

HİPER-KİŞİSELLEŞTİRME UYGULAMALARININ TÜKETİCİNİN ÇEVİRİMİÇİ ETKİLEŞİME DEVAM ETME DAVRANIŞINA ETKİSİ*

Şebnem BAŞİMİ HOLZER² Nesrin ALPTEKİN³

Öz

Bu çalışmanın amacı, hiper-kişiselleştirme uygulamalarının çevrimiçi mahremiyetle ilişkisini mahremiyet hesabı teorisi çerçevesinde incelemek ve tüketicinin etkileşime devam etme davranışına etkisini ölçmektir. Kolayda örnekleme yöntemi ile seçilen Türkiye'deki 18 yaş ve üzeri düzenli olarak çevrimiçi alışveriş yapan, sosyal medya hesaplarını ve eğlence platformlarını kullanan 400 tüketiciden çevrimiçi anket yoluyla elde edilen veriler kısmi en küçük kareler yapısal eşitlik modellemesi ile analiz edilmiştir. Analiz sonucunda elde edilen bulgular değerlendirildiğinde, mahremiyet hesabı teorisi çerçevesinde hiper-kişiselleştirme uygulamalarının tüketicilerin fayda ve risk algıları üzerinde pozitif yönde anlamlı bir etkisi olduğu görülmüştür. Algılanan faydanın ve riskin algılanan değer üzerinde ve algılanan değer kişisel bilginin kullanımına isteklilik üzerinde pozitif yönde anlamlı etkisi vardır. Daha önce yaşanmış mahremiyet ihlali deneyiminin algılanan risk ve kişisel bilginin kullanımına isteklilik değişkenleri üzerinde anlamlı bir etkisi bulunmamakta, ancak işletmeye ve/veya platforma duyulan güven unsuru kişisel bilginin kullanımına isteklilik üzerinde pozitif yönde anlamlı bir etkiye sahiptir. Kişisel bilginin kullanımına istekliliğin çevrimiçi etkileşime devam etme davranışı üzerinde pozitif yönde anlamlı bir etkisi olduğu bulunmuştur.

Anahtar Kelimeler: Hiper-kişiselleştirme, Mahremiyet Hesabı, Etkileşime Devam Etme Davranışı

JEL Kodları: C12, C83, M31

THE EFFECT OF HYPER-PERSONALIZATION APPLICATIONS ON CONSUMER'S CONTINUATION TO ONLINE INTERACTION BEHAVIOR

Abstract

The aim of this study is to examine the relationship of hyper-personalization applications with online privacy within the framework of privacy calculus theory and to measure their impact on the consumer's continuation to interaction behavior. The data obtained through an online survey from 400 consumers aged 18 and over in Turkey were selected by convenience sampling method and who regularly shop online, use social media accounts and entertainment platforms were analyzed by partial least squares structural equation modelling. When the findings obtained as a result of the analysis were evaluated, it was seen that hyper-personalization applications had a positive and significant effect on consumers' benefit and risk perceptions within the framework of privacy calculus theory. Perceived benefit and risk have a significant positive effect on perceived value and perceived value has a significant positive effect on willingness to use personal information. It has been found that previous privacy violation experience does not have a significant effect on the variables of perceived risk and willingness to use personal information, while the element of trust in the business and/or platform has a positive significant effect on the willingness to use personal information. It has been found that willingness to use personal information has a positive and significant effect on continuation to online interaction behavior.

Keywords: Hyper-personalization, Privacy Calculus, Continuation to Online Interaction Behavior

JEL Codes: C12, C83, M31

* Bu çalışma için Anadolu Üniversitesi Etik Kurulu'nun 30/05/2023 tarihli toplantısında 524149 nolu kararı ile etik kurul onayı alınmıştır.

Bu çalışma Anadolu Üniversitesi Bilimsel Araştırma Projeleri Koordinasyon Birimi Koordinatörlüğü'nün SBA-2023-1880 numaralı projesi ile desteklenmiştir.

² Bağımsız araştırmacı, holzeracad@gmail.com, <https://orcid.org/0009-0000-3131-3980>

³ Prof. Dr., Anadolu Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, nesrinesen@anadolu.edu.tr, <https://orcid.org/0000-0002-8967-8955>

GİRİŞ

Teknolojik gelişmelerin yarattığı dönüşümle birlikte müşterilerin ihtiyaç ve talepleri, etkin iletişim, müşteri sadakati ve sürdürülebilirlik konuları öne çıkmıştır. Bilgi ve iletişim teknolojileri, web tabanlı ortamlar ve sosyal medyanın aralıksız gelişimi, gündelik alışkanlıkları ve iş yapma biçimlerini büyük ölçüde etkilemektedir. Büyük veri, bulut sistemleri ve veri analitiği olanakları kişiselleştirme uygulamalarını geliştirirken maliyetleri de düşürmektedir. İşletmeler pazarlarındaki dinamik değişimleri anlayabilmek için artan biçimde müşterilerine dair kişisel verilerin toplanmasına bağımlı hale gelmektedir (Rust ve Huang, 2014; Sabharwal ve Miah, 2021). Bu süreci yönetmeye çalışan işletmeler yoğun rekabet ortamında, teknolojik ve sosyal dönüşümleri göz ardı etmeden kendilerini uyarlamak ve müşterileriyle iletişim kalitelerini en üst düzeye çıkarmak durumundadırlar.

İşletmelerin müşterileriyle kurdukları etkileşimden veri elde etme yetenekleri artarken, hızla gelişen iletişim teknolojileri hiper-kşiselleştirme uygulamalarını kolaylaştırmaktadır. Hiper-kşiselleştirme, yapay zekâ uygulamaları ve gerçek zamanlı verilerin kullanımı yoluyla müşterilerin internetteki davranışlarının gözlemlendiği bir süreçtir. Böylece markalar müşterilerini daha iyi tanıyıp, elde ettikleri verileri özel ürün ve hizmetler sunmak için kullanabilirler. Hiper-kşiselleştirme ayrıca markaların gerçekleştirdikleri kişiselleştirme uygulamalarının en gelişmiş yolu ya da geleneksel kişiselleştirme yöntemlerinin bir adım ilerisi olarak ifade edilebilir (Deloitte, 2020; Dotcms, 2018).

Çevrimiçi etkileşim esnasında tüketicilerin karşılaştığı sorunlar da bu süreçte farklılaşmaktadır. İletişim teknolojilerinin sunduğu yeni olanaklar ve çevrimiçi alışveriş platformlarının sağladığı sayısız avantaj, çağın hızına ayak uydurmaya çalışan tüketiciler açısından gerekli görülebilmektedir. Ancak bu durum aynı zamanda düzenli kullanılan teknolojik araçları sadece kısmen tanıyan ve içerdiği güvenlik risklerini tam tahlil edemeyen tüketicilerin bilişsel çelişki yaşamasına neden olabilmektedir. Mahremiyet paradoksu olarak da ifade edilebilen bu çelişki, tüketicilerin çevrimiçi ortamda mahremiyet endişesi yaşamalarına rağmen kişisel bilgilerini ifşa etmelerinden kaynaklanmaktadır (Bandara, Fernando ve Akter, 2020; Barnes, 2006; Brown, 2001; Dienlin ve Trepte, 2015; Massara, Raggiotto ve Voss, 2021; Norberg, Horne ve Horne, 2007).

Çevrimiçi etkileşim sürecinde tüketici, kişisel bilgilerinin toplanmasının olası negatif ve pozitif sonuçları hakkında içsel bir muhakeme yani mahremiyet hesabı yapmaktadır (Li, 2012). Literatürde mahremiyet hesabı teorisi olarak adlandırılan kavram, bilgi ifşasının algılanan risk, fayda ve değerini ifade etmektedir. Tüketicinin çevrimiçi ortamda risk, fayda ve değer algılarının nasıl şekillendiğini anlamaya yönelik çeşitli bilimsel araştırmalar yapılmıştır (Ackermann, Burkhalter, Mildenerger, Frey ve Bearth,

2022; Hallam ve Zanella, 2017; Hayes, Brinson, Bott ve Moeller, 2021; Jahari, Hass, Hass ve Joseph, 2022; Lee ve Rha, 2016; Vimalkumar, Sharma, Singh ve Dwivedi, 2021). Bu araştırmalar işletmeler ve tüketicilere yönelik önemli veriler sunmaktadır. Bu veriler işletmelerin en uygun etkileşim ortamını nasıl yaratacakları ve tüketicilerin de varolan güvenlik endişelerini aşarak bu etkileşim ortamından en yüksek faydayı nasıl elde edecekleri konusunda yol göstericidir (Aguirre, Mahr, Grewal, de Ruyter ve Wetzels, 2015; Vimalkumar, Sharma, Singh ve Dwivedi, 2021).

