

10 grzechów reklamy internetowej

29 stycznia 2020

Nie sposób dziś obejrzeć filmu lub przejrzeć ulubionego serwisu informacyjnego, nie wpadając na co najmniej kilka reklam. Do tego dochodzą jeszcze okienka domagające się akceptacji ciasteczek. Większość użytkowników sieci (według niektórych szacunków nawet dwie trzecie) irytują te utrudnienia. Ale ostatecznie – czy bezpłatny dostęp do treści i narzędzi online nie jest wart tych małych poświęceń?

Biznes reklamy internetowej twierdzi, że spersonalizowane reklamy pozwalają użytkownikom na darmowe przeglądanie Internetu, jednocześnie umożliwiając wydawcy zarobienie na udostępnianej treści. Wygląda na to, że wszyscy wygrywają, prawda?

Rzeczywistość jest jednak zupełnie inna. Reklama internetowa w obecnym kształcie stanowi ogromne zagrożenie dla prywatności, obniża jakość mediów i jest platformą dla poważnych malwersacji, umożliwiając finansowanie przestępczości zorganizowanej.

Przedstawiamy (niewyczerpującą) listę dziesięciu grzechów reklamy internetowej.

1. Iluzja zgody

Dostawcy reklamy internetowej i związanych z nią narzędzi (firmy z tzw. branży adtech) twierdzą, że użytkownicy dobrowolnie zgadzają się na udostępnianie swoich danych, żeby „doświadczać sieci w sposób spersonalizowany”. Jednak to, co firmy adtech nazywają „zgoda”, często nie ma nic wspólnego z przepisami RODO.

Wyskakujące okienka powitalne na stronach internetowych są zaprojektowane tak, żeby nami manipulować – na banerze świeci się wielki zielony guzik z napisem „Akceptuję”, tymczasem ukryta za prawniczym żargonem opcja odmowy wymaga co najmniej kilku kliknięć. Często więc, zmęczeni nieustannymi pytaniami o „zgode”, zamykamy baner, żeby tylko się go pozbyć. A tu niespodzianka: w wielu przypadkach kliknięcie w X również zostanie zinterpretowane jako zgoda. W świetle prawa, aby zgoda była ważna, musi być świadoma, co oznacza faktyczne zrozumienie tego, jak dane będą wykorzystywane. Tymczasem informacje, które podaje wiele firm, są zbyt ogólnikowe, żeby na ich podstawie można było podjąć świadomą decyzję. Poza tym, czy bez specjalistycznej wiedzy jesteśmy w ogóle w stanie zrozumieć konsekwencje udzielenia zgody na coś tak skomplikowanego i nieprzejrzystego?

2. Inwazyjne profilowanie

Biznes reklamowy wytworzył szereg narzędzi, które umożliwiają śledzenie ludzi w sieci. Zasysając informacje z wielu różnych serwisów jednocześnie (cross-site tracking), dostawcy reklam łączą dane o tym, co oglądamy i czytamy w trakcie całej naszej aktywności online. Na skonstruowanie jeszcze dokładniejszego profilu pozwala wymiana tych informacji między urządzeniami (cross-device tracking), np. prywatnym smartfonem i służbowym komputerem. Biznes reklamowy wykorzystuje nowe, niewidoczne dla laika metody śledzenia, których zadaniem jest obejście ustawień przeglądarki blokującej ciasteczka. Taką rolę spełnia np. odcisk palca przeglądarki (browser fingerprinting). Normą jest wymiana danych: po skończonej licytacji reklamowej firmy biorące w niej udział udostępniają sobie nawzajem nasze identyfikatory w procesie synchronizacji ciasteczek (cookie syncing). Oznacza to, że przy następnej licytacji uczestnicy aukcji będą w stanie ustalić, że „Użytkownik 123” w ich bazach danych to ta sama osoba, która w serwisie Onet.pl ma identyfikator „ABC”.

Wszystkie te techniki mają na celu stworzenie naszych szczegółowych profili, dzięki którym firmy będą skuteczniej targetować reklamy. Takie internetowe profile zawierają m.in. listę wszystkiego, co czytaliśmy, adresy IP, dokładne położenie, dane techniczne urządzenia i interakcje z treścią stron – właściwie wszystko, co wiadomo o nas na podstawie naszej aktywności w sieci. Wiele z tych informacji to dane wrażliwe dotyczące zdrowia, orientacji seksualnej, poglądów politycznych i religijnych. Według RODO informacje te mogą co prawda być przetwarzane na podstawie zgody, ale w praktyce nikt o nią nie pyta. Jak ustalił brytyjski organ ochrony danych ICO, prowadzący dochodzenie w sprawie przetwarzanie danych w branży adtech, firmy bezmyślnie zbierają, co tylko się da, nie zwracając uwagi na przydatność danych. Brytyjska organizacja Doteveryone szacuje, że nawet 84% zebranych o nas danych nie jest obecnie używane. Niewielka to pociecha, biorąc pod uwagę, że prawdopodobnie już wkrótce uczenie maszynowe umożliwi marketingowcom wykorzystanie tych złóż informacji.

