL pode reduzir custos de comunicação e armazenamento associados à centralização massiva.

Por outro lado, a abordagem apresenta desafios específicos. A heterogeneidade estatística (*non-IID data*) é um dos mais relevantes, pois a distribuição dos dados entre clientes pode variar substancialmente, dificultando a convergência de um modelo único. A comunicação também pode tornar-se um gargalo, já que, embora não se transmitam dados brutos, as atualizações de modelo ainda requerem largura de banda. Finalmente, a própria arquitetura federada amplia a superfície de ataque, exigindo mecanismos de segurança robustos, como criptografia e privacidade diferencial, para mitigar ameaças de adversários maliciosos.

10.3 Trabalhos Relacionados

A interseção entre Aprendizado Federado (*Federated Learning* – FL) e Modelos de Linguagem de Grande Escala (*Large Language Models* – LLMs) configura uma fronteira de pesquisa ativa e de elevada relevância. Embora este trabalho tenha se concentrado na aplicação de conceitos de FL a dados tabulares de estatísticas vitais, a literatura recente evidencia esforços consistentes para transpor os benefícios dessa abordagem para o domínio dos LLMs, enfrentando desafios particulares de escala, custo computacional e eficiência de comunicação. A seguir, são discutidos trabalhos recentes que ilustram as principais linhas de investigação nesse campo e que estão sintetizados na Tabela 10.1.

Uma vertente de pesquisa crucial diz respeito à eficiência do *fine-tuning* em ambientes federados. O custo de treinar e transmitir atualizações de um LLM com bilhões de parâmetros é, na prática, proibitivo. Nesse contexto, Chen; Dai; Zhang et al. (20) propõem o *FATE-LLM*, um *framework* para *fine-tuning* federado de LLMs. A estratégia central do *FATE-LLM* consiste em congelar a maior parte dos parâmetros do modelo e treinar apenas um subconjunto reduzido, empregando técnicas como o *Low-Rank Adaptation* (LoRA). Com isso, reduz-se de forma significativa a sobrecarga de comunicação entre clientes e servidor central, viabilizando o *fine-tuning* colaborativo sem prejuízo relevante de desempenho em tarefas específicas.

Ampliando essa abordagem, Cui; Zhang; Yao et al. (25) investigam o impacto de dados ruidosos no *fine-tuning* federado. O trabalho apresenta o *FedNoisy-Adapter*, método que combina a eficiência de adaptadores, pequenos módulos neurais inseridos no LLM, com uma estratégia para mitigar o efeito de dados de baixa qualidade oriundos de determinados clientes. O *FedNoisy-Adapter* identifica e atribui menor peso às atualizações provenientes de clientes com dados ruidosos durante a agregação no servidor, resultando em um modelo global mais robusto e preciso. Tal solução é particularmente relevante em cenários reais, nos quais a qualidade dos dados distribuídos é intrinsecamente heterogênea.

Outra linha de investigação concentra-se na infraestrutura necessária para o pré-treinamento federado, tarefa ainda mais intensiva em recursos computacionais. Li; Lin; Zou et al. (58) apresentam o *Shepherd*, uma plataforma projetada para orquestrar o pré-treinamento eficiente de LLMs em múltiplos *clusters* de GPUs geograficamente distribuídos. O sistema otimiza a comunicação ao sobrepor-la ao cálculo local (*communication-computation overlap*) e gerencia de forma adaptativa os *stragglers* – clientes que, por diferentes razões, apresentam desempenho inferior aos demais. O *Shepherd* demonstra que questões de sistemas operacionais e computação distribuída são centrais para viabilizar FL em larga escala.

Por fim, a aplicação de FL em contextos linguísticos específicos também constitui um campo ativo. Zhang; He; Song et al. (109) propõem o *FL-CPT*, um *framework* de Aprendizado Federado para *Transformers* pré-treinados em chinês (*Chinese Pre-trained Transformers*). O trabalho aborda dois desafios críticos: o esquecimento catastrófico, em que o modelo perde informações gerais ao especializar-se em dados locais, e o gargalo de comunicação. O *FL-CPT* utiliza uma estratégia de otimização que preserva o conhecimento do modelo base enquanto o adapta aos dados locais, evidenciando que o êxito do FL frequentemente exige ajustes específicos ao domínio e ao idioma.

Em conjunto, esses estudos indicam que, embora a presente PoC tenha explorado dados estruturados, os princípios de colaboração, preservação da privacidade e desafio de generalização são universais. As soluções desenvolvidas para LLMs, como comunicação eficiente e robustez frente à heterogeneidade dos dados, são diretamente aplicáveis e inspiram possíveis evoluções do trabalho com dados vitais.

Tabela 10.1: Resumo de trabalhos relacionados sobre Aprendizado Federado aplicado a LLMs.

Trabalho	Foco da Pesquisa	Metodologia	Contribuições Principais
Chen; Dai; Zhang et al. (20) – FATE-LLM	<i>Fine-tuning</i> federado eficiente	Congelamento da maioria dos parâmetros e uso de LoRA	Redução da sobrecarga de comunicação e viabilização prática do <i>fine-tuning</i> colaborativo
Cui; Zhang; Yao et al. (25) – FedNoisy-Adapter	Mitigação de dados ruidosos no FL	Uso de adaptadores e ponderação de atualizações conforme qualidade dos dados	Modelo global mais robusto e resiliente a dados heterogêneos
Li; Lin; Zou et al. (58) – Shepherd	Pré-treinamento federado em larga escala	Orquestração de múltiplos <i>clusters</i> de GPUs e <i>communication-computation overlap</i>	Maior eficiência no pré-treinamento e gerenciamento de <i>stragglers</i>
Zhang; He; Song et al. (109) – FL-CPT	FL para <i>Transformers</i> em chinês	Otimização para evitar esquecimento catastrófico e reduzir gargalo de comunicação	Preservação do conhecimento do modelo base e adaptação a contextos linguísticos específicos

10.4 Desenvolvimento da Prova de Conceito

O desenvolvimento da PoC ocorreu de forma iterativa e pragmática. Cada fase — desde a obtenção dos dados até a implementação da interface final — apresentou desafios práticos que informaram e refinaram a abordagem subsequente, culminando em uma demonstração robusta e elucidativa.

10.4.1 Da Coleta ao Tratamento dos Dados

A fase inicial do projeto foi dedicada à obtenção dos dados do portal SIDRA/IBGE. Embora conceitualmente simples, o processo rapidamente evidenciou as dificuldades inerentes ao trabalho com dados do mundo real. Os arquivos *CSV* exportados pela plataforma continham múltiplas linhas de cabeçalho e rodapé, que precisaram ser descartadas programaticamente. Além disso, colunas numéricas apresentavam valores textuais como “-” ou “...”, e até mesmo notas de rodapé completas, exigindo rotinas de limpeza e conversão de tipos.

Outro desafio significativo foi a dessincronia temporal entre as fontes de dados. Os registros vitais eram anuais, enquanto os indicadores socioeconômicos do Censo eram decenais. Para criar um *dataset* coeso — no qual cada ano de cada município tivesse um conjunto completo de *features* — foi necessário implementar uma estratégia de preenchimento combinando *forward-fill* (propagação do último valor conhecido para anos subsequentes) e *backward-fill* (uso do próximo valor conhecido para preencher anos anteriores). A superação desses obstáculos evidenciou a importância crítica de um *pipeline* de *ETL* (*Extract, Transform, Load*) robusto e bem planejado.

10.4.2 Arquitetura da Análise Comparativa

Considerando a complexidade de uma implementação completa com o *TensorFlow Federated* (TFF) para o escopo de uma PoC inicial, optou-se por simular a essência do conceito por meio de uma análise comparativa rigorosa. Foram desenvolvidos dois modelos de rede neural com arquiteturas idênticas, garantindo equidade na comparação.

O primeiro, denominado **Modelo Local**, foi treinado exclusivamente com a série histórica de dados de Florianópolis, representando um cenário de isolamento de dados sem colaboração. O segundo, denominado **Modelo Federado**, foi treinado com o conjunto de dados dos nove municípios catarinenses analisados, representando o resultado final de um processo de Aprendizado Federado, no qual o conhecimento de todos os clientes foi agregado. A comparação direta do desempenho preditivo desses dois modelos constituiu o núcleo da análise e a principal evidência do valor da colaboração.

10.4.3 A Aplicação Web como Ferramenta de Demonstração

Para apresentar os resultados de forma clara, interativa e convincente, foi desenvolvida uma aplicação web. O *backend* foi implementado com *FastAPI* (86), criando uma API *RESTful* responsável por servir os dados históricos e realizar previsões em tempo real a partir dos modelos pré-treinados.

No *frontend*, optou-se pelo *Streamlit*, *framework* que permite criar interfaces ricas e interativas utilizando apenas Python. Essa combinação tecnológica possibilitou a construção de um “Laboratório de Previsão”, seção do *dashboard* em que o usuário pode selecionar um município, ajustar parâmetros e comparar visualmente o desempenho dos dois modelos. Dessa forma, uma análise técnica complexa foi convertida em uma demonstração intuitiva e acessível.

10.5 Resultados e Discussões

O ponto culminante da Prova de Conceito foi a demonstração controlada do desempenho preditivo dos modelos. Para assegurar que a comparação fosse inequívoca e didática, foi elaborado um cenário de teste específico para o município de Florianópolis, com o objetivo de avaliar a robustez dos modelos diante de uma inflexão na tendência histórica.

Nesse cenário, o valor da TMI em 2024 foi fixado em 5,40, servindo como principal variável preditiva ($TMI_{ano_anterior}$) para a previsão do ano subsequente. O valor real da TMI para 2025 — considerado o gabarito — foi estabelecido em 6,50 no conjunto de dados, representando um leve aumento e rompendo a tendência de queda, o que configura um desafio realista para qualquer modelo preditivo.

Ao submeter os dados de 2024 ao sistema, os resultados foram apresentados de forma clara no *dashboard*. O **Modelo Federado** previu uma TMI de 6,31 para 2025, valor notavelmente próximo do real, resultando em um erro absoluto de apenas 0,19. Em contrapartida, o **Modelo Local**, treinado exclusivamente com a série histórica de Florianópolis, previu uma TMI de 8,02, valor significativamente superestimado que resultou em um erro absoluto de 1,52.

Essa análise comparativa revela de forma conclusiva que o Modelo Federado, ao ser exposto à diversidade de dados provenientes de múltiplos municípios durante o treinamento, demonstrou capacidade de generalização substancialmente superior. O modelo conseguiu capturar relações mais complexas e robustas entre as variáveis, resultando em previsões precisas mesmo diante de uma alteração sutil na tendência. Já o Modelo Local mostrou-se frágil e pouco confiável quando confrontado com um cenário divergente de seu histórico restrito, evidenciando sua limitação para apoiar decisões no mundo real. A Tabela 10.2 sintetiza essa disparidade de desempenho.

Tabela 10.2: Comparativo de desempenho dos modelos no cenário de teste para Florianópolis.

Métrica	Modelo Federado (SC)	Modelo Local (Florianópolis)
TMI Real (2025)	6,50	6,50
TMI Prevista	6,31	8,02
Erro Absoluto	0,19	1,52

10.6 Aprendizados e Evolução Adquirida

A trajetória de desenvolvimento desta Prova de Conceito revelou-se tão ou mais valiosa que o próprio resultado final, proporcionando evolução tangível no entendimento da aplicação prática de Inteligência Artificial e Segurança da Computação. A escolha pelo Aprendizado Federado foi inicialmente motivada por um interesse teórico em conciliar a necessidade de dados para IA com o direito fundamental à privacidade. Ancorar esse conceito em um problema de relevância social, como a mortalidade infantil, conferiu ao projeto propósito claro e direção bem definida.

