reflektif
SOSYAL BİLİMLER DERGİSİ
JOURNAL OF SOCIAL SCIENCES

Reflektif Journal of Social Sciences, 2025, Vol. 6(2)

2025, Vol. 6(2), 735-757

DOI: 10.47613/reflektif.2025.239
Article type: Research Article

Received: 02.12.2025
Accepted: 01.05.2025
Published Online: 21.07.2025

Murat Uluk*

Sessiz ve Saklı: "Çerezsiz Dünya"da Çevrimiçi Gözetim
Silent and Hidden: Online Surveillance in the "Cookieless World"

Öz

Çerezsiz dünya, çevrimiçi gözetim süreçlerinde geleneksel yöntemlerden birisi olan çerezlerin kullanımının yerine geçecek yeni yöntemleri içeren bir konsepttir. Son 20 yılda çerezler çevrimiçi izleme ve gözetimin en önemli aracı haline gelmiştir. Büyük teknoloji şirketleri ve reklam sektörü bu veriler üzerinden kayda değer kazanç elde etmiştir. Çerezlerin bu alandaki kullanımının yarattığı mahremiyet endişeleri hem tarayıcılar tarafından engellenmelerine hem de yasalar tarafından katı kurallara tabi olmalarına neden olmuştur. Çerezlere alternatif bir yöntem arayışına giren sektör, yeni ürünler geliştirmiş ve yeni gözetleme taktikleri benimsemiştir. Çalışma, çerezsiz dünya kavramını, yeni nesil izleme yöntemlerini ve gizlilik üzerindeki etkilerini incelemeyi amaçlamaktadır. Yerli literatürde internet çerezlerine ait oldukça sınırlı çalışma varken, çerezsiz dünyayla ilişkili bir çalışma yer almamaktadır. Bu eksikliği gidermek üzere ilgili alandaki yabancı literatür ve belgeler doküman incelemesi yoluyla analiz edilmiştir. Elde edilen veriler yorumlayıcı bir yaklaşımla değerlendirilmiştir. Çalışmada, çerezsiz gözetim teknolojilerinin geleneksel yönteme kıyasla daha az görünür, daha zor tespit edilebilir ve engellenmesi zor olduğu görülmüştür.

Abstract

The concept of a "cookieless world" refers to emerging methods designed to replace cookies, a traditional tool in online surveillance processes. Over the past two decades, cookies have become a cornerstone technology for online tracking and surveillance, enabling significant profits for major technology companies and the advertising industry. However, privacy concerns surrounding the use of cookies have led to their increasing restriction by browsers and stringent regulation through legal frameworks. In response, the industry has sought alternatives by developing new products and adopting advanced surveillance tactics. This study explores the concept of a cookieless world, next-generation surveillance methods, and their implications for privacy. Although the existing Turkish literature includes only a limited number of studies on internet cookies, there is no scholarly work specifically focusing on the cookieless world. To address this gap, relevant international literature and documents in the field were analyzed through document analysis. The findings were then interpreted using an interpretive approach. The findings of this study reveal that cookieless surveillance technologies are less visible, more challenging to detect, and harder to block compared to traditional methods.

Anahtar Sözcükler
Çerez, çerezsiz dünya, gözetim, dijital reklam

Keywords
Cookie, cookieless world, surveillance, dijital advertising

* İstanbul Beykent Üniversitesi, uluk.murat@gmail.com, ORCID: 0000-0001-5923-8468.

Giriş

Çerezler, web tarayıcıları ile sunucular arasında bilgi alışverişini sağlayan küçük veri parçalarıdır (Kristol, 2001). Bilgisayar ile uzak sunucular arasındaki iletişimin anonimliği 1994'ten beri kullanımda olan çerezler ile son bulmuştur. Çerezlerin kullanımı uzak sunucu ile bilgisayar arasında doğrudan ve tanımlanabilir bir ilişki ortaya çıkarmıştır (Peacock, 2014)2014. Lokke'nin (2018: 63) çerezleri "tekil kullanıcıya has elektronik ayak izleri" olarak tanımlaması, durumu son derece açık bir şekilde ifade etmektedir.

Çerezler aracılığıyla bir web sitesinin kullanıcıyı izleme ve bilgi toplama süreci şu şekilde başlamaktadır: Kullanıcılar, tarayıcı aracılığıyla web sitesine erişim sağlar. Bu noktada, web sitesi kullanıcı cihazına çerez dosyaları yerleştirir. Çerezler, kullanıcının sayfa aktivitelerini, tarayıcı ve cihaz bilgilerini, IP adresini ve coğrafi konumu gibi çeşitli verileri toplar. Web sitesinin işlevselliği için gerekli olan zorunlu çerezler, genellikle oturum yönetimi ve kullanıcı deneyimini iyileştirme gibi görevleri yerine getirir. Ancak, web sitesinin kendi işleyişine ek olarak sitede izin verdiği üçüncü taraf çerezler de devreye girebilir. Bu çerezler, genellikle reklam verenler, analiz araçları ve sosyal medya platformları tarafından kullanılır ve kullanıcı etkinliklerini takip eder. Bu süreçte, kullanıcı davranışları izlenir; ne kadar süreyle hangi sayfaların ziyaret edildiği, hangi ürünlerin incelendiği ya da hangi içeriklerle etkileşime girildiği kaydedilir. Her çerez, kullanıcıyı tanımlayan bir kimlik numarası içerir. Bu numarayı sağlayan üçüncü taraf şirket, aynı kullanıcının farklı web sitelerindeki hareketlerini de izleyebilir, kayıt altına alabilir ve analiz ederek kişi hakkında kapsamlı bir profil oluşturabilir.

Son 10 yılda dijital alanda mahremiyetin korunmasına yönelik yerel ve küresel farkındalığın artması, uluslararası düzeyde veri koruma tüzüklerinin yasalaşması ve popüler tarayıcıların üçüncü taraf çerezleri engelleme girişimleri ile çerezsiz dünya kavramı gündeme gelmiştir. Kavram, kullanıcı gözetiminin, veri toplamanın ve hedefli reklamcılığın çerezsiz olarak yürütüleceği yeni nesil sistemleri betimlemektedir. Üçüncü taraf çerezlerin devre dışı bırakılmasıyla çevrimiçi gözetimin yeni araçları bu dünyanın başrol oyuncuları olmuştur. Google, Meta, Amazon ve Microsoft gibi dünyanın en büyük teknoloji şirketlerinin yanı sıra dijital reklam endüstrisinde faaliyet gösteren kurumlar da kendi çözüm yollarını üretmeye, yeni taktikler geliştirmeye başlamıştır. Tüm bu çabalar neticesinde, önerilen çözümler takip sistemlerinde köklü değişimlere neden olmuş; kamuoyuyla paylaşımlar ise "gizlilik odaklı", "şeffaf" ve "mahremiyete saygılı" ifadeleriyle yapılmıştır.

Yerli literatürde çerezsiz gözetimle ilgili herhangi bir çalışmaya rastlanmazken, internet çerezlerine yönelik çalışmalar da oldukça sınırlıdır. Taşkaya ve Talay (2019), çerezleri ve açık rızayı hukuki açıdan ele almış, uzman görüşleriyle bu kavramları değerlendirmiştir. Untila Kaplan (2020), Türkiye, Romanya ve Rusya'da internet gazeteciliğinde çerez kullanımını ve kullanıcıların mahremiyet algısını karşılaştırmalı olarak incelemiştir. Uluk (2023) ise Türkiye'deki haber sitelerinin çerez izinlerini kullanıcıdan yasal ve etik açıdan sorunlu biçimde aldığını ortaya koymuştur.

Bu çalışma, çerezlerin olduğu dünyayı ana hatlarıyla ele alırken çerezsiz dünya şemsiyesi altında çalışmalar yürüten şirketlerin yeni nesil izleme teknolojilerini ve çerezsiz izleme stratejilerini incelemeyi amaçlamaktadır. Çalışmada veri toplama yöntemi olarak doküman inceleme kullanılmış, elde edilen veriler nitel olarak analiz edilip yorumlayıcı bir yaklaşımla değerlendirilmiştir. Bu doğrultuda çerezsiz sistemlerin çerezle izlemelerden farkları ve çalışma prensipleri ayrıntılarıyla el alınırken akademisyenlerin, mühendislerin, güvenlik uzmanlarının ve derneklerin bunlara ilişkin rapor ve çalışmaları ile güncel bir tartışma gerçekleştirilmiştir. Değerlendirmeler sonucunda yeni gözetim taktiklerinin çerezlere nazaran daha zor tespit edilebilir, kapalı ve saklı şekilde gerçekleşebildiği; yasaları ve tarayıcıların otomatik engelleme mekanizmalarını aşabilen yöntemlere sahip oldukları tespit edilmiştir.

Gözetleme Aracı Olarak Çerezlerin Kullanımı

Lyon (2013: 11), günümüzde insanların gün doğumundan batımına kadar oldukları her yerde ağ tabanlı teknolojilerin kuşatması altında yaşamaya devam ettiğinin altını çizer. İnternet çerezleri, bu kuşatma altında kullanıcıların çevrimiçi davranışlarını izlemek ve uzak sunuculara aktarmak için etkili bir araç olarak karşımıza çıkar.

Çerezler, işlevsellik bakımından kaynağına, kullanım süresine ve yerleştirilme amacına göre sınıflandırılabilir (GDPR, t.y.): (1) kaynağına göre çerezler, iki temel gruba ayrılır. Birinci taraf çerezler, kullanıcının ziyaret ettiği web sitesi tarafından doğrudan yerleştirilir. Üçüncü taraf çerezler, kullanıcının ziyaret ettiği site aracılığıyla başka bir grup tarafından yerleştirilen çerezlerdir. (2) kullanım süresine göre çerezler, kullanıcının site ziyareti sona erdiğinde otomatik olarak silinen oturum çerezleri ile cihazda daha uzun süreler boyunca saklanan kalıcı çerezler olarak ayrılmaktadır. (3) yerleştirilme amaçlarına göre çerezler ise dört kategoriden oluşmaktadır. Zorunlu çerezler, web sitesinin temel işlevlerini yerine getirebilmesi için gerekli olan çerezlerdir. Tercih çerezleri, kullanıcıların kişisel tercihlerini hatırlamaya ve siteyi bu tercihlere uygun şekilde kişiselleştirmeye yönelik çalışır. Analitik çerezler, kullanıcıların siteyi nasıl kullandığını ve etkileşimleri anlamak için veri toplayan çerezlerdir. Reklam çerezleri ise kullanıcılara hedefli reklamlar sunmak, reklam etkinliklerini ölçmek ve davranışları enine boyuna analiz etmek amacıyla kullanılır.

