UNIWERSYTET EKONOMICZNY W KATOWICACH

INFORMATYKA I EKONOMETRIA

NATALIA JABŁOŃSKA
129095

WPŁYW WYCOFANIA THIRD-PARTY COOKIES NA RETARGETING

IMPACT OF DECOMISSIONING THIRD-PARTY COOKIES ON RETARGETING

Praca licencjacka
napisana w Katedrze Informatyki
pod kierunkiem prof. UE dr hab. Artura Strzeleckiego

Oświadczam, że niniejsza praca została przygotowana pod moim kierunkiem
i stwierdzam, że spełnia wymogi stawiane pracom dyplomowym

Pracę akceptuję

……
……
(data) (podpis promotora)

KATOWICE 2022

Katowice, dnia 30.09.2022

Natalia Jabłońska

.....

Imię i nazwisko

Informatyka

.....

Wydział

Informatyka i Ekonometria

.....

Kierunek

OŚWIADCZENIE

Świadoma odpowiedzialności prawnej oświadczam, że złożona praca licencjacka/inżynierska/magisterska pt.: Wpływ wycofania third-party cookies na retargeting została napisana przeze mnie samodzielnie.

Równocześnie oświadczam, że praca ta nie narusza praw autorskich w rozumieniu ustawy z dnia 4 lutego 1994 roku o prawie autorskim i prawach pokrewnych (tj. Dz. U. z 2018 r., poz. 1191, z późn. zm.) oraz dóbr osobistych chronionych prawem.

Ponadto praca nie zawiera informacji i danych uzyskanych w sposób niedozwolony i nie była wcześniej przedmiotem innych procedur związanych z uzyskaniem dyplomów lub tytułów zawodowych uczelni wyższej.

Wyrażam zgodę na nieodpłatne udostępnienie mojej pracy w celu oceny jej oryginalności przez Jednolity System Antyplagiatowy prowadzony przez Ministra Nauki i Szkolnictwa Wyższego oraz przechowywania jej w Ogólnopolskim Repozytorium Prac Dyplomowych oraz wewnętrznej bazie prac dyplomowych Uniwersytetu Ekonomicznego w Katowicach. Zostałem poinformowany o zasadach dotyczących oceny oryginalności pracy dyplomowej przez Jednolity System Antyplagiatowy.

Oświadczam także, że ostateczna wersja pracy przesłana przeze mnie drogą elektroniczną jest zgodna z plikiem poddanym ocenie w Jednolitym Systemie Antyplagiatowym.

Jednocześnie oświadczam, że jest mi znany przepis art. 233 § 1 Kodeksu karnego określający odpowiedzialność za składanie fałszywych zeznań.

Jednocześnie oświadczam, że jest mi znany przepis art. 233 § 1 Kodeksu karnego określający odpowiedzialność za składanie fałszywych zeznań.

(podpis składającego oświadczenie)

Spis treści

Wstęp

Funkcjonowanie przedsiębiorstwa na rynku wymaga ustalenia i zrealizowania określonej strategii działania. W ogólnym sensie, strategia rozumiana jest jako proces przygotowania i przeprowadzenia działań zmierzających do realizacji określonych celów. Na poziomie całego przedsiębiorstwa jest sposobem kierowania organizacją jako całością. Strategie na poziomie różnych branż, produktów są planami działania wykorzystywanymi przy kierowaniu tymi branżami. Jednym z kluczowych elementów w prowadzeniu działalności jest promowanie własnej działalności, produktów oraz prezentowanie wizerunku swojej marki w jak najlepszym świetle. Strategia e-marketingowa lub inaczej strategia marketingowa w Internecie powinna być traktowana jako element strategii marketingowej, będący ważną częścią ogólnej strategii rozwojowej przedsiębiorstwa, w którym kanały elektroniczne i media cyfrowe wspierają inne kanały komunikacji i sprzedaży. Stworzenie skutecznej strategii e-marketingowej wymaga precyzyjnego określenia w jakim celu oraz jak będą wykorzystywane kanały komunikacji internetowej. Jedną ze strategii w online marketingu jest retargeting, który uważany jest za ważny element całej strategii e-marketingu firmy.

Celem przedstawionej pracy jest rozpoznanie powyższej strategii marketingowej, pokazanie jej nadużyć w kontekście ochrony danych osobowych oraz zbadanie wpływu nadchodzącego wycofania plików cookie stron trzecich w ekosystemie reklamy targetowanej.

Celem poznawczym jest rozpoznanie metod prowadzenia strategii remarketingu oraz zbadanie, jak zbierane dane o użytkownikach mają wpływ na jej efektywność.

Celem empirycznym pracy jest ocena zagrożeń dla reklamy behawioralnej po procesie wycofania third-party cookies.

W pierwszym rozdziale przedstawione zostanie czym są pliki cookie, na jakie rodzaje możemy je podzielić, a także zostanie przedstawiona historia stojąca za decyzją wycofania z funkcjonowania plików śledzących.

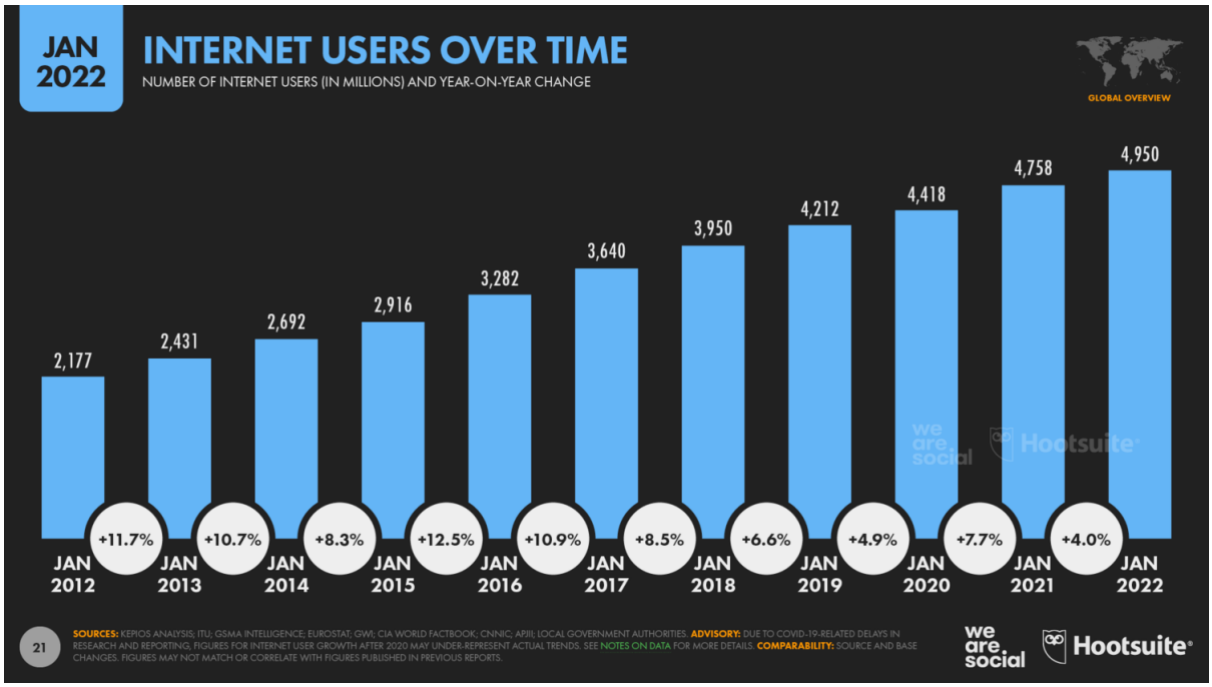
W drugim rozdziale zostanie omówiony sposób działania retargetingu oraz aukcji real time bidding. Zbadane zostanie także, w jaki sposób wykorzystywane są dane użytkowników w procesie aukcyjnym.

W ostatnim rozdziale przedstawione zostaną wyniki badań przeprowadzonych na grupie osób bezpośrednio zaangażowanych w zmiany ekosystemu remarketingowego.

1. Pliki cookie w środowisku webowym

Gdy w 1969 roku na Uniwersytecie kalifornijskim w Los Angeles powstał Internet nikt nie spodziewał się, że kilkadziesiąt lat później osiągnie on taką skalę, a dostęp do niego będzie miało prawie 5 miliardów ludzi, czyli 63% populacji. Dzięki technologii Elona Muska „starlink" wkrótce Internet będzie dostępny praktycznie z każdego miejsca na Ziemi. Internet ma bardzo wiele zalet. Dzięki niemu w kilka sekund możemy w bardzo łatwy sposób znaleźć wszelkie informacje, których zwykle szukalibyśmy w bibliotekach. Internet pełni również funkcję rozrywkową jak i społeczną. Dzięki social mediom możemy w kilka sekund komunikować się z innymi niezależnie od odległości a także poznawać nowe osoby. Dodatkowo w sieci możemy robić zakupy, dzięki czemu oszczędzamy czas, energię. Umożliwia on także prowadzenie zdrowej konkurencji, gdyż mamy dostęp do tego samego produktu od różnych sprzedawców. Dzięki temu możemy również oszczędzić nasze pieniądze.

Niewątpliwie Internet ma wiele zalet jednak w XXI wieku powyższe funkcje stały się podstawowymi czynnościami, a przedsiębiorcy szukają coraz to ciekawszych sposobów na zarabianie w Internecie. Jednak większość biznesów i technologii internetowych ma jeden, wspólny czynnik, który determinuje ich sukces. Od wielu dekad firmy gromadzą dane osobowe swoich użytkowników lub klientów, które następnie wykorzystują w celach marketingowych lub niejednokrotnie sprzedają. Dane osobowe stały się nowym złotem, a ten który posiada ich najwięcej i potrafi je dobrze analizować wygrywa na rynku. Powstało wiele internetowych technologii, które skutecznie śledzą użytkownika, w celu ich identyfikowania, a później efektywnego wykorzystania tych danych do zdobycia najbardziej dochodowych klientów. Największą ofiarą takich działań są użytkownicy, których każdy najmniejszy ruch w sieci, wyszukiwanie, decyzje zakupowe są śledzone, zbierane, analizowane i wykorzystywane. Jednym z rozwiązań używanych do śledzenia użytkowników są pliki cookie.



Rysunek 1 - Użytkownicy Internetu w przeciągu dekady. Źródło: https://datareportal.com/reports/digital-2022-global-overview-report

Jak wynika z powyższego wykresu (Rysunek 1) ilość użytkowników Internetu stale rośnie, a problem prywatności będzie dotyczył coraz większej ilości ludzi.

1.1.Definicja plików cookie.

Pliki cookie to pliki tekstowe z małymi fragmentami danych, których zadaniem jest identyfikacja komputera podczas korzystania z sieci. Określone pliki cookie, znane jako pliki cookie HTTP, służą do identyfikacji określonych użytkowników i usprawnienia przeglądania stron internetowych.[1] Dane są tworzone przez serwer w momencie połączenia się z Internetem. W tej chwili użytkownik otrzymuje unikalny identyfikator, dzięki któremu można śledzić jego ruch. Ciasteczka zostały stworzone, aby ułatwić użytkownikowi korzystanie z przeglądarek np. uzupełniać loginy i hasła, aby nie było konieczności ich zapamiętywania i wpisywania za każdym razem, gdy chce ich użyć. Pliki cookie możemy podzielić na kilka grup:

- Plik cookie sesyjny to tzw. nietrwały plik cookie zapisany w pamięci tymczasowej sesji, co oznacza, że jest przechowywany tylko na czas przeglądania strony lub do czasu wylogowania się z aplikacji. System identyfikuje ten rodzaj plików na

[1] https://www.kaspersky.com/resource-center/definitions/cookies (dostęp 01.09.2022)

podstawie braku informacji o dacie ich wygaśnięcia. Ten rodzaj ciasteczek potrzebny jest do poprawnego działania aplikacji czy rozpoznawania użytkowników podczas logowania, dlatego są one obowiązkowe.

- Plik cookie stały to trwały plik tekstowy, który ma przypisany do siebie czas życia, po którym wygasa. Podczas jego czasu egzystowania będzie on zbierał i przekazywał informacje, za każdym razem, gdy użytkownik odwiedzi stronę, na której dany plik został zaimplementowany lub ogląda jakąś treść należącą do danego wydawcy (np. reklama). Z tego powodu nazywa się go często plikiem śledzącym, gdyż jest wykorzystywany przez marketingowców do zbierania cennych danych o nawykach ludzi, ich sposobie przeglądania, lokalizacji itp. Oprócz funkcji śledzącej plik ten usprawnia działanie niektórych funkcji przeglądarek internetowych np. zapamiętują dane logowania, abyśmy nie musieli ich każdorazowo wpisywać.
- Plik cookie stron trzecich – jest to plik, którego właścicielem jest firma, która należy do innej domeny niż strona, na której się znajduje użytkownik. Nie służy on do udostępniania żadnych funkcjonalności, a jedynie do identyfikacji użytkownika. Dzięki umieszczaniu swojego kodu na stronie strony trzeciej (często nazywany także partnerem) ma dostęp do wielu informacji o użytkowniku.

1.2.Historia plików cookie

Pierwszy raz ciasteczka zostały użyte w 1994 przez pracownika firmy Netscape Lou Montulli. Stworzył on „obiekt trwałego stanu klienta", który nazwał cookie. Jego celem było stworzenie wirtualnego koszyka zakupowego klienta. [2] W 1995 roku Montulli wystąpił o nadanie patentu na technologię śledzącą cookie[3]. Jeszcze w tym samym roku nowa technologia została zaimplementowana do przeglądarek Netscape Navigator i Internet Explorer 2.

[2] https://www.nytimes.com/2001/09/04/business/giving-web-a-memory-cost-its-users-privacy.html (dostęp 01.09.2022)

[3]https://worldwide.espacenet.com/publicationDetails/originalDocument?FT=D&date=20070809&DB=&locale=en_EP&CC=US&NR=2007185978A1&KC=A1&ND=1

Tim Jackson

This bug in your PC is a smart cookie

Dear Mr Jackson: Our in-store cameras have recorded your repeated visits to our fruit and vegetable counter. Yet even though you buy things in other departments – I hope last month's kid gloves came in handy during the cold snap! – we see that you have never bought fresh produce from us.

Three times last week, you stood in front of the fresh mangoes, but never took the plunge. So I'm writing to let you know about our upcoming special offer on tropical fruit.

As far as I know, no shopper has ever received such a letter. Camera technology is many years from being able to follow a single person around a department store, let alone tally that person's movements against sales records.

Yet these methods of keeping tabs on the behaviour of customers are possible today in cyberspace. Technology is already in place – and ready to be put to use on the World Wide Web of the Internet – that will allow Web site owners to gather an alarming range of information on the people who look at their Web pages from PCs at home.

Most Internet users are not aware that such possibilities exist. They believe, correctly, that when they surf the Web, the information sent from their PC to the Web site is an IP address – a string of digits that specify the Internet location of the computer they are logging in from. Tracking down the customer from that information alone is an inexact science, since a single IP address can be shared by hundreds of people working at a company, or thousands of people using an online service.

But the leading software used on the Web contains a little-known wrinkle that increases the power of companies to find out who their customers are and what they are up to. It allows companies to track which Web pages an individual looks at, when, for how long, and in what order.

That information can be tallied against information the customer provides of his own free will – for instance, when he "registers" for membership by giving a name and e-mail address, or provides a credit card number and a address when ordering a delivery – to produce a comprehensive record of individual behaviour.

Most extraordinary of all, this information can be stored on customers' own PCs without their knowledge. It can be kept in a form so that only the company that collected the information can benefit from it. And when the customer connects to the Web site later, the site can silently interrogate his PC and pick up the information.

The formal name for the objects where the information is stored is "persistent client-state hypertext transfer protocol cookies". Those who dismiss this as an early April Fool joke can find the specification describing the cookies by using the search engine on Netscape Communications' home page.

