ISSN 2447-1097

Direito & TI–Porto Alegre/RS www.direitoeti.com.br

FACEAPP: SERÁ APENAS ESTE APLICATIVO A COLETAR NOSSOS DADOS?

Alesandro Gonçalves Barreto[1]
Hericson dos Santos[2]

RESUMO

Diversas são as aplicações de *internet* que fornecem serviços "gratuitos". Nesse contexto, insere-se o aplicativo *FaceApp* que é uma plataforma com tecnologia de rede neural para fazer o envelhecimento de fotografias. Após a viralização do aplicativo, vários foram os questionamentos sobre a coleta massiva de dados. Procuraremos, para tanto, fazer uma análise de outras ferramentas virtuais a fim de demonstrar que não é apenas este aplicativo a realizar este procedimento.

Palavras-chave: *FaceApp*; *Internet*; Privacidade.

INTRODUÇÃO

O aplicativo *FaceApp*, desenvolvido pela empresa russa *Wireless Lab* e disponível para IOS e *Android*, utiliza tecnologia de rede neural para fazer transformações nas fotografias armazenadas no *smartphone* do usuário ou tiradas com o próprio aplicativo. Recentemente, assistimos a viralização desse *software* em redes sociais e aplicativos de mensageria, em especial pelo fato de projetar fotos com cabelos brancos e rostos envelhecidos.

Como regra, os usuários dos serviços de *internet* não leem a política de privacidade ou termos de uso de um serviço, apenas preocupam-se com o trecho onde se diz: "Eu li e concordo". Não foi diferente com a aplicação em apreço. Famosos e anônimos fizeram o *download* e utilizaram as funcionalidades nele existentes para fazer o *upload* de milhões de fotografias.

[1] Delegado de Polícia Civil do Estado do Piauí e coautor dos livros *Inteligência Digital, Manual de Investigação Cibernética e Investigação Digital em Fontes Abertas*, Deep Web, da Editora Brasport; *Vingança Digital*, Mallet Editora; Cibercrimes e seus Reflexos no Direito Brasileiro, Editora Juspodivm e; Cybercards. Coordenador do Núcleo de Fontes Abertas da Secretaria Extraordinária para Segurança de Grandes Eventos nos Jogos Olímpicos e Paralímpicos Rio 2016. Contato: delbarreto@gmail.com

[2] Perito Criminal do Instituto de Criminalística da Superintendência da Polícia Técnico-Científica. Bacharel em Ciência da Computação. Especialista em Redes e Telecomunicações e Perícia Forense Aplicada à Informática. Co-autor do livro *Deep Web* Investigação no Submundo da Internet, da Editora Brasport. Instrutor de Investigação de Pedopornografia da *Child Rescue Coalition* e Instrutor de Cybercrimes da SENASP. Contato: hericson.hs@policiacientifica.sp.gov.br.

Nesse contexto, diversas matérias foram publicadas sobre os dados coletados pelo aplicativo, notadamente o rastreio de navegação e o compartilhamento de dados com terceiros. Não obstante, cabe-nos fazer um questionamento: Será que apenas o *FaceApp* coleta nossos dados e compartilha-os com terceiros?

DA COLETA MASSIVA DE DADOS

A leitura da política de privacidade do *FaceApp* demonstra quais os tipos de informações que o serviço coleta do usuário, assim como a sua utilização e a partilha com terceiros. Sua leitura demonstra qual tipo de informação é obtida:

- Informações fornecidas diretamente pelo usuário: fotos e outros conteúdos publicados no serviço;
- *Analytics:* tráfego e tendências de uso do serviço; informações enviadas pelo dispositivo ou pelo aplicativo; páginas *web* visitadas; complementos e; outros dados;
- *Cookies* e tecnologias similares: utilizam *cookies*, *pixels*, *web beacons* e armazenamento local para coletar informações;
- Arquivos de *log*: informações de acesso em *sites* e aplicativos; solicitações *web*; protocolos de internet; *browser*; nomes de domínio; páginas visualizadas; *urls*; quantidade de *clicks* e; interação com os *links* do serviço;
- Identificadores do dispositivo informático;
- *Metadados*.

Por outro lado, a aplicação de *internet* afirma que essas informações coletadas têm com escopo a melhoria e eficácia do serviço prestado, diagnóstico ou solução de problemas e fornecimento de conteúdo personalizado, dentre outras. Quanto ao compartilhamento de informações com terceiros, a empresa assegura excluir dados identificadores dos usuários. Não obstante, afirma que pode repassar para empresas do mesmo grupo informações de arquivos de *log*, identificadores de dispositivos, *cookies*, conteúdo do usuário e suas informações, além dos dados de localização.

