

**ARQUITETURAS DE INTELIGÊNCIA ARTIFICIAL NA DETECÇÃO DE
DESINFORMAÇÃO: UMA ANÁLISE SOBRE O DESENVOLVIMENTO DE
SOFTWARE E O COMBATE ÀS FAKE NEWS**

**ARTIFICIAL INTELLIGENCE ARCHITECTURES IN DETECTING
MISINFORMATION: AN ANALYSIS OF SOFTWARE DEVELOPMENT AND
COMBATING FAKE NEWS**

**ARQUITECTURAS DE INTELIGENCIA ARTIFICIAL PARA LA DETECCIÓN DE
DESINFORMACIÓN: UN ANÁLISIS DEL DESARROLLO DE SOFTWARE Y LA
LUCHA CONTRA LAS NOTICIAS FALSAS**



10.56238/sevened2026.001-014

Felipe Menezes de Abreu

Pós-graduado em Gestão de Tecnologia da Informação

Instituição: Universidade do Estado do Pará (UEPA)

E-mail: felipe.md.abreu@aluno.uepa.br

Elias Ramos Quaresma

Graduando em Engenharia de Software

Instituição: Universidade do Estado do Pará (UEPA)

E-mail: eliasramos.educ@gmail.com

Emerson Leandro da Silva Silva

Graduando em Engenharia de Software

Instituição: Universidade do Estado do Pará (UEPA)

E-mail: emersonleandrodss@gmail.com

Glaucia Nunes de Lima Santos

Graduação em Pedagogia – Universidade Paulista (UNIP);

Graduanda em Engenharia de Software

Instituição: Universidade do Estado do Pará (UEPA)

E-mail: glauciaa.nunes@gmail.com

Maria Joselia Mendes das Chagas

Graduanda em Engenharia de Software

Instituição: Universidade do Estado do Pará

E-mail: Maria.chagas@aluno.uepa.br

Paulo Adriano Maciel da Silva

Graduando em Engenharia de Software

Instituição: Universidade do Estado do Pará

E-mail: Paulo.amdsilva@aluno.uepa.br

Paulo Cristiano Abreu de Jesus

Pós-graduado em Matemática, suas Tecnologias e o Mundo do Trabalho

Instituição: Universidade Federal do Piauí

E-mail: paulo.jesus3547@escola.seduc.pa.gov.br

RESUMO

O presente artigo investiga o papel da Inteligência Artificial (IA) como ferramenta central na identificação e mitigação de notícias falsas (fake news) no ecossistema digital contemporâneo. Através de uma abordagem técnica e metodológica, explora-se como algoritmos de Aprendizado de Máquina (Machine Learning) e Processamento de Linguagem Natural (PLN) são integrados ao ciclo de vida de desenvolvimento de software para criar sistemas de verificação automatizada. A pesquisa aborda desde a engenharia de requisitos para sistemas inteligentes até a implementação de redes neurais profundas, discutindo concomitantemente os desafios éticos e a aplicação de IA nos processos de teste e qualidade de software que sustentam essas plataformas.

Palavras-chave: Inteligência Artificial. Fake News. Engenharia de Software. Processamento de Linguagem Natural. Deep Learning.

ABSTRACT

This article investigates the role of Artificial Intelligence (AI) as a central tool in identifying and mitigating fake news in the contemporary digital ecosystem. Through a technical and methodological approach, it explores how Machine Learning and Natural Language Processing (NLP) algorithms are integrated into the software development lifecycle to create automated verification systems. The research covers everything from requirements engineering for intelligent systems to the implementation of deep neural networks, simultaneously discussing the ethical challenges and the application of AI in the software testing and quality processes that underpin these platforms.

Keywords: Artificial Intelligence. Fake News. Software Engineering. Natural Language Processing. Deep Learning.