Um dos aprendizados mais significativos emergiu não da complexidade da construção da rede neural, mas da etapa de preparação dos dados. A realidade do trabalho de um

cientista de dados manifestou-se na depuração do *pipeline* de *ETL*. A primeira, e talvez mais impactante, lição foi constatar a complexidade inerente ao tratamento de dados do mundo real. Lidar com erros de codificação de caracteres, `ValueError` durante conversões de tipos e `AttributeError` decorrentes de incompatibilidades de versão de bibliotecas foi experiência prática inestimável, que evidenciou a importância da resiliência, da depuração sistemática e da escrita de código defensivo.

O *insight* técnico mais relevante, entretanto, foi a compreensão do chamado “abismo da extrapolação” e do motivo pelo qual o modelo local apresentava desempenho tão insatisfatório. Entender o papel crucial da normalização de dados (`StandardScaler`) e como essa etapa pode amplificar diferenças entre distribuições de dados de diferentes municípios foi um verdadeiro *momento aha!*. Isso consolidou o entendimento de que a robustez e a capacidade de generalização de um modelo são diretamente proporcionais à diversidade de seus dados de treinamento, e que testar um modelo com dados “fora da distribuição” (*out-of-distribution*) é a prova de fogo definitiva para aferir sua utilidade.

Além disso, o projeto reforçou a noção de que construir um modelo preciso é apenas metade da jornada; a outra metade reside na capacidade de comunicar seu valor de forma eficaz. A decisão de desenvolver um *dashboard* interativo com *Streamlit* e de roteirizar um cenário de teste claro foi fundamental para transformar uma coleção de métricas em uma narrativa compreensível e convincente. Isso demonstrou que a visualização de dados e a criação de interfaces intuitivas são habilidades essenciais para o cientista de dados, constituindo a ponte entre a análise técnica e a tomada de decisão estratégica.

Ao refletir sobre a trajetória, a evolução pessoal foi marcante. No início da disciplina, conceitos como Aprendizado Federado eram abstratos; ao final, a transição foi de um entendimento passivo para uma capacidade ativa de projetar, implementar, depurar e, sobretudo, demonstrar uma solução complexa capaz de abordar um problema de ponta a ponta. A aptidão para articular não apenas o que foi feito, mas também as razões por trás de cada decisão, representa a consolidação mais significativa do conhecimento adquirido.

10.7 Conclusão

Esta Prova de Conceito atingiu com êxito seu objetivo principal: demonstrar, de forma prática e conclusiva, o valor de abordagens de aprendizado colaborativo que preservam a privacidade dos dados. Os resultados evidenciaram que um modelo treinado com uma visão mais ampla e diversa — simulando os benefícios do Aprendizado Federado — não é apenas marginalmente superior, mas substancialmente mais robusto e confiável do que um modelo treinado de forma isolada.

O projeto validou a tese de que a sinergia entre Inteligência Artificial e Segurança da Computação é não apenas viável, mas também essencial para o desenvolvimento de soluções de IA éticas, justas e eficazes diante dos desafios do mundo real. Os obstáculos enfrentados na etapa de tratamento de dados e na implementação da arquitetura reforçaram a importância de competências sólidas em engenharia de software ao longo de todo o ciclo de vida de um projeto de *machine learning*.

O resultado final é uma demonstração funcional convincente e uma base consistente para futuras explorações. Entre os próximos passos recomendados, destacam-se:

- o enriquecimento do modelo com um conjunto mais abrangente de *features* socioeconômicas;
- a migração da simulação para uma implementação real utilizando *frameworks* distribuídos, como o *TensorFlow Federated* (TFF);
- a validação da arquitetura em um ambiente verdadeiramente descentralizado, com múltiplas fontes de dados reais.

Em consonância com diretrizes internacionais, como as *OECD Principles on Artificial Intelligence* (72), iniciativas de IA voltadas a serviços públicos devem priorizar não apenas desempenho técnico, mas também transparência, equidade, segurança e proteção da privacidade. Essa convergência de requisitos técnicos e princípios éticos é essencial para garantir que as soluções adotadas sejam sustentáveis, confiáveis e socialmente legítimas.

Parte III - Preservação Digital e Gestão de Acervos Históricos do Registro Civil

A conversão de acervos históricos analógicos em recursos digitais estruturados e pesquisáveis constitui um problema central para a ciência da informação e para a preservação da memória cultural. Esse desafio é particularmente relevante no caso de documentos manuscritos, cuja variabilidade gráfica, associada à degradação física ao longo do tempo, impõe barreiras significativas aos métodos convencionais de digitalização.

Este eixo temático reúne pesquisas que investigam a aplicação de modelos de aprendizado profundo para automatizar e ampliar a escala dos processos de compreensão e transcrição de documentos históricos do Registro Civil. As investigações aqui apresentadas decompõem o problema em duas subtarefas computacionais interdependentes:

- **Reconhecimento de Texto Manuscrito:** Avalia a eficácia de arquiteturas de última geração, como os *Transformers*, na transcrição de caligrafia cursiva complexa do século XIX;
- **Análise de Estruturas Documentais:** Emprega modelos de detecção de objetos para segmentar regiões de interesse lógico (por exemplo, averbações, assinaturas) previamente à etapa de transcrição textual.

Uma contribuição de destaque deste eixo é a incorporação do *Aprendizado Federado* ao processo, propondo uma metodologia que viabiliza a colaboração entre diferentes arquivos e instituições para o treinamento de modelos mais robustos, sem a necessidade de compartilhamento dos documentos originais.

Em conjunto, os estudos aqui reunidos delineiam um panorama abrangente sobre os potenciais de aplicação da Inteligência Artificial na preservação documental, favorecendo a transformação do patrimônio histórico em dados acessíveis, pesquisáveis e estruturados.

11 Reconhecimento de Escrita Manuscrita em Documentos Históricos

Autor: Gibram Goulart Farias

Tutor: Matheus Saldanha

11.1 Introdução

Vastos acervos de documentos históricos, como registros de batismo, casamento e óbito, contêm informações de valor inestimável para pesquisas genealógicas, históricas e sociais. Entretanto, grande parte desse conteúdo permanece inacessível, aprisionado em caligrafias antigas e disponível apenas para consulta física (97). A tecnologia de Reconhecimento de Texto Manuscrito (*Handwritten Text Recognition* – HTR) configura-se como uma solução promissora para transpor essa barreira, ao automatizar a transcrição e possibilitar a busca e análise de dados em larga escala (69, 5).

Apesar dos avanços recentes em modelos de Inteligência Artificial aplicados a essa tarefa (52), persiste um desafio significativo em domínios específicos: a escassez de conjuntos de dados (*datasets*) de alta qualidade, particularmente para documentos históricos em língua portuguesa. O desempenho de qualquer modelo de HTR está diretamente condicionado à qualidade e representatividade dos dados de treinamento, cuja elaboração exige trabalho minucioso e tecnicamente rigoroso.

Diante dessa lacuna, este trabalho apresenta o desenvolvimento de uma Prova de Conceito (*Proof of Concept* – PoC) com duplo objetivo:

- Detalhar o processo de criação de um *dataset* customizado a partir de registros civis brasileiros datados entre 1850 e 1930;
- Avaliar a viabilidade de aplicação de um modelo de Reconhecimento Óptico de Caracteres (*Optical Character Recognition* – OCR) pré-treinado para a transcrição automática desses documentos.

11.2 Trabalhos Relacionados

A aplicação de Inteligência Artificial para a transcrição de documentos históricos constitui uma área de pesquisa já consolidada. Estudos como o de [Khan et al. \(52\)](#) apresentam revisões abrangentes de diversas abordagens de Reconhecimento Óptico de Caracteres (*Optical Character Recognition* – OCR) aplicadas às humanidades, enquanto outros se concentram em desafios específicos, como a análise de documentos com *layouts* complexos ([36](#)) ou o processamento de textos de baixa qualidade e fisicamente degradados ([65](#)).

A criação de conjuntos de dados (*datasets*) especializados, como a proposta neste trabalho, constitui uma contribuição recorrente e relevante na literatura, com exemplos direcionados ao folclore irlandês ([70](#)) e a manuscritos gregos ([83](#)).

Por fim, a avaliação de ferramentas de OCR comerciais e de código aberto, como o Tesseract e APIs de serviços em nuvem, permanece um tema frequente. Nesse contexto, *benchmarks* como o conduzido por [Hegghammer \(43\)](#) fornecem subsídios para a seleção de modelos mais adequados a diferentes tipos de documentos históricos.

11.3 Metodologia

A metodologia adotada neste trabalho foi estruturada em duas frentes principais:

- construção de um novo conjunto de dados (*dataset*) para o português histórico;
- implementação de uma Prova de Conceito (*Proof of Concept* – PoC) para Reconhecimento de Texto Manuscrito (*Handwritten Text Recognition* – HTR).

11.3.1 Construção do Conjunto de Dados

Dada a escassez de recursos especializados para HTR em documentos históricos brasileiros, a criação de um *dataset* de alta fidelidade constituiu a etapa mais crítica do projeto. Estudos prévios demonstram que a disponibilidade de conjuntos de dados bem estruturados é fator determinante para o desempenho de modelos de HTR, como evidenciado por bases de referência internacional, incluindo o IAM Handwriting Database ([61](#)), o Bentham Dataset ([91](#)) e o READ-BAD Dataset ([53](#)). No contexto brasileiro, inexistem repositórios equivalentes para documentos históricos manuscritos em língua portuguesa, o que reforça a relevância desta iniciativa.

As fontes primárias utilizadas foram obtidas no portal FamilySearch, com ênfase em registros de batizado e certidões de nascimento datados entre 1850 e 1930. O processo de construção do *dataset* foi conduzido manualmente, garantindo alinhamento preciso entre cada imagem e sua transcrição textual.

O *pipeline* de preparação dos dados foi composto por quatro etapas principais:

1. **Obtenção de dados brutos:** coleta de imagens provenientes do FamilySearch, abrangendo livros de registro de batizados, certidões de nascimento e óbito;

2. **Transcrição manual:** reprodução fiel do conteúdo textual, visando máxima precisão na criação do *ground truth*. Esta é possivelmente a etapa mais relevante, pois a qualidade do modelo depende diretamente da qualidade dos dados de entrada. Documentos com caligrafia excessivamente ilegível foram excluídos do conjunto final;
3. **Segmentação:** recorte da imagem original em segmentos menores, cada um correspondendo a uma única linha de texto. Apesar de manual, o processo é altamente paralelizável;
4. **Associação:** criação de um arquivo de metadados (.csv) vinculando cada imagem de linha (por exemplo, `pagina150_rosalina_linha01.jpg`) à respectiva transcrição textual.

A automação do processo de transcrição elimina barreiras físicas e reduz custos para pesquisadores, genealogistas, estudantes e o público em geral, além de possibilitar buscas otimizadas e análises sistemáticas de grandes volumes de documentos. Essa abordagem favorece o avanço de estudos acadêmicos subsequentes e a preservação do patrimônio histórico documental.

11.3.2 Modelo de HTR e Ambiente Experimental

Para a tarefa de reconhecimento de texto, adotou-se um modelo de OCR pré-treinado da Microsoft, escolha pragmática considerando que o objetivo central desta PoC é validar o *pipeline* de dados. A execução dos experimentos e o ajuste fino (*fine-tuning*) foram realizados em uma estação de trabalho pessoal equipada com uma GPU NVIDIA RTX 3060, cuja capacidade de processamento mostrou-se adequada ao volume de dados utilizado neste estudo.

