INTERNET

A *FaceApp* voltou. Os riscos são os mesmos?

Há um ano, a *FaceApp* tornou-se conhecida por mostrar como ficariam os utilizadores quando forem mais velhos. Os problemas com a segurança surgiram quase imediatamente. Agora, a aplicação voltou aos tops, mas a forma como usa os dados parece ter mudado.

Inês Chaíça
19 de Junho de 2020, 20:30 actualizado a 21 de Junho de 2020, 15:53

Começou com uma brincadeira nas redes sociais: ver como ficariam os políticos se tivessem nascido com características de outro género. E assim voltou a *FaceApp*, aplicação que permite manipular imagens de forma a alterar a aparência dos utilizadores – tornando-os mais velhos ou mudando o género. E se nada disto te parece estranho é porque a aplicação já teve um pico de popularidade, no ano passado — envolto em dúvidas sobre a segurança dos dados dos utilizadores.

Desta vez, o que despertou a curiosidade dos utilizadores não foi perceber como seriam uns anos mais velhos, como aconteceu em 2019, mas outra funcionalidade: a de mudança de género, que já existia no ano passado, mas que foi melhorada agora. O salto qualitativo

é óbvio: "**As fotografias da *FaceApp* mais recentes são excelentes.** São altamente convincentes", considera Mário Figueiredo, professor catedrático no Instituto Superior Técnico e especialista em *machine learning,* ao P3. Mas mantêm-se os problemas do passado?

Em 2019, e apesar do seu êxito quase instantâneo, a aplicação causou apreensão junto de utilizadores e especialistas. Afinal, a empresa que desenvolveu a aplicação, a russa Wireless Lab, estava a recolher as informações dos utilizadores e a construir uma base de dados à custa dos filtros que oferecia. Recolhia informações do histórico de navegação do *browser*, cliques e identificadores de dispositivo, que depois podiam ser partilhados com terceiros.

Agora, três anos volvidos desde a sua criação, a *FaceApp* volta a estar no top dos *downloads* da PlayStore (para Android) e App Store (da Apple), onde é disponibilizada de forma gratuita. A sua política de privacidade sofreu pelo menos três alterações nos últimos seis meses: a 10 de Dezembro de 2019, a 10 de Janeiro e a última a 4 de Junho, com alterações de peso desde o ano passado.

Fotos (já) não são guardadas, mas *app* recolhe informação

Por exemplo, em Agosto de 2019, a política de privacidade da empresa disponível *online* admitia que as fotografias alteradas eram guardadas (sem especificar onde) e que a aplicação podia usar "*cookies* e tecnologias semelhantes" para recolher informação sobre como cada utilizador usa a aplicação. Cada dispositivo (como telemóvel ou *tablet*) que o utilizador usasse para aceder à aplicação tinha um "identificador" próprio com o objectivo de "melhorar, testar e monitorizar a eficácia" do serviço.

Em 2020, algumas coisas mudaram: entre elas, a garantia de que todas as fotografias ficam apenas guardadas durante um período máximo de 48 horas, após o qual são apagadas. "Não usamos as fotografias que nos dás quando usas a *app* para outra coisa que não dar-te a funcionalidade de edição", lê-se na política de privacidade.

"A tecnologia IA [Inteligência Artificial] que usamos nos nossos filtros requer cálculos avançados num servidor, o que torna impossível editar a fotografia num smartphone", explica a empresa, em resposta ao PÚBLICO. As fotografias que não forem editadas não são enviadas para os servidores – e as editadas são guardadas temporariamente de forma "totalmente anónima" e "encriptada", garante a empresa. "Não podemos identificar-te, ao teu dispositivo ou qualquer outro tipo de dados com base nas fotografias. Não as usamos para publicidade nem outros usos públicos."

DR

Como deixar de ver os mesmos anúncios em toda a Internet?

"Ninguém vê essas fotografias" processadas apenas por computadores, salvaguarda a FaceApp. A aplicação diz ainda não ter acesso a dados como "endereços de e-mail, Apple ID ou contas do Google".

"Não me pareceu haver nada de muito preocupante" nas políticas de privacidade da empresa, afirma Mário Figueiredo. "Estamos sempre à mercê do facto de quererem manter uma boa reputação. Se começarem a haver muitas queixas má utilização dos dados, pode correr mal para eles e, por isso, têm interesse em manter uma boa reputação — o que não quer dizer que não usem os dados para outras coisas, nomeadamente publicidade."