RESUMEN

Este artículo investiga el papel de la Inteligencia Artificial (IA) como herramienta clave para identificar y mitigar las noticias falsas en el ecosistema digital contemporáneo. Mediante un enfoque técnico y metodológico, explora cómo los algoritmos de Aprendizaje Automático y Procesamiento del Lenguaje Natural (PLN) se integran en el ciclo de vida del desarrollo de software para crear sistemas de verificación automatizados. La investigación abarca desde la ingeniería de requisitos para sistemas inteligentes hasta la implementación de redes neuronales profundas, analizando simultáneamente los desafíos éticos y la aplicación de la IA en los procesos de prueba y calidad de software que sustentan estas plataformas.

Palabras clave: Inteligencia Artificial. Fake News. Ingeniería de Software. Procesamiento del Lenguaje Natural. Deep Learning.

1 INTRODUÇÃO

A disseminação de desinformação em escala industrial representa um dos maiores desafios à integridade democrática e à saúde pública no século XXI. O fenômeno das fake news, potencializado pela velocidade das redes sociais e pela economia da atenção, ultrapassou a capacidade humana de verificação manual. Neste cenário, a tecnologia deixa de ser apenas um meio de propagação para se tornar a única barreira viável de contenção. A computação, historicamente focada no processamento de dados estruturados, enfrenta agora o desafio de interpretar a semântica, o contexto e a intenção por trás da linguagem humana.

A Inteligência Artificial (IA), especificamente através de subcampos como o *Deep Learning*, emerge como a infraestrutura crítica para esta tarefa. No entanto, a construção de sistemas capazes de distinguir fatos de invenções não é trivial. Ela exige uma reconfiguração dos processos tradicionais de desenvolvimento de software. Conforme apontam pesquisas recentes, a inserção de IA no desenvolvimento não serve apenas para o produto final, mas altera a própria metodologia de engenharia, exigindo novos paradigmas de testes, validação de dados e manutenção de modelos (PRESSMAN, 2021).

O problema central que este estudo ataca é a necessidade de automatizar a verificação de veracidade sem incorrer em censura ou viés algorítmico excessivo. A complexidade reside no fato de que as *fake news* são camaleônicas, adaptando-se rapidamente para evadir filtros simples. Portanto, o software de detecção deve ser evolutivo. A literatura técnica sugere que a aplicação de IA no próprio processo de desenvolvimento, como na geração automática de casos de teste ou na detecção de anomalias no código, é fundamental para garantir a robustez dessas ferramentas (SOMMERVILLE, 2020).

Este artigo propõe-se a analisar essa intersecção: como as arquiteturas de IA são projetadas para detectar desinformação e como as modernas práticas de engenharia de software baseadas em IA sustentam a criação dessas soluções complexas.

2 OBJETIVOS

2.1 OBJETIVO GERAL

Analisar as arquiteturas de Inteligência Artificial utilizadas na detecção de fake news, compreendendo como o desenvolvimento de software orientado a dados e assistido por IA permite a criação de sistemas de verificação robustos e escaláveis.

2.2 OBJETIVOS ESPECÍFICOS

Primeiramente, busca-se mapear as principais técnicas de Processamento de Linguagem Natural (PLN) e Redes Neurais (como BERT e LSTM) aplicadas à análise de veracidade textual e

propagação em redes. Em segundo lugar, pretende-se examinar como a IA é aplicada aos processos de desenvolvimento de software (Engenharia de Software para IA e IA para Engenharia de Software), especificamente na fase de testes e qualidade de dados necessários para treinar detectores de desinformação. Por fim, discutir-se-á as implicações éticas e as limitações técnicas, como o viés algorítmico e a necessidade de explicabilidade (Explainable AI) em sistemas críticos de moderação de conteúdo.

3 METODOLOGIA

A metodologia adotada para este estudo caracteriza-se como uma pesquisa exploratória e descritiva, fundamentada em uma revisão bibliográfica sistemática de fontes publicadas. A natureza do objeto de estudo, algoritmos opacos e fenômenos sociais complexos, exige uma abordagem qualitativa sobre a arquitetura técnica, complementada por uma visão crítica sobre os processos de engenharia.

