Girişimcilik İnovasyon ve Pazarlama Araştırmaları Dergisi
Yıl:2026, 10(19) :1-19

Journal of Research in Entrepreneurship Innovation and Marketing
Year:2026, 10(19) :1-19

Makale Türü: Araştırma Makalesi
Paper Type : Research Paper

Geliş Tarihi / Received: 04.04.2026
Kabul Tarihi / Accepted: 04/05/2026

Dijital Pazarlamanın Yeni Altın Standardı: Yapay Zeka Destekli Zero-Party Data

https://doi.org/10.31006/gipad.1923227

Sabiha KILIÇ*

Öz

Bu çalışmada, dijital pazarlamada üçüncü taraf çerezlerin döneminin kapanmaya başladığı "post-cookie" döneminde, tüketici gizliliğinin pasif takipten gönüllü veri paylaşımına evrilen 20 yıllık entelektüel eğilim yapısının haritalandırılması amaçlanmaktadır. Çalışma, kişisel verilerin korunmasına ilişkin yasal düzenlemelerin giderek sıkılaşması ve tüketicilerin veri güvenliğine yönelik endişelerinin artması nedeniyle, markaların dijital pazarlama faaliyetlerinde tüketici verilerini şeffaf olmayan yöntemlerle toplamasının giderek zorlaştığı varsayımına dayanmaktadır. CiteSpace bibliyometrik veri analizleri, bu yeni dönemin merkezinde "güven" kavramının bulunduğunu ve "yapay zeka" ekseninde kişiselleştirme-gizlilik paradoksunun dengelenebileceğini ortaya koymaktadır. Bulgular, yapay zeka destekli zero-party data yaklaşımının tüketicilerin veri paylaşım süreçlerinde daha aktif rol üstlenmelerini teşvik ederek kişiselleştirme-gizlilik paradoksunun azaltılmasına katkı sağlayabileceğini göstermektedir. Özellikle şeffaf ve etik bir yaklaşımla desteklenen bu yöntem, tüketicilerin harcama eğilimlerinin artmasını sağlayarak markalar ve tüketiciler arasında sürdürülebilir bir sadakat köprüsü kurmaktadır. Bulgular, yapay zeka destekli zero-party data yaklaşımının tüketicilerin veri paylaşım süreçlerinde daha aktif rol üstlenmelerini teşvik ederek kişiselleştirme-gizlilik paradoksunun azaltılmasına katkı sağlayabileceğini göstermektedir.

***Anahtar Kelimeler**: Dijital Gizlilik, Zero-Party Data, Gizlilik Paradoksu, Dijital Pazarlama, CiteSpace.*

The New Gold Standard of Digital Marketing: AI-Powered Zero-Party Data

Abstract

This study aims to map the 20-year intellectual trend of consumer privacy, which has evolved from passive tracking to voluntary data sharing, during the "post-cookie" era as the era of third-party cookies in digital marketing comes to an end. It is based on the assumption that increasingly stringent legal regulations regarding the protection of personal data and growing consumer concerns about data security are making it more difficult for brands to collect consumer data through non-transparent methods in their digital marketing activities. Analyses of CiteSpace bibliometric data reveal that the concept of "trust" lies at the center of this new era and that the personalization-privacy paradox can be balanced along the "artificial intelligence" axis. Findings suggest an AI-powered zero-party data approach could mitigate the personalization-privacy paradox by encouraging consumers to actively participate in data-sharing processes. Supported by transparency and ethics, this method fosters increased consumer spending and builds a sustainable bridge of loyalty between brands and consumers. These findings imply that an AI-powered zero-party data approach could mitigate the personalization-privacy paradox by encouraging consumers to play an active role in data-sharing processes.

***Keywords:** Digital Privacy, Zero-Party Data, Privacy Paradox, Digital Marketing, CiteSpace.*

* Prof. Dr., Hitit Üniversitesi, İİBF, İşletme Bölümü, sabihakilic@hitit.edu.tr
ORCID: https://orcid.org/0000-0002-0906-4567

Expanded Abstract

Objective of the Study

This study aims to map the 20-year intellectual trend in consumer privacy, tracing its evolution from passive tracking to voluntary data sharing within the "post-cookie" era. The primary premise is that brands can no longer secretly collect consumer data due to increasingly stringent legal regulations—such as GDPR and various US state laws—and a growing sense of distrust among consumers regarding personal data protection. Specifically, the research seeks to answer how the digital privacy literature has evolved over the last 30 years, where Zero-Party Data (ZPD) fits within this evolution, and how AI-powered ZPD is transforming consumer trust and privacy perceptions. Ultimately, the study provides strategic guidance for businesses to transition from "unauthorized stalkers" to "transparent value partners" to ensure sustainability in a cookieless economy.

Content and Methodology

The research utilizes a bibliometric data analysis approach to synthesize the structural and temporal dynamics of the digital privacy field. The content is centered on the "personalization-privacy paradox," where consumers desire tailored services but feel vulnerable when their data is collected without explicit consent. The methodology involves using the CiteSpace scientific mapping program to analyze 1,309 scientific works retrieved from the Web of Science (WoS) database. The dataset spans from 1999 to 2026 and includes contributions from 4,318 authors across 814 journals. The analysis focuses on co-citation networks, citation bursts, and keyword centrality to identify "landmark," "hub," and "pivot" nodes that represent significant shifts in the academic discourse. Furthermore, the study contrasts traditional data collection methods (first, second, and third-party) with the emerging importance of Zero-Party Data.

Scope

The scope of this study encompasses the global intellectual landscape of digital privacy and marketing from the late 1990s to the present. It specifically examines the transition of browsers like Chrome, Firefox, and Safari toward restricting third-party cookies, which has forced a shift toward ZPD. The bibliometric scope includes 20 distinct research clusters, with primary focus on "customer satisfaction," "big data," "artificial intelligence," and "privacy protection". The study also reviews seminal works in the field, such as those by Hair et al. (1987) on multivariate analysis and Culnan and Armstrong (1999) on information privacy concerns, to provide a historical context for modern data ethics and consumer behavior.

Results and Discussions

The bibliometric analysis reveals that "Trust" is the most central concept in the new era of digital marketing, appearing as a core keyword with 252 citations. This scientific evidence suggests that trust acts as a "psychological contract" for voluntary disclosure. Another significant finding is the massive "citation burst" for "Artificial Intelligence" (35.45), indicating a paradigm shift from traditional marketing models to technology-driven predictive models. The results show that while the academic maturity of digital privacy is still evolving (evidenced by low network density), it is rapidly becoming a multidisciplinary field where "ethics" and "machine learning" intersect.

The discussion highlights that AI-powered Zero-Party Data effectively resolves the personalization-privacy paradox. Unlike intrusive cookies, ZPD is provided proactively by consumers in exchange for a better experience. AI supports this by making data collection

interactive and "delightful" through chatbots, quizzes, and recommendation engines, rather than being "intrusive".

Strategic recommendations for businesses include:

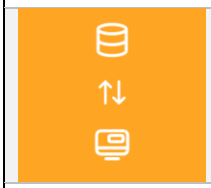
- Establishing a "Value Exchange": Clearly explaining the benefits consumers receive for their data, such as discounts or time savings.
- Trust as a "Product Feature": Treating transparency and data protection as core competitive advantages rather than just legal policies.
- Empowering Consumer Control: Allowing users to manage, delete, or see their data, which significantly reduces privacy anxiety.

In conclusion, the study proves that for businesses to survive in the post-cookie economy, they must adopt AI-powered ZPD as the new "gold standard". This model elevates the consumer from a monitored target to a powerful partner, fostering sustainable loyalty through ethical data management and transparent value creation.

1. Giriş

Günümüz tüketicilerinin paylaştıkları kişisel bilgilerini markaların nasıl kullandıklarına dair bilinç düzeyleri arttıkça, etkileşim kurmayı tercih ettikleri şirketlerden giderek daha fazla şeffaflık ve değer bekledikleri artık bilinen bir gerçektir (Braze, 2025). Tüketicilerin paylaştıkları kişisel verilerin korunmasına ilişkin kuralları belirleyen ve 25 Mayıs 2018 tarihinde yürürlüğe giren Genel Veri Koruma Yönetmeliği GDPR, Avrupa Birliğine üye olan tüm ülkelerde geçerli ve doğrudan bağlayıcı olan bir yönetmeliktir. Yönetmelik, AB vatandaşlarının kişisel verilerinin korunması için usul ve esasları düzenlemektedir (European Parliament and Council of the European Union, 2016). Amerika Birleşik Devletleri'nde ise, 1974 yılından günümüze pek çok gizlilik yasası çıkartılmıştır. 1974 ABD gizlilik yasası, federal hükümetin bireysel gizliliğin korunmasını arttırmak amacıyla yürürlüğe koyduğu bir yasadır. Bu yasa, ABD hükümet kurumlarının kişisel bilgilerin toplanması, kullanımı ve ifşasına ilişkin kurallar ve düzenlemeler sunmaktadır (Varonis, 2023a). Ülkede, 1996 yılında bireylerin tıbbi bilgilerini koruyan Sağlık Sigortası Taşınabilirliği ve Hesap Verebilirlik Yasası (HIPAA) yürürlüğe girmiştir. Bu yasa, sağlık hizmeti sağlayıcıları, hastaneler ve sigorta şirketleri de dahil olmak üzere korunan sağlık bilgilerini işleyen tüm kuruluşlar için geçerlidir (Varonis, 2023b). Amerikan kongresi, 13 yaşın altındaki çocukların çevrimiçi gizliliğini korumak amacıyla 1998 yılında Çocukların Çevrimiçi Gizliliğini Koruma Yasası'nı (COPPA) yürürlüğe koymuştur. COPPA, çocuklardan kişisel bilgi toplayan, kullanan veya ifşa eden tüm web siteleri ve çevrimiçi hizmetler için geçerli olan bir yasadır (Varonis, 2023c). Amerikan hükümeti 1999 yılında tüketici gizliliğini koruyan ve kişisel bilgileri toplayan, kullanan veya açıklayan tüm finansal kurumlar için geçerli olan Gramm-Leach-Bliley Act Yasasını yürürlüğe koymuştur. Bu yasa, finansal kuruluşların çevrim içi olarak toplanan bilgiler de dahil olmak üzere her türlü tüketici verisini kapsamaktadır (Varonis, 2023d). ABD'de 2020 yılı itibariyle başta Kaliforniya olmak üzere, Colorado, Connecticut, Maryland, Massachusetts, New York ve Virginia'da eyalet gizlilik yasaları çıkartılmıştır (Varonis, 2023e). Tüketicilerin, işletmeler ve kuruluşlar tarafından hangi bilgilerin toplandığı ve nasıl kullanıldığına dair gizlilik hakları konusunda bilinçli hale gelmeleriyle birlikte tüketici verilerinin toplanma ve kullanma biçimleri de gelişme göstermektedir. Tüketicilerden veri toplama biçimleri dört başlık altında incelenebilir. Bunlar aşağıda özetlenmektedir:

Tablo 1: Tüketici Verisi Toplama Yöntemleri

Birinci Taraf Verileri	**İkinci Taraf Verileri**	**Üçüncü Taraf Verileri**	**Sıfır Taraflı Veriler**
			
Müşteri ile doğrudan ilişki	Dolaylı müşteri ilişkisi	Dolaylı müşteri ilişkisi	Müşteriyle doğrudan ilişki
Onay alınarak toplanır	Onay alınarak toplanır	Onay alınarak toplanıp toplanmadığı bilinmiyor (veri sağlayıcısına bağlıdır)	Onay alınarak toplanır
Kişisel veriler	Kişisel veriler	Toplu veriler	Bireysel veriler
Yüksek doğruluk ve güvenilirlik	Yüksek doğruluk ve güvenilirlik	Düşük doğruluk ve güvenilirlik	Yüksek doğruluk ve güvenilirlik
Paylaşılmaz	Yalnızca güvenilir iş ortaklarıyla paylaşılır	Birçok şirketle paylaşılır	Paylaşılmaz
Örnekler: Müşteri e-postası, telefon numarası, satın alma geçmişi, destek geçmişi, sadakat programı bilgileri	Örnekler: Web sitesi etkinliği, sosyal medya profilleri, müşteri geri bildirimleri, müşteri anketleri	Örnekler: Gelir, yaş, eğitim, ziyaret edilen web siteleri, anket yanıtları	Örnekler: İletişim tercihleri, ürün tercihleri, kişiselleştirilmiş hesap yapılandırmaları

Kaynak: Treanor, 2025.

Veri gizliliği düzenlemeleri arttıkça ve üçüncü taraf veri kaynakları azaldıkça, işletmelerin kişiselleştirmeyi güçlendirebilmek ve güven oluşturabilmek amacıyla yeni veri toplama yöntemlerine olan ihtiyaç giderek önem kazanmaktadır. Çerezler, internet aracılığıyla tüketici verilerini izlemek ve toplamak için uzun zamandır kullanılan en temel araçlardan biridir. Ancak kişisel verilerin toplanması ve kullanılmasına yönelik usul ve esaslar sürekli değişmektedir. Chrome, 2023 yılı itibariyle kullanıcılarına izlenme bilgilerini seçme imkanı sunmaktadır. Diğer bir ifadeyle, kullanıcılar çerez öncelikleri hakkında bilinçli seçimler yapabilmektedirler. Diğer tarayıcılar da üçüncü taraf çerezlerini kısıtlamış ya da kullanımdan kaldırmışlardır. Firefox, Gelişmiş İzleme Koruması (ETP) özelliği sayesinde izleyicilerden gelen üçüncü taraf çerezlerini engellemektedir. Apple Safari Akıllı İzleme Önleme (ITP) özelliğiyle üçüncü taraf çerezlerini tamamen engellemektedir (Braze, 2025). Dolayısıyla, yasal düzenlemeler ve teknolojik ortamdaki değişiklikler ile birlikte tüketici algılarının da değişmesi kişiselleştirme kapsamında veri gizliliğini korumanın önemini giderek daha belirgin hale getirmiştir. Kişiselleştirme düzeyi arttıkça hizmetin amacına hizmet etme düzeyi ile tüketici kabulü artmakla birlikte bu amaçla paylaşılan kişisel veriler tüketicilerin kendilerini savunmasız hissetmelerine de neden olmaktadır. Tüketiciler bir yandan kendilerine sunulan ürün ve hizmetlerden memnuniyet düzeylerinin yüksek olmasını talep ederlerken diğer yandan gizliliklerinin ihlal edilmemesini, kişisel bilgilerinin güvenli bir şekilde saklanmasını ve sadece iyi niyetli amaçlar için kullanılmasını istemektedirler (Kutty vd., 2021). Üçüncü taraf çerezlerin olmadığı bir dünyada şirketlerin tüketici deneyimlerini izlemek ve kişiselleştirmek için başka bir yol bulmaları gerekmektedir ki bu yol Sıfır Taraf Verisi (ZPD)'dir. Bu terim ilk olarak Forrester Research'ın sektör analistleri tarafından tanımlanmış ve kullanıma sunulmuş olsa da konuya ilişkin pek çok araştırmada da benzer şekilde ifade edilmektedir. Buna göre ZPD, tüketicilerin gönüllü ve proaktif olarak bir markayla paylaştığı her türlü bilgiyi ifade eder. Bu bilgiler genellikle, tüketicilerin karşılığında daha iyi bir deneyim elde edecekleri beklentisiyle paylaşılır (Liu vd., 2025; Khatibloo vd., 2017; Britt, 2020; Gilliland, 2020; Yun vd., 2020).

Dijital pazarlama alanındaki teknolojik gelişmeler ve tüketici verilerinin gizliliği konuları alanın profesyonelleri, araştırmacıları ve akademisyenlerini motive ederek önemli bir literatür birikimine de neden olmuştur. Özellikle verilerin tüketicilerden habersiz veya pasif yöntemlerle toplandığı bir ekosistemden, gönüllü ve proaktif paylaşımla elde edildiği yeni bir ekosistemin oluşmaya başladığı bu dönemde pazarlamacıların artık çerezlere güvenerek strateji geliştirmeleri pek de mümkün görünmemektedir. Bu nedenle üçüncü taraf çerez kullanımının kaldırılması ve gizliliği arttıran teknolojilerin yaygınlaşması sonucunda proaktif bir değer değişim mekanizması olarak Sıfır Taraf Verileri (ZPD) giderek artan oranda gündemdeki yerini almaktadır.

Bu çalışma, Sıfır Taraf Verileri (ZPD) konusunu, yapay zeka, bulut bilişim, veri saklama teknolojileri, tüketici güveni ve müşteri memnuniyeti ekseninde gizlilik konusunda gerçekleştirilmiş akademik çalışmalar kapsamında incelemektedir. Böylece, yaklaşık son 30 yılda gizlilik konusunda gerçekleştirilen bilimsel çalışmalar ışığında pasif izlemeden gönüllü ifşaya uzanan gizlilik konusunun entelektüel gelişim süreci ortaya konulmuştur. Sunulan entelektüel eğilim haritası, işletmelerin izinsiz izleme yerine sıfır taraf verilerini önceliklendirerek post-cookie ekonomisinde sürdürülebilirliklerini nasıl sağlayabileceklerine dair yardımcı olabilecek stratejiler geliştirmelerine imkan sunabilecektir.

2. Yöntem

Çalışmanın amacı, tüketici gizliliği konusunda pasif izlemeden gönüllü ifşaya uzanan süreçte alana ilişkin bilimsel eserlerin entelektüel eğilim yapısını haritalandırmaktır. Böylece pazarlamacılara müşteri memnuniyeti sağlamalarında yol gösterici olan ve işletmelerin post-cookie ekonomisinde sürdürülebilirliklerini sağlamalarında yardımcı olabilecek politika önerileri sunulmuştur. Öyle ki literatürde, üçüncü taraf çerezlerden zero-party data'ya uzanan sürecin entelektüel gelişim yapısının bütüncül olarak incelendiği bir çalışmaya rastlanılmamıştır. Bu kapsamda çalışmanın üç temel araştırma sorusu bulunmaktadır. Bunlar;

a) Dijital gizlilik literatürünün son 30 yılı nasıl bir evrim geçirmiştir?

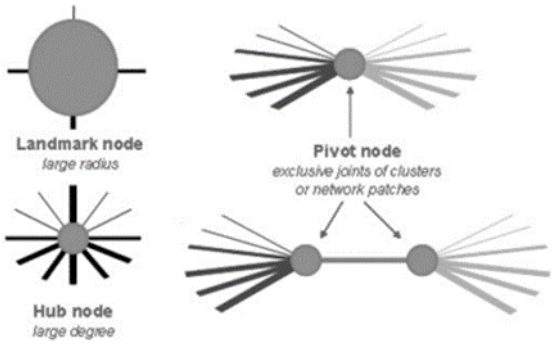
b) Zero-Party Data, dijital gizlilik literatürü evriminin neresindedir?

c) Yapay zeka destekli zero-party data müşteri güveni ve dijital gizlilik algısını nasıl dönüştürmektedir?

Çalışmanın amacı ve araştırma soruları kapsamında Web of Science (WoS) bibliyografik veri tabanından elde edilen veriler CiteSpace bilimsel haritalama programıyla ayrıntılı olarak analiz edilmiştir. 03/03/2026 tarihinde WoS bibliyografik veri tabanında "zero-party data", "artificial intelligence", "customer trust", "digital marketing", "data ethics", "privacy preserving", "cookie-less" ve "data privacy" anahtar kelimeleri yazılarak yapılan advanced research sonrasında bu konularda 1999-2026 yılları arasında yazılmış 1455 adet bilimsel esere erişilmiştir. CiteSpace bilimsel haritalama programında veri setinin analize uygun hale getirilmesi aşamasında tekrarlı olan yayınlar elenmiş olup alana ilişkin 1309 adet bilimsel eser, bu eserlerin yayımlandığı 814 adet dergi, yayınlara katkıda bulunan 4318 yazar, bu yazarların görev yaptıkları 3444 adet kurum ve yazarların menşei olduğu 363 adet ülkeden oluşan veri seti elde edilmiştir. Dolayısıyla yaklaşık olarak son 30 yılda tüketici verilerinin gizliliğini konu alan uluslararası düzeyde bilimsel olarak nitelikli dergilerde bin adetten fazla bilimsel eserin üretildiği söylenebilir. İşletmelerin tüketicileri hakkında veri toplama yöntemlerinde son zamanlarda yaşanan evrim, tüketici mahremiyeti, gönüllü ifşa, şeffaflık, ikna vb. konuların tartışılmaya başlandığı ve tüketici verilerinin toplanmasındaki güç dengesinin işletmelerden tüketicilere geçtiği bir dönemi başlatmıştır. Bu anlamda gerçekleştirilen bilimsel eserlerin ortak

atıf performansı, atıf patlaması, disiplinlerarası etkileşim, merkeziyetlik ve konunun yıllar içerisinde nasıl evrildiği kapsamında ayrıntılı olarak analiz edilmesi amacıyla CiteSpace bilimsel haritalama programından yararlanılmıştır.

