Dobre Praktyki w obszarze Brand Safety

LIPIEC 2020

Spis treści:

1. Wstęp

Rozwój internetu i rosnące w dynamicznym tempie budżety reklamowe w tym kanale sprawiają, że poprawa Brand Safety stała się jednym z najważniejszych elementów planowania i egzekucji kampanii reklamowych. Świadome i odpowiedzialne marki rozumieją znaczenie kontekstu reklam. Znanych jest wiele przykładów naruszenia wizerunku firmy poprzez wyświetlenie jej reklam wśród nieodpowiednich treści (np. odwołujących się do radykalnych poglądów politycznych, wiadomości o katastrofach lub nieprawdziwych informacji).

W zależności od grupy docelowej, a także oczekiwań i założeń samej marki, konieczne jest posiadanie indywidualnej, odpowiednio dopasowanej polityki bezpieczeństwa. Jednak podstawowy zakres działań niezbędnych do zapewnienia ochrony wizerunku marek będzie dosyć uniwersalny, nawet na poziomie międzynarodowym.

Natomiast by poprawiać ogólną jakość emisji reklamy online, utrzymać jej dobrą reputację, zabezpieczać budżety przeznaczane na ten kanał, niezbędna jest stała współpraca i proaktywna postawa wszystkich stron procesu zakupowego.

Niniejszy dokument ma na celu przedstawienie wspomnianych uniwersalnych działań dla poszczególnych typów podmiotów, zebranie i objaśnienie dobrych praktyk, które powinny wcielać w życie poszczególne strony, a także zwrócenie uwagi na wyzwania w obszarze Brand Safety, z którymi nadal mierzymy się jako branża.

2. Grupa Robocza Brand Safety

Grupa Robocza Brand Safety przy IAB Polska koncentruje się na zagadnieniach związanych z narzędziami i procesami marketingu online, które mają za zadanie zapobiegać wyświetlaniu reklamy w niechcianym lub szkodliwym dla marki kontekście.

Kluczowe w działaniach Grupy jest zapewnienie, poprzez edukację, wzrostu świadomości strony popytowej i podażowej rynku online w temacie bezpieczeństwa marek, otoczenia i jakości powierzchni reklamowej.

W skład **Grupy Roboczej Brand Safety** wchodzą przedstawiciele firm:

Adrino
Agora
Bonnier Business
Cyfrowy Polsat
Gemius
GSK Commercial
Initiative Media
Mindshare Polska
Meetrics
Nestlé Polska
Nielsen
Polska Press
RASP
RTB House
Społeczności.pl
Ströer
TVN Media
Telewizja Polska
Wavemaker
Wirtualna Polska Media
Yieldbird

3. Brand Safety

3.1. Definicja

Granice definicji Brand Safety są trudne do wytyczenia i mogą przebiegać w nieco innym miejscu dla każdej marki. Powszechnie uznaje się jednak, że:

Brand Safety (pl. *bezpieczeństwo marki*) to szereg działań oraz narzędzi, którymi posługują się podmioty biorące udział w realizacji procesu reklamowego, a które mają na celu stworzenie środowiska niewpływającego negatywnie na odbiór marki/produktu/usługi, oraz nie naraża marki na straty wizerunkowe, finansowe czy negatywne skutki prawne. Dotyczy zatem zapewnienia dla każdej emisji reklamy odpowiedniego kontekstu, w którym reputacja marki nie zostanie naruszona.

3.2. Kategorie contentowe

Wyróżnia się kilka kategorii treści powszechnie uznawanych jako niepożądane dla wizerunku marek. Są to:

1) Treści naruszające prawo i społecznie szkodliwe bądź sprzeczne z dobrymi obyczajami, w tym przede wszystkim:
    a. pirackie, naruszające prawa autorskie lub prawo własności przemysłowej/prawo do znaków towarowych[1],
    b. propagujące przemoc, terroryzm i nawołujące do przestępstwa[2],
    c. propagujące rasizm, neo-nazim, nazizm,
    d. propagujące faszyzm, totalitaryzm[3],
    e. dyskryminujące lub ksenofobiczne[4],
    f. promujące hazard,
    g. czyny nieuczciwej konkurencji,
    h. propagujące pedofilię, pornografię,
    i. promujące narkotyki, substancje psychoaktywne,

---

[1] *Prawo własności przemysłowej z dnia 30 czerwca 2000 r. (Dz.U. 2001 Nr 49, poz. 508 z późn. zm.); Ustawa o prawie autorskim i prawach pokrewnych (Dz.U. 1994 nr 24 poz. 83 z późn. zm.).*

[2] *Art. 255 k.k. (Nawoływanie i pochwalanie przestępstwa)*

[3] *Art. 256 k.k. (Propagowanie faszyzmu i totalitaryzmu)*

[4] *Ustawa o wdrożeniu niektórych przepisów Unii Europejskiej w zakresie równego traktowania z dnia 3 grudnia 2010 r. (Dz.U. Nr 254, poz. 1700 z późn. zm.)*

j. zawierające mowę nienawiści/wulgaryzmy,

k. zniesławiające lub znieważające,

l. profanujące[5],

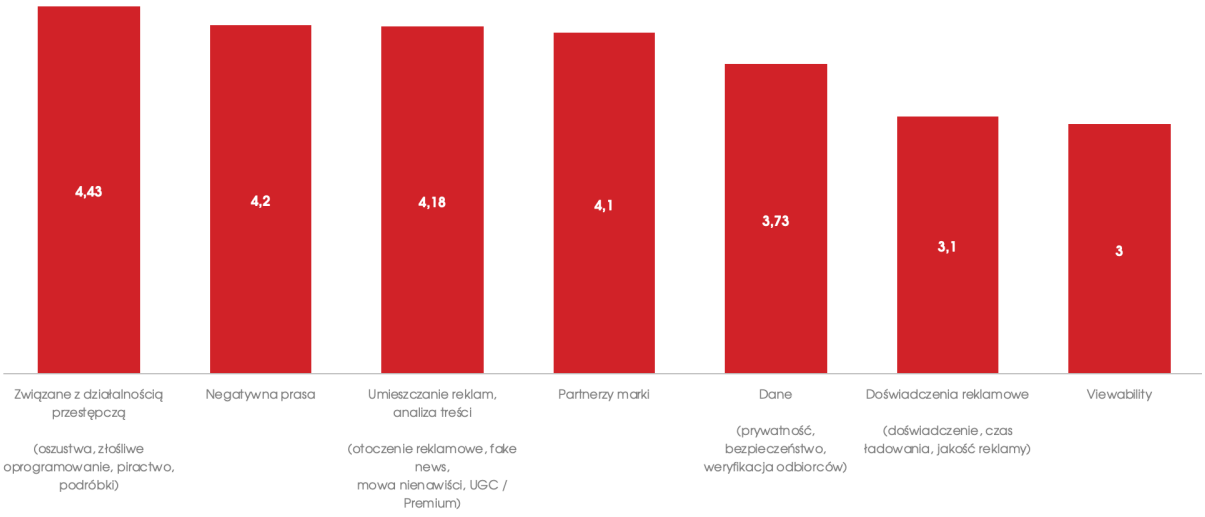
m. zawierające złośliwe oprogramowanie/spyware/malware/trojany,

n. niemoralne lub o charakterze nieetycznym;

2) Niemoderowane treści tworzone przez użytkowników (UGC – User Generated Content).

3) Fake news / treści celowo wprowadzające w błąd.

4) Innego rodzaju treści uznawane indywidualnie przez wybraną markę za naruszające jej reputację.



Najczęściej pojawiające się hasła w wypowiedziach ankietowanych marketerów - w nawiązaniu do Brand Safety, pogrupowane w kategorie (np. fraud i złośliwe oprogramowanie pod wspólnym hasłem "Związane z działalnością przestępczą")[6] Hasła oceniane były pod kątem ich znaczenia dla ogólnej koncepcji bezpieczeństwa marki w skali od 1 do 5, gdzie 5 stanowi ocenę "wysoki" bądź "bardzo wysoki" .