A technical note written in July 1995 describes the specification as preliminary, and warns users to treat it with caution. But the facility has been fully operational on Netscape browser software since version 1.2.

Each cookie, or nugget of information, can be up to four kilobytes and each server is allowed to deposit 20 cookies on every client computer. The total of 80 kilobytes that this represents is roughly equivalent to 18 articles the length of this one. But this limit can be circumvented by the simple device of having a number of different servers inside the company. As a result, a company can theoretically store 1.2 megabytes of information – twice the length of *Persuasion* – on each customer PC.

As a group, those who inhabit the online world tend to be watchful of their privacy. When they became aware last year that MSN, Microsoft's online service, was able to download a list of programs on customers' PCs as they logged in from home or work, there was such a fuss that the company was forced into a hasty damage-control exercise to reassure the world that its intentions were honourable.

Client-state cookies are in a slightly different category. They do not allow one company to snoop on another, and they gather only information about consumers' behaviour at a single company's Web site, or information that customers themselves volunteer.

But many PC users may take a dim view of Netscape's failure to draw their attention to the fact that their behaviour may be tracked in this way. Moreover, there appears to be only one way to disable the facility: by manually amending or deleting the *COOKIE.TXT* file containing all the cookies.

Netscape describes the system as "a powerful new tool which enables a host of new types of applications to be written for Web-based environments", and of course the company is right. Cookies allow customers to do repeat business with companies without having to retype their details. There are plenty of other very useful purposes to which the cookies could be put in future.

Yet the tale of these cookies is an illustration of the possibilities that Internet marketing opens up. In the old days, placing an advertisement was like firing a blunderbuss: remember the old quip that half the money spent on advertising was wasted, but that no-one knew which half. Today, technology has created silver bullets that allow companies to target people individually.

In the long term, this is a good thing, for it will tailor advertising more closely to what consumers want. But at stake is the issue of privacy which needs to be debated.

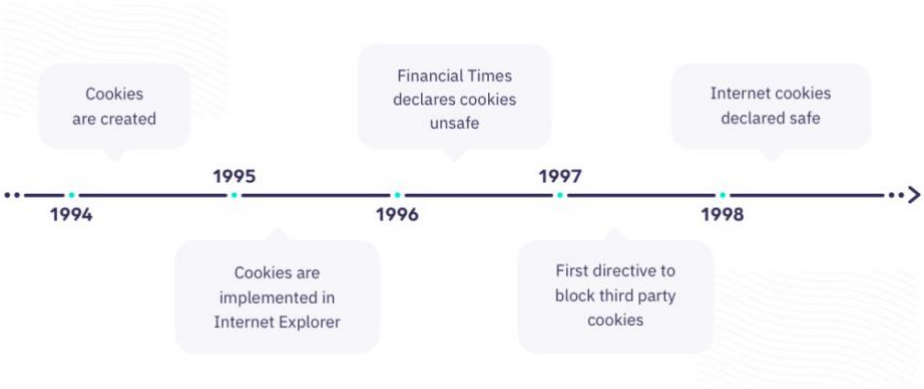
The only consolation is that breaches of privacy using this technology are unlikely to have any life-and-death consequences. The worst thing most companies will do, after all, is try to sell you something.

Tim Jackson can be reached at Tim.Jackson@zobaz.com

Rysunek 2 - Artukuł " The bug in your PC is a smart cookie" - Tim Jackson

Pierwszy raz o plikach śledzących opinia publiczna dowiedziała się w 1996 roku dzięki Timowi Jacksonowi, który na łamach gazety The Financial Times (Rysunek 2) oświadczył, że pliki cookie istnieją oraz wyjaśnił ich działanie.

W roku 1997 stowarzyszenie Internet Engineering Task Force, które nieformalnie zajmuje się ustalaniem standardów związanych z działalnością w Internecie stworzyła pierwszy wzór pliku cookie, który rekomendował zachowanie zbieranych informacji o użytkowniku dla siebie i niewymienianie się danymi z innymi użytkownikami sieci.



Rysunek 3 - Oś czasu powstawania plików cookie – źródło: https://newprogrammatic.com/blog/what-are-browser-cookies-in-digital-advertising/#:~:text=Cookies%20were%20created%20in%201994,in%20a%20virtual%20shopping%20cart.

Uzmysłowienie sobie faktu, że pliki cookie i informacje w nich zawarte mogą być dowolnie użyczane i wymieniane pomiędzy różnymi witrynami stało się wielką szansą dla wielu przedsiębiorstw, które widziały w tym ogromny potencjał marketingowy. Wkrótce agencje zaczęły używać ciasteczek do celów sprzedażowych, a także zaczęły je śledzić za pomocą kampanii reklamowych. Cały proces powstawania i implementacji ciasteczek można zauważyć na osi czasu (Rysunek 3), który wyraźnie pokazuje, że pliki cookie bardzo szybko zaczęły niepokoić użytkowników swoim działaniem.

W 2002 Unia Europejska ustanowiła pierwsze rozporządzenie mówiące o tym, że pliki cookie dotyczą danych osobowych i umożliwiła użytkownikom wyrażanie niezgody na zbieranie takowych danych.[4] Witryny internetowe powinny od tego dnia zawierać informację o zbieraniu danych osobowych oraz o formach ich przetwarzania. Jeżeli użytkownik nie wyraził zgody na zbieranie danych, przeglądarki mogły wykorzystywać ciasta jedynie do transmisji łączności i zapewnienia podstawowych funkcji strony internetowej. Jednak nawet status prawny ciasteczek nie zmusił wydawców, do ograniczenia zbierania danych od swoich użytkowników. Przedsiębiorstwa dokonywały licznych naruszeń, które nie były właściwie ścigane przez podmioty za to odpowiedzialne. Dodatkowo witryny utrudniały użytkownikom

[4] DYREKTYWA 2002/58/WE PARLAMENTU EUROPEJSKIEGO I RADY z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej)

rezygnację z ciasteczek, umieszczając je na stronie tak, aby użytkownik miał duże problemy ze znalezieniem ich.

7 lat później w 2009 roku z polecenia Federalnej Komisji Handlu i Unii Europejskiej powstała Dyrektywa Parlamentu Europejskiego i Rady 2009/136/WE, która miała zastąpić nieskuteczną wersję z 2002 roku. Głównym założeniem nowego prawa była zmiana sposobu zbierania zgód użytkownika na wykorzystanie plików cookie stron trzecich. Od teraz użytkownik musiał wyrazić świadomą zgodę na przekazywanie i wykorzystywanie swoich danych oraz powinien otrzymać jasne i wyczerpujące informacje, między innymi o celach ich przetwarzania.[5] Dokładnie wtedy zaczęła się era tzw. „wyskakujących okienek" na każdej stronie internetowej, które zawierały powyższe informacje. Dzięki tej decyzji jedynie osoby wyrażające zgodę mogły być podmiotem działań marketingowych.

Dzięki presji użytkowników od 2015 firmy technologiczne zaczęły zauważać, że użyteczność plików cookie znacznie wykracza poza pierwotne cele ich stosowania. Zamiast jedynie polepszać odczucia użytkownika podczas korzystania z Internetu, systemy analizujące dane zaczęły profilować ludzkość i używać przetworzonych danych w celu manipulacji decyzjami zakupowymi, politycznymi, a także światopoglądem.

Apple była pierwszą firmą, która zapoczątkowała cookieless-ową rewolucję. Zaczęła od blokowania reklam pochodzących z innych źródeł niż ich własna sieć. Następnie blokowała wszystkie pliki cookie third-party, aby finalnie ograniczyć możliwość używania nawet plików cookie first-party. W ślad za smartphonowym gigantem poszły inne firmy technologiczne, które stopniowo wycofują używanie third-party cookies. Największa firma oferująca aukcje reklamowe, czyli Google zapowiedziała całkowite wycofanie tych plików na 2023 rok.

1.3.Dane zawarte w plikach cookie

Możliwości rodzajów zbieranych danych o użytkownikach są w tym momencie nieograniczone. Głównie zależy on jedynie od poziomu zaawansowania systemów skanujących. Niestety kwestie prawne nie regulują tego, jakie dane mogą być zbierane, a jedynie sposób ich używania, dlatego firmy mogą zbierać dowolne informacje, jeżeli tylko otrzymają na to zgodę. Przykładami zbieranych danych są:

- Identyfikator użytkownika,

[5] DYREKTYWA PARLAMENTU EUROPEJSKIEGO I RADY 2009/136/WE z dnia 25 listopada 2009 r.

- Informacje o urządzeniu: model, system operacyjny, rozdzielczość, IP,
- Informacje o koncie: adres email, data urodzenia, numer telefonu,
- Dane geolokalizacyjne – kraj, kod pocztowy, miasto, współrzędne geograficzne,
- Historia wyszukiwania,
- Historia aktywności na stronie: wyświetlenia, kliknięcia, inne zachowania na stronie,
- Decyzja o zakupie,
- Informacje o stronie internetowej i jej zawartości.

Połączenie powyższych informacji z metadanymi „może określić dokładny profil osoby, obejmujący także jego cechy osobowościowe, opis przyzwyczajeń i indywidualnego trybu życia”[6].

1.4.Podstawy prawne mówiące o plikach cookie stron trzecich

W Polsce i Europie głównym aktem prawnym regulującym ochronę danych osobowych i ich przepływ w Internecie jest Rozporządzenie parlamentu europejskiego i rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. Według prawa europejskiego danymi osobowymi nazywamy „informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”)[7]”. Oznacza to, że zbierane przez firmy dane muszą być na tyle anonimowe lub przetworzone w procesie pseudonimizacji, aby niemożliwe było zidentyfikowanie osoby, do której dane należą.

Głównymi założeniami rozporządzenia są:

- prawo do niepodlegania decyzji opartej na profilowaniu –
- obowiązek poinformowania użytkownika – użytkownik powinien być każdorazowo poinformowany w jakim celu będą zbierane i przetwarzane jego dane osobowe,
- zebranie zgody – każdy podmiot, który przetwarza dane osobowe, które nie służą do poprawnego funkcjonowania witryny powinien uzyskać uprzednio „dobrowolną, świadomą i jednoznaczną” zgodę użytkownika w formie pisemnej lub ustnej. Dodatkowo zgoda, która zazwyczaj pojawia się po wejściu na stronę

[6] Katarzyna Szymielewicz, W. A. (2017). Śledzenie i profilowanie w sieci. W czym problem? Co się zmieni w prawie? Jak może wyglądać przyszłość? Warszawa: Fundacja Panoptykon

[7] PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ. "ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych iw sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)."

nie powinna zakłócać jej funkcjonowania. W Europie mamy do czynienie ze zgodą typu opt-in, czyli użytkownik musi wyrazić dobrowolną chęć na zbieranie plików cookie. Zignorowanie zgody będzie równoznaczne z jej niewyrażeniem,

- prawo do bycia zapomnianym – każdy użytkownik ma prawo prosić podmiot gromadzący jego dane o usunięcie ich z systemu,
- naruszenie danych – w przypadku utraty, kradzieży bądź nielegalnego dostępu do danych, administrator ma obowiązek natychmiast powiadomić krajowy organ nadzoru danych oraz osobę, której dane dotyczą, jeżeli wyciek wiąże się z wysokim ryzykiem[8].

W Stanach zjednoczonym nie istnieje federalne prawo mówiące o ochronie danych osobowych. Jednak powszechnie stosuje się California Consumer Privacy Act, ponieważ regulacje w nim zawarte stosują się do każdego użytkownika w stanie California. Jeżeli przedsiębiorstwo chce zbierać dane rezydentów tego regionu musi podporządkować się pod to rozporządzenie. Oprócz tego warunku firma musi spełnić jeszcze jeden z poniższych warunków, aby podlegać pod to prawo:

- Ma roczny przychód brutto w wysokości co najmniej 25 mln USD,
- Kupuje, otrzymuje lub sprzedaje dane osobowe od ponad 50 000 konsumentów, gospodarstw domowych lub urządzeń w Kalifornii,
- Zarabia 50% lub więcej swoich rocznych przychodów ze sprzedaży danych osobowych[9].

Kalifornijska ustawa jasno mówi, że dane zbierane za pośrednictwem plików cookie to dane osobowe. Głównymi założeniami regulacji są

- prawo dostępu do danych oraz informacji w jaki sposób są wykorzystywane,
- prawo żądania ich usunięcia,
- prawo do uniemożliwienia ich sprzedaży osobom trzecim,
- prawo do niedyskryminacji w wykonywaniu swoich praw CCPA[10].

[8] https://europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-online-privacy/index_pl.htm#shortcut-10 (dostęp 27.09.2022)
[9] https://www.cookieyes.com/blog/what-is-ccpa/#ccpa-steps (dostęp 28.09.2022)
[10] California Consumer Privacy Act (CCPA)

W odróżnieniu od europejskiego prawa, nie jest tam wymagane uzyskanie zgody od użytkownika. W rozumieniu amerykańskiego prawa zgoda działa na zasadzie opt-out, co oznacza, że użytkownik ma prawo do zrezygnowania ze zbierania danych osobowych.

W Azji jedną z ustaw regulujących prawo do ochrony prywatności jest Ustawa o ochronie danych osobowych (PDPA) działająca na terytorium Singapuru. Jej głównymi zasadami są:

- obowiązek odpowiedzialności,
- obowiązek powiadomienia,
- obowiązek wyrażenia zgody,
- obowiązek ograniczenia celu,
- obowiązek dokładności,
- obowiązek ochrony,
- obowiązek ograniczenia retencji,
- obowiązek ograniczenia transferu,
- obowiązek dostępu i korekty,
- obowiązek powiadomienia o naruszeniu danych,
- obowiązek przenoszenia danych.

Inne kraje azjatyckie również posiadają swoją politykę danych, jednak organy ścigające nadużycia w tym aspekcie nie są aż tak restrykcyjne, jak organy europejskie czy amerykańskie.

1.5.Zastosowanie plików cookie:

Podstawowymi funkcjami plików cookie są:

- Zarządzanie sesją – pierwotną funkcją ciasteczek było umożliwienie dodawania produktów do wirtualnego koszyka w celu zrobienia zakupów w sklepie internetowym. W dzisiejszych czasach informacja o produktach w koszyku przechowywana jest w bazie danych na serwerze, a pliki cookie służą jedynie do identyfikacji jego właściciela. Każdorazowa wizyta klienta na stronie wywołuje komunikację serwerów w celu rozpoznania klienta i wyświetlenia mu spersonalizowanej oferty produktowej. Jednak nie tylko sklepy internetowe używają ciasteczek do rozpoznawania powracających użytkowników. Przy pierwszym logowaniu się do witryny internetowej, użytkownik otrzymuje unikatowy numer, dzięki któremu serwer może zapamiętać jego dane, udostępnić mu dostęp do usług oraz usprawnić jego poruszanie się po serwisie. Dzięki temu nie musi się od logować do niego po każdym odświeżeniu strony.

- Personalizacja – dzięki plikom cookie możemy personalizować swoje ustawienia dotyczące wyświetlania i działania serwisów internetowych. Działa to także w drugą stronę. Algorytmy tworzą obraz użytkownika i na jego podstawie dopasowują treści, reklamy czy wyniki wyszukiwania.
- Analityka danych– dzięki unikatowym identyfikatorom możliwe jest śledzenie zwyczajów zachowania się użytkowników w Internecie. Dzięki specjalnie zaimplementowanym skryptom w kodzie źródłowym strony internetowej możemy precyzyjnie sprawdzać, co oglądał odwiedzający, jak długo, co przykuło jego uwagę, czy skąd przyszedł. W wyniku tego istnieje możliwość tworzenia wielopoziomowych statystyk o osobach odwiedzających stronę i wykorzystywanie danych do własnych celów.
- Cele marketingowe – dzięki informacjom dostarczanym w plikach cookie, działy promocji mogą łatwo określić, czym są zainteresowani potencjalni klienci i na tej podstawie wyświetlać im odpowiednią reklamę. Poprzez pliki śledzące mogą oni kontrolować, gdzie i kiedy użytkownik zobaczył przekaz.