CiteSpace, akademik literatürün organizasyonel ve kronolojik değişimlerini saptamada kullanılan temel yazılımların başında gelmektedir. Bu aracın sunduğu yetenekler; çalışma alanlarındaki ilerleme rotalarının, mühim kavramların, yazarların ortaklık yapılarının ve atıf sistemlerinin şematik gösterimine imkan verir. Bu çerçevede, CiteSpace aracılığıyla gerçekleştirilen bibliyometrik tetkikler, disiplinlerarası çalışmalar adına kuvvetli bir yöntemsel zemin hazırlamaktadır. Yazılımın ana hedefi, akademik külliyatın görselleştirilmesi ve sayısal incelenmesi vasıtasıyla belli bir branşın düzenini çözümlemektir. Bilim insanlarına, süratle evrilen sahalardaki kritik verileri ve akımları takip etmeleri amacıyla yetkin bir düzenek sunar. Bir çalışma konusunun literatürünü görsel-analitik yöntemle tetkik etmek üzere kurgulanmıştır. Kaynakça verilerini girdi kabul ederek, uzmanlık alanının düşünsel formunu sentezlenmiş ağ yapıları şeklinde modeller. Yeni trendlerin saptanmasında ve ani kopuşların teşhisinde mühim metodolojik faydalar sağlar. Mesela, bir branştaki "en yeni" odak noktalarını tayin eder. Bu süreçte ortak atıf haritalarından faydalanır (Chen, 2006; Chen, 2020). Şematize edilmiş bir sistemde dönüm noktası, merkez ve pivot düğümleri yer alır. Bu düğümler, bilgi kümesindeki temel makalelerin bulunmasını kolaylaştırır. Haritalandırılmış ağdaki düğüm çeşitleri aşağıda sunulmuştur (Chen, 2004).



Şekil 1: Görsel Ağ Düğümleri

Kaynak: Chen, 2004.

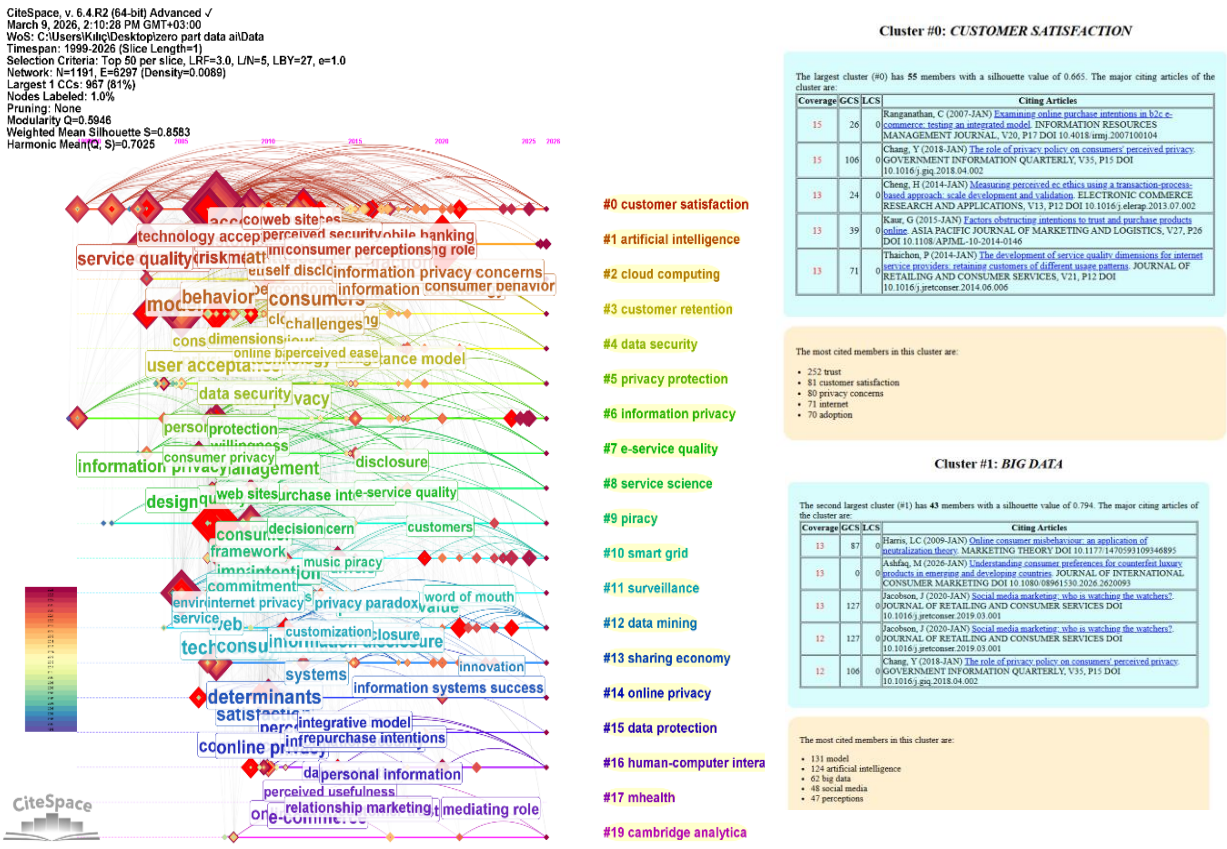
Dönüm noktası düğümleri (Landmark node), yoğun şekilde atıf alan ve kendi branşına mühim değerler katarak geniş yankı uyandıran eserleri içerir. Merkez düğümler (Hub node) ise göreceli olarak değerli katkılar sunan yayınların bulunduğu kısımdır. Bu düğümdeki çalışmalar, dahil oldukları akademik sahaya ciddi fikri katkılar sağlama kapasitesine sahip metinlerdir. Bu eserler, ağ yapısı içerisinde yüksek derecede bağlantısallık merkeziyeti sergilerler. Diğer noktaları birbirine kenetleyen geçiş yollarının tam ortasında konumlanırlar. Genellikle yapısal boşluklarda yer alan bu makaleler; yaratıcılık, özgünlük ve farklı disiplinler arasında köprü kurma yetisi taşırlar. Pivot düğümleri (Pivot node) ise ayrı ağ yapıları arasındaki temas noktalarını temsil ederler. Aracılık merkeziyeti skorları yüksek olan bu unsurlar, iki ağın paylaştığı ortak noktalar veya bağlantı sağlayan birer geçit işlevi görürler. Bilimsel gelişim sürecindeki paradigma değişimlerinin veya düşünsel geçiş evrelerinin muhtemel işaretçileri olarak tanımlanabilirler. CiteSpace görsellerinde bu pivot noktalar çoğunlukla mor bir çemberle işaretlenir. Bu sayede, görsel analizlerde dikkat çekerek araştırmacıların zihinsel yükünü hafifletir ve incelenecek yayın sayısının sınırlandırılmasına yardım ederler. İşlevsel olarak merkez düğümlere benzeseler de, özellikle iki ayrı küme arasındaki geçişi temsil eden çalışmalar burada konumlanır (Chen, 2004; Chen vd., 2010).

3. CiteSpace Ağ Haritalama Analizleri

Bu bölümde dijital gizlilik literatürüne ilişkin anahtar kelime ve yazar ağ analizleri yer almaktadır.

3.1 Anahtar Kelime Ağ Haritası

Geçtiğimiz son yirmi yılda tüketici verilerinin izlenmesine ilişkin yöntemlerin tartışıldığı bilimsel eserlerde kullanılan anahtar kelimelerin CiteSpace bilimsel haritalama programı aracılığıyla gerçekleştirilmiş olan ağ haritası Şekil 2'de görülmektedir. 1999-2026 yılları arasında gerçekleştirilen bilimsel eserlerde toplam 1191 anahtar kelimenin yer aldığı ve bu bilimsel eserler arasında toplam 6297 adet ortak atıf ağının bulunduğu söylenebilir. Bu ortak atıf ağı "Zero-Party Data" ve "Dijital Gizlilik" etrafında yapılanmaktadır. Ağda 20 küme bulunmaktadır. Bu kümelerin topluluk yapısı (community structure) geçerliliği, Modularity (Q) ve Silhouette (S) değerlerine göre belirlenmektedir. Analizlerde $Q > 0,3$ değeri, kelime ağının anlamlı bir kümelenme yapısına sahip olduğunu ifade etmektedir. Bu değer literatürün yüksek yapısal ayrışmaya sahip olup olmadığının değerlendirilmesinde kullanılır. Silhouette (S) değeri ise, küme içerisindeki düğümlerin birbirleriyle benzerlik düzeyinin tespit edilmesini sağlamaktadır. Bu değer, kümelerin kendi içindeki tutarlılık düzeyinin değerlendirilmesinde kullanılmaktadır. Çalışmadaki kelime ağ analizinde Q değeri 0,5946, S değeri ise 0,8497 olarak hesaplanmıştır. Her iki değerin harmonic mean (Q, S) değeri ise 0,6996'dır. Bu durumda, kelime ağ analizinin kümelenme yapısının anlamlı olduğu ve kümelerin kendi içindeki homojenliğinin ise yüksek olduğu söylenebilir. Ayrıca anahtar kelime ağının yoğunluk değeri (density) 0,0089 olarak hesaplanmıştır. Density, anahtar kelime ağındaki bağlantıların birbirlerine ne kadar sıkı tutunduğunun göstergesidir. Çalışmadaki anahtar kelime ağ analizinin yoğunluk değeri düşüktür. Bu durumda, dijital gizlilik konusunda yapılan bilimsel eserlerin disiplinlerarası bir özellik taşıdığını, yeni makalelerin eski klasik makalelerle yoğun bir ağ oluşturamadığını, dolayısıyla da akademik olgunluk düzeyinin düşük yani, yeni ve keşfedilmemiş bir alanı temsil ettiğini söylemek mümkündür.



