

Warszawa, dn. 21.04.2026 r.

## **Dlaczego widzę reklamy rzeczy wyszukiwanych w Google na Facebooku?**

Na pewno niejednokrotnie spotkaliście się z taką sytuacją: planujesz urlop w słonecznych Włoszech, wyszukujesz loty na stronach linii lotniczych, hotele na Bookingu, sprawdzasz strony sklepów z kostiumami kąpielowymi, po czym wyłączasz przeglądarkę. Po godzinie uznajesz, że warto sprawdzić na Facebooku, czy w trakcie Twojego urlopu nie ma jakichś interesujących wydarzeń na miejscu. I co? Od razu po włączeniu aplikacji Twój feed jest pełen reklam z Bookingu, postów o słonecznej Italii, zdjęć stroju kąpielowego, który oglądałeś/aś. Myślisz sobie: „ten internet nas śledzi i podsłuchuje!!”.

Zamiast od razu pisać skargę do Mety czy Google, przeczytaj poniższy artykuł i dowiedz się jak naprawdę to działa.

### **Dlaczego widzę na Facebooku reklamy rzeczy, które wyszukiwałem w Google?**

Na początku warto zrozumieć jedną kwestię: to nie jest tak, że Google od razu przekazuje Twoje wyszukiwanie do Facebooka. Współczesny internet nie działa na zasadzie „Google wysyła Facebookowi”, a na bardzo rozbudowanym systemie reklamowym. Twoje dane są zbierane w wielu miejscach jednocześnie: na stronach internetowych, w aplikacjach, przez różne narzędzia analityczne i systemy reklamowe, a następnie łączone i wykorzystywane do tworzenia profilu zainteresowań. Reklamy są wynikiem całej serii drobnych sygnałów, które razem tworzą spójny obraz użytkownika.

Najważniejszy moment w całym procesie dzieje się, gdy wchodzisz na konkretną stronę internetową. Tam uruchamiają się mechanizmy, które sprawiają, że później widzisz reklamy. Większość stron, zwłaszcza sklepów internetowych korzysta z narzędzi marketingowych i analitycznych. Wśród nich są piksele śledzące, czyli niewielkie fragmenty kodu, które rejestrują Twoje zachowanie na stronie. Następnie informują one systemy reklamowe, że dany użytkownik odwiedził stronę, oglądał konkretny produkt, spędził na nim określony czas albo wrócił do niego.

Jednym z najczęściej stosowanych rozwiązań jest technologia Meta (Meta Pixel), która pozwala później wyświetlić reklamę tego samego produktu na Facebooku lub Instagramie. W praktyce działa to tak, że odwiedzasz stronę, system zapisuje Twoje zainteresowanie, a następnie przypomina Ci o produkcie w mediach społecznościowych („Czy nie zapomniałaś o swoim koszyku w X?”).

### **Cookies i fingerprinting**

Oprócz pikseli dużą rolę odgrywają pliki cookies i różnego rodzaju identyfikatory. Pliki cookies (ciasteczka) to małe pliki zapisywane w Twojej przeglądarce, gdy wchodzisz na strony internetowe. Dzięki nim strona może pamiętać, czy jesteś zalogowany/a lub co przeglądałeś/aś wcześniej. Cookies pomagają dopasować treści oraz reklamy do użytkownika. Dzięki nim systemy reklamowe potrafią rozpoznać, że to właśnie Ty wróciłeś/aś na inną stronę, nawet jeśli wcześniej się na nią nie logujesz.

Współczesne technologie idą jednak coraz dalej. Coraz częściej stosuje się cyfrowy odcisk palca przeglądarki („fingerprinting”), metodę śledzenia użytkownika w internecie, która polega na zbieraniu informacji o Twoim urządzeniu i przeglądarce, żeby stworzyć unikalny profil Ciebie online. Na jego podstawie system może rozpoznać użytkownika nawet po takich szczegółach jak urządzenie czy system operacyjny. To sprawia, że śledzenie nie zależy już wyłącznie od cookies, które można usunąć. Systemy potrafią działać nawet wtedy, gdy użytkownik próbuje ograniczyć swoją widoczność.

