DR

■ **"DEEPFAKES" É O ABUSO DO MOMENTO NA INTERNET**

Os meandros da manipulação de vídeos

A "Deepfake" é usada para combinar uma fala qualquer a um vídeo já existente e pode ser utilizada para gerar notícias falsas. O resultado final pode enganar até olhares mais atentos

Osvaldo Gonçalves

O termo "fake news" entrou no léxico das pessoas. Já quase ninguém fala em boatos e a zongolagem tornou-se mais sofisticada. Agora, após as notícias falsas, recurso predilecto de alguns políticos e de empresários envolvidos em concorrências desleais, que têm causado muitos problemas sociais, surgiram as "deepfakes", técnica de síntese de imagens ou sons humanos baseada no uso da inteligência artificial.

"Deepfake" é uma siglominização dos termos em inglês "deep learning" (aprendizagem profunda) e "fake" (falso) e é usada para combinar uma fala qualquer a um vídeo já existente e pode ser utilizada para gerar notícias falsas e embustes maliciosos. Também é muito usada na pornografia. Os sites pornográficos estão ultimamente recheados de vídeos nos quais rostos de actrizes e actores porno são trocados pelos de celebridades.

Essa prática ganhou o nome de "upskirting" e o resultado final pode enganar até olhares mais atentos. A 20 de Junho do ano passado, a Primeira-Ministra do Reino Unido, Theresa May, afirmou que isso passou a ser considerado crime. Os criminosos podem ser punidos com até dois anos de cadeia.

Inicialmente, considerava-se "upskirting" como a prática de fazer fotografias não autorizadas sob a saia de uma mulher ou o kilt do homem, capturando uma imagem da área da virilha, roupas íntimas e, às vezes, agenitália. Hoje, o que era visto como uma forma de fetichismo sexual ou voyeurismo ganha novos contornos.

A preocupação das autoridades britânicas resultou da grande utilização da técnica na produção de vídeos pornográficos e na chamada pornografia de vingança, o que levou alguns sites porno a banirem a "deepfake".

"Deepfake" é uma siglominização dos termos em inglês "deep learning" (aprendizagem profunda) e "fake" (falso) e é usada para combinar uma fala qualquer a um vídeo já existente e pode ser utilizada para gerar notícias falsas e embustes maliciosos. Também é muito usada na pornografia. Os sites pornográficos estão ultimamente recheados de vídeos nos quais rostos de actrizes e actores porno são trocados pelos de celebridades

Passado ligado à pornografia

A história remonta a 2017, quando um utilizador do Reddit, sob o pseudónimo "Deepfakes", publicou vários vídeos pornográficos na Internet.

O Reddit é um site de media social, baseado em São Francisco, Califórnia (EUA), em que os utilizadores podem divulgar ligações para conteúdo na Web, para que outros votem nas ligações divulgadas, fazendo com que apareçam de uma forma mais ou menos destacada na sua página inicial.

A coisa chamou a atenção quando Daisy Ridley, actriz de "Star Wars VII – O Despertar da Força", foi usada num vídeo desses e quando Gal Gadot, que interpretou "Mulher-Maravilha", aparece num vídeo falso a fazer sexo com o seu meio-irmão.

Desde então, várias outras pessoas famosas, entre actrizes e políticos, também foram vítimas de "Deepfakes", vídeos que, mesmo sendo desmascarados pouco tempo depois, provando-se que as cenas não eram reais, provocaram danos de alguma forma irreparáveis.

Em sites de streaming, como o Youtube, é fácil encontrar vídeos falsos não pornográficos. Novos aplicativos de manipulação de vídeos e imagens são hoje famosos e são desenvolvidos e disponibilizados por gigantes da Internet.

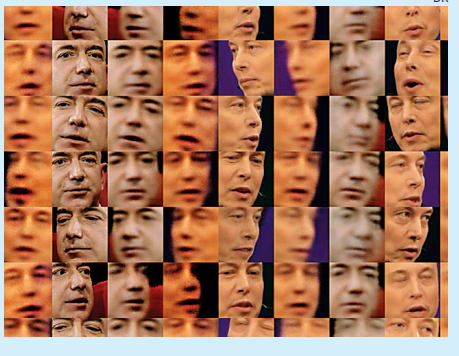
Forma de protecção deste fenómeno

"Deepfakes" só funcionam bem em vídeos que tenham foco num falante e exigem, pelo menos, 40 minutos de dados de entrada, base do treinamento da inteligência artificial do software utilizado. É importante que o falso discurso não seja muito diferente do original.