O levantamento bibliográfico concentrou-se em bases de dados de alto impacto, incluindo IEEE Xplore, ACM Digital Library e repositórios de teses nacionais, cobrindo o período de 2018 a 2024. Este recorte temporal justifica-se pela explosão do uso de arquiteturas *Transformer* (como o GPT e BERT) que revolucionaram tanto a geração quanto a detecção de textos falsos. A seleção dos trabalhos priorizou aqueles que tratavam da interseção entre "Detecção de Desinformação", "Machine Learning" e "Processos de Desenvolvimento de Software".

A análise de dados seguiu a categorização temática. Inicialmente, foram segregados estudos focados puramente na eficácia algorítmica (precisão, recall). Em seguida, foram analisados trabalhos que discutem a engenharia por trás desses modelos, incluindo o uso de IA para otimizar o próprio ciclo de vida do desenvolvimento (SDLC), conforme proposto por autores que investigam a automação de testes e a manutenção de sistemas inteligentes (HARMAN; JIA, 2019). A triangulação dessas fontes permitiu construir uma visão holística que não apenas descreve "o que" a IA faz, mas "como" ela é construída e mantida.

4 REFERENCIAL TEÓRICO

4.1 O ECOSISTEMA DAS FAKE NEWS E A RESPOSTA COMPUTACIONAL

A definição de fake news no contexto computacional vai além da mentira simples; envolve a intenção de enganar e a mimetização de formatos jornalísticos. Segundo Wardle e Derakhshan (2017), a desordem da informação divide-se em desinformação (intencional) e má informação (erro não intencional). Para um algoritmo, essa distinção é sutil e depende de padrões linguísticos e de metadados de rede. A resposta computacional evoluiu de abordagens baseadas em regras (listas negras de sites) para modelos probabilísticos complexos.

A detecção automática opera, fundamentalmente, em três níveis: baseada em conteúdo (análise léxica e semântica), baseada em contexto (análise de propagação na rede social) e híbrida. Nos últimos anos, a predominância de modelos de *Deep Learning* tornou-se absoluta. Redes Neurais Convolucionais (CNNs) e Redes Neurais Recorrentes (RNNs), especialmente as LSTMs (*Long Short-Term Memory*), demonstraram capacidade superior em capturar dependências de longo prazo em textos, essenciais para detectar incoerências narrativas típicas de notícias fabricadas (SHU et al., 2019).

4.2 ARQUITETURAS DE DEEP LEARNING E PROCESSAMENTO DE LINGUAGEM NATURAL

O estado da arte na detecção de fake news reside nos modelos Transformers, como o BERT (Bidirectional Encoder Representations from Transformers). Diferente de modelos anteriores que liam o texto sequencialmente, o BERT analisa a sentença inteira de uma vez, compreendendo o contexto bidirecional das palavras. Estudos de Kaliyar et al. (2020) demonstram que o uso de BERT fine-tuned (ajustado) para bases de dados de fact-checking atinge taxas de precisão superiores a 90%, superando significativamente métodos estatísticos tradicionais como Support Vector Machines (SVM).

Além da análise textual, a IA é aplicada na análise multimodal. Notícias falsas frequentemente utilizam imagens manipuladas ou fora de contexto. Redes adversárias (GANs - *Generative Adversarial Networks*) são utilizadas tanto para criar quanto para detectar *deepfakes*. O desenvolvimento desses sistemas exige um pipeline de dados robusto, onde o pré-processamento (limpeza, tokenização, remoção de *stop words*) consome grande parte do esforço de engenharia. A complexidade dessas arquiteturas impõe desafios severos ao processo de desenvolvimento de software, que precisa gerenciar versões de modelos, e não apenas versões de código.

4.3 INTELIGÊNCIA ARTIFICIAL APLICADA AO PROCESSO DE DESENVOLVIMENTO DE SOFTWARE (AI4SE)

A construção de detectores de fake news não é apenas um problema de ciência de dados, mas um desafio de engenharia de software. Para lidar com a complexidade e a escala desses sistemas, a própria IA tem sido aplicada aos processos de desenvolvimento. Segundo Harman e Jia (2019), a "Engenharia de Software Search-Based" e o uso de aprendizado de máquina para automação de testes são tendências consolidadas. No contexto de detectores de desinformação, a IA auxilia na geração automática de dados de teste (*data augmentation*), criando variações sintéticas de notícias falsas para treinar o modelo, aumentando sua robustez contra ataques adversários.