HTTP protokolü üzerinde çalışan çerezler, kullanıcıların web siteleriyle etkileşimlerini izlemek ve bu etkileşimleri yönetmek üzere tasarlanmıştır. Kullanım aşamasına ilişkin temel noktalar şöyle özetlenebilir (Kristol, 2001):

1. Durum Yönetimi: Çerezler, HTTP protokolünün "stateless" (durumsuz) doğasını aşmak için kullanılır. Her HTTP isteği, sunucu tarafından bağımsız olarak ele alındığı için, çerezler kullanıcının oturum bilgilerini ve diğer durumsal verileri saklamak için bir yol sağlar. Örneğin, bir alışveriş sepetindeki ürünlerin takibi için çerezler kullanılır.

2. **Kullanıcı Tanımlama:** Çerezler, kullanıcıların kimlik bilgilerini saklamak için de kullanılır. Örneğin, bir web sitesi, kullanıcının giriş bilgilerini çerezlerde saklayarak, her ziyaretinde kullanıcıdan tekrar giriş yapmasını istemez.
3. **Site İçi İzleme:** Web siteleri, kullanıcıların hangi sayfaları ziyaret ettiğini izlemek için çerezleri kullanabilir. Bu bilgiler, site sahipleri ve yöneticilerine kullanıcıların siteyi nasıl kullandığını anlamalarına yardımcı olur ve site arayüz tasarımında gerekli düzenlemeleri yapmak için yol gösterebilir.
4. **Kişiselleştirme:** Çerezler, web sitesi geliştiricilerine kullanıcı etkileşimlerini daha iyi yönetme ve web sitesi deneyimlerini kişiselleştirme imkânı tanıyan uygulamalar hazırlamalarına yardımcı olabilir.
5. **Üçüncü Taraf Çerezler:** Çerezler, yalnızca ziyaret edilen web sitesinden değil, aynı zamanda o siteye entegre edilmiş üçüncü taraf içeriklerden (örneğin, reklam veya analitik) de alınabilir. Bu durum, kullanıcıların farkında olmadan başka sitelerden çerez almasına neden olabilir.
6. **Mahremiyet:** Çerezlerin kullanımı, kullanıcıların mahremiyet hakları ile ilgili endişeleri beraberinde getirir. Kullanıcılar, çerezlerin nasıl kullanıldığını yönetme hakkına sahip olmalıdır.

Kristol'un çerez kullanımına yönelik değindiği temel başlıklar bir yandan platformun işlevselliği ve kullanıcı deneyimiyle doğrudan ilintiliyken diğer yandan mahremiyet endişelerine dikkat çekmektedir. Bu endişeler şüphesiz ki üçüncü taraf çerezlerin kullanımıyla yoğunlaşmaktadır. Web sitelerinin reklam gösterimi ve analitik bilgi edinme amacıyla çerezlere sıkça başvurması yüksek miktarda verinin üçüncü taraflara aktarımıyla sonuçlanmaktadır. Söz konusu çerezlerin kullanım sıklığı ise oldukça fazladır.

Tablo 1

Analiz Edilen 440,886 Web Sitesi Arasında Türkiye'de Reklam Teknolojilerini Kullanan Sitelerinin Dağılımı (BuiltWith, 2024a).

Reklam Teknolojisi	Web Sitesi Sayısı	%
DoubleClick.Net	188,416	42.74
Google Adsense	36,427	8.26
Facebook Custom Audiences	33,001	7.49
Google Remarketing	23,268	5.28
Ads.txt	16,404	3.72
Google Direct	16,281	3.69
AdBlock Acceptable Ads	16,062	3.64
Trellian	2,625	0.60
Google Reseller	1,629	0.37
PubMatic	1,550	0.35

Tablo 1'de yer alan veriler, Türkiye'de yaygın olarak kullanılan reklam teknolojilerini ve bu teknolojilerin ne oranda kullanıldığını göstermektedir.

Tabloya göre, Türkiye'deki en yaygın reklam teknolojisi, Google'a ait olan DoubleClick.Net reklam çerezleridir. %42,74'lük kullanım oranıyla Türkiye'deki 188.416 web sitesinde bu teknolojinin yer aldığı görülmektedir. Söz konusu DoubleClick çerezleri, kullanıcının gezdiği web sitelerini takip ederek profilleme yapar ve kullanıcının ilgi alanlarına göre reklamlar sunulmasını sağlar. DoubleClick'in Türkiye'deki dijital reklamcılık sektöründe ne denli önemli bir aktör olduğu web sitelerinin neredeyse yarısında yer almasıyla kendisini belli etmektedir. Yine Google'ın popüler reklam teknolojilerinden birisi olan ve web sitelerinin reklam göstermelerine olanak tanıyan Adsense, %8,26'lık bir payla 36.427 web sitesinde kullanılmaktadır. Tabloda sosyal medya kaynaklı reklamcılığın da web sitelerinde bulunduğu görülmektedir. Facebook Custom Audiences, %7,49'luk kullanım oranı ile 33.001 web sitesinde yer almakta ve çerez tabanlı kullanıcı izleme teknolojisini kullanarak reklamların kişiselleştirilmesini sağlamaktadır. Bu durum, sosyal medya platformlarının kullanıcı verilerini toplayarak, kullanıcıların ilgi alanlarını analiz etmelerine ve reklamcıların hedef kitlesine ulaşmalarına imkân vermektedir. Daha düşük kullanım oranına sahip diğer teknolojiler arasında Google Remarketing (%5,28), Ads.txt (%3,72), ve Google Direct (%3,69) bulunmaktadır.

Görüldüğü üzere, Türkiye'de de reklam teknolojilerinin büyük çoğunluğu, çerezler aracılığıyla kullanıcı bilgilerini toplamakta ve bu veriler doğrultusunda reklamcılık stratejilerini şekillendirmektedir. Çerezlerin bu kadar yaygın ve etkin kullanımı, dijital reklamcılığın temel yapı taşlarından biri olduğunu ve kişiselleştirilmiş reklamların dijital ekosistemde merkezi bir rol oynadığını göstermektedir.

Reklamlar dışında üçüncü taraf çerezlerin sıkça başvurulduğu bir diğer alan, web sitelerinin performansını ölçmek ve ziyaretçi trafiğini analiz etmek için kullanılan analitik araç-

Tablo 2

Analiz Edilen 631,975 Web Sitesi Arasında Türkiye'de Analitik Teknolojilerini Kullanan Sitelerin Dağılımı (BuiltWith, 2024b).

Analitik Teknolojisi	Web Sitesi Sayısı	%
Google Analytics	191,576	30.31
Global Site Tag	169,882	26.88
Facebook Pixel	34,496	5.46
Facebook Conversion Tracking	30,617	4.84
Google Conversion Tracking	26,621	4.21
Google Conversion Linker	24,684	3.91
Facebook Domain Insights	20,955	3.32
Facebook Signal	18,404	2.91
Yandex Metrika	13,292	2.10
Cloudflare Insights	11,278	1.78

lardır. Analitik hizmeti veren araçlar, kullanıcıların bir web sitesinde nasıl davrandığını, hangi sayfaları ziyaret ettiklerini, ne kadar süre geçirdiklerini ve hangi cihazlardan erişim sağladıklarını izlemek için çerez yerleştirmektedir.

Tablo 2'de Türkiye'de analitik araçları kullanan web sitelerinin dağılımı yer almaktadır. Tablonun zirvesinde %30,31'lik oran ile Google'ın bir hizmeti olan Google Analytics (GA) bulunmaktadır. Dönüşüm takibi ve yeniden pazarlama gibi stratejileri yönetmek ve GA, Google Ads ve diğer Google hizmetlerini entegre etmek için kullanılan Google Site Tag listenin ikinci sırasında yer almaktadır. Reklam hedefleme, reklam kampanyalarının performansını ölçme, Facebook ve Instagram etkileşimleri/trendleri, yeniden pazarlama ve dönüşüm oranları takibi gibi amaçlarla kullanılan Meta'ya ait Facebook Pixel, Facebook Conversion Tracking, Facebook Domain Insights ve Facebook Signal sistemleri tablonun devamında önemli bir yere sahiptir. Tablo, Türkiye'deki web sitelerinin tıpkı reklam amaçlı olduğu gibi analitik amaçlar doğrultusunda da yoğun olarak Google merkezli ürün ve çözümlere başvurduğunu göstermektedir. Onu, Türkiye'de yadsınamaz bir kullanıcı sayısına sahip olan Meta uygulamaları takip etmektedir. Bu iki büyük teknoloji şirketinin yanında Yandex'in analitik uygulaması olan Metrica ve Cloudflare'e bağlı hizmetler için sunulan Insights hizmeti de alternatif teknolojiler olarak dikkat çekmektedir.

Liberty (2015) üçüncü tarafların çerezler aracılığıyla kullanıcıları benzersiz şekilde tanımladığını belirtir ve bunu kuş bilimcilerin kuşlara taktığı takip bilekliklerine benzetir. Ancak bu durum kullanıcı mahremiyeti ve veri gizliliği açısından ciddi endişelere yol açmaktadır. Üçüncü taraf reklam ve analitik çerezleri, kullanıcıların izni olmadan geniş çaplı veri toplama süreçlerinin bir parçası olarak görülmekte ve bu da çerez kullanımına yönelik daha sıkı düzenlemeler ve engelleyici politikaların gündeme gelmesine neden olmaktadır. Diğer yandan üçüncü taraf olarak hizmet sağlayanlar aynı görüşe sahip olmayabilmektedir. Dolayısıyla verilerin ticari kullanımını hedefleyen şirketler ile bireylerin mahremiyetlerini koruma isteği arasında örtük bir çatışma olduğu açıktır. Şirketler, büyük veri üzerinden kâr elde etmeyi amaçlarken, mahremiyet savunucuları ise bunun mahremiyet üzerinde ciddi riskler taşıdığına dikkat çekmektedir. Bu iki yaklaşım arasındaki fark hem teknolojinin sunduğu fırsatlar hem de potansiyel tehlikeler açısından derinleşmektedir. Şirketlerin gözünde veri, büyük kazançlar vadederken, mahremiyet aktivistleri için bu durum, bireylerin özel yaşamının ihlali anlamına gelmektedir (Lokke, 2018: 69). Çerezsiz dünya, her iki zıt kutbu birbirine yakınlaştırmak üzere ortaya atılmış bir kavram olarak durmaktadır: şirketler, gözetim sistemlerini demokrasiye ve insan haklarına saygılı, mahremiyet öncelikli ürünlerle değiştirdiklerini vadederken kapitalizmin gerekliliği olan kârlılığı da yine gözetim üzerinden sürdürme niyetlerinden vazgeçmemektedir.

Çerezsiz Dünyaya Nasıl Geldik?

