

A IMPORTÂNCIA DO PET DE REDE DA INTEGRIDADE DA INFORMAÇÃO NA SEGURANÇA DIGITAL E NO COMBATE A DESINFORMAÇÃO¹

Autores(as): LEONARDO PEREIRA SILVA, RIQUELME JATAY RIBEIRO SCARCELA
BEZERRA, FABRICIO ELIZIO LIMA DOS SANTOS, GABRIEL FARIAS LEANDRO,
FELIPE RODRIGUES FERRAZ DE ALENCAR, VALDIMIRO ALVES DOS SANTOS
NETO, KAYKY MOREIRA MORAIS;

Tutor(a): FRANCINEIDE AMORIM COSTA SANTOS;

leonardo.pereira@aluno.ufca.edu.br, riquelme.jatay@aluno.ufca.edu.br,
fabricio.elizio@aluno.ufca.edu.br, gabriel.farias@aluno.ufca.edu.br,
ferraz.felipe@aluno.ufca.edu.br, valdimiro.alves@aluno.ufca.edu.br,
kayky.morais@aluno.ufca.edu.br, francineide.amorim@ufca.edu.br.

PET REDE DE INTEGRIDADE DA INFORMAÇÃO/UFCA;
UNIVERSIDADE FEDERAL DO CARIRI (UFCA).

RESUMO: O ambiente digital, apesar de ter ampliado o acesso à informação e o exercício da cidadania, também intensificou desafios sociais e tecnológicos, como a disseminação intencional de desinformação e o aumento de golpes virtuais. Esses problemas evidenciam a necessidade de ações voltadas à formação crítica e à conscientização sobre segurança digital. Nesse contexto, o artigo apresenta as edições II e III da Maratona de Combate à Desinformação, promovidas pelo PET RII/UFCA entre julho e setembro de 2025, que abordaram temas como algoritmos de recomendação, *fake news*, educação midiática e segurança digital. As atividades foram realizadas por meio de *workshops online*, transmitidos no *YouTube*, com dinâmicas interativas e momentos de debate. Os resultados apontaram alto engajamento do público, média de 25 espectadores simultâneos e feedbacks positivos quanto à relevância e clareza das discussões. Além disso, destacaram-se sugestões de novas abordagens, como cibersegurança e impactos das inteligências artificiais generativas. Conclui-se que as ações contribuíram de forma significativa para a promoção da educação midiática e da segurança digital, fortalecendo o pensamento crítico dos participantes diante das vulnerabilidades e riscos do ambiente virtual.

¹ Área de conhecimento: Tecnologia e Inovação

Palavras-chave: Algoritmos de recomendação; Educação Midiática; Golpes Digitais; Redes Sociais;

THE IMPORTANCE OF PETRII IN DIGITAL SECURITY AND COMBATING DISINFORMATION

ABSTRACT : The digital environment, while expanding access to information and citizenship, has also intensified social and technological challenges, such as the intentional spread of disinformation and the rise of online scams. These issues highlight the need for initiatives focused on critical thinking and digital security awareness. In this context, the article presents the 2nd and 3rd editions of the Disinformation Combat Marathon, organized by PET RII/UFCA between July and September 2025, addressing topics such as recommendation algorithms, fake news, media literacy, and digital safety. The activities consisted of online workshops broadcast on YouTube, featuring interactive dynamics and discussions. Results indicated strong audience engagement, with an average of 25 simultaneous viewers and positive feedback regarding the relevance and clarity of the content. Participants also suggested new themes, including cybersecurity and the impacts of generative artificial intelligence. It is concluded that the initiative significantly contributed to promoting media literacy and digital security education, enhancing participants' critical thinking and awareness of digital vulnerabilities.

Keywords: Recommendation algorithms; Media literacy; Digital scams; Social networks;

Introdução

O ambiente digital, embora tenha se consolidado como um espaço essencial para o exercício da cidadania (LUVIZOTTO; SENA, 2022), também propiciou o surgimento de novas problemáticas sociais e tecnológicas. Dentre os desafios decorrentes da democratização digital, destaca-se a desinformação; nesse contexto, o termo pode ser compreendido como o ato de disseminar informações falsas ou tendenciosas intencionalmente, a fim de manipular comportamentos ou percepções individuais e coletivas (PINHEIRO; BRITO, 2014). A literatura indica que a ascensão das redes sociais e suas práticas, como o emprego algoritmos de recomendação, podem potencializar o alcance dessa prática e de agravantes, como o preconceito (DELMAZO; VALENTE, 2018; COSTA, 2025), e suas consequências já se refletem em múltiplos setores, como a saúde pública (REIS *et al.*, 2023).