Bu çalışmanın amacı hiper-kişiselleştirme uygulamalarının çevrimiçi mahremiyetle ilişkisini mahremiyet hesabı teorisi çerçevesinde incelemek ve tüketicinin rasyonel akıl yürütme sürecinin etkileşime devam etme davranışına etkisini ölçmektir. Araştırma kapsamında tasarlanan model, Türkiye’deki 18 yaş ve üzeri tüketicilerin çevrimiçi davranışına odaklıdır ve daha önce yaşanmış mahremiyet ihlali deneyimini ve işletmeye ve/veya platforma duyulan güven faktörlerini öncül olarak göz önünde bulundurmaktadır. Araştırma modelinde kullanılan mahremiyet hesabı teorisi, çevrimiçi etkileşim sürecinde tüketicinin, kişisel bilgilerinin toplanmasının olası negatif ve pozitif sonuçları hakkında içsel bir muhakeme yani mahremiyet hesabı yaptığını vurgulamaktadır. Bilgi ifşasının algılanan faydası ve riskini göz önüne alan tüketici bilgi ifşası deneyimine dair bir değer algısına sahip olmaktadır. Çalışma kapsamında tüketicilerin çevrimiçi etkileşimde hiper-kişiselleştirme uygulamalarıyla karşılaşp veri ifşasında bulunduklarında mahremiyet endişesi yaşayıp yaşamadıkları incelenmiştir. Takip eden süreçte tüketicinin risk, fayda ve değer algısının kişisel bilginin kullanımına istekliliği üzerindeki etkisi incelenmiş ve bunun etkileşime devam etme davranışı üzerinde etkisinin olup olmadığı araştırılmıştır.

Hiper-kişiselleştirme konusundaki çalışmalar henüz yenidir ve Türkiye’deki tüketicilerin hiper-kişiselleştirme uygulamalarına dönük farkındalık ve algıları üzerinde yapılan çalışma sayısı kısıtlıdır. Türkiye’deki tüketicilerin çevrimiçi mahremiyet algıları ve bu algıların davranışları üzerindeki etkilerini ölçmek üzere tasarlanmış araştırmalar bulunmakla birlikte mahremiyet hesabı teorisi çerçevesinde konuya yaklaşan araştırma sınırlı sayıdadır. Mahremiyet hesabı teorisi çerçevesinde konuya yaklaşmasından dolayı bu araştırmanın, Türkiye’deki tüketicilerin çevrimiçi ortamdaki tecrübelerinin algılarını ve davranışlarını nasıl etkileyebileceği konusunda yapılan öncü çalışmalardan olacağı düşünülmektedir.

KAVRAMSAL ÇERÇEVE ve ARAŞTIRMA HİPOTEZLERİ

Kişiselleştirme ve Hiper-kişiselleştirme

Dijital pazarlamada iletişim birden çok kanal üzerinden ilerleyebilen gerçek zamanlı bir etkinliktir (Dunakhe ve Panse, 2022). Tiago ve Verissimo (2014) müşteri geri dönüşlerinin interaktif şekilde alınmasının iletişimi güçlendirdiğini ve verimliliği artırdığını vurgulamaktadırlar. Kotler (2021) ise,

Pazarlama 4.0 ile geleneksel pazarlamadan dijital geçiş yaptığımızı ve bugün de Pazarlama 5.0 yani insan için teknoloji anlayışını konuştuğumuzu ifade etmiştir.

Büyük veri ve veri madenciliği, yapay zekâ ve makine öğrenmesi, CRM sistemleri, Nesnelerin İnterneti, gerçek zamanlı analitik ve bulut bilişim, dijital pazarlamada hiper-kişiselleştirme uygulamalarını mümkün kılan başlıca teknolojik gelişmelerdir (Arora vd. 2020; BTK, 2021; Plangger, Grewal, Ruyter ve Tucker, 2022). Büyük işlem hızı nedeniyle insan zekâsından farklı olan yapay zekâ, bir amaca dönük davranış için veriyi işleme ve bilgiye dönüştürme yeteneği olarak tanımlanabilir (Paschen, Kietzmann ve Kietzmann, 2019, s. 1411). Kaplan ve Haenlein (2019, s.17) yapay zekâyı bir sistemin dış verileri doğru bir şekilde yorumlaması, bu veri vasıtasıyla öğrenmesi ve esnek uyumlanma sürecinde bu öğrendiklerini belirli hedeflere ulaşmak için kullanması olarak tanımlamışlardır. Perakende sektöründe yapay zekâ teknolojisi genellikle, artırılmış gerçeklik ve görüntü tanıma gibi diğer teknolojilerle birlikte kullanılmaktadır (Saponaro, Le Gal, Guisiano ve Maniere, 2018). Otomasyonun artışı, azalan maliyetler, artan esneklik ve kolaylaşan etkileşim yapay zekânın sağladığı avantajlar olarak sayılabilir (Aldoseri, Al-Khalifa ve Hamouda, 2024). Diğer yandan yapay zekâ teknolojisine bağımlılık ve müşteri verisine duyulan ihtiyacın sürekli artışı, tüketiciler üzerinde güven sorunlarına yol açabilmektedir (Dwivedi vd., 2019). Bu nedenle yapay zekâ destekli müşteri deneyimleriyle ilgili diğer potansiyel sorunların daha iyi anlaşılması gerekmektedir (Bitkina vd., 2020; Chen, Prentice, Weaven ve Hisao, 2022; Malle, Scheutz, Arnold, Voiklis ve Cusimano, 2015; Shank, Graves, Gott, Gamez ve Rodriguez, 2019).

Makine öğrenimi, bilgisayarları belirli istatistiksel modeller kullanarak insan davranışını simüle ederek tahmin etmeleri için eğiten, yapay zekânın bir alt kümesidir (Davenport, Guha, Grewal ve Bressgott, 2020). Makine öğrenimi müşteri tercihlerini tahmin etmek için pazarlama alanına uygulandığında, yöneticiler web sitelerini müşteri tercihlerine ve ödeme isteklerine uyacak şekilde özelleştirebilmektedirler (Bastos ve Bernandes, 2024). Ancak makine öğrenimi ve yapay zekâ yöntemiyle üretilen çözümlerin ne derece iyi olduğu eldeki verilerin kalitesine bağlıdır. Veri kalitesinin düşük olması ise eksik, tutarsız, yanlış, mükerrer veriler gibi çeşitli şekillerde kendini göstermektedir (Do ve Trang, 2020; Gudivada, Apon ve Ding, 2017). Toplanan veri miktarı arttıkça yeni ihtiyaçlar ortaya çıkmakta, bu verilerin bir anlam ifade edebilmesi için gruplanması, yorumlanması, analiz edilmesi gerekmektedir. Bu ihtiyaç büyük veri uygulamalarının ön plana çıkmasına neden olmuştur (Doğan ve Arslantekin, 2016; Wu, Zhu, Wu ve Ding, 2014). Karim ve Rahman (2013, s. 196) veri madenciliğini “büyük veri gruplarından anlamlı ve yararlı bilgiler çıkarma süreci” olarak tanımlamışlardır. Veri madenciliği öncelikle işletmelerin perakende ve satış, finans ve pazarlama, mesajlaşma gibi günlük ve önemli faaliyetlerinde kullanılmaktadır (Mach-Król ve Hadasik, 2021). Veri madenciliği yaparak büyük veri kümeleri arasındaki örüntüler belirlenir ve böylece müşteri

davranışı tahmin edilebilir, karmaşık sorgu sonuçları elde edilebilir, aktif bilgi üretilebilir ve gereksiz bilgi ayıklanabilir (Liu, Zhao ve Yang, 2022; Maheswari ve Priya, 2017). Huang ve Rust (2017), geliştirilmiş müşteri iletişimi, büyük veri ve bu verilerin geliştirilmiş analizlerinin, kişiselleştirilmiş hizmet ve güçlendirilmiş müşteri ilişkisi için fırsat yarattığını vurgulamaktadır.