11.4 Resultados e Discussão

A avaliação do modelo treinado apresentou resultados mistos. Embora a mensuração quantitativa de métricas de acurácia não tenha sido o foco principal, a análise qualitativa revelou aspectos relevantes sobre a viabilidade e os desafios da tarefa, confirmando o trabalho como uma Prova de Conceito (*Proof of Concept* – PoC) bem-sucedida.

Os erros de transcrição observados podem ser atribuídos a fatores intrínsecos à natureza dos documentos históricos, entre os quais se destacam:

- **Ambiguidade da caligrafia cursiva:** a grande variação nos estilos de escrita manual entre diferentes escrivães e períodos históricos representa um desafio significativo para qualquer modelo de Reconhecimento de Texto Manuscrito (*Handwritten Text Recognition* – HTR);
- **Normas ortográficas antigas:** o uso de abreviações, grafias arcaicas e construções frasais típicas do português dos séculos XIX e XX introduz uma complexidade substancial, distinta daquela encontrada em textos modernos, nos quais muitos modelos pré-treinados se baseiam;

- **Variância nos dados:** a degradação física do papel, manchas de tinta e a qualidade variável das digitalizações contribuem para níveis elevados de ruído e variabilidade nas imagens de entrada.

Apesar das limitações de precisão, o objetivo central do projeto foi alcançado: demonstrar a viabilidade de construir um *pipeline* completo, abrangendo desde a coleta e o tratamento de fontes primárias até o treinamento e a inferência de um modelo de Inteligência Artificial para transcrição de documentos históricos do Registro Civil brasileiro.

Os resultados, embora insuficientes para aplicação imediata em ambiente de produção, estão alinhados com o escopo de uma PoC e indicam que a acurácia geral do modelo pode ser significativamente aprimorada com a ampliação do conjunto de dados e a diversificação das amostras. Essa constatação justifica a continuidade e o aprofundamento desta linha de pesquisa.

11.5 Conclusão

Os resultados obtidos foram heterogêneos: não suficientemente expressivos para um projeto de escopo amplo, mas plenamente válidos como Prova de Conceito (*Proof of Concept* – PoC) e como base para trabalhos futuros. Os erros de transcrição observados decorrem, em grande parte, da natureza ambígua dos dados, caracterizados por caligrafia cursiva, normas ortográficas do português histórico e elevado grau de variabilidade nas amostras. Ainda assim, mesmo com a precisão limitada do modelo, é plausível inferir que a ampliação e diversificação do conjunto de dados resultariam em melhorias significativas na acurácia geral, reforçando a viabilidade da abordagem proposta.

O desenvolvimento deste trabalho proporcionou avanços substanciais no aprendizado prático sobre o uso e a construção de modelos de Inteligência Artificial, abrangendo desde a coleta e a curadoria de dados até a otimização e a implantação de modelos. Constatou-se que é viável projetar aplicações úteis e de alta complexidade, com grande potencial de aplicabilidade. O processo também favoreceu o aprofundamento em técnicas de otimização, produção de conjuntos de dados e configuração de ambientes experimentais.

Em termos pessoais, o projeto mostrou-se altamente satisfatório e despertou o interesse em expandir a pesquisa com um conjunto de dados mais amplo. A experiência evidenciou que é possível conceber e implementar soluções tecnológicas avançadas para problemas inicialmente considerados excessivamente complexos, revelando o caráter interdisciplinar da área, que combina fundamentos de matemática, estatística e ciência da computação. Além disso, ao observar os trabalhos desenvolvidos por colegas, tornou-se evidente a importância de estabelecer métricas de segurança e explorar a integração entre este campo e outras áreas correlatas.

Por fim, ressalta-se que iniciativas de digitalização e preservação de acervos históricos estão alinhadas às recomendações de organismos internacionais. A UNESCO (98) estabelece diretrizes para a preservação e o acesso seguro ao patrimônio documental, inclusive em formato digital, reforçando a importância de padrões técnicos e jurídicos robustos. De forma complementar, a OCDE destaca que governos devem tratar os dados como ativos estratégicos, adotando políticas de governança que conciliem abertura, interoperabilidade, transparência e proteção de dados (74, 73).

Repositório da Prova de Conceito: <https://github.com/Xilbram/DatasetRegistros>

12 Do Tinteiro ao Silício: Transcrição de Manuscritos Cursivos com Inteligência Artificial

Autor: Murillo Cordeiro Guindani

Tutor: Wellington Fernandes Silvano

12.1 Introdução

O reconhecimento óptico de caracteres (*Optical Character Recognition* – OCR) constitui uma ferramenta promissora para a preservação e digitalização de documentos históricos (88). Este trabalho apresenta uma Prova de Conceito (*Proof of Concept* – PoC) baseada no uso do modelo TrOCR (*Transformer-based OCR*) (55), desenvolvido pela Microsoft, para a transcrição automatizada de documentos manuscritos cursivos datados do século XIX, especificamente registros paroquiais do estado do Rio de Janeiro (*Registros Paroquiais de Terras sec. XIX*) (33). A motivação central reside na aplicação de tecnologias de leitura automatizada em larga escala, visando à preservação digital e à extração de informações estruturadas desses documentos históricos. Tal abordagem atende demandas do Registro Civil relacionadas à leitura e ao tratamento de arquivos manuscritos antigos, frequentemente caracterizados por grafia cursiva, variações ortográficas e degradação visual.

Durante o desenvolvimento da PoC, utilizou-se como base o modelo TrOCR pré-treinado pela Microsoft (`microsoft/trocr-base-handwritten` disponível no Hugging Face, [s.d.]) para reconhecimento de manuscritos. Foram testadas também versões com ajuste fino (*fine-tuning*), incluindo modelos treinados com documentos jurídicos em finlandês (`Kansallisarkisto/court-records-htr`, [s.d.]) e com documentos históricos do Arquivo Nacional da Suécia (`Riksarkivet/trocr-base-handwritten-hist-swe-2`, [s.d.]). Curiosamente, o modelo sueco apresentou o melhor desempenho entre os testados, mesmo diante de diferenças linguísticas, provavelmente devido à sua familiaridade com caligrafia antiga resultante do grande volume de dados históricos utilizados no treinamento.

A proposta manteve o caráter de PoC, priorizando uma implantação simplificada via API da Hugging Face, sem integração com ferramentas auxiliares de detecção de texto, como o EasyOCR (48) ou o MMOCR (78). No entanto, foram identificadas limitações relevantes, como a incapacidade do modelo de processar frases completas com precisão, sendo necessário dividir as imagens palavra por palavra, além de dificuldades na personalização

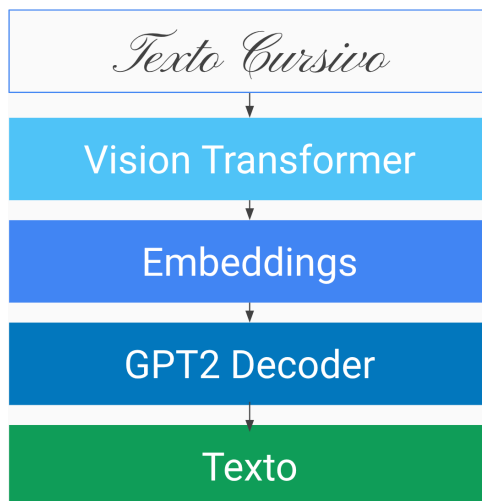
da decodificação (por exemplo, evitar caracteres suecos como “ö”).

O desenvolvimento do projeto demandou compreensão de arquiteturas avançadas, incluindo o estudo do artigo *Attention Is All You Need* (102), a participação em aulas introdutórias de *Deep Learning* (como o curso MIT 6.S191) e a leitura técnica da documentação do TrOCR. Um dos principais aprendizados foi reconhecer o potencial da Inteligência Artificial não apenas como ferramenta de automação, mas como aliada estratégica na preservação da memória documental e histórica.

12.2 Fundamentos Teóricos

Transformers são arquiteturas de deep learning baseadas exclusivamente em mecanismos de atenção, introduzidas por Vaswani et al. (102) no artigo "Attention is All You Need". Eles revolucionaram o campo de Processamento de Linguagem Natural (PLN) ao substituir mecanismos sequenciais como RNNs e LSTMs por um sistema capaz de modelar dependências globais entre palavras, permitindo treinamentos mais paralelizáveis e escaláveis. A base da arquitetura está no mecanismo de atenção escalada dot-product, que permite ao modelo focar em diferentes partes da entrada ao gerar a saída. No caso de OCR com TrOCR, esse conceito é estendido para o domínio visual.

O Vision Transformer (ViT) é a aplicação do paradigma transformer para imagens. Introduzido por Dosovitskiy et al. (34), o ViT divide uma imagem em pequenos patches (como se fossem "palavras visuais"), transforma cada patch em um vetor via embedding linear, e processa a sequência de vetores como um transformer tradicional faria com palavras.



Fluxograma demonstrando o processamento do TrOCR

No TrOCR, o ViT funciona como encoder visual, extraindo características da imagem que serão interpretadas pelo decoder textual. Entre o encoder visual (ViT) e o decoder textual (GPT2-like) do TrOCR, ocorre a transformação das representações visuais contínuas em embeddings posicionais e semânticos, os quais são usados como contexto para a geração de texto. Esses embeddings permitem ao decoder autorregressivo interpretar os elementos visuais da imagem como unidades linguísticas.

12.3 Resultados

Por se tratar de uma Prova de Conceito (*Proof of Concept* – PoC), os resultados apresentados não têm como objetivo validar estatisticamente o desempenho do modelo, mas sim demonstrar seu potencial e identificar limitações práticas que possam orientar desenvolvimentos futuros.

Foram utilizados recortes de documentos paroquiais manuscritos do século XIX, provenientes do estado do Rio de Janeiro, contendo nomes, datas e localidades. As imagens foram submetidas a pré-processamento com aumento de contraste e, posteriormente, processadas pelo modelo TrOCR por meio da API da Hugging Face.

A Figura 12.1 apresenta um exemplo de amostra utilizada.

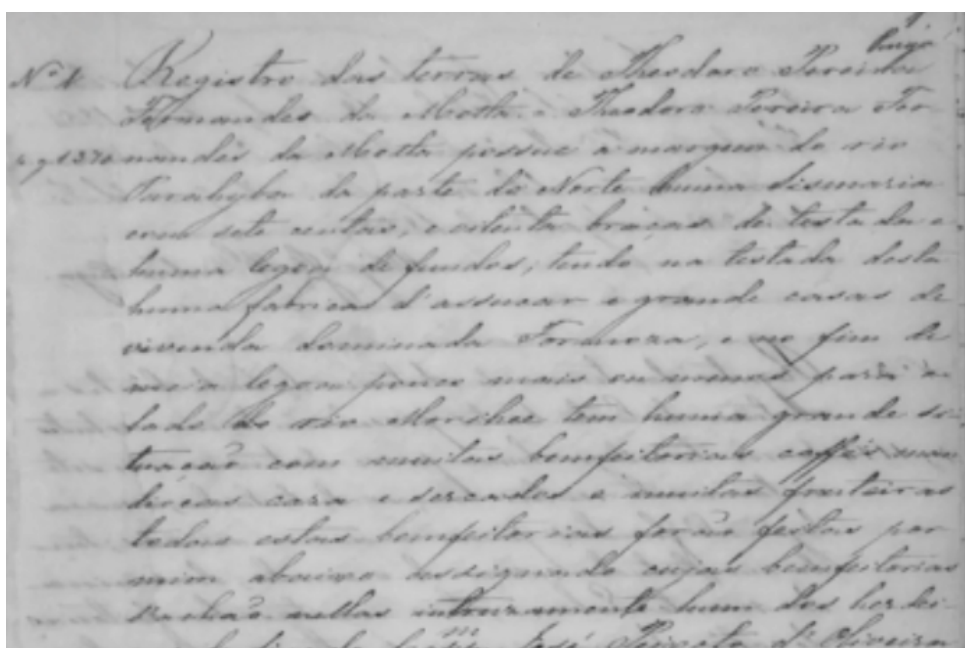


Figura 12.1: Exemplo de amostra utilizada contendo trecho de documento manuscrito do século XIX.