Ainda nesse contexto de vulnerabilidade digital, outro problema relevante são os golpes virtuais, que englobam práticas nocivas como compras fraudulentas, roubo de dados pessoais e pagamentos indevidos. Esses crimes cibernéticos representam um problema de massa: cerca de um terço da população brasileira afirma ter sido vítima de algum tipo de golpe virtual entre os anos de 2024 e 2025 (BARRA, 2025). Tal panorama evidencia uma

lacuna significativa tanto na segurança digital quanto na formação crítica dos cidadãos frente às ameaças virtuais, e torna-se necessária a tomada de ações para a conscientização social, como defendido por Frasão, Heinrich e Garcia (2025).

Diante do exposto, um dos caminhos mais promissores para enfrentar esses desafios é a educação, por meio da disseminação da educação midiática (GROSSI; LEAL; SILVA, 2021), crucial para capacitar os cidadãos a desenvolverem senso crítico diante das informações que consomem, e a educação para a segurança digital (TÁVORA *et al.*, 2025) como forma de capacitação de indivíduos conscientes perante os riscos do ambiente virtual.

Partindo dessa premissa, esse trabalho tem como objetivo apresentar duas das três edições da **Maratona de Combate à Desinformação**, uma série de intervenções educativas promovidas pelo PET RII/UFCA entre os meses de julho e setembro de 2025, com a finalidade de mitigar os problemas anteriormente discutidos. Nas seções seguintes, serão descritos a metodologia de formulação e execução das ações, os resultados alcançados com sua aplicação e as discussões que emergem dessas experiências.

Método

Essa seção se dedica a abordar como os *workshops* foram executados para abordar os temas de (a) **Algoritmos e Desinformação nas Redes Sociais**, (b) **Golpes Digitais**, (c) **Educação Midiática** e (d) **Segurança Digital na Escola** com o intuito de orientar a população sobre a relevância dessa discussão, bem como formas de se proteger de *fake news* e possíveis fraudes sobretudo com o crescente “fenômeno” dos modelos de linguagem de larga escala (LLMs).

O público alvo das ações foi a população em geral, no caso das ações i e ii, e a comunidade docente e científica, no caso das ações iii e iv. Para o fomento do conteúdo educativo foram utilizadas as plataformas de pesquisa científica SCIELO e *Google Scholar*, buscando sempre trabalhos acadêmicos recentes, visto a atualidade das temáticas, e de respaldo científico, na busca sempre de levar a informação de maneira íntegra e fundamentada para o público alvo.

Os cursos foram ofertados em eventos *online* na plataforma do *YouTube*, através do canal do nosso grupo PET, com o uso do *software OBS*² responsável por estabelecer a transmissão ao vivo de uma sala virtual no *Google Meet*. A divulgação foi realizada através das mídias sociais, além da divulgação pelos meios institucionais. A participação do público ocorreu através do credenciamento na plataforma do *Even3*. O Grupo se dividiu em palestrantes, organizadores e mediadores, para balancear as responsabilidades, sendo o mediador encarregado de fazer a comunicação em tempo real entre o *chat* do *Youtube* e o palestrante, contribuindo para um ambiente de aprendizado dinâmico. No fim de cada apresentação é disponibilizado um formulário, gerado a partir do *Google Forms*, para averiguar os *feedbacks*, possíveis melhorias e registrar a presença.