Kişiselleştirme, bugün ve gelecekteki iş fırsatlarını en üst düzeye çıkarmak için doğru içeriği doğru kişiye doğru zamanda sunmayı amaçlayan müşteri odaklı bir pazarlama stratejisidir (Tam ve Ho, 2006). Nobile ve Kalbaska (2020) kişiselleştirmeyi, belirli müşteri tercihlerinin dikkate alınması suretiyle ulaşılan bireye özel kılma olarak ifade etmektedirler. Bilginin tek bir müşterinin ihtiyaçlarına ve tercihlerine göre uyarlanması olarak da ifade edilebilen kişiselleştirme böylece olumlu deneyimlerin önemli bir belirleyicisini oluşturur (Bilgihan, Kandampully ve Zhang, 2016; Tiisonen ve Felfernig, 2017). Kişiselleştirme ile genel olarak web kişiselleştirmesi anlaşılsa da e-ticaret, e-posta, web, app, sohbet robotu ve tıklama başına ödeme (Pay Per Click, PPC) gibi farklı türleri de vardır (Krishnan, Gupta, Gupta ve Singh, 2022).

Bir web sitesi ya da çevrimiçi platformun kişiselleştirilmiş kabul edilmesi için bazı karakteristik özellikleri barındırması gerekmektedir. Öncelikle kullanıcı kimliğinin saptanması, kullanıcı hakkında verinin toplanmaya başlanması ve bu verinin gerçek zamanlı analizi gerçekleşmektedir. Kullanıcının belirli sayıdaki etkileşiminden sonra kim, ne, nerede, ne zaman ve neden sorularına cevap verecek şekilde profili ortaya çıkmaktadır. Uygun arayüz ve içerikle sistem bilgiyi anlamlı bir şekilde birleştirmekte ve sunmaktadır (Toch, Wang ve Cranor, 2012). Bu noktaya kadar atılan adımlar ne kadar çok tekrar edilirse o denli fazla veri elde edilir. Bu süreç kullanıcı profilinin daha da detaylandırılmasına, kullanılan teknolojik araçların iyileştirilmesine ve daha verimli hale getirilmesine imkân sunmaktadır. Örneğin ürün öneri sistemleri ya da diğer adıyla tavsiye sistemleri, müşterinin daha önce yaptığı tercihlere göre elde edilmiş verileri kullanarak onların bir sonraki adımlarını ve tercihlerini tahmin eder ve bu tahminlere dayalı öneriler sunar (Zhou, Xiong ve Chen, 2023). Öneri sistemleri böylece müşterilerin hangi filmi izleyebilecekleri, hangi müziği dinleyebilecekleri ya da hangi ürünü satın alacakları gibi konularda karar verirken desteklemeyi amaçlar (Budak ve Gümüştaş, 2022).

2010'lu yıllara kadar alışılmış kişiselleştirme uygulamalarını kullanan işletmelerin çevrimiçi ortamda, hizmet verdikleri müşterilerinin ön adlarını, bulundukları bölge ya da alışveriş tarihçesi gibi temel bilgilerini edinmeleri yeterli olmaktaydı. Bu bilgiler tanıtım maillerinde ve daha önce ilgi göstermiş oldukları ürünleri hatırlatan reklamlarda kullanılmaktaydı. Bu şekildeki temel düzey kişiselleştirme uygulamaları artık yetersiz kalmaktadır ve işletmeler müşteri segmentleri için oluşturdukları kimliklerinin (persona) ötesine geçmek ihtiyacı hissetmektedir (Toch, vd., 2012). Yapay zekâ, makine öğrenmesi ve tahmine dayalı analitik kullanımı artık bir zorunluluk olarak karşılına çıkmaktadır. Yapay zekâ ve makine

öğrenimi alanları, kişiselleştirme uygulamalarının optimizasyonuna ve her zamankinden daha doğru algoritmik karar ve tahmin modelleri oluşturmaya odaklanmaktadır (Zanker, Rook ve Jannach, 2019).

Hiper-kşiselleştirilmiş, gerçek zamanlı müşteri deneyimleri davranışsal verilerin toplanmasıyla gerçekleştirilebildiğinden müşterinin tam adının talep edilmesi, arama esnasında geçirilen zamanın kaydı, geçmiş alışverişlere dair kayıtların tutulması, bir önceki alışverişin zamanı, ortalama alışverişte harcanan para miktarının tespiti, internette gezinme verilerinin gözetimi gibi uygulamaları içermektedir (Fayyaz, Ebrahimian, Nawara, Ibrahim ve Kashef, 2020). Her bir bireyin bir pazar segmenti olarak kabul edildiğı, iletişimsel analizlerin çok daha ileri düzeyde yapıldığı bu yaklaşımda markalar bireylere en etkili kanallar üzerinden ve onların en çok ilgisini çekecek teklif ve mesajlarla yaklaşabilmektedir. Böylece müşterilerinin ihtiyaçlarını beklentilerine uygun şekilde karşılayan markalar müşteri memnuniyetini artırdıkça müşteri sadakati de artmaktadır (Kim ve Baek, 2017; Tyrväinen, Karjaluo ve Saarijärvi, 2020).

Çevrimiçi Mahremiyet ve Mahremiyet Paradoksu

Hiper-kşiselleştirme uygulamaları yardımıyla yapılan çevrimiçi davranış analizi, müşterilerin özel verilerine erişimi ve bu verilerin işlenmesini gerektirdiğinden, çevrimiçi veri mahremiyeti endişesini de beraberinde gelmektedir (Choi, Park ve Jung, 2018; Malhotra, Kim ve Agarwal, 2004; Quinn, 2014). Bilgiye kimlerin erişiminin olacağı gibi konulardaki belirsizlik müşteride gözlemlendiğı, talep etmediğı ticari işlemlere maruz kalacağı, kimlik hırsızlığına uğrayacağı gibi korkular yaratabilmektedir (Milne, Rohm ve Bahl, 2004). Çevrimiçi mahremiyet, müşterilerin diğer müşteriler ve kurumlarla etkileşimde bulunurken ne kadar erişilebilir olduklarının ve gizlilik düzenlemeleri yoluyla aktif olarak erişilebilirlik düzeylerini ne kadar belirleyebileceklerinin değerlendirmesidir (Trepte, 2020).

Bu bağlamda, müşteriler kişisel verilerinin ifşa edilmesi karşılığında elde edecekleri faydaları ve potansiyel mahremiyet ihlali riskini karşılaştırır ve bir muhakeme yaparlar (Kim, Park, Park ve Ahn, 2019). Bilgi ifşasının algılanan faydası, müşterinin kişisel veri paylaşımı karşılığında alacağı kişiselleştirilmiş hizmetler veya daha iyi bir çevrimiçi deneyim gibi avantajlarla ilişkilidir. Bilgi ifşasının algılanan riski, bu bilgilerin kötüye kullanılması, gizliliğın ihlal edilmesi veya üçüncü taraflara izinsiz aktarılması gibi olasılıkları kapsamaktadır. Fayda ve risk karşılaştırması yapılan bu bilişsel süreç sonunda müşteri bilgi ifşasına dair bir değer algısına sahip olmaktadır (Culnan ve Armstrong, 1999; Dinev ve Hart, 2006; Princi ve Krämer, 2020). White (2004), tüketicilerin bilgi ifşa etme kararlarında, elde edecekleri yararların algılanan risklerden ağır basması durumunda daha istekli olduklarını ifade etmektedir. Ancak mahremiyet kaybı ya da utanma gibi riskler varsa, bu durum bilgi ifşa etme istekliliğini azaltmaktadır. Özellikle, daha kişiselleştirilmiş faydalar karşılığında gizliliğı korunan bilgiler daha fazla ifşa edilirken,

utanç verici bilgiler için bunun tersi geçerlidir. Müşterinin algıladığı faydanın kısa ve uzun vadede farklılaştığını belirten Wilson ve Valacich (2012), fayda algısı zaman geçtikçe zayıfladığından, müşterilerin uzun vadede fayda olarak görülebilecek unsurları gözardı ettiğini vurgulamaktadırlar.