Outra aplicação crítica da IA no processo de desenvolvimento é a manutenção preditiva do código e a detecção de bugs. Ferramentas baseadas em IA analisam o repositório de código dos detectores para identificar padrões que levam a falhas de desempenho ou vulnerabilidades de

segurança. Amershi et al. (2019), em seus estudos sobre a engenharia de software na Microsoft, destacam que o desenvolvimento de sistemas de IA (Software 2.0) requer um ciclo contínuo de monitoramento e re-treino. A IA é usada para monitorar a "degradação do conceito" (*concept drift*), alertando os desenvolvedores quando o padrão das *fake news* muda e o modelo precisa de atualização, automatizando parte do pipeline de DevOps (MLOps).

5 DISCUSSÃO E ANÁLISE

5.1 A CORRIDA ARMAMENTISTA: GERAÇÃO VS. DETECÇÃO

A análise das tecnologias atuais revela um cenário de "corrida armamentista". Ao mesmo tempo que se desenvolvem IAs para detectar fake news, modelos de geração de linguagem (LLMs) como o GPT-4 podem ser utilizados para produzir desinformação em massa, altamente persuasiva e gramaticalmente correta, dificultando a detecção baseada em sintaxe. Zellers et al. (2019) argumentam que a melhor defesa contra geradores neurais de fake news são discriminadores neurais treinados nos próprios geradores. Isso cria um ciclo recursivo no desenvolvimento de software: o sistema de defesa precisa ser constantemente testado contra o sistema de ataque mais recente, exigindo uma integração contínua (CI/CD) extremamente ágil e automatizada.

5.2 DESAFIOS DE ENGENHARIA: EXPLICABILIDADE E VIÉS

Um ponto crítico na discussão é a "caixa preta" do Deep Learning. Para que um sistema de software seja aceito socialmente como juiz da verdade, ele precisa ser explicável. A área de XAI (Explainable AI) tornou-se um requisito não funcional essencial no desenvolvimento desses sistemas. Não basta o software apontar que uma notícia é falsa; ele deve destacar os trechos suspeitos ou a fonte da inconsistência. A engenharia de software para IA deve, portanto, incorporar interfaces que traduzam pesos matemáticos em justificativas humanas.

Além disso, o viés nos dados de treinamento representa uma falha de "requisitos de software". Se o conjunto de dados usado para treinar a IA contiver um viés político ou racial, o software replicará esse preconceito. Pesquisas de Buolamwini e Gebru (2018) sobre disparidades em sistemas de IA alertam que a falha na curadoria dos dados é uma falha de engenharia tão grave quanto um erro de lógica no código. O processo de desenvolvimento deve incluir etapas rigorosas de auditoria de dados, assistidas por algoritmos de detecção de viés, antes que o modelo entre em produção.

5.3 INFRAESTRUTURA E ESCALABILIDADE

A implementação técnica de detectores de fake news em plataformas como Facebook ou Twitter exige uma infraestrutura de Big Data capaz de processar petabytes de informação em tempo real. Isso remete aos desafios de arquitetura de software distribuída. A IA aplicada à otimização de

recursos em nuvem torna-se vital. Algoritmos preditivos são usados para alocar capacidade de processamento (GPUs/TPUs) dinamicamente, garantindo que o detector funcione durante picos de tráfego (como em eleições) sem colapsar. A eficiência do código, otimizada por compiladores inteligentes, é crucial para a viabilidade econômica desses sistemas.

5.4 DESIGN INCLUSIVO E REGIONALIZAÇÃO DE ALGORITMOS

A eficácia técnica de um modelo de Inteligência Artificial torna-se irrelevante se a interface de entrega não for acessível às populações mais vulneráveis à desinformação. O desenvolvimento de software para combate a *fake news* deve transcender a lógica puramente algorítmica e incorporar elementos de Design de Experiência do Usuário (UX) que considerem o letramento digital e o contexto cultural. Um exemplo paradigmático dessa abordagem é o desenvolvimento do agente "CheckAI", voltado para a região amazônica. Conforme detalham Abreu et al. (2025), a ferramenta foi projetada para operar diretamente no WhatsApp, rompendo barreiras de instalação de novos aplicativos, e utiliza uma *persona* regional que classifica informações falsas como "Potoca" (gíria local).