3.3. Brand Safety a Brand Suitability

Bezpieczeństwo marki powinno zawsze być najważniejsze dla reklamodawców, szczególnie w dzisiejszym cyfrowym świecie. Uznanie, że środowisko jest

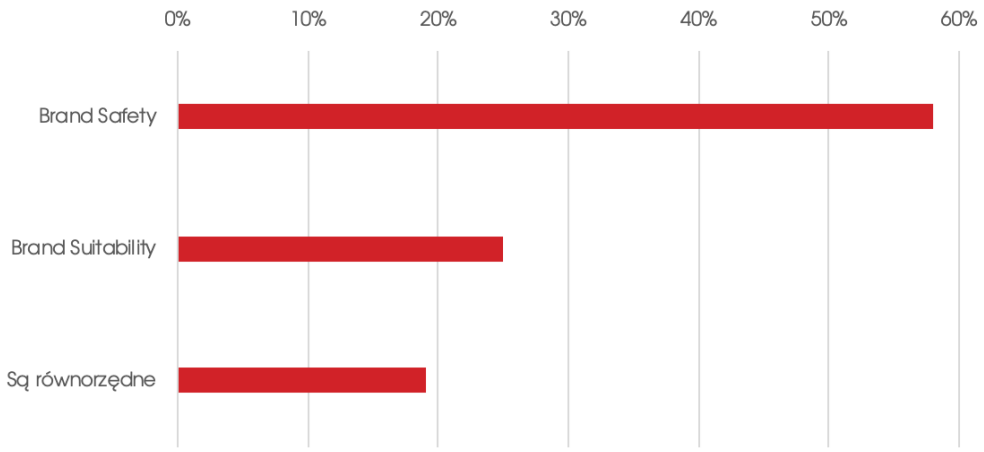
---

[5] Art. 196 k.k. (Obraza uczuć religijnych) Kto obraża uczucia religijne innych osób, znieważając publicznie przedmiot czci religijnej lub miejsce przeznaczone do publicznego wykonywania obrzędów religijnych, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

[6] Defining Brand Safety, Trustworthy Accountability Group i Brand Safety Institute, Lipiec 2018.

„bezpieczne", niekoniecznie jednak oznacza, że jest to optymalne miejsce do wyświetlania reklamy. Dążenie do szukania i „tworzenia" bezpiecznego, pożądanego środowiska dla reklamy określamy pojęciem **Brand Suitability** (pl. *przydatność marki*).

Brand Suitability na poziomie witryny ma na celu unikanie umieszczania reklam na stronach, które chociaż ogólnie nie zawierają szkodliwej treści pod kątem Brand Safety, to są niezgodne z zasadami dotyczącymi danej marki. Przydatność marki na poziomie poszczególnych treści ma na celu uniknięcie umieszczania reklam przy treściach, które mogą być niepożądane dla marek, choć umieszczone w odpowiednim kontekście.



Pytanie: Co jest obecnie większym priorytetem: bezpieczeństwo marki czy przydatność?[7].

4. Wyzwania i priorytety marek w kontekście zapewnienia bezpieczeństwa

Kluczowa w ocenie środowiska emisyjnego pod kątem Brand Safety jest decyzja marketera/brand managera odnośnie fundamentalnych założeń contentowych, które wpisują się w świat marki, czyli zdefiniowania marki oraz skojarzeń, które za sobą niesie. Ostateczną decyzję odnośnie akceptacji otoczenia reklamowego ma więc marka, dla której finalnym ograniczeniem pozostają jedynie przepisy obowiązującego prawa.

Po stronie marketera jest dobranie słów kluczowych czy kontekstów, które mogą mieć swoje źródło w elementach marki: tj. pochodzenie promowanego produktu lub

[7] *The State of Brand Suitability, IAS, 2019.*

usługi, jej nazwa, przewodnie hasło, ikona, moment użycia czy przeznaczenie. To on określa ostateczne korzyści emocjonalne i racjonalne jakie daje marka - w związku z czym, w sposób rozstrzygający, formułuje wytyczne odnośnie akceptacji kategorii znanych powszechnie jako niebezpieczne za nienaruszające jej reputacji, o ile pozostają w zgodzie z aktualnymi normami prawnymi.

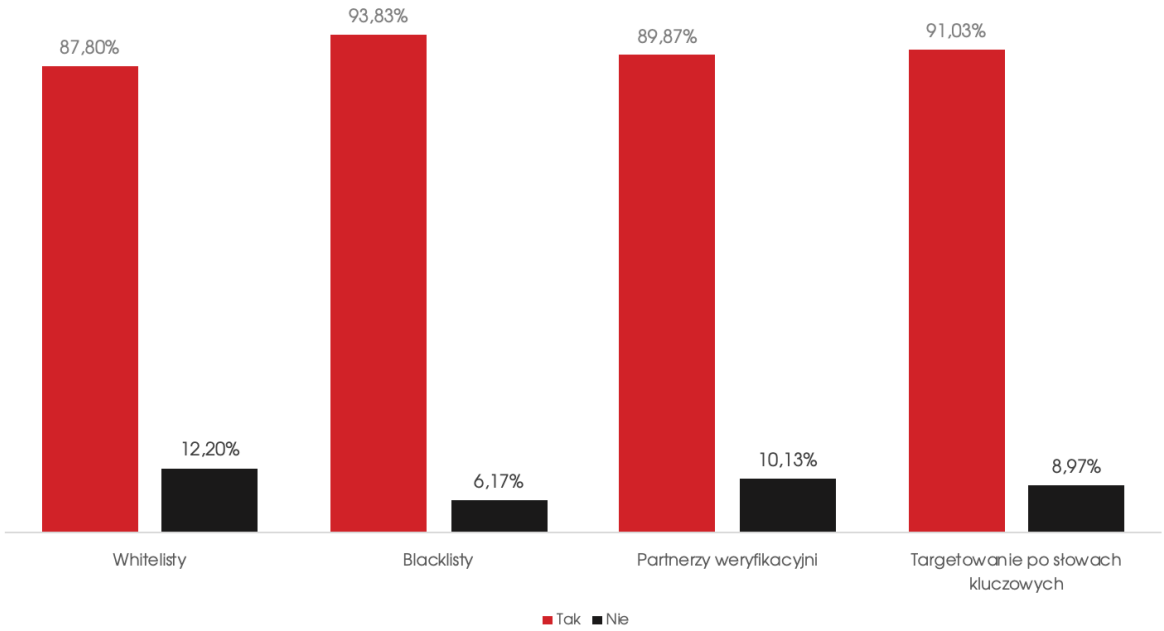
Coraz więcej klientów bierze kwestie Brand Safety pod uwagę przy planowaniu i prowadzeniu kampanii.

Część z nich (zwłaszcza globalnych), rozpoczynając współpracę z agencją ma już wyznaczone swoje standardy, a wśród nich preferencje dotyczące wyboru narzędzia pomiarowego.

Z drugiej strony, również wśród mniejszych reklamodawców obserwuje się zainteresowanie tematem, o czym świadczą prośby o rekomendację rozwiązania, oszacowanie kosztów związanych z monitoringiem czy dopytywanie o szczegóły dotyczące jakościowej emisji reklamy (ad fraudy, viewability i właśnie brand safety).

4.1. Działania marek

W ostatnich latach widać wśród reklamodawców większą świadomość wyzwania i chęć zapobiegania problemom związanym z bezpieczeństwem marki, ale podejście klientów już w trakcie emisji kampanii jest różnorakie. Część z nich (przede wszystkim duzi, globalni marketerzy) stosują szereg działań chroniących przed pojawianiem się ich marek przy niepożądanych treściach. Obejmują one zarówno emisję display, jak i wideo (również YouTube) w zakupie bezpośrednim i programatycznym.