1999 yılında Intel, Pentium III işlemcisinde benzersiz bir kimlik numarası olan İşlemci Seri Numarası'nı (Processor Serial Number - PSN) tanıtır. Bu numara, her işlemciye özgüdür ve internet tarayıcıları aracılığıyla web sunucuları tarafından okunabilen bir özelliğe sahiptir. Diğer bir deyişle, her işlemci tıpkı çerezler gibi benzersiz bir kimlik numarası taşır. O dönem Intel, bu teknolojinin güvenlik, kimlik doğrulama ve çevrimiçi işlemlerin güvenli hale getirilmesi amacıyla faydalı olacağını iddia eder. Ancak uygulama, mahremiyet savunucuları tarafından büyük bir tepkiyle karşılanır. Eleştiriler, bu benzersiz kimlik numarasının çevrimiçi platformlar tarafından kullanıcıları izlemek ve gözetlemek için kullanılabileceği üzerinde yoğunlaşır. Bu durum, kişisel verilerin korunmasına yönelik önemli bir tehdit olarak değerlendirilir. Gelen yoğun eleştiriler üzerine Intel, PSN'yi devre dışı bırakılmasını sağlayan bir güncelleme yayımlar ve sonraki sürümlerde bu özelliği tamamen kaldırır (Lyon, 2018: 208). Bu olay, teknoloji şirketlerinin veri toplama yöntemlerine dair önemli bir dönüm noktası olmuştur. Gözetleme için cihazların içerisine donanımsal bir parça eklemek tamamen rafa kalkarken, bunu yazılımsal çözümlerle gerçekleştirme yolları çeşitlenmiştir.

Çerez yerleştirme, web tabanlı platformlara sahip teknoloji şirketlerinin en yaygın gözetleme girişimlerinden birisi olmuştur. Bu denli yaygın bir kullanım ağına sahip ve tüm üçüncü taraf hizmetlerin bağlı olduğu; işlevselliği ve sağladığı kârlılığın tartışılmaz olduğu çerezler bir anda neden yok sayılmaya başlanmıştır? Reklam endüstrisi, bu yok sayma sürecini tanımlamak için yeni bir isim üretmemiş; bunun yerine, çerez sisteminin zıttı gibi görünen "çerezsiz dünya" ifadesini kullanmıştır. Üstelik bu dünyayı kuran mahremiyet aktivistleri değil, gelir modeli gözetime dayalı şirketler olmuştur. Durum, dünyanın en büyük tütün firmalarının ansızın tütünsüz dünya kampanyalarına başlamasına benzemektedir. Buradaki amaç tütünden doğan zararları bitirmekten ziyade, zararın bilimsel kanıtlarını zayıflatacak çözümler üretmektir. Yeni ürettikleri ürün aslında yine sağlığa zararlı ve bireyleri doğrudan olumsuz etkileyecek bir maddedir. Fakat, verdiği zarar kanıtlanamayacaksa veya çok dolaylı ve meşakkatli şekilde kanıtlanacaksa, doğrudan zararı kanıtlanmış sigarayı yeni ürün için feda etmek hiç de zor değildir. Çerezsiz dünya kavramı da aynı bu anlayışa sahip şekilde, çerezler olmadan gözetimin farklı yöntemlerle devam ettiği bir sistemi anlatmaktadır.

Çerezsiz dünya, uluslararası alanda veri koruma tüzüklerinin yasalaşması ve mahremiyete ilişkin endişelerin ve farkındalığın artmasıyla ortaya çıkmıştır. Web 2.0 sonrası sosyal ağların özgürlükçü yapısı ve iletişim alanındaki devrimleri ön planda tutulurken sistemin yarattığı gizlilik sorunları bugünkü kadar yüksek sesle konuşulmamıştır. Google ve Meta gibi Silikon Vadisi'nin büyük şirketlerine ait skandallar veya bu şirketlerin neden olduğu ihlaller, genellikle gizlilik ve güvenlik uzmanları tarafından ortaya çıkarılmıştır. Geriye dönüp baktı-

ğımızda, veriye dayalı reklamcılığın mucitlerinden olan ve hedeflenebilir kitle oluşturmada çığır açan DoubleClick, çerezleri kişiselleştirilmiş reklam amacıyla kullanan ilk reklam şirketlerinden biri olmuştur. 1996'dan 2007'ye kadar çevrimiçi reklam endüstrisinde söz sahibi olan şirket, 2007 yılında 3.1 milyar dolar karşılığında Google tarafından satın alınmıştır (Story & Helft, 2007). Gizlilik ve güvenlik savunucularının endişe ve şikâyetleri üzerine ABD Federal Ticaret Komisyonu (FTC), sekiz aylık bir değerlendirmenin ardından gizlilik endişelerini kabul etse de Google'ın satın alma işlemini onayladığını beyan etmiştir (FTC, 2007). FTC'nin basın açıklamasında dikkat çeken kısım ise gizlilik endişelerinin sadece Google veya DoubleClick'e özgü olmadığı, problemin tüm çevrimiçi reklam pazarıyla ilgili olduğunu kabul etmesi olmuştur. Sorunun varlığı böylelikle resmî bir kanaldan dile getirilmiştir. Yine aynı yıl Facebook, kullanıcıların diğer web sitelerindeki harcamalarını takip edip bu bilgileri arkadaşlarıyla paylaşma özelliği olan "Beacon" adındaki reklam fikrini tanıtmıştır (Facebook, 2007). Facebook'un çerezler aracılığıyla kullanıcılarının başka sitelerdeki aktivitelerini açık rızalarını almadan takip etmesi kısa sürede tepki çekmiş ve yaklaşık bir ay sonra projeden vazgeçilmiştir (Clark, 2007). Bu iki şirketin çerezler yoluyla arka kapıları zorlayarak kullanıcıları izleme isteği 2010'lara geldiğimizde de devam etmiştir. 2011'de Facebook'un kullanıcılarını oturumu kapattıktan sonra bile çerezler kullanarak çevrimiçi davranışlarını izlemeye devam ettiği ortaya çıkmıştır. Facebook, bunun bir hata sebebiyle "kasıtsız" olarak gerçekleştiğini beyan etse de çerez yerleştirme prosedürlerinin şeffaf ve açık rızaya ihtiyaç duyduğu konusunda tartışmalar başlamıştır (Gilbert, 2011). 2012'de Google, Safari tarayıcısında üçüncü taraf çerezlerin takibini engelleyen kullanıcıları bir güvenlik açığından sızarak izinsiz şekilde takip etmesinden dolayı FTC tarafından 22,5 milyon dolar cezaya çarptırılmıştır (Kravets, 2012). 2016 ABD Başkanlık seçimleri sonrasında Cambridge Analytica skandalı, 87 milyon kullanıcının kişisel verilerinin çerezler de dahil çeşitli gözetleme yöntemleriyle toplandığını ve siyasi kampanyalarda kullanılmak üzere analiz edildiğini ortaya koymuştur (Salinas, 2018). Hâlen çevrimiçi reklam sektörünün lokomotifi ve en büyük pay sahibi olan Google ve Meta'nın (Statista, 2023) karıştığı bu skandallar ve tartışmalar, gözetim faaliyetleri ve çerez kullanımına yönelik düzenleme ihtiyacını giderek artırmıştır.

Web tarayıcılarının çerezlerle ilişkisi çevrimiçi mahremiyet farkındalığının ve güvenlik ihtiyacının artması ile sürekli değişime uğramıştır. 2004'te pazar payının %95'ine sahip Internet Explorer (Routley, 2020), yayımladığı bir güncelleme ile üçüncü taraf çerezleri engelleme özelliğini duyurmuştur. Tarayıcı ayarlarından etkinleştirilebilen bu özellik varsayılan olarak engelleme yapmasa da üçüncü taraf çerezlerin engellenmesine imkan sağlamıştır (Microsoft, 2004). 2010'lu yıllarla birlikte Mozilla Firefox ve Safari gibi popüler tarayıcılar çerezleri engelleme konusunda daha gelişmiş ayarlar sunmaya başlamıştır. 2011'de W3C (World Wide Web Consortium) tarafından standartlaştırılan "Do Not Track" özelliği dönemin üç büyük tarayıcısı olan Google Chrome, Mozilla Firefox ve Internet Explorer'a bir özellik olarak eklenmiş ve çevrimiçi takibi kısıtlamayı amaçlamıştır. Fakat tarayıcıların özelliği verimli bir şekilde

kullanmaması ve kullanıcıların mahremiyet endişelerini gidereememesi hayal kırıklığına neden olmuştur (McDonald & Peha, 2011) 2017'de Safari, farklı web sitelerini ziyaret eden kullanıcıların sürekli gözetimini kısıtlayan ve üçüncü taraf çerezleri otomatik olarak engelleyen Akıllı Takip Önleme (Intelligent Tracking Prevention) sistemini tanıtmıştır (Wilander, 2017). 2020'de Mozilla Firefox, Gelişmiş Takip Koruması (Enhanced Tracking Protection) özelliği ile kapsamlı bir çerez engelleme sistemini duyurmuştur (Deckelmann, 2020). Yine 2020'yle birlikte tarayıcı kullanım pazarının lideri Google Chrome da üçüncü taraf çerezleri aşamalı olarak kaldıracağına ilişkin notlar paylaşmaya başlamıştır. 14 Ocak 2020'de üçüncü taraf çerezlerin iki yıl içinde varsayılan olarak engelleneceğini açıklayan Google (Schuh, 2020), 24 Haziran 2021'de engelleme tarihini 2023'ün ortalarına (Goel, 2021), 27 Temmuz 2022'de 2024'ün ortalarına (Chavez, 2022), 23 Nisan 2024'te 2025'in ilk yarısına ertelemiştir (The Privacy Sandbox, 2024). Yıllar içinde süregelen ertelemelerden sonra Google, 27 Temmuz 2024'te yayımlanan yeni notta üçüncü taraf çerezleri tamamen engelleme sürecini devre dışı bıraktığını paylaşmıştır (Chavez, 2024). 2012 yılından beri tarayıcı pazarında zirveyi bırakmayan ve şu anda tarayıcılar arasında %65'lik bir paya sahip Google Chrome'un (Statista, 2024c) son durumda üçüncü taraf çerezleri varsayılan olarak engellemediğini söyleyebiliriz.

Yakın zamanda özellikle Avrupa Birliği'ndeki Genel Veri Koruma Tüzüğü (GDPR) ve ABD'deki California Tüketici Gizliliği Yasası (CCPA) gibi yasalar, kullanıcıların kişisel verilerinin nasıl toplandığı ve işlendiğine dair daha katı kurallar getirmiştir. Özellikle GDPR (t.y.), kullanıcıların gizlilik haklarının korunması için çerezlerin kullanımını belirli kurallar altına toplamıştır. Bunlar ana hatlarıyla şu şekildedir: 1) zorunlu olmayan çerezler, kullanıcıdan onay alınmaksızın aktif hâle getirilmemelidir. 2) Kullanıcılara, çerez ayarları üzerinde tam kontrol imkânı sunulmalı, böylece kendileri hangi çerezlerin aktif olacağına karar verebilmelidir. 3) "Çerez kullanımını kabul ediyorsunuz" gibi ifadeler, yalnızca aktif kullanıcı onayı ile geçerli olmalıdır. 4) Çerez ayarları sırasında, sadece "Evet" ve "Daha fazla bilgi" seçenekleri değil, kullanıcıların çerez kullanımını tamamen reddedebilmeleri için tasarlanmış görünür bir "Hayır" butonu da sunulmalıdır. 5) Çerezlerin hangi amaçla yerleştirildiği ve ne kadar süreyle cihazda kalacağı, kullanıcıya açık ve anlaşılır bir şekilde açıklanmalıdır. 6) Üçüncü taraflara iletilen veriler, örneğin IP adresi veya ziyaret edilen sayfalar gibi bilgiler, kullanıcılara net bir şekilde bildirilmeli ve bunun için açık rıza alınmalıdır. Bunun yanı sıra kullanıcılar verdikleri rızayı diledikleri zaman geri çekebilmelidir. Söz konusu kurallar bütünü, çerezlerin yaygın kullanımı üzerinde baskı oluşturmuş ve diğer bahsedilen unsurlarla birlikte çerezsiz dünyanın ortaya çıkmasına zemin hazırlamıştır.