ClusterID	Size	Silhouette	Label (LSI)	Label (LLR)	Label (MI)	Average Year
0	55	0.665	multi-group analysis	customer satisfaction (511.49, 1.0E-4)	regulatory environment (2.55)	2015
1	43	0.794	examining factor	big data (453.8, 1.0E-4)	regulatory environment (2.18)	2014
2	31	0.86	designing monitoring system	cloud computing (538.52, 1.0E-4)	hybrid approach (0.43)	2014
3	30	0.82	social networking site	online banking (180.31, 1.0E-4)	regulatory environment (0.65)	2015
6	25	0.842	digital marketing	virtual reality retail (154.75, 1.0E-4)	regulatory environment (0.18)	2015
10	22	0.876	designing monitoring system	smart grid (257.21, 1.0E-4)	regulatory environment (0.13)	2019
5	20	0.892	uncovering sociotechnical tradeoff	recommender systems research (87.29, 1.0E-4)	social media privacy policies (0.02)	2013
11	20	0.914	measuring user	online information disclosure (129.58, 1.0E-4)	wallet adoption (0.34)	2011
4	18	0.969	lifelong policy carrying	privacy-preserving coalition loyalty program (212.34, 1.0E-4)	enabling information confidentiality (0.04)	2015
9	18	0.904	affecting online privacy concern	digital piracy behaviour (155.92, 1.0E-4)	person-specific information (0.47)	2014
13	15	0.884	measuring user	understanding adoption (126.37, 1.0E-4)	monitoring customer relationship (0.19)	2018
15	15	0.905	permissioned blockchain	online survey (89.88, 1.0E-4)	customer satisfaction (0.01)	2016
7	14	0.92	examining online purchase intention	trust violation (87.63, 1.0E-4)	security-related antecedent (0.04)	2013
8	13	0.892	haptic platform	website audience (96.59, 1.0E-4)	haptic platform (0.02)	2016
12	13	0.957	online recommendation setting	online recommendation setting (122.71, 1.0E-4)	topics methodological approaches data (0.03)	2021
14	12	0.936	examining factor	information security failure (130.78, 1.0E-4)	regulatory environment (0.18)	2015
16	11	0.915	digital payment service	signaling theory perspective (106.45, 1.0E-4)	regulatory environment (0.06)	2016
19	5	0.99	non-financial disclosure	analytica breach (52.84, 1.0E-4)	customer satisfaction (0.01)	2018
17	3	0.999	digital health app development standard	health information (33.22, 1.0E-4)	customer satisfaction (0.01)	2018
23	2	0.998	anonymous single-sign-on for n designated services with traceability	traceability (19.18, 1.0E-4)	customer satisfaction (0.01)	2018

Şekil 2: Anahtar Kelime Ağ Analizi

Kaynak: CiteSpace, 2026.

Şekil 2'de yer alan "#0 customer satisfaction" kümesinde en yüksek ortak atıf sayısına sahip 5 anahtar kelime sırasıyla " 252 trust", "81 customer satisfaction", "80 privacy concerns", "71 internet" ve "70 adoption" dır. Bu kümede yer alan yayınlarda en fazla ortak kullanıma sahip "trust" kelimesi, dijital pazarlama ve e ticaret alanında dijital gizlilik eksenindeki entelektüel gelişimin "trust" kavramı etrafında şekillendiğini, tüketicilerin pasif izlenmesinden ziyade gönüllü ifşaya geçiş sürecinde bu kavramın kilit unsur olduğunu ifade etmektedir. Öyle ki "trust" gönüllü ifşa eyleminin psikolojik sözleşmesini temsil etmektedir. Tüketicilerin gönüllü veri paylaşımlarında güvenin ön koşul olduğu kümenin hacminden ve atıf yoğunluğundan anlaşılmaktadır. Şekil 2'de yer alan "#1 big data" kümesinde en yüksek ortak atıf sayısına sahip ilk üç anahtar kelime "131 model" , "124 artificial intelligence" ve "62 big data"dır. Bu küme teknik ve yıkıcı trendlerin bulunduğu bir kümedir. Bu durum, dijital pazarlamanın sadece reklam, görsel ve metinlerden ibaret olmadığını, aynı zamanda veri işleme

kapasitesine de sahip olduğunu ifade eder. Dijital gizlilik verilerinin işlenmesi için gerekli teknik altyapılar bu kümede yer alan yayınların ortak tartışma konusudur.

Şekil 2'de yer alan 20 kümenin atıf sayıları (citiation counts), atıf patlamaları (bursts), bağlantısallık ve etki gücü (degree), aracılık merkeziliği (centrality) ve sigma analizine ilişkin veriler aşağıdaki tabloda yer almaktadır:

Tablo 2: Küme Analiz Değerleri

Citation Counts	Node Name	DOI	Cluster ID
252	trust		0
131	model		1
124	artificial intelligence		1
123	impact		9
111	privacy		3
95	technology		11
81	customer satisfaction		0
80	privacy concerns		0
71	internet		0
70	adoption		0

Bursts	Node Name	DOI	Cluster ID
35.45	artificial intelligence		1
8.63	cloud computing		2
7.79	impact		9
6.98	framework		9
6.52	digital marketing		1
6.33	machine learning		2
6.28	perceived risk		14
5.67	ethics		1
5.54	corporate social responsibility		6
5.52	user acceptance		3

Degree	Node Name	DOI	Cluster ID
107	model		1
93	technology		11
92	antecedents		0
92	determinants		13
91	consumers		1
88	consumer trust		11
86	behavior		1
82	acceptance		0
82	e commerce		0
79	customer satisfaction		0

Centrality	Node Name	DOI	Cluster ID
0.00	model		1
0.00	technology		11
0.00	antecedents		0
0.00	determinants		13
0.00	consumers		1
0.00	consumer trust		11
0.00	behavior		1
0.00	acceptance		0
0.00	e commerce		0
0.00	customer satisfaction		0

Sigma	Node Name	DOI	Cluster ID
1.00	model		1
1.00	technology		11
1.00	antecedents		0
1.00	determinants		13
1.00	consumers		1
1.00	consumer trust		11
1.00	behavior		1
1.00	acceptance		0
1.00	e commerce		0
1.00	customer satisfaction		0

Kaynak: CiteSpace, 2026.

Tablo 2'deki *citiation counts*, bir kavramın literatürde ne kadar kabul gördüğünü ifade etmektedir. "Trust" kavramı 252 adet atıf sayısıyla dijital gizlilik konusunda yapılan araştırmaların temel dayanağını oluşturmaktadır. Benzer şekilde "model-131 adet atıf", "artificial intelligence-124 adet atıf", "privacy-111 adet atıf", "customer satisfaction-81 adet atıf" ve "privacy concerns-80 adet atıf" kavramları dijital gizlilik konusunda alanın en büyük tartışma konularını oluşturmaktadırlar.

Bursts, trend olan ve odak noktası haline gelen güncel konuları içermektedir. Bursts tablosunda yer alan anahtar kelimeler atıf patlaması yaşayan ve odak noktası haline gelen yayınlarda en sık tercih edilen anahtar kelimeleri ifade etmektedir. "artificial intellgence-35,45" dijital gizlilik konusundaki literatürü domine eden büyük bir kırılma noktasıdır. "cloud computing-8,63" ve "machine learning-6,33", dijital gizlilik konusunda ilginin geleneksel pazarlama modellerinden teknoloji odaklı tahmine dayalı modellere kaydığını ifade etmektedir. Öyle ki "post-cookie" ekonomisiyle birlikte işletmelerin sürdürülebilirliğinde verileri sadece toplamak değil yapay zeka araçlarıyla anlamlandırabilecek bulut tabanlı bir mimariye sahip olmak giderek önemli hale gelmektedir. Bununla birlikte bursts tablosunda yer alan "ethics-5,67" kelimesi, yapay zekayla birlikte dijital gizlilik literatüründe etik konuların da tartışılmaya başlandığının göstergesidir.

Degree, ağdaki bir kavramın, ağdaki diğer kaç kavramla bağlantılı olduğunu, diğer bir ifadeyle etki gücünü ve ne kadar merkezi olduğunu ölçmeye yaramaktadır. Bu anlamda "model-107", "technology-93" ve "antecedents-92" düğümleri, dijital gizlilik literatüründeki hemen

hemen tüm çalışmaların bu üç kavramın etrafında döndüğünü ve araştırmacıların tüketici davranışlarını açıklamak amacıyla bu üç kavramda yoğun şekilde yararlandıklarını ifade etmektedir.

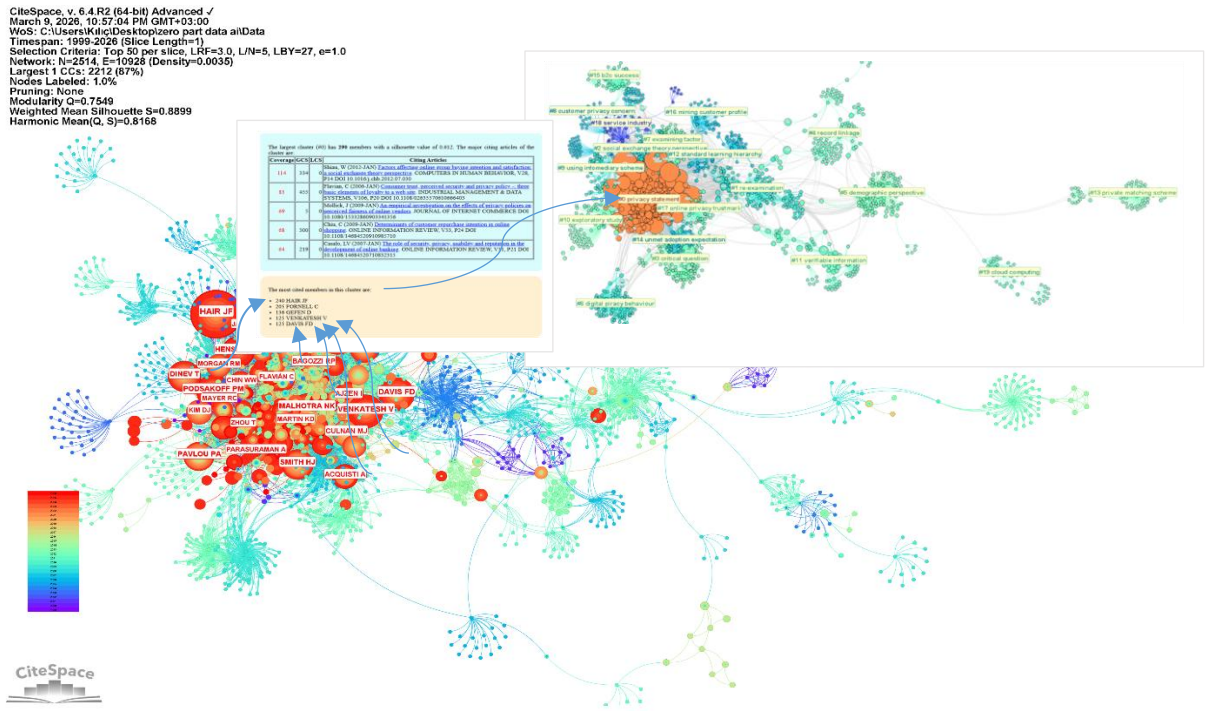
Centrality, bilgi köprüsü anlamına gelen, bir düğümün ilgili literatürün farklı bölümleri arasında bir köprü olup olmadığını belirlemeye yarayan bir değerdir. Tabloda yer alan merkezilik skorlarının 0,00 olması, ağın ana omurgasını oluşturan anahtar kelimeleri ifade etmektedir. Bu anlamda "model, technology, antecedents, determinants, consumers, consumer trust, behavior, acceptance, e-commerce ve customer satisfaction" anahtar kelimeleri dijital gizlilik literatürüne ilişkin çalışmalarda merkezi kavramlar olarak alanın temel yapı taşlarıdır. Dijital gizlilik literatürünün entelektüel eğilim yapısının gelişimine yön veren ve alanlar arası köprü görevi gören en temel kavramlardır.