3. Masowy wyciek danych

Kiedy dane trafiają na serwer giełdy reklamowej, tracimy nad nimi kontrolę. Intymne szczegóły na nasz temat wędrują do setek albo tysięcy firm, miliardy razy dziennie.

Nie ma żadnych gwarancji, że dane będą bezpieczne, bo firmy poprzestają na umownych postanowieniach. Na przykład z wytycznych reklamowych Google'a dowiadujemy się, że jedynie zwycięzca danej aukcji może wykorzystać dane do wzbogacenia profilu użytkownika. Jest to jednak tylko zapis w umowie, za którym nie idą zabezpieczenia techniczne. Informatorzy z branży reklamowej twierdzą wręcz, że niektóre firmy biorą udział w aukcjach właśnie po to, żeby wzbogacić swoje bazy, a wcale nie po to, aby wygrać. Jak ujął to szef firmy Tapad, specjalizującej się w śledzeniu użytkowników między różnymi urządzeniami: „W tym ekosystemie wszyscy zgadzają się, że wymiana danych jest korzystna dla wszystkich stron”. Ten

nieustanny wyciek danych dotyczy praktycznie każdego, kto kiedykolwiek używał Internetu, i jest prawdopodobnie największym odnotowanym wyciekiem danych w historii.

4. Brak przejrzystości

Jako użytkownicy nie tylko nie mamy dostępu do swoich danych – często całkowicie tracimy je z oczu. Dla przeciętnego użytkownika samo zidentyfikowanie firm, które dysponują jego danymi, jest niezwykle trudne. Kluczowe identyfikatory wykorzystywane przez brokerów danych do oznaczania konkretnych użytkowników i personalizowania reklam nie są ujawniane osobom, których dotyczą. Ten swoisty paragraf 22 jest nie do pogodzenia z wymaganiami RODO, zwłaszcza z zasadą przejrzystości.

Nawet jeśli uda nam się dotrzeć do firm reklamowych, które przetwarzają nasze dane, i uzyskać identyfikator, usłyszymy serię wymówek: że ciasteczka identyfikują urządzenie, a nie użytkownika (widać brokerzy danych nie zauważyli, że smartfony i laptopy pełnią obecnie raczej funkcję szczoteczki do zębów niż lodówki, do której każdy może zajrzeć), albo że kategorie wykorzystywane w tworzeniu danego profilu objęte są tajemnicą handlową. Chociaż niektóre firmy decydują się ujawnić zgromadzone dane, robią to w formie niezrozumiałego wykazu znaków i wykresów. Bez jakiegokolwiek opisu, który pomógłby zorientować się, na co patrzymy – o wykryciu potencjalnych naruszeń nie wspominając.

5. Potencjał dyskryminacji

Skuteczność systemów targetowania zależy od jakości wykorzystywanych przez nie danych, zaś skuteczność algorytmów – od tego, jak zostały zaprogramowane. A programiści to tylko ludzie, bywają stronniczy. Istotą targetowania behawioralnego jest optymalizacja reklam pod kątem osób, które potencjalnie będą nimi najbardziej zainteresowane. Ma to sens w przypadku

kupujących narzędzia, ale zawodzi w przypadku ogłoszeń o pracę. Szczególnie widoczne jest to w branżach, w których pracuje mniejszy odsetek kobiet, mniejszości etnicznych czy innych marginalizowanych grup społecznych. Mechanizmy targetowania przyczyniają się do utrwalania nierówności, rzadziej podsuwając osobom należącym do tych grup oferty pracy. Bywa i tak, że cechy takie jak pochodzenie czy miejsce zamieszkania stają się podstawą do wykluczenia osoby z dostępu do danej usługi. Co ciekawe nawet próby zaradzenia tej sytuacji poprzez sztuczne zrównoważenie danych, nie przynoszą rezultatu. Algorytmy mediów społecznościowych będą dalej próbowały optymalizować reklamy, a w konsekwencji – pogłębiać dyskryminację.