Çerezsiz Dünyada Gözetim Teknolojileri

Çevrimiçi dünyadaki gizlilik endişeleri birçok kişi ve kurum tarafından sıkça dile getirilmektedir. Üçüncü taraf çerez kullanımının yasalar tarafından sınırlandırılması ve bazı büyük tarayıcılar tarafından yasaklanması bu endişeleri gidermek üzere atılmış adımlar olarak sayılabil-

mektedir. Bu adımlar neticesinde, özellikle reklam endüstrisi çerezler olmadan gözetlemenin nasıl olabileceği üzerine kafa yormaya başlamış ve yeni nesil izleme teknolojilerinin hazırlanmasına önayak olmuştur. Birçok testten geçerek hazırlanan ürünler, engellemeleri aşacak farklı taktikler ve yapay zekanın aktif kullanımıyla geliştirilen sistemler bu alanda kullanıma sunulmuştur. Bu başlık altında detaylıca incelenecek olan yeni gözetim mantığından ilki sunucu taraflı izleme yöntemidir.

Büyük reklam platformları, çerezlerin aktif rol aldığı istemci taraflı izleme yöntemleri yerine sunucu taraflı izleme teknolojilerinin geliştirilmesine ağırlık vermeye başlamıştır. Bu iki yöntemin genel hatları aşağıdaki tabloda verilmektedir.

Tablo 3'te görüldüğü üzere sunucu taraflı kullanıcı takibi bir yandan güvenilir olması ile ön plana çıkartılırken diğer yandan gözetimin varsayılan şekilde gerçekleşmesi sürecini devam ettiren taktiklere sahiptir. Başta Google ve Meta olmak üzere reklam endüstrisinin lider şirketleri çeşitli yöntemlerle olası engellemeleri bertaraf etmek için yeni yol arayışlarına girmiştir. Çerezsiz gelecekteki en yaygın gözetim tekniklerini, platformlar ve uygulamalar üzerinden inceleyebiliriz.

Google, kendi tarayıcısı Chrome'da üçüncü taraf çerezlerin otomatik olarak engellenmesini rafa kaldırmış olsa da gerek yasa uygulayıcıların gerekse diğer popüler tarayıcıların güncellemeleri nedeniyle farklı çözüm yolları geliştirmeye başlamıştır. Google bu çözüm yollarını, 2019'da Privacy Sandbox olarak adlandırdığı projeyi duyurarak paylaşmıştır (Schuh, 2019). Projenin tanıtımıyla birlikte ilerleyen süreçlerde üçüncü taraf çerezlerin yerini alacak, hedefli reklamcılığı devam ettirecek ve kullanıcı gizliliğini de üst düzeyde koruyacak projeler geliştirilmeye başlanmıştır.

Privacy Sandbox kapsamında ilk çözüm önerisi FLoC (Federated Learning of Cohorts) olmuştur (Roviaro, 2020; Temkin, 2021). Üçüncü taraf çerezlere alternatif olarak geliştirilen

Tablo 3
İstemci Taraflı İzleme ve Sunucu Taraflı İzleme Karşılaştırması (Mathew, 2022).

İstemci Taraflı İzleme	Sunucu Taraflı İzleme
Tarayıcı tabanlı izleme.	Web sitesinin bulut sunucusu tabanlı izleme yöntemi.
Google Tag Manager gibi istemci taraflı etiketleme ile kurulur.	Google Tag Manager Sunucu Taraflı Etiketleme gibi yöntemlerle kurulur.
Kullanıcıları izlemek için üçüncü taraf JavaScript kodu siteye eklenir.	Kullanıcıları izlemek için üçüncü taraf JavaScript kodu eklenmez.
Üçüncü taraf çerezler kapsamında değerlendirilir: Adblocker'lar ve Safari gibi tarayıcılar varsayılan olarak üçüncü taraf çerezleri engelleyebilir.	Üçüncü taraf çerezler kapsamında değerlendirilmez: Veriler, web sitesi sahibinin bulut sunucusunda işlendiği için birinci taraf verisi olarak kabul edilir ve ardından Google Analytics, Google Ads, Facebook gibi sağlayıcılara iletilir.
Üçüncü taraf çerezlerin büyük bir kısmı engellendiğinden güvenilir bir izleme seçeneği değildir.	Güvenilir bir izleme ve ölçüm seçeneğidir.
Gizlilik düzenlemelerine uyumlu değildir.	Gizlilik düzenlemelerine uyumludur.

bu sistem kullanıcıları bireysel olarak takip etmek yerine, kullanıcıların tarayıcı geçmişlerini dikkate alarak benzer kullanıcıları aynı kategoriler altına toplamayı hedeflemiştir. Yapay zekânın tarama geçmişlerini analiz ederek kullanıcıları gruplara ayırmada aktif rol oynadığı bu yöntemin vaadi, bireyleri anonimleştirmektir. Bu vaadin sahadaki yansımalarını sınamak isteyen dijital güvenlik uzmanı Eric Rescorla (2021), FLoC'un gizlilik endişelerini gidermek yerine yeni sorunlar yarattığını tespit etmiştir. Buna göre, her ne kadar bireyler büyük kategoriler altına yerleştirilse de tarayıcı parmak izi veya oturum bilgisi gibi farklı verilerle kategori içindeki kullanıcılar filtrelenerek doğrudan hedeflenebilir hale gelebilmektedir. FLoC sistemi, kullanıcıların birden fazla siteye yaptıkları ziyaretleri engelleyen güvenlik önlemlerini de aşabilmektedir. Koruma mekanizmalarının aşılması ve FLoC sistemi ile her hafta kullanıcılara atanan yeni kategorilerin düzenli takibi, kişilerin doğrudan berlirlenebilmesine olanak tanımaktadır. Yarattığı yeni sorunlarla birlikte kullanıcı mahremiyetine ilişkin endişeleri de gidermekte zorluk yaşayan Google, üçüncü taraf çerezlerin yerini almasını öngördüğü FLoC sistemini 2022'nin başında sonlandırmıştır (Goel, 2022).

FLoC'un sonlandırılmasıyla birlikte tanıtılan yeni proje Topics API olmuştur (Goel, 2022). FLoC'a benzer şekilde Topics API, kullanıcının gezdiği sitelere göre ilgi alanlarını sınıflandırmakta ve reklam verenlerin bu sınıflara göre hedefleme yapmasını sağlamaktadır. Bu teknolojide, çerez kullanımı yerine kullanıcılara, en sık ziyaret ettikleri web siteleri verisi üzerinden beş kategori atanır (Johnson & Neumann, 2024). Her ne kadar kullanıcıları kategorilere atarken FLoC gibi tarama geçmişi baz alınsa da bu yöntemde ziyaret edilen sitenin tam URL adresine veya içeriğe göre değil yalnızca alan adının ne olduğuna dikkat edilmektedir. Örneğin, FLoC sisteminde ornekmagaza.com/giyim/kazak sayfasını ziyaret etmiş bir kullanıcı "kazak arayanlar" kategorisine eklenebilmektedir. Topics API'de ise yalnızca ornekmagaza.com sitesini ziyaret etmiş olması göz önünde bulundurulur ve kullanıcı daha genel olarak "alışveriş" kategorisine yerleştirilir. Google'ın gizlilik bağlamında güçlü gördüğü bu sistem üzerine yapılan bazı araştırmalarda, mahremiyet endişelerinin tamamıyla giderilmediği görülmektedir. Beugin ve McDaniel (2023), Topics API'yi gerçekçi senaryolarla analiz ettiği çalışmasında kullanıcıların bu yöntemle bile benzersiz şekilde tanımlanabileceğini ortaya koymuştur. Buna göre kötü niyetli bir reklam veren, kullanıcıların tarayıcı aktivitelerini ne kadar çok gözlemlerse onların kim olduklarını tahmin etmesi o kadar çok kolaylaşmaktadır. Sürekli değişen kategorilerin düzenli takibi ile kullanıcılar %75'e kadar doğru şekilde tahmin edilebilmektedir. Bir başka araştırmada ise 1000 kullanıcılık bir havuzdaki kişileri doğrudan belirleme oranı %15 ile 17 arasında çıkmıştır (Jha vd., 2023). Mozilla'da mühendis olan Thomson'ın (2023), Topics API'yi analiz ettiği raporunda ise sistemin kullanıcıların tanımlanması ve izlenmesini engelleyecek bir güvence sağlamadığına vurgu yapılmaktadır. Yazar, Beugin ve McDaniel gibi yeterli süre boyunca tekrarlanan gözlemler neticesinde kullanıcıların tanımlanabilir hale geldiğinin altını çizmektedir.

Google'ın bir diğer güncel çerezsiz gözetleme yöntemi Protected Audience API'dir. Bu yöntem daha çok yeniden pazarlama ile ilişkilidir. Yeniden pazarlamaya yönelik uygulama-

ların üçüncü taraf çerezlere bağlılığını azaltmak üzerine geliştirilmiştir. Sistem şu şekilde çalışmaktadır: reklamverenlerin web sitesini ziyaret eden kullanıcılar bir ilgi grubuna eklenir, bu gruplar kullanıcının cihazında 30 gün boyunca saklanır. Başka bir web sitesi/reklamveren kullanıcıya bu ilgi alanına göre reklam göstermek istediğinde açık artırma işlemleri cihaz üzerinde yapılır ve üçüncü taraf sunucularla iletişim oldukça sınırlı şekilde gerçekleşir (Philipse, 2024: 7). Bu yanıyla da çerezlerden oldukça farklı bir çalışma prensibine sahiptir. PA API'yi ilk test edenler arasında 2022 yılında Criteo ve RTB House gelmiştir. Her iki reklam şirketi de milyonlarca kullanıcıyı ilgi gruplarına ekleyerek reklamverenlerin hedeflemesine açmıştır (Johnson & Neumann, 2024: 7-8). Thomson'ın PA API'yi gizlilik ekseninde incelediği raporu, bize sistemin hâlen reklam endüstrisini cezbetmek için birçok tavizde bulunduğunu anlatmaktadır (2024). Long ve Evans'ın (2024) yürüttükleri ampirik çalışma da PA API'nin vadettiği gizlilik garantisinin zayıf yanlarını ortaya çıkarmaktadır. Buna göre kötü niyetli bir reklamveren, mevcut gizlilik önlemlerini aşarak iki farklı siteye yapılan ziyaretleri aynı kişiyle eşleştirme olanağına hâlen sahiptir. Her ne kadar Google'ın bir projesi olsa da açık kaynak olarak GitHub'ta yer alan ve geliştirilmeye devam eden sistem henüz tam olarak yaygınlaşmamıştır.