Wszystkie Twoje dane trafiają do systemów reklamowych, które działają w czasie rzeczywistym. Jeśli odwiedzasz stronę z produktem, system oznacza Cię jako osobę zainteresowaną. Jeśli takich sygnałów jest więcej to reklama staje się bardziej prawdopodobna. Kiedy później otwierasz Facebooka, system reklamowy już wie, że istnieje duża szansa, że Twojego zainteresowania danym produktem i dlatego pokazuje Ci reklamę dokładnie wtedy, kiedy jest większa szansa, że w nią klikniesz. Nie musisz kupować danej rzeczy lub mieć jej w koszyku. Wystarczy, że zatrzymasz się na stronie z produktem, wrócisz do niej albo klikniesz na podobne rzeczy. Każda aktywność na stronie jest sygnałem, który tworzy Twój profil zainteresowań.

Kiedy system zbierze już wcześniej zebrat wystarczająco dużo danych, żeby przewidzieć Twoje zainteresowanie, reklama może pojawić się w idealnym momencie („czyta nam w myślach”). Wystarczy, że należysz do grupy użytkowników o podobnych zachowaniach albo wcześniej wykonałeś/aś działanie związane z danym tematem.

### Ramy prawne

System reklamowy nie działa bez kontroli, ponieważ podlega regulacjom takim jak RODO. Przepisy wymagają, aby firmy informowały użytkowników o przetwarzaniu danych, celu ich zbierania oraz możliwości wycofania zgody. W teorii każdy użytkownik ma więc kontrolę nad swoimi danymi. W praktyce większość osób akceptuje zgody cookies automatycznie, bez analizy ich treści. Pomimo tego, że zgoda na cookies marketingowe, analityczne i śledzenie powinna być domyślnie niezaznaczona („opt-in”), nie każdy właściciel strony internetowej o tym pamięta. Choć formalnie system jest uregulowany, to jego skala działania pozostaje ogromna. Trzeba pamiętać, że prawo daje narzędzia ochrony, ale nie zastępuje świadomego wyboru.

### Jak się chronić przed śledzeniem?

Nie da się całkowicie zniknąć z systemów reklamowych internetu, ale można znacząco ograniczyć ilość zbieranych danych. Ważne jest przede wszystkim świadome zarządzanie zgodami cookies: nie każda strona musi mieć dostęp do danych marketingowych. Warto też korzystać z przeglądarek, które blokują trackery i automatycznie ograniczają śledzenie. Znaczenie ma również sposób korzystania z kont. Logowanie się wszędzie tym samym profilem ułatwia łączenie danych w jeden spójny obraz użytkownika. Ograniczenie tego może zmniejszyć poziom profilowania. Na końcu pozostaje najprostsza zasada: im mniej informacji zostawiasz w internecie, tym mniej dokładny staje się Twój cyfrowy profil.

Poniżej przedstawiam listę praktycznych wskazówek, które mogą ograniczyć śledzenie i reklamy personalizowane:

1. **Ogranicz zgody na cookies** - zamiast klikać „akceptuję wszystko”, wybieraj tylko niezbędne pliki cookies lub ręcznie wyłącz marketingowe i analityczne.
2. **Sprawdzaj ustawienia prywatności w przeglądarce i reklam na stronach internetowych, z których korzystasz** - włącz blokowanie trackerów (narzędzi śledzących do zbierania informacji o tym, co robisz online) i ochronę przed śledzeniem (większość przeglądarek ma takie opcje domyślnie).
3. **Korzystaj z trybu prywatnego (incognito)** - nie zapisuje on historii i ogranicza część śledzenia lokalnego (choć nie zapewnia pełnej anonimowości).
4. **Regularnie czyść dane przeglądarki** - usuwaj cookies, pamięć podręczną i dane stron.
5. **Ogranicz logowanie do wielu usług tym samym kontem** - korzystanie z jednego konta (np. Google) w wielu miejscach ułatwia łączenie Twojej aktywności.
6. **Używaj przeglądarek lub rozszerzeń blokujących trackery** - narzędzia takie jak adblock i anti-tracking zmniejszają liczbę skryptów śledzących.

### Podsumowanie

Reklamy, które idą za użytkownikiem, nie są wynikiem jednego mechanizmu czy jednej aplikacji. To efekt działania całego ekosystemu, który zbiera drobne informacje o Twoim zachowaniu i łączy je w jeden obraz. Nie chodzi więc o to, że internet czyta w myślach. Chodzi o to, że bardzo dobrze analizuje Twoje działania (nawet te najmniejsze) i to dlatego reklamy wydają się tak trafne.

**Gabriela Tokarska** - młodsza specjalistka ds. ochrony danych osobowych w iSecure sp. z o.o.