Pytanie: Które z wymienionych narzędzi stosuje Twoja firma do zapewnienia bezpieczeństwa marki?[8]

Najczęściej wykorzystywane mechanizmy to m.in.:

- Whitelisty i blacklisty - głównie rekomendowane przez agencje, ale najbardziej wrażliwi klienci potrafią umieszczać samodzielnie na nich nawet 300 tys. witryn czy ponad 1,5 tys. aplikacji;
- Wykluczenia:
    - Keywords - blokowane słowa kluczowe, głównie związane z tematyką seksualną, terrorystyczną, narkotykami, przemocą, a niekiedy także z dziećmi (np. zabawki);
    - Kategorie treści - klienci wykluczają emisję przy treściach oznaczonych jako dla dorosłych czy związanych np. z przemocą, alkoholem, narkotykami, hazardem, polityką itp.;
    - Etykiety treści - dopuszczalna jest obecność reklam np. jedynie przy treściach zaklasyfikowanych jako dozwolone dla nastolatków i dorosłych, a wyklucza się emisję przy treściach z etykietą "dla dorosłych", bądź zupełnie nieskategoryzowanych;
    - Embeded videos, livestreams, downloads – zabroniona jest reklama na wideo osadzonym na zewnętrznych stronach oraz transmisjach

[8] *Ankieta Brand Safety, IAB Europe, listopad 2019.*

na żywo (ang. *livestream*), co związane jest z brakiem pełnej kontroli nad zawartością serwisu czy transmitowanego contentu;

- Wiek „Unknown" – klienci nie kierują reklam do osób zaklasyfikowanych przez Google jako „Unknown" (jest to ostatnia wytyczna Google, która ma zapobiec docieraniu reklam do dzieci - według nich największa część użytkowników poniżej 13. roku życia znajdowała się właśnie w tej grupie);

- Ustawienia na platformach programatycznych – korzystanie wyłącznie z Private Deals z wydawcami, bez wykorzystywania modelu Open Market;
- Zewnętrzne systemy monitoringu i blokowania odsłon reklam – narzędzia takie jak np. Double Verify, Gemius czy MOAT wykorzystują własne blacklisty słów kluczowych oraz domen;
- Wykluczenia na YouTube:
  - YouTube Blacklist – założenie częstej aktualizacji blacklisty kanałów na YouTube przy filmach, na których klient nie życzy sobie wyświetlania reklam (dane dotyczące kanałów pochodzą z systemu monitoringu i blokowania Double Verify);
  - Tematy/kategorie YouTube - wyłączenie treści religijnych, politycznych, szokujących, związanych z przemocą i zdrowiem. Oprócz tego funkcjonuje również szeroka lista treści nawiązujących tematyką do dzieci (literatura dziecięca, gry wideo, rodzina, rodzicielstwo, zabawki, filmy familijne, komiksy, bajki, rysowanie i kolorowanie). Kategorie te bywają często bardzo szczegółowe np. Zdrowie > Medycyna alternatywna i naturalna > Akupunktura i chińska medycyna.

Nie wszyscy jednak klienci podchodzą do tematu z aż taką dbałością i nie każdy ma potrzebę głębszych analiz problemu. Głównie bazują na white- i blacklistach rekomendowanych przez agencję, a wybrani stosują monitoring zewnętrznymi narzędziami takimi jak Meetrics, MOAT, Integral Ad Science lub z raportów z Google DCM (lista URL, contentu). Analizy pozwalają na ewentualną reakcję w trakcie trwania kampanii lub dopiero od następnej, po weryfikacji postbuy'a. Zauważalne jest, że część klientów reaguje dopiero, kiedy faktycznie dojdzie do ekspozycji marki przy nieodpowiednim contencie - kiedy zostanie wychwycona taka emisja - osobiście lub na podstawie wspomnianych raportów, jeśli stosują odpowiednie narzędzia.

W przypadku YouTube'a czy Facebook'a najczęstszą praktyką jest stosowanie narzędzi zewnętrznych (np. OpenSlate, IAS, MOAT, DoubleVerify, Nielsen itp.) bądź po prostu ograniczenie wykorzystywanych powierzchni, wierząc, że np. emisja w news feed Facebooka pozwoli zapewnić najwyższy możliwy poziom Brand Safety na tej platformie. Trzeba przy tym zauważyć, że występujące co pewien czas wpadki w obu tych serwisach (m.in. emisja spotów dużych marek przy treściach zamieszczanych przez terrorystów czy innych treściach wideo uznawanych za kontrowersyjne) nie zniechęciły na stałe większości reklamodawców do rezygnacji z promowania się na tych platformach - traktują te wydarzenia raczej jako incydenty, nie wpływające znacznie na atrakcyjność oferty reklamowej tych globalnych platform.

Warto również zaznaczyć, że wraz z rosnącą liczbą narzędzi Brand Safety stosowanych w procesie zakupu reklam, istotnie rosną także koszty całej kampanii. Do podstawowych kosztów technicznych za monitoring czy adserving kampanii dochodzą tutaj dodatkowe obciążenia związane z analizą treści pod kątem Brand Safety. Oznacza to, że w budżecie kampanii udział kosztów technicznych wzrasta, co często skutecznie zniechęca klientów do inwestowania środków w takie narzędzia.

Co więcej - bardzo restrykcyjne podejście do Brand Safety mocno ogranicza miejsca emisji czy liczbę partnerów. Przekłada się to często na zmniejszane zasięgi oraz ponownie – na większe koszty kampanii. Stawiając bowiem tylko na współpracę z dostawcami premium, gwarantującymi największą kontrolę nad jakością i bezpieczeństwem treści, musimy się po prostu nastawić na wyższe stawki współpracy (większe CPM). Realia te muszą brać pod uwagę klienci - zwłaszcza ci przyzwyczajeni do "benchmarkowania" kampanii względem kosztów i nastawionych na maksymalizację zasięgu po najniższych kosztach jednostkowych.

Wartościową cecha internetu jako medium, jest rozwój palety narzędzi, które możemy stosować do tego, by podnosić jakość kampanii. Jednak bezrefleksyjne ich wdrażanie może wiązać się z dużym ryzykiem. Temat Brand Safety powinien być zatem traktowany z odpowiednią dozą ostrożności.

Rekomendowane działania po stronie reklamodawcy:

- Określ, jakie konteksty stanowią dla marki największe ryzyko w kontekście Brand Safety;

- Sprawdź, czy w ramach narzędzi, które już wykorzystujesz w kampanii, masz możliwość wykluczenia najbardziej ryzykownych kontekstów;
- Stwórz blacklisty i whitelisty, które pomogą określić serwisy, na których będzie bądź nie będzie emitowana kampania;
- Jeśli definitywnie musisz skorzystać z dodatkowo płatnych narzędzi - porównaj oferty kosztowe, wady i zalety wszystkich dostępnych na rynku i wiarygodnych narzędzi do monitoringu Brand Safety;
- Wybierz rozwiązanie, które będzie optymalne pod wszystkimi możliwymi aspektami (koszty, funkcjonalności, użyteczność platformy, sposób obsługi itp.);
- Pamiętaj, że mocno restrykcyjne podejście do implementacji narzędzi Brand Safety w praktyce może istotnie podnieść koszty kampanii;
- Jeśli masz możliwość, skorzystaj z konsultacji agencji lub domu mediowego, która na bazie wypracowanych doświadczeń (również z innych rynków) może doradzić satysfakcjonujące rozwiązania;
- Współpracuj z zaufanymi i doświadczonymi wydawcami;
- Wprowadź monitoring i raportowanie.

5. Domy mediowe i agencje a Brand Safety

Zagadnienie Brand Safety, sposób podejścia do tematyki, radzenia sobie ze związanymi z tym wyzwaniami, czy też wypracowanie standardów powinny stanowić integralną część polityki każdej nowoczesnej agencji i domu mediowego. Kompleksowa obsługa pod kątem Brand Safety obecnie nie jest opcją a „must have", będącą nierzadko elementem procesu przetargowego czy kluczowym zapisem umowy o współpracy. Starając się zapewnić jak najwyższą jakość realizacji kampanii swoich klientów, agencje dbają o dostarczenie narzędzi i know-how, które zapewnią markom bezpieczną ekspozycję.

Niezwykle ważna jest komunikacja z reklamodawcą odnośnie jego oczekiwań, ewentualnych wymagań na szczeblu globalnym i/lub lokalnym oraz dokładnej charakterystyki kryteriów Brand Safety dla każdej promowanej marki. Wszelkie działania obejmować powinny obustronne zrozumienie wypracowanych procedur akceptowania i decyzyjności.

Implementacji strategii Brand Safety dla danego klienta powinna towarzyszyć analiza pożądanych działań i procedur, wykorzystywanych narzędzi czy potencjalnych zagrożeń takich jak np. spadek potencjału wykorzystania danego zasobu (ang. *inventory*) reklamowego czy też brak możliwości emisji w którymś z popularnych kanałów.

Rolą agencji jest nie tylko bycie odbiorcą oczekiwań klientów, ale także występowanie w roli eksperta czy edukatora. Do jej zadań należy doradztwo w zakresie najlepszych dostępnych rozwiązań, przedstawienie i rekomendowanie narzędzi (monitoringu, blokowania treści, analizy), konsultowanie konkretnych parametrów związanych z bezpieczeństwem marki podczas emisji kampanii (słowa kluczowe, kategorie, treści, blacklisty), planowanie ekspozycji u zaufanych wydawców, a wreszcie raportowanie i omawianie wyników z uwzględnieniem wskaźników informujących o spełnieniu przyjętych dla reklamodawcy standardów.