Privacy Sandbox projesinin iki önemli teknolojisi Protected Audience API ve Topics API'nin en temel amacı çerezlere ihtiyaç duymadan kişiselleştirilmiş reklamcılığı devam ettirmektir. Bu teknolojiler Google Chrome tarayıcısı için geliştirilmiştir ve yalnızca bu tarayıcı üzerindeki aktiviteler ve etkileşimler üzerinden çalışmaktadır. Dolayısıyla API'lerin doğrudan diğer tarayıcılarla iş birliği içinde olmadığını söylemek mümkündür.

Topics API'nin çalışma prensibinde açık rıza kavramı çerez kullanım izinlerinden biraz daha farklıdır. Kullanıcılar, Google Chrome tarayıcı ayarlarından ilgi alanlarının oluşturulmasını ve paylaşılmasını aktif veya pasif hale getirebilir. Android işletim sistemlerinde de bu ayarlar mevcuttur. Web siteleri tarafında ise mevcut çerez bildirimlerindeki gibi "kabul et" veya "reddet" gibi seçenekler daha kısıtlı geçerliliğe sahiptir. Topics API'nin veri işlemesine ilişkin açıklamaların web sitelerinin aydınlatma metinleri veya çerez politikalarında yer alması gerektiği belirtilmektedir. İlgi gruplarının oluşturulması işlemleri tarayıcı üzerinde yapıldığı için tercihler buradaki ayarlar sayfasında yer almaktadır. Kullanıcılar kendilerine atanan veya atanacak olan ilgi gruplarını görüntüleyebilmekte veya silebilmektedir. Protected Audience API'nin çalışma biçimi de aynı şekildedir. Sistemlerin çalışmasına ilişkin verilen izin tarayıcı üzerinden yapılır. Web sitelerinin aydınlatma dışında doğrudan bir yükümlülüğü yoktur.

Google'ın üçüncü taraf çerezlere alternatif olarak sunduğu ve kullanıcı korumalı alan olarak tanıttığı Privacy Sandbox projesi bir yanıyla kendi birinci taraf izleme sistemidir. Viyana merkezli Avrupa Dijital Hakları Merkezi'nin (NOYB) paylaştığı bir yazıda Privacy Sandbox projesinin mahremiyet odaklı aksayan yanlarına dikkat çekilmektedir (Noyb, 2024). Buna göre Chrome'un API'leri aktif hale getirmek ve kullanıcılardan rıza almak için çıkarttığı pencerede "reklam gizliliği özelliğini aç" ifadesi yer almaktadır. Pencerede sunulan bilgilerin reklamcılık ve izlemeyle ilgili olduğu konusunda şeffaflık eksikliği söz konusudur. Olumlu gibi sunulan bu özellik aslında birinci taraf izlemeye onay verme durumunu yansıtmaktadır.

Noyb'a göre "koruma" ve "gizlilik" gibi ifadelerle kullanıcılar tasarım ve dil bakımından aldatılmaya çalışılmaktadır. Bu bakımdan Google'ın izin alma şeklinin GDPR'ın koşullarını sağlamadığı, dolayısıyla projenin kullanıcı verilerini işlemek için yeterli hukuki zemine dayanmadığı iddia edilmektedir. Topics API gibi sistemlerin yarattığı gizlilik endişelerinden bir diğeri de kullanıcıların hangi verileriyle hedeflendikleri hakkında çok kısıtlı bir bilgiye sahip olmalarıdır (Arthur, 2023). Fransa Veri Koruma Kurumu (CNIL), tarayıcı üzerinden API'ler aktif edilse bile yayıncı web sitelerinin yasal yükümlülüklere uymaları, yani onay almaları ve gizlilik sözleşmelerinde şeffaf bir bilgilendirme yapmaları gerektiğine dikkat çekmektedir (CNIL, 2023). Privacy Sandbox girişimleri halen geliştirilme aşamasında olsa da akademisyenlerin, araştırmacıların, gizlilik savunucularının ve yasa uygulayıcıların kullanıcı mahremiyeti merkezli bir yaklaşımla sistemi ele alması ve onun açıklarını ortaya çıkarması gelecek adına umut vadetmektedir.

Silikon Vadisi'nin bir diğer büyük aktörü olan Meta (Jo Dixon, 2024), tıpkı Google gibi (Zandt, 2024) gelirinin en büyük kısmını reklamlardan elde etmektedir. Meta, Meta Piksel olmadan yoluna devam edebilmek için Facebook Conversions API'yi geliştirmiştir (Meta, 2024). Meta Piksel, çerezlere benzer şekilde, JavaScript kodu aracılığıyla kullanıcı etkinliklerinin toplanması için kullanılan bir teknoloji olarak tanımlanmaktadır. Çerezlerin ve izleme amaçlı JavaScript'lerin engellenmesi, AdBlock gibi uygulamalar ve gizliliğe odaklı yenilikler sonrasında bir alternatif olarak Conversions API tanıtılmıştır. (Weinlich vd., 2022). Bu API, tarayıcılara ve tarayıcı çerezlerine bağlılığı azaltarak kullanıcı davranışlarının izlenmesine devam etmeyi amaçlamaktadır. Böylelikle yayıncılar sitelerindeki satışları, kayıtları, etkileşimleri ve gezinim sırasındaki tüm sayfa verilerini takip edebilmektedir. Kullanıcı verileri doğrudan Meta'nın sunucularına iletilmektedir. Yayıncılar hedef kitlelerini daha iyi anlamak ve onlara uygun reklamlar yayınlamak istediklerinde bu verileri kullanabilmektedir. Tarayıcılarda üçüncü taraf çerezler otomatik olarak engelli olsa bile veri toplama işlemi devam eder. Bir nevi yayıncı ile meta arasındaki tarayıcıyı aradan çıkartarak doğrudan iletişim kurulmaktadır. İster bir web sitesi isterse bir mobil uygulama olsun, yayıncıdan toplanan veriler Meta sunucularında toplanarak kendi reklam platformuna aktarılır. Meta, API'nin tanıtım belgesinde yayıncıların yasal yükümlülüklerini yerine getirmelerini ve kullanıcı mahremiyetine saygı duymalarını önerse de bu sistemi kullanırlarken açık rıza almanın gerekliliğinden bahsetmemiştir (Meta, 2024). Fraihi ve arkadaşlarının (2024) yaptıkları bir araştırma Conversions API'nin bir web sitesi ziyaretçilerinin %34 ile %51'ini Meta ürünlerinde bulunan kullanıcı profilleriyle eşleştirebildiğini ortaya koymaktadır. Bu eşleştirmeler ziyaretçilerin IP adresi, kullanıcı aracısı ve konum verisi gibi temel verilere dayalı yapılmaktadır. Piksel tabanlı izlemelerde eşleştirme ve doğrululuk oranı daha yüksek olsa da Conversions API aracılığıyla da bir kişinin doğrudan tanımlanabilme imkânının olduğunu söylemek mümkündür.

Ürün ve hizmetlerinin kullanımını üçüncü taraf çerezlerle sağlayan Meta ve Google; tarayıcıların, eklentilerin, işletim sistemlerinin ve yasaların bu alandaki kısıtlamalarını aşmak için kendilerini birinci taraf olarak gösterecek çözümler de üretmektedir. Birinci taraf çerezler,

kullanıcıların tarayıcılarında, ziyaret ettikleri web sitesinin alan adı altında saklanan bilgi parçacıklarıdır (Fraihi vd., 2024). Söz konusu teknik genellikle web sitesinin CNAME (Canonical Name) alanına üçüncü tarafların verdiği bilgiyi girmesiyle başlar. Böylelikle kullanıcının her web sitesi ziyaretinde Google ve Meta gibi platformlar kendisini birinci taraf olarak gösterir ve engellenme girişimlerini aşar. CNAME gizleme tekniği şu şekilde çalışır: orneksite.com, aslında xxx.orneksite.com gibi bir alt alan adı kullanarak içerik yerleştirir. Ancak xxx.orneksite.com, teknik olarak, üçüncü taraf bir sunucuda barındırılan yyy.basksite.com alan adına yönlendiren bir CNAME kaydıdır. Yani, bu alt alan adı aslında bir izleyiciyi barındıran bir sitenin alan adına yönlendirilmiş bir takma addır. Bu yöntem, gizlilik korumalarını yanıltmaktadır. Tarayıcı, xxx.orneksite.com'u, orneksite.com'un bir parçası olarak kabul eder ve bu sayede birinci taraf çerezlere erişim sağlanır. Bu durum, üçüncü taraf çerezlere gerek kalmadan ve güvenlik bariyerine takılmadan kullanıcıların izlenmesini sağlar. Çerezler, aslında üçüncü taraf sunucularına gönderilse de tarayıcı bunu sanki kullanıcı aynı siteyi ziyaret ediyormuş gibi kabul eder. Bu da izleme sistemlerinin giderek daha fazla kısıtlandığı günümüzde, izleyicilerden daha etkili ve gizlice veri toplanmasına olanak tanır (Olejnik, 2021). Demir ve arkadaşlarının (2022) gerçekleştirdikleri araştırmanın bulguları bize inceledikleri sitelerin %76'sının bu teknikle kullanıcı izlediğini söylemektedir. Üstelik 2021 itibariyle bu yöntemin kullanımında %50'den fazla bir artış gözlemlenmiştir. Dimova ve arkadaşları (2021), e-posta ve oturum bilgisi (kimlik bilgisi) gibi kullanıcının doğrudan tanımlanabildiği hassas bilgilerin CNAME aracılığıyla izleyicilere aktarıldığını tespit etmişlerdir. Benzer bir diğer araştırmada ise (Ren vd., 2021) özellikle kimlik doğrulama ve kişisel bilgilerin birinci taraf çerezler neticesinde sızmasına dikkat çekilerek durumun ciddi güvenlik riskleri taşıdığı belirtilmiştir. Kullanıcı verilerinin birinci taraf olarak belirtilen platformlara CNAME kaydı aracılığıyla aktarımının, üçüncü taraf çerezlere nazaran daha arka planda gerçekleştiği ve ortaya çıkarılmasının daha teknik bilgi gerektirdiği söylenebilir.