A Tabela 12.1 apresenta exemplos qualitativos de transcrição obtidos pelo modelo.

Tabela 12.1: Resultados qualitativos da transcrição automática.

Imagem	Transcrição	Correto?
	Registro	Sim
	terras	Sim
	dasterns	Não
	de Skreddare	Não

Os exemplos acima foram extraídos manualmente em segmentos curtos (palavras ou expressões breves). Observou-se que, ao processar blocos maiores de texto, o modelo não

conseguiu gerar transcrições satisfatórias, evidenciando uma limitação na capacidade de lidar com sequências mais extensas.

12.4 Considerações Finais

Este trabalho investigou o uso do modelo TrOCR como solução baseada em Inteligência Artificial para o reconhecimento de texto manuscrito histórico, com foco em documentos do século XIX no Brasil. A adoção dessa tecnologia visa contribuir para a digitalização, preservação e catalogação de acervos arquivísticos de relevância para o Registro Civil, promovendo maior acessibilidade e eficiência na consulta a esses registros.

Os resultados obtidos foram heterogêneos: não suficientemente expressivos para um projeto de escopo amplo, mas plenamente válidos como Prova de Conceito (*Proof of Concept* – PoC) e como base para trabalhos futuros. Os erros de transcrição observados decorrem, em grande parte, da natureza ambígua dos dados, caracterizados por caligrafia cursiva e normas ortográficas do português histórico, além de um elevado grau de variabilidade nas amostras. Ainda assim, mesmo com a precisão limitada do modelo, é plausível inferir que a ampliação e diversificação do conjunto de dados resultariam em melhorias significativas na acurácia geral, reforçando a viabilidade da abordagem proposta.

O desenvolvimento desta PoC exigiu compreensão aprofundada de arquiteturas de atenção e do funcionamento interno de modelos do tipo *encoder-decoder*, resultando em um aprendizado técnico substancial. Observou-se que é viável projetar aplicações úteis e de alta complexidade, com grande potencial de aplicabilidade. O processo favoreceu também o aprofundamento em técnicas de otimização, produção de conjuntos de dados e configuração de ambientes experimentais.

A análise crítica evidenciou que o TrOCR combina desempenho satisfatório, facilidade de implementação e requisitos computacionais acessíveis, configurando-se como uma base sólida para projetos de preservação documental. Contudo, sua utilização em contextos de produção requer complementação com técnicas de pré-processamento, segmentação e especialização linguística, a fim de superar limitações e garantir consistência em acervos históricos mais complexos.

Em termos pessoais, o projeto foi altamente satisfatório e despertou o interesse em expandir a pesquisa com um conjunto de dados mais amplo. A experiência mostrou que é possível conceber e implementar soluções tecnológicas avançadas para problemas que inicialmente pareciam excessivamente complexos, evidenciando o caráter interdisciplinar da área, que combina fundamentos de matemática, estatística e ciência da computação. Além disso, observando os trabalhos de colegas, tornou-se evidente a importância de estabelecer métricas de segurança e explorar a integração entre esse campo e outras áreas correlatas.

Repositório da Prova de Conceito: <https://github.com/Xilbram/DatasetRegistros>

13 Identificação de Estruturas Gráficas em Documentos Históricos com Aprendizado Federado

Autor: Lucas Castro Truppel Machado

Tutor: Gustavo Biage

13.1 Introdução

O presente trabalho foi desenvolvido no âmbito da disciplina de Segurança e Inteligência Artificial, com o objetivo de investigar a interseção prática entre estas duas áreas por meio de uma prova de conceito (*proof of concept*). O foco central consistiu na aplicação de técnicas de Inteligência Artificial (IA) para a identificação de estruturas gráficas em documentos históricos, abordando um desafio de segurança fundamental: a preservação da privacidade de dados sensíveis.

A motivação do estudo decorre de um problema concreto enfrentado por cartórios e arquivos históricos: o grande volume de documentos – como assentos de nascimento – que necessitam ser digitalizados e processados. A estrutura desses documentos antigos é frequentemente complexa e heterogênea, o que dificulta a extração de informações por meio de ferramentas convencionais de Reconhecimento Óptico de Caracteres (*Optical Character Recognition* – OCR). Nesse contexto, a IA apresenta-se como uma alternativa promissora para automatizar a detecção e a segmentação de seções visuais relevantes, otimizando o desempenho e a acurácia das etapas subsequentes de OCR, como evidenciado por [Reul et al.](#) (88).

Contudo, o treinamento de um modelo de IA robusto requer um volume significativo de dados, preferencialmente oriundos de múltiplos cartórios. Surge, então, um desafio crítico de segurança: como treinar um modelo de forma colaborativa sem centralizar documentos que contenham informações pessoais e sensíveis? A solução adotada foi o Treinamento Federado (*Federated Learning*), abordagem que possibilita o treinamento de um modelo global mantendo os dados de cada participante em sua origem, com a troca apenas dos parâmetros aprendidos (pesos) do modelo, conforme a metodologia proposta por [McMahan et al.](#) (63).

13.2 Ferramentas Utilizadas

A execução deste projeto foi viabilizada por um conjunto de ferramentas de software que abstraem grande parte da complexidade subjacente ao desenvolvimento, permitindo que o foco se mantivesse na lógica da aplicação, no tratamento do *dataset* e na análise dos resultados.

13.2.1 *Framework* Ultralytics

A implementação do modelo YOLO (96) foi realizada com o auxílio da biblioteca Ultralytics (50). Este *framework* é amplamente reconhecido na comunidade de visão computacional por sua facilidade de uso, fornecendo *pipelines* integrados para treinamento, validação, teste e exportação de modelos. A utilização do Ultralytics simplificou significativamente a aplicação de um modelo de detecção de objetos de última geração, permitindo concentrar esforços nas etapas de pré-processamento dos dados e análise dos resultados.

13.2.2 *Framework* Flower

Para orquestrar o processo de Aprendizado Federado, foi adotado o *framework* Flower (8). A principal vantagem do Flower é ser agnóstico em relação à biblioteca de *machine learning*, possibilitando integração com modelos desenvolvidos em PyTorch (como os da Ultralytics), TensorFlow, entre outros. O Flower é projetado para ser flexível e de fácil utilização, permitindo que pesquisadores e desenvolvedores convertam *pipelines* de treinamento centralizado em sistemas federados com poucas modificações no código.

13.2.3 UltraFlwr

O UltraFlwr é um repositório de código aberto disponível no GitHub, que integra diretamente o Ultralytics ao *framework* Flower (57). Essa integração fornece uma solução prática para aplicar modelos YOLO em cenários federados, sem a necessidade de configuração manual da infraestrutura de comunicação entre cliente e servidor.

Com o UltraFlwr, basta preparar os conjuntos de dados locais e configurar parâmetros básicos do treinamento, como o número de rodadas (*federated rounds*) e o número de clientes participantes. O repositório já disponibiliza a estrutura necessária para iniciar o treinamento federado de forma distribuída, cuidando da sincronização dos pesos, da separação entre cliente e servidor e da execução das tarefas locais.

13.2.4 COCO Annotator

Para a anotação das imagens utilizadas no treinamento do modelo de detecção, foi empregada a ferramenta COCO Annotator (16), uma aplicação web para anotação de imagens, versátil e eficiente na criação de dados rotulados voltados a tarefas de detecção de objetos.

O COCO Annotator oferece uma interface intuitiva, que facilita o processo de marcação manual mesmo em conjuntos de dados extensos. Entre suas funcionalidades mais relevantes, destacam-se:

- Possibilidade de rotular partes específicas de uma imagem;
- Exportação direta no formato COCO – padrão amplamente utilizado em projetos de visão computacional.

13.3 Desenvolvimento da Prova de Conceito

Esta seção descreve o processo prático de construção da solução, abrangendo desde a preparação dos dados até a implementação do *frontend* de demonstração.

13.3.1 Preparação do *Dataset*

A base de qualquer projeto de *machine learning* é um conjunto de dados (*dataset*) de alta qualidade. Dada a natureza específica do problema, foi necessário construir um *dataset* customizado. O processo seguiu três etapas principais:

1. **Extração de imagens:** Os documentos de origem estavam em formato PDF, contendo imagens JPEG embutidas. Foi desenvolvido um *script* em Python para identificar e extrair diretamente essas imagens, obtendo os dados em formato compatível com as ferramentas de visão computacional utilizadas posteriormente;
2. **Anotação manual:** Utilizando localmente a ferramenta COCO Annotator, cada uma das 133 imagens foi anotada, conforme ilustrado na Figura 13.1. Foram desenhadas caixas delimitadoras (*bounding boxes*) ao redor das duas estruturas de interesse: averbação (normalmente inserida nas margens) e declaração (seção de autoria do oficial de registro). O processo apresentou desafios inerentes a documentos históricos, como variações de caligrafia, layouts não padronizados e texto sobreposto ou manuscrito em ângulos variados, tornando a definição de limites precisa e subjetiva;
3. **Conversão de formato:** O COCO Annotator exporta as anotações no formato COCO (*JSON*). Entretanto, os modelos YOLO da Ultralytics requerem um formato específico: um arquivo de texto (*.txt*) por imagem, com cada linha contendo o ID da classe seguido pelas coordenadas da caixa delimitadora (centro x , centro y , largura e altura). Foi utilizado o utilitário de conversão do Ultralytics para gerar este formato, finalizando a preparação dos dados para treinamento.

O *dataset* final, composto por 133 imagens anotadas, foi dividido em um conjunto de treinamento (70%, 93 imagens) e um de validação (30%, 40 imagens).

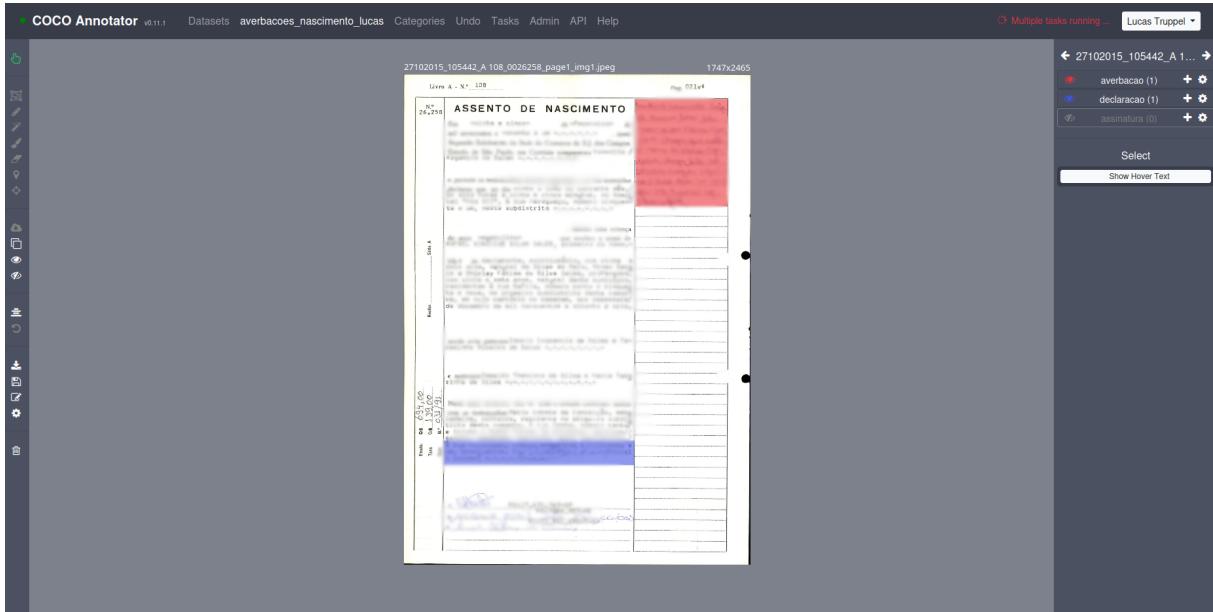


Figura 13.1: Processo de anotação de um assento de nascimento.