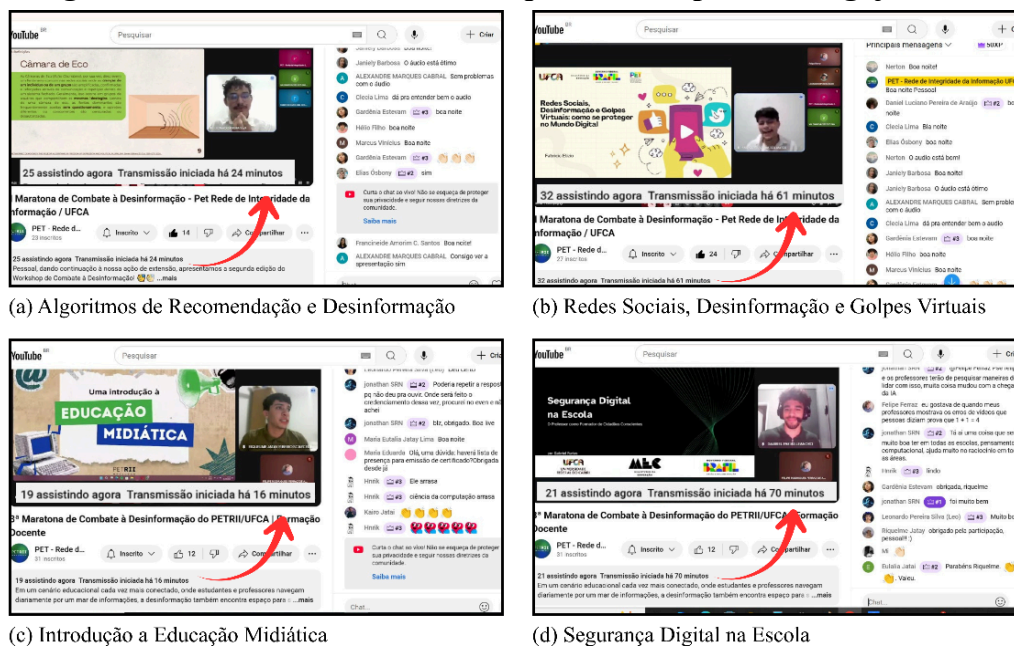
² OBS é um software gratuito e de código aberto para gravar e transmitir vídeos ao vivo pela internet.

Resultados e Discussão

Dentro dos aspectos trabalhados na temática integridade da informação, foram abordados segurança informacional, algoritmos de recomendação, educação midiática, redes sociais, notícias falsas, golpes e segurança digital. Todos esses foram pilares para construção de conhecimento na composição das atividades descritas.

No que diz respeito às *lives* Maratona de combate a Desinformação II e Maratona de Combate a Desinformação III, o engajamento e contato com público foi rico, chegando a um pico de 40 e uma média de 25 espectadores simultâneos, como mostra a Figura 1.

Figura 1 – Transmissão dos *workshops* e seus respectivos engajamentos



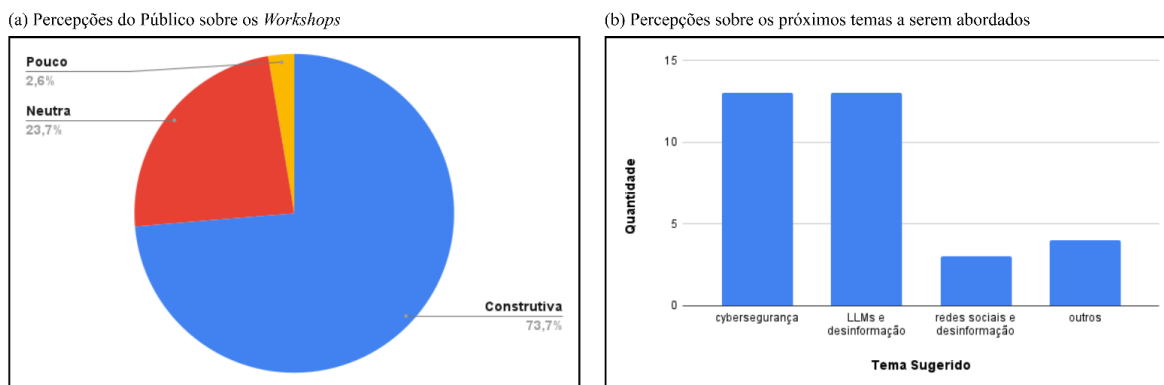
Fonte: produção dos autores.

Em geral, os *feedbacks* recebidos no que diz respeito a qualidade das informações passadas, bem como a pauta foram bem recebidas pelo público alvo que recebeu desde elogios a críticas pertinentes quanto ao tempo de apresentação e capacidade de prender o público. As dinâmicas interativas realizadas durante os momentos, como em (a) mostrando timelines enviesadas ou (b) apresentando uma série de anúncios no intuito de aplicar as orientações ensinadas no respectivo *workshop*, foram ressaltadas como de grande importância por parte do público, sobretudo para garantir a compreensão conteúdo trabalhado. O momento “tira-dúvidas” feito no final de cada apresentação funcionou para construção e fomento, junto com o público, de um conhecimento rico acerca das temáticas trabalhadas, tal momento também foi destacado como proveitoso (Figura 2, a).