Wszystkie te działania powinny uwzględniać szerzenie wiedzy wśród klientów, szczególnie jeżeli chodzi o prowadzenie konkretnych działań na ich markach. Warto również śledzić światowe rozwiązania w dziedzinie Brand Safety - dzięki wymianie doświadczeń z innymi rynkami możliwe jest m.in. wdrożenie niestandardowych metod zapewniania bezpieczeństwa marce lub rozwijanie procedur już istniejących, bazujących na alternatywnych pomysłach.

Należy również pamiętać, że działania z zakresu bezpieczeństwa marki obejmują wiele podmiotów na rynku reklamy – a więc również i wydawców. Do zadań agencji należy reprezentowanie reklamodawcy i przedstawienie jego wytycznych co do treści, przy których pojawia się reklama, a więc dopuszczalnej tematyki, stylu prezentowanego contentu czy zawartości materiałów wizualnych (wideo, zdjęcia) obecnych na stronie. Dialog na linii agencja-wydawca i przedstawianie wzajemnych oczekiwań służy nie tylko interesom każdego z trzech podmiotów, ale także rozwojowi całego rynku reklamy digital poprzez szerszą dyskusję i finalne wypracowanie standardów.

Rekomendowane działania po stronie agencji/domu mediowego:

- Zadbaj o opracowanie całościowej strategii działań związanych z zagadnieniem Brand Safety (procedury, narzędzia, blacklisty itd.), edukuj i uświadamiaj zalety jej posiadania;
- Upewnij się, jakie oczekiwania ma klient odnośnie bezpieczeństwa każdej z jego marek, poznaj dogłębnie procedury i kwestie akceptacji przed startem kampanii;
- Zdiagnozuj ryzyka, jakie mogą towarzyszyć polityce Brand Safety klienta w kontekście realizacji kampanii (np. wzrost kosztów działań, ograniczenie inventory, rezygnacja z danego typu aktywności itd.);
- Wykorzystuj dostępne na rynku (lub wybrane przez klienta) narzędzia do monitorowania, blokowania i analizy kampanii Twoich klientów pod kątem Brand Safety;
- Prowadź dialog z dostawcami na temat oczekiwań Twoich klientów i możliwości unikania ryzyka ekspozycji marki przy niebezpiecznych z jej punktu widzenia treściach;
- Analizuj kampanie i ewaluuj wydawców, twórz profile zaufanych stron i treści, przy których marka klienta będzie bezpieczna;
- Edukuj klientów, którzy nie są świadomi ryzyka związanego z niewłaściwą ekspozycją ich marek;
- Dbaj o poszerzanie własnej wiedzy (np. z innych rynków), która będzie budowała Twoją przewagę konkurencyjną i pracowała na zadowolenie klienta ze świadczonych mu usług.

6. Serwisy pirackie

Jak pokazują dane, jedną z największych obaw marketerów w kontekście Brand Safety jest ryzyko kojarzenia marek z działalnością przestępczą taką jak m.in. piractwo internetowe, które bardzo często wiąże się z rozprowadzeniem złośliwego oprogramowania, wyłudzaniem pieniędzy, kradzieżą danych czy nachalną lub szkodliwą formą reklamy.

Niestety reklamodawcy i domy mediowe często nie mają możliwości ocenienia, czy działalność danego portalu jest zgodna z prawem. Tym bardziej, że serwisy pirackie chętnie tworzą pozory legalności poprzez pobieranie opłat abonamentowych czy umieszczanie reklam.

Ułatwieniem w rozpoznaniu legalności serwisów może być bezpłatne narzędzie jakim dysponuje i dzieli się z rynkiem reklamowym Stowarzyszenie Sygnał[9]. Na podstawie informacji na temat stron internetowych zamieszczających treści audiowizualne bez zgody właścicieli praw, a także dzięki regularnemu monitoringowi emitowanych w nich reklam i innych form monetyzacji, opracowana została tabela zgłaszanych przez firmy członkowskie naruszeń. Narzędzie jest także w pełni zintegrowane z powszechnie stosowanym przez rynek reklamy badaniem Gemius AdReal™. Wszystkie firmy przystępujące do inicjatywy Follow the Money[10], otrzymują bieżące dane wskazujące na serwisy, które w sposób bezsprzeczny łamią obowiązujące prawa. Tym samym, marketerzy chcący zapewnić bezpieczeństwo marki swoich klientów poprzez bardziej świadome lokowanie budżetów reklamowych, już od samego początku planowania kampanii mogą wykluczać serwisy pirackie ze swych media planów, jednocześnie przyczyniając się do odcinania tychże od źródeł finansowania.

---

[9] Stowarzyszenie Sygnał działa na rzecz poszanowania własności intelektualnej od 2001 roku. Obecnie w jego w skład wchodzi 18 największych firm z branży mediów i telekomunikacji.

[10] Inicjatywa na rzecz odcinania serwisów naruszających od źródeł finansowania, wskazywana przez UE jako najskuteczniejszy sposób walki z komercyjną nielegalną dystrybucją treści online, więcej: „Copyright enforcement online: policies and mechanisms", Europejskie Obserwatorium Audiowizualne (EOA), 14.01.2016.

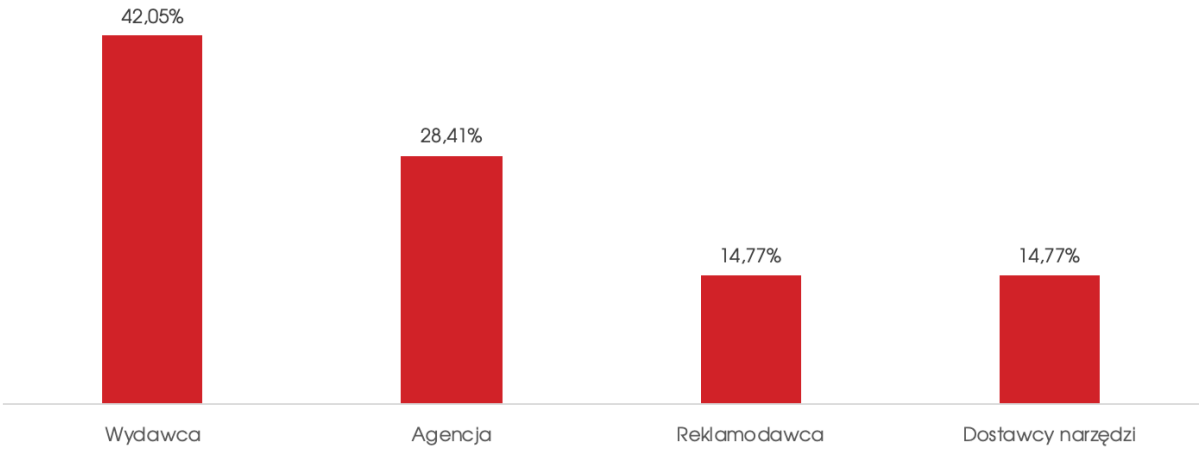
7. Działania wydawców a bezpieczeństwo marek

Powierzchnia reklamowa udostępniona przez wydawcę powinna gwarantować emisję reklam jedynie w bezpiecznym otoczeniu zgodnie z wcześniejszą definicją i kategoriami treści.

Dobrą praktyką wydawców jest umożliwienie blacklistowania oraz whitelistowania emisji kampanii. Wydawca powinien zapewnić opcję filtrowania emisji na podstawie listy wytycznych opartych o domeny, adresy stron lub kategorie witryn.

Podczas realizacji kampanii reklamowej, ważna jest współpraca reklamodawcy oraz wydawcy i szybka reakcja w przypadku zidentyfikowania miejsc zagrażających bezpieczeństwu marki polegająca na wykluczeniu w trakcie trwania emisji wybranej powierzchni, witryny, adresów URL.

Elementem filtrowania kampanii pod kątem Brand Safety może być również zarządzanie emisji za pomocą pozycji na stronie jak np. emisja ATF/BTF, formaty występujące w treści/samodzielnie, powierzchnia redakcyjna/sekcja komentarzy.