13.3.2 Treinamento

A implementação do *pipeline* de Aprendizado Federado (*Federated Learning*) foi acelerada pelo uso do repositório de código aberto UltraFlwr (57), que integra os modelos YOLO (96) da Ultralytics ao *framework* Flower. A escolha pelo UltraFlwr decorreu da complexidade técnica da integração direta de um modelo avançado como o YOLO a um ambiente genérico de aprendizado federado, especialmente quanto à serialização e desserialização corretas do estado do modelo para intercâmbio de parâmetros entre cliente e servidor.

Ao adotar o UltraFlwr, foi possível contornar essas questões de baixo nível e concentrar esforços na preparação do *dataset*, configuração do experimento e análise dos resultados.

A simulação foi estruturada com um servidor central responsável por:

- Inicializar o modelo global;
- Selecionar os clientes participantes em cada rodada;
- Agregar os pesos recebidos;
- Redistribuir o modelo atualizado.

O fluxo está ilustrado na Figura 13.2.

Foram simulados dois clientes, representando cartórios distintos, cada um com sua própria fração dos dados. O conjunto de treinamento (93 imagens) foi particionado entre os clientes (46 e 47 imagens), simulando um cenário realista no qual cada cartório mantém seu acervo documental privado.

Foi utilizado o modelo YOLOv11n (96), uma variante leve da família YOLOv11, cujo sufixo *n* indica a versão *nano*, otimizada para restrições de recursos computacionais. A escolha buscou reduzir o tempo de treinamento e viabilizar a simulação local. O processo

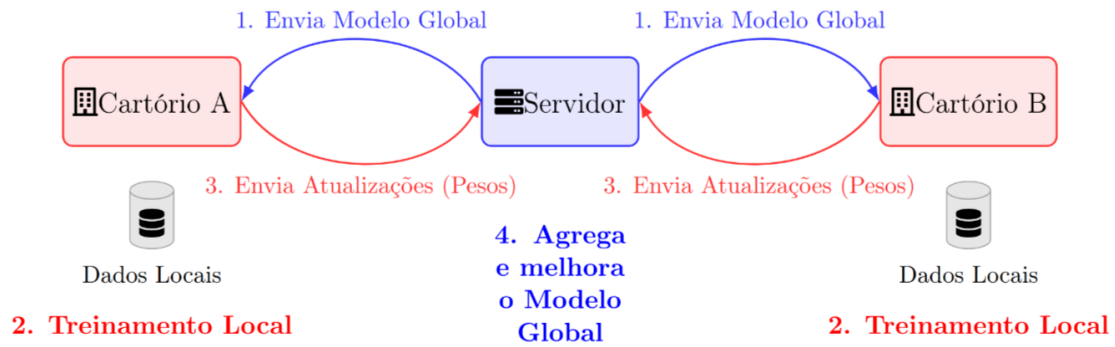


Figura 13.2: Diagrama do ciclo de treinamento federado.

federado foi conduzido ao longo de 100 rodadas, com cinco repetições independentes por rodada, totalizando cerca de 8 horas e 30 minutos de execução. Esse tempo reflete tanto o esforço computacional quanto a complexidade adicional da agregação contínua de modelos locais.

Para consolidar as atualizações locais, o servidor utilizou a estratégia FedAvg (*Federated Averaging*) (63), que consiste em calcular a média ponderada dos parâmetros recebidos de cada cliente, considerando o tamanho do conjunto de dados local. O modelo global é atualizado com essa média, promovendo aprendizado colaborativo eficaz sem compartilhamento direto dos dados originais.

13.4 Aplicação Web

Para validar a funcionalidade da solução de forma tangível e demonstrar seu potencial de aplicação, foi desenvolvida uma aplicação web simples utilizando o *framework* Django (31). A aplicação consiste em uma única página com interface de usuário minimalista, estruturada para proporcionar interação direta e objetiva. O fluxo de utilização segue as etapas abaixo:

1. O usuário acessa a página web e visualiza um campo para *upload* de arquivo;
2. O usuário seleciona e envia uma imagem de um documento de registro civil;
3. No *backend*, a imagem enviada é processada pelo modelo YOLOv11n (96) treinado. O modelo realiza a inferência, identificando as localizações das estruturas “averbação” e “declaração”;
4. A aplicação sobrepõe caixas delimitadoras (*bounding boxes*) à imagem original, nos locais detectados;
5. A imagem resultante, com as marcações, é retornada e exibida na página para o usuário.

Essa interface funciona como uma *Proof of Concept* (POC), evidenciando de forma clara e imediata o resultado do processo de detecção automática e validando a aplicabilidade prática do modelo desenvolvido.

A Figura 13.3 apresenta a interface antes do envio da imagem, enquanto a Figura 13.4 mostra o resultado retornado com as anotações sobre a imagem original.



Figura 13.3: Interface gráfica antes do envio da imagem.

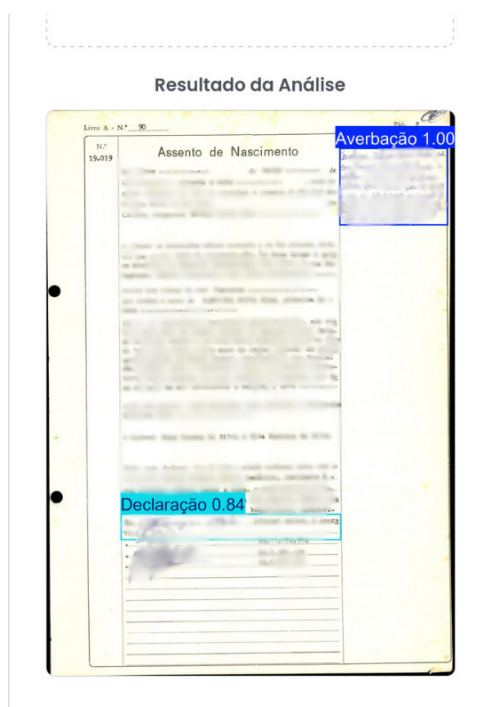


Figura 13.4: Interface gráfica após o envio da imagem.

13.5 Repositório do Projeto

O desenvolvimento do projeto pode ser acompanhado por meio dos seguintes repositórios:

- **Repositório do projeto:** Contém o código-fonte da aplicação web desenvolvida, bem como os *scripts* utilizados para a preparação do *dataset*;
- **UltraFlwr** (57): Repositório externo utilizado para realizar o treinamento do modelo. Foi necessário adicionar um diretório contendo os dados, conforme descrito no arquivo `README.md` do projeto, além de configurar o arquivo `config.py`.

13.6 Resultados Gerais

Esta seção apresenta os resultados obtidos na fase de validação do modelo. Primeiramente, definem-se as métricas de avaliação utilizadas, seguidas pela análise quantitativa dos dados.

13.6.1 Métricas de Avaliação para Detecção de Objetos

Para avaliar objetivamente o desempenho de um modelo de detecção de objetos, é fundamental utilizar métricas padronizadas. Neste projeto, adotaram-se as seguintes:

- **Precisão (P – *Precision*):** Mede a exatidão das previsões positivas, representando a fração de detecções corretas entre todas as detecções realizadas pelo modelo. Em termos simples, responde à pergunta: De todas as caixas que o modelo desenhou, qual porcentagem estava correta?;
- **Recall (R – *Revocação*):** Mede a completude das detecções, ou seja, a fração de verdadeiros positivos (TP) em relação a todos os objetos reais presentes nos dados. Em termos simples, responde: De todos os objetos existentes, qual porcentagem o modelo conseguiu detectar?;
- **mAP@50 (*mean Average Precision at IoU 0.50*):** Calcula a média da precisão para todas as classes, considerando correta uma predição cuja sobreposição (*Intersection over Union* – IoU) com a caixa real seja de, no mínimo, 50%. É uma métrica mais permissiva, adequada para indicar se o modelo identifica corretamente os objetos, mesmo com imprecisões na localização;
- **mAP@50-95:** Métrica mais rigorosa e abrangente, calculada sobre dez limiares de IoU, variando de 0,50 a 0,95 em incrementos de 0,05. Fornece uma visão detalhada da qualidade das detecções, exigindo precisão tanto na classificação quanto na localização dos objetos. Costuma apresentar valores menores que o mAP@50, refletindo de forma mais realista a performance geral.

13.6.2 Análise Quantitativa do Desempenho do Modelo

Os resultados no conjunto de validação, composto por 40 imagens e 55 instâncias de objetos, estão apresentados na Tabela 13.1. Esses valores foram obtidos diretamente a partir da rotina de validação do Ultralytics (50) com o modelo final treinado.

Tabela 13.1: Métricas de validação do modelo final.

Classe	Imagens	Instâncias	P	R	mAP50	mAP50-95
all	40	55	0,896	0,939	0,948	0,671
averação	14	15	0,937	0,991	0,970	0,788
declaração	40	40	0,855	0,886	0,925	0,555

Análise dos Resultados:

- **Desempenho geral:** O modelo apresentou desempenho robusto. A precisão geral de 0,896 indica que quase 90% das detecções foram corretas, enquanto o *recall* de 0,939 mostra que quase 94% das instâncias reais foram identificadas;
- **Detecção versus localização:** O mAP@50 de 0,948 confirma que o modelo localiza as estruturas de interesse com alta eficácia. Contudo, a redução para 0,671 no mAP@50-95 revela que as caixas delimitadoras nem sempre se ajustam de forma precisa aos objetos, sendo penalizadas nos limiares mais altos de IoU;
- **Desempenho por classe:** Observa-se superioridade da classe *averbação* sobre *declaração* em todas as métricas. O mAP@50-95 de 0,788 para averbação é substancialmente maior que o de 0,555 para declaração, indicando maior precisão na localização dessa classe.

Quanto à velocidade de inferência, o modelo apresentou tempo médio de 62,9 milissegundos por imagem no hardware de validação, desempenho adequado para aplicações web em que o usuário envia um único documento e aguarda o processamento.

Síntese e implicações práticas. Os resultados obtidos evidenciam que o modelo desenvolvido possui maturidade técnica para ser aplicado em cenários reais de cartórios e arquivos históricos, sobretudo para a detecção de averbações, que apresentam maior uniformidade visual. Apesar de pequenas limitações na precisão de localização fina, o tempo de resposta e a alta taxa de acertos tornam a solução viável para integrar fluxos de digitalização e indexação documental, reduzindo trabalho manual e potencializando a acurácia de etapas subsequentes, como OCR especializado para manuscritos.