Mahremiyet paradoksu ise çevrimiçi platformlarda veri mahremiyeti endişesi yaşamalarına rağmen veri paylaşma eğilimi göstermelerindeki çelişkiyi ortaya koymaktadır (Acquisti, 2004; Beke, Eggers, Verhoef ve Wieringa, 2022; Hoffmann, Lutz ve Ranzini, 2016; Tufekci, 2008; Young ve Quan-Haase, 2013). Kişisel verilerinin korunması için daha fazla güvence bekleyen müşteriler, kişiselleştirilmiş hizmetler alma arzusundan da vazgeçmemektedir. Barnes (2006) sosyal medya kullanıcılarının davranışlarını incelediği çalışmasında bu çelişkiye dikkat çekmiş ve kullanıcıların mahrem bilgilerin çevrimiçi ortamdaki sızıntısına karşı hassas olmalarına rağmen sosyal medyayı kullanırken mahrem bilgi ifşasında bulunabildiklerini vurgulamıştır.

Baek, Kim ve Bae (2014), müşterilerin iç ve dış çevresel faktörlerin etkisiyle rasyonel akıl yürütmede bir sınırlama yaşadıklarını vurgulamışlardır. Bir başka deyişle, tüketicilerde mahrem bilgi ifşa edildiğinde karşılaşılabilecek risklerin neler olabileceği konusunda önyargılar oluşmaktadır. Örneğin mahrem bilgi sızıntısı riskine dair algı, kişisel olmayan deneyim ifadelerine dayandığında iyimserlik önyargısı oluşmaktadır. Bu nedenle bireyler böylesi bir risk konusunda değerlendirme yaparken diğerlerinden daha şanslı olduklarına dair bir yanılsamaya kapılmaktadırlar. Literatürde karşılaştırmalı iyimserlik olarak ifade edilen bu durum, aslında bir trafik kazası ya da ağır bir hastalık gibi durumlar için de geçerlidir (Helweg-Larsen ve Shepperd, 2001). İyimserlik önyargısı kültür, cinsiyet, eğitim durumu ve yaş gibi faktörlerden bağımsız her kesimde görülebilmektedir (Klein ve Helweg-Larsen, 2002). Müşterinin gizlilik ifşası ya da mahremiyet ihlali riskiyle başa çıkma becerilerine duyduğu yüksek güven de yine aynı şekilde iyimser bir önyargı doğurmaktadır (Jensen, Potts ve Jensen, 2005).

Tüketicilerin çevrimiçi etkileşim sürecinde kullandıkları teknolojik gereçler üzerindeki hakimiyetlerinin mahremiyet endişesine olan etkilerini inceleyen birçok araştırma bulunmaktadır (Boerman, Kruikemeier ve Borgesius, 2018; Chiasson, Abdelaziz ve Chanchary, 2018; Estrada-Jiménez, Parra-Arnau, Rodriguez-Hoyos ve Forné, 2016; Leon vd., 2012; Martin ve Murphy, 2017; Smit, Van Noort ve Voorveld, 2014). Jensen, Potts ve Jensen (2005) çevrimiçi mahremiyetlerini koruma konusunda yüksek donanımına sahip olduğunu düşünen kullanıcıların sadece dörtte birinden daha azının mahremiyet risklerini nasıl önleyeceğini bildiğini vurgulamaktadırlar. Boerman vd. (2018) müşterilerin çerezlerin silinmesi veya reddedilmesi, lokasyon temelli hizmetlerin kısıtlanması, arama motoru tarihçesinin temizlenmesi, izleme önleme yazılımlarının kullanılması gibi önlemleri sadece kısmen aldıklarını gözlemlemişlerdir. Çevrimiçi mahremiyet konusunda endişeleri olan bu müşterilerin %20'sinden fazlası mahremiyet ihlaline karşı

kullanabilecekleri en temel teknik donanımları tanımamakta, örneğin bilgisayarlarında bu ayarların yapıp yapılmadığını bilmemektedir.

Kişiselleştirme-mahremiyet paradoksu kavramı bir işletmenin müşteri deneyimlerini kişiselleştirmek için tüketici bilgilerine olan ihtiyacı ile, bir müşterinin mahremiyet ihtiyacı arasındaki sürekli gerilim olarak ifade edilebilir. Modern teknolojinin gelişimiyle bu gerilim daha da yoğunlaşmaktadır, öyle ki, işletmeler teknolojik araçlar vasıtasıyla tüketicilerin kişisel verilerine erişirken, tüketici çoğu zaman verdiği onayın içeriğini ve rızanın koşullarını tam olarak anlamamaktadır (Bornschein, Schmidt ve Maier, 2020). İşletmeler bu bilgileri genellikle müşterilerin çevrimiçi deneyimlerini iyileştirmek için kullanıyor olsalar da kötüye kullanım riski gizlilik endişesi yaratmaktadır. Bu nedenle işletmeler kişisel verilerin toplanması ile müşterilerin mahremiyet endişelerinin azaltılması arasında bir denge bulma çabasıdadır (Aguirre vd., 2015; Bleier, Goldfarb ve Tucker, 2020).

Müşterilerin mahremiyet kararlarını nasıl aldıklarını anlamaya yönelik araştırmalar (Bélanger ve James, 2020; Bleier ve Eisenbeiss, 2015) konuya farklı açılardan yaklaşmakta ve bu denge bulma çabasına katkıda bulunmaya çalışmaktadır. Örneğin tüketicinin kişisel bilgilerinin kullanımı veya akışı üzerinde kontrol sağlaması mahremiyet endişelerini hafifletmek için bir taktik olarak görülebilir. Sonuçta tüketiciler, savunmasızlıklarını, ihlal duygularını ve belirsizliği azaltmayı vaat eden bu tür mahremiyet kontrollerine değer vermektedir (Martin, Borah ve Palmatier, 2017). Bu kontrollerin yoğunlukla müşterinin algısına yönelik olduğu, veri erişimi konusunda aslında bir değişim yaratmadıkları ve kişisel bilgilerin korunma seviyesi üzerinde çok az etkilerinin bulunduğunu ifade ettikleri çalışmalarında Brandimarte, Acquisti ve Loewenstein (2013) ayrıca, tüketicilere güçlenme hissi veren mahremiyet kontrollerinin riskli durumlarda bile bilgi ifşası eğilimi yaratmasından dolayı zararlı olabileceğini vurgulamışlardır. Mousavi, Chen, Kim ve Chen (2020) sosyal medya ağı kullanıcılarının platformun önerdiği gizlilik güvence mekanizmalarını kendi hesaplarını özelleştirmek için kullanırken mahrem bilgi ifşası konusunda daha dikkatli hale geldiklerini ifade etmişlerdir. Ancak kullanıcı risk unsurunun azaldığını ve kişisel bilgileri üzerinde daha fazla kontrolü olduğunu düşündüğünden dolayı yoldan mahrem bilgi ifşasına eğimli hale gelmektedir. Tüm bu bilgiler ışığında, hiper-kşiselleştirme uygulamalarının bilgi ifşasının algılanan faydası ve riski üzerindeki etkisini ölçmek amacıyla oluşturulan hipotezler aşağıdaki gibidir:

H₁: Hiper-kşiselleştirme uygulamalarının bilgi ifşasının tüketici tarafından algılanan faydası üzerinde anlamlı bir etkisi vardır.

H₂: Hiper- kşiselleştirme uygulamalarının bilgi ifşasının tüketici tarafından algılanan riski üzerinde anlamlı bir etkisi vardır.