Fransız reklam şirketi Criteo, Silikon Vadisi çıkışlı Google, Meta ve Amazon gibi çevrimiçi reklam sektörünün öncüleri dışında, Avrupa menşeli en büyük şirketlerden biridir. Son 5 yıllık kazancı her yıl ortalama 2 milyar dolardır (Statista, 2024b). Üçüncü taraf çerezleri engelleme girişimleri ve siteler arası gözetleme faaliyetlerinin kısıtlanmasıyla birlikte gözetim tekniklerini çeşitlendirmeye başlamıştır. 2020'de yayımladıkları "Online Identification at Criteo" başlıklı rapor, söz konusu strateji ve yöntemleri içermektedir (Criteo, 2020). Bu rapordaki yöntemler ana hatlarıyla şu şekildedir:

1) Birinci Taraf Veriler: Criteo, 20.000'den fazla müşterisinin web sitesi ve mobil uygulamasından topladığı tüm verileri birinci taraf veri olarak kabul etmektedir. Bu veriler kullanıcı ile doğrudan etkileşimler sonucunda toplanmakta ve üçüncü taraf çerezlere bağlı olarak çalışmamaktadır. Örneğin, Criteo iş ortağı bir e-ticaret sitesini ziyaret eden kullanıcının ürün inceleme, sepete ekleme, satın alma gibi aktiviteleri Criteo için toplanabilir birinci taraf veriler-

dir. Diğer yandan, web siteleri ve mobil uygulamalardaki reklam alanlarının satışını sağlayan Criteo'nun Direct Bidder adlı teknolojisi, 5.000' yakın yayıncıya bağlıdır ve bu platformlardaki e-posta veya oturum açma bilgisi gibi birinci taraf kimlik bilgilerine doğrudan erişim sağlayabilmektedir. Son olarak Criteo büyük perakende firmalarıyla iş birliği içinde olduğu Retail Media adlı sistemi ile bu pazardaki birinci taraf verileri de toplamaktadır. Birinci taraf verilere dayalı çözümleriyle Criteo hem reklam hedeflemesi hem de kişiselleştirme konusunda kontrol alanını güvende tutmaya çalışmaktadır. Bu çabalar neticesinde üçüncü taraf çerezlere ilişkin yaptırımların etkilerini en aza indirmeyi amaçlamaktadır.

2) Kimlik Grafiği (Identity Graph): Criteo'nun en güçlü ürünlerinden birisi sahip olduğu kimlik grafiğidir. 2 milyardan fazla kullanıcıya sahip olan bu veritabanı ile Criteo kendisini birçok rakibinden ayırmaktadır. Kimlik grafiğindeki verilerin büyük çoğunluğu kullanıcı – veri eşleşmesini yüksek doğrulukla gerçekleştirmekte, dolayısıyla deterministik verilere dayanmaktadır. Dört farklı doğrulama yöntemi ile toplanan verilerin gerçekten ilgili kullanıcılardan geldiği tespit edilir ve kesin bir eşleştirme sağlanır. Neredeyse Google ve Meta kadar kullanıcı verisine sahip olan Criteo, birinci taraflardan sağladığı veri akışı ile kimlik grafiğini zenginleştirmeye devam etmektedir.

3) Cihaz Tanımlayıcılar: Criteo'nun çerezsiz izleme yöntemlerinden bir diğeri, cihaz tanımlayıcılarını kullanarak kimlik doğrulama yapmak ve kullanıcıyı cihazı aracılığıyla belirlemektir. Diğer ifadeyle, bir kullanıcının kim olduğunu cihazına yüklediği birçok uygulama üzerinden teyit edebilecek izleme yöntemine sahiptirler. Böylesine bir güce sahip olmalarının arkasında, 22.600'den fazla mobil uygulamaya erişim imkânı bulunmaktadır. Çerez kullanmadan bu kadar çok mobil uygulamaya bağlanabilmesi, yüklü cihazların ve dolayısıyla kullanıcıların kimliklerini tespit etmesine olanak tanır. Böylelikle bir e-ticaret uygulamasında ürün arayan, görüntüleyen, sepete ekleyen, satın alan veya almaktan vazgeçen bir kullanıcı bir başka uygulamada gezinmeye devam ettiğinde söz konusu alışveriş davranışına göre hedefli reklamlarla karşılaşabilmektedir. Üçüncü taraf çerezler engellense bile hem kimlik grafiği hem de cihaz tanımlayıcı yöntemleri sayesinde kullanıcılar tanımlanabilir ve hedeflenebilir olmaya devam etmektedir.

4) Makine Öğrenimi: Criteo, kullanıcıları farklı platformlarda ve cihazlarda tek bir kimlik altında birleştirmek için makine öğreniminden yararlanmaktadır. Bu sayede aynı kullanıcı farklı ağlarda, platformlarda ve cihazlarda tespit edilerek tek bir çatı altında toplanır. Bir kullanıcı, gündüz iş yerindeki bilgisayarında, akşam ise mobil cihazında bir alışveriş sitesini ziyaret ettiğinde, oturum bilgileri veya eşleştirilebilecek diğer kimlik tanımlayıcılar aracılığıyla bu kişinin aynı kullanıcı olduğu sonucuna varılabilir. Bu yöntem bir yandan çapraz aygıt eşleşmesinin de bir parçasıdır. Cihaz eşleşmesi yapılan kişiler hakkında farklı öngörüler oluşturulması mümkündür. Örneğin, kişinin her gün işe gidip geldiği tespit edilebilir: cihazlar arasında muhtemel eşleşmeler oluşturmak için günün saati, konum, cihaz türü, işletim sistemi vb. binlerce veri noktası algoritmik olarak analiz edilir. Cep telefonu, tablet ve dizüstü bilgisayar

hafta içi her gün aynı yerde kablosuz ağa bağlanıyorsa, bu üç cihazın sürekli işe gidip gelen birine ait olduğunu tahmin etmek basittir (Christl & Spiekermann, 2016:92). IAB'ın (İnteraktif Reklamcılık Derneği) çerezsiz dönem için öngördüğü senaryoların birisinde makine öğrenimine ilişkin daha net bir tablo çizilmiştir (Ivaturi vd., 2024). Normalde çerez gibi tanımlayıcılar sayesinde toplanan verilerle bir kişinin "anne" olabileceği tahmin edilebilirken, çerezsiz dünyada Spotify verisi üzerinden belirli saatlerde dinlediği müzik türü ile öngörülmektedir. Bu da platformların makine öğrenimine sıkça başvurması anlamına gelmektedir. Belirli verilerin işlenerek yeni anlamlar üretilmesi, bu alanda makine öğrenimini vazgeçilmez kılmaktadır.

Görüldüğü üzere Criteo'nun çerezsiz gözetime ilişkin çözümleri birinci taraf verilere, eskiden beri toplayıp geliştirdiği büyük veri tabanına, mobil uygulamalar aracılığıyla cihazları tanımlayarak aktivitelerin izlenmesine ve makine öğrenimine dayanmaktadır. Güncel olarak toplanmaya devam eden tüm veriler kendi veri tabanlarını da eğitmeye ve geliştirmeye devam etmektedir. Sadece toplanan veriler değil, bunların ürettiği yeni öngörüler de ilgili şirketin kimlik grafiğini zenginleştirmektedir.

Dijital reklam sektörünün içinde olan veya dolaylı bağlantısı olan tüm platformlar çerezsiz dünyaya ayak uydurabilecek iyileştirmeler yapmaktadır. 2023 geliri neredeyse 2 milyar dolar olan (Statista, 2024a) ABD merkezli reklam teknoloji şirketi The Trade Desk, Unified ID 2.0 (UID 2.0) adını verdiği reklam teknolojisinin altyapısını hazırlamıştır. Bu teknoloji kullanıcıların e-posta veya telefon numarası gibi kimlik bilgilerine dayalı, kullanıcıyı doğrudan belirleyen bir sistemdir. Bugün telif hakkı olmayan ve bağımsız bir kuruluşa devredilen sistem reklam ekosistemindeki tüm paydaşların kullanımına açıktır (Unified ID 2.0, t.y.). Kullanıcılar, UID 2.0'ı destekleyen bir web sitesine girdiklerinde e-posta adreslerini doğruladıkları anda sisteme dahil olurlar. Bir kez onay verdiklerinde, UID 2.0 ağına bağlı tüm web siteleri bu kullanıcıya kişiselleştirilmiş reklamlar gösterme olanağı elde eder. Sistem, her kullanıcı için eşsiz ve şifreli bir tanımlayıcı üretir. Bu tanımlayıcı, üçüncü taraf çerezlerde olduğu gibi kullanıcının takibini sağlar. Şu anda Xandr gibi reklam platformları, The Washington Post gibi basın kuruluşları ve LiveRamp gibi büyük veri şirketleri bu ağa aktif olarak dahildir (theTradeDesk, 2024).

Polonya merkezli reklam şirketlerinden RTB House, yeniden hedeflemeye ilişkin hazırladığı raporda çerezsiz dünyada veri toplama işlemleri için çeşitli öneri ve öngörülerde bulunmuştur (RTB House, 2024). Raporda şu başlıklar dikkat çekmektedir: (1) birinci taraflardan, yani web siteleri ve uygulamaların kendilerinden veri toplamak oldukça kıymetli hale gelmektedir. (2) Google'ın Privacy Sandbox çözümü, kullanıcı kimliklerine dayalı olmadan yeniden hedefleme için oldukça güçlü araçlar sunmaktadır. (3) kullanıcı davranışları ve ilgi alanlarını anlık olarak izleyip analiz eden derin öğrenme yöntemleri kullanıcı verisi toplama ve üretmede etkin bir rol oynamaktadır. RTB House çerezsiz veri toplama süreçlerinde bu üç yöntemin değerli olduğuna dikkat çekmektedir.

Microsoft'un geliştirdiği Ad Selection API (AS API) ile üçüncü taraf çerezlere gerek

duymadan kullanıcıları ilgisine göre kategoriler altında toplamaktadır. Çalışma mantığı PA API'ye benzeyen AS API, Edge tarayıcısı üzerinde çalışarak veri toplamaktadır. 2024'ün ikinci yarısıyla birlikte ilgili tarayıcı üzerinde deneme testleri yürütülmektedir (Microsoft Edge Team, 2024).

Dünyanın en değerli şirketlerinden birisi olan, dijital reklam alanında da yıldan yıla büyük bir sıçrama yaşayan ve 2023'teki reklam geliri yaklaşık 47 milyar dolar (Faria, 2024) olan Amazon da çerezsiz dünyaya yönelik kendi çözümünü oluşturmaya başlamıştır. Ad Relevance adını verdiği reklam hedefleme hizmeti, çerezlere ihtiyaç duymadan Amazon'un kendi platformundaki birinci taraf verileri yapay zekayla birleştirerek yeni veri setleri ve anlamların üretimini kapsamaktadır. Milyarlarca gezinme, satın alma ve hatta Amazon Prime yayınlarını izleme sinyalleri yapay zekâ desteği ile analiz edilmektedir (Amazon Ads, 2024). Bu araç aracılığıyla kullanıcılar farklı cihazlarda (bilgisayar, telefon, akıllı tv, tablet), farklı kanallarda (sosyal medya, web siteleri) ve farklı içerik türlerinde (alışveriş siteleri, haber siteleri, videolar) hedeflenebilmektedir.