Pytanie: Która grupa interesariuszy jest w największej mierze odpowiedzialna za brand safety?[11]

7.1. Targetowanie i szczególne wytyczne

Szczegółowe metody targetowania pod kątem Brand Safety takie jak targetowanie demograficzne, po kontekście, słowach kluczowych, tagach, kategoriach OpenRTB, nacechowaniu emocjonalnym treści lub innych parametrach, leżą po stronie indywidualnej oferty każdego wydawcy.

[11] *Ankieta Brand Safety, IAB Europe, listopad 2019.*

Zapewnienie wyłączności reklamowej na stronie analogicznie pozostaje w gestii wydawcy, jego aktualnej oferty reklamowej oraz w ramach indywidualnych ustaleń z reklamodawcami.

7.2. User Generated Content a Brand Safety

Wydawcy posiadający User Generated Content (UGC) powinni dołożyć należytej staranności do zachowania standardów treści oraz jej moderację, a w zidentyfikowanych przypadkach, gdy reklama klienta pokazałaby się przy niepowołanych treściach, zobowiązują się do usunięcia takich treści. Wydawcy są odpowiedzialni za jakość komentarzy i ponoszą konsekwencje prawne, finansowe i wizerunkowe za treści, które pojawiają się na ich powierzchniach. Na rynku istnieje niewiele "dobrych" i w pełni skutecznych systemów moderacji komentarzy.

Większość wydawców udostępnia możliwość komentowania artykułów i informuje o stosowanym procesie moderacji. Narzędzia wykorzystywane do tych celów są autorskimi rozwiązaniami i opierają się na pre- bądź post-moderacji. Czołowe polskie serwisy informacyjne umożliwiają komentowanie artykułów tylko zidentyfikowanemu użytkownikowi, czy to na zasadzie aktywnego subskrybenta czy też utworzonego konta w samym serwisie bądź w serwisie społecznościowym (np. logowanie za pomocą konta Facebook).

Serwis	**Adres**	**Moduł komentarzy**	**Dostępność modułu komentarzy**	**Moderacja**
Wyborcza	wyborcza.pl	TAK	Subsrkrypcja, po zalogowaniu się	TAK
Onet	onet.pl	NIE	N/A	N/A
Wirtualna Polska	wp.pl	TAK	Wszyscy użytkownicy	TAK
Interia	interia.pl	TAK	Wszyscy użytkownicy po weryfikacji antybotowej (capcha)	TAK
mediaPPG /Polskapress	mediappg.pl	TAK	Na osobnej zakładce/ wszyscy użytkownicy	TAK

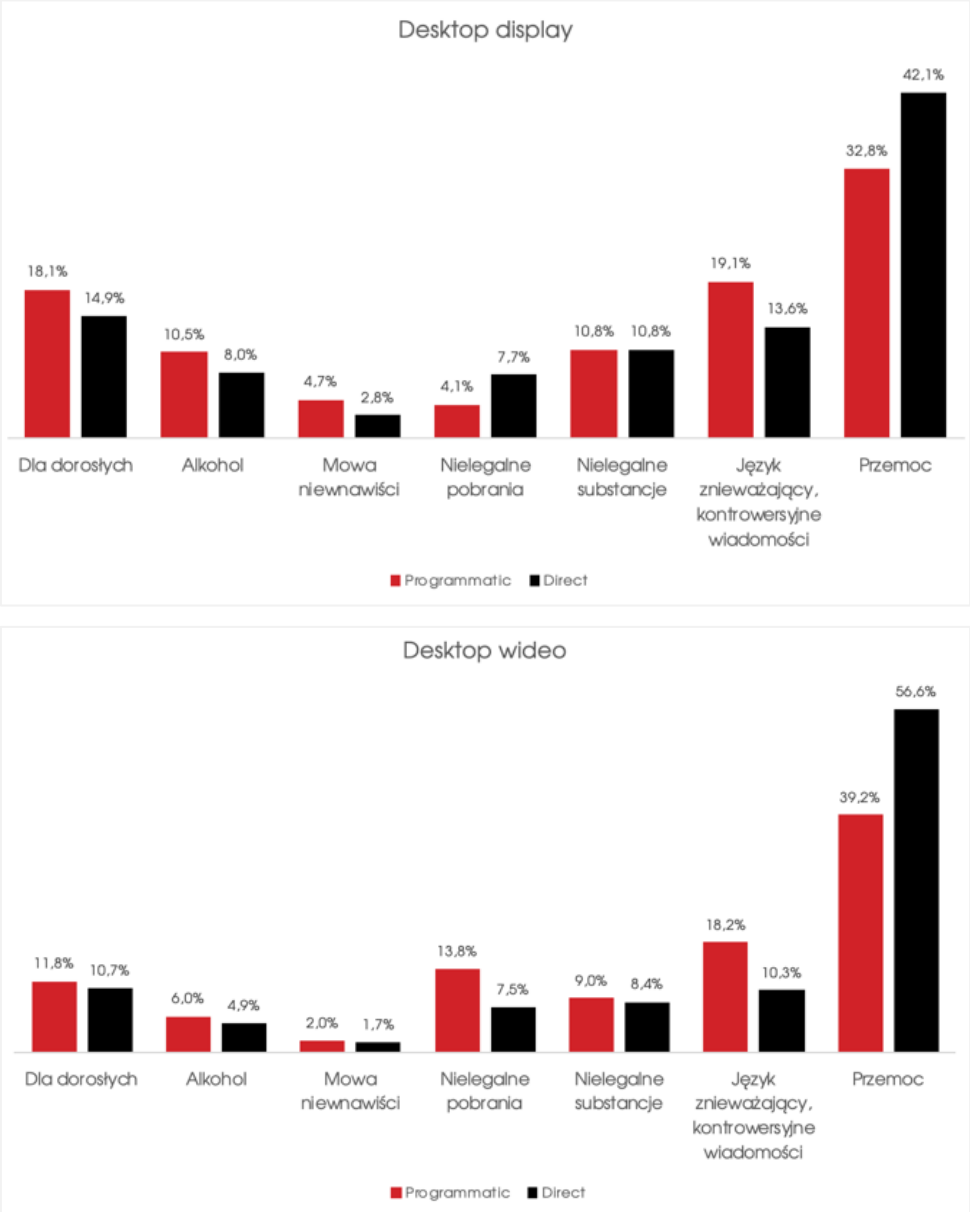
Polityka największych polskich wydawców do publikowania komentarzy od użytkowników oraz moderacji.

Rekomendowane działania po stronie wydawcy:

- Zadbaj, aby reklamy wyświetlały się obok trafnych, wysokiej jakości treści;
- Postaraj się o odpowiedni dobór produktów reklamowych pod kątem niskiej intruzywności, aby emisja reklam nie wpływała na ich negatywny odbiór przez użytkownika;
- Kontroluj wszelkiego rodzaju treści tworzone przez Twoich użytkowników i staraj się maksymalnie ograniczać wrażliwe treści lub wyłączać w ich otoczeniu emisję reklam;
- Opisuj i kategoryzuj treści w odpowiedni sposób - przy użyciu tagów i innych dostępnych narzędzi, aby umożliwić reklamodawcom wybór bezpiecznych z ich punktu widzenia treści;
- Dbaj o jakość reklam wyświetlanych w serwisie, aby uchronić reklamy Twoich klientów przed wyświetlaniem się w towarzystwie innych nieodpowiednich komunikatów;
- Opracuj procedurę szybkiej reakcji na reklamy pojawiające się w niewłaściwym otoczeniu kontekstowym;
- Postaraj się zapewnić reklamodawcom maksymalny poziom transparentności odnośnie tego, gdzie i komu wyświetlane są w Twoim serwisie ich reklamy.

8. Rodzaje treści a problem Brand Safety

Możliwości analizy treści i zapewnienia markom bezpieczeństwa emisji mogą się znacznie różnić w zależności od rodzaju contentu, w kontekście którego przekaz reklamowy jest wyświetlany. Zdecydowanie najprostsze pod tym kątem są treści tekstowe, natomiast mimo znacznego rozwoju technologii, analiza treści wideo jest dopiero w fazie wczesnego rozwoju i pierwszych testów na małych próbach.



Ocena stopnia ryzyka ze względu na kategorie treści oraz model zakupu (Programmatic vs. Direct), w podziale na display i wideo[12].

[12] Media Quality Report US, H1 2018, Integral Ads Science.