1.6.Nadużywanie plików cookie

Europejskie rozporządzenie o ochronie danych osobowych (GDPR) jest jednym z najsurowszych na świecie. Zgodnie z nią organ ma prawo nałożyć grzywny na przedsiębiorstwa w wysokości do 20 mln euro (około 20 372 000 USD) lub 4% światowych obrotów za poprzedni rok obrotowy – w zależności od tego, która z tych wartości jest wyższa.[11]Jednak firmy technologiczne niejednokrotnie nie przestrzegają obowiązujących przepisów przy tym łamiąc prawo użytkownika do ochrony jego prywatności. Robią to, ponieważ przychód z nielegalnie użytych danych jest wielokrotnie wyższy niż otrzymane kary. W przeciągu ostatnich kilku lat wiele największych firm otrzymało ogromne kary przez organy ścigające, ale nie tylko. Łącznie kar na łamanie przepisów GDPR było prawie 1400[12].

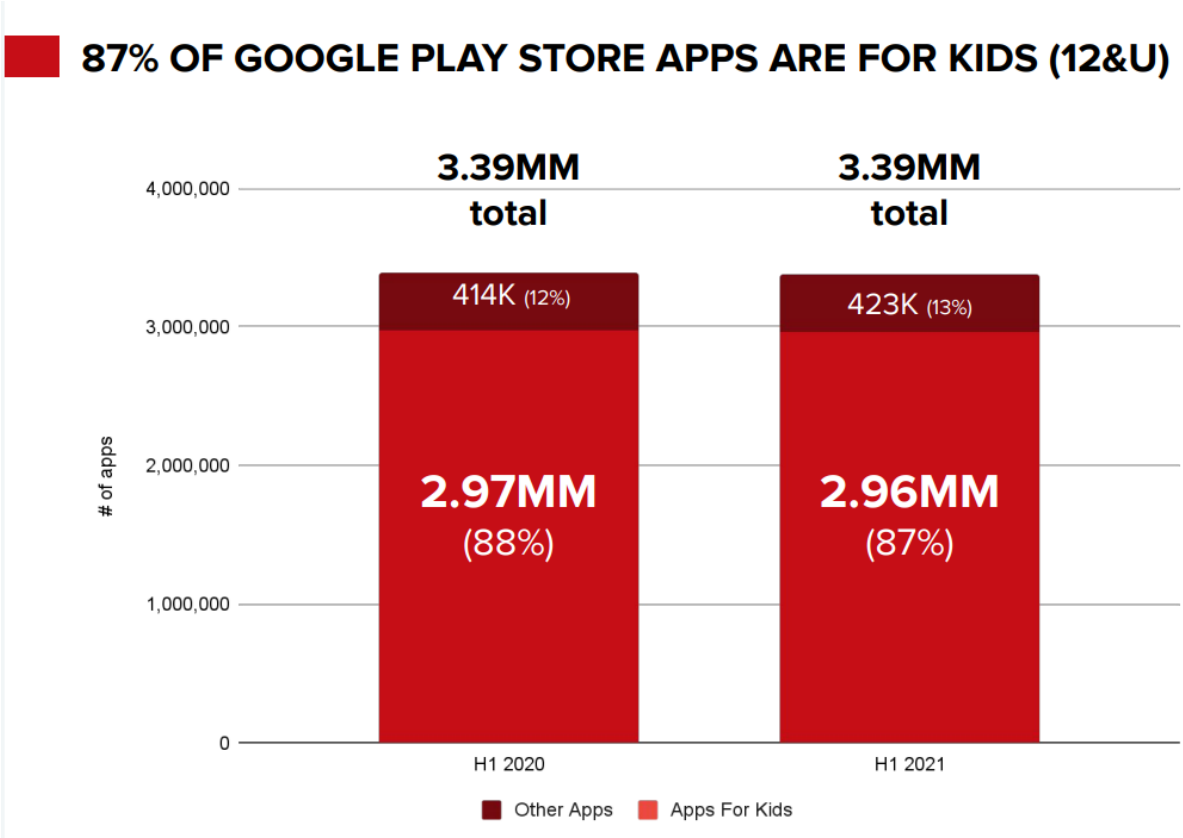
Największą karą w historii została obarczona firma Amazon[13]. W raporcie rocznym, który wykazała firma znalazła się gigantyczna kwota 746 milionów euro. Za oficjalną przyczynę

[11] Regulation (EU) 2016/679 (General Data Protection Regulation)
[12] https://www.enforcementtracker.com/ (dostęp 19.09.2022)
[13] https://www.sec.gov/ix?doc=/Archives/edgar/data/0001018724/000101872421000020/amzn-20210630.htm#i5986f88ea1e04d5c91ff09fed8d716f0_103 (dostęp 19.09.2022)

nałożenia kary podano „niezgodność z ogólnymi zasadami przetwarzania danych". Dokładny powód przyznania tak ogromnej grzywny nie jest znany dla opinii publicznej.

W 2022 roku Irlandzki Komisarz Ochrony Danych ukarał kolejną firmę, którą był Instagram (przedsiębiorstwo należące do spółki Meta). Otrzymali oni karę 402 milionów dolarów za naruszenie ogólnego rozporządzenia o ochronie danych (RODO) poprzez nieprawidłowe przetwarzanie danych dzieci aktywnych na platformie. Zarząd spółki odwołał się od decyzji sądu pierwszej instancji, jednak 15 września 2022 sąd w Brukseli rozstrzygając spór uznał firmę Meta winną zarzucanych im czynów i nałożył na spółkę karę w wysokości 405 milionów dolarów. [14] Decyzja dotyczyła sprawy publicznego ujawnienia przez Instagram adresów e-mail i/lub numerów telefonów dzieci korzystających z funkcji konta biznesowego na Instagramie oraz domyślnego ustawienia publicznego dla osobistych kont dzieci na tej platformie. Przewodnicząca Europejska Rada Ochrony Danych Andrea Jelinek skomentowała całą sprawę w następujący sposób „To historyczna decyzja. Nie tylko ze względu na wysokość grzywny – jest to druga najwyższa grzywna od wejścia w życie RODO – jest to również pierwsza ogólnounijna decyzja w sprawie praw dzieci do ochrony danych. Dzięki tej wiążącej decyzji EROD wyraźnie stwierdza, że firmy skierowane do dzieci muszą zachować szczególną ostrożność. Dzieci zasługują na szczególną ochronę w odniesieniu do ich danych osobowych." Warto dodać, że wg raportu Pixalate przedstawionym na rysunku 4 aż 87% aplikacja znajdujących się na sklepie Google stanowią aplikacje skierowane do dzieci. Z tego samego raportu wynika, że 20% aplikacji dostępnych w sklepie Google nie posiada żadnej polityki prywatności, co stanowi ogromną lukę w egzekwowaniu prawa ochrony prywatności dzieci[15].

[14] https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-decisions_en (dostęp 27.09.2022)
[15] Raport Global mobile ad supply chain: Privacy & Safety on apps for children – Google Play store



Rysunek 4 - MOBILE PRIVACY & SAFETY ON APPS FOR KIDS: GOOGLE PLAY STORE (H1 2021), źródło: pixalate.com

Firma Google została już kilkakrotnie ukarana grzywnami przez różne organy ścigania na świecie. W samej Europie technologiczny gigant musiał zapłacić 7 różnych kar za nieprzestrzeganie prawa GDPR.

Największą z tych kar nałożył w 2022 roku Francuski urząd ochrony danych. Przedsiębiorstwo zostało obciążone kwotą 90 milionów euro za nieprawidłowe wdrożenie procesu uzyskiwania zgód przez użytkowników w serwisie YouTube. Francuski urząd trafnie zauważył, że wyrażenie zgody na zbieranie danych jest proste i dostępne dzięki jednemu kliknięciu, jednak odrzucenie polityki prywatności i zgody na ich zbieranie wymagało kilku kliknięć. Sąd uznał, że brak wyrażenia zgody powinno być tak proste do wykonania, jak zgoda.

Kolejną firmą ukaraną gigantyczną grzywną w wysokości 60 milionów euro jest Facebook. Powód był identyczny, jak w przypadku firmy Google – utrudniona procedura niewyrażania zgody na zbieranie plików cookie.

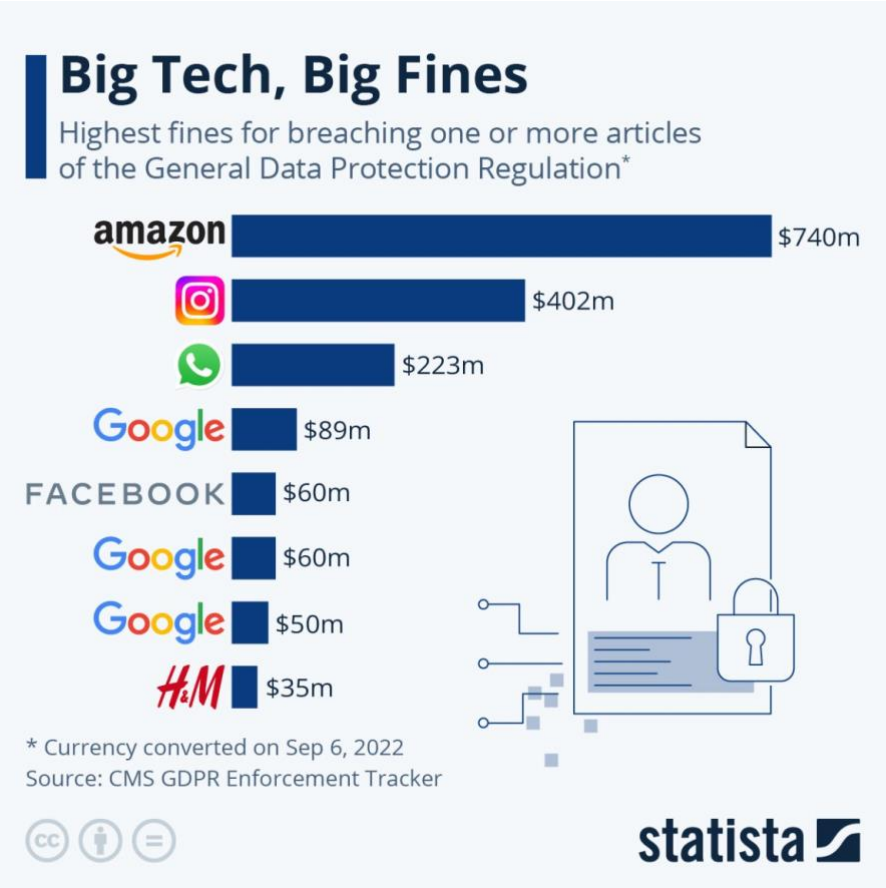
W 2020 roku Urząd Ochrony Danych w Hamburgu w Niemczech wymierzył karę ponad 35 milionów dolarów na sprzedawcę odzieży H&M. Jeden z największych retaillerów na świecie naruszał RODO przez kontrolowanie swoich pracowników. Pracownicy, którzy wracali

z urlopów lub zwolnienia chorobowego byli zmuszani do spotkania, którego tematem był powrót do pracy. Niektóre ze spotkań zostały nagrane i udostępnione zespołowi menadżerów. Zarząd zdobył dzięki temu ogromną wiedzę, na temat swoich pracowników. Wiele informacji było nieistotnych, jednak wiedza na temat wierzeń religijnych, czy sprawy rodzinne do błahych już nie należą. Ten profil pracowników był wykorzystywany do wielu decyzji odnośnie ich zatrudnienia, czy ocenę ich pracy. Firma H&M w tym przypadku nie przestrzegała zasady minimalizacji danych. H&M powinien zapewnić tym danym również należytą kontrolę i szczegółowo sprawdzać, kto ma do nich dostęp. Ostatnim aspektem jest to, że cechy osobiste, czy ich różnorakie preferencje nie powinny mieć żadnego znaczenia w podejmowaniu decyzji związanych z zatrudnieniem.

Jako kolejny przypadek łamania praw do ochrony danych można wymienić firmę Wind. Włoska firma telekomunikacyjna została ukarana kwotą 17 milionów euro za naruszenie praw prywatności w zakresie marketingu bezpośredniego. Użytkownicy skarżyli się, że bez ich zgody wysyłane są do nich setki reklam tzw. spam, czyli każdy rodzaj nichcianej komunikacji internetowej, która jest rozpowszechniana masowo za pośrednictwem poczty email, mediów społecznościowych, czy telekomunikacji.[16], a gdy chcieli oni zrezygnować, napotykali na nieprawidłowe dane firmy, przez które nie mogli zrezygnować z otrzymywania natrętnych reklam.

Na rysunku 5 pokazane zostały najwyższe kary przyznane przez organy ścigające nadużycia używania plików cookie. Szczególnie można zauważyć, że do rekordzistów należą przedsiębiorstwa należące do tzw. walled garden, czyli gigantyczne firmy z treściami przeznaczonymi tylko dla zalogowanych użytkowników.

[16] https://www.malwarebytes.com/spam (dostęp: 27.09.2022)



Rysunek 5 - Największe kary za nieprzestrzeganie GDPR, źródło: https://www.statista.com/chart/25691/highest-fines-for-gdpr-breaches/

Jednak problem z plikami cookie sięga dużo dalej. W 2019 roku nowozelandzka dziennikarka Talia Shadwell opublikowała na łamach Daily Mirror artykuł o bardzo niepojącej sytuacji. Według autorki pewnego dnia zaczęły pojawiać się jej reklamy sponsorowane produktów dla niemowląt, witamin czy książek dla dzieci, mimo że nie posiadała ona żadnych potomków. Wyświetlanie się spersonalizowanych reklam trwało kilka dni, aż Talia zorientowała się, że zapomniała dodać informacji o swojej miesiączce w aplikacji śledzącej cykl menstruacyjny. Zaraz po zaktualizowaniu danych reklamy przestały się pojawiać.[17] Dziennikarka może jedynie spekulować, dlaczego jej oczom ukazywały się głównie spersonalizowane reklamy dla matek. Mimo, że aplikacja, której używała gwarantowała poufność danych, ewidentnie zostały one udostępnione stronom trzecim. Do wielu aplikacji użytkownicy mają darmowy dostęp, a ich funkcje skutecznie ułatwiają nam życie. Jednak tak

[17] https://primer.com.au/period-tracker-data-shared-google-facebook/ (dostęp 19.09.2022)

naprawdę za używanie tych programów zapłatą są własne dane osobowe, które wykorzystywane są do tworzenia skutecznych kampanii marketingowych.

Reklama targetowana była także jednym z powodów wygranej Donalda Trumpa w wyborach prezydenckich w 2016 roku. Sztab wyborczy stworzył precyzyjny plan marketingowy, który przy użyciu reklamy personalizowanej miał celować do 13,5 miliona niezdecydowanych wyborców i przekonać ich, aby swój ostateczny głos oddali właśnie na tego kandydata. W książce „Śledzenie i profilowanie w sieci" autorka wspomina, że „architekci kampanii publicznie chwalili się możliwościami niejawnego wpływania na poglądy i postawy wyborców" (Katarzyna Szymielewicz, 2017).

Podobną strategię zastosowała firma Cambridge Analytica podczas kampanii Leave.EU. Stosując dokładnie przygotowaną kampanię opartą na dokładnej analizie grupy i mikrotargetowaniu. Kampania miała na celu odpowiednio zrozumieć odbiorców, aby finalnie przekonać ich do zagłosowania za wyjściem z Unii Europejskiej. Zadaniem kampanii było manipulowanie ich wartościami, przekonaniami i decyzjami. Sama firma mówi o sobie „Cambridge Analytica jest specjalistą w dostarczaniu kreatywnych rozwiązań opartych na badaniach dla rządów, wojska, partii politycznych i firm komercyjnych, aby przekonać kluczowe grupy odbiorców do wymiernej zmiany ich zachowania."[18] Firma chwali się, że do budowy zaawansowanych obrazów wyborców używa ogromnych ilości danych w tym: „konsumenckie historie, informacje o stylu życia, sprawozdania ze spisów i historyczne zapisy głosowania".