Até as falsificações serem criadas, os vídeos de base passam por algumas etapas. São *scaneados* para a captação de fonemas e do modelo 3D da parte inferior do rosto dos falantes. Os fonemas são depois combinados com as expressões faciais de cada som. Entendidos afirmam que para as pessoas se protegerem dos "deepfakes, o mais sensato é evitarem a compartilha de vídeos pessoais ou não hospedá-los nas redes sociais de forma pública, o que dificulta o trabalho dos editores.

Por se tratar de uma tecnologia nova, a sociedade, de forma geral, está ainda a ajustar-se às "deepfakes". Porém, o mais aconselhável é que se ande depressa, dando respaldo legal a esse fenómeno.

DR



Até na indústria cinematográfica

A indústria cinematográfica também faz muito recurso às "deepfakes". Cenas de luta, cenários de guerra, etc., são recreados com amplo sucesso. Pesquisadores sugerem que a técnica pode trazer vantagens. Nos filmes, falas equivocadas poderiam ser consertadas, sem ser preciso regravar as cenas por completo.

Em Junho passado, cientistas da Universidade de Stanford, do Instituto Max Planck de Informática, da Universidade de Princeton e da AdobeResearch, nos Estados Unidos, demonstraram como a técnica de "deepfake" se tem tornado cada vez mais acessível e convincente.

Num estudo que envolveu 138 voluntários, cerca de 60 por cento apontaram haver edições nos vídeos falsos, enquanto apenas 80 por cento acertaram nos legítimos. Os pesquisadores alertaram que o facto de os participantes saberem que se tratava de uma pesquisa sobre edição de vídeos pode ter influenciado nas respostas.

APLICATIVO QUE ENVELHECE PESSOAS

FaceApp cria polémica, mas "toma" a Internet

Criado em Janeiro de 2017, pela empresa russa Wireless Lab, o aplicativo passou meses sem chamar a atenção, até que, de um dia para o outro, tomou conta da Internet

Osvaldo Gonçalves

O sucesso repentino do aplicativo FaceApp, aquele que faz as pessoas envelhecerem, levantou grande polémica no mundo inteiro devido à histeria provocada a partir da segunda semana de Julho.

Criado em Janeiro de 2017, pela empresa russa Wireless Lab, o aplicativo passou meses sem chamar a atenção, até que, de um dia para o outro, tomou conta da Internet. Com tal sucesso, surgiram também os alertas, primeiro de especialistas, depois de políticos e, por último,o FaceApp passou a ser investigado pela Polícia.

A principal suspeita é que, com a autorização dos utilizadores, a empresa russa estaria a recolher informações sobre os mesmos e a construir uma enorme base de dados à custa de filtros e outras funcionalidades.

A Wireless Lab foi acusada de partilhar essas informações com os serviços de inteligência russos. A empresa negou-o e garantiu não vender ou parftilhar dados com terceiros e explicou que a maioria das imagens são apagadas dos servidores ao fim de 48 horas. Mas isso não impediu o agravamento das suspeitas, sobretudo, após Chuck Schumer, senador democrata de Nova Iorque, considerar "preocupante" a forma como os dados são tratados e ter pedido ao FBI para investigar, o que, segundo algumas informações, passou a ser feito.

É o fim da privacidade

Ramón López de Mántaras, director do Instituto de Pesquisa de Inteligência Artificial do Centro Superior de Pesquisas Científicas da Espanha, que apoia a proibição do uso de sistemas de reconhecimento facial, na generalidade, afirmou que, nos dias de hoje, entregamos a nossa privacidade de "forma excessivamente frívola e alegre".

Numa entrevista concedida, em Junho, ao jornal espanhol "El País", López de Mántaras afirmou que, com a chegada do 5G e a incorporação de um grande número de dispositivos inteligentes nas residências, será como viver numa casa com paredes de vidro, que permitem que qualquer um do lado de fora veja tudo o que se faz dentro, conheça os nossos movimentos, hábitos e comportamentos.

Ele mencionou os casos de companhias como a Amazon, Google e Apple, que têm funcionários que revisam diariamente conversas aleatórias que os usuários mantêm com os assistentes para melhorar o sistema.

"Ter um monte de objectos e aparelhos em casa ligados à Internet é uma péssima ideia", afirmou, porque "eles podem saber o que você consome, o que compra, quando lava a roupa, o que cozinha, o que come e até coisas tão íntimas como as que ocorrem dentro do banheiro".

O risco de se ter a privacidade violada vem de todos os lados. Utilizadores alegam que os telemóveis, tablets ou computadores portáteis conseguem ouvir conversas privadas e que é possível que os sistemas de reconhecimento de voz estejam activados 24 horas por dia. Eles garantem que, após conversarem sobre determinados assuntos com parentes ou amigos perto dos aparelhos ligados à Internet, no dia seguinte, ou até momentos depois, viram surgir nos feeds de notícias publicidade sobre esses mesmos assuntos.

