Deepfake: a tecnologia que ameaça a verdade. Por Raphael Pinheiro.

A verdade é uma só: todo mundo, um dia, vai ficar com dúvida sobre a autenticidade de uma imagem ou vídeo (Arte digital por Raphael Pinheiro).

A tecnologia *deepfake* tem chamado a atenção de especialistas em segurança cibernética, governos e empresas de mídia, devido ao seu potencial para manipular imagens e vídeos de maneira realista e impactante. De acordo com pesquisas recentes, a tecnologia está sendo utilizada tanto para fins criativos e artísticos, quanto para fins maliciosos, como a disseminação de notícias falsas e a criação de vídeos de intimidade sem autorização.

Mas afinal, o que é realmente *deepfake*? Essa tecnologia é baseada em algoritmos de **inteligência artificial**, especificamente em **redes neurais**, que são treinados com grandes quantidades de dados para imitar a aparência e comportamento humanos. Essa tecnologia foi originada na **matemática computacional**, utilizada para identificar padrões e reconhecê-los no tempo, permitindo a criação desses conteúdos artificiais de maneira eficiente. O resultado, nesse caso, é uma imagem ou vídeo que parece ser de alguém, mas na verdade é algo gerado artificialmente pelo computador, contudo, sem deixar a impressão da artificialidade. No início, essa tecnologia era conhecida como *face-swap* e usada, principalmente, para produzir vídeos divertidos para as redes sociais, nos quais nossos rostos eram colocados em corpos de celebridades, emulando cenas de filmes, shows e outras situações. Atualmente, o *deepfake* é utilizado em diversos setores, incluindo entretenimento, propaganda política e até mesmo em jogos de realidade virtual.

No entanto, como toda tecnologia, o *deepfake* também possui aplicações muito perigosas. A capacidade de criar imagens e vídeos totalmente reais e que parecem enganar o olho humano tem sido amplamente usada para fins escusos. Por exemplo, *fake news*, vídeos manipulados, campanhas de ameaça e muitos outros tipos de conteúdos de má-fé que tentam enganar as pessoas e gerar desinformação. Um exemplo disso é o vídeo falso de Barack Obama, ex-presidente dos Estados Unidos, que foi editado com tais técnicas para aparentar que ele estava falando palavrões e, assim, tentar prejudicar sua imagem.

Com isso, os riscos dessa tecnologia são enormes e crescentes, já que é cada vez mais fácil criar vídeos falsos e difundi-los na internet, justamente por ser um método extremamente acessível e facilmente aplicável. Do usuário mais casual ao *hacker* mais experiente, qualquer pessoa pode usar o *deepfake* para gerar imagens e vídeos reais para fins nefastos.

A possibilidade de se criar notícias falsas e propaganda enganosa ilustradas com provasé apenas a ponta do iceberg, uma vez que o *deepfake* também pode ser usado para ameaçar a privacidade e a segurança das pessoas, especialmente de mulheres, que são mais vulneráveis a ataques, utilizando suas imagens em vídeos de teor erótico. Isso, então, pode ocasionar uma variedade de problemas graves, desde fraudes financeiras até danos à reputação de pessoas, empresas e até mesmo governos.

Um estudo realizado pela **Universidade de Berkeley** apontou que cerca de 75% das pessoas que viram vídeos *deepfakes* não conseguiram identificar que eles eram falsos. Esse resultado reforça a necessidade de conscientização sobre os perigos da tecnologia e de medidas para identificar e impedir seu uso para fins maliciosos.

Infelizmente, até o momento não há soluções simples para evitar o uso malicioso da técnica. Algumas empresas de tecnologia estão trabalhando em soluções para detectar *deepfakes*, mas é uma tarefa difícil, já que os algoritmos estão sempre evoluindo e tornando-se cada vez mais sofisticados.

Para evitar os cenário negativos, algumas medidas de prevenção foram sugeridas para tentar vencer a tecnologia *deepfake*. O compromisso da mídia e da comunidade acadêmica de produzir maior consciência do problema é uma delas. Como alternativa, ferramentas são desenvolvidas com a intenção de detectar e bloquear tais fraudes através de métodos de verificação de autenticidade e identidade. Por fim, a inclusão de técnicas de criptografia e outras camadas de segurança em documentos, áudios e vídeos para entregar um trabalho genuíno e substancialmente seguro ao detentor é também uma tentativa de prevenção que ainda está em desenvolvimento.

No entanto, não podemos esquecer que a tecnologia *deepfake* também pode ser utilizada para fins positivos. Por exemplo, em filmes para criar efeitos especiais mais realistas. Um caso concreto foi o uso no filme **Velozes e Furiosos 7**, onde a tecnologia foi usada para recriar o personagem interpretado por Paul Walker, falecido durante as filmagens. O ator não havia concluído sua parte nas gravações, porém, graças à

tecnologia, puderam usar sua imagem em outro corpo e terminar a história como um tributo.

Em outros âmbitos, a tecnologia é amplamente usada pelo setor educacional, onde contribui para a criação de materiais digitais realistas e interativos. Essa tecnologia também tem sido usada por diversas empresas, por exemplo, para animações de produtos para fins comerciais, em campanhas de marketing, criação de personagens digitais caricaturados para jogos, entre outras aplicações.

De acordo com uma pesquisa da **OpenAI**, a tecnologia *deepfake* está se tornando cada vez mais acessível, o que significa que sua utilização irá aumentar nos próximos anos. Logo, dado o aumento do acesso à tecnologia *deepfake*, não é exagero requer medidas de segurança e regulamentações para evitar seu uso indevido e proteger a sociedade contra a manipulação nociva de imagens e vídeos. É importante estarmos atentos às possibilidades e riscos da tecnologia e usarmos sua força para fins positivos, sem prejudicar a sociedade.

O *deepfake* é uma ferramenta poderosa, mas também é uma faca de dois gumes. Seu potencial para manipular imagens e vídeos de maneira realista é enorme. Ele pode ser usado tanto para fins positivos quanto negativos. Por isso, é importante que governos, empresas e a sociedade em geral estejam atentos aos riscos da técnica e trabalhem juntos a fim de encontrar soluções para evitar seu uso malicioso. A verdade é a chave para uma sociedade saudável e justa e precisamos protegê-la, especialmente no mundo digital, onde nem tudo que parece, é.

A propósito, a imagem que ilustra este artigo foi completamente gerada por uma **inteligência artificial**, através de parâmetros fornecido por mim, e utilizando, dentre outras técnicas, algumas semelhantes ao *deepfake*. Isso assusta, não?

Raphael Pinheiro é escritor, com parte de seus textos traduzidos para espanhol e italiano, e pós-graduado em **Marketing Digital e Comércio Eletrônico**. Possui mais de duas décadas de experiência em tecnologia, tendo passado por importantes instituições públicas e privadas, como a **RIOTUR** e a **Fundação Getúlio Vargas**. Há 17 anos é editor-chefe do Portal da **Academia Brasileira de Letras**, uma das maiores e mais importantes instituições culturais do país. Colabora em sua coluna com a **Pressenza**, agência internacional de notícias com representação em mais de vinte países e com o **Observatório de Comunicação Institucional**.