Tablo 2'de yer alan *Sigma* değeri, bir düğümün hem köprü olma yani aracılık gücünü hem de atıf hızını yani hızlı yükselişini ifade etmektedir. Sigma değeri 1.0 ve üzerinde olan düğümler literatürdeki geçiş kapılarıdır. Anahtar kelime ağ analizinde 1.0 değerine sahip anahtar kelimeler arasında "model, technology, antecedents, determinants, consumers, consumer trust, behavior, acceptance, e-commerce ve customer satisfaction" yer almaktadır. Bu anahtar kelimelere ait düğümlerin dijital gizlilik konusunda hem teknik hem de güven odaklı alanları birleştiren disiplinlerarası bir köprü görevi gördüğü söylenebilir.

Şekil 2 ve Tablo 2 de yer alan veriler birlikte değerlendirildiğinde, dijital gizlilik alanına ilişkin literatürün, entelektüel eğilim yapısının merkezinde "güven"in yer aldığı söylenebilir. Tüketicilerin üçüncü taraf çerezler yoluyla izlenmesinden gönüllü ifşaya geçildiği dönemde "güven", Zero-Party Data sayesinde gizlilik endişesinin azalmasına aracılık etmektedir.

3.2. Yazar Ağ Analizi

Tüketici verilerinin izlenmesi ve dijital gizlilik konusunda yapılan bilimsel eserlerin yazarlarına ilişkin ağ analizinde 2 bin 514 yazar ve bu yazarların yayınları arasında 10 bin 928 adet ortak atıf ağı olduğu belirlenmiştir. Yazarların üretmiş olduğu bilimsel eserler kapsamında analizde 30 farklı çalışma kümesi bulunmaktadır. Bunlar arasında Label (Latent Semantic Indexing-LSI) başlığı altında yer alan "privacy statement" anahtar kelimesi 290 adet bilimsel eserde ortak anahtar kelime olarak kullanılmış olup bu yayınların birbirleriyle benzerlik ve tutarlılık düzeyi Silhouette 0,612 oranıyla oldukça iyidir. #0 privacy statement kümesinde yer alan bilimsel eserler en yüksek ortak atıf sayısına sahiptir ve bu eserlerde ortak kullanılan anahtar kelime "privacy statement"dır. Bu kümede yer alan bilimsel eserler ortak atıf ağının en yüksek atıf sayısına sahip olmakla birlikte dijital gizlilik literatürüne yön veren dönüm noktası niteliğindeki bilimsel eserlerdir. Düğümlerin büyüklükleri ilgili bilimsel çalışmalara yapılan atıf sayısıyla doğru orantılıdır. Atıf sayısı ne kadar yüksekse düğümler de o kadar büyüktür. Şekil 3'de bu durum görülmektedir:



ClusterID	Size	Silhouette	Label (LSI)	Label (LLR)	Label (MI)	Average Year
0	290	0.612	privacy statement	electric vehicle (174.81, 1.0E-4)	municipal service (8.5)	2020
1	165	0.847	re-examination	digital right (51.86, 1.0E-4)	affecting online buying decision (0.02)	2020
2	137	0.702	re-examination	security privacy usability (69.59, 1.0E-4)	smartphone banking service (0.03)	2020
3	126	0.899	critical question	contemporary issue (211.89, 1.0E-4)	litigation intention (0.11)	2020
4	121	0.957	record linkage	data privacy policies (120.18, 1.0E-4)	practical secure computation (0.05)	2020
5	119	0.97	demographic perspective	computational complexity (88.71, 1.0E-4)	municipal service (0.03)	2020
6	110	0.982	digital piracy behaviour	predictors moderator (13.25, 0.001)	empirical study (0.02)	2020
7	94	0.948	re-examination	social exchange theory perspective (121.72, 1.0E-4)	cognitive attitude (0.14)	2020
8	84	0.992	customer privacy concern	customer trust (14.26, 0.001)	empirical study (0.02)	2020
9	83	0.924	using infomediary scheme	privacy policies (70.07, 1.0E-4)	empirical study (0.01)	2020
10	82	0.971	exploratory study	buying behavior (57.15, 1.0E-4)	empirical study (0.01)	2020
11	82	0.964	verifiable information	electric vehicle (200.72, 1.0E-4)	social connection (0.06)	2020
12	78	0.897	standard learning hierarchy	e-trustin online loyalty development (41.84, 1.0E-4)	empirical study (0.01)	2020
13	64	1	private matching scheme	sensitive customer data (27.8, 1.0E-4)	empirical study (0.02)	2020
14	60	0.967	unmet adoption expectation	e-marketplace failure (54.72, 1.0E-4)	empirical study (0.01)	2020
15	60	0.959	b2c success	digital scholarship (42.67, 1.0E-4)	empirical study (0.02)	2020
16	57	0.995	mining customer profile	role (23.31, 1.0E-4)	empirical study (0.02)	2020
17	51	0.95	online privacy trustmark	digital advertising (125.31, 1.0E-4)	moderated-moderation model (0.07)	2020
18	48	0.957	service industry	conducting e-business (47.4, 1.0E-4)	empirical study (0.02)	2020
19	46	1	cloud computing	sticky policies (60.76, 1.0E-4)	empirical study (0.02)	2020
20	43	0.869	secondary use	customer trust (126.21, 1.0E-4)	influencing internet banking adoption (0.02)	2020
21	37	0.989	key stakeholder	privacy-preserving data dissemination (56.92, 1.0E-4)	empirical study (0.02)	2020
22	33	1	permissioned blockchain	professional ethics (70.25, 1.0E-4)	empirical study (0.02)	2020
23	31	1	strategic and ethical considerations in managing digital privacy	managing digital privacy (17.06, 1.0E-4)	empirical study (0.02)	2020
24	24	0.981	it security and privacy issues in global financial services institutions: do socio-economic and cultural factors matter?	global financial services institution (18.1, 1.0E-4)	empirical study (0.02)	2020
25	22	1	barriers and solutions of e-commerce in china: an exploratory study	china (17.6, 1.0E-4)	empirical study (0.02)	2020
26	21	0.993	ai-powered personalised recommendation	social network data trustworthiness (172.09, 1.0E-4)	unpacking customer experience (0.02)	2020
28	17	1	a proposed model of customer e-loyalty measurement in internet banking	customer e-loyalty measurement (16.01, 1.0E-4)	empirical study (0.02)	2020
30	14	0.991	future agenda	bibliometric-systematic review (244.58, 1.0E-4)	young consumers behaviour (0.04)	2020
31	13	1	customer satisfaction in municipal services: an empirical study in majlis perbandaran sungai petani (mpspk)	municipal service (17.6, 1.0E-4)	empirical study (0.02)	2020

Şekil 3: Yazar Ağ Haritası

Kaynak: CiteSpace, 2026.

Şekil 3'de en yüksek atıf sayısına sahip yayın J.E. Hair, R.E. Anderson ve R.I., Tatham tarafından 1987 yılında yayımlanan "Multivariate Data Analysis with Readings" başlıklı kitaptır. Bu kitap, 240 adet bilimsel eserden toplam 8 bin 444 adet ortak atıf almıştır. Kitap, dijital gizlilik konusunda yapılan model esaslı ve saha araştırmalarına dair bilimsel çalışmalar tarafından sıklıkla kullanılan önemli bir referans kaynağıdır. Hair ve arkadaşlarının (1987) kitabına atıfta bulunan ve en yüksek ortak atıf alan bilimsel eser Mary J. Culnan ve Pamela K. Armstrong tarafından 1997 yılında Organization Science dergisinde yayımlanmış olan "Information privacy concerns, procedural fairness and impersonal trust: An empirical investigation" başlıklı eserdir. Çalışmada, 1000 adet rastgele seçilen 18 yaş ve üzeri Amerikalı tüketicinin kişisel bilgilerinin toplanması ve kullanılması ile gizlilik arasında ortaya çıkan endişe ve gerilimleri incelenmiştir. Yazarlar, günümüz elektronik dünyasında firmaların rekabet stratejilerini geliştirirken müşteri verilerine ihtiyaç duyduklarını ancak buna karşılık

tüketicilerin paylaştıkları verileri konusunda gizlilik endişelerinin bulunduğunu ifade etmektedirler. Yazarlara göre, işletmeler bireysel gizliliği korumak için adil prosedürler uyguladıklarında müşteriler kişisel bilgilerini ifşa etmeye ve bu bilgilerin daha sonra iş amaçlı tüketici profilleri oluşturmak için kullanılmasına izin vereceklerdir. Çalışmada müşterilere adil bilgi uygulamalarının kullanıldığı açıkça söylendiğinde, profillerinin oluşturulmasını isteyen ve istemeyen tüketicilerin gizlilik endişeleri arasında fark olmadığı belirlenmiştir. Öyle ki gizlilik konusunda önceki yıllarda yapılan bazı araştırmalarda (Laufer ve Wolfe, 1977; Milne ve Gordan, 1993; Stone ve Stone, 1990), bireylerin kişisel bilgilerini, - kişisel bilgilerinin daha sonra adil bir şekilde kullanılacağı ve olumsuz sonuçlara maruz kalmayacakları - yönünde açıklama yapılarak bazı ekonomik veya sosyal faydalar sunulduğunda ifşa etmeye istekli olduklarına dair bulguların elde edildiği vurgulanmaktadır (Culnan ve Armstrong, 1999). Geçen yaklaşık 25 yılda tüketici verilerinin internet teknolojisindeki gelişmelere bağlı olarak çerezler aracılığıyla toplandığı ve yorumlandığı bir dünyadan kişisel verilerin korunmasına ilişkin yasal düzenlemeler neticesinde doğrudan müşterilerden toplandığı Zero-Party Data yönteminin tartışıldığı bir dünyaya gelinmiştir. Arada geçen sürede 1990'lı yıllarda tartışılan ve doğruluğu kanıtlanan veri toplama yöntemine geri dönülmüş olması ise, işletmelerin veri toplama yöntemlerinde açık ve şeffaf olmalarının müşteri güveni yaratılmasında ve dolayısıyla da müşteri sadakatinin sağlanarak verilerini ifşa etme konusunda istekli müşteri portföyüne sahip olunmasında ne kadar önemli olduğunu kanıtlar niteliktedir.