Especialistas em cybersegurança apontam a existência de uma série de "gatilhos" (palavras-chave) que, quando ditos, accionam dispositivos que levam alguém, algures, a prestar atenção ao que dizemos, sem que, necessariamente, esse alguém seja uma pessoa.

O Google afirma abertamente que usa "gatilhos", o que, dizem, "faz sentido de um ponto de vista de marketing", até porque os seus acordos de uso e a lei permitem-no". Outras grandes companhias do sector negam com veemência o uso desses artifícios, mas tudo indica que possuam milhares de gatilhos, só que, sendo estes criptografados, é muito difícil nos apercebermos da sua existência.

Cuidados

Os cuidados para não termos a nossa privacidade violada vão dos mais simples aos mais complexos, como obrigar as pessoas a frequentarem cursos de iniciação para utilizadores da Internet. Mas, algumas medidas são demasiado básicas e começam pela necessidade de ler os acordos sempre, antes de aceder aos aplicativos.

Mas, tal como acontece com a maioria dos serviços, quase ninguém lê esses acordos. Adere simplesmente e, dessa forma, abre a porta para que a sua vida seja monitorizada.

Origem da polémica

Toda a polémica à volta do FaceApp terá sido causada por um programador da Virgínia, que, tarde da noite, publicou no Twitter uma nota em que expressava a sua revolta contra tal aplicativo, por, alegadamente, lhe ter roubado todas as fotos do celular sem autorização. A denúncia veio reforçar a percepção geral sobre a invasão de privacidade que vimos sendo alvo das mais variadas formas, sob o pretexto da melhoria das condições de vida e da segurança.

A principal suspeita é que, com a autorização dos utilizadores, a empresa russa estaria a recolher informações sobre os mesmos e a construir uma enorme base de dados à custa de filtros e outras funcionalidades

Analistas apontam duas realidades que terão feito disparar os alarmes em relação a esse aplicativo, que emprega um sistema neuronal baseado na inteligência artificial, que analisa a fotografia para conseguir os efeitos desejados, envelhecer ou rejuvenescer o protagonista com um realismo surpreendente: primeiro, os servidores encontram-se na Rússia; segundo, a política de privacidade é demasiado vaga.

Esta não é a primeira grande polémica à volta do FaceApp. Em Agosto de 2017, o aplicativo introduziu um filtro "racial", que permitia pessoas mudarem a cor da pele. A maka foi tanta que a empresa acabou por retirá-lo, deixando apenas que estas vissem a si mesmas mais velhas ou mais novas.

"Made in" Rússia

Apesar de toda a polémica, os utilizadores da Internet continuaram a brincadeira, demonstração de que gostaram de se ver mais velhas e a coisa tornou-se ainda mais "viral", quando o aplicativo passou a ser usado com fotos de celebridades.

Alguns analistas referiram que toda a polémica não inibiria as pessoas e que, se estas deixassem de usar o FaceApp, passariam a usar outro aplicativo similar. Quando em causa está a privacidade, afirmaram, o problema não está apenas na origem do produto, pois tal foi apenas o abrir de uma janela a um cenário onde a privacidade dos utilizadores é a última prioridade.

A pânico gerado à volta do FaceApp deveu-se, sobretudo, ao facto de ser de origem russa, quando, de facto, é da China que provêm os maiores apps de sucesso nos países ocidentais.

O editor do site CNet, RyCrist, afirmou, a propósito, que o aplicativo FaceApp veio, uma vez mais, demonstrar não estarmos preparados para lidar com os desafios relativos à privacidade na Internet.

Para aquele editor, é incrível como as pessoas estão totalmente despreocupadas sobre os poderes que dão aos criadores do aplicativo, não apenas por ser russa, mas pela facilidade com que permitimos que as nossas informações vão parar às mãos de uma empresa praticamente desconhecida da população.

Big brother entre nós

Num cenário hipotético, mas funcional, os clientes não precisariam de sair de casa para ir às compras, pois os frigoríficos, ligados à Internet, comunicariam aos fornecedores quando o stock de determinado produto está no fim e, sendo tudo processado por criptomoedas, as nossas contas seriam pagas imediatamente.

O mesmo aconteceria com outros aparelhos e serviços básicos, como o fornecimento e consumo de água e electricidade, pelo que seriam dispensáveis as torneiras e os interruptores. Até as nossas casas passariam a "reconhecer-nos", franqueando as portas para entrarmos e trancando-as depois disso ou quando saíssemos para trabalhar.

Só que, pelo facto de grande parte dos acidentes ocorrerem nos domicílios, seria necessário que alguém estivesse permanentemente de olho em nós, uma espécie de "grande irmão" (big brother). Seria o mesmo que atirar pela janela o mínimo de privacidade que ainda julgamos deter.