Dążenie marek do tego, żeby pojawiać się w środowisku dla nich bezpiecznym (brand safe environment), sprawia, że niektóre rodzaje treści otrzymują etykietę „niemonetyzowalnych”, pozbawiając ich wydawców dochodów z reklam. Marki tworzą czarne listy stron i słów kluczowych, w towarzystwie których nie chcą się reklamować, co zapobiega wspieraniu mowy nienawiści lub dezinformacji klimatycznej. Na przykład linia lotnicza nie chce kojarzyć się ze słowami „terror” lub „katastrofa”. Ale listy słów kluczowych mogą blokować (i często tak się dzieje) treści, w których pojawiają się słowa takie jak „lesbijki” lub „muzułmanie”, co ogranicza możliwości zarabiania na reklamie treściom tworzoną dla społeczności muzułmańskich i LGBTQ+. Brytyjska organizacja branży reklamowej Outvertising szacuje, że w ten sposób wykluczanych z możliwości pozyskiwania środków z reklam jest aż 73% bezpiecznych treści związanych z LGBTQ+.

6. Zepsute „domyślnie” i „w fazie projektowania”

RODO wprowadziło pojęcia privacy by design (prywatność w fazie projektowania) oraz privacy by default (prywatność jest

chroniona domyślnie). Oznacza to, że każda firma, projektując, wdrażając i wykorzystując narzędzia do przetwarzania danych osobowych, jest zobowiązana uszanować prywatność osób, których dane przetwarza. Wysoki standard ochrony prywatności powinien być ustawiony domyślnie, co oznacza, że użytkownik nie musi podejmować żadnych działań (np. zmieniać ustawień), żeby się nią cieszyć.

Reklama targetowana jest całkowicie sprzeczna z tymi zasadami. Jest zaprojektowana i ustawiona w sposób, który domyślnie ignoruje prawo do prywatności. Przykłady? Firmy nie respektują wyraźnego życzenia użytkowników, którzy nie zgadzają się na śledzenie; w systemie reklamowym Google'a domyślne ustawienia dla wydawców zakładają przesyłanie danych użytkowników do podmiotów trzecich; firmy sprzedające reklamy kontekstowe nie mają możliwości rezygnacji z otrzymywania danych osobowych poprzez zapytania z giełd reklamowych. Wreszcie: użytkownicy nie mają jak w prosty sposób cofnąć zgody ani uzyskać dostępu do zgromadzonych na ich temat informacji.

7. Wspieranie zepsutego Internetu...

Istotą reklamy jest monetyzacja uwagi. Im więcej ludzi wyświetli reklamę lub w nią kliknie, tym więcej reklamodawcy są gotowi zapłacić. Ten mechanizm ponosi sporą część winy za popularyzację clickbaitów i taniej sensacji, a co za tym idzie – pogorszenie jakości mediów i dyskursu publicznego. Całkowicie zautomatyzowane i nieprzejrzyste systemy licytacji są atrakcyjne dla wydawców fake newsów. W ten sposób pieniądze przeznaczone na reklamy przez największe światowe marki wspierają ekstremistyczne i fałszywe treści. Do tego szacuje się, że w 2019 r. reklamodawcy na całym świecie stracili ponad 30 miliardów dolarów przez oszustów wykorzystujących boty do nabijania kliknięć i wyświetleń. Światowa Federacja Reklamodawców ocenia, że do 2025 r. malwersacje związane z reklamą będą drugie na świecie pod względem wielkości – po handlu narkotykami.

8. ...i pośredników – zamiast prawdziwych mediów

Reklamy wspierają wydawców, pozwalając im płacić za tworzenie treści, i umożliwiają dostęp do wiadomości każdemu, niezależnie od zasobności jego portfela – to najmocniejszy argument branży reklamowej, który ma zniechęcić twórców prawa i urzędów do narzucania ściślejszych reguł. W rzeczywistości do wydawców trafia tylko niewielki ułamek pieniędzy przeznaczanych na spersonalizowaną reklamę. Między 55% (dane branżowe) a 70% (zgodnie z eksperymentem brytyjskiej gazety „The Guardian”) pieniędzy wydanych na reklamę trafia w ręce pośredników (por. Krajobraz marketingowy w 2019 r.). Określa się to mianem „podatku adtechowego”.