Mahremiyet Hesabı Teorisi

Alan Westin'in çalışmaları (1967), bireylerin mahremiyet tercihlerini fayda-maliyet analizi bağlamında değerlendiren fikirlerin öncüsü olarak kabul edilmektedir ve mahremiyet davranışlarına ilişkin teorilerin gelişiminde önemli bir referans noktasını oluşturmaktadır (Smith, Dinev ve Xu, 2011). Mahremiyet hesabı teorisi ilk kez Laufer ve Wolfe (1977) tarafından öne sürülmüştür. Bu teori, bireylerin mahremiyetle ilgili kararlarını fayda-maliyet analizi ve sosyal psikolojideki sosyal sözleşme ve sosyal değişim teorilerine dayandırarak açıklamaktadır (Zhu, Cao ve Liu, 2022). Culnan ve Bies'in (2003) çalışması, dijital ortamda mahremiyet kararlarının fayda-maliyet analizi üzerine kurulu olduğunu açıklayarak mahremiyet hesabı teorisinin çevrimiçi dünyadaki uygulamasını açıklamaktadır. Bu çalışmaya göre tüketiciler, kişisel verilerini paylaşma kararlarını verirken potansiyel riskler ve elde edilecek faydalar arasında denge kurma çabasıdadır. Dinev ve Hart (2006) ise Westin (1967)'in bireylerin mahremiyet ve fayda dengesi üzerine kurulu analizlerinin mahremiyet hesabı teorisi gibi modern teorilere nasıl katkı sağladığını açıklamakta ve mahremiyet hesabı teorisini e-ticaret bağlamında ele almaktadır.

Mahremiyet hesabı teorisine göre müşteri çevrimiçi etkileşim sürecinde, kişisel bilgilerini paylaşmanın potansiyel risk ve faydalarını tartarak bir karara varmaktadır (Tang, Zhang ve Xiao, 2022; Li, 2012). Müşteri bir taraftan etkileşimin olası risklerini değerlendirirken diğer taraftan da çevrimiçi etkileşimden çeşitli ekonomik ve sosyal faydalar elde edeceğine, eğlenme, sosyal ilişkiler kurma, kimlik inşa etme gibi beklentilerini karşılayabileceğine dair bir algıya sahiptir. Müşterilerin mahremiyetle ilgili algıları, bu faydalar ve riskler arasındaki değerlendirmeler sonucu şekillenir ve nihai paylaşım kararı etkiler (Tian, Chen ve Zhang, 2022).

Al-Jabri, Eid ve Abed (2019), kişisel bilgilerin ifşasının algılanan faydalarının müşterilerin çevrimiçi etkileşimlerine olan etkisini vurgulamaktadırlar. Algılanan faydaların, kişisel bilgi paylaşımını artırdığına dair sonuçlar ortaya koyarak fayda algısının artmasıyla, müşterilerin bu bilgileri paylaşma istekliliklerinin de arttığı belirtilmektedirler. Wang, Zhao, Zhou ve Li (2022), tüketicilerin kişiselleştirilmiş hizmetler gibi faydalar risk algılarına göre daha ağır bastığında ifşa eğiliminde olduklarını vurgulamaktadırlar. Araştırmada özellikle kültürel arka plan ve çevrimiçi platformun tipi gibi moderatör değişkenler bu ilişkiyi etkileyen önemli değişkenler olarak belirlenmiştir.

Ioannou, Tussyadiah ve Lu (2020), özellikle hassas biyometrik verilerin paylaşılması söz konusu olduğunda, algılanan gizlilik risklerinin, müşterilerin veri ifşası kararlarını doğrudan etkilediğini ifade etmektedirler. Toch vd. (2012), belli başlı kişiselleştirme uygulamalarına bağlı mahremiyet risklerini analiz etmişler ve iki boyuta dayalı bir çerçeve önermişlerdir. Bu iki boyut kişiselleştirmenin derecesi ve

mahremiyet kontrolüdür. Kişiselleştirme dereceleri, veri toplanması fazı, kullanıcı modeli yaratma fazı ve adaptasyon fazından oluşmaktadır. İkinci boyut olan mahremiyet kontrolü, müşterinin kişiselleştirme sürecinde hem algıladığı hem de tecrübe ettiği, kendi verileri üzerindeki kontrol düzeyiyle ilişkilidir.

Yapay zekânın kullanıldığı hiper-kişiselleştirme uygulamalarının tüketici deneyimine nasıl yansıtıldığı bilgi ifşasının algılanan faydasına etki etmektedir. Komiak ve Benbasat (2006), müşterilerin çevrimiçi etkileşim esnasında hiper-kişiselleştirme uygulamalarını tecrübe ettiklerinde bu tecrübeyi markanın yetkinliği ile ilişkilendirdiğini vurgulamışlardır. Ayrıca etkileşim sürecinde çeşitli seçeneklerin sunulduğu müşteri, kendi tercihlerinin işletme/marka için önemli olduğu ve markanın sağladığı tavsiyelerin de tarafsız olduğu algısına sahip olmaktadır (Aguirre vd., 2015).

Müşterinin fayda-risk dengesini değerlendirmesiyle gelişen değer algısı, çevrimiçi ortamdaki kişisel bilgilerini paylaşma istekliliği üzerinde doğrudan bir etkiye sahiptir (Anderson ve Agarwal, 2011; Chen, Huang ve Qi, 2024; Dinev ve Hart, 2006; Fu, Zhang ve Li, 2023; Omarzu, 2000). Chaudoir ve Fisher (2010) bilgi ifşası süreçlerinin karmaşık bir şekilde geliştiğini vurgulamaktadırlar. Araştırmaya göre kısa vadeli faydalar ile uzun vadeli riskler arasında bir denge kurulmaya çalışılmakta ve bu denge gelecekteki ifşa davranışlarını etkileyebilecek "yukarıya doğru sarmallar" (daha fazla görünürlük) ya da "aşağıya doğru sarmallar" (daha fazla gizleme) ile sonuçlanabilmektedir.

Mahremiyet hesabı teorisi çerçevesinde, tüketicilerin bilgi ifşasında bulunduklarında algıladıkları fayda ve risk ile algıladıkları faydanın kişisel bilginin kullanımına isteklilik üzerindeki etkisini ölçmeye yönelik olarak aşağıdaki hipotezler geliştirilmiştir:

H₃: Bilgi ifşasının algılanan faydasının, bilgi ifşasının algılanan değeri üzerinde anlamlı bir etkisi vardır.

H₄: Bilgi ifşasının algılanan riskinin bilgi ifşasının algılanan değeri üzerinde anlamlı bir etkisi vardır.

H₅: Bilgi ifşasının algılanan değerinin kişisel bilginin kullanımına isteklilik üzerinde anlamlı bir etkisi vardır.

Rasyonel Akıl Yürütme Sürecine Etki Eden Öncül Faktörler

Bireyin geleceğe dair öngörüler, geçmişte yaşadığı deneyimlere dayalı olarak şekillenmekte ve bu durum, karar alma süreçlerinde önemli bir rol oynamaktadır. Özellikle çevrimiçi etkileşimlerde, bireylerin geçmiş deneyimleri, kişisel bilgilerini paylaşma konusundaki tutumlarını, algılarını ve davranışsal kararlarını doğrudan etkilemektedir (Xu, 2007). Araştırma kapsamında, tüketicilerin geçmişte yaşadığı

çevrimiçi mahremiyet ihlali deneyimi ve çevrimiçi etkileşimde bulunduğu işletme ya da platforma duyduğu güven, rasyonel akıl yürütme sürecine etki eden faktörler olarak ele alınmıştır. Bireylerin geçmişte yaşadığı olumsuz deneyimler, çevrimiçi etkileşimlerde rasyonel akıl yürütme sürecine etki etmektedir (Smith, Milberg ve Burke, 1996).

Kişisel verilerin aşırı toplanması, veri sızıntıları veya cezai yaptırım gerektiren çevrimiçi suistimaller gibi olayları içeren mahremiyet ihlali deneyimleri, bireylerin bilgi ifşasına yönelik tutumlarını olumsuz yönde etkileyen önemli faktörler arasında yer almaktadır (Tang, Zhang ve Xiao, 2022). Bu durumu ele alan araştırmalar (Tsohou ve Papaioannou, 2021; Ho, Ho-Dac ve Huang, 2023; Punj, 2018) benzer şekilde, olumsuz mahremiyet deneyimi yaşayan bireylerin kişisel bilgilerini ifşa etme konusunda daha isteksiz olduklarını ortaya koymaktadır. Geçmiş mahremiyet ihlali deneyimlerine ait bulgular, mahremiyet ihlallerinin müşteri davranışları üzerindeki geniş kapsamlı etkilerini desteklemektedir (Malhotra, Kim ve Agarwal, 2004).

