

O que o #10yearschallenge tem a ver com a sua privacidade?

O Brasil de Fato consultou especialistas sobre os riscos de compartilhamento de dados pessoais na internet

Lu Sudré

Brasil de Fato | São Paulo (SP), 19 de Janeiro de 2019 às 07:52

COMPARTILHE



O "desafio dos 10 anos" trouxe à tona discussão sobre segurança e privacidade de dados na internet / (Foto: David McnewAFP)

Qualquer pessoa que utiliza redes sociais já percebeu que, seja no Facebook, Instagram ou Twitter, a #10yearschallenge (o desafio dos dez anos) está fazendo sucesso. Nos últimos dias, o desafio que estimula usuários a postarem fotos antigas, de dez anos atrás, ao lado de imagens atuais, se popularizou em diversos países, incluindo o Brasil.

Apesar de aparentar ser uma brincadeira inocente, o desafio trouxe à tona a discussão sobre segurança e privacidade de dados na internet. Tudo começou quando Kate O'Neill, especialista em tecnologia e empreendedora, **fez uma publicação no Twitter** questionando o que a exposição poderia gerar para os próprios usuários.

"Eu há dez anos: provavelmente teria entrado na brincadeira e postado minhas fotos no Facebook e Instagram. Eu hoje: penso em como todos esses dados podem ser usados para treinar algoritmos de reconhecimento facial a reconhecer o envelhecimento e sua progressão", escreveu O'Neill. Com grande repercussão na rede, a mensagem dividiu opiniões.

Para o sociólogo **Sérgio Amadeu**, conselheiro do **Comitê Gestor da Internet (CGI)**, de fato é preciso tomar cuidado com as informações pessoais expostas na internet.

"Atualmente, os dados pessoais valem muito. São utilizados para organizar os perfis de consumidores, descobrir a opinião e as tendências comportamentais dos cidadãos e modular comportamentos. Mesmo que tenha surgido como brincadeira, a postagem de suas fotos antigas geram mais dados sobre você. Podem ajudar os algoritmos de aprendizagem de máquina (*machine learning*) a aperfeiçoar o reconhecimento facial das pessoas, inclusive as projeções de envelhecimento", argumenta Amadeu.

Gustavo Gus, um dos organizadores da **Cryptorave** (evento anual de atividades sobre segurança, criptografia, privacidade e liberdade na rede), explica que a ideia da técnica *machine learning* é observar padrões e educar programas a reconhecê-los

com o objetivo de oferecer publicidade e produtos para público segmentados, uma tendência da indústria tecnológica que se consolidou. No caso do “desafio dos 10 anos”, empresas privadas poderiam identificar processos de envelhecimento ou até mesmo realizar uma setorização em faixas etárias para direcionar ofertas de mercadorias diversificadas.

Ele ressalta que, além do uso dos dados sem autorização, não há transparência nas ações. “É um mistério, uma caixa preta. Todas as semanas temos notícias de vazamento de dados, monstruosos, gigantescos. Não sabemos como esses dados estão sendo armazenados, para quê estão sendo utilizados”, afirma Gus, em tom crítico a grandes empresas como Facebook, Instagram e Twitter.

“Tudo é de graça. Você pode publicar vídeo, publicar matéria, se conectar aos seus amigos e etc. Porque tudo é de graça? Como eles mantêm esse império todo? Como mantêm 1 bilhão de usuários em uma rede social? Vendendo dados e perfis das pessoas ou ainda procurando palavras chaves ou comportamentos que se tenha na rede social”, responde o integrante do **Tor Project**, organização responsável por manter um software livre e de código aberto de forma anônima.

O próprio funcionamento das redes sociais incentiva a exposição, sem uma devida proteção aos nossos dados. Gus cita, por exemplo, que ao marcar outras pessoas em fotos ou fazer “check-in” (marcar sua localização em alguma das plataformas) em lugares visitados, também é uma forma de disponibilizar informações da sua vida pessoal na rede, sem saber quem pode utilizá-las.

Apesar da #10yearschallenge ter se propagado no Facebook, a empresa negou envolvimento ou interesse no “meme”. Contudo, Bia Barbosa, do coletivo **Intervozes**, afirma que de qualquer forma, as fotos postadas na plataforma são utilizadas para desenvolver os algoritmos de reconhecimento facial, mesmo que o recurso não esteja habilitado no perfil de cada indivíduo. Pelos critérios da rede social, as imagens estão submetidas a esse tipo de tratamento.

“É óbvio que mesmo que não tenha sido a empresa a responsável por promover a brincadeira da *hashtag* para incentivar os seus usuários a colocar essas fotos de 10 anos atrás no ar, essa fotos que vão ser postadas e vão passar a fazer parte desse enorme e gigantesco banco de dados do Facebook. E sim, como todas as outras fotos que estão sendo publicadas, serão usadas no desenvolvimento desses algoritmos de reconhecimento facial”, sustenta Barbosa.

Brincadeiras e testes que recebemos nas redes sociais, como por exemplo, responder aos questionamentos: “Qual personagem de filme que mais se parece com você?” ou “Qual alimento mais combina com você?”, também foram desenvolvidas para coletar dados.