Essa estratégia de engenharia de software, que alinha processamento de linguagem natural (PLN) com identidade cultural, demonstrou aumentar significativamente a confiança e a adesão de usuários idosos e "imigrantes digitais". O estudo de caso evidencia que a arquitetura do software deve prever não apenas a precisão da checagem, mas também a empatia da resposta. Além disso, o ciclo de desenvolvimento do CheckAI, validado em ambiente de *Hackathon* com testes de estresse reais, reforça a premissa de que soluções de IA para problemas sociais complexos exigem metodologias ágeis que permitam correções rápidas de falhas lógicas (como *loops* de interação) para garantir a estabilidade do serviço em momentos críticos, como crises sanitárias ou eventos climáticos.

6 CONCLUSÃO

A análise aprofundada conduzida ao longo desta investigação permite inferir com segurança que a Inteligência Artificial não se posiciona apenas como um mecanismo de suporte, mas como a pedra angular e, concomitantemente, o desafio mais complexo e multifacetado no enfrentamento da desinformação contemporânea, visto que a mesma potência computacional utilizada para detectar falsidades é frequentemente a base para a sua criação. As arquiteturas modernas, fundamentadas em Deep Learning e, mais especificamente, nos modelos Transformers, comprovaram uma eficácia superior na categorização e classificação de conteúdos enganosos, ultrapassando as limitações biológicas humanas no que tange à velocidade de processamento e à capacidade de analisar volumes massivos de dados em tempo real, permitindo uma varredura semântica e contextual que métodos tradicionais jamais conseguiriam atingir. Entretanto, é imperativo ressaltar que a sofisticação algorítmica por si só é insuficiente se não estiver alicerçada em um processo de desenvolvimento de

software rigoroso e de alta qualidade, pois a eficácia tecnológica depende intrinsecamente da robustez da engenharia que a sustenta.

Fica evidente, diante do exposto, que a construção de detectores de fake news transcende a codificação estática tradicional, exigindo uma mudança de paradigma para um ciclo dinâmico e iterativo de engenharia de dados e aprendizado de máquina, conhecido como MLOps, onde o monitoramento contínuo é vital. A incorporação de técnicas de Inteligência Artificial dentro dos próprios pipelines de desenvolvimento, seja para a automação de testes de estresse, para a geração de dados sintéticos destinados ao treinamento robusto contra cenários adversários ou para a manutenção preditiva da integridade do código, demonstrou ser uma estratégia inalienável para assegurar que os modelos permaneçam relevantes e precisos diante da mutação constante e acelerada das táticas de disseminação de desinformação. Conclui-se, portanto, que o êxito no combate sistêmico às fake news não reside na busca utópica por um "algoritmo mágico" ou uma solução única e definitiva, mas sim na implementação de uma arquitetura de software resiliente, auditável, transparente e escalável, que seja continuamente refinada por práticas avançadas de engenharia, garantindo assim uma resposta tecnológica à altura dos desafios sociais da era digital.

7 CONSIDERAÇÕES FINAIS

As reflexões trazidas por este artigo apontam que estamos entrando em uma era onde a verdade digital é mediada por software. Isso impõe uma responsabilidade ética monumental aos engenheiros de software e cientistas de dados. O futuro da detecção de fake news passará inevitavelmente pela colaboração homem-máquina, onde a IA atua como uma ferramenta de triagem e alerta, mas a decisão final sobre nuances contextuais complexas ainda pode requerer supervisão humana.

7.1 O FUTURO DA AUTENTICAÇÃO DE CONTEÚDO

Uma tendência emergente identificada é a mudança do foco da detecção para a autenticação. Tecnologias de blockchain e criptografia, integradas a sistemas de IA, poderão criar cadeias de custódia digital para notícias, garantindo a proveniência da informação desde a fonte. O desenvolvimento de protocolos padronizados de autenticidade de conteúdo será um campo fértil para a engenharia de software nos próximos anos.