8.1. Teksty

Teksty są najprostszym rodzajem treści w kontekście analizy Brand Safety, w szczególności, jeśli są one odpowiednio otagowane i posegmentowane przez wydawcę. Zapewnia to reklamodawcom możliwość wykluczenia emisji ich reklam w otoczeniu niepożądanych kategorii treści już na etapie ustawiania kampanii i ich szczegółowego targetowania.

W razie potrzeby, aby zapewnić lepsze bezpieczeństwo emisji, klienci mają także możliwość wykorzystania analizy tekstu pod kątem słów kluczowych przy użyciu algorytmów oferowanych przez firmy takie Double Verify czy Integral Ad Science, które w przypadku wychwycenia na stronie niepożądanych zwrotów zablokują emisję kreacji należących do reklamodawcy.

8.2. Grafiki

Analiza i filtrowanie treści graficznych pod kątem Brand Safety są nieco trudniejsze ze względu na bardziej ograniczone możliwości technologiczne narzędzi. Mimo wszystko, widać znaczną poprawę w tym aspekcie na przestrzeni ostatnich lat.

W grudniu 2018 roku firma GumGum opublikowała aktualizację swojego badania[13] w kontekście bezpieczeństwa marki, według którego 21% marketerów stwierdziło, że ich narzędzia do kontroli i poprawy bezpieczeństwa marki obejmowały rozpoznawanie obrazów (dwa lata wcześniej było to jedynie 12%).

Jednak wartość tych danych jest znikoma, jako że dostawcy bezpieczeństwa marki często nie skanują faktycznie zawartości obrazu czy grafiki, ale używają w tym celu jedynie informacji kontekstowych, takich jak tagi graficzne i inne metadane.

8.3. Wideo

Treści wideo niosą ze sobą znacznie większy i bardziej złożony zestaw uwarunkowań, zaś metody badania i poprawy Brand Safety w kontekście tego produktu są dopiero w początkowej fazie rozwoju. Możemy jednak wymienić przynajmniej część podstawowych zasad, którymi powinny kierować się podmioty działające w internecie, aby do minimum ograniczyć ryzyko po stronie marek, promujących swoje towary i usługi.

[13] *The Brand Safety Crisis One Year Later, GumGum, 2018.*

Jak opisuje to Integral Ad Science w raporcie zatytułowanym „Bezpieczeństwo marki: Niezbędnik"[14] treści otaczające film (tytuły, opisy, słowa kluczowe) można wykorzystać do oceny jego potencjalnego ryzyka i zagrożenia dla bezpieczeństwa marki. Jednak znacznie trudniejsze i o wiele bardziej kosztowne jest przeanalizowanie samej treści materiałów wideo. Chodzi tu o zarówno warstwę werbalną, wizualną, a nawet ścieżkę dźwiękową, która może zawierać np. obraźliwy język.

Na rynku pojawiają się już różnego rodzaju firmy oferujące technologie wspierające weryfikację złożonych materiałów audiowizualnych, jednak wiąże się to zwykle z dużej skali kosztami technologicznymi, a dodatkowo problemem i ograniczeniem jest wersja językowa materiałów (zdecydowana większość narzędzi działa w oparciu o język angielski). Dopóki więc nie zostanie opracowane lepsze i bardziej osiągalne finansowo rozwiązanie technologiczne, własna weryfikacja treści wideo przez wydawcę oraz odpowiednie ich opisywanie i kategoryzowanie nadal będą nieocenione w ograniczeniu ryzyka reklamodawcy.

Aktualnie, jako praktyczne zastosowania w zakresie automatycznej weryfikacji bezpieczeństwa, treści wideo stanowić mogą jedynie narzędzia analizujące treści okalające wideo jak np. tytuł, nagłówek lub alternatywnie treść artykułu. W przypadku materiałów wideo stanowiących element artykułów i szerszych opracowań tekstowych, jest to zazwyczaj wystarczający model weryfikacji. Dla szerokiego grona serwisów VOD oraz serwisów UGC (User Generated Content), w których wideo stanowi treść przewodnią strony, to jednak zdecydowanie za mało.

Treści wideo serwisów VOD podlegają obowiązkowej i określonej prawnie kategoryzacji wiekowej i odpowiedniemu oznakowaniu wizualnym materiałów. Z tego względu zdecydowana większość wydawców działających na polskim rynku dokonuje dokładnej klasyfikacji i kategoryzacji materiałów. Zazwyczaj klasyfikacja obejmuje nie tylko dopuszczalność treści dla określonej kategorii wiekowej, ale także kategoryzację rodzaju treści, tematyki itp. To pozwala klientowi/marce, we współpracy z wydawcą, na dokładne określenie tematyki, przy jakiej dana marka chce się wyświetlać. Dopasowanie treści w przypadku większych wydawców oraz dostawców VOD można więc opierać na klasyfikacji treści okalających (np. tytuł, opis) oraz kategoryzacji treści stosowanej przez wydawców.

Największe wyzwanie stanowią dostawcy treści UGC oraz wydawcy, którzy nie kategoryzują treści wideo i u których jednocześnie stanowi ono treść główną strony. W przypadku tych podmiotów sama analiza treści okalających będzie

[14] *Brand Safety: the essentials, IAS, 2014.*

niewystarczająca. Taka sytuacja może mieć miejsce chociażby u wydawców niezarejestrowanych na terytorium Polski. Na znacznej części serwisów z treściami UGC, materiały wideo zamieszczane przez użytkowników nie podlegają zatwierdzeniu przez moderatorów czy redakcję serwisu. W takiej sytuacji nie można mówić o skutecznym wypełnieniu warunków bezpiecznej treści dla marki.

9. Narzędzia wspierające Brand Safety

Ponieważ kwestie związane z bezpieczeństwem marki stają się coraz poważniejszym problemem dla reklamodawców, na rynku pojawiło się wiele narzędzi, które mają zaradzić tym problemom lub zwiększyć bezpieczeństwo kampanii na poziomie samej transakcji.

Większość ze wspomnianych we wcześniejszych rozdziałach produktów opiera się na bazie algorytmów, które pomagają zidentyfikować bezpieczne dla marki, zabezpieczone przed oszustwami i widoczne dla użytkownika treści reklamowe jeszcze przed ich emisją na stronie. Częścią tego rozwiązania jest zazwyczaj analiza kontekstowa, która zapewnia przegląd treści i klasyfikację w czasie rzeczywistym w odniesieniu do większości adresowalnej powierzchni otwartej sieci. Wśród narzędzi wspierających Brand Safety wymienić możemy takie platformy jak: IAS, Moat, DoubleVerify, Meetrics, Gemius, Nielsen, Cheq, Matis, TrustMetrics, WhiteOps i wiele innych.

Problematyczne w doborze narzędzi do Brand Safety jest to, że nie posługują się one jednym standardem, a funkcje choć pozornie zbliżone, w praktyce mogą działać w zupełnie inny sposób. Jak więc marketerzy mogą określić, które narzędzie najlepiej spełni ich potrzeby?

Warto posłużyć się poniższym zestawem pytań:

1) Jak dostawca definiuje bezpieczeństwo marki?

Niestety, nie ma jednej powszechnie uzgodnionej definicji bezpieczeństwa marki. Przed wybraniem rozwiązania upewnij się, że definicje platformy są zgodne z Twoimi. Jeśli nie, sprawdź, czy są w stanie dopasować zakres do Twoich potrzeb.

2) W jaki sposób rozwiązanie wpływa na Brand Suitability?

Podczas gdy niektóre miejsca docelowe reklam są wręcz szkodliwe i problematyczne, inne po prostu nie są idealne. Bezpieczeństwo marki odnosi się do problemów, które mogą zaszkodzić reputacji i/lub wynikowi marki. Miejsce docelowe, które po prostu nie jest odpowiednie, może postawić reklamodawcę w niewygodnej sytuacji - ale nic poza tym. Ważne jest, aby wybrać platformę, która może dokonać tego kluczowego rozróżnienia.

3) W jaki sposób narzędzie rozróżnia różne środowiska?

Wiele marek dąży do tego, by ich reklamy były wyświetlane w różnych środowiskach cyfrowych, od komputerów, po urządzenia mobilne czy Smart TV. Podczas prowadzenia kampanii na różnych urządzeniach bardzo ważne jest, aby wybrane rozwiązanie technologiczne mogło rozróżniać środowiska i związane z nimi ryzyka.

4) Jak współdziała to narzędzie z innymi platformami reklamowymi?