Mahremiyet ihlali deneyimi yaşayan bireylerin, mahremiyet konusunda daha temkinli oldukları literatürde yaygın olarak desteklenmiştir. Malhotra vd., (2004), bu tür olumsuz deneyimlerin, bireylerin mahremiyet endişelerini artırdığını ortaya koymuştur. Benzer şekilde, Ampong, Mensah, Adu, Addae, Omoregie ve Ofori (2018) araştırmalarında, sosyal ağ platformu kullanıcılarının geçmişte yaşadıkları mahremiyet ihlallerinin, bilgi ifşasına yönelik istekliliklerini azalttığını tespit etmişlerdir. Ayrıca, Metzger'in (2007) araştırması, e-ticaret alanında olumsuz mahremiyet deneyimi yaşamış bireylerin, sonraki kişisel bilgi ifşası kararlarında daha dikkatli davrandıklarını göstermektedir. Özellikle e-ticaret konusunda daha tecrübeli müşterilerin, çevrimiçi platformlarda doğru olmayan veri girişi yapma eğiliminde oldukları belirlenmiştir, bu da mahremiyet endişelerinin bilgi paylaşımına olan etkisine dair bulguları pekiştirmektedir.

Araştırma kapsamında, tüketicinin geçmişte yaşadığı çevrimiçi mahremiyet ihlali deneyimi rasyonel akıl yürütme sürecine etki eden bir faktör olarak ele alınmıştır. Bu doğrultuda tüketicilerin geçmişte yaşadığı mahremiyet ihlali deneyimlerinin bilgi ifşasının algılanan riski ile kişisel bilginin kullanılmasına isteklilik değişkenleri üzerindeki etkisini ölçmek amacıyla oluşturulan hipotezler aşağıdaki gibidir:

H₆: Daha önce yaşanmış mahremiyet ihlali deneyiminin bilgi ifşasının algılanan riski üzerinde anlamlı bir etkisi vardır.

H₇: Daha önce yaşanmış mahremiyet ihlali deneyiminin kişisel bilginin kullanılmasına isteklilik üzerinde anlamlı bir etkisi vardır.

Rasyonel akıl yürütme sürecine etki eden bir diğer önemli faktör, müşterinin çevrimiçi etkileşimde bulunduğu işletme ya da platforma duyduğu güvendir. Güven, bireyin çevrimiçi etkileşimde bulunmadan önce hizmet sağlayıcı ya da işlem ortamı hakkında sahip olduğu olumlu inançlar olarak tanımlanabilir (Kim, Park, Park ve Ahn, 2019, s. 274). Ancak güven kavramı, internet teknolojilerine duyulan güven, satıcıya duyulan güven gibi çeşitli boyutlara sahiptir (McKnight, Choudhury ve Kacmar, 2002). Bu çalışmada güven, kişisel bilgi paylaşımı bağlamında, müşterilerin etkileşimde bulundukları platformların güvenilirliğine duydukları inançları ifade etmektedir.

Çevrimiçi bilgi ifşasında güvenin rolü birçok araştırmanın konusu olmuştur (Chen vd, 2024; Osatuyi, Passerini, Ravarini ve Grandhi, 2018; Wang, Cao ve Zhu, 2024). Veltri, Lupiáñez-Villanueva, Folkvord, Theben ve Gaskell (2020), çevrimiçi arama bilgileri, sözleşmeye taraf olanların detayları ve tüketici koruma ile kullanıcı yorumlarının şeffaflığının artırılmasının tüketici tercihlerine etkisini araştırmışlardır. Bu çalışmanın sonuçları, şeffaflığın müşteri üzerinde güven duygusu yarattığını ve bu güvenin, ürün seçme olasılığını artırdığını göstermektedir. Bu bulgular, güvenin çevrimiçi bilgi ifşası kararlarında önemli bir rol oynadığını ve güvenin artırılmasının müşteri davranışlarını olumlu yönde etkilediğini ortaya koymaktadır.

Yapılan araştırmalar, güvenin rasyonel akıl yürütme sürecine önemli bir etkisi olduğunu ve güvenin artmasının kişisel bilgilerin ifşasına olan istekliliği artırdığını göstermektedir (Bansal, Zahedi ve Gefen, 2016; Malhotra vd., 2004; Craig, Shim, Johnson ve Jiang, 2006). Örneğin, Amin, Johnson, Prybutok ve Koh'un (2024) araştırması, yaşlı bireylerin yapay zekâ destekli bakım robotlarıyla kişisel sağlık bilgilerini paylaşma istekliliğinin, güven duygusunun artmasıyla doğru orantılı olduğunu ortaya koymuştur. Bununla birlikte, mahremiyet endişesi yüksek olan bireyler, güven duygusu artsa dahi bilgi paylaşımı konusunda daha temkinli davranmaktadırlar. Benzer şekilde, Sun, Pelet, Dai ve Ma (2023), sosyal medya platformları üzerinden doğrudan ürün ve hizmet satın alma davranışını incelemiş ve platforma duyulan güvenin, satın alma kararlarını olumlu yönde etkilediğini ifade etmişlerlerdir. Geçmişte yapılan çalışmalardan yola çıkılarak, çevrimiçi unsura duyulan güven faktörünün kişisel bilginin kullanımına isteklilik üzerindeki etkisini ölçmeye yönelik aşağıdaki hipotez oluşturulmuştur:

H₈: Etkileşimde bulunulan çevrimiçi unsura duyulan güven kişisel bilginin kullanılmasına isteklilik üzerinde anlamlı bir etkiye sahiptir.

Rasyonel akıl yürütme sürecinde mahremiyet hesabı teorisine göre, bilgi ifşasının algılanan faydasını ve riskini göz önüne alan kullanıcı bilgi ifşası deneyimine dair bir değer algısına sahip olmaktadır. Bu durum ise kullanıcının kişisel bilgilerinin kullanılmasına istekliliği üzerinde bir etki bırakmaktadır. Araştırma modeli istekliliğin etkileşime devam etme davranışına dönüşeceğini öngörmektedir. Buradaki etkileşime

devam etme davranışı, davranışı gerçekleştirmeye yönelik niyetin gücünün ölçüsüdür (Bansal vd., 2016; Craig vd., 2006). Müşterilerin kişisel bilgilerini ifşa etme istekliliği ile etkileşime devam etme veya ürün satın alma kararları arasındaki ilişkiyi araştıran Ferreyra, Kroll, Aïmeur, Stieglitz ve Heisel (2020), risk farkındalığına dayalı stratejiler kullanarak, müşterilerin olası sonuçları daha iyi anlamalarını sağlamışlardır. Bu yöntem çevrimiçi ortamlarda bilgi ifşası kararlarını olumlu yönde etkilemiştir. Araştırmacılar, risk farkındalığının müşterilerin gizlilik endişelerini azaltarak daha güvenli bir bilgi paylaşımına katkıda bulunduğu vurgulamışlardır. Bu bulgular, kişisel bilginin kullanılmasına olan istekliliğin artmasının çevrimiçi etkileşime devam etme davranışını olumlu yönde etkileyebileceğini göstermektedir. Benzer şekilde, Van Der Schyff ve Flowerday (2023), sosyal medya kullanıcılarının bilgi ifşasından doğabilecek fayda ve risk algılarının, hizmet sağlayıcıya duydukları güven ile özel verilerini ifşa etme niyetleri arasındaki ilişkiyi etkilediğini vurgulamaktadırlar. Bu araştırma sonuçları, kullanıcıların bilgi paylaşma davranışlarının, güvenin yanı sıra fayda ve risk algılarıyla da şekillendiğini göstermektedir. Tüm bu değerlendirmelerden yola çıkılarak, tüketicilerin çevrimiçi ortamda kişisel bilgilerinin kullanılmasına isteklilik halinin etkileşime devam etme davranışı üzerindeki etkisini ölçmeye yönelik araştırma hipotezi aşağıdaki gibi oluşturulmuştur:

H₉: Kişisel bilginin kullanılmasına isteklilik, etkileşime devam etme davranışı üzerinde anlamlı bir etkiye sahiptir.

