Reklam Doğrulaması

Ad Verification

IAB Türkiye Programatik Çalışma Grubu

Tarafından Hazırlanmıştır

Haziran 2018

İÇİNDEKİLER

REKLAM DOĞRULAMASI NEDİR?

Reklam doğrulama sistemleri; markaların reklamlarının isteklerine göre yayınlandığını onaylayan teknolojilerdir. Reklamların güvenli alanlarda gösterildiğini, ne kadar "görüntülenebilir" (viewable) olduğunu, hedeflemelerinin doğruluğunu onaylayarak, reklam sahteciliğinin belirlenmesi ve önlenmesinde kullanılırlar.

Reklam doğrulaması önemlidir çünkü kötü/ilgisiz içeriklerin yanında yer alan reklamlar markalara zarar verebilir. Ayrıca görüntülenemeyen ve/veya sahte reklamlar kampanya performansını ve ROI'yi etkiler.

Tüm bu nedenlerden ötürü doğrulama (verification) araçları hem programatik hem de programatik olmayan satın alma modellerinde ajans ve reklamverenler tarafından 3 ana konuda kullanılır.

- Görünürlük (Viewability)
- Reklam Kalitesi ve Sahtecilik (Ad Quality & Fraud)
- Marka Güvenliği (Brand Safety)

GÖRÜNÜRLÜK (VIEWABILITY)

Görünürlük ölçümünün hedefi, kullanıcının reklamı görme fırsatını olup olmadığını belirlemektir. Bu sebeple 3 soruya cevap verir:

- Reklam yayınlandı mı?
- Görünür alanda mıydı?
- Kullanıcının reklamı görme fırsatı var mıydı?

Buradan yola çıkarak bir dijital reklamın, yüzdesel olarak görüntülenme oranının belirli kriterlere göre ölçümlenmesi Görünürlük (Viewability); tüm gösterimler içindeki görünürlük kriterine uygun reklamların oranı da Görünürlük Oranı (Viewability Rate) olarak tanımlanır.

Görünürlük Standartları IAB, 3MS Girişimi (Making Measurement Make Sense) ve MRC (Media Rating Council) tarafından belirlenmiştir ve tüm dünyada bu standartlar kabul görmektedir. MRC görünürlük standartları:

1. Piksel: Reklam görselinin toplam kapladığı alanın en az %50'sinin aktif olan pencerede yer alması
2. Zaman: Görüntülü reklamların (display) kesintisiz en az 1 saniye, video reklamların ise kesintisiz 2 saniye süre ile aktif pencerede kalması.

Görünürlük ölçüm ve hedefleme hizmeti veren firmalar (Viewability Vendors) viewability metriği olarak MRC standartlarını baz alır. Buna ek olarak bu firmaların bazıları, ajansların veya markaların kendi belirledikleri görünürlük standartlarına göre ölçüm imkanı da sunar (örneğin, reklam alanının %100'ünün 5 saniye aktif pencere içerisinde kalması).

Görünürlükle ilgili detaylı bilgi için: IAB Türkiye Açıklıyor: Şimdi Görünür Gösterim Zamanı Raporu – IAB Türkiye Endüstri Standartları Yürütme Kurulu

REKLAM KALİTESİ VE SAHTECİLİK (AD QUALİTY & FRAUD):

Reklam kalitesi, reklamın yayınlandığı ortamın markaların "hijyen" standartlarına uygun olup olmadığını, reklamların gerçekten söylenen alanlarda yer alıp almadığını belirler. Reklam kalitesi araçları reklamverenlere ve ajanslara aşağıdaki soruların yanıtlarına ulaşmalarını sağlar:

1. Kampanyam nasıl ortamlarda yayınlandı/yayınlanacak?
2. Reklamlarım gerçekten bana taahhüt edilen reklam alanlarında yer aldı mı?
3. Reklamım sayfayı kaç tane başka reklamla paylaştı/paylaşacak?
4. Reklamım bir sahtecilik faaliyetine veya bana taahhüt edilmeyen bir duruma maruz kaldı mı?

5. Video reklamı verdiğim sayfada video oynatıcı var mıydı? Boyutları istediğim gibi miydi?

Reklam sahteciliği (Ad fraud) bir reklamın doğru mesajı, doğru alanda, doğru kişiye vermesini önleyen ve dijital reklam endüstrisi gelirlerinden haksız pay elde etme amaçlı yapılan faaliyetlerdir. Yasal olarak da suçtur. IAB - Ernst & Young Kasım 2015 tarihli "What is an Untrustworthy Supply Chain Costing US Digital Advertising Industry" raporunda göre sahtecilik türleri 3 ana grupta incelenir:

1. Geçersiz trafik (insan dışı trafik, görülemeyen reklamlar, reklam kodu korsanlığı vb.)
2. Zararlı Eklenti/Yazılım
3. Çalıntı İçerik

Sahtecilik farklı tekniklerle, hacker'lar yani yazılım korsanları tarafından gerçekleştirilebilir. Bu tekniklerden bazıları şunlardır:

Gizli Reklamlar (Hidden ads) → Kullanıcıya görünmeyecek şekilde sayfaya yerleştirilen reklamlardır.