Ostatecznie bezpieczeństwo marki stanowi problem dotyczący całego ekosystemu. Wystarczy jedno słabe ogniwo, aby pojawił się problem, który dotknie wszystkich innych. Idealne rozwiązanie technologiczne ma głęboką integrację ze wszystkimi zaangażowanymi podmiotami zarówno po stronie podaży, jak i popytu.

5) W jaki sposób rozwiązanie kategoryzuje treści?

Każde urządzenie ma swoją definicję tego, jak wyglądają zasoby premium, a jak potencjalnie problematyczne mogą być poszczególne miejsca docelowe. Im bardziej szczegółowe dane są dostępne z poziomu konta klienta, tym większa możliwość rozwiązania problemu i bardziej prawdopodobne jest uniknięcie niebezpiecznego miejsca docelowego.

6) Kiedy wdrażana jest ochrona bezpieczeństwa marki?

W ramach reklamy cyfrowej narzędzia bezpieczeństwa marki działają albo przed, albo po wzięciu udziału w licytacji i złożeniu oferty przez reklamodawcę. Większość narzędzi oferuje pierwszą opcję i skanuje stronę pod kątem z góry określonego zestawu reguł, aby upewnić się, że strona, na której pojawi się reklama, jest odpowiednia. Wyzwanie związane z tą metodą polega na tym, że każda taka decyzja zapada w mniej niż 200 milisekund. Należy więc podejmować je na tyle szybko, aby nie tracić okazji do dotarcia do odbiorców.

Drugą opcją jest weryfikacja powierzchni po wyświetleniu reklamy. Zamiast aktywnie zapobiegać wyświetlaniu reklamy w niebezpiecznych środowiskach, narzędzie raportuje, gdzie były wyświetlane reklamy poprzedniego dnia i pozwala reklamodawcom określić, czy wszystkie miejsca docelowe są odpowiednie i czy chcą wprowadzić jakiekolwiek zmiany w regułach dla kolejnych uruchomień.

7) W jaki sposób narzędzie określa, gdzie wyświetla się reklama?

Na to z pozoru proste pytanie, odpowiedź nie zawsze jest oczywista. Na przykład, gdy oszustwa takie jak fałszowanie domen i fałszowanie SDK stają się coraz bardziej

powszechne, czasami trudno jest ustalić, gdzie reklama się wyświetlała. Ustalenie, czy reklama była widoczna i pojawiła się w oczekiwanej lokalizacji, może być trudne. Używane narzędzie do zabezpieczania marki powinno uwzględniać tego typu sytuacje.

8) Czy narzędzie stosuje inne taktyki oprócz białych i czarnych list?

Czarne i białe listy należą do najczęściej stosowanych taktyk bezpieczeństwa marki. Czarne listy obejmują blokowanie niektórych warunków lub właściwości. Białe listy pozwalają na wyświetlanie reklam tylko w określonych predefiniowanych scenariuszach. Oba narzędzia są w dużej mierze skuteczne, ale czasami aż nazbyt. Mogą bowiem uniemożliwić marce uzyskanie maksymalnego możliwego zasięgu kosztem bezpieczeństwa marki. Dobre narzędzie wykorzystuje więcej technik w celu szerokiego dotarcia do pożądanych odbiorców przy jednoczesnej gwarancji bezpieczeństwa.

9) W jaki sposób narzędzie podchodzi do niejednorodnych treści?

W niektórych przypadkach łatwo jest ustalić, czy dana powierzchnia jest bezpieczna dla marki czy nie. Na przykład witryna pornograficzna jest praktycznie całkowicie niedostępna dla większości marek z punktu widzenia bezpieczeństwa marki. Ale co z aplikacjami lub witrynami z wiadomościami zawierającymi treści generowane przez użytkowników? Chociaż w jednym przypadku mogą być one w porządku, w innych mogą być całkowicie nieodpowiednie. Idealnie, gdy narzędzie ma możliwość określenia bezpiecznych dla marki miejsc docelowych na poziomie poszczególnych treści.

10. Brand Safety a programmatic

Jak informuje eMarketer (2018)[15], bezpieczeństwo marki jest obecnie jednym z kluczowych problemów dla ponad 59% reklamodawców kupujących odsłony w tym kanale. Wraz z rozwojem programatycznego modelu zakupowego, przesuwaniem budżetów, a także rosnącą liczbą podmiotów biorących udział w procesie, na znaczeniu będą zyskiwały wszelkie rozwiązania wspierające Brand Safety przykładowo ads.txt, czy Kodeks Dobrych Praktyk Reklamy Programmatic IAB Polska[16].

10.1. Open Market vs Private Market Place

Zarówno kupujący, jak i sprzedający w ostatnich dwóch latach przyczynili się mocno do wzrostu popularności transakcji typu Programmatic Direct. Wydawcy domagali się większej kontroli nad tym, jakie reklamy wyświetlają się na ich stronach internetowych i jak wykorzystywane są dane ich odbiorców. Reklamodawcy natomiast stali się bardziej nieufni wobec otwartej aukcji i potrzebowali lepszego dostępu do zasobów powierzchni premium. Tendencje te doprowadziły do większej liczby ofert Private Market Place (PMP), które dają reklamodawcom i wydawcom większą możliwość negocjowania warunków cenowych i dostępu do danych niż Open Market.

Chociaż główną ideą stojącą za wprowadzeniem programatycznego zakupu reklam było wyeliminowanie potrzeby relacji kupujący-sprzedający, ten trend wskazuje, że umowy indywidualne oraz dodatkowy zakres bezpieczeństwa zapewniany przez znajomość serwisów, na których zachodzi emisja reklam zyskuje na znaczeniu. Należy jednak pamiętać, że wszystko co dobre ma swój koszt i ze względu na lepszą jakość powierzchni oferowanych w PMP, reklamodawcy muszą płacić za odsłony w tym modelu odpowiednio wyższe stawki, a także zawężają sobie w ten sposób bazę użytkowników do których mogą dotrzeć - ryzykując realizację założeń ilościowych kampanii.

[15] *Five Charts Explaining the State of Brand Safety, eMarketer, 2018.*

[16] *Kodeks Dobrych Praktyk Reklamy Programmatic, IAB Polska.*

11. Podsumowanie

Bezpieczeństwo marki jest ciągle ewoluującym i trudnym do osiągnięcia w pełni celem. Im bardziej branża się rozwija i zmienia, tym większa jest potrzeba, by skutecznie identyfikować nowe wyzwania i opracowywać coraz skuteczniejsze ich rozwiązania. Jednak świadomi problemów już istniejących, a także stale rozwijających się narzędzi i strategii będących już w naszym zasięgu, powinniśmy szukać, testować i opracowywać jak najskuteczniejsze rozwiązania.

Bezpieczeństwo marki jest niezwykle ważnym, ale nadal nie do końca sprecyzowanym obszarem. Mamy nadzieję, że przedstawiony zbiór dobrych praktyk pomoże podmiotom działającym w świecie cyfrowym odczarować Brand Safety i dostarczyć wielu praktycznych rozwiązań.

12. Syllabus

Ad Fraud: wszystkie celowe działania związane z emisją reklam (reklamy display, reklamy wideo, reklamy w aplikacjach, reklamy efektywnościowej (performance'owe) i content marketing) w miejscu (serwisie internetowym/aplikacji) lub do grupy docelowej innej niż ustalone w warunkach kontraktowych. Działanie takie generuje bezpośrednio stratę finansową dla reklamodawcy (także dla wydawcy) lub utratę możliwości zarobkowej.

Ad Server: system informatyczny umożliwiający emisję i zarządzanie internetowymi kampaniami reklamowymi, a także raportowanie i analizę wyników kampanii.

Ad Exchange: to swego rodzaju internetowy rynek, na którym towarem obracanym w czasie rzeczywistym jest przestrzeń reklamowa. Kontakt tutaj mogą nawiązać między sobą sprzedawcy (redaktorzy sieci, sieci powiązane z reklamą) i nabywcy (agencje reklamowe, klienci bezpośredni).

Brand Safety (pl. *bezpieczeństwo marki*): to szereg działań oraz narzędzi, którymi posługują się podmioty biorące udział w realizacji procesu reklamowego, a które mają na celu stworzenie środowiska niewpływającego negatywnie na odbiór marki/produktu/usługi, oraz nie naraża marki na straty wizerunkowe, finansowe czy negatywne skutki prawne. Dotyczy zatem zapewnienia dla każdej emisji reklamy odpowiedniego kontekstu, w którym reputacja marki nie zostanie naruszona.