Co więcej: zysk z reklamy behawioralnej nie usprawiedliwia naruszenia prywatności. Nowe badania zaprzeczają danym branżowym i pokazują, że w porównaniu do reklamy kontekstowej spersonalizowane reklamy przynoszą jedynie 4% więcej zysku dla wydawcy. Jeśli do tego wziąć pod uwagę wydatki związane z dostarczaniem reklamy behawioralnej (np. koszt infrastruktury lub zapewnienie zgodności z RODO), okaże się, że wydawca może do niej dopłacać. Tymczasem, firmy dostarczające sprzyjającej prywatności reklamy kontekstowej pokazują, że wydawcy zarabiają na niej więcej.

Topniejące przychody i trudne decyzje sprawiają, że wydawcy poddają się zasadom narzucanym przez większe firmy. Jeśli nie będą udostępniać informacji o swoich użytkownikach, reklamodawcy pójdą gdzie indziej. Przykład? Jeśli wydawca chce wyświetlać reklamy z wykorzystaniem infrastruktury Google’a, musi zaakceptować, że firma ta wykorzysta swoją pozycję monopolisty do osiągnięcia własnych korzyści. Google wykorzystuje informacje o osobach odwiedzających niezależne strony po to, żeby wzbogacić swoją bazę profili i dokładniej targetować reklamy w ramach własnych serwisów, np. YouTube’a.

9. Potężny ślad węglowy

Ogrom (niepotrzebnych) danych trzeba gdzieś przechować i przetworzyć. To wymaga gigantycznych zasobów energii. Według badań przeprowadzonych w 2016 r. reklama internetowa zostawia za sobą ślad węglowy wielkości 60 milionów ton, co odpowiada 10% całej emisji generowanej przez infrastrukturę internetową na świecie – albo 60 milionom lotów między Londynem a Nowym Jorkiem.

Od tego czasu ta liczba wzrosła i będzie to robić dalej, szczególnie że coraz większą popularność zyskuje wyjątkowo energochłonne uczenie maszynowe. Biorąc pod uwagę obecny kryzys klimatyczny, nie możemy tak po prostu zignorować tego aspektu reklamy internetowej, szczególnie przy braku przekonujących argumentów za gromadzeniem tak wielu niepotrzebnych danych.

10. Element większego problemu

Obraz ukazujący skalę problemów pozostanie niepełny, póki nie spojrzymy szerzej na Internet i gospodarkę opartą na danych. W obecnej postaci system reklamy internetowej zasila modele biznesowe oparte na śledzeniu i założeniu, że ludzie i informacje o ich intymnych sprawach są towarem. Najlepiej oddaje to żargon używany w branży reklamowej. Uwaga użytkowników („impresja”) jest wystawiana na aukcjach, oni sami są kategoryzowani w „segmenty”, które – jak chwali się jedna z firm – można dowolnie formować przy użyciu 92 milionów ciasteczek, a „niezliczone dane z niezliczonych urządzeń” to nic innego jak intymne szczegóły naszego życia.

Chociaż na rynku działają tysiące firm reklamowych, reklama internetowa pozostaje duopolem Google’a i Facebooka. Według niektórych szacunków dwaj giganci reklamowi kontrolują 84% rynku reklamy online. Większość reklam sprzedają w ramach własnych serwisów (jak Instagram czy YouTube), chociaż Google

dodatkowo zarządza giełdami reklam na zewnętrznych stronach. Nawet jeśli mechanizmy śledzenia przez podmioty trzecie i giełdy reklamowe przestaną być legalne, Google i Facebook przetrwają dzięki danym zgromadzonym przez swoje własne platformy internetowe. To nie znaczy, że powinniśmy ignorować naruszenia, do których dochodzi na giełdach reklam, ale że musimy traktować ten wątek jako element szerszej debaty o przyszłości Internetu.

Czas porozmawiać o alternatywach

Aukcje w czasie rzeczywistym (real-time bidding, RTB) pojawiły się ponad dekadę temu, w 2009 r. Bob Hoffman, weteran branży reklamowej i autor wielu książek na jej temat, nazywa ostatnie dziesięciolecie „dekadą reklamowego mydlenia oczu”. Niecałe dziesięć lat po narodzinach aukcji RTB w życie weszło RODO. Nie ulega wątpliwości, że system reklamy behawioralnej nie został zaprojektowany po to, aby chronić prywatność i prawa człowieka; wręcz przeciwnie: opiera się na wykorzystywaniu masowych ilości danych, żeby wpływać na decyzje użytkowników. Jest zepsuty na wielu poziomach – półśrodki i kosmetyczne poprawki mogą wyłącznie złagodzić objawy, ale nie rozwiążą systemowego problemu.