13.7 Discussão, Limitações e Aprendizados

O principal êxito deste trabalho foi demonstrar a viabilidade de uma abordagem de Aprendizado Federado (*Federated Learning*) para resolver um problema real de detecção de objetos em dados sensíveis. O modelo YOLO (96) mostrou-se uma ferramenta eficaz para a tarefa proposta. Contudo, reconhecem-se limitações relevantes na prova de conceito: o *dataset* utilizado foi reduzido (133 imagens) e o ambiente federado foi simulado com apenas dois clientes. Em um cenário real, seria necessário dispor de um volume de dados substancialmente maior e de uma infraestrutura com número significativamente mais elevado de clientes.

Ao longo do desenvolvimento, a evolução foi notável. Inicialmente, a ideia de combinar Inteligência Artificial e Segurança da Computação tinha caráter mais conceitual. O projeto exigiu compreender, na prática, o problema enfrentado, lidando com todo o ciclo de vida de um projeto de *machine learning*, desde a coleta e o pré-processamento dos dados até o treinamento e a avaliação do modelo.

Houve também um aprofundamento no entendimento da importância da privacidade. A implementação do treinamento federado tornou o conceito de *Privacy by Design*, conforme as diretrizes da OECD (76), mais concreto, elevando a segurança de um aspecto secundário para pilar central da arquitetura da solução.

Outro aprendizado importante foi reconhecer o valor de construir sobre o trabalho da comunidade. O uso de ferramentas e repositórios de código aberto, como os oferecidos pela Ultralytics (50), pelo *framework* Flower (8) e pelo UltraFlwr (57), foi essencial para acelerar o desenvolvimento e permitir foco nos elementos mais inovadores do projeto.

Por fim, o trabalho contribuiu para consolidar habilidades técnicas, aprofundar o domínio de *frameworks* específicos e aprimorar a configuração de ambientes voltados ao aprendizado de máquina.

Conclui-se que a disciplina cumpriu seu objetivo de permitir a exploração de uma fronteira do conhecimento, na qual a Inteligência Artificial não é apenas uma ferramenta de automação, mas também uma tecnologia que pode e deve ser projetada com base em princípios fundamentais de segurança e privacidade.

13.8 Trabalhos Futuros

Como desdobramento natural deste projeto, diversos caminhos podem ser explorados para aprimorar tanto a robustez quanto a aplicabilidade da solução desenvolvida.

Em primeiro lugar, é essencial expandir o *dataset* com exemplos provenientes de diferentes cartórios, possibilitando ao modelo aprender uma maior variedade de padrões e, consequentemente, melhorar sua capacidade de generalização.

Propõe-se também testar o ambiente federado com um número significativamente maior de clientes e, idealmente, executar os clientes em máquinas distintas, de modo a simular de forma mais realista os desafios e comportamentos de um cenário distribuído. Além disso, a utilização de uma infraestrutura de hardware mais potente para o treinamento, bem como a adoção de uma versão mais robusta do modelo YOLO (96), pode contribuir para um desempenho superior na detecção.

Do ponto de vista funcional, há espaço para ampliar o escopo do modelo de detecção a fim de identificar outras seções relevantes dos documentos, além das áreas de averbação e declaração. A aplicação de OCR nas regiões segmentadas também se apresenta como um passo importante, permitindo a extração automática do conteúdo textual para análises posteriores.

Por fim, estratégias de Aprendizado Federado mais sofisticadas, como o FedProx (56), podem ser exploradas para lidar com a heterogeneidade dos dados e dos dispositivos participantes, aumentando a robustez e a aplicabilidade da solução em contextos reais.

Referências

- 1 ADHATARAO, Supriya e LAURADOUX, Cédric. Exploitation and sanitization of hidden data in pdf files: Do security agencies sanitize their pdf files? In: PROCEEDINGS of the 2021 ACM Workshop on Information Hiding and Multimedia Security. [S. l.: s. n.], 2021. P. 35–44.
- 2 ADOBE INC. **Adobe Scan: Mobile PDF Scanner App**. [S. l.: s. n.], 2025. <https://acrobat.adobe.com/us/en/mobile/scanner-app.html>. Versão 24.6.14. Acesso em: 8 jul. 2025.
- 3 AFIFI, Mahmoud. 11K Hands: Gender recognition and biometric identification using a large dataset of hand images. **Multimedia Tools and Applications**, 2019. DOI: [10.1007/s11042-019-7424-8](https://doi.org/10.1007/s11042-019-7424-8). Disponível em: <https://doi.org/10.1007/s11042-019-7424-8>.
- 4 ARTIFEX SOFTWARE. **PyMuPDF**. [S. l.: s. n.], 2024. Python bindings for MuPDF's rendering library. Disponível em: <https://pymupdf.readthedocs.io/>. Acesso em: 15 jan. 2025.
- 5 ASKAROV, M. et al. Preserving Historical Documents Using OCR and Natural Language Processing (NLP). In: 2025 International Conference on Computational Innovations and Engineering Sustainability (ICCIES). [S. l.: s. n.], 2025. P. 1–6. DOI: [10.1109/ICCIES63851.2025.11032769](https://doi.org/10.1109/ICCIES63851.2025.11032769).
- 6 BANEGAS, Gustavo. **Pentanômios irredutíveis sobre $GF(2^m)$** . 2015. Diss. (Mestrado) – Universidade Federal de Santa Catarina, Florianópolis, SC. Dissertação de Mestrado.
- 7 BANEGAS, Gustavo; CUSTÓDIO, Ricardo e PANARIO, Daniel. A new class of irreducible pentanomials for polynomial-based multipliers in binary fields. **Journal of Cryptographic Engineering**, Springer, v. 9, n. 4, p. 359–373, 2019. ISSN 2190-8508. DOI: [10.1007/s13389-018-0197-6](https://doi.org/10.1007/s13389-018-0197-6).
- 8 BEUTEL, Daniel J et al. Flower: A Friendly Federated Learning Research Framework. **arXiv preprint arXiv:2007.14390**, 2020.
- 9 BITANSKY, N. et al. From extractable collision resistance to succinct non-interactive arguments of knowledge, and back again. In: PROCEEDINGS of the 3rd Innovations in Theoretical Computer Science Conference. New York, NY, USA: Association for Computing Machinery, 2012. (ITCS '12), p. 326–349. ISBN 9781450311151. DOI: [10.1145/2090236.2090263](https://doi.org/10.1145/2090236.2090263). Disponível em: <https://doi.org/10.1145/2090236.2090263>.
- 10 BLACKLEDGE, Jonathan e MOSOLA, Napo. Applications of Artificial Intelligence to Cryptography. **Transactions on Engineering and Computing Sciences**, v. 8, n. 3, p. 21–60, jun. 2020. DOI: [10.14738/tmlai.83.8219](https://doi.org/10.14738/tmlai.83.8219). Disponível em: <https://journals.scholarpublishing.org/index.php/TMLAI/article/view/8219>.
- 11 BRASIL. **Lei nº 8.069, de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências**. [S. l.: s. n.], 1990. Diário Oficial da União.
- 12 _____. **Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil**. [S. l.: s. n.], 2002. Diário Oficial da União.
- 13 _____. **Lei nº 12.965, de 23 de abril de 2014. Marco Civil da Internet**. **Diário Oficial da União**, Brasília, DF, abr. 2014.
- 14 _____. **Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD)**. [S. l.: s. n.], 2018. Diário Oficial da União. Brasília, DF, 15 de agosto de 2018.

- 15 BRENT, Richard P. e ZIMMERMANN, Paul. Irreducible Polynomials over $GF(2)$ with Three Prescribed Coefficients. **Applicable Algebra in Engineering, Communication and Computing**, Springer, v. 22, n. 5-6, p. 387–396, 2011. DOI: [10.1007/s00200-011-0155-8](https://doi.org/10.1007/s00200-011-0155-8).
- 16 BROOKS, Justin. **COCO Annotator: web-based image annotation tool for object detection and localization**. [S. l.: s. n.], 2019. GitHub repository. Disponível em: <https://github.com/jsbroks/coco-annotator>. Acesso em: 8 ago. 2025.
- 17 CASTIGLIONE, Aniello; DE SANTIS, Alfredo e SORIENTE, Claudio. Security and privacy issues in the Portable Document Format. **Journal of Systems and Software**, Elsevier, v. 83, n. 10, p. 1813–1822, 2010.
- 18 CHARFI, Nesrine et al. **REST database**. [S. l.]: IEEE Dataport, 2021. DOI: [10.21227/7gf6-v687](https://doi.org/10.21227/7gf6-v687). Disponível em: <https://iee-dataport.org/open-access/rest-database>.
- 19 CHEN, Xiangrong e GONG, Ziman. **YOLOv5-Lite: Lighter, faster and easier to deploy**. [S. l.: s. n.], 2021. DOI: [10.5281/zenodo.5241425](https://doi.org/10.5281/zenodo.5241425).
- 20 CHEN, Y.; DAI, W.; ZHANG, Y. et al. FATE-LLM: A Federated Learning-based Large Language Model. In: ACM. PROCEEDINGS of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. [S. l.: s. n.], 2024.
- 21 CLARK, Kevin et al. ELECTRA: Pre-training Text Encoders as Discriminators Rather Than Generators. **arXiv preprint**, arXiv:2003.10555, 2020. Disponível em: <https://arxiv.org/abs/2003.10555>.
- 22 CNJ. **Provimento nº 16, de 17 de fevereiro de 2012**: Dispõe sobre a expedição de certidão de nascimento nos casos de filhos de casais homoafetivos. [S. l.: s. n.], 2012. Publicado em 17 fev. 2012. Disponível em: <https://atos.cnj.jus.br/atos/detalhar/1523>. Acesso em: 8 ago. 2025.
- 23 _____. **Resolução CNJ nº 332, de 21 de agosto de 2020**: Dispõe sobre a ética, a transparência e a governança na produção e no uso de inteligência artificial no Poder Judiciário. Brasília, DF: [s. n.], 2020. Diário da Justiça Eletrônico, n.º 274, p. 4–8. Publicada em 25 ago. 2020. Disponível em: <https://hdl.handle.net/20.500.12178/176410>. Acesso em: 8 ago. 2025.
- 24 CUI, Cheng et al. PaddleOCR 3.0 Technical Report. **arXiv preprint arXiv:2507.05595**, 2025.
- 25 CUI, G.; ZHANG, Y.; YAO, R. et al. FedNoisy-Adapter: A Parameter-efficient Fine-tuning Method for Federated Learning of Large Language Models with Noisy Data. **Information Fusion**, Elsevier, v. 115, p. 102830, 2025.
- 26 CUNHA, Luís F. e RAMALHO, José C. **bert-portuguese-ner: Named-Entity Recognition model for Portuguese**. [S. l.: s. n.], 2024. <https://huggingface.co/lfcc/bert-portuguese-ner>. Hugging Face model card. Acesso em: 8 ago. 2025.
- 27 DASH, Bibhu e ULLAH, Sameeh. Quantum-safe: Cybersecurity in the age of Quantum-Powered AI. **World Journal of Advanced Research and Reviews**, v. 21, n. 1, p. 1555–1563, 2024.
- 28 DENG, Jiankang et al. Sub-center ArcFace: Boosting Face Recognition by Large-Scale Noisy Web Faces. In: PROCEEDINGS of the European Conference on Computer Vision (ECCV). Glasgow, United Kingdom: Springer-Verlag, 2020. Part XI, p. 741–757. ISBN 978-3-030-58620-1. DOI: [10.1007/978-3-030-58621-8_43](https://doi.org/10.1007/978-3-030-58621-8_43). Disponível em: https://doi.org/10.1007/978-3-030-58621-8_43.
- 29 DENG, Wei; LI, Jun e ZHANG, Wei. BioAu-SVM+ZKP: Privacy-preserving biometric authentication using support vector machines and zero-knowledge proofs. **Computers & Security**, Elsevier, v. 141, p. 103089, 2024. DOI: [10.1016/j.cose.2024.103089](https://doi.org/10.1016/j.cose.2024.103089).
- 30 DEVLIN, Jacob et al. BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding. **arXiv preprint arXiv:1810.04805**, 2018.
- 31 DJANGO SOFTWARE FOUNDATION. **Django Documentation**. [S. l.: s. n.], 2025. Disponível em: <https://docs.djangoproject.com/en/stable/>. Acesso em: 8 ago. 2025.
- 32 DOCUSIGN, INC. **DocuSign eSignature**. [S. l.: s. n.], 2025. <https://www.docusign.com>. Plataforma de assinatura eletrônica. Acesso em: 8 ago. 2025.