METODOLOJİ

Araştırmanın Amacı ve Değişkenleri

Araştırmanın amacı hiper-kişiselleştirme uygulamaları sonucu tüketicinin yaşadığı rasyonel bilişsel süreci mahremiyet hesabı teorisi çerçevesinden incelemek ve önceki çevrimiçi mahremiyet tecrübesi ve etkileşimde bulunduğu çevrimiçi unsura duyduğu güvenin kişisel bilgilerinin kullanılmasına duyduğu isteklilik üzerindeki etkisini araştırmaktadır. Kişisel bilginin kullanımına istekliliğin ise çıktı değişken olan tüketicinin etkileşime devam etme davranışına dönüşeceği öngörülmektedir.

Araştırma Modeli

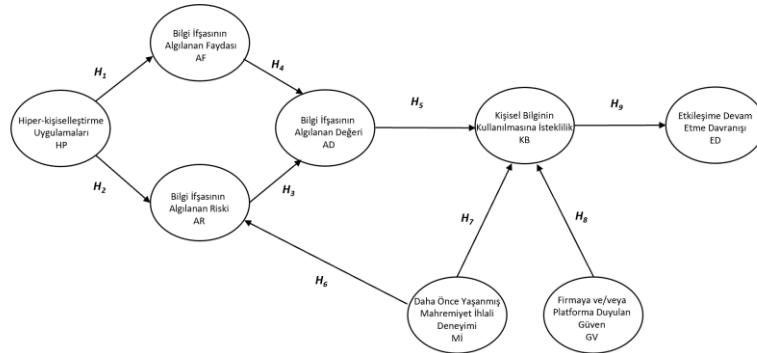
Bu araştırmaya yön veren kavramsal çalışmaların bulguları ışığında bir değerlendirme yapıldığında, çevrimiçi etkileşim esnasında müşterinin bilişsel karar sürecini etkileyen pek çok faktör olduğu anlaşılmaktadır. Etkileşimin gerçekleştiği zaman aralığı, müşterinin fiziksel ve ruhsal durumu, fiziksel ortama ve sosyal ortama dair özellikler, müşterinin varolan algıları, inançları, korkuları, etkileşim esnasında kullanılan teknolojik araçlar üzerindeki hakimiyeti, dijital okuryazarlık oranı gibi pek çok etmen çevrimiçi

etkileşimde müşterinin niyet ve davranışları üzerinde etki yapmaktadır. Araştırma modeli oluşturulurken çevrimiçi ortamda tüketicinin rasyonel, bilişsel düşünme sürecine yoğunlaşmıştır. Modelde kullanılan mahremiyet hesabı teorisi, çevrimiçi etkileşim sürecinde tüketicinin, kişisel bilgilerinin toplanmasının olası negatif ve pozitif sonuçları hakkında içsel bir muhakeme yani mahremiyet hesabı yaptığını vurgulamaktadır. Mahremiyet Hesabı Teorisi, bireylerin davranışsal tepkilerinin gelecekteki sonuçlarını düşündüklerini varsaymaktadır. Bu teoriye göre bireyler zihinlerinde potansiyel olarak rekabet eden faktörleri tartmakta, yani beklenen fayda ve riske yönelik bir analiz yapmaktadır (Li, 2012).

Yapılan literatür taraması sonrasında, çevrimiçi ortamda tüketici davranışlarını etkileyen unsurlar içinden daha önce pek çok araştırmacı tarafından da ele alınmış olan iki önemli faktör göz önüne alınarak modele dahil edilmiştir. Bunlar tüketicinin etkileşimde bulunduğu çevrimiçi unsura duyduğu güven ve daha önce yaşadığı mahremiyet ihlali tecrübesidir (Chen vd, 2024; Osatuyi, Passerini, Ravarini ve Grandhi, 2018; Wang, Cao ve Zhu, 2024; Malhotra vd., 2004).

Hiper-kişiselleştirme uygulamalarıyla bilgi ifşasında bulunan tüketicilerin risk, fayda ve değer algılarının kişisel bilgilerinin kullanımına isteklilik ve takip eden süreçte etkileşime devam etme davranışı üzerindeki etkisini ölçmeyi amaçlayan bu çalışmadaki araştırma modeli Şekil 1’de gösterilmiştir.

Şekil 1: Araştırma modeli



Örneklem ve Veri Toplama Aracı

Parametrik olmayan bir yöntem olan Kısmi En Küçük Kareler Yapısal Eşitlik Modellemesinde (PLS-SEM) örneklem hacminin belirlenmesinde sıklıkla kullanılan “10 kat kuralı” modelde tahmin edilen parametre sayısının 10 katı veya daha büyük olması ölçüsüne dayanmaktadır (Hair, vd. 2011). Bu çalışmada tahmin edilecek parametre sayısı 21 olduğundan 10 kat kuralına göre örneklem hacminin 210’dan fazla olması gerekmektedir. Çalışmanın örneklem büyüklüğü için yapılan güç analizinde, istenilen güç düzeyi

0.80 ve etki gücü 0.40 olmak üzere %95 güven düzeyinde minimum örneklem büyüklüğü 149 olarak hesaplanmıştır. Bu nedenle çalışmadaki $n = 400$ örneklem büyüklüğü yeterli olarak bulunmuştur. Araştırma, kolayda örnekleme yöntemi ile seçilmiş 18 yaş ve üzeri internet üzerinden alışveriş yapan veya en az bir dijital platforma üye olan bir diğer ifade ile düzenli çevrimiçi etkileşim tecrübesi olan 400 tüketici ile gerçekleştirilmiştir. Çevrimiçi (online) uygulanan anket formu tüketicilere elektronik posta ve whatsapp ile iletilmiş ve tüketiciler tarafından gönüllülük esasına uygun olarak veriler toplanmıştır. Ankete katılan tüketicilerin çevrimiçi alışveriş ve üyelik deneyimlerine ilişkin bilgiler Ek 1’de verilmiştir.

Bu çalışma için ihtiyaç duyulan verilerin elde edilmesi amacıyla üç bölümden oluşan bir anket formu hazırlanmıştır. Araştırma modeli kapsamındaki değişkenlere ilişkin ölçekler yapılan literatür incelenmesi sonucunda ilgili çalışmalardan uyarlanarak anket formu oluşturulmuştur. Tüm ölçeklerde 5’li Likert ölçeği kullanılmıştır. Anket formunun birinci kısmında yer alan sorular katılımcıların demografik özelliklerini belirlemeye yöneliktir. Anket formunun ikinci kısmında yer alan ifadeler katılımcıların çevrimiçi etkileşim esnasındaki hiper-kişiselleştirme uygulamaları sonucunda algılanan fayda, risk ve değer ile kişisel bilginin kullanımına isteklilik ve sonrasında etkileşime devam etme davranışını ölçmeye yöneliktir. Hiper-kişiselleştirme uygulamalarına yönelik 3 ifade Xu, Lou, Carroll ve Rosson (2011), bilgi ifşasının algılanan faydasına ait 3 ifade Unni ve Harmon (2007), bilgi ifşasının algılanan riskine ait 3 ifade Dinev ve Hart (2006), bilgi ifşasının algılanan değerine ait 3 ifade Kim, Chan ve Gupta (2007), kişisel bilginin kullanımına istekliliğe ait 2 ifade Culnan ve Armstrong (1999) ve etkileşime devam etme davranışına ait 2 ifade Xu vd. (2011)’den uyarlanmıştır. Anket formunun üçüncü kısmında yer alan ifadeler ise araştırma modelinde rasyonel akıl yürütme sürecinin öncülleri olan daha önce yaşanmış mahremiyet ihlali deneyimi ile işletme ve/veya platforma duyulan güveni ölçmeye yöneliktir. Daha önce yaşanmış mahremiyet ihlali deneyimine ait 2 ifade Smith, Milberg ve Burke (1996) ve güven unsuruna ait 5 ifade ise Harris ve Goode (2010)’nin çalışmasından uyarlanmıştır.

Çalışma için Anadolu Üniversitesi Etik Kurulunun 30.05.2023 tarihli ve 524149 nolu kararı ile etik kurul onayı alınmıştır.