Şekil 3'te yer alan ikinci en yüksek atıf sayısına sahip yayın Cales Fornell ve David F. Larcker tarafından Journal of Marketing Research dergisinde 1981 yılında yayımlanmış olan "Evaluating structural equation models with unobservable variables and measurement error" başlıklı eserdir. Bu eser 205 adet bilimsel eserden toplam 8 bin 619 adet ortak atıf almıştır. Eser dijital gizlilik konusunda gerçekleştirilen niceliksel ve model esaslı pek çok çalışma tarafından sıklıkla atıf alan bir referans kaynağıdır. Fornell ve Larcker (1981)'ın bilimsel çalışmasına atıfta bulunan ve en yüksek atıf sayısına sahip bilimsel eser 2015 yılında Alizabeth Aguirre, Dominik Mahr, Dhruv Grewal, Ko de Ruyter ve Martin Wetzels tarafından Journal of Retailing dergisinde yayımlanan "Unraveling the personalization paradox: The effect of information collection and trust-building strategies on online advertisement effectiveness" başlıklı çalışmadır.

Çalışmada, perakendecilerin müşteri verilerini açık ve gizli olarak toplamalarına karşılık müşterilerin nasıl tepki verdikleri incelenmiştir. Yazarlar, perakendeciler tarafından sunulan kişiselleştirilmiş hizmet düzeyi arttıkça, hizmetin müşterilerle alaka düzeyinin ve müşterilerin bu hizmetleri benimseme düzeylerinin arttığını ifade etmektedirler. Ancak perakendecilerin müşterilerin çevrimiçi davranışları hakkında çerezler aracılığıyla bilgi toplayarak daha fazla kişiselleştirme sağlamaları, müşterilerin savunmasızlık hislerini arttırmakta, paradoksal olarak her ne kadar hizmet müşterilerle alakalı olsa da benimsenme düzeylerini düşürebilmektedir. Bu nedenle müşterilere yönelik kişiselleştirilmiş hizmetler için veriler rızaları alınmadan toplandığında ve müşteriler bunu fark ettiklerinde hizmeti almaktan vazgeçmektedirler. Yazarlar, perakendecilerin sosyal medya sitelerinden açıkça bilgi topladıklarında müşterilerin hizmeti benimseme düzeylerinin arttığını, ancak gizli bilgi topladıklarında ise savunmasızlık duygularının müşterilerin benimseme düzeylerinde kırılganlıklara neden olduğunu iddia etmektedirler. Çalışma, bilgi toplamanın rolünü ve bunun kırılganlık oranları üzerindeki etkisini açıklayarak kişiselleştirme-gizlilik paradoksunu dengelemeye yardımcı olacak öneriler sunmaktadır (Aguirre vd., 2015). Dolayısıyla müşterilere ilişkin verilerin ikinci taraf veya üçüncü taraf çerezler aracılığıyla toplanmasının müşteri memnuniyetini arttırmaktan ziyade gizlilikten endişe eden ve kendini savunmasız hisseden müşteriler yarattığı söylenebilir. Kişisel verilerin korunmasına ilişkin tüm dünyada yürürlükte olan ve düzenleme aşamasında olan

yasalar dolayısıyla işletmelerin açık, şeffaf ve dürüst olarak müşterileriyle iletişim kurmaları, onlardan doğrudan ve güvenilir bilgi edinilmesini sağlayacaktır.

Bununla birlikte yapay zeka destekli Zero-Party Data, tüketicilerin bir yandan kişiselleştirilmiş hizmet beklemeleri diğer yandan ise gizlilik endişesi duymaları olarak ifade edilen "kişiselleştirme paradoksu"na da çözüm sunmaktadır. Yapay Zeka Destekli Zero-Party Data'da yapay zeka, gizliliği ihlal etmeden bilgi edinme imkanı sağlayabilmektedir. Öyle ki, yapay zeka sohbet robotları, kişiselleştirilmiş öneri motorları ve etkileşimli quizler aracılığıyla tüketicileri yormadan, zahmetsiz, aksine keyifli bir deneyim sunarak tüketici gizlilik hakları ihlal edilmeksizin gönüllülük esasına dayalı olarak müşteri verileri toplanabilmektedir. Toplanan bu verilerin analizi de yapay zeka sayesinde daha hızlı, daha akıllı ve daha az müdahaleci hale getirilmektedir. Böylece, veri toplama sürecinin daha akıcı hale gelmesi sağlanmaktadır. CiteSpace bilimsel haritalama programı aracılığıyla yapılan analizlerde dijital gizlilik konusunda yapılan yayınlar arasında atıf patlaması en yüksek olan çalışmalarda yapay zeka anahtar kelimesinin 35,45 atıf patlaması değerine sahip olduğu, dolayısıyla da literatürdeki dijital gizlilik tartışmalarına yön verdiği söylenebilir. Bu anlamda dijital gizlilik literatüründe ilginin geleneksel pazarlama modellerinden teknoloji odaklı tahmine dayalı modellere kaydığı da ifade edilebilir. CiteSpace analizinde benzer şekilde güven kavramı en merkezi düğüm olarak öne çıkmaktadır. Analizlerde güven, yapay zekanın etik bir çerçevede veriyi işlemesiyle desteklendiğinde, markalar ve tüketiciler arasındaki şeffaflık ve dürüstlük ilkeleri ekseninde sürdürülebilir müşteri sadakatinin yaratılmasının anahtarı olarak ön plana çıkmaktadır. Bu bağlamda, yapay zeka destekli Zero-Party Data yaklaşımının kişiselleştirme ile gizlilik arasındaki dengeyi sağlamada önemli bir stratejik araç olarak öne çıktığı söylenebilir.

4. Kişiselleştirme – Gizlilik Paradoksundaki Denge Kurucu: Yapay Zeka Destekli Zero-Party Data

Günümüz tüketicilerinin "sürekli çevrimiçi – always-on" olma durumu, teknolojinin ve özellikle mobil cihazların yaygınlaşmasıyla birlikte bir yaşam biçimi haline gelmiştir (Iucolano, 2019). Tüketicilerin bu sürekli çevrimiçi olma durumu literatürde hiperbağlantılılık olarak kavramsallaştırılmış olup, tüketicilerin markalar, perakendeciler ve birbirleriyle gerçek zamanlı, dinamik etkileşimler kurmasını ifade etmektedir (Quan-Haase ve Wellman, 2005; Wellman, 2001). Öyle ki dünya genelinde akıllı telefon sevkiyatları 2025 yılında bir önceki yıla göre %1,9 oranında artarak 1,26 milyar adede ulaşmıştır (Elagina, 2026). Tüketiciler, mobil cihazlarda geçirdikleri zamanın büyük çoğunluğunu web tarayıcılarında değil, mobil uygulamalarda harcamaktadırlar. 2025 yılında yapılan bir araştırmada, tüketicilerin günde ortalama 6 saatini dijital medya ve eğlenceye ayırdıkları belirlenmiştir. Z kuşağının %56'sı ve Y kuşağının %43'ü, sosyal medya içeriklerini geleneksel TV programlarına ve filmlere tercih etmektedirler. Medya tüketim alışkanlıklarındaki köklü değişiklikler ve dijital harcamalardaki artışla birlikte özellikle Üretken Yapay Zeka (Gen AI) kullanımı da giderek yaygınlaşmıştır. Tüketicilerin %53'ü 2025 yılı verilerine göre Gen AI araçlarını denemekte veya düzenli kullanmaktadırlar. Bu oran 2024 yılında %38 düzeyindeydi. Düzenli kullanıcı oranı ise geçen yıla göre iki katı artarak %20'ye ulaşmıştır. Gen AI kullanıcılarının %51'i bu araçları her gün, %38'i ise haftada bir kez kullanmaktadırlar. Kullanıcıların %65'i bu araçlara telefonlarındaki bağımsız uygulamalar üzerinden, %60'ı ise web siteleri aracılığıyla erişmektedirler. Buna karşılık tüketicilerin yaklaşık %25'i alışveriş esnasında yapay zeka kullanırken dolandırıcılık riski konusunda endişe taşımaktadırlar. Veri gizliliği ve güvenliği konusunda endişe duyanların oranı ise 2025 yılında bir önceki yıla göre %60'tan %70'e çıkmıştır. Tüketiciler arasında teknoloji sağlayıcılarının verilerini güvende tutacağına "yüksek" düzeyde inananların oranı

sadece %27'dir (Widener vd., 2025; Fineberg vd., 2025). Bu veriler 2025 yılı itibariyle tüketicilerin mobil uygulamalar üzerinden sürekli çevrimiçi olduklarını, yapay zeka gibi inovasyonlara büyük ilgi gösterdiklerini ancak diğer yandan veri güvenliği ve gizlilik konularında giderek daha temkinli hale gelmeye başladıklarını ifade etmektedir.

Tüketicilerin sürekli çevrimiçi olma durumları, hem tüketiciler hem de pazarlamacılar açısından karmaşık bir "ver ve al" ikilemi yaratmaktadır (Verhoef vd., 2010). Bu durum her iki taraf için de hem büyük fırsatlar hem de yapısal riskler barındıran bir güç değişimi olarak değerlendirilebilir. Tüketiciler açısından değerlendirildiğinde sürekli çevrimiçi olma durumu, her şeyden önce güçlenme aracıdır. Tüketiciler bilgiye benzeri görülmemiş erişim, sayısız seçenek, kişiselleştirme fırsatları ve markalarla gerçek zamanlı etkileşim kurma yeteneği sayesinde kendilerini "altın çağda" hissetmektedirler (Dünya Ekonomik Forumu, 2017). Özellikle Gen AI gibi teknolojilerin yaygınlaşmasıyla tüketicilerin %53'ü bu araçları üretkenlik ve yaratıcılıklarını artırmak için kullanmaktadırlar (Fineberg vd., 2025). Ayrıca tüketicilerin %77'si sanal deneme, %76'sı ise yapay zeka destekli alışveriş asistanları gibi dijital kolaylıkları talep etmektedirler (Watty, 2025). Ancak sürekli çevrimiçi olma, beraberinde stres bilgi bombardımanı, teknoloji bağımlılığı ve mahremiyet kaybı gibi olumsuzlukları da getirmektedir (Anderson ve Rainie, 2017). Tüketicilerin %70'i veri gizliliği ve güvenliği konusunda ciddi endişeler taşımakta (Fineberg vd., 2025), bu da "kişiselleştirme-gizlilik paradoksu"nu derinleştirmektedir. Tüketiciler kişiselleştirilmiş hizmet beklerken, aynı zamanda verilerinin gizlice toplanmasından dolayı kendilerini savunmasız hissetmektedirler (Kutty vd., 2021; Aguirre vd., 2015).