A análise da política de privacidade e/ou termos de uso de outras aplicações de *internet* demonstra que tipo de dado é coletado, seja fornecido pelo usuário ou obtido diretamente pela plataforma. A leitura desses documentos demonstra uma infinidade de dados reunidos pelo *Facebook*, *Instagram*, *WhatsApp* e *Google* e, em alguns casos, informação muito mais relevante do que aquela recolhida pelo *FaceApp*, senão vejamos:

- Atividade de Compras;
- Agenda de Contatos;
- Páginas Acessadas;
- Dados de dispositivos e conexões;
- Localização GPS;
- Aplicativos Instalados;
- Dados de *Cookies* Armazenados

Algumas dessas aplicações de internet citadas ainda capturam informações de localização de uma foto, espaço de armazenamento disponível, acesso à câmera e fotos e pontos de acesso *wi-fi*. O *WhatsApp*, todavia, não fornece informações claras sobre as páginas acessadas pelo usuário e nem dados referentes aos aplicativos instalados pelo usuário. Quanto aos dados de localização, estes só serão recolhidos quando o usuário utiliza o recurso ou ainda nas situações necessárias para diagnosticar ou solucionar problemas.

Tal e qual, existem milhares de outros aplicativos ou serviços ofertados de forma "gratuita". Não obstante, quando instalados no dispositivo informático, transformam o usuário em produto. Os dados por ele fornecidos (geolocalização, *sites* visitados, agendas de contatos, dispositivos informáticos, aplicações instaladas) são muito mais valorosos do que os serviços gratuitos ofertados.

GOODMANN (2015) adverte sobre os problemas decorrentes dessa coleta massiva de dados[i]:

> Como já deve ter ficado claro, a vigilância é um modelo de negócio na *internet*. Você cria contas "gratuitas" em serviços como *Snapchat*, *Facebook*, *Google*, *LinkedIn*, *Foursquare* e *PatientsLikeMe* e baixa aplicativos gratuitos como o *Angry Birds*, *Candy Crush Saga*, *Words with Friends* e *Fruit Ninja* e, em troca, você, de forma consciente ou não, permite que essas empresas possam acompanhar todos os seus movimentos, agregar, correlacionar e vender as informações para o maior número possível de pessoas pelo maior preço, livres de regulamentação, decência ou limitação ética. No entanto,

> poucos param para perguntar quem mais tem acesso a todos esses detritos de dados e como eles podem ser usados contra nós. A vigilância de dados é a tendência do momento e seus usos, capacidades e poderes deverão crescer rapidamente, de maneira que poucos consumidores, governos ou tecnólogos possam imaginar.

CONCLUSÃO

Os usuários de *internet*, como regra, não costumam ler a política de privacidade ou termos de uso de um serviço, apenas aderem ao serviço ofertado sem saber como ele funciona; quais dados são coletados, como são empregados e o compartilhamento com terceiros. Não apenas o *FaceApp* captura dados dos usuários, mas uma infinidade de aplicações de *internet* ora existentes.

É certo que essa coleta excessiva de dados é de grande relevância tanto na manutenção da segurança e integridade quanto na personalização e aprimoramento de produtos e serviços, todavia, essa oferta de serviços "sem custos" nos faz lembrar uma expressão do velho oeste americano: "Não existe almoço grátis". Nos tempos do "Velho Oeste" americano, alguns locais costumavam oferecer comida de forma gratuita aos compradores de bebida alcoólica. A oferta, em princípio era generosa, todavia, as refeições eram feitas com bastante sal, o que obrigava os consumidores a comprar mais bebida.

Nada diferente nos tempos modernos. Necessitamos, pois, entender como esses serviços funcionam, através da leitura de suas políticas e fazer o *download* apenas daqueles essenciais ao nosso dia a dia. O usuário deve entender que seus dados valem muito e, por não conhecer como a plataforma funciona, oferta-os gratuitamente para tornar-se, ao final, o produto.

REFERÊNCIAS

BARRETO, Alesandro Gonçalves. BRASIL, Beatriz Silveira. **Manual de Investigação Cibernética à Luz do Marco Civil da Internet**. Rio de Janeiro: Ed. Brasport, 2016.

BARRETO, Alesandro Gonçalves; KUFA, Karina. SILVA, Marcelo Mesquita. **Cibercrimes e seus Reflexos no Direito Brasileiro**. Salvador: Editora Juspodivm, 2020.

FACEAPP. **Privacy Policy**. Disponível em: https://www.faceapp.com/privacy-en.html. Acesso em: 08 dez. 2019.

FACEBOOK. **Termos e Políticas do Facebook.** Disponível em: https://www.facebook.com/policies. Acesso em: 08 dez. 2019.

GOOGLE. **Política de Privacidade**. Disponível em: https://policies.google.com/privacy?hl=pt-BR. Acesso em: 08 dez. 2019.

GOODMAN, Marc. Future Crimes: Tudo está conectado, todos somos vulneráveis e o que podemos fazer sobre isso. HSM Editora, 2015.

HOBACK, CULLEN. **Terms and Coditions May Apply**. Hirax Films. 2013
INSTAGRAM. **Política de Privacidade**. Disponível em: https://help.instagram.com/402411646841720. Acesso em: 08 dez. 2019.

WHATSAPP. **Termos do Serviço**. Disponível em: https://www.whatsapp.com/legal?eea=0#terms-of-service. Acesso em: 08 dez. 2019.

[i] GOODMAN, Marc. Future Crimes: Tudo está conectado, todos somos vulneráveis e o que podemos fazer sobre isso. P.75.