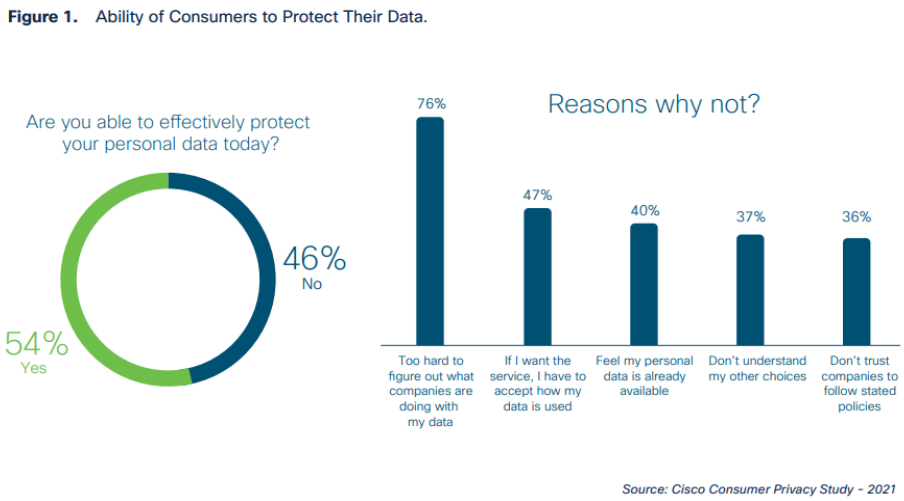
Jak można zauważyć większość grzywn przyznanych przez organy ścigające, wynikają z nieprzejrzystej polityki zbierania zgód lub utrudnianie jej niewyrażenia. Jednak oficjalnie podane powody pozwalają nam wysnuwać różnorakie hipotezy, dlaczego firmom tak zależy na posiadaniu danych użytkownikom. Zbieranie zgód jest oczywistą formalnością narzucaną przez prawo, a utrudnianie zarządzania nimi pomaga przedsiębiorstwom zachować do nich dostęp. Ponadto profilowanie użytkowników nie ogranicza się do manipulacji jedynie ich decyzjami zakupowymi. Powyższe przykłady dowodzą, że przedsiębiorstwa analityczne i marketingowe inwigilują ludzi, a przez zaawansowane metody statystyczne i psychologiczne mogą manipulować naszym światopoglądem, wartościami oraz decyzjami mającymi wpływ nie tylko

[18] https://www.parliament.uk/globalassets/documents/commons-committees/culture-media-and-sport/BK-Background-paper-CA-proposals-to-LeaveEU.pdf (dostęp 27.09.2022)

na nas samych, ale na całe społeczeństwo. Kolejnymi zarzutami wobec firm technologicznych są: szerzenie propagandy, nieetyczne praktyki handlowe oraz brak świadomości społecznej.

1.7.Potrzeba wycofania plików cookie stron trzecich

Celem wycofania plików cookie stron trzecich jest zapewnienie należytej prywatności użytkowników, która w wielu krajach widnieje jako podstawowe prawo człowieka.



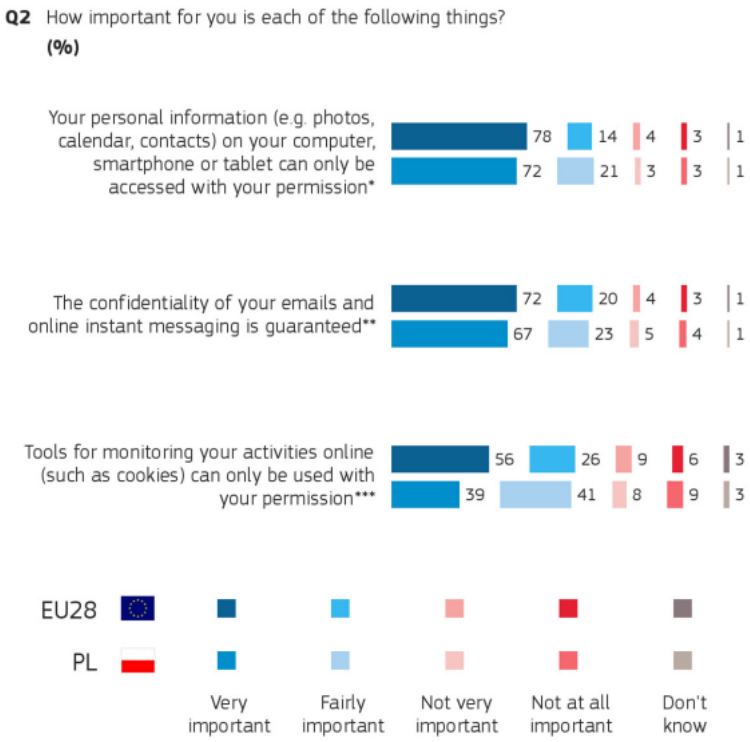
Rysunek 6 - Ability of Consumers to Protect Their Data, źródło: Cisco Consumer Privacy Study - 2021

Według badań wykonanych przez firmę Cisco (Rysunek 5) 46% pytanych uważa, że nie jest w stanie efektywnie zarządzać swoimi danymi osobowymi. Za główny powód, dlaczego tak jest podają brak należytej informacji, w jaki sposób dane są wykorzystywane i przetwarzane. Kolejnym powodem jest uzyskanie pełnej funkcjonalności usługi, jedynie po akceptacji wszystkich zgód na zbieranie danych.

Jedno z badań pokazało, że aż 89 procent uczestników uważa, że ich prywatność została naruszona w erze informacji. (Udo, 2001)[19] Inne badanie wykazało, że nastawienie klientów

[19] Privacy and security concerns as major barriers for e-commerce: A survey study [dostęp: 25.09.2022]

do spersonalizowanej reklamy będzie negatywne, jeżeli mają obawy dotyczące swojej prywatności. (Martin, 2017)



Rysunek 7 - Ankieta w celu oceny ogólnych opinii obywateli w całej UE w odniesieniu do kluczowych kwestii, które są częścią prywatności w Internecie, źródło: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex:32009L0136

Jak wynika z badań Komisji Europejskiej (Rysunek 6) ochrona danych osobowych jest dla Polaków bardzo ważna. Większość zgadza się, że chciałoby mieć wpływ na zbieranie danych i móc dobrowolnie wyrazić na to zgodę.

Jak donoszą wielokrotnie prowadzone eksperymenty naukowe targetowanie behawioralne powoduje także dyskryminację cenową. Te same produkty lub usługi są oferowane użytkownikom w różnych cenach, bazując na wcześniejszej analizie i prescoringu[20]. Dzieje się tak, gdyż algorytmy uważają, że Ci użytkownicy są bardziej chętni do skorzystania z oferty. Takie sytuacje mogą być również motywowane przez indywidualne czynniki np. model telefonu, który wskazywałby na status społeczny użytkownika.

1.8.Urządzenia mobilne, a pliki cookie

W środowisku mobilnym także wykorzystuje się tradycyjne pliki cookie. Działają one w taki sam sposób co w środowisku webowym. Jednak dotyczy to jedynie przeglądarek

[20] Punktacja wskazująca na prawdopodobieństwo wystąpienia konkretnej sytuacji.

internetowych. Firmy do śledzenia swoich użytkowników na urządzeniach mobile wykorzystują unikatowe identyfikatory reklam mobilnych, które dają możliwość pseudoanonimowego uzyskiwania danych pochodzących z tego urządzenia. Użytkownicy mają możliwość zmiany swojego identyfikatora w dowolnym momencie, a także usunięcia go, aby nie być przedmiotem personalizacji. W zależności od rodzaju systemu rozróżniamy dwa rodzaje identyfikatorów:

- AAID/GAID – jest to unikatowy numer nadawany dla użytkowników smartfonów z oprogramowaniem Android,
- IDFA - jest to unikatowy numer nadawany dla użytkowników smartfonów marki Apple.

Dzięki numerom identyfikacyjnym administrator danych ma możliwość zbierania danych o aktywności użytkowników. Do zbieranych informacji należą m.in. dane o urządzeniu, lokalizacja, czas, informacje o aplikacji, a także różne informacje o naszych działaniach np. szybkość przesuwania palcem po ekranie.

Główną różnicą między plikiem cookie, a mobilnym identyfikatorem jest jego czas życia. Pliki cookie zawsze mają określony czas działania w odróżnieniu od wersji mobilnej. Dlatego tak ważna jest świadomość o zbieraniu danych, gdyż w przypadku tych drugich to użytkownik może sam zmienić unikalny numer. Dodatkowo przedsiębiorstwa marketingowe mogą w łatwy sposób zidentyfikować użytkownika i znaleźć jego odpowiednik w środowisku webowym, co pozwala na jeszcze skuteczniejsze śledzenie i personalizowanie kreacji.

Podsumowując pliki cookie to krótkie pliki tekstowe, zapisywane w pamięci komputera lub urządzenia służące do poprawnego funkcjonowania witryn internetowych, a także umożliwiają śledzenie użytkownika w sieci. Dzięki plikom cookie stron trzecich możliwe jest obserwowanie zachowań ludzi na różnych stronach i dzielenie się tymi informacjami z innymi.

W rozdziale pierwszym szczegółowo opisane została definicja plików cookie oraz ich rodzaje. Wymienione zostały przypadki nadużyć stosowania plików cookie przez przedsiębiorstwa, a także przyczyny powstania pomysłu wycofania plików śledzących. Na podstawie badań przedstawiona została opinia publiczna na temat praktyk stosowanych w reklamie behawioralnej, a także zagrożenia jakie może ona przynosić, nie tylko na zasobność portfeli ludzi, ale także na ich światopogląd czy preferencje seksualne.

2. Retargeting, a pliki cookie stron trzecich

Marketing internetowy to wszelkie działania mające na celu opracowanie strategii dla wprowadzenia produktu na rynek, jego promocji oraz przedstawienie w korzystny sposób marki przy wykorzystaniu Internetu. „Działania w marketingu internetowym zmierzają do zwiększenia widoczności firmy w Internecie, a jednym z najczęściej używanych w tym celu narzędzi jest między innymi strona WWW”[21]. Marketing internetowy skupia się na kreowaniu oraz utrzymywaniu więzi pomiędzy marką, a klientem. W przeciwieństwie do marketingu tradycyjnego, w marketingu internetowym rola odbiorcy jest znacznie większa. Odbiorca internetowy ma możliwość prowadzenia dialogu z firmą oraz wyrażenia swojej oceny na jej działanie[22].

Przykładami marketingu internetowego są przede wszystkim:

- reklamy banerowe (display),
- e-mail marketing,
- social media,
- artykuły sponsorowane wraz z linkami,
- pozycjonowanie stron WWW i SEO,
- reklamy Ads,
- marketing afiliacyjny,
- video marketing,
- remarketing,
- retargeting,
- współpraca z blogosferą,
- marketing wirusowy,
- content marketing.

Większości rodzajów marketingu używa się, aby zwabić użytkownika do naszego sklepu, w celu dokonania zakupu. Jednak jak wynika z najnowszych badań jedynie 4% odwiedzających witrynę po raz pierwszy dokonuje decyzji zakupowej.[23] Pozostałe 96% użytkowników stanowi dla marketerów duże wyzwanie, ale też ogromną szansę. Są to bowiem potencjalni klienci,

[21] https://www.eactive.pl/blog-o-seo/co-to-jest-marketing-internetowy/
[22] https://www.eactive.pl/pozycjonowanie-stron/co-to-jest-marketing-internetowy/
[23] https://www.criteo.com/what-is-retargeting/

których uwagę już przykuł dany produkt, a przekonanie ich do powrotu do sklepu i dokończenia procesu zakupowego może przyczynić się do zwiększenia przychodów firmy. Retargeting jest skutecznym narzędziem, ponieważ inwestujemy w reklamę kierowaną do osób już zainteresowanymi naszymi produktami, co oznacza, że użytkownik zna już markę i jest gotów jej bardziej zaufać.

2.1.Definicja retargetingu

Retargeting to inaczej reklama behawioralna. Definiowana jest jako forma reklamy bazująca na badaniu zachowań użytkowników Internetu i polegająca na oferowaniu im reklam powiązanych z ich zainteresowaniami." (Namysłowska, 2012)

Definicja Google mówi, że „Remarketing umożliwia wyświetlanie reklam osobom, które odwiedziły Twoją witrynę lub korzystały z Twojej aplikacji mobilnej. Na przykład, gdy użytkownicy opuszczają Twoją witrynę bez kupowania czegokolwiek, remarketing pomaga Ci ponownie nawiązać z nimi kontakt, wyświetlając trafne reklamy na różnych urządzeniach.[24]

Obie definicje zgadzają się ze sobą, że retargeting to umiejętność odzyskania potencjalnego klienta przy pomocy danych zebranych o użytkowniku. Mogłoby się wydawać, że wielokrotne atakowanie użytkownika reklamą tego samego produktu sprawi, że zacznie on ignorować ten komunikat i skutecznie zniechęci go od dokonania zakupu. Działa to jednak odwrotnie, dzięki zjawisku znanym z psychologii tzn. „efektem zwykłej ekspozycji". Według słownika psychologii APA jest to „odkrycie, że osoby wykazują zwiększoną preferencję (lub upodobanie) do bodźca w wyniku powtarzającej się ekspozycji na ten bodziec. Ten efekt jest najbardziej prawdopodobny, gdy nie istnieje wcześniej negatywny stosunek do obiektu będącego bodźcem, który zwykle jest najsilniejszy, gdy osoba nie jest świadomie świadoma prezentacji bodźca."[25] Oprócz oswajania osoby z towarem, dodatkowo budujemy jego świadomość o brandzie.

Często nazwa remarketingu używana jest zamiennie z retargetingiem, jednak w środowisku specjaliści rozróżniają te dwa pojęcia. Obie formy to strategia konwersji osoby, która jeszcze nie dokonała zakupu, jednak już odwiedziła witrynę. Remarketing próbuje skłonić odwiedzających do złożenia zamówienia za pośrednictwem poczty e-mail. Strona internetowa korzysta z własnych danych i przypomina użytkownikowi, że nie dokończył zakupów.

[24] https://support.google.com/google-ads/ (dostęp 19.09.2022)
[25] https://dictionary.apa.org/mere-exposure-effect (dostęp 19.09.2022)

Retargeting próbuje przekonać odwiedzającego do złożenia zamówienia za pośrednictwem reklam banerowych i natywnych na innych stronach lub aplikacjach, niż ich własne. Taka forma reklamy wymaga przekazania informacji o użytkowniku stronom trzecim.[26]

2.2.Wykorzystanie plików cookie w remarketingu

Działanie mechanizmu retargetingu można opisać w następujący sposób:

1. Witryna umieszcza w kodzie swojej strony krótki fragment kodu nazywany pikselem remarketingu.
2. Za pierwszym razem, gdy użytkownik odwiedza daną witrynę: produkt lub usługę, pobierany jest indywidualnie przypisany piksel, który informuje o tym co przeglądał, skąd przyszedł, czy jak dużo czasu spędził na stronie.
3. Za każdym razem, gdy użytkownik odwiedza inną witrynę lub aplikację, plik cookie informuje sieć reklamową, że dany użytkownik jest aktywny i może być zainteresowany reklamą. W tym momencie mamy możliwość wyświetlenia użytkownikowi reklamę ztargetowaną z produktami, którymi był wcześniej zainteresowany.