Pazarlamacılar açısından ise sürekli çevrimiçi olma durumu, tüketici davranışlarını anlamak ve onlara ulaşmak için devasa bir veri havuzu anlamına gelmektedir. Öyle ki kişisel veriler dijital ekonominin "yeni petrolü" olarak görülmekte ve gelişmiş analitiki araçlar sayesinde markalar, müşteri deneyimini daha önce hiç olmadığı kadar geliştirebilmektedirler (Marketing Science Institute, 2014; World Economic Forum, 2011). Yapay zeka araçları, içerik üretimini hızlandırmakta ve reklam hedeflemesini daha isabetli hale getirmektedir. Özellikle Zero-Party Data stratejileri, çerezlerin kalktığı bir dünyada markaların tüketicilerle güvene dayalı ilişkiler kurmasını sağlamaktadır (Britt, 2020; Widener vd., 2025). Buna karşılık tüketicilerin sürekli çevrimiçi olma durumları arttıkça, teknoloji sağlayıcılarına duyulan güven de azalmaktadır. Tüketicilerin sadece %27'si verilerinin güvende olduğuna dair yüksek güven duymaktadırlar. Pazarlamacılar için asıl meydan okuma, sadece "hızlı yenilikçi" olmak değil, aynı zamanda veriyi şeffaf ve güvenli işleyen "güvenilir öncü" konumuna yükselebilmektir. Zira veriler güven ve şeffaflıkla birleştiğinde tüketicilerin harcama eğiliminde %62'ye varan bir artış görülmektedir (Fineberg vd., 2025).

Kişiselleştirme-Gizlilik paradoksu kısaca, tüketicilerin bir yandan kendilerine özel, alakalı ürün ve hizmetler talep ederken, diğer yandan bu kişiselleştirmeyi mümkün kılan veri toplama süreçlerine karşı derin bir şüphe ve savunmasızlık hissetmeleri durumu olarak tanımlanabilir (Kutty vd., 2021). Bu paradoksun aşılmasında yapay zeka destekli Zero-Party Data, dijital pazarlamanın yeni "altın standardı" olarak merkezi bir rol oynamaktadır (Braze, 2025). Yapay zeka destekli Zero-Party Data'nın bu dengeyi nasıl sağlayacağı ve bu sürecin nasıl hayata geçirilebileceği aşağıda ayrıntılı olarak tartışılmaktadır:

4.1. Zero-Party Data'nın Paradoksu Çözmedeki Rolü

Geleneksel veri toplama yöntemleri, üçüncü taraf çerezler gibi, genellikle tüketicinin bilgisi dışında veya pasif yöntemleri içerir. Bu da tüketicilerde "takip edilme" ve "gözetlenme

endişesi" yaratarak güveni zedeler (InMoment, 2018; Turow, 2017). Zero-Party Data ise tüketicinin gönüllü, proaktif ve bilinçli olarak paylaştığı verilerdir. Veriyi "izinsiz almak" yerine "istemeye" dayalı bir ekosistem yaratır. Tüketicilerin %70'inin veri gizliliği konusunda endişeli olduğu bir dönemde, bu yöntem güvenin psikolojik sözleşmesini temsil eder (Yun vd., 2020; Fineberg vd., 2025). Tüketiciler, daha iyi bir deneyim beklentisiyle bu bilgileri doğrudan verdikleri için verinin doğruluğu ve güvenilirliği en üst düzeydedir. Veriler gizlice değil, açık bir rıza ve adil bir değişim çerçevesinde toplandığı için tüketicilerin kendilerini savunmasız hissetme ihtimali de azalır (Aguirre vd., 2015).

4.2. Yapay Zekanın Paradoksu Çözümlemedeki Desteği

Yapay zeka, Zero-Party Data'nın toplanma ve işlenme sürecini daha akıllı, daha hızlı ve daha az müdahaleci hale getirerek kişiselleştirme-gizlilik paradoksunu dengeleyen bir ana mekanizma olduğu söylenebilir. Yapay zeka etkileşimli quizler, kişiselleştirilmiş öneri motorları ve sohbet robotları aracılığıyla tüketicileri yormadan, keyifli deneyimler sunarak verileri toplar. Konuya ilişkin yapılar araştırmalarda tüketicilerin %76'sının yapay zeka destekli alışveriş asistanlarını talep ettikleri belirlenmiştir (Watty, 2025). Yapay zeka aynı zamanda ham olan Zero-Party Data verilerini analiz ederek tüketicilerin o anki niyetlerini ve tercihlerini saniyeler içinde anlayabilmektedir. Bu sayede pazarlamacılar genel bir reklam yerine tüketicilerin tam o anda ihtiyaç duydukları anlamlı ve alakalı içeriği sunabilmektedirler (Fineberg vd., 2025). Bununla birlikte yapay zeka, etik bir çerçevede işletildiğinde, markaların tüketicilere dürüst ve şeffaf ilişkiler kurmasına da yardımcı olur.

4.3. Yapay Zeka Destekli Zero-Party Data Stratejileri

Kişiselleştirme ve gizlilik arasındaki dengeyi sağlamada yapay zeka destekli Zero-Party Data sürecinin aşağıda sıralanan stratejik adımları sunması önemlidir. Bunlar;

- "Değer Değişimi" Sunmak: Tüketiciler, kişisel bilgilerini genellikle indirim, kişiselleştirilmiş hizmet, zaman tasarrufu gibi faydalar karşılığında paylaşmaya isteklidirler. Bu nedenle işletmelerin verinin neden toplandığını ve karşılığında ne tür bir fayda sağlayacaklarını net bir şekilde açıklamaları önemlidir (Zhu vd., 2017; Fineberg vd., 2025).
- Güveni Bir" Ürün Özelliği" Haline Getirmek: Şeffaflık ve veri koruması sadece hukuki bir politika değil, ürünün ayrılmaz bir parçası olarak tasarlanmalıdır. Güvenilir Öncü olarak sınıflandırılan firmalar, yüksek inovasyonu güçlü bir veri sorumluluğu ile birleştirerek tüketici harcamalarını %62'ye kadar artırabilmektedirler (Fineberg vd., 2025).
- Tüketiciye Kontrol Vermek: Tüketicilerin kendi verilerini görme, silme ve paylaşım tercihlerini yönetme yetkisi olmalıdır. Veri üzerinde kontrol sahibi olduğunu hisseden tüketicilerin gizlilik endişeleri azalmaktadır (Dommeyer ve Gross, 2003; Fineberg vd., 2025).
- Yapay Zekayı Şeffaf Kullanmak: Yapay zekanın kararları açıklanabilir olmalıdır. Öyle ki yapılan çalışmalarda tüketicilerin %25'inin yapay zeka kullanımında dolandırıcılık endişesi taşıdığı unutulmamalıdır. Bu nedenle güvenlik önlemleri her aşamada şeffafça paylaşılmalıdır (Watty, 2025; Fineberg vd., 2025).

Yapay zeka destekli Zero-Party Data, işletmelerin post-cookie ekonomisinde sürdürülebilirliklerini sağlamaları için güçlü bir araçtır. Bu model, tüketiciyi "izlenen bir nesne" konumundan, verisini kendi rızasıyla paylaşan "güçlü bir aktör" konumuna yükselterek kişiselleştirme-gizlilik paradoksunu çözer. Böylece, tüketicilerin gizlilik endişelerini arttırmadan, benzersiz ve kişiselleştirilmiş müşteri deneyimleri sunulabilmesine imkan tanır.

5. Bulgular, Sonuç ve Tartışma

Bu çalışma, dijital pazarlamanın son yirmi yıldaki dönüşümünü, özellikle üçüncü taraf çerezlerin kullanımının sınırlandırıldığı bir dünyada tüketici gizliliği ve veri toplama yöntemleri ekseninde kapsamlı bir şekilde ortaya koymaktadır. CiteSpace bibliyometrik haritalama programı aracılığıyla yapılan bibliyometrik analizler ve literatür taraması, dijital pazarlama alanında sadece teknik bir değişim değil köklü bir paradigma kaymasının yaşandığını kanıtlamaktadır. WoS veri tabanından elde edilen 1999-2026 yılları arasında yaklaşık son 30 yılda yayımlanan 1309 adet bilimsel eserin analizi, literatürün son derece dinamik ve disiplinlerarası bir yapıya sahip olduğunu göstermektedir. Anahtar kelime ağ haritasında hesaplanan düşük yoğunluk değeri (0,0089), dijital gizlilik konusunun hala keşfedilmemiş alanlar barındıran bir akademik olgunluk düzeyinde olduğunu ifade etmektedir. Analizlerin en dikkat çekici bulgusu "Güven" anahtar kelimesinin 252 atıf sayısıyla diğer bir ifadeyle 252 adet yayında ortak anahtar kelime olarak kullanılmasıyla tüm literatürün merkezinde, en temel düğüm olarak konumlanmasıdır. Bu durum, tüketicilerin pasif birer izleme nesnesi olmaktan çıkıp verilerini gönüllü ifşa ettikleri sürece geçişte güvenin bir "psikolojik sözleşme" işlevi gördüğünün bilimsel olarak doğrulanması olarak ifade edilebilir. Bununla birlikte yapay zeka kavramının 35,45 gibi büyük bir atıf patlaması değerine sahip olması, literatürün geleneksel pazarlama modellerinden teknoloji odaklı, tahmine dayalı modellere doğru büyük bir kırılma yaşadığını kanıtlamaktadır.

