

BOTHA, Johnny; PIETERSE, Heloise. Fake news and deepfakes: A dangerous threat for 21st century information security. In: **ICCWS 2020 15th International Conference on Cyber Warfare and Security. Academic Conferences and publishing limited**. 2020. p. 57.

O trabalho inicia falando sobre as fake news e como elas surgiram há muito tempo em nossa sociedade e como elas apenas se difundiram mais a partir do século passado, com o advento da evolução dos meios de comunicação. Essas notícias falsas foram usadas em contextos de guerra e políticos por muito tempo em mídias grandes e influenciadoras. O autor ainda diz que atualmente as fake news são um grande problema global e tem afetado muitos setores como o político nas eleições dos Estados Unidos em 2016.

De acordo com o texto as deepfakes são a evolução das fake News. Essa tecnologia que surgiu em uma página do reddit tem cada dia mais evoluído e criado vídeos extremamente convincentes de personagens da mídia fazendo e falando coisas que ele não faria oualaria normalmente. Isso pode ser usado para acabar com reputações e identidades dessas pessoas. A exemplo disso há um vídeo muito famoso do Barack Obama feito com deepfake publicado pelo buzzfeed alertando sobre a veracidade do conteúdo presente na internet.

Para identificar fake news e amenizar o problema o autor sugere algumas instituições e aplicações para verificar fatos: Snopes, PolitiFacts, Fact-Check, Channel-4-Fact-Check, Africa-Check. Esses sites podem oferecer passos iniciais para a verificação, porém é necessário ir adiante com algumas outras ferramentas para efetivamente detectar essas notícias falsas. Essas ferramentas usam deep learning para apurar os fatos e as citadas pelo autor são: fake-news-detection-with-deep-learning, Fake-News-Detection, FakeBuster. Todas abertas e divulgadas no GitHub.

Para a detecção de deepfakes o artigo cita duas abordagens: detecção manual e detecção utilizando software. Na detecção manual pode se usar o comportamento de quantidade de vezes que o olho humano pisca em média em uma certa duração de tempo, a predição de como deve ser a angulação da cabeça e do rosto e pode se usar a detecção de algumas imperfeições (artefatos) criados na criação dessas imagens modificadas. Para a detecção baseada em software pode-se usar uma rede neural convolucional pré treinada especializada em reconhecimento de imagens. O foco dessa solução é usar essa rede para a classificação de vídeos em vídeos fakes e reais. Além disso o autor fala sobre a MesoNet, uma solução para ajudar a detectar violações em faces e detectar se houve alguma alteração nelas.

Por fim, o trabalho fala que as deepfakes estão evoluindo cada vez mais e além de imagens

estão conseguindo alterar e criar vozes. Concluindo, assim, que há um perigo iminente das notícias falsas e sua nova ferramenta, o deepfake, para o mundo todo e é necessário continuamente criar métodos e soluções para que esse perigo possa ser amenizado.