7.2 SOBERANIA ALGORÍTMICA E EDUCAÇÃO

Por fim, é imperativo considerar que a tecnologia, por si só, não resolverá um problema que é fundamentalmente social. A educação para a mídia (media literacy) deve caminhar lado a lado com o desenvolvimento tecnológico. Além disso, o desenvolvimento de soluções nacionais de IA para detecção de fake news é uma questão de soberania, evitando que a moderação do debate público

brasileiro seja realizada exclusivamente por algoritmos "caixa preta" desenvolvidos no exterior. A pesquisa contínua e o investimento em formação de engenheiros de software especializados em IA e ética são os caminhos para um ecossistema informacional mais saudável.

REFERÊNCIAS

- ABREU, Felipe Menezes de et al.** Inteligência Artificial e soberania informacional na Amazônia: o desenvolvimento do agente "CheckAI" como estratégia de combate à desinformação socioambiental rumo à COP 30. **Revista Contemporânea**, v. 5, n. 12, p. 01–14, 2025. DOI: 10.56083/RCV5N12-085. Disponível em: <https://ojs.revistacontemporanea.com/ojs/index.php/home/article/view/9962>. Acesso em: 08 jan. 2026.
- ALLCOTT, Hunt; GENTZKOW, Matthew. **Social media and fake news in the 2016 election**. Journal of Economic Perspectives, v. 31, n. 2, p. 211-236, 2017.
- AMERSHI, Saleema et al. **Software engineering for machine learning: A case study**. In: 2019 IEEE/ACM 41st International Conference on Software Engineering: Software Engineering in Practice (ICSE-SEIP). IEEE, 2019. p. 291-300.
- BONDIO, Rico; SCHMITT, Markus. **Mobile phone addiction and the impact of artificial intelligence in software development**. Journal of Systems and Software, v. 145, p. 1-15, 2019.
- BUOLAMWINI, Joy; GEBRU, Timnit. **Gender shades: Intersectional accuracy disparities in commercial gender classification**. In: Conference on fairness, accountability and transparency. PMLR, 2018. p. 77-91.
- CHOLLET, François. **Deep Learning with Python**. Shelter Island: Manning Publications, 2018.
- GOODFELLOW, Ian et al. **Generative adversarial nets**. Advances in neural information processing systems, v. 27, 2014.
- HARMAN, Mark; JIA, Yue. **Start here: a roadmap for the search based software engineering field**. International Symposium on Search Based Software Engineering. Springer, Cham, 2019.
- KALIYAR, Rohit Kumar et al. **FNDNet – A deep convolutional neural network for fake news detection**. Cognitive Systems Research, v. 61, p. 32-44, 2020.
- LEWIS, James A. **Artificial Intelligence and Software Development: The Future of Coding**. Center for Strategic and International Studies, 2021.
- PRESSMAN, Roger S.; MAXIM, Bruce R. **Engenharia de Software: Uma Abordagem Profissional**. 9. ed. Porto Alegre: AMGH, 2021.
- SHU, Kai et al. **Fake news detection on social media: A data mining perspective**. ACM SIGKDD explorations newsletter, v. 19, n. 1, p. 22-36, 2017.
- SHU, Kai et al. **Defend: Explainable fake news detection**. In: Proceedings of the 25th ACM SIGKDD international conference on knowledge discovery & data mining. 2019. p. 395-405.
- SOMMERVILLE, Ian. **Software Engineering**. 10. ed. Boston: Pearson, 2020.
- VASWANI, Ashish et al. **Attention is all you need**. Advances in neural information processing systems, v. 30, 2017.
- VOSOUGHI, Soroush; ROY, Deb; ARAL, Sinan. **The spread of true and false news online**. Science, v. 359, n. 6380, p. 1146-1151, 2018.

WARDLE, Claire; DERAKHSHAN, Hossein. **Information disorder: Toward an interdisciplinary framework for research and policymaking**. Council of Europe report, v. 27, 2017.

ZELLERS, Rowan et al. **Defending against neural fake news**. Advances in neural information processing systems, v. 32, 2019.