W 2020 r. znaleźliśmy się w decydującym momencie. Organy ochrony danych z kilkunastu krajów Unii Europejskiej analizują działanie biznesu reklamowego, a głosy zaniepokojenia słychać już nawet wewnątrz branży. Nadszedł czas, żeby porozmawiać o alternatywnych rozwiązaniach, które z szacunkiem dla prywatności i praw człowieka pozwolą tworzyć zdrowszy ekosystem medialny. Wszyscy powinniśmy wziąć udział w tej dyskusji. Zbyt wiele mamy do stracenia.

Co możesz zrobić, żeby choć trochę

zadbać o swoją prywatność?

1. Nie klikaj w reklamy ani sponsorowane wyniki wyszukiwania!
2. Zainstaluj wtyczkę (np. [NoScript](#)), która będzie blokować skrypty śledzące w Twojej przeglądarce (uwaga, zobaczysz zupełnie inny Internet).
3. Wybierz alternatywną przeglądarkę (np. [Firefox](#)) i wyszukiwarkę (np. [DuckDuckGo](#)).
4. Regularnie czyść ciasteczka i identyfikatory reklamowe na swoich urządzeniach.
5. Wspieraj organizacje walczące o Twoją wolność i prywatność w sieci (np. Panoptikon).

Autorstwo: Karolina Iwańska

Współpraca: Harriet Kingaby, Mozilla Fellow w organizacji Consumers International, Stanisław Arendarski (tłumaczenie), Anna Obem i Maria Wróblewska (redakcja)

Źródło: [Panoptikon.org](https://panoptikon.org)

Bibliografia

1.
<https://news.stanford.edu/2018/03/21/this-stanford-scholar-learned-clickbait-will-surprise/>
2.
<https://wfanet.org/knowledge/item/2016/06/06/WFA-issues-first-advice-for-combatting-ad-fraud>
3.
<https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf>
4.
<https://blog.mozilla.org/firefox/cross-site-tracking-lets-unpa>

ck-that/

5. <https://arxiv.org/abs/1905.09581>

6.

<https://panoptikon.org/wiadomosc/wyciek-danych-na-gieldach-reklam>

7.

<https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf>

8. <https://www.doteveryone.org.uk/report/digital-attitudes/>

9.

<https://brave.com/wp-content/uploads/2019/07/Scale-billions-of-bid-requests-per-day-RAN2019061811075588.pdf>

10.

<https://www.google.com/intl/en/doubleclick/adxbuyer/guidelines.html>

11.

<https://adexchanger.com/data-exchanges/tapad-ceo-on-cross-device-graphs-and-where-its-data-comes-from-hint-not-telenor/>

12. <https://brave.com/DPC-google/>

13.

<https://en.panoptikon.org/articles/black-boxed-politics-opacity-choice-ai-systems>

14.

<https://www.europeanscientist.com/en/public/women-are-seeing-less-stem-job-ads-than-men-are-marketing-algorithms-promoting-gender-bias/>

15.

<https://www.propublica.org/article/facebook-advertising-discrimination-housing-race-sex-national-origin>

16 .

<https://www.nytimes.com/2019/08/20/upshot/housing-discrimination-algorithms-hud.html>

17 .

<https://www.linkedin.com/pulse/save-digital-advertising-world-togetherwecan-jerry-daykin/>

18 .

<https://gizmodo.com/do-not-track-the-privacy-tool-used-by-millions-of-peop-1828868324>

19 .

<https://www.thetimes.co.uk/edition/news/big-brands-fund-terror-knnxfgb98>

20 .

<https://www.tandfonline.com/doi/full/10.1080/21670811.2018.1556314>

21 .

<https://www.businessinsider.com/wfa-report-ad-fraud-will-cost-advertisers-50-billion-by-2025-2016-6?IR=T>

22 .

<https://www.adweek.com/digital/3-benefits-resulting-from-ad-tech-tax-cuts/>

23 .

<https://mediatel.co.uk/newsline/2016/10/04/where-did-the-money-go-guardian-buys-its-own-ad-inventory/>

24 .

<https://techcrunch.com/2019/05/31/targeted-ads-offer-little-extra-value-for-online-publishers-study-suggests/>

25. <https://kobler.no/contextual-insights/>

26 .

<https://www.sciencedirect.com/science/article/pii/S01959255173>

03505

27 .

<https://www.theguardian.com/environment/ng-interactive/2019/jul/19/carbon-calculator-how-taking-one-flight-emits-as-much-as-many-people-do-in-a-year>

28 .

<https://chiefmartec.com/2019/04/marketing-technology-landscape-supergraphic-2019/>

29 .

<http://adcontrarian.blogspot.com/2019/10/advertisings-decade-of-delusion.html>