Çalışmada, perakendecilerin ve markaların uzun süredir içinde bulunduğu "kişiselleştirme-gizlilik paradoksu" derinlemesine tartışılmaktadır. Tüketiciler bir yandan kendilerine özel ve alakalı hizmetler talep ederlerken, diğer yandan verilerini rızaları dışında çerezler aracılığıyla toplanmasından dolayı kendilerini oldukça savunmasız hissetmektedirler. Aguirre vd.,(2015)'nin çalışmalarıyla desteklendiği üzere, gizli veri toplama yöntemleri tüketicilerde tepkiselliğe yol açarak hizmetlerin benimsenme düzeyini düşürmektedir. Buna karşın, Culnan ve Armstrong (1997)'un yıllar önce vurguladığı gibi, tüketicilere "adil bilgi uygulamaları" açıkça sunulduğunda ve ekonomik / sosyal bir fayda sağlandığında, verilerini paylaşmaya çok daha istekli oldukları görülmektedir. Günümüzde bu durum markaların "izinsiz takipçi" yerine "şeffaf bir değer ortağı" olmaları gerektiğini her zamankinden daha zorunlu kılmaktadır.

Çalışmada yer alan tartışmaların odak noktasında yer alan "Zero-Party Data", tüketicinin proaktif ve bilinçli olarak paylaştığı bilgilerdir. Yapay zeka bu verilerin toplanma sürecini "müdahaleci" olmaktan çıkarıp "keyifli bir deneyime" dönüştürmektedir. Yapay zeka etkileşimli quizler, sohbet robotları ve öneri motorları aracılığıyla elde edilen veriler etik çerçevede işlendiğinde, kişiselleştirme ve gizlilik arasındaki o hassas denge kurulabilmektedir. Bu anlamda post-cookie ekonomisinde sürdürülebilir rekabet avantajı elde etmek isteyen işletmelerin

veri toplama süreçlerini sadece kendi çıkarlarına değil, tüketicilerin zaman tasarrufu veya kişiselleştirilmiş hizmet gibi net bir fayda elde edecekleri, bir "takas" olarak kurgulamaları önemlidir. Veri toplama sürecinde "veri" hem işletmeler hem de tüketiciler için değer sunan bir

takas aracı olmalıdır. Şeffaflık sadece yasal bir zorunluluk değil, markanın rekabet avantajı sağlayan bir vaadi olmalıdır. Bu anlamda güven, ürün özelliği olarak sunulmalıdır. Ayrıca, tüketicilerin veri üzerinde kontrol haklarının olması gizlilik endişelerini azaltacaktır. Bu noktada kontrolün tüketiciye verilmesi ve açıklanabilir yapay zeka araçlarının kullanımı benzersiz bir karşılıklı güven süreci inşa edecektir. Bu model, tüketicilerin veri paylaşım süreçlerinde daha etkin bir rol üstlenmelerini desteklemektedir.

Kaynakça

Aguirre, A., Mahr, D., Grewal, D., de Ruyter, K., & Wetzels, M. (2015). Unraveling the personalization paradox: The effect of information collection and trust-building strategies on online advertisement effectiveness. *Journal of Retailing*, 91(1), 34-49.

Anderson, J., & Rainie, L. (2017). *The future of well-being in a tech-saturated world*. Pew Research Center.

Braze. (2025). *What is zero-party data?*. https://www.braze.com/resources/articles/what-is-zero-party-data

Britt, P. (2020). *Zero-party data: Personalization and privacy can coexist*. Destination CRM. https://www.destinationcrm.com/Articles/Editorial/Magazine-Features/Zero-Party-Data-Personalization-and-Privacy-Can-Coexist-141000.aspx.

Chen, C. (2004). Searching for intellectual turning points: Progressive knowledge domain visualization. *Proceedings of the National Academy of Sciences*, *101*(Suppl. 1), 5303–5310. https://doi.org/10.1073/pnas.0307513100

Chen, C. (2006). CiteSpace II: Detecting and visualizing emerging trends and transient patterns in scientific literature. *Journal of the American Society for Information Science and Technology*, *57*(3), 359–377.

Chen, C. (2020). *CiteSpace: A practical guide for mapping scientific literature*. Nova Science Publishers.

Chen, C., Ibekwe-SanJuan, F., & Hou, J. (2010). The structure and dynamics of co-citation clusters: A multiple-perspective co-citation analysis. *Journal of the American Society for Information Science and Technology*, *61*(7), 1386–1409. https://doi.org/10.1002/asi.21309

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness and impersonal trust: An empirical investigation. *Organization Science*. INFORMS, vol. 10(1), pages 104-115, February. https://doi.org/10.1287/orsc.10.1.104

Dommeyer, C. J., & Gross, B. L. (2003). What consumers know and what they do: An investigation of consumer knowledge, awareness, and use of privacy protection strategies. *Journal of Interactive Marketing*, *17*(2), 34–51.

Elagina, D. (2026, 2 Mart). *Smartphone unit shipments worldwide 2009-2026*. Statista. https://www.statista.com/statistics/271491/worldwide-shipments-of-smartphones-since-2009/?srsltid=AfmBOoqj3HWbZqFYdDb8jT0PK55FvHG0UloM69nb8q37-SJs2RAsAwer

European Parliament and Council of the European Union. (2016). *General Data Protection Regulation (GDPR): Article 2 - Material scope*. https://gdpr-info.eu/art-2-gdpr/

Fineberg, S., Hupfer, S., Loucks, J., Steinhart, M. & Mazumder, S. (2025, 25 Eylül). *2025 In the gen AI economy, consumers want innovation they can trust.* Deloitte Insights. https://www.deloitte.com/us/en/insights/industry/telecommunications/connectivity-mobile-trends-survey.html

Forrester. (2025). *An illustrated guide to collecting zero-party data*. https://www.forrester.com/report/An-Illustrated-Guide-To-Collecting-ZeroParty-Data/RES161015

Hair, J. E., Anderson, R. E., & Tatham, R. I. (1987). *Multivariate data analysis with readings*.

Hoofnagle, C. J., King, J., Li, S., & Turow, J. (2010). *How different are young adults from older adults when it comes to information privacy attitudes and policies?* (Vol. 2017). University of Pennsylvania. (Not: Kaynak listesinde 2017 yılı cilt/versiyon bilgisi olarak yer almaktadır).

InMoment. (2018). *2018 CX trends report: What brands should know about creating memorable experiences*. InMoment.

Iucolano, D. M. (2019). *Hyperconnectivity giveth and taketh away: Reconciling being an "always-on" empowered consumer and privacy in an era of pervasive personal data exchanges* (Doktora Tezi). Case Western Reserve University, Weatherhead School of Management.

Kutty, R. N., Orellana-Rodriguez, C., Brigadir, I., & Diaz-Aviles, E. (2021). *Personalization, privacy, and me*. arXiv. https://doi.org/10.48550/arXiv.2109.06990

Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues*, *33*(3), 22–42. https://doi.org/10.1111/j.1540-4560.1977.tb01880.x

Marketing Science Institute. (2014). *MSI research priorities: 2014-2016*. Marketing Science Institute.

Milne, G. R., & Gordon, M. E. (1993). Direct mail privacy-efficiency trade-offs within an implied social contract framework. *Journal of Public Policy & Marketing*, *12*(2), 206–215. https://doi.org/10.1177/074391569101200206

Quan-Haase, A., & Wellman, B. (2005). Local virtuality in an organization: Implications for community of practice. P. Van den Besselaar, D. M. G., J. Preece, & C. Simone (Ed.), *Communities and technologies 2005: Proceedings of the Second Communities and Technologies Conference* içinde (ss. 215–238). Springer.

Stone, E. F., & Stone, D. L. (1990). Privacy in organizations: Theoretical issues, research findings, and protection mechanisms. In K. M. Rowland & G. R. Ferris (Eds.), *Research in personnel and human resources management* (Vol. 8, pp. 349–411). JAI Press.

Treanor, T. (2025). *What is the difference between first-party, second-party and third-party data?* CDP. https://cdp.com/articles/the-difference-between-first-party-second-party-and-third-party-data/.

Varonis. (2023a, 11 Mayıs). *US privacy laws: US Privacy Act of 1974*. https://www.varonis.com/blog/us-privacy-laws#us-privacy-act-of-1974

Varonis. (2023b, 11 Mayıs). *US privacy laws: Health Insurance Portability and Accountability Act (HIPAA)*. https://www.varonis.com/blog/us-privacy-laws#health-insurance-portability-and-accountability-act-hipaa

Varonis. (2023c, 11 Mayıs). *US privacy laws: Children's Online Privacy Protection Act (COPPA)*. https://www.varonis.com/blog/us-privacy-laws#childrens-online-privacy-protection-act-coppa

Varonis. (2023d, 11 Mayıs). *US privacy laws: Gramm-Leach-Bliley Act (GLBA)*. https://www.varonis.com/blog/us-privacy-laws#gramm-leach-bliley-act-glba

Varonis. (2023e, 11 Mayıs). *US privacy laws: New US state data privacy laws*. https://www.varonis.com/blog/us-privacy-laws#new-us-state-data-privacy-laws

Verhoef, P. C., Reinartz, W. J., & Krafft, M. (2010). Customer engagement as a new perspective in customer management. *Journal of Service Research*, *13*(3), 247–252.

Watty, F. (2026, 8 Haziran). *U.S. consumers using generative AI for online shopping 2025.* Statista. https://www.statista.com/statistics/1645128/us-consumers-using-ai-for-online-shopping/?srsltid=AfmBOoqdc1r1DIhGmVoCUwnMRRQwpfxJ6B_BYejQfrhiI4eWQV0wDeKy

Wellman, B. (2001). Physical place and cyberplace: The rise of personalized networking. *International Journal of Urban and Regional Research*, *25*(2), 227–252.

Widener, C., Arbanas, J., Van Dyke, D., Arkenberg, C., Matheson, B. & Auxier, B. (2025). *2025 Digital Media Trends: Social platforms are becoming a dominant force in media and entertainment. Deloitte Insights*. https://www.deloitte.com/us/en/insights/industry/technology/digital-media-trends-consumption-habits-survey/2025.html

World Economic Forum. (2011). *Personal data: The emergence of a new asset class*. World Economic Forum.

Yun, J. T., Segijn, C. M., Pearson, S., Malthouse, E. C., Konstan, J. A., & Shankar, V. (2020). Challenges and future directions of computational advertising measurement systems. *Journal of Advertising*, *49*(4), 446–458. https://doi.org/10.1080/00913367.2020.1795757

Zhu, H., Ou, C. X., Van den Heuvel, W., & Liu, H. (2017). Privacy calculus and its utility for personalization services in e-commerce: An analysis of consumer decision-making. *Information & Management*, *54*(4), 427–437. https://doi.org/10.1016/j.im.2016.10.001