- 33 DOCVIRT. **Registro de Terras Página 13705**. [S. l.: s. n.]. https://app.docvirt.com/reg_terra3/pageid/13705. Acesso em: 8 jul. 2025.
- 34 DOSOVITSKIY, Alexey et al. An image is worth 16x16 words: Transformers for image recognition at scale. **arXiv preprint arXiv:2010.11929**, 2020.
- 35 FIAT, Amos e SHAMIR, Adi. How to Prove Yourself: Practical Solutions to Identification and Signature Problems. In: **ADVANCES in Cryptology – CRYPTO’ 86**. [S. l.]: Springer, 1987. P. 186–194. DOI: [10.1007/3-540-47721-7_12](https://doi.org/10.1007/3-540-47721-7_12).
- 36 FLEISCHHACKER, D.; KERN, R. e GÖDERLE, W. Enhancing OCR in historical documents with complex layouts through machine learning. **International Journal on Digital Libraries**, v. 26, p. 3, 2025. DOI: [10.1007/s00799-025-00413-z](https://doi.org/10.1007/s00799-025-00413-z).
- 37 GAO, Shuhong e PANARIO, Daniel. Tests and Constructions of Irreducible Polynomials over Finite Fields. **Foundations of Computational Mathematics**, Springer, v. 10, n. 6, p. 689–711, 2010. DOI: [10.1007/s10208-010-9072-x](https://doi.org/10.1007/s10208-010-9072-x).
- 38 GOLDREICH, Oded. **Foundations of Cryptography: Volume 1, Basic Tools**. [S. l.]: Cambridge University Press, 2019. DOI: [10.1017/9781108589081](https://doi.org/10.1017/9781108589081).
- 39 GORDON, Andrew D. e JEFFREY, Alan. Secrecy despite compromise: Types, cryptography, and the pi-calculus. In: **INTERNATIONAL Conference on Concurrency Theory**. Berlin, Heidelberg: Springer, 2005. P. 186–201.
- 40 GRINBERG, Miguel e RONACHER, Armin. **Flask: A micro web framework for Python**. [S. l.: s. n.], 2010. <https://flask.palletsprojects.com/>. Acesso em: 8 ago. 2025.
- 41 GUHA, Abhijit et al. A deep learning model for information loss prevention from multi-page digital documents. **IEEE Access**, IEEE, v. 9, p. 80451–80465, 2021.
- 42 GUO, Daya et al. Deepseek-r1: Incentivizing reasoning capability in llms via reinforcement learning. **arXiv preprint arXiv:2501.12948**, 2025.
- 43 HEGGHAMMER, T. OCR with Tesseract, Amazon Textract, and Google Document AI: a benchmarking experiment. **Journal of Computational Social Science**, v. 5, p. 861–882, 2022. DOI: [10.1007/s4009-022-00199-3](https://doi.org/10.1007/s4009-022-00199-3).
- 44 HOFFSTAETTER, Samuel. **pytesseract**. [S. l.: s. n.], 2024. Python-tesseract is an optical character recognition (OCR) tool for python. Disponível em: <https://pypi.org/project/pytesseract/>. Acesso em: 15 jan. 2025.
- 45 IBGE. **SIDRA Sistema IBGE de Recuperação Automática**. [S. l.: s. n.]. <https://sidra.ibge.gov.br/>. Acesso em: 8 ago. 2025.
- 46 IBM. **Cost of a Data Breach Report 2024**. [S. l.], 2024. Baseado em análise de violações ocorridas entre março de 2023 e fevereiro de 2024.
- 47 IZADPANAHKAKHK, M. et al. Novel mobile palmprint databases for biometric authentication. **International Journal of Grid and Utility Computing**, v. 10, n. 5, p. 465–474, 2019. Sapienza dataset. Disponível em: <https://www.kaggle.com/datasets/mahdieizadpanah/sapienza-university-mobile-palmprint-databasesmpd>.
- 48 JAIDED AI. **EasyOCR: Ready-to-use OCR with 80+ Languages Supported**. [S. l.: s. n.], 2020. <https://github.com/JaidedAI/EasyOCR>. Versão 1.6.2. Acesso em: 8 ago. 2025.
- 49 JIANG, Albert Q. et al. Mistral 7B. **arXiv preprint**, arXiv:2310.06825, 2023. DOI: [10.48550/arXiv.2310.06825](https://doi.org/10.48550/arXiv.2310.06825). Disponível em: <https://arxiv.org/abs/2310.06825>.
- 50 JOCHER, Glenn; QIU, Jing e CHAURASIA, Ayush. **Ultralytics YOLO**. [S. l.]: Ultralytics, jan. 2023. URL: <https://ultralytics.com>. Disponível em: <https://github.com/ultralytics/ultralytics>.
- 51 KEYLESS. **Zero-Knowledge Biometrics**. [S. l.: s. n.], 2024. <https://keyless.io/technology/zero-knowledge-biometrics>. Acesso em: 8 ago. 2025.

- 52 KHAN, Arsh et al. OCR Approaches for Humanities: Applications of Artificial Intelligence/Machine Learning on Transcription and Transliteration of Historical Documents. **Digital Studies in Language and Literature**, v. 1, n. 1-2, p. 85–112, 2024. DOI: [10.1515/ds11-2024-0013](https://doi.org/10.1515/ds11-2024-0013).
- 53 KÖHLER, Andreas et al. The READ-BAD Dataset for Baseline Detection in Archival Documents. In: IEEE. 2017 14th IAPR International Conference on Document Analysis and Recognition (ICDAR). [S. l.: s. n.], 2017. P. 138–143. DOI: [10.1109/ICDAR.2017.30](https://doi.org/10.1109/ICDAR.2017.30).
- 54 KUMAR, Surya e WEAVER, John. **AI and Quantum Cryptography: Safeguarding Information Security in a New Era**. [S. l.: s. n.], 2025. Preprint, ResearchGate. DOI: [10.13140/RG.2.2.31275.14887](https://doi.org/10.13140/RG.2.2.31275.14887). Disponível em: <https://www.researchgate.net/publication/389319105>.
- 55 LI, Minghao et al. TrOCR: Transformer-based Optical Character Recognition with Pre-trained Models. **arXiv preprint**, arXiv:2109.10282, 2021. Disponível em: <https://arxiv.org/abs/2109.10282>.
- 56 LI, Tian et al. Federated Optimization in Heterogeneous Networks. In: PROCEEDINGS of Machine Learning and Systems 2020 (MLSys 2020). [S. l.: s. n.], 2020. P. 429–450. Disponível em: <https://proceedings.mlsys.org/paper/2020/file/38c5ce64d64e1d1d9a54f3f7da0b0c8e-Paper.pdf>.
- 57 LI, Yang et al. UltraFlwr—An Efficient Federated Medical and Surgical Object Detection Framework. **arXiv preprint arXiv:2503.15161**, 2025.
- 58 LI, Z.; LIN, W.; ZOU, J. et al. Shepherd: A Platform for Efficient Federated Pre-training of Large Language Models. In: ACM. PROCEEDINGS of the ACM Symposium on Operating Systems Principles. [S. l.: s. n.], 2025.
- 59 LIANG, Xu et al. PKLNet: Keypoint Localization Neural Network for Touchless Palmprint Recognition Based on Edge-Aware Regression. **IEEE Journal of Selected Topics in Signal Processing**, v. 17, n. 3, p. 662–676, 2023. DOI: [10.1109/JSTSP.2023.3241540](https://doi.org/10.1109/JSTSP.2023.3241540).
- 60 MADHAVAN, Arjun; PATEL, Kiran e WONG, Daniel. BioZero: Decentralized Biometric Authentication with Zero-Knowledge Proofs and Blockchain. **arXiv preprint arXiv:2409.17509**, 2024.
- 61 MARTI, U-V e BUNKE, Horst. The IAM-database: an English sentence database for offline handwriting recognition. **International Journal on Document Analysis and Recognition**, Springer, v. 5, n. 1, p. 39–46, 2002. DOI: [10.1007/s100320200071](https://doi.org/10.1007/s100320200071).
- 62 MCDONALD, Graham; MACDONALD, Craig e OUNIS, Iadh. How the accuracy and confidence of sensitivity classification affects digital sensitivity review. **ACM Transactions on Information Systems (TOIS)**, v. 39, n. 1, p. 1–34, 2020.
- 63 MCMAHAN, H. Brendan et al. Communication-Efficient Learning of Deep Networks from Decentralized Data. In: PROCEEDINGS of the 20th International Conference on Artificial Intelligence and Statistics (AISTATS). [S. l.: s. n.], 2017. P. 1273–1282. Disponível em: <https://arxiv.org/abs/1602.05629>.
- 64 MUNOZ-HERNANDEZ, Mario Diego; MORALES-SANDOVAL, Miguel e GARCIA-HERNANDEZ, Jose Juan. An end-to-end security approach for digital document management. **The Computer Journal**, British Computer Society, v. 59, n. 7, p. 1076–1090, 2016.
- 65 MURUGAN, R. et al. AI-Powered OCR for Handwritten Documents with Low Quality and Degradation. **MSRDG International Journal of Computer Science and Technology in Engineering**, v. 11, n. 2, 2025. Disponível em: <https://msrdginternationaljournal.com/doc/MSRDG-IJCSTEE-V112P102.pdf>.
- 66 MUSGRAVE, Kevin; BELONGIE, Serge J. e LIM, Ser-Nam. PyTorch Metric Learning. **arXiv preprint**, abs/2008.09164, 2020. Disponível em: <https://arxiv.org/abs/2008.09164>.
- 67 NIST. **FIPS PUB 197: Advanced Encryption Standard (AES)**. [S. l.: s. n.], nov. 2001. U.S. Department of Commerce. Disponível em: <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf>. Acesso em: 8 ago. 2025.