Sam sposób działania retargetingu wydaje się mało skomplikowany i potencjalnie niegroźny. Wydaje się, że użytkownikowi została wyświetlona reklama produktu, którego zakup rozważał. Na pierwszy rzut oka nie widać zagrożenia wynikającego ze zbierania naszych danych, jednak domniemanych klientów zainteresowanych produktem lub usługą może być wielu. Wyzwaniem retargetingu stało się, aby w danym momencie dostosować pokazywaną reklamę konkretnemu użytkownikowi, który wykazuje największe prawdopodobieństwo wykonania konwersji. W tym celu używa się targetowania behawioralnego, który na podstawie informacji dostarczonych w plikach cookie wybrał taką osobę, która będzie jak najbardziej zainteresowana produktem, ponieważ sklep, tak jak i marketer zarabiają tylko wtedy, gdy reklama będzie skuteczna.

Głównymi zaletami retargetingu są:

[26] https://funkymedia.pl/remarketing-vs-retargeting-roznice.html#remarketing-vs-retargeting-roznice (dostęp 27.09.2022)

- Optymalizowanie budżetu reklamowego, dzięki kierowaniu reklamy do użytkowników zainteresowanych Twoimi usługami lub produktami, zamiast do nowych osób, których motywacja zakupowa jest kompletnie nieznana,
- Aktywizacja nieaktywnych użytkowników poprzez przypominanie im o marce i swoich produktach,
- Możliwość zachęcania klientów, którzy dokonali zakupu do zapoznania się z nową ofertą,
- Remarketing działa na każdym etapie ścieżki zakupowej (pełny koszyk, oglądanie produktów itp.). Reklama ma za zadanie po prostu przenieść go do kolejnego etapu.
- Możliwość testowania kreacji na różnych grupach kohortowych,
- Zmniejszanie zasięgu reklam konkurencji,
- Zwiększenie sprzedaży oraz liczby odwiedzin w witrynie,
- Możliwość docierania do potencjalnych klientów przez różne urządzenia tzw. cross-device.

99% działań retargetingowych opiera się na licytacjach w czasie rzeczywistym tzw. real time bidding. Jest to rodzaj aukcji internetowej mającej miejsce w momencie ładowania się strony internetowej, czy aplikacji, która jest realizowana za pomocą algorytmów. W tym modelu mało istotna jest witryna, na której reklama zostanie wyświetlona, a dużą większą wartość ma dopasowanie odpowiedniej reklamy do użytkownika odwiedzającego stronę. Sposób dobierania odpowiedniej reklamy do użytkownika opiera się na danych first-party oraz hurtowniach danych third-party. Dzięki wcześniej zgromadzonym informacjom możemy zbudować profil użytkownika, dzięki któremu będziemy znać jego dane demograficzne, zainteresowania, historię wyszukiwania i wszystkie wcześniej wymienione dane, które są przekazywane za pomocą plików cookie. Dzięki profilowaniu użytkowników możemy dokładnie określić strategię marketingową, która będzie docierać do szczegółowej grupy odbiorców.

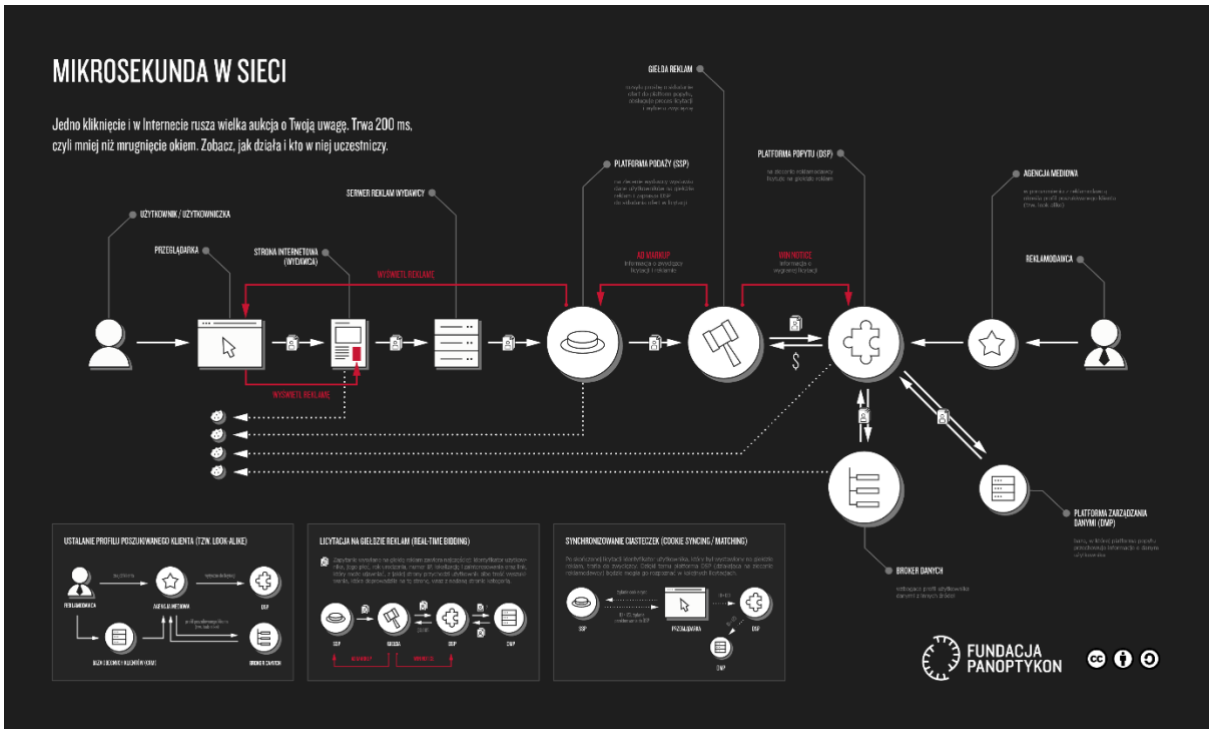
2.3.Jak działa RTB?

W skład sieci aukcji reklamowych wchodzi wiele podmiotów tj.:

- Wydawcy, czyli strony lub aplikacje chcące sprzedać swoją powierzchnię reklamową,
- SSP (Supply Side Platforms), czyli przedsiębiorstwa zajmujące się skupianiem wydawców w jednym miejscu,

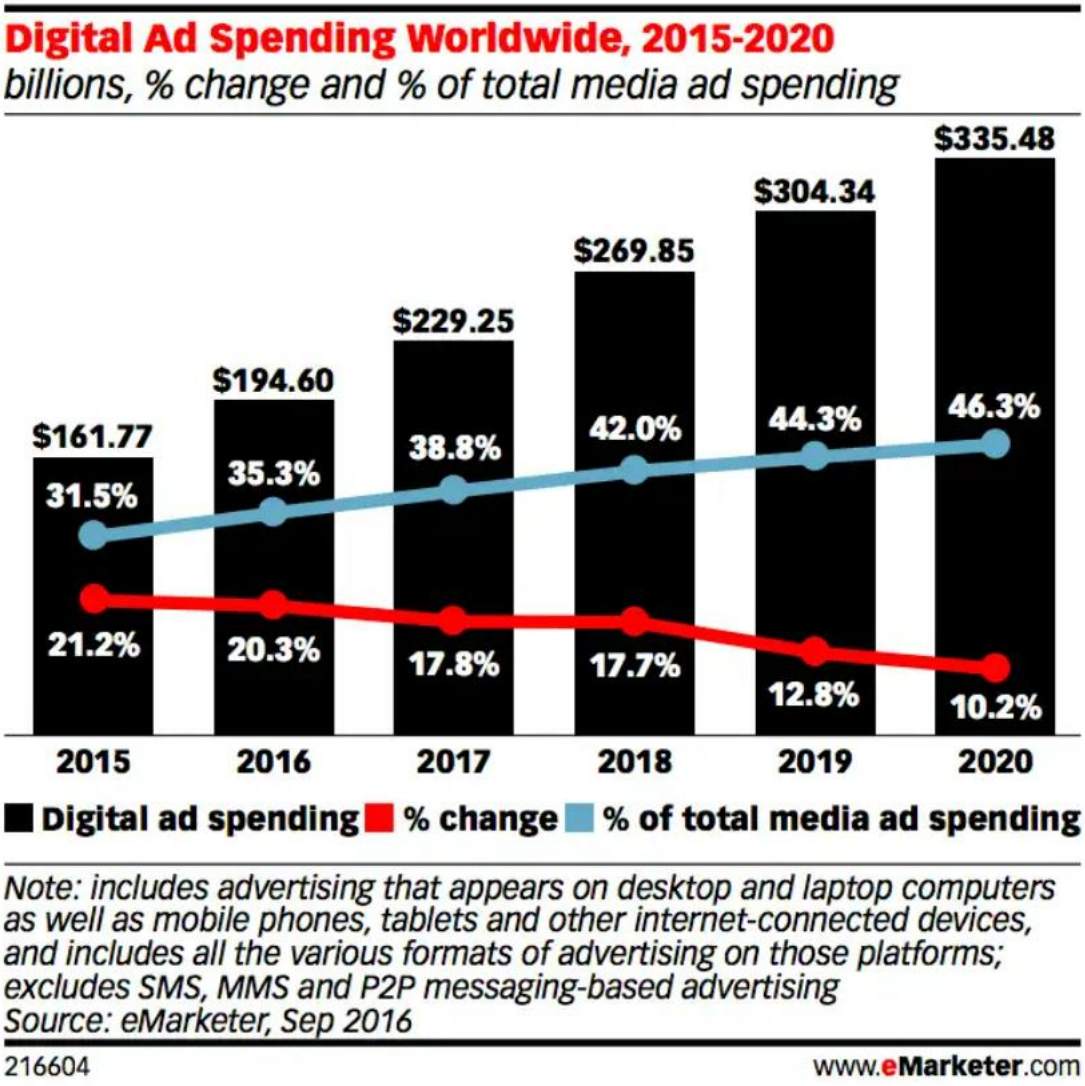
- DSP (Demand-side Platform), czyli platforma popytowa, która pośredniczy pomiędzy reklamodawcami, a wydawcami. DSP w imieniu reklamodawców licytuje powierzchnie reklamowe,
- Reklamodawcy, czyli przedsiębiorstwa zainteresowane kupieniem powierzchni reklamowej w celach marketingowych.

Reklamodawcy za pośrednictwem DSP licytują powierzchnie reklamowe w momencie, gdy witryna wydawcy się ładuje. DSP dzięki zebranym danym robi wycenę wyświetlenia reklamy i wysyła swoją odpowiedź do wydawców wraz z kodem kreacji do wyświetlenia i linkiem odnoszącym do strony reklamodawcy. W ułamku sekundy dochodzi do skomplikowanych decyzji zakupowych przedstawionych na diagramie (Rysunek 7), podejmowanych na podstawie danych o użytkowniku zebranych ze stron trzecich oraz ze stron samych reklamodawców.



Rysunek 8 - Mikrosekunda w sieci, źródło: Fundacja Panoptykon

Głównymi działaczami na rynku RTB są technologiczni giganci jak Google, Criteo, czy Xandr. Według raportu emarketer.com ukazanym na Rysunku 8 wydatki na reklamę digitalową stale rosną, a w samym 2020 roku na reklamy programowalne reklamodawcy wydali ponad 330 miliardów dolarów.



Rysunek 9 - Wydatki na reklamę digitalową, źródło: www.emarketer.pl

Reklama behawioralna budzi wiele kontrowersji w kontekście ochrony danych osobowych. Świadomość użytkowników o wykorzystywaniu swoich danych rośnie proporcjonalnie do presji wywieranej na światowych gigantach do zmiany formy działań marketingowych. Czują się oni śledzeni i manipulowani, co znacząco wpływa na ich zaufanie do nowych technologii. Każdy z nas jako uczestnik tej gałęzi biznesu w mniejszym lub większym stopniu jest świadomy o magazynowaniu naszych danych. Mamy prawo do monitorowania zebranych informacji, jednak nigdy nie uzyskamy dostępu do zaawansowanych analiz, które firmy przeprowadzają w celu najefektywniejszego targetowania.

Z tego powodu firmy podjęły wspólne działania, aby odbudować zaufanie swoich klientów i zbudować ekosystem, który nie będzie aż w takim stopniu inwigilował pojedynczych osób i da im większe poczucie prywatności.

3. Koncepcje remarketingu bez plików cookie stron trzecich

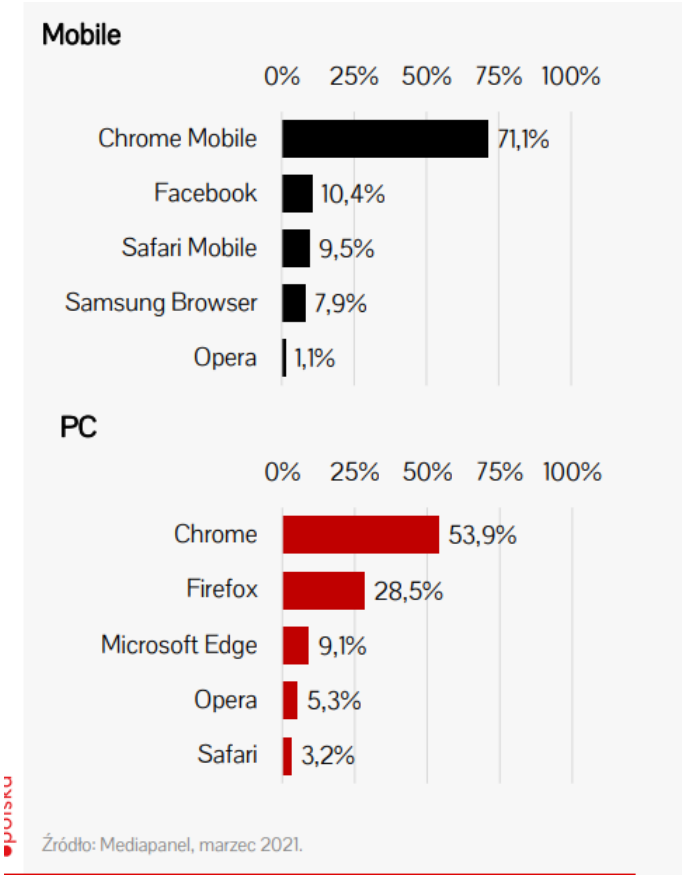
W związku ze wzrostem świadomości użytkowników Internetu reklamy behawioralne będą musiały przejść dużą transformację w najbliższej przyszłości. Wiele przeglądarek już zdecydowało się na ten krok i wycofało używanie plików cookie stron trzecich do targetowania reklam.

W 2020 roku firma Apple zmieniła swoją politykę odnośnie domyślnego zbierania informacji o użytkowniku w przeglądarce Safari, całkowicie blokując pliki cookie third party. Już od roku 2017 dzięki wprowadzeniu ITP. 1.0, czyli funkcji blokujących przez inteligentnym śledzeniem zablokowali większość plików cookie stron trzecich, dzięki uczeniu maszynowym w przeglądarce. Finalnie, jeżeli użytkownik nie wykazał interakcji z witryną przez 30 dni, jego dane były usuwane, a zapisane wcześniej pliki cookie – blokowane. W przeciągu kolejnych lat firma Apple udoskonalała funkcjonalność swojej wtyczki zapobiegając nadużyciom, aż ostatecznie w iteracji ITP. 2.3 zablokować całkowicie reklamy targetowane w przeglądarce Safari.

Mozilla Firefox również poszła śladem swoich rywali i walcząc o zachowanie prywatności już od 2018 roku pracuje nad rozwiązaniem reklam behawioralnych bez wykorzystywania danych od stron trzecich. Obecnie w przeglądarce domyślnym ustawieniem jest blokowanie wszystkich plików cookie third-party, jednak daje ona wybór użytkownikowi. Jeżeli ten chciałby z nich korzystać ma takie prawo. Mozilla nie zaimplementowała żadnego alternatywnego rozwiązania w celach remarketingowych, jednak w dalszym ciągu taka funkcja jest tam dostępna, dzięki uniwersalnym ID tworzonym przez strony trzecie na witrynach wydawców.