Örneğin:

- Ad Stacking: *Tek bir reklam alanına birden çok reklam eklendiğinde sadece en üstteki reklam görüntülenebilir. Kullanıcı alttaki reklamları görmese bile, reklamveren gösterimler için ödeme yapmak durumunda kalabilir.*
- Pixel Stuffing: *Bir veya birden fazla reklamın; 1X1 pixel boyutunda yayınlanmasıdır. Bu nedenle bazı reklamlar yayınlanmış gibi raporlansa dahi web-sitelerinde gözle görülemez.*

Proxy trafik → Kullanıcı trafiği proxy cihazlar veya ağlar üzerinden yönlendirildiğinde kullanıcıya ait lokasyon gibi veriler anonimleştirilebilir. Lokasyon, reklamverenler için medya planlarının önemli bir parçasıdır. Ajanslar/markalar farklı bölgelerde reklam yapabilmek için normal görüntülenme maliyetinin üzerinde maliyetlere katlanır. Sahtecilik yapan taraflar web sitesi trafiğini farklı bir lokasyondan geliyormuş gibi göstererek haksız kazanç sağlar.

Çerez Sahteciliği → Çerezler (cookie) kullanıcı davranışlarını takip etmek için önemli bir araçtır. Aynı zamanda reklam performansını (talep, tıklama, satın alma vb.) veya kullanıcıların ilgi alanlarını belirlemeye yardımcı olur. Kullanıcının ziyaret ettiği A sitesi (gerçek site) yerine B sitesinden (tamamen farklı bir site) kullanıcıya çerez eklenir ve kullanıcı daha sonra dönüşüm (talep, tıklama, satın alma vb.) sağlarsa, bu veri çerezle B sitesine kaydedilir. Böylelikle B sitesinin ziyaretçileri yüksek kaliteli kullanıcılar olmasa bile öyleymiş gibi gösterilir.

Domain Sahteciliği (Domain Spoofing) → Real-time bidding (RTB)'de gerçekleşir. Reklamları düşük kaliteli web sitelerinde göstermelerine rağmen, premium web sitelerinde yayınlanıyormuş gibi göstermek için kullanılır. Etkileşimler ve kullanıcılar gerçektir ancak envanterler çarpıtılarak gösterilir ve çok daha yüksek CPM oranlarında değerlendirerek haksız kazanç sağlanır.

Reklam sahteciliğiyle ilgili detaylı bilgi için: IAB Türkiye Reklamda Sahtecilik Raporu – IAB Türkiye Endüstri Standartları Yürütme Kurulu

MARKA GÜVENLİĞİ (BRAND SAFETY)

Marka güvenliği araçları reklamların marka değerine zarar verecek içeriklerde çıktığı durumları raporlayan veya bunu önceden engelleyen araçlardır. Marka güvenliğine zarar verebilecek içerikler; markaların büyük çoğunluğu için güvenli olmayan kategoriler ve sektörden sektöre, markadan markaya değişen kategoriler şeklinde genelde 2 bölümde değerlendirilir.

Marka güvenliği açısından genel olarak zararlı görülen kategoriler alkol, kumar, terör, şiddet, yetişkinlere yönelik içeriklerdir. Bunlar tüm firmaların reklam gösterip markalarıyla eşleştirmesini istemeyecekleri içerik türleridir. Özel kategoriler ise markadan markaya, hatta kampanya bazlı dahi değişebilecek kriterleri içerir (örneğin, bir otomotiv firması için yüksek benzin fiyatları haberi).

Marka güvenliğiyle ilgili detaylı bilgi için: IAB Türkiye Marka Güvenliği Raporu – IAB Türkiye Endüstri Standartları Yürütme Kurulu

DOĞRULAMA (VERİFİCATİON) ARAÇLARI ÇALIŞMA MODELLERİ

Doğrulama (verification) araçları 3 sahtecilik türüyle ilgili olarak iki şekilde hizmet verebilir. Bazı firmalar her ikisini de kullanırken, bazıları sadece birine odaklanabilir. Bu çalışma modelleri:

1. Raporlama
2. Hedefleme/Engelleme

RAPORLAMA

Reklam yayın kodları veya kreatiflere eklenen ek kodlar aracılığıyla, belirlenen kriterlere göre görüntüleme (viewability) metrikleri, reklam kalitesi unsurları ve marka güvenliği kategorileri ölçülür. Bu ölçümler belirli sıklıklarda veya gerçek zamanlı olarak raporlanır. Doğrulama Raporları markalar/ajanslar tarafından farklı şekillerde değerlendirilebilir.