- 68 NIST. **Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC**. [S. l.: s. n.], 2007. SP 800-38D.
- 69 NOCKELS, J. **Making the past readable: a study of the impact of handwritten text recognition (HTR) on libraries and their users**. [S. l.: s. n.], 2025. Doctoral dissertation, University of Edinburgh. DOI: [10.7488/era/5988](https://doi.org/10.7488/era/5988).
- 70 Ó RAGHALLAIGH, Brian; PALANDRI, Andrea e MAC CÁRTHAIGH, Críostóir. Handwritten Text Recognition (HTR) for Irish-Language Folklore. In: PROCEEDINGS of the 4th Celtic Language Technology Workshop within LREC2022. Marseille, France: European Language Resources Association, jun. 2022. P. 121–126.
- 71 OECD. **Blockchain’s Unchained: Blockchain Technology and Its Use in the Public Sector**. Paris, France: [s. n.], 2018. https://www.oecd.org/content/dam/oecd/en/publications/reports/2018/06/blockchains-unchained_fc5d568f/3c32c429-en.pdf. Acesso em: 8 ago. 2025.
- 72 _____. **OECD Principles on Artificial Intelligence**. [S. l.: s. n.], 2019. <https://oecd.ai/en/ai-principles>. Acesso em: 8 ago. 2025.
- 73 _____. **Going Digital Guide to Data Governance Policy Making**. Paris, França: [s. n.], 2022. https://www.oecd.org/en/publications/going-digital-guide-to-data-governance-policy-making_40d53904-en.html. Acesso em: 8 ago. 2025.
- 74 _____. **Going Digital to Advance Data Governance for Growth and Well-being**. Paris, França: [s. n.], 2022. https://www.oecd.org/en/publications/going-digital-to-advance-data-governance-for-growth-and-well-being_e3d783b0-en.html. OECD Digital Economy Papers, No. 339. DOI: [10.1787/e3d783b0-en](https://doi.org/10.1787/e3d783b0-en). Acesso em: 8 ago. 2025.
- 75 _____. **OECD Recommendation on Enhancing Access to and Sharing of Data**. Paris: [s. n.], 2022. OECD. Aprovada em 15 de junho de 2021 e publicada em 2022. Disponível em: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0463>.
- 76 _____. **Privacy and Data Protection**. [S. l.: s. n.], 2023. <https://www.oecd.org/en/topics/privacy-and-data-protection.html>. Acesso em: 8 ago. 2025.
- 77 _____. **2023 OECD Digital Government Index: Results and Key Findings**. Paris: [s. n.], 2024. OECD Public Governance Policy Papers, No. 44, OECD Publishing. DOI: [10.1787/1a89ed5e-en](https://doi.org/10.1787/1a89ed5e-en). Disponível em: <https://doi.org/10.1787/1a89ed5e-en>. Acesso em: 8 ago. 2025.
- 78 OPENMMLAB. **MMOCR: OpenMMLab Text Detection, Recognition and Understanding Toolbox**. [S. l.: s. n.], 2020. GitHub repository. Disponível em: <https://github.com/open-mmlab/mmlab/mocr>. Acesso em: 8 ago. 2025.
- 79 _____. **MMPose: OpenMMLab Pose Estimation Toolbox and Benchmark**. [S. l.: s. n.], 2020. <https://github.com/open-mmlab/mmpose>. Acesso em: 8 ago. 2025.
- 80 OSTEC. Provas de conhecimento zero e sua aplicação em autenticação segura. **Blog Ostec**, 2023. Acesso em: 8 ago. 2025.
- 81 OTTO, Mark e THORNTON, Jacob. **Bootstrap 5: The world’s most popular framework for building responsive, mobile-first sites**. [S. l.: s. n.], 2021. <https://getbootstrap.com/>. Acesso em: 8 ago. 2025.
- 82 PASZKE, Adam et al. PyTorch: An Imperative Style, High-Performance Deep Learning Library. **Advances in Neural Information Processing Systems**, v. 32, 2019. Disponível em: <https://pytorch.org/>.
- 83 PERDIKI, E. **List of manuscripts containing John Chrysostom’s Homilies and the relevant manual transcriptions**. Versão 1.2. [S. l.]: Zenodo, fev. 2023. DOI: [10.5281/ZENODO.7681132](https://doi.org/10.5281/ZENODO.7681132).
- 84 PYTHON CRYPTOGRAPHIC AUTHORITY. **Cryptography**. [S. l.: s. n.], 2024. Python library which provides cryptographic recipes and primitives. Disponível em: <https://cryptography.io/>. Acesso em: 15 jan. 2025.

- 85 RADFORD, Alec et al. Learning transferable visual models from natural language supervision. In: PMLR. INTERNATIONAL conference on machine learning. [S. l.: s. n.], 2021. P. 8748–8763.
- 86 RAMÍREZ, Sebastián. **FastAPI**. [S. l.: s. n.]. GitHub repository. Disponível em: <<https://github.com/tiangolo/fastapi>>. Acesso em: 8 ago. 2025.
- 87 ON-RCPN. **Cartilha de Boas Práticas para o Uso Responsável, Equitativo e Ético da Inteligência Artificial no Registro Civil Brasileiro**. 1. ed. [S. l.], abr. 2025. Disponível em: <https://onrcpn.org.br/IA/>. Disponível em: <<https://onrcpn.org.br/wp-content/uploads/2025/04/ON-RCPN-Cartilha-IA-3.pdf>>. Acesso em: 8 ago. 2025.
- 88 REUL, Christian et al. OCR4allAn open-source tool providing a (semi-) automatic OCR workflow for historical printings. **Applied Sciences**, MDPI, v. 9, n. 22, p. 4853, 2019.
- 89 ROGERS, Anna; KOVALEVA, Olga e RUMSHISKY, Anna. A primer in BERTology: What we know about how BERT works. **Transactions of the Association for Computational Linguistics**, v. 8, p. 842–866, 2020.
- 90 RUPA, Ch e MIDHUNCHAKKARAVARTHY, Divya. Preserve security to medical evidences using blockchain technology. In: IEEE. 2020 4th international conference on intelligent computing and control systems (ICICCS). [S. l.: s. n.], 2020. P. 438–443.
- 91 SÁNCHEZ, Joan Andreu et al. ICFHR2014 Competition on Handwritten Text Recognition on the Bentham Collection. In: IEEE. 2014 14th International Conference on Frontiers in Handwriting Recognition. [S. l.: s. n.], 2014. P. 785–790. DOI: [10.1109/ICFHR.2014.137](https://doi.org/10.1109/ICFHR.2014.137).
- 92 SCHROFF, Florian; KALENICHENKO, Dmitry e PHILBIN, James. Facenet: A unified embedding for face recognition and clustering. In: PROCEEDINGS of the IEEE conference on computer vision and pattern recognition. [S. l.: s. n.], 2015. P. 815–823.
- 93 SMITH, Ray. An Overview of the Tesseract OCR Engine. In: PROCEEDINGS of the 9th International Conference on Document Analysis and Recognition (ICDAR). [S. l.: s. n.], 2007. P. 629–633. DOI: [10.1109/ICDAR.2007.4376991](https://doi.org/10.1109/ICDAR.2007.4376991).
- 94 _____. **Tesseract-OCR: An open source optical character recognition engine**. [S. l.: s. n.], 2007. <https://github.com/tesseract-ocr/tesseract>. Acesso em: 8 ago. 2025.
- 95 SU, Le et al. Complete Region of Interest for Unconstrained Palmprint Recognition. **IEEE Transactions on Image Processing**, v. 33, p. 3662–3675, 2024. DOI: [10.1109/TIP.2024.3407666](https://doi.org/10.1109/TIP.2024.3407666).
- 96 TECH4HUMANS. **YOLOv8s-Signature-Detector: modelo de detecção de assinaturas manuscritas**. [S. l.: s. n.], 2025. HuggingFace Model Card. Versão publicada em 4 abr. 2025. Disponível em: <<https://huggingface.co/tech4humans/yolov8s-signature-detector>>.
- 97 TERRAS, Melissa. The role of the library when computers can read: Critically adopting Handwritten Text Recognition (HTR) technologies to support research. In: WHEATLEY, A. e HERVIEUX, S. (Ed.). **The Rise of AI: Implications and Applications of Artificial Intelligence in Academic Libraries**. [S. l.]: ACRL - Association of College & Research Libraries, 2022. P. 137–148.
- 98 UNESCO. **Recommendation concerning the preservation of, and access to, documentary heritage including in digital form**. Paris, França: [s. n.], 2015. <https://unesdoc.unesco.org/ark:/48223/pf0000244286>. Aprovada pela Conferência Geral da UNESCO na sua 38ª sessão, Paris, 17 de novembro de 2015. Acesso em: 8 ago. 2025.
- 99 _____. **Recommendation on the Ethics of Artificial Intelligence**. Paris: [s. n.], 2021. UNESCO. Disponível em: <<https://unesdoc.unesco.org/ark:/48223/pf0000381137>>.
- 100 UNION, European. **Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)**. [S. l.: s. n.], 2016. Official Journal of the European Union, L 119, 4 May 2016. Accessed: 8 Aug. 2025. Disponível em: <<https://eur-lex.europa.eu/eli/reg/2016/679/oj>>.

- 101 UNITED NATIONS STATISTICS DIVISION. **Principles and Recommendations for a Vital Statistics System**. Rev. 3. New York: United Nations, 2014. ISBN 978-92-1-161563-0. Disponível em: <https://unstats.un.org/unsd/demographic-social/Standards-and-Methods/files/Principles_and_Recommendations/CRVS_M11Rev3-E.pdf>.
- 102 VASWANI, Ashish et al. Attention is all you need. In: ADVANCES in neural information processing systems. [S. l.: s. n.], 2017. v. 30.
- 103 WHO. **Improving the Quality and Use of Birth, Death and Cause-of-Death Information: Guidance for a Standards-Based Review of Country Practices**. Geneva: World Health Organization, 2021. <https://apps.who.int/iris/handle/10665/341556>.
- 104 WIGHTMAN, Ross. **PyTorch Image Models**. [S. l.: s. n.], 2019. <https://github.com/rwightman/pytorch-image-models>. DOI: 10.5281/zenodo.4414861.
- 105 WOLF, Thomas et al. **Transformers: State-of-the-Art Natural Language Processing**. [S. l.: s. n.], 2020. eprint: [arXiv:1910.03771](https://arxiv.org/abs/1910.03771). Disponível em: <<https://huggingface.co/transformers>>. Acesso em: 8 ago. 2025.
- 106 YANG, An et al. Qwen3 technical report. **arXiv preprint arXiv:2505.09388**, 2025.
- 107 YU, Cunxi; HOLCOMB, Daniel e CIESIELSKI, Maciej. Reverse engineering of irreducible polynomials in $GF(2^m)$ arithmetic. In: IEEE. DESIGN, Automation & Test in Europe Conference & Exhibition (DATE), 2017. [S. l.: s. n.], 2017. P. 1558–1563.
- 108 YUSUF, Samuel Omokhafa et al. Analyzing the efficiency of AI-powered encryption solutions in safeguarding financial data for SMBs. **World Journal of Advanced Research and Reviews**, World Journal of Advanced Research e Reviews, v. 23, n. 03, p. 2138–2147, 2024. DOI: 10.30574/wjarr.2024.23.3.2753. Disponível em: <<https://wjarr.com/sites/default/files/WJARR-2024-2753.pdf>>.
- 109 ZHANG, H.; HE, C.; SONG, L. et al. FL-CPT: A Federated Learning Framework for Chinese Pre-trained Transformers. **IEEE Transactions on Knowledge and Data Engineering**, IEEE, 2024.
- 110 ZHANG, Lin et al. Towards contactless palmprint recognition: A novel device, a new benchmark, and a collaborative representation based identification approach. **Pattern Recognition**, v. 69, p. 199–212, 2017. ISSN 0031-3203. DOI: 10.1016/j.patcog.2017.04.016. Disponível em: <<https://www.sciencedirect.com/science/article/pii/S0031320317301681>>.
- 111 ZHANG, Yingyi et al. Towards Palmprint Verification On Smartphones. **arXiv preprint**, arXiv:2003.13266, 2020. DOI: 10.48550/arXiv.2003.13266. Disponível em: <<https://arxiv.org/abs/2003.13266>>.