Cross-device: łączenie identyfikatorów jednego użytkownika na różnych platformach (desktop, tablet, smartfon). Dzięki temu można kierować reklamę do wybranych użytkowników bez względu na to, z jakiego urządzenia w danej chwili korzystają. Umożliwia również analizę wpływu różnych kanałów komunikacji (atrybucja).

DSP (ang. *Demand-Side Platform*): platforma przeznaczona dla kupujących, stanowiąca panel do zarządzania kampaniami prowadzonymi w modelu programmatic oraz raportowania wyników.

Floor price: to minimalna cena za daną powierzchnię akceptowana przez wydawcę na poziomie aukcji otwartej. Ceny minimalne można ustawić na serwerze reklam na różne sposoby, na przykład na poziomie domeny, geografii, rozmiarze reklamy, miejscu docelowym lub na poziomie użytkownika. Każdy serwer reklam inaczej obsługuje progi cenowe. Na przykład wydawcy, którzy ustawili zbyt wysoką cenę

minimalną, mogą napotkać problem niskiego wypełnienia, a tym samym znacząco wpłynąć na ogólny zysk.

Fake news: fałszywa wiadomość, często o charakterze sensacyjnym, publikowana w mediach z intencją wprowadzenia odbiorcy w błąd w celu osiągnięcia korzyści finansowych, politycznych lub prestiżowych.

OpenRTB (ang. *Real-Time Bidding*): protokół obsługujący komunikację pomiędzy platformami DSP i SSP. Odpowiada za wycenę każdej dostępnej odsłony reklamowej osobno, w ramach modelu aukcyjnego, w czasie rzeczywistym.

Open Market: inaczej otwarta aukcja, dostępna na tych samych zasadach dla wszystkich kupujących. W Open Market informacja o możliwości zakupu odsłony jest wysyłana do uczestników rynku i wygrywa ten, kto oferuje najwięcej. Dla wydawcy taki model daje możliwość optymalizacji wykorzystania powierzchni (każda odsłona jest sprzedawana za maksymalnie wysoką cenę, jaką ktoś chce zapłacić) oraz dostęp do puli kampanii niedostępnych w modelu direct. Dla reklamodawcy uczestnictwo w takim rynku oznacza dostęp do najszerszego możliwego inventory i elastyczne kształtowanie wydatków. Przy dużej ilości dostępnej powierzchni cena CPM może być bardzo niska.

PMP (ang. *Private Market Place*): inaczej Private Auction (PA), to tradycyjna licytacja, mająca jednak miejsce zanim dojdzie do aukcji w Open Market. Żeby dołączyć do PA niezbędne jest wcześniejsze zaproszenie wydawcy oraz dostosowanie się do tzw. floor price, czyli minimalnej stawki bid, jaką należy zaoferować, aby w ogóle przystąpić do licytacji. Również ten typ PMP wiąże się ze zwiększonymi kosztami emisji (większość floor price jest znacznie wyższa niż stawki znane z Open Market), dlatego kampanie prowadzone na tych powierzchniach powinny cechować się wysokimi wskaźnikami kliknięć i konwersji, jak ma to miejsce np.w remarketingu. Warto z drugiej strony zauważyć, że korzystanie z PMP pozwala korzystać z dodatkowych możliwości w zakresie uzyskiwania brand safety, dostępnych jedynie w ad serwerach wydawców. W zależności od używanej przez nich technologii może to sprowadzać się np. do wykluczania niektórych działów, kategorii tematycznych lub haseł (tagów) w całych serwisach (np. wykluczenie artykułów o wypadkach z serwisu informacyjnego, albo wykluczenie z emisji na całym serwisie dotyczącym zdrowia sekcji powiązanych ze zdrowiem seksualnym), albo do targetowania wyłącznie na konkretne artykuły, oznaczone przez zewnętrzne narzędzie jako bezpieczne z punktu widzenia danej marki.

Prebid: to nazwa technologii typu open source, która zarządza procesem technicznym emisji reklam z platform SSP zapewniając wspólny limit czasu, wybierając najwyższą stawkę zwracaną na giełdach i wstrzykując tę wartość do serwera reklam.

Postbid: mechanizm licytacji który pozwala źródłom popytu wydawcy konkurować na jednej aukcji na podstawie ceny po tym, jak serwer reklam odmówił wyboru elementu zamówienia sprzedawanego bezpośrednio lub w kanale programatycznym.

Postbuy: pomiar skuteczności reklamy na zakończenie zakupu mediów. Skuteczność mierzy się za pomocą testów wycofania i rozpoznania przez konsumentów oraz pod względem świadomości produktu, znajomości produktu i sprzedaży produktu, chociaż wpływ reklamy na sprzedaż może nie być natychmiast zauważalny ze względu na wpływ innych zmiennych zewnętrznych, takich jak konkurencyjne produkty, problemy z dystrybucją lub wyjątkowe działania konkurencji.

Preferred deal: to określenie stosowane w reklamie w modelu RTB. Jest to umowa między wydawcą lub właścicielem strony a platformą RTB (SSP lub DPS) na sprzedaż powierzchni reklamowej w stałej cenie. W normalnej sytuacji w RTB obowiązuje minimalna cena licytacji (tzw. floor price), wygrywa licytację ten, kto poda najwyższą cenę, a końcowa cena to cena wyższa o cent od stawki wylicytowanej przez drugiego w kolejności licytującego. W przypadku preferred deal aukcja również następuje, aby wyłonić zwycięzcę, jednakże odsłona sprzedawana jest w stałej stawce równej stawce minimalnej lub innej wspólnie ustalonej (tzw. fixed price). Najczęściej taka umowa wydawcy z platformą RTB ma najwyższy priorytet w licytacji i sprzedaży odsłony przez daną platformę RTB, choć zdarza się sytuacja odwrotna – że platforma RTB nie ma gwarancji dostępności powierzchni reklamowej w przypadku przelicytowania stawki przez innego reklamodawcę.

SSP (ang. Supply-Side Platform): platforma dla wydawców, z poziomu której udostępniają oni powierzchnię oraz organizują i optymalizują jej sprzedaż w omawianym modelu.

RTB: to model sprzedaży w programmatic, dzięki któremu wartość każdej poszczególnej odsłony udostępnianej przez wydawcę jest wyceniana w modelu aukcyjnym (aukcja drugiej ceny). Potencjalni reklamodawcy określają, ile maksymalnie są w stanie zapłacić za emisję reklamy i na tej podstawie wyceniana jest emisja.

Viewability: to miara określająca jaki proc. odsłon reklamy znajdowało się w polu widzenia użytkownika (tj. było widocznych na ekranie), dzięki czemu użytkownik mógł zapoznać się z reklamą. Według standardu IAB[17], reklama może być uznana za widzialną, jeśli przynajmniej połowa jej powierzchni była widoczna przez minimum sekundę na ekranie urządzenia (monitora lub ekranu).

[17] *Standard Viewability w kampaniach reklamowych online, IAB Polska.*

14. O IAB Polska

Związek Pracodawców Branży Internetowej IAB Polska jest organizacją zrzeszającą 240 najważniejszych firm polskiego rynku internetowego, w tym największe portale internetowe, sieci reklamowe, domy mediowe, agencje interaktywne, firmy technologiczne oraz reklamodawców. Jego głównym celem jest szeroko pojęta edukacja rynku w zakresie wykorzystania internetu jako skutecznego narzędzia prowadzenia biznesu i komunikacji marketingowej. Propaguje skuteczne rozwiązania e-marketingowe i reklamowe, oraz tworzy, prezentuje i wdraża branżowe standardy jakościowe. Przygotowuje raporty, badania rynku online i poradniki, m.in. Raport Strategiczny czy AdEx, którego wyniki są bazą analiz wydatków reklamowych. Jest organizatorem konferencji (Forum IAB, IAB HowTo), konkursów (MIXX Awards), warsztatów i szkoleń (Akademia DIMAQ). Jednym z flagowych projektów IAB Polska jest DIMAQ – standard kompetencji oraz program certyfikujący wiedzę z dziedziny e-marketingu.

IAB Polska działa od 2000 roku, jest częścią światowych struktur IAB, członkiem IAB Europe oraz IAB Tech Lab, a także Związku Stowarzyszeń Rada Reklamy, Krajowej Izby Gospodarczej i Business Center Club.