Şirketlerin çerezler ile gözetleme faaliyetlerine gelen engellemeler özellikle veriye dayalı reklam endüstrisinin devamlılığını sağlamada problemler yaratırken ilgili kuruluşların yeni çözümler üretmelerine de önayak olmuştur. Çözümlerin nihai amacı, kullanıcıların gizliliğini korumaktan ziyade, kapitalist bir yapıya sahip olmaları nedeniyle öncelikle kendi gelirlerini ve endüstrideki diğer paydaşların gelirlerini korumak ve artırmaktır. Bu süreçte birçoğunun projelerini "gizlilik dostu", "kullanıcı dostu", "anonim" gibi ifadelerle taçlandırdığı görülmektedir. Sistemlerin henüz yeni geliştirilme aşamasında yapılan araştırmalar halen birçok noktada çevrimiçi mahremiyetin ihlal edildiğini ortaya koymaktadır. Gerek Google'ın gerekse Meta'nın ürünlerinde gizlilik bağlamında hala açık kapılar yer almaktadır. Geniş bir bakış açısıyla ele alırsak Sivan-Sevilla ve Parham'ın (2022) geliştirdikleri ölçek üzerinden yaptıkları araştırma, çerezsiz izleme yöntemlerinin çevrimiçi gözetimi daha geniş alana yayarak daha kalıcı ve daha kırılgan hale getirebileceğini göstermektedir. Araştırmacılar, çerezsiz çözümlerin kullanıcıları daha kısıtlı ve anonim şekilde takip edeceği varsayımlarının aksine daha ayrıntılı hedefleme ve profilleme yapmalarına imkân sağladığına dikkat çekmektedir. Kullanıcı açısından ele alırsak, çerezsiz gözetim yöntemlerinin çerezler gibi gözle görülebilir ve sıradan kullanıcıların kolay erişebileceği teknikler içermediği görülmektedir. Aksine, tespiti daha zor ve bu nedenle genellikle açık rıza almayı bile gerektirmeyecek sistemlerden oluşmaktadırlar. Bu bakımdan da GDPR gibi yasal düzenlemelerle uyumlu şekilde çalışmasının şüpheli olduğu ve temel hakları ihlal etme noktasında sorunlar oluşturduğu düşünülmektedir.

Sonuç

Bu çalışmada çerezlerin kullanımına yönelik gelen kısıtlamalara çözüm olarak ortaya atılan çerezsiz dünya ve ona ait yeni nesil izleme yöntemleri irdelenmiştir. Üçüncü taraf çerezler tarayıcılar tarafından engellendikçe ve yasalar bu çerezlerin kullanımını katı kurallarla sınırlandır-

dıkça, veri toplayan ve gelir modeli veri olan aktörler çerez tabanlı iş akışlarını azaltmaya başlamıştır. Geliştirilen yeni ürünler ve sunulan alternatif stratejiler, çevrimiçi gözetimde köklü değişimlerin yaşandığını göstermektedir. Köklü değişim sadece teknik düzeyde bir ilerlemeden ziyade, dijital gözetim pratiklerinin doğasında yapısal bir değişim yaşandığını göstermektedir.

Çerezsiz dünyaya geçişin öncüsü olan teknoloji şirketleri aynı zamanda gözetleme faaliyetlerinden en çok gelir elde edenlerdir. Çalışmalar, bu şirketlerin geliştirdikleri sistemlerin henüz vadettikleri gizliliği sağlayamadıklarını göstermektedir. Diğer yandan birinci taraf verilerin kullanımı, sunucu taraflı izleme ve CNAME ile birinci tarafmış gibi maskeleme yöntemleri ile veri toplama çerezlerle kıyaslandığında daha zor tespit edilebilir ve daha az görünür şekilde gerçekleşmektedir. Bu bağlamda çerezsiz dünya, yalnızca bir teknolojik geçiş süreci değil; bireylerin mahremiyet, rıza ve "sessiz/saklı" gözetim karşısındaki konumunu da yeniden tanımlayan bir iletişim paradigması olarak değerlendirilebilir. Gözetim kapitalizmi, platform ekonomisi ve veri sömürüsü gibi güncel dijital iletişim tartışmaları yeni nesil izleme yöntemlerinin sosyoekonomik ve kültürel etkilerini anlamlandırmak açısından önemli kavramsal dayanaklar sunmaktadır.

Makine öğrenimi ile var olan veri setlerinin zenginleştirilmesi, tahminler üretilmesi ve gelecek öngörüleri de çerezsiz dünyanın bir parçası haline gelmiştir. Kullanıcılar hangi verilerinin toplandığı ve bunların nasıl kullanıldığı konusunda çoğu zaman habersiz olabilirler. Mahremiyetin kâr maksimizasyonu adına doğrudan zedelendiği bu gibi yöntemler tarayıcılar tarafından engellenemeyeceği gibi yasaların radarına girme durumu da soru işareti barındırmaktadır. Dolayısıyla veri koruma düzenlemelerinin etkinliği, zor tespit edilebilir bu sistemler karşısında daha kırılgan olabilmektedir. Yazılım geliştiricileri, sivil toplum kuruluşları, sosyal bilimciler, akademisyenler ve araştırmacıların bu alandaki denetleyici ve güncel saha araştırmaları, çerezsiz dünyada söz sahibi olan şirketler üzerinde baskı oluşturabileceği gibi, aynı zamanda temel insan haklarından biri olan mahremiyetin korunmasına da destek sağlayacaktır.

Kaynakça

Amazon Ads. (2024, Ekim 15). *Deliver more relevant ads everywhere, independent of ad ids, with Ad Relevance*. Amazon Ads. 17 Kasım 2024 tarihinde https://advertising.amazon.com/resources/whats-new/ad-relevance adresinden alınmıştır.

Arthur. (2023, Ekim 4). *Unpacking Data Privacy Concerns in Google's Privacy Sandbox*. 11 Eylül 2024 tarihinde https://heydata.eu/en/magazine/data-privacy-concerns-with-google-s-privacy-sandbox adresinden alınmıştır.

Beugin, Y., & McDaniel, P. (2023). *Interest-disclosing Mechanisms for Advertising are Privacy-Exposing*.

https://doi.org/10.48550/arXiv.2306.03825

BuiltWith. (2024a, Eylül 24). *Advertising Technologies Web Usage Distribution in Turkey*. 24 Eylül 2024 tarihinde https://trends.builtwith.com/ads/country/Turkey adresinden alınmıştır.

BuiltWith. (2024b, Eylül 24). *Analytics Technologies Web Usage Distribution in Turkey*. 24 Eylül 2024 tarihinde https://trends.builtwith.com/analytics/country/Turkey adresinden alınmıştır.

Chavez, A. (2022, Temmuz 27). *Expanding testing for the Privacy Sandbox for the Web*. Google. 13 Eylül 2024 tarihinde https://blog.google/products/chrome/update-testing-privacy-sandbox-web/ adresinden alınmıştır.

Chavez, A. (2024, Temmuz 19). *A new path for Privacy Sandbox on the web*. Privacy Sandbox. 28 Eylül 2024 tarihinde https://privacysandbox.com/news/privacy-sandbox-update adresinden alınmıştır.

Christl, W., & Spiekermann, S. (2016). *Networks of Control. A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy*. Facultas. http://crackedlabs.org/en/networksofcontrol

Clark, A. (2007, Aralık 6). Facebook apologises for mistakes over advertising. *The Guardian*. 29 Ekim 2024 tarihinde https://www.theguardian.com/technology /2007/dec/06/facebook.socialnetworking adresinden alınmıştır.

CNIL. (2023, Temmuz 12). *"Privacy Sandbox" sur Google Chrome: Quelles conséquences pour les utilisateurs? | CNIL*. 2 Kasım 2024 tarihinde https://www.cnil.fr/fr/privacy-sandbox-sur-google-chrome-quelles-consequences-pour-les-utilisateurs adresinden alınmıştır.

Criteo. (2020). *Online Identification at Criteo*. https://criteo.investorroom.com/download/Deck_CriteoOnlineIdentification.pdf

Deckelmann, S. (2020, Ağustos 4). *Latest Firefox rolls out Enhanced Tracking Protection 2.0; blocking redirect trackers by default | The Mozilla Blog*. 28 Ekim 2024 tarihinde https://blog.mozilla.org/en/products/firefox/latest-firefox-rolls-out-enhanced-tracking-protection-2-0-blocking-redirect-trackers-by-default/ adresinden alınmıştır.

Demir, N., Theis, D., Urban, T., & Pohlmann, N. (2022). *Towards Understanding First-Party Cookie Tracking in the Field* . https://doi.org/10.48550/arXiv.2202.01498

Dimova, Y., Acar, G., Olejnik, L., Joosen, W., & Van Goethem, T. (2021). The CNAME of the Game: Large-scale Analysis of DNS-based Tracking Evasion. http://arxiv.org/abs/2102.09301

Facebook. (2007, Kasım 6). Leading Websites Offer Facebook Beacon for Social Distribution. *Meta*. 16 Ekim 2024 tarihinde https://about.fb.com/news/2007/11/leading-websites-offer-facebook-beacon-for-social-distribution/ adresinden alınmıştır.

Faria, J. (2024, Şubat 29). *Amazon global ad revenue 2023*. Statista. 15 Ekim 2024 tarihinde https://www.statista.com/statistics/259814/amazons-worldwide-advertising-revenue-development/ adresinden alınmıştır.

Fraihi, A. E., Amieur, N., Rudametkin, W., & Goga, O. (2024). Client-side and Server-side Tracking on Meta: Effectiveness and Accuracy. *Proceedings on Privacy Enhancing Technologies*. 11 Kasım 2024 tarihinde https://petsymposium.org/popets/2024/popets-2024-0086.php adresinden alınmıştır.

FTC. (2007, Aralık 20). *Federal Trade Commission Closes Google/DoubleClick Investigation*. 3 Kasım 2024 tarihinde https://www.ftc.gov/news-events/news/press-releases/2007/12/federal-trade-commission-closes-googledoubleclick-investigation adresinden alınmıştır.

GDPR. (t.y.). *Cookies, the GDPR, and the ePrivacy Directive*. GDPR. 5 Ekim 2024 tarihinde https://gdpr.eu/cookies/ adresinden alınmıştır.

Gilbert, J. O. (2011, Eylül 26). *New Privacy Fear: Facebook Allegedly Tracking Users Who Log Out (UPDATE)*. 23 Ekim 2024 tarihinde https://www.huffpost.com/entry/facebook-logout-cookies-privacy-tracking_n_980838 adresinden alınmıştır.

Goel, V. (2021, Haziran 24). *An updated timeline for Privacy Sandbox milestones*. Google. 13 Eylül 2024 tarihinde https://blog.google/products/chrome/updated-timeline-privacy-sandbox-milestones/ adresinden alınmıştır.

Goel, V. (2022, Ocak 25). *Get to know the new Topics API for Privacy Sandbox*. Google. 13 Eylül 2024 tarihinde https://blog.google/products/chrome/get-know-new-topics-api-privacy-sandbox/ adresinden alınmıştır.