“Ao aceitar fazer essas brincadeiras, se acaba dando a essas empresas que desenvolveram aplicativos, acesso a todas as suas fotos. Elas coletam as imagens e as tratam (autorizadas pelo cidadão, mas por muitas vezes, mediante a uma autorização desinformada). As pessoas fazem isso sem saber que tipo de consequência esse tratamento e essa análise de imagem pode ter para sua privacidade e para seus direitos”, alerta a integrante do Intervozes.

Vigilância constante

O controle por meio da divulgação de dados não autorizada e de reconhecimento facial estão mais próximas do que imaginamos. Na última quarta-feira (16), deputados federais e senadores da bancada do Partido Social Liberal (PSL), legenda de Jair Bolsonaro, foram até a China para conhecer o sistema de reconhecimento facial do país.

Os políticos garantem que em fevereiro, logo no início do ano legislativo, apresentarão um projeto de lei (PL) para determinar a implantação de uma tecnologia de reconhecimento facial em locais públicos. A bancada alega que a instalação dos equipamentos tem como objetivo auxiliar forças de segurança públicas no combate à criminalidade.

O ativista Gustavo Gus alerta que a implementação de tecnologias de reconhecimento facial é uma perigosa ação política a partir do momento em que uma pequena classe de programadores, detentores das tecnologias de mapeamento, podem determinar, por exemplo, o que seria uma “feição criminosa” a partir da base de dados adquirida. “Existe essa preocupação de criarem modelos estatísticos que vão representar o racismo, o preconceito e a xenofobia. São valores políticos”.

Bia Barbosa acrescenta que estados autoritários usam o reconhecimento facial massivo de cidadãos para muitas questões que ultrapassam o enfrentamento à violência. Ela lembra que, recentemente, o **Instituto Brasileiro de Defesa do Consumidor (Idec)**, ganhou uma **ação na Justiça de São Paulo contra a ViaQuatro**, companhia privatizada da Linha 4 do metrô da capital paulista. A tecnologia foi implementada para contabilizar quantos usuários do metrô viam determinadas propagandas do lado de dentro dos vagões, assim como para registrar suas reações.

Em setembro de 2018, o Tribunal de Justiça de São Paulo (TJ-SP) compreendeu que havia violação da privacidade dos cidadãos e determinou que a ViaQuatro desinstalasse as aplicações de reconhecimento facial.

Gus analisa que, as democracias do ocidente, no geral, estão desenvolvendo em ritmo acelerado um outro modelo de vigilância, que não se resume à censura de regimes ditatoriais. “É como se dissessem: ‘Você fala o que quiser, o tempo todo, está tudo liberado. Mas está tudo gravado. Quando precisarmos, vamos fazer uma investigação retroativa para falar que em determinado dia, aquela pessoa fez alguma coisa’. Isso é o que é a liberdade de expressão. Tudo que falarmos está sendo registrado e qualquer dia pode ser cobrado”, explica.

“Estamos alimentando essa máquina. Ela não teria capacidade de vigiar se não fossemos nós mesmos. Esse é o grande paradoxo da coisa: essa máquina de vigilância existe por conta dos usuários”, lamenta o organizador da Cryptorave.

Manipulação eleitoral

O **polêmico caso da empresa de dados Cambridge Analytica** nas eleições presidenciais estadunidenses elucida como o uso não autorizado de informações de usuários da internet pode ser manipulado com objetivos bem maiores do que o lucro das empresas: o que está em jogo é o controle das opiniões de cada cidadão usuário das plataformas.

Uma investigação jornalística do The Guardian e do The New York Times revelou que dados pessoais de até 50 milhões de estadunidenses foram obtidos irregularmente do Facebook e utilizados de modo indevido para fins eleitorais. O serviço foi prestado pela empresa a Donald Trump, ganhador das eleições.

Amadeu, que também é professor da Universidade Federal do ABC (UFABC), enfatiza a importância de proteger os dados publicados nas redes sociais. “Toda a navegação e publicação que as pessoas fazem nas redes é coletada por grandes e pequenas empresas. Quanto mais dados as corporações coletam sobre nós, mais frágeis ficamos. Do ponto de vista econômico, abrir mão da nossa privacidade, não proteger os nossos dados é um desastre. Do ponto de vista político, as agências de vigilância das grandes potências fazem uma vigilância massiva. Não espionam somente alvos, mas reúnem informações de todos com o objetivo de prever comportamentos e atuar sobre as nossas tendências”, finaliza o sociólogo.

Edição: Mauro Ramos

COMPARTILHE



RELACIONADAS

Hackers roubaram dados de 29 milhões de usuários do Facebook

Lei de Proteção de Dados trará impactos a pessoas, empresas e governos

SP vai receber 'CryptoRave' grande encontro sobre ativismo e liberdade nas redes

OUTRAS NOTÍCIAS

Das 92 vagas do Mais Médicos em áreas indígenas, apenas quatro estão ocupadas

Violência contra jornalistas cresceu em 2018; período eleitoral concentrou agressões

Prefeitura assume compromisso após mobilização popular contra mineração no Serro (MG)

Brasil de Fato





Todos os conteúdos do Brasil de Fato podem ser reproduzidos, desde que não sejam alterados e que se dêem os devidos créditos.