Zmiany na rynku digitalowym dotkną w szczególności open marketu, który najbardziej narażony jest na spadek przychodów. Jak wspomina szefowa grupy roboczej programmatic przy IAB Polska Elżbieta Kondzioła „Dzięki rozwijaniu projektów takich jak Privacy Sandbox Google czy REARC IAB Tech Lab, cała branża zwiększa zaufanie użytkowników do reklamy internetowej i stosowanych w niej technologiach pomiaru, co przekłada się na możliwość jej dalszego wzrostu.” (IAB/PBI, 2021)

Światowy lider rynku remarketingowego Google zapowiedziało wycofanie cookies do 2023 roku, jednak już przesunęli ostateczną datę śmierci plików śledzących. Firma obawia się, że rynek potrzebuję dużo więcej czasu na przystosowanie się do nowego ekosystemu bez narażania wydawców na utratę środków do tworzenia niezależnych treści. Rozwiązanie Google nazwane „Piaskownicą prywatności" ma na celu zwiększenie prywatności użytkowników, w skład którego wchodzą dwa projekty FLOC i FLEDGE. Ma to również uniemożliwić stosowanie ukrytych praktyk śledzących takich jak „odciski palców", czyli zbierania szczątkowych informacji o urządzeniu i użytkowniku, aby umożliwić jego identyfikację, nawet wtedy, gdy nie zbierane są pliki cookie. Rozwiązania Google są szczególnie ważne dla ekosystemu, ponieważ zdecydowana większość użytkowników w Polsce, jak wynika z raportu Mediapanel (Rysunek 9) używa przeglądarki Chrome jako domyślnej przeglądarki.



Rysunek 10 - Raport udziału przeglądarek na rynku polskim, źródło: Mediapanel, Marzec 2021

3.1.Rozwiązania kohortowe

Dzięki rozwiązaniom kohortowym marketerzy będą w stanie uniknąć polegania na danych pochodzących od stron trzecich. „Ideą kohort jest łączenie podobnych użytkowników w czasie rzeczywistym i umieszczanie tych użytkowników w zagregowanych grupach u różnych wydawców, a wszystko to bez potrzeby stosowania plików cookie stron trzecich i śledzenia w wielu witrynach”[27].

3.1.1. FLEDGE

Flagowym pomysłem kohortowym na funkcjonowanie retargetingu w nowym ekosystemie Chrome ma być projekt pod nazwą FLEDGE (First "Locally-Executed Decision over Groups" Experiment). Jest to nowa iteracja pomysłu Google – Turtledove. Propozycja została zaprojektowana tak, aby stosowanie plików cookie stron trzecich nie było konieczne. Do profilowania użytkowników FLEDGE używa grup zainteresowań, w wyniku czego użytkownik nie jest unikalnie identyfikowany, a trafia do grupy ludzi o podobnych upodobaniach. Grupy zainteresowań mogą być tworzone przez firmy adtech, które zarządzają bidowaniem, wydawców, którzy swoje grupy tworzyć będą na podstawie zachowań użytkowników na ich stronach, a także przez samych reklamodawców, którzy będą w stanie śledzić swoich klientów dzięki first-party cookie. Finalnie, te trzy grupy będą musiały się porozumieć, aby docierać do najbardziej prosperujących osób. Czas utrzymywania tej samej grupy zainteresowań ma wynosić 30 dni. Po tym czasie lista zainteresowań ma być aktualizowana. W celu ochrony prywatności firmy adtech nie będą mogły krzyżować danych dostarczonych przez różnych reklamodawców.

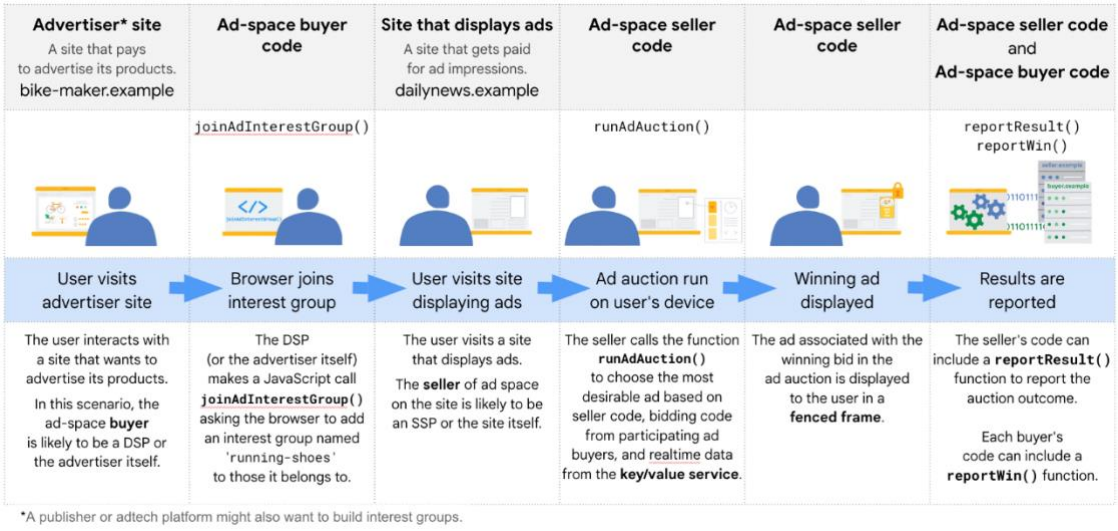
System działania FLEDGE można opisać w następujący sposób (Rysunek 10):

1. Użytkownik odwiedza stronę (np. sklep rowerowy), która zainteresowana jest wyświetleniem mu reklamy retargetingowej w przypadku, gdy nie nastąpi konwersja.
2. Użytkownikowi zostaje przypisana grupa zainteresowań (rowery). DSP wysyła sygnał, aby zaktualizować swoją listę zainteresować o tego użytkownika.
3. Gdy użytkownik odwiedzi inną witrynę wyświetlającą reklamy wysyła wiadomość do DSP, że użytkownik z grupy zainteresowań rowery jest gotowy

[27] https://www.sharethrough.com/blog/6-reasons-why-ssps-are-advertisers-best-friends-in-a-cookieless-world (dostęp 28.09.2022)

do zobaczenia reklamy. Dodatkowo wysyłany jest kod witryny oraz obsługi aukcji.

4. Kampania, która uzyska najwyższy wynik, czyli taka której wyświetlenie ma największą szansę na konwersję wygrywa aukcję i jej reklama zostanie pokazana użytkownikowi w zabezpieczonej ramce (tzn. bez pikseli śledzących, jak jest teraz).
5. Do DSP wysyłana jest informacja z raportem, który zawiera informację, czy użytkownik wyświetlił reklamę i czy nastąpiło kliknięcie.



Rysunek 11 - System działania FLEDGE, źródło: https://developer.chrome.com/docs/privacy-sandbox/fledge/

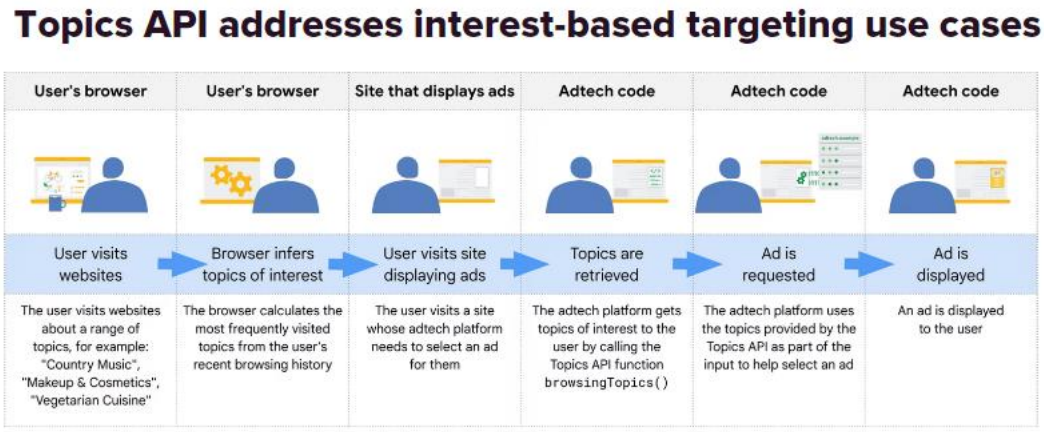
3.1.2. Topics API

Projekt Topic API to kontynuacja wycofanego już projektu FLOC. Firma Google wraz z partnerami udoskonaliła poprzednią propozycję targetowania reklam opartych na zainteresowaniach. Funkcjonowanie Tematów polega na przyporządkowywaniu zainteresowań do użytkownika na podstawie jego historii wyszukiwania. Dane te przechowywane będą przez 3 tygodnie, a następnie aktualizowane o nowe kategorie, ponieważ użytkownik rzadko odwiedza te same strony przez dłuższy czas. Tematy są całkowicie przechowywane na urządzeniu i żaden inny serwer nie ma do nich dostępu, w tym Google. Gdy użytkownik odwiedza witrynę, która chce mu wyświetlić reklamę w aukcji przekazywane są 3 tematy zapisane z ostatnich trzech tygodni, którymi się on interesował. Lista 350 kategorii została starannie przygotowana, aby nie dotykała żadnych wrażliwych tematów tj. rasa, religia czy

orientacja seksualna)[28]. Każdy użytkownik będzie miał dostęp do swojej listy tematów oraz wpływ na to co się w niej znajduje. Istnieje możliwość usunięcia lub dodania tematów, którymi jesteśmy zainteresowani. Projekt przewiduje także możliwość nieuczestniczenia w targetowaniu według tego schematu.

Schemat działania projektu Topic API można opisać w następujący sposób (Rysunek 11):

1. Użytkownik odwiedza stronę, która chciałaby wyświetlić reklamę retargetingową użytkownikowi (np. sklep z płytami).
2. Przeglądarka na podstawie historii wyszukiwania przypisuje osobie tematy, którymi był najbardziej zainteresowany w ostatnim czasie.
3. Następnie użytkownik odwiedza stronę, która ma możliwość wyświetlenia mu reklamy.
4. Firma DSP dostaje sygnał od właściciela powierzchni reklamowej, że użytkownik o danych zainteresowaniach jest gotowy do zobaczenia reklamy.
5. Jeżeli DSP stwierdzi, że ma odpowiednią reklamę dla tej osoby wyślę odpowiedź na ofertę.
6. Reklama zostanie wyświetlona użytkownikowi.



Rysunek 12 - System działania Topics API, źródło: https://iabaustralia.com.au/understanding-googles-topics-api/

Funkcjonowanie projektu FLEDGE i Topics API jest mylące i trudne do rozróżnienia. Głównymi różnicami między nimi są:

Wykres 1 - Porównanie FLEDGE i Topics API

Obszar	**FLEDGE**	**Topics API**

[28] https://privacysandbox.com/intl/en_us/proposals/topics (dostęp 28.09.2022)

Dane używane do grupowania	Ziarniste dane (pochodzące od strony pierwszej)	Generalne dane o zachowaniu użytkownika bazujące na nazwach witryn lub hostów
Twórca grupy kohortowej	Właściciel strony lub odpowiedzialny sprzedawca	Przeglądarka internetowa
Funkcja	Retargeting i targetowanie na podstawie zainteresowań	Targetowanie na podstawie zainteresowań

Istotną zmianą przy zastosowaniu tego rozwiązania jest to, że strony trzecie nie będą miały już możliwości śledzenia historii wyszukiwania swoich użytkowników, co daje im większe poczucie prywatności i mniejsze zagrożenie wycieku danych.

3.1.3. PARAKEET

PARAKEET (Prywatne i anonimowe żądania reklam, które zachowują skuteczność i zwiększają przejrzystość) to propozycja firmy Microsoft (właściciela przeglądarki Edge), której celem jest pomoc branży marketingowej przy zachowaniu poufności danych.

Propozycja Microsoftu działa na zasadach tworzenia kohorty zainteresowań, do których należą użytkownicy. Będą mieć nad nimi kontrolę tzn. będą mogli decydować, z którymi grupami zainteresowań są powiązani. Fundamentalną różnicą między rozwiązaniem Chrome Sandbox ma być anonimizowanie danych osobowych, a dodatkowo aukcja ma odbywać się kompletnie poza kontrolą przeglądarki. „Parakeet wykorzystuje serwer proxy, który stoi między użytkownikiem a firmą reklamową. Użytkownicy mieliby unikalny identyfikator znany tylko serwerowi proxy. Gdy strona internetowa żąda reklamy, żądanie jest kierowane przez zaufany serwer proxy, a do każdego wyniku dodawana jest niewielka ilość szumu statystycznego, aby zamaskować rzeczywiste prywatne dane użytkownika". (Surur, 2021)

Wspomniany wcześniej szum ma obejmować:

- Anonimizacje witryny żądającej reklamy,
- Anonimizacje geolokalizacji, z którego użytkownik żąda treści,
- Anonimizacje adresu IP,
- Anonimizacje ciągu „user agent”, który jest używany do dopasowywania treści do możliwości urządzenia z dostępem do Internetu,

- Dodanie szumu lub innych stochastycznych informacji do różnych próśb unikatowego klienta z obsługą sieci WWW,
- Zmniejszenie szczegółowość zainteresowań odbiorców,
- Dodanie zakodowanego wektora ostatniej aktywności przeglądania, nazywanego reprezentacjami.[29]

Stosowanie tych działań jest na tyle istotne, aby zapewniać prywatność jednostce, ale na tyle małe, aby nie wpływać znacząco na precyzję danych analitycznych. Po procesie anonimizacji informacje są przekazywane do partnerów reklamowych, którzy na podstawie wyliczeń algorytmów kierują adekwatny przekaz do użytkownika. Wszystkie procesy w rozwiązaniu Parakeet zachodzą na serwerze proxy, dzięki temu firma Microsoft może kontrolować, jakie dane są przesyłane sprzedawcom i wydawcom. Twórcy rozwiązania oczekują jednak za nie zapłaty. Ostateczna decyzja odnośnie rozwiązania do reklamy targetowanej przeglądarka Edge podejmie po rozważeniu wszystkich oferowanych opcji i planuje podążać za standardami branżowymi, co może być dla osób wiążących duże nadzieje z Parakeet-em dużym rozczarowaniem.

3.2. Rozwiązania oparte na danych wydawców.

3.2.1. Zaszyfrowane sygnały

Era cookieless nie poradziłaby sobie jednak bez nadawania użytkownikom identyfikatorów. Głównym pomysłem na poszanowanie prywatności, a jednocześnie skuteczną reklamę ma być uniwersalny identyfikator. To taki typ identyfikatora, który jako fundament do swojego istnienia wykorzystuje autoryzowane zdarzenie (np. wprowadzenie adresu e-mail, numeru telefonu). Aby zapobiec wyjawienia tożsamości stosuje się metodę hashowania maila tzn. zmianę znaków na inne, a jako dodatkową ochronę dodaje się do zahashowanego adresu kolejne losowe znaki. „Ponieważ te identyfikatory są oparte na uwierzytelnianiu użytkownika w wielu witrynach i urządzeniach połączenie jest deterministyczne, a ponieważ wynikowy identyfikator nie jest bezpośrednio powiązany z wartością wejściową, są one również uważane za pseudonimowe”[30]. W związku z wycofaniem plików cookie wyzwaniem dla marketerów stało się śledzenie cross device (między różnymi urządzeniami), a ten identyfikator może

[29] https://wiki.prebid.org/wiki/Parakeet (dostęp 19.09.2022)
[30] https://iabeurope.eu/wp-content/uploads/2021/02/IAB-Europes-Updated-Guide-to-the-Post-Third-Party-Cooke-Era-February-2021-1.pdf (dostęp 28.09.2022)

skutecznie pomóc z tym problemem. Do najpopularniejszych rozwiązań tego typu należą: identyfikator Liveramp oraz Unified ID 2.0. Jednak przyszłość tego rozwiązania jest niepewna z uwagi na niedokładną ochronę danych. Mimo, że są one animizowane mogą pozwolić na identyfikację użytkownika.

