

Rosyjski FaceApp nie jest groźniejszy od samego Facebooka

20 lipca 2019

Czy zaspokojenie ciekawości, jak możesz wyglądać za kilkadziesiąt lat, naprawdę jest warte tak dużo, by w zamian oddać dostęp do wrażliwych danych nieznanej aplikacji, do tego rosyjskiej? Maciej Kawecki z Ministerstwa Cyfryzacji przestrzega przed bezrefleksyjnym korzystaniem z usługi FaceApp, która zgrabnie przerabia nasze twarze, ale przy tym wymaga udostępnienia zdjęć zapisanych na telefonie.

<https://www.youtube.com/watch?v=bdmf6MK5fc4>

Z kolei „Niebezpiecznik” w swoim materiale uspokaja wszystkich, którym na hasło „rosyjska robota” automatycznie podniosło się ciśnienie: to prawda, aplikację napisał Rosjanin, ale nie ma dowodów, że robi z naszymi danymi więcej niż to, na co sami się zgodziliśmy. Skoro ma przerobić zdjęcie, np. postarzyć naszą twarz, niewątpliwie musi dostać do niego dostęp. A więc w czym problem?

W sieci jesteśmy celem

Zaczniemy od początku – a więc od portalu, bez którego globalna kariera żadnej gry, quizu czy apki przerabiającej zdjęcia nie byłaby możliwa. Dla całych pokoleń wchodzących w świat internetu po 2000 r. Facebook stał się naturalnym środowiskiem. Tkwimy w nim jak żaby w podgrzewanej wodzie – jeszcze nie wyskakujemy, bo woda nie wrze, ale już zrobiło się gęsto i ciężko. Dociera do nas, jak groźne i nieprzyjazne jest to środowisko dopiero wtedy, gdy na scenę wychodzi ktoś pokroju Trumpa, Putina albo spindoktora obracającego milionami psychometrycznych profili. Zdecydowanie zbyt rzadko.

Gra o wpływ na nasze wybory – małe i duże, błahe i bardzo poważne – toczy się na Facebooku przez cały czas. Nawet gdyby jakiś giełdowy kataklizm nagle wymiótł z tej sieci wszystkie aplikacje wyłudzające dostęp do naszych danych, Facebook nadal miałby nietknięte, kompletne profile miliardów ludzi. Zlepione nie tylko z ich zdjęć, ale z tysięcy wiele więcej mówiących interakcji: z treści postów i prywatnych wiadomości, z lajków, z punktów, w których dali się zlokalizować, a nade wszystko z wniosków, jakie na bazie okruszków danych wyciągają coraz lepsze algorytmy. Nawet jeśli nie ujawnię na Facebooku poglądów politycznych, chorób, problemów psychicznych i zakrętów życiowych, nawet jeśli nie podam, z kim utrzymuję relacje intymne i zawodowe albo ile w rzeczywistości zarabiam, portal społecznościowy bez problemu tę wiedzę w swojej bazie uzupełni, analizując moje zachowanie i porównując je do dobrze zbadanych wzorców zachowań ludzi do mnie podobnych.

Ta wiedza nie leży odłogiem. Codziennie wypracowuje zysk dla Facebooka, ponieważ umożliwia targetowanie ludzi w oparciu o to, kim są i czego pragną. Naprawdę cenne dane z Facebooka nigdzie nie muszą wyciekać, by stać się dla nas groźne. Są groźne właśnie dlatego, że każdy płacący reklamodawca czy spindoktor – rosyjski, amerykański, ale i polski, bo na tym rynku nie ma dyskryminacji – może w oparciu o tę wiedzę wywrzeć na nas wpływ. Dyskretnie, np. zamiast ordynarnych reklam sponsorując treści, które wyglądają na neutralne newsy. Wreszcie taki wpływ codziennie i w każdej chwili wywiera na nas sam Facebook – dobierając naszą dietę informacyjną i kształtując obraz naszego świata według własnych, komercyjnych interesów.

Własna twarz może nas zdradzić

Czy na tym tle to, co robi aplikacja FaceApp (i wiele innych o podobnych funkcjach), rzeczywiście jest groźne? Może się tak okazać, jeśli zdjęcia, do których jej twórcy dostali dostęp od ludzi złapanych na wędkę ciekawości, wcale nie znikną z

serwerów po wykonaniu usługi, tylko posłużą im do innych celów. Dobrej jakości zdjęcia milionów już zidentyfikowanych (dzięki danym profilowym) ludzi można wykorzystać – przy odpowiednio złych zamiarach, pewnej determinacji i oczywiście z naruszeniem RODO – do kradzieży tożsamości albo szantażu (dość wspomnieć rosyjski przypadek szantażowania młodych kobiet pracujących w seksbiznesie właśnie dzięki aplikacji rozpoznającej twarze FindFace). Ale też wcale nie trzeba.

Baza danych biometrycznych – w tym przypadku zdjęć – sama w sobie ma komercyjną wartość, bo można dzięki niej trenować algorytmy i uczyć sieci neuronowe (jeszcze lepszego) rozpoznawania twarzy. W tę technologię inwestowane są dziś potężne środki, bo potencjał w niej widzą nie tylko służby i wojsko, ale w zasadzie każda branża podlegająca automatyzacji. Za jakiś czas może się okazać, że nasze twarze nie tylko otwierają bramki „paszportowe” na lotniskach, naprowadzają militarne drony i „zdradzają” naszą tożsamość kamerom na każdym skrzyżowaniu, ale też zastępują bilety wstępu na komercyjne wydarzenia i karty płatnicze. Możemy sobie wyobrazić świat, w którym nasza twarz staje się równie czytelna (oczywiście dla tych, którzy dysponują odpowiednią technologią) co profil na Facebooku i działa jak klucz otwierający drzwi do różnych usług i ułatwień. Czy w ogóle chcemy go sobie wyobrażać i zmierzać w tym kierunku, to zupełnie inna sprawa.

Bezrefleksyjnie karmimy danymi algorytmy, nie wiedząc i nie potrafiąc przewidzieć, w jakim celu ich zdolność rozpoznawania naszych cech biometrycznych i modelowania zachowań – od tego, jak się poruszamy, po to, co i kiedy kupujemy – będzie wykorzystywana przez komercyjne firmy i korzystające z ich wiedzy państwa. Jeśli reagujecie lekkim niepokojem na hasło „rosyjska aplikacja”, zachęcam, by zachować sceptycyzm wobec wszelkich aplikacji, które dają coś błahego w zamian za wartościowe dane. A przede wszystkim przyglądać się temu, co z bezkonkurencyjną (co do wielkości i jakości) bazą danych o

ludziach robi sam Facebook.

Autorstwo: Katarzyna Szymielewicz

Źródła: Panoptikon.org