Essa continua a ser uma possibilidade e, apesar de a empresa escrever que "não vende informação pessoal", também admite que pode partilhar os dados do utilizador de forma "anónima, agregada e desidentificada" com terceiros para fins comerciais. "Há aqui uma

máxima muito simples que as pessoas devem ter em mente. Se estou a utilizar uma coisa e não estou a pagar por ela, é porque das duas uma: ou eu sou o produto, e isso pode significar que estão a vender a minha atenção, por exemplo, para mostrar publicidade (o produto que está a ser vendido é o meu tempo); ou então são os meus dados", coloca o professor do IST.

Os dados que a empresa afirma recolher não preocupam o investigador: "Aparentemente eles não recolhem muitos dados pessoais a não ser coisas como onde é que eu estou, que tipo de dispositivo usei, que tipo de *browser,* que página *web* visitei antes do *site* deles. Parece uma coisa relativamente *standard*", classifica. Mas hesita em considerar a aplicação completamente segura: **"Não meto as minhas mãos no fogo por ela."**

Apesar disso, há aplicações que considera mais perigosas, como a *ClearView*, usada por várias forças de segurança nos EUA e Austrália e que consegue identificar qualquer pessoa com base numa pesquisa *online*. "Não é só fazer uma pesquisa por conteúdo, como se faz no Google Images, é [um *software*] dedicado a encontrar caras e consegue encontrar imagens identificadas daquela pessoa pela Internet", explica Mário Figueiredo.

Como se melhora esta aplicação?

A verdade é que a aplicação *FaceApp* continua a somar *downloads* e as pessoas que a usam obtêm resultados que consideram realistas. O aumento de qualidade das manipulações pode ser explicado pela conjunção de três factores: melhorias nos algoritmos usados pela aplicação, no desempenho do *hardware* e das bases de dados.

Mário Figueiredo admite não conhecer exactamente as bases de dados da *app*, mas o processo para as recolher acaba por ser transversal a outras aplicações do género: quando uma empresa começa a ter sucesso, atrai clientes e **quantos mais utilizadores tiver, maior a sua base de dados.** A partir daí, "melhoram cada vez mais".

Aumenta "não só a quantidade de dados que eles podem usar para treinar os modelos", mas também recolhem *feedback* sobre a qualidade do sistema: "Conseguem saber quando a pessoa que fez uma transformação ficou ou não satisfeita, se guardou a imagem, se tenta fazer outra", explica o professor. E isso faz com que consigam melhorar cada vez mais.

Deepfakes: o perigo é real?

Mário Figueiredo é peremptório: a *FaceApp* é ainda muito limitada no tipo de manipulações de imagem que faz. "Não faz coisas como pegar na imagem de numa pessoa e pô-la noutro sítio, nem ao lado de outra com a qual ela nunca esteve, de forma convincente", classifica. Por isso será difícil fazerem vídeos falsos com resultados credíveis, como acontece com os *deepfakes*.

A *FaceApp* dedica-se a modificar a imagem dos utilizadores, mas apenas com base em imagens estáticas da cara. Algo que já era possível fazer antes, em *softwares* dedicados à manipulação de imagem, como o Photoshop, mas "a diferença é que a *FaceApp* permite

que qualquer amador o faça em segundos, sem saber nada": **“Ela não muda radicalmente aquilo que é possível, [apenas] o democratiza brutalmente.”**

A criação de vídeos pode ser o próximo passo para a aplicação, mas neste momento é “um salto muito grande e que não vai acontecer amanhã ou daqui a seis meses”, classifica o professor catedrático. “É duas ordens de grandeza mais difíceis”, não só pela quantidade de dados processados (que é muito superior no caso dos vídeos), mas também porque “os seres humanos são extremamente sensíveis a erros de movimento e de *timings* em vídeos”. Somos muito sensíveis a movimentos pouco naturais”, realça. Por isso, é “mais difícil criar um vídeo que pareça natural do que criar imagens paradas” – e, especialmente, quando o objectivo é fazer com que se mantenham parecenças suficientes com o vídeo original.

Sobre o futuro dos resultados destas aplicações, é ainda mais difícil fazer projecções. Um destino óbvio é o entretenimento porque “não é novo, misturar actores virtuais e reais”. Mas, neste momento, só há uma que dá como certa: “As previsões são quase garantidamente erradas, há sempre alguma coisa que nos surpreende.”

Notícia actualizada às 15h53 do dia 21 de Junho com a resposta da empresa.