3.2.2. Targetowanie oparte na ID wydawców

Jednym z najbardziej chroniącym dane użytkowników rozwiązaniem targetowania jest bazowanie na danych wydawców zbierane bezpośrednio od ich odwiedzających. W istocie to oni są w stanie powiedzieć, jakich treści ich widownia oczekuje i jakie reklamy chciałaby oglądać. Ponadto wszelkie informacje, które zostały podane przez użytkowników są oznakowane jako własne (first-party). Tylko w takim wypadku mają oni pełną kontrolę nad ich dostarczaniem i kontrolowaniem. Jeżeli osoba stwierdzi, że nie chce się jakąś informacją dzielić, bądź jest ona zbyt intymna, nie będzie jej udostępniać. Przykładami danych, które można gromadzić są: historia logowania, wyświetlania, kliki, wyszukiwania, posty czy komentarze. Dodatkową prywatność zapewnia fakt, że ujawnianie tego typu niezaszyfrowanych informacji jest surowo zabronione przez rozporządzenie RODO. Dla korzyści remarketingu możliwe będzie kontrola ilości wyświetlonych reklam jednemu użytkownikowi.

3.2.3. Odbiorcy zdefiniowani przez sprzedawcę

Rozwiązaniem zaproponowanym przez stowarzyszenie IAB jest możliwość definiowania odbiorców przez sprzedawców powierzchni reklamowych. Na podstawie zbieranych danych first-party wydawcy mogą przypisywać etykiety swoim odbiorcom i wysyłać je w ofertach zakupowych. Sam IAB o swoim rozwiązaniu mówi tak: „Podstawowa koncepcja jest prosta. Wydawcy lub ich dostawcy danych określają atrybuty odbiorców na podstawie interakcji użytkowników w swoich usługach, przypisują podobne grupy użytkowników do szerokich, ustandaryzowanych opisów atrybutów taksonomii (systematyka odbiorców), dokumentują charakterystykę/metadane odbiorców za pomocą znormalizowanego schematu przejrzystości (standard przejrzystości danych , czyli DTS), a następnie przekazują identyfikatory taksonomii w ramach OpenRTB, aby informować o przekazywaniu sygnałów przez kupujących.[31]”Dzięki temu rozwiązaniu wytworzy się zdrowa konkurencja między wydawcami o to kto potrafi najlepiej analizować swoich gości, a także będą dbać o ich jakość. Dodatkowo obok danych o użytkowniku będzie można przesyłać dane kontekstowe wynikające z treści witryny.

[31] https://iabtechlab.com/blog/tech-lab-releases-seller-defined-audiences/ (dostęp 28.09.2022)

3.3. Rozwiązania kontekstowe

Targetowanie kontekstowe bazuje na technologii AI. Wewnętrzne systemy skanują treść witryny, na której ma zostać wyświetlona reklama i na tej podstawie dopasować kreację do użytkownika. Taki sposób działania jest realną alternatywą do dotychczasowych działań i dużą szansą dla reklamodawców, ponieważ nie są do tego potrzebne żadne pliki cookie stron trzecich. Najefektywniej reklama kontekstowa będzie działała z połączeniem z innymi propozycjami firm, dającym jakiekolwiek informacje o odwiedzającym stronę. Przykładowo użytkownik wyszukiwał najlepsze wakacyjne destynacje, a wydawca lub Google przypisało mu zainteresowanie tematyką podróży. Dzięki targetowaniu kontekstowemu jesteśmy w stanie wyświetlać temu użytkownikowi reklamy biur podróży, wycieczek, czy tanich lotów.

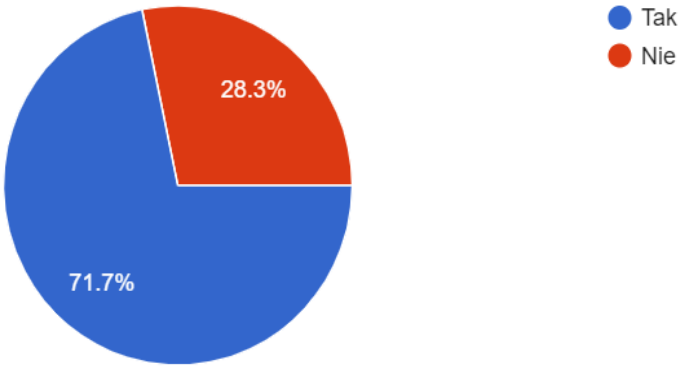
4. Analiza i prezentacja wyników badań

Ankieta została przeprowadzona wśród 100 osób bezpośrednio zaangażowanych w zmianę w ekosystemie marketingowym. Ankietowani to osoby z branży reklamowej, technologicznej, a przede wszystkim użytkownicy Internetu, których także dotyczy targetowanie behawioralne. W ankiecie nie zadałam pytań o płeć czy wiek, gdyż wydaje mi się to w kontekście omawianego tematu nieistotnym parametrem.

Badanie zostało przeprowadzone jednorazowo za pomocą kwestionariusza online Google Form, z możliwością odpowiedzi jednokrotnego, wielokrotnego wyboru lub odpowiedzi własnej. Formami dystrybucji ankiety były wewnętrzna komunikacja z współpracownikami oraz droga mailowa.

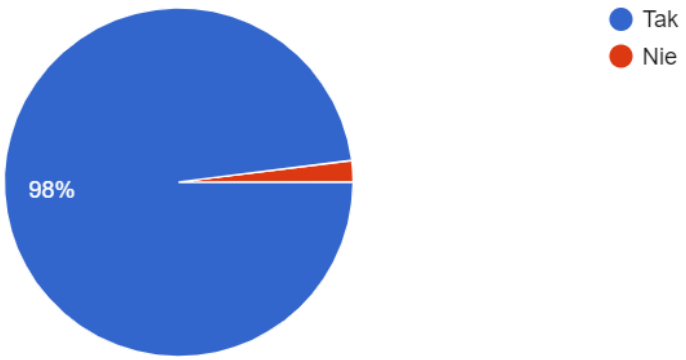
Jak wynika z wykresu 1 blisko 72% respondentów uważa, że dane, które zamieszczają w Internecie to ich dane osobowe.

Wykres 1 – Ocena danych zbieranych w Internecie jako dane osobowe, źródło: badania własne



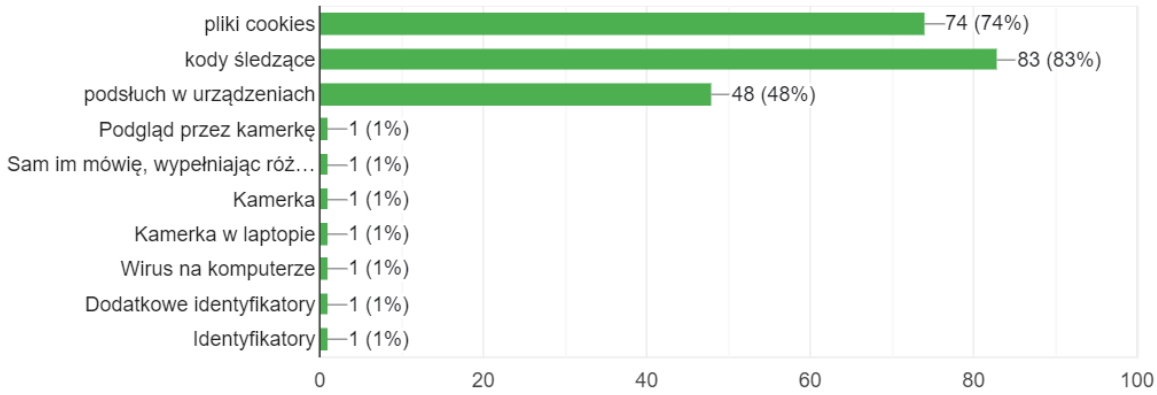
Aż 98% osób uważa, że czują się śledzeni w Internecie, jak wynika z wykresu 2.

Wykres 2 - Odczucia względem bycia śledzonym w Internecie.



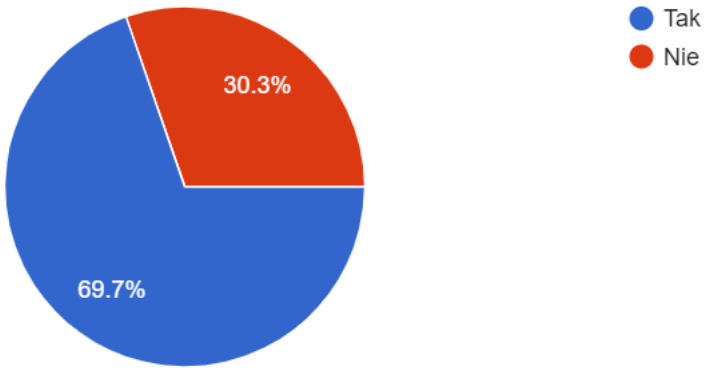
Według respondentów głównym mechanizmem pozwalającym na śledzenie ich w Internecie są kody śledzące. Z badania wynika, że 74% osób uważa, że obserwowanie ich zachowań wynika z używania plików cookie, a 48% pytanych sądzi, że firmy podsłuchują ich przez urządzenie. Jako dodatkowe narzędzie respondenci zaliczają kamerkę w urządzeniu, która miałaby podglądać i rejestrować ich rozmowy i zachowanie (Wykres3).

Wykres 3 - Przyczyna możliwości wyświetlania reklam targetowanych

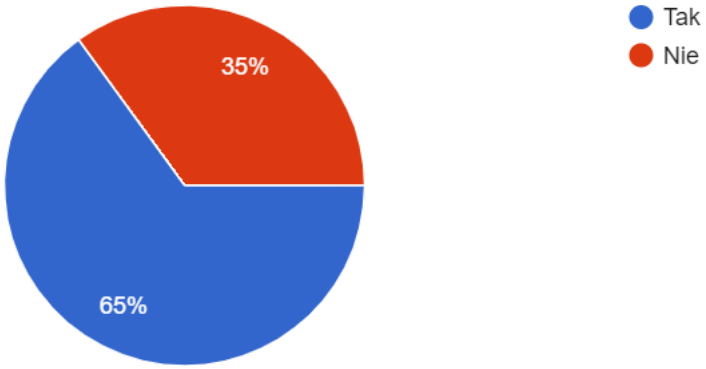


Jak wynika z wykresu 4 30% użytkowników nie jest świadoma tego jakie dane są zbierane przez Internet. Dodatkowo blisko 35 % osób nie wie skąd czerpać informacje na temat ochrony swojej prywatności i przetwarzania danych (wykres 5).

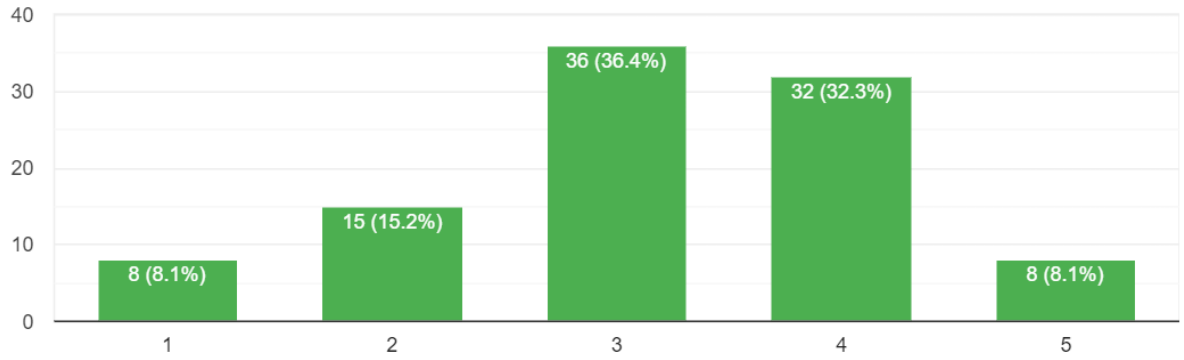
Wykres 4 - Świadomość użytkowników o rodzaju zbieranych danych



Wykres 5 - Świadomość o źródłach czerpania wiedzy na temat ochrony danych osobowych i sposobach ich przetwarzania



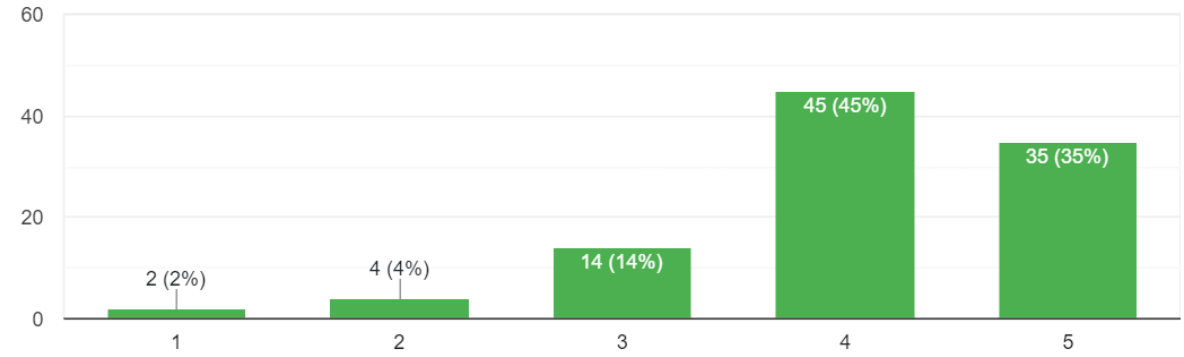
Wykres 6 - Ocena zaufania do social mediów w kwestii ochrony praw osobowych



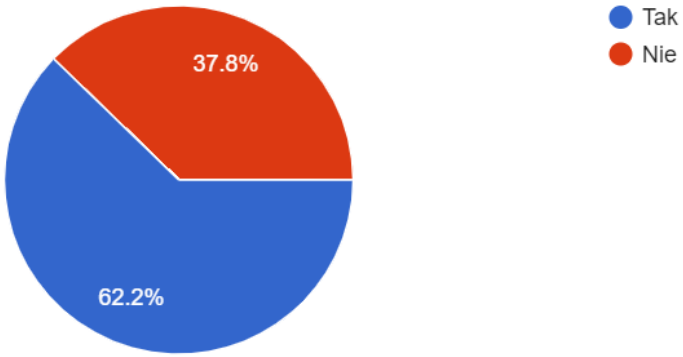
36% respondentów uważa, że ich poziom zaufania do social mediów jest na średnim poziomie. Można powiedzieć, że ponad połowa osób nie ufa, bądź minimalnie ufa firmom z kwesti ochrony praw osobowych (wykres 6).

Porównując dane odnośnie social mediów do stron rządowych, możemy zauważyć znaczną różnicę w poziomie zaufania. Blisko 80% respondentów odpowiedziało, że ufa stronom zarządzającym przez Państwo w sprawie ochrony ich danych osobowych (wykres 7).