Dentre os temas destacados pelos espectadores como bons temas para o grupo abordar no futuro, (Figura 2, b) destacaram-se, cibersegurança e a relação entre LLMs e desinformação, sendo amplamente citados em várias situações, como: cultura hacker,

segurança de senhas e dados privados, segurança relacionada a crianças nas redes sociais, uso de inteligência artificial (IA) para gerar imagens e notícias falsas, uso de IA generativa de texto dentro da academia e como essas LLMs atuais afetam o meio ambiente. Ainda, outros temas importantes mas em menor quantidade, destacaram-se: a Lei Geral de Proteção de Dados, uso excessivo de redes sociais e vício digital.

Figura 2 – Feedback do Público Sobre o Workshop e Próximos Temas



Fonte: produção dos autores.

Conclusões

Conclui-se, portanto, que os *workshops* “Maratona da Desinformação II: Algoritmos de Recomendação e Golpes em Redes Sociais”, “Maratona do Combate a Desinformação III: Educação Midiática, Segurança Digital na Escola e o Papel do Professor” contribuíram satisfatoriamente com a temática integridade da informação, bem como apresentou evidências de melhoria na compreensão do tema por parte do público presente nas ações, haja vista a constante interação e argumentação no chat e as respostas coletadas via formulário. Os espectadores ressaltaram a satisfação e a taxa de participação tem se mantido constante, contribuindo assim para o combate à desinformação. Por fim, espera-se ter mais encontros com resultados também satisfatórios, abordando novos temas, como os sugeridos pelos participantes e ressaltando a importância dos temas já trabalhados.

Agradecimentos

Gostaríamos de agradecer ao Ministério da Educação (MEC) pelo financiamento e apoio para o exercício deste projeto e a manutenção do Grupo PET RII/UFCA. Ademais, somos agradecidos também à Universidade Federal do Cariri (UFCA) pelo suporte institucional e a gratidão a Tutora Francineide Amorim Costa Santos, visto que sua orientação e apoio são os pilares para o sucesso do Grupo PET. Estendemos nosso agradecimento aos palestrantes, organizadores, mediadores e espectadores dos *workshops* realizados, cujo empenho e cooperação foram imprescindíveis para o resultado alcançado.

Referências

ALBERTO, C. Integridade da informação: um novo conceito para o estudo da desinformação.

Revista Comunicação Midiática, v. 19, n. 1, p. 207–226, 2024.

BARRA, H. **Golpes virtuais financeiros afetaram cerca de 56 milhões de brasileiros.**

Disponível em: <<https://11nq.com/w8vUS>>. Acesso em: 19 out. 2025.

COSTA, Anderson Paulo da Fonseca. O ALGORITMO COMO ATOR INVISÍVEL: BOLHAS INFORMACIONAIS, CRENÇAS REFORÇADAS E POLARIZAÇÃO DIGITAL.

OIDLES Observatorio Iberoamericano del Desarrollo Local y la Economía Social, [S. l.], v. 19, n. 39, p. e944, 2025. DOI: 10.51896/oidles.v19i39.944. Disponível em: <<https://11nq.com/XaekT>>.

DELMAZO, C.; VALENTE, J. C. L. Fake news nas redes sociais online: propagação e reações à desinformação em busca de cliques. **Media & Jornalismo**, v. 18, n. 32, p. 155–169, 2018.

FRASÃO, Anderson; HEINRICH, Tiago; GARCIA, Vinicius Fulber. O Cenário Atual de Golpes em Redes Sociais: Uma Revisão da Literatura. **Anais do Computer on the Beach**, v. 16, p. 406-413, 2025.

GROSSI, M. G. R.; LEAL, D. C. C. C.; SILVA, M. F. DA. Educação midiática, cultura digital e as fake news em tempos de pandemia. **Educação em Revista**, v. 22, n. esp2, p. 179–198, 22 dez. 2021.

LUVIZOTTO, C. K.; SENA, K. E. R. Cidadania Digital e tecnologia em rede: entre comunicação, algoritmos e aplicativos cívicos. **Liinc em Revista**, v. 18, n. 2, p. e6070, 19 nov. 2022.

PINHEIRO, M. M. K.; BRITO, V. P. Em busca do significado da desinformação. **DataGramZero**, v. 15, n. 6, 2014.

REIS, J. et al. Desinformação em Plataformas Digitais: Conceitos, Abordagens Tecnológicas e Desafios. In: **Jornada de Atualização em Informática 2023**. [s.l.] Sociedade Brasileira de Computação, 2023.

TÁVORA, C. G. et al. A importância da Educação para golpes e fraudes digitais. **Caderno Pedagógico**, v. 22, n. 11, p. e19837–e19837, 12 set. 2025.