- Anlık olarak takip edilerek, istenmeyen durumlar oluşursa kampanya hedeflemesine müdahale edilebilir.
- Düzenli raporlanarak ilerideki kampanyalara içgörü sağlayabilir.
- Marka, mecra özel anlaşmalarında (Programmatic Direct) fiyat belirleyici unsur olarak kullanılabilir.

HEDEFLEME/ENGELLEME

Doğrulama araçlarıyla programatik ortamda belirlenen olumlu kriterlere sahip mecralar hedeflenebilir veya olumsuz kriterlerdeki mecralar engellenebilir. Bu, araçların teknolojik altyapılarına göre 2 şekilde yapılabilir:

PRE-BİD

Araç mecraya teklif verme aşamasında, mecranın istenen kriterlere uygunluğunu test eder ve tarihsel içerik test sonuçlarına göre açık artırmaya girme veya girmeme kararını verir. Bu

sistem reklam alanının satın alınmasını engellediğinden uygun olmayan ortamlara para ödenmesini engeller.

POST-BİD

Reklam alanı satın alındıktan sonra mecranın istenen kriterlere uygunluğunu test eder. Reklam alanının bulunduğu ortam kriterlere uymuyorsa, bu alanda reklam haricinde bir görsel gösterir (örneğin, düz beyaz bir görsel). Bu sistem reklam alanının satın alınmasını engellemez, sadece reklamın gösterilmesini engeller. Pre-bid'den farklı olarak, tüm envanterde satın alma fırsatı sağlar çünkü reklam doğrulama hizmetini sağlayan teknoloji, satın almadan sonra devreye girer.

SAHTECİLİK (FRAUD) HERKESİN PROBLEMİ

Yukarıda da detaylıca geçildiği gibi doğru reklamı, doğru kişiye, doğru zamanda ve görülebilir olarak sunabilmek günümüzün en önemli işlerinden biridir. Reklam sahteciliği, sadece görünmeyen, yanlış hedeflenen veya etkili olmayan bir envanterden ibaret değildir, aynı zamanda bir güven ihlalidir. Bu problem sadece reklamverenleri değil, aynı zamanda yayıncıları, ajansları, networkleri özetle reklamcılık endüstrisindeki tüm kurumları da etkiler.

Bu nedenle programatik olsun ya da olmasın, dijital medya satın almalarında daha iyi performans metriklerine yatırım yapmak, sahteciliği engellemek için doğrulama teknolojilerini mutlaka kullanmak gerekir.

VERİFİCATİON TEKNOLOJİLERİ

Markaların ve ajansların hizmetine sunulan birçok farklı doğrulama teknolojisi bulunur.

Pazarda hizmet veren doğrulama firmaları (alfabetik olarak): Adloox, comScore, DoubleClick, DoubleVerify, Integral Ad Science, Meetrics, MOAT, Sizmek – Peer39.

İki tür doğrulama firması vardır:

1. Gelişmiş doğrulama (advance verification) teknolojileri: Yukarıda belirtilen 3 ana doğrulama faaliyetinin tümünde post/pre-bid hedefleme ve raporlama hizmeti veren, asıl işi doğrulama olan firmalar
2. Temel doğrulama (basic verification) teknolojileri: Yukarıda bahsedilen hizmetlerin bir kısmını sağlayabilen ve asıl işi diğer dijital pazarlama faaliyetleri olan firmalar

TEKNOLOJİ SEÇİMİ

Bir teknoloji seçimi yapmadan önce dikkat edilmesi gereken konular:

- Marka güvenliği, reklam sahteciliği ve görünürlük konularında hizmet veriyor mu?
- Bu hizmetleri hangi formatlarda sağlıyor? (display, video, native)
- Bu hizmetleri hangi cihazlarda sağlıyor? (desktop, tablet, mobil)
- Tespit edebildiği sahtecilik türleri neler?
- Demand Side Platform'larına (DSP) entegrasyonları var mı? Eğer yoksa, DSP'lerde kullanmak için süreç nedir?
- Engelleme (Blacklist) / Hedefleme (Whitelist) / Kelime Bazlı (Keyword) listeleri tanımlama imkanı var mı?
- Teknolojileri, semantik (kelime bazlı değil, metnin bütünsel anlamının tespit edilebilmesi) olarak Türkçe içerikte çalışabiliyor mu?
- Markaya özel görünürlük tanımlamaları yapılabiliyor mu?
- Geriye dönük raporlar ne zamana kadar alınabiliyor?

Yukarıdaki sorular doğrulama teknolojilerinin en sık kullanılan özelliklerinin belirlenmesi için sorulmalıdır. Bunun dışında özel kullanımlar için değerlendirilmesi gereken önemli konular da olabilir.