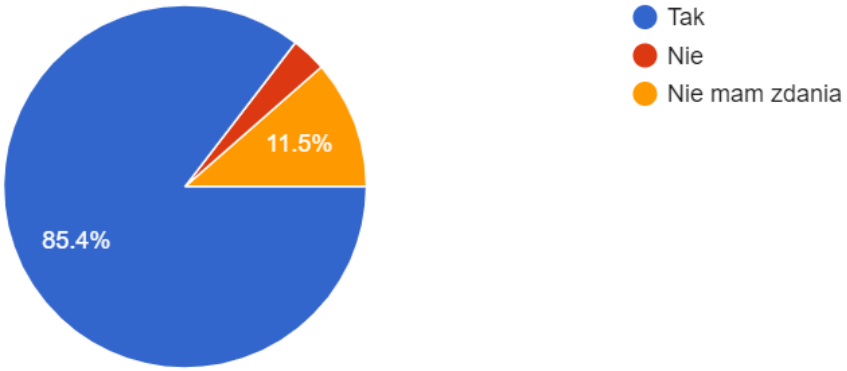
Wykres 7 - Ocena zaufania do stron rządowych w kwestii ochrony praw osobowych



Wykres 8 - Świadomość nadchodzących zmian związanych z wycofaniem plików cookie stron trzecich

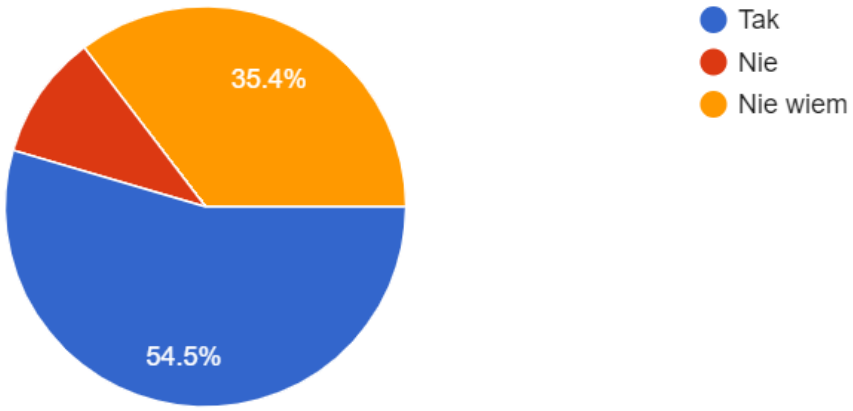


Wykres 9 - Zadowolenie z troski firm technologicznych w zakresie ochrony danych osobowych



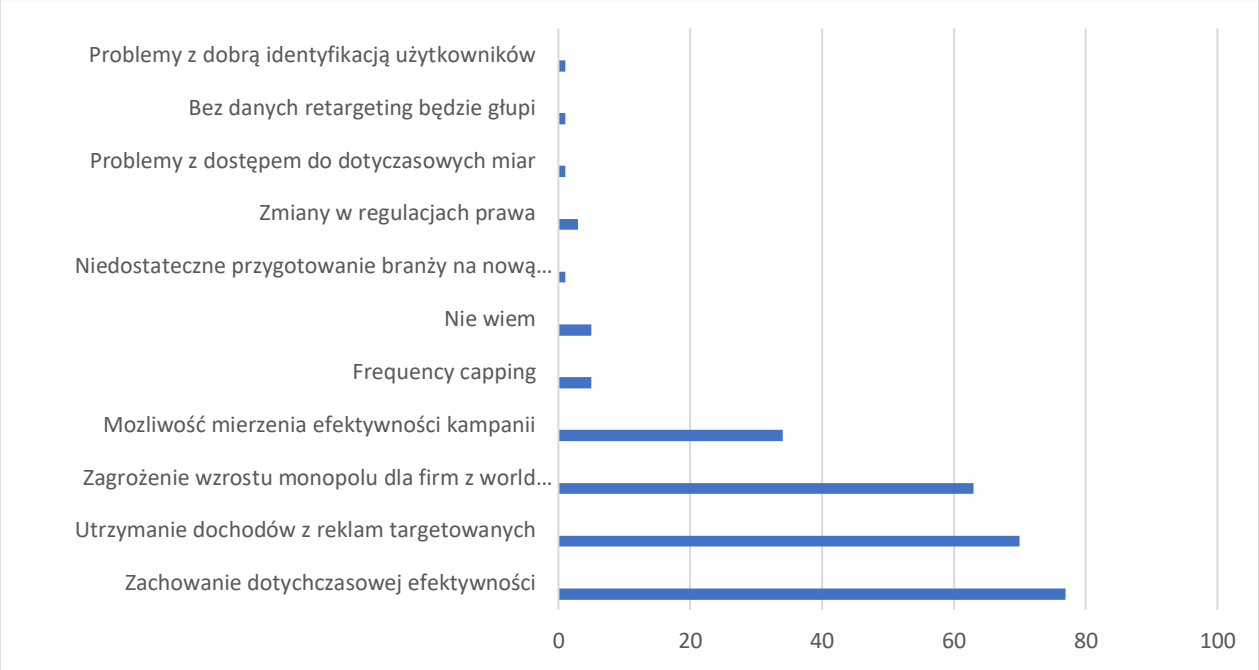
Ponad 62% pytanych słyszało o projekcie wycofywania plików cookie (wykres 8), a 85% osób wyraża zadowolenie z faktu, że firmy technologiczne przejmują się i dbają o podwyższenie standardów ochrony ich danych (wykres 9).

Wykres 10 - Ocena poprawy bezpieczeństwa danych dzięki wycofaniu plików cookie stron trzecich



Blisko 55% pytanych uważa, że poziom bezpieczeństwa ich danych osobowych poprawi się po wycofaniu plików cookie stron trzecich. 35% pytanych nie jest w stanie ocenić skutków, jakie ten proces wywoła w kontekście ochrony danych (wykres 10).

Wykres 11 - Największe wyzwania w retargetingu po wycofaniu plików cookie third-party

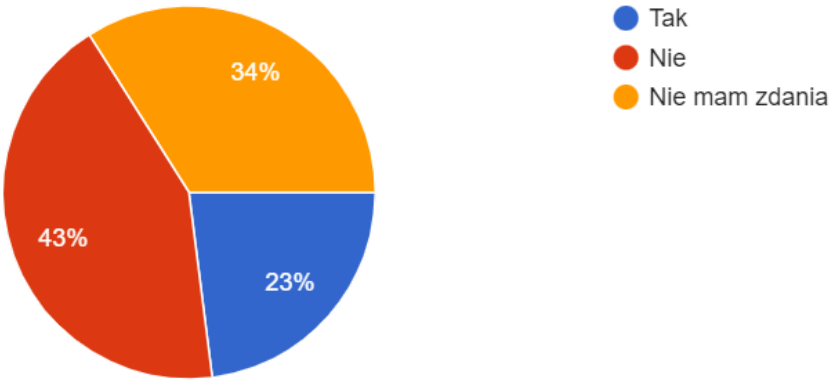


77% respondentów uważa, że największych wyzwaniem, z którym będzie trzeba się zmierzyć po wycofaniu plików cookie stron trzecich będzie utrzymanie dotychczasowej efektywności. 70% osób obawia się, że ciężko będzie utrzymać dotyczasowy dochód z reklam targetowanych, a ponad 60% boi się, że firmy z grupy walled garden zwiększą swój monopol

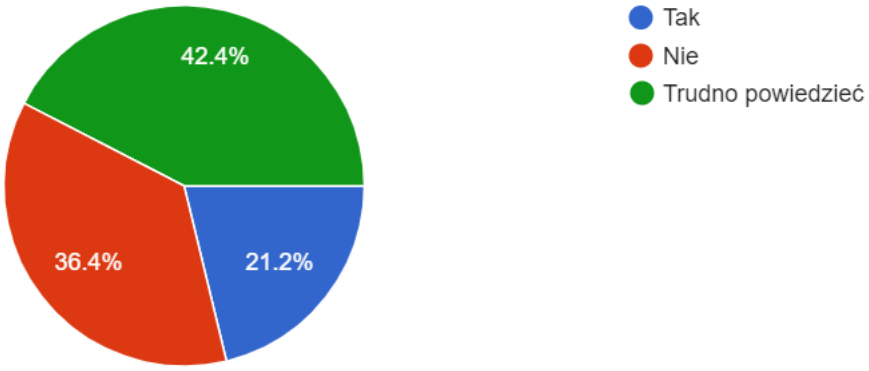
na usługi retargetongowe. Pytani uważają także, że zagrożeniem może być problem z pomiarami efektywności kampanii, niezapowiedziane zmiany w regulacji prawa, czy niedostateczne stopień przygotowania branży na nową rzeczywistość (wykres 11).

43% respondentów uważa, że organy regulujące prawo o ochronie prywatności niedostatecznie dbają o ich bezpieczeństwo (wykres 12).

Wykres 12 - Ocena zaangażowania organów prawa w zapewnienie ochrony prywatności



Wykres 13 - Zaufanie do firmy Google po wycofaniu ciasteczek stron trzecich



Blisko 37% respondentów nie gwarantuje zaufania do firmy Google w zakresie używania danych osobowych zebranych poprzez wydawców. Ponad 42% osób nie jest w stanie ocenić tego zjawiska.

Według badania użytkownicy dbają o ochronę swoich danych osobistych, za które uważają to co sami udostępniają w Internecie. Wiedza na temat tego, jakie dane są przetwarzane przez firmy Adtech jest na poziomie 60%, jednak 30% użytkowników ma problem ze znalezieniem źródła informacji na temat bezpieczeństwa danych. Zdecydowana większość respondentów czuje się śledzona w Internecie i nie ufa większości stron internetowych w aspekcie przechowywania i przetwarzania ich danych osobowych. Największym wyzwaniem dla ekosystemu marketingowego jest utrzymanie efektywności i przychodów z retargetingu.

5. Podsumowanie

Wycofanie plików cookie stron trzecich stanowi duże wyzwanie dla firm technologicznych. Rynek retargentingu wynosi blisko 800 miliardów dolarów rocznie i daje możliwość tworzenia niezależnych treści przez wydawców. Jednocześnie zakres wykorzystywanych danych znacznie przekracza granice prywatności użytkowników. Wizja tego świata jest dla wielu organizacji niewyobrażalna. Wiele z nich nie zaczęło jeszcze przygotowań do nowego ekosystemu. Dużym zagrożeniem jest także wzrost monopolu na dane przez firmy z walled garden, czyli tzw. ogrodzony murem ogród. Jest zbiór stron internetowych lub aplikacji, które utrudniają dostęp do treści użytkownikom, którzy nie będą członkami ich społeczności.[32] Przykładami aplikacji należących do walled garden są Facebook, Instagram, Twitter, Google, Apple App Store i Google Play Store, czy Amazon. Mimo, że third-party cookie będą wycofane, pionier reklamy digitalowej Google oferuje szereg innych usług tj. Analytics, gdzie znajdować się będą dane first-party zbierane przez wydawców. Choć zapewniają oni, że nie będą korzystać z danych zebranych w taki sposób, część rynku zastanawia się, czy wywiążą się z obietnicy. Jak historia pokazuje giganci często nadużywają prawa i stosują praktyki niezgodne z prawem, a korzyści płynące z takich czynów są znacznie większe niż przyznawane kary. Ważnym aspektem jest również nadzieja, że organy regulujące prawo zintensyfikują swoje działania w celu ochrony prywatności użytkowników. Wraz z rozwojem technologii analizy danych, jak i działania prowadzone na podstawie ich analizy mogą mieć krzywdzący i dyskryminujący wpływ na życie jednostek. Jak wspomina dyrektor Thomas Mendrina „W firmie Xandr wierzymy, że podejście wielopłaszczyznowe, oparte na różnorodnych rozwiązaniach, będzie przyszłością reklamy cyfrowej, a największy sukces odniosą dostawcy technologii, którzy będą elastycznie wdrażać zróżnicowane, interoperacyjne funkcjonalności mające na celu zaspokojenie potrzeb szerszego ekosystemu reklamy internetowej". Prawdą jest, że firmy będą musiały wykazać się innowacyjnością i elastycznością w wyborze rozwiązań, aby dostosować się do nowej rzeczywistości. Jednak zasięg działań i zyski czerpane z retargetingu powinny być wystarczającą motywacją do poszukiwania odkrywczych rozwiązań, przy zachowaniu prywatności użytkowników.

[32] https://www.techtarget.com/searchsecurity/definition/walled-garden (dostęp 29.09.2022)

Załączniki

Załącznik 1. Kwestionariusz ankiety pt. „Badanie na temat wpływu wycofania ciasteczek third-party na retargeting”

1. Czy uważasz, że dane, które podajesz w Internecie (np. historia wyszukiwania, geolokalizacja, adres email) zbierane przez ekosystem internetowy to dane osobowe?

☐ Tak

☐ Nie

2. Czy kiedykolwiek czułeś się śledzony w Internecie?

☐ Tak

☐ Nie

3. Co według Ciebie sprawia, że reklamodawcy wiedzą, jakimi produktami jesteś zainteresowany?

☐ pliki cookies

☐ kody śledzące

☐ podsłuch w urządzeniach

☐ inne

4. Czy jesteś świadomy jakie informacje posiadają o Tobie strony internetowe i aplikacje?

☐ Tak

☐ Nie

5. Czy wiesz skąd czerpać informacje o danych zbieranych w Internecie na Twój temat?

☐ Tak

☐ Nie

6. W jakim stopniu ufasz social mediom (Facebook, Instagram, Tik tok) w kwestii ochrony Twoich danych?

7. W jakim stopniu ufasz serwisom informacyjnym w kwestii ochrony Twoich danych?

	1	2	3	4	5	
Nie ufam	○	○	○	○	○	Ufam

8. W jakim stopniu ufasz stronom rządowym w kwestii ochrony Twoich danych?

	1	2	3	4	5	
Nie ufam	○	○	○	○	○	Ufam

9. W jakim stopniu ufasz zwykłym witrynom internetowym w kwestii ochrony Twoich danych?

	1	2	3	4	5	
Nie ufam	○	○	○	○	○	Ufam

10. Czy słyszałeś o pomyśle wycofaniu plików cookie stron trzecich?

☐ Tak

☐ Nie

11. Czy jesteś zadowolony, że firmy technologiczne zwracają uwagę na ochronę prywatności w sieci?

☐ Tak

☐ Nie

☐ Nie mam zdania

12. Czy uważasz, że wycofanie plików cookie stron trzecich poprawi bezpieczeństwo Twoich danych?

☐ Tak

☐ Nie

☐ Nie wiem

13. Co uważasz za największe wyzwanie dla retargetingu w świecie bez ciasteczek stron trzecich?

☐ Zachowanie dotychczasowej efektywności

☐ Utrzymanie dochodów z reklam targetowanych

☐ Możliwość mierzenia efektywności kampanii

☐ Zagrożenie wzrostu monopolu dla firm z world garden (Google, Microsoft, Meta)

☐ Inne

14. Czy uważasz, że branża retargetingu znacząco zmniejszy swoją efektywność po wycofaniu ciasteczek?

☐ Tak

☐ Nie

☐ Może

15. Czy uważasz, że regulatorzy prawa wystarczająco dbają o ochronę prywatności w Internecie?

☐ Tak

☐ Nie

☐ Nie mam zdania

16. Czy ufasz firmie Google, że nie będzie korzystała z danych first-party wydawców w celach zwiększenia swojej przewagi na rynku retargetingowym?

☐ Tak

☐ Nie

☐ Trudno powiedzieć

Bibliografia

IAB/PBI. (2021). *Reklama online w dobie postcookie.* IAB Polska.

Katarzyna Szymielewicz, W. A. (2017). *Śledzenie i profilowanie w sieci. W czym problem? Co się zmieni w prawie? Jak może wyglądać przyszłość?* Warszawa: Fundacja Panoptykon.

Martin, B. P. (2017). Data privacy: Effects on customer and firm performance.

Namysłowska, M. (2012). *Reklama. Aspekty prawne.* Warszawa.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne . (brak daty).

Surur. (2021). *Microsoft prefers their PARAKEET to Google's FLoC*. Pobrano z lokalizacji https://mspoweruser.com/microsoft-prefers-their-parakeet-to-googles-floc/

Udo, G. J. (2001). *Privacy and security concerns as major barriers for e-commerce: A survey study.*

Spis rysunków

Spis tabel