Ivaturi, N. M., Ramdhani, B., Erikson, A., Rehberg, B., & Fung, F. (2024). *Targeting & Measurement in a Cookieless World*. https://iabseaindia.com/wp-content/uploads/2024/08/IAB_Guide-targeting-Cookieless-World.pdf

Jha, N., Trevisan, M., Leonardi, E., & Mellia, M. (2023). *On the Robustness of Topics API to a Re-Identification Attack*. https://doi.org/10.48550/arXiv.2306.05094

Jo Dixon, S. (2024, Şubat 12). *Global Meta advertising revenue 2023*. Statista. 6 Ekim 2024 tarihinde https://www.statista.com/statistics/271258/facebooks-advertising-revenue-worldwide/ adresinden alınmıştır.

Johnson, G. A., & Neumann, N. (2024). *The advent of privacy-centric digital advertising: Tracing privacy-enhancing technology adoption*. https://pep.gmu.edu/wp-content/uploads/sites/28/2024/04/Johnson-Neumann.pdf

Kravets, D. (2012, Ağustos 9). 9 Kasım 2024 tarihinde *FTC Dings Google $22.5M in Safari Cookie Flap*. Wired. https://www.wired.com/2012/08/ftc-google-cookie/ adresinden alınmıştır.

Kristol, D. M. (2001). HTTP Cookies: Standards, privacy, and politics. *ACM Transactions on Internet Technology*, *1*(2), 151-198. https://doi.org/10.1145/502152.502153

Libert, T. (2015). Exposing the Invisible Web: An Analysis of Third-Party HTTP Requests on 1 Million Websites. *International Journal of Communication*, *9*(0), Article 0.

Lokke, E. (2018). *Mahremiyet Dijital Toplumda Özel Hayat* (D. Başak, Çev.). Koç Üniversitesi Yayınları.

Long, M., & Evans, D. (2024). *Evaluating Google's Protected Audience Protocol* https://doi.org/10.48550/arXiv.2405.08102

Lyon, D. (2013). *Gözetim Çalışmaları* (A. Toprak, Çev.). Kalkedon Yayınları.

Lyon, D. (2018). *Gözetlenen Toplum Günlük Hayatı Kontrol Etmek* (G. Soykan, Çev.; 2. bs). Kalkedon Yayınları.

Mathew, E. (2022, Nisan 27). The Death of 3rd-Party Cookies: Benefits of Google Server-Side Tagging. 9

Kasım 2024 tarihinde *Ayruz Data Marketing: Data Driven Digital Marketing and Analytics Agency*. https://ayruz.com/the-death-of-3rd-party-cookies-benefits-of-google-server-side-tagging/ adresinden alınmıştır.

McDonald, A., & Peha, J. (2011). *Track Gap: Policy Implications of User Expectations for the "Do Not Track" Internet Privacy Feature*.

Meta. (2024). *Dönüşümler API'si: Reklam Performansının Optimize Edilmesi ve Artırılması*. Meta for Business. 6 Ekim 2024 tarihinde https://tr-tr.facebook.com/business/tools/conversions-api adresinden alınmıştır.

Microsoft. (2004, Eylül 3). *How to Manage Cookies in Internet Explorer 6 (283185)*. 6 Ekim 2024 tarihinde https://ftp.zx.net.nz/pub/Patches/ftp.microsoft.com/MISC/KB/en-us/283/185.HTM adresinden alınmıştır.

Microsoft Edge Team. (2024, Mart 5). *New Privacy-Preserving Ads API coming to Microsoft Edge*. 17 Kasım 2024 tarihinde https://blogs.windows.com/msedgedev/2024/03/05/new-privacy-preserving-ads-api/ adresinden alınmıştır.

Noyb. (2024, Haziran 13). *Google Sandbox: Online tracking instead of privacy*. 14 Kasım 2024 tarihinde https://noyb.eu/en/google-sandbox-online-tracking-instead-privacy adresinden alınmıştır.

Olejnik, L. (2021, Şubat 23). *Large-scale Analysis of DNS-based Tracking Evasion—Broad data leaks included?* Security, Privacy & Tech Inquiries. 6 Ekim 2024 tarihinde http://blog.lukaszolejnik.com/large-scale-analysis-of-dns-based-tracking-evasion-broad-data-leaks-included/ adresinden alınmıştır.

Peacock, S. E. (2014). How web tracking changes user agency in the age of Big Data: The used user. *Big Data & Society*, *1*(2), 2053951714564228. https://doi.org/10.1177/2053951714564228

Philipse, M. (2024). *Post-Third-Party Cookies: Analyzing Google's Protected Audience API* [Yayımlanmamış Yüksek Lisans Tezi]. Radboud University.

Ren, T., Wittmany, A., Carli, L. D., & Davidsony, D. (2021). An Analysis of First-Party Cookie Exfiltration due to CNAME Redirections. *Proceedings 2021 Workshop on Measurements, Attacks, and Defenses for the Web*. Workshop on Measurements, Attacks, and Defenses for the Web. https://doi.org/10.14722/madweb.2021.23018

Rescorla, E. (2021, Haziran 10). *Privacy analysis of FLoC*. 25 Eylül 2024 tarihinde https://blog.mozilla.org/en/mozilla/privacy-analysis-of-floc/ adresinden alınmıştır.

Routley, N. (2020, Ocak 20). *Internet Browser Market Share (1996–2019)*. 12 Eylül 2024 tarihinde Visual Capitalist. https://www.visualcapitalist.com/internet-browser-market-share/ adresinden alınmıştır.

Roviaro, N. (2020, Aralık 17). *A more private web can help businesses grow*. Google. 23 Eylül 2024 tarihinde https://blog.google/around-the-globe/google-europe/more-private-web-can-help-businesses-grow/ adresinden alınmıştır.

RTB House. (2024). *Your Concise Retargeting Guide for Classifieds*. RTB House. 23 Eylül 2024 tarihinde https://www.rtbhouse.com/resources/your-concise-retargeting-guide-for-classifieds adresinden alınmıştır.

Salinas, S. (2018, Nisan 4). *Facebook says the number of users affected by Cambridge Analytica data leak is 87 million*. CNBC. 8 Kasım 2024 tarihinde https://www.cnbc.com/2018/04/04/facebook-upda-

tes-the-number-of-users-impacted-by-cambridge-analytica-leak-to-87-million-.html adresinden alınmıştır.

Schuh, J. (2019, Ağustos 22). *Building a more private web*. Google. 13 Eylül 2024 tarihinde https://blog.google/products/chrome/building-a-more-private-web/ adresinden alınmıştır.

Schuh, J. (2020, Ocak 14). Building a more private web: A path towards making third party cookies obsolete. *Chromium Blog*. 13 Eylül 2024 tarihinde https://blog.chromium.org/2020/01/building-more-private-web-path-towards.html adresinden alınmıştır.

Sivan-Sevilla, I., & Parham, P. T. (2022). *Toward (Greater) Consumer Surveillance in a 'Cookie-less' World: A Comparative Analysis of Current and Future Web Tracking Mechanisms*. OSF. https://doi.org/10.31235/osf.io/rauwj

Statista. (2024a, Mart 6). *Revenue generated by The Trade Desk, Inc. From 2016 to 2023*. Statista. 29 Ekim 2024 tarihinde https://www.statista.com/statistics/1221457/the-trade-desk-revenue/ adresinden alınmıştır.

Statista. (2024b, Nisan 5). *Criteo revenue 2023*. Statista. 28 Ekim 2024 tarihinde https://www.statista.com/statistics/1361058/criteo-revenue/ adresinden alınmıştır.

Statista. (2024c, Eylül). *Internet browser market share 2012-2024*. Statista. 28 Ekim 2024 tarihinde https://www.statista.com/statistics/268254/market-share-of-internet-browsers-worldwide-since-2009/ adresinden alınmıştır.

Story, L., & Helft, M. (2007, Nisan 14). Google Buys DoubleClick for $3.1 Billion (Published 2007). *The New York Times*. 28 Ekim 2024 tarihinde https://www.nytimes.com/2007/04/14/technology/14DoubleClick.html adresinden alınmıştır.

Taşkaya, M., & Talay, Ö. (2019). *Dijital Gözetimin Pazarlama Amaçlı Aracıları: "Çerezler" ve Çerez Kullanımında "Açık Rıza"*. Akdeniz Üniversitesi İletişim Fakültesi Dergisi(31), 356-376. https://doi.org/10.31123/akil.534603

Temkin, D. (2021, Mart 3). *Charting a course towards a more privacy-first web*. Google. 7 Ekim 2024 tarihinde https://blog.google/products/ads-commerce/a-more-privacy-first-web/ adresinden alınmıştır.

The Privacy Sandbox. (2024, Mayıs 3). *Update on the plan for phase-out of third-party cookies on Chrome*. Privacy Sandbox. 7 Ekim 2024 tarihinde https://privacysandbox.com/ news/update-on-the-plan-for-phase-out-of-third-party-cookies-on-chrome/ adresinden alınmıştır.

theTradeDesk. (2024). *Unified ID Solution 2.0 | The Trade Desk*. 22 Eylül 2024 tarihinde https://www.thetradedesk.com/us/about-us/industry-initiatives/unified-id-solution-2-0 adresinden alınmıştır.

Thomson, M. (2023). *A Privacy Analysis of Google's Topics Proposal*. Mozilla. https://mozilla.github.io/ppa-docs/topics.pdf

Thomson, M. (2024). *Protected Audience Privacy Analysis*. Mozilla. https://mozilla.github.io/ppa-docs/protected-audience.pdf

Uluk, M. (2023). "*Sitemizi ziyaret ederek çerezleri kabul etmiş sayılırsınız": Türkiye'deki haber sitelerinin çerez kullanım izinleri üzerine bir araştırma*. Connectist: Istanbul University Journal of Communication Sciences, 64, 213-247. https://doi.org/10.26650/CONNECTIST2023-1219698

Unified ID 2.0. (t.y.). *About | Unified ID 2.0*. https://unifiedid.com/

Untila Kaplan, O. (2020). *The Use of Digital Monitoring Technologies (Cookies) in Turkish, Romanian and Russian Internet Journalism: Comparative Privacy and Practice Criterion*. Turkish Studies-Social Sciences. http://dx.doi.org/10.29228/TurkishStudies.42954

Weinlich, P., Semerádová, T., & Dostál, M. (2022). *Replacing Cookies in Online Advertising with API Conversion Tracking* (SSRN Scholarly Paper 4275103). Social Science Research Network. https://doi.org/10.2139/ssrn.4275103

Wilander, J. (2017, Haziran 5). Intelligent Tracking Prevention. 11 Ekim 2024 tarihinde https://webkit.org/blog/7675/intelligent-tracking-prevention/ adresinden alınmıştır.

Zandt, F. (2024, Eylül 10). *Infographic: Google's Ad Revenue Dwarfs Competitors*. Statista Daily Data. 18 Ekim 2024 tarihinde https://www.statista.com/chart/33017/annual-advertising-revenue-of-selected-tech-companies-offering-search-solutions adresinden alınmıştır.