Araştırmanın Yöntemi

Araştırmada bağımsız değişkenlerin bağımlı değişkenler üzerindeki etkisini test etmek amacıyla ikinci nesil çok değişkenli istatistik analiz tekniklerinden biri olan Kısmi En Küçük Kareler Yapısal Eşitlik Modellemesi (PLS-SEM) kullanılmıştır. PLS-SEM, doğrudan gözlemlenemeyen ancak çeşitli göstergeler yardımıyla dolaylı olarak ölçülebilen gizil değişkenler ile gözlenen değişkenler arasındaki karmaşık ilişkilerin modellenmesinde yinelemeli, regresyona dayalı parametrik olmayan ve çok değişkenli bir analiz

teknigi (Yılmaz ve Kınaş, 2021: 138). PLS-SEM’ in tercih edilmesinin nedenleri normal dağılım varsayımına sahip olmaması, küçük örneklemelerde dahi sonuç üretebilmesi, modeldeki faktörün tek bir ifadeden oluşması durumunda dahi çalışabilmesi ve en önemli avantajı ise hem yansıtıcı (reflective) hem de biçimlendirici (formative) yapıları açıklamada kullanılabilmektedir (Çakır, 2019 :116).

Yansıtıcı (reflective) yapılarda nedensellik gizil yapıdan gözlenen yapılara doğru iken biçimlendirici (formative) yapılarda nedensellik gözlenen yapılardan gizil yapıya doğrudur. Sosyal bilimler alanında yapılan çalışmalarda değişkenler ağırlıklı olarak yansıtıcı (reflective) yapıdadır (Yıldız, 2021). Bu çalışmada önerilen araştırma modelinin değişkenleri de yansıtıcı (reflective) yapıdadırlar. Araştırmanın ölçüm ve yapısal modeli SmartPLS v.4.1.0.4 programı kullanılarak analiz edilmiştir.

ARAŞTIRMA VERİLERİNİN ANALİZİ ve BULGULAR

Tanımlayıcı İstatistikler

Araştırmaya katılan 400 katılımcıya ait tanımlayıcı istatistikler Tablo 1’de verilmiştir.

Tablo 1: Tanımlayıcı istatistikler

Değişken	Düzey	Frekans	Yüzde
Cinsiyet	Kadın	183	45,75
	Erkek	217	54,25
Yaş	18-26	164	41,0
	27-42	106	26,5
	43-58	92	23,0
	59-77	38	9,5
Eğitim Durumu	İlköğretim	35	8,75
	Lise	142	35,5
	Önlisans	67	16,75
	Lisans	143	35,75
	Lisansüstü	13	3,25
Toplam		400	100

PLS-SEM parametrik olmayan bir istatistiksel yöntem olduğundan verilerin normal dağılımı gerekliliği bulunmamaktadır. Normallikten aşırı derecede uzak olan verilerin analiz sonuçlarının değerlendirilmesi açısından sorun yaratmaması amacıyla verilerin normal dağılıp dağılmadığının test

edilmesi önemlidir (Hair vd., 2014). Bu nedenle araştırma değişkenlerine ait verilerin betimleyici istatistikleri Tablo 2’de verilmiştir. Değişkenlerin çarpıklık ve basıklık değerlerinin bazılarının -1 ve +1 aralığının dışında kalması nedeniyle veriler normal dağılmamaktadır.

Tablo 2: Değişkenlerin normallik analizi sonuçları

Faktör	Madde	Ortalama	Standart Sapma	Çarpıklık	Basıklık
Algılanan Değer (AD)	AD1	3.215	1.052	-0.075	-0.765
	AD2	3.100	0.915	-0.140	-0.369
	AD3	3.418	0.998	-0.303	-0.315
Algılanan Fayda (AF)	AF1	3.448	0.880	-0.405	0.110
	AF2	3.650	0.911	-0.851	0.842
	AF3	3.223	0.933	-0.228	-0.298
Algılanan Risk (AR)	AR1	3.570	0.920	-0.207	-0.269
	AR2	3.580	0.962	-0.415	-0.263
	AR3	3.588	0.854	-0.093	-0.263
Etkileşime Devam (ED)	ED1	3.188	0.977	-0.173	-0.572
	ED2	3.290	0.879	-0.111	-0.354
Güven (GV)	GV1	3.083	1.081	-0.057	-0.803
	GV2	3.258	0.924	-0.322	0.114
	GV3	3.433	0.882	-0.653	0.693
	GV4	3.220	0.874	-0.330	0.170
	GV5	3.298	0.968	-0.342	-0.081
Hiper-kişiselleştirme Uygulamaları (HP)	HP1	3.653	1.012	-0.720	0.254
	HP2	3.928	0.886	-1.011	1.231
	HP3	3.883	0.920	-1.039	1.381
Kişisel Bilginin Kullanımı (KB)	KB1	2.623	1.036	0.316	-0.508
	KB2	3.033	1.147	-0.365	-0.906
Mahremiyet İhlali (Mİ)	Mİ1	2.410	0.921	0.624	-0.018
	Mİ2	3.435	1.046	-0.573	-0.369

Ortak Yöntem Varyansı

Ortak yöntem varyansı ankete dayalı çalışmalarda katılımcıların yanıtlama biçimleri, madde özellikleri ile ölçümler aynı veya benzer yöntemler kullanılarak toplandığında çalışma bulgularının

geçerliliğini tehdit eden sistematik hata varyansı olarak tanımlanmaktadır (Podsakoff, MacKenzie ve Podsakoff, 2012). Ortak yöntem yanlılığının olup olmadığını test etmede Harman'ın tek faktör testi literatürde sıklıkla kullanılmaktadır (Kock, Berbekova ve Assaf, 2021). Harman'ın tek faktör testinde eşik değer olan %50'nin üzerinde çıkan sonuçlar ortak yöntem varyansının varlığını göstermektedir (Aguirre-Urreta ve Hu, 2019). SPSS programı üzerinde açıklayıcı faktör analizi aracılığıyla çıkarım metodu olarak ana eksen faktörleştirme metodu (principal axis factoring) seçilmiş ve herhangi bir faktör döndürme metodu seçilmeden analiz yapılmıştır. Elde edilen sonuçlar incelendiğinde, tüm ifadelerin tek bir faktöre bağlanması sonucunda açıklanan toplam varyansın %21,02 olduğu görülmüştür. Bu sonuç çalışma kapsamında kullanılan ifadelerin oluşturduğu tek bir faktörün değişkenler arasındaki kovaryansın çoğunluğunu açıklamadığından, bu çalışmada ortak yöntem yanlılığının olmadığını doğrulamaktadır.

Ölçüm Modeli

PLS-SEM' de analizler ölçüm modeli ve yapısal model olarak iki aşamada gerçekleştirilmektedir. Ölçüm modeli, gözlenen değişkenler ve gizil değişkenler arasındaki ilişkileri değerlendirmektedir. PLS-SEM'de doğrulayıcı faktör analizi için ölçüm modeli kullanılmaktadır. Ölçüm modelinin değerlendirilmesinde öncelikle araştırmada kullanılan ölçeklerin yakınsak ve ayrışma geçerliliğine bakılmıştır.

Değişkenlere ait ifadelerin birbirleri ve oluşturdukları faktör ile ilişkilerini ifade eden yakınsak geçerliliği için ölçeğe ilişkin tüm CR (Composite Reliability) değerlerinin 0,7'den ve aynı zamanda AVE (Average Variance Extracted) değerlerinden, AVE değerlerinin de 0,5'ten büyük olması gerekmektedir (Hair, vd. 2014). Tablo 2'de değişkenlere ait birleşik güvenirlik (CR) ve çıkarılan ortalama varyans (AVE) değerleri verilmiştir. Tablo 2'den görüleceği üzere değişkenlere ait tüm CR değerleri 0,7'den ve aynı zamanda AVE değerlerinden büyüktür. AVE değerlerinin de 0,5'den büyük olduğu Tablo 3'den görülmektedir.

Tablo 3: CR ve AVE değerleri

	Birleşik Güvenilirlik (CR)	Çıkarılan Ortalama Varyans (AVE)
AD	0.774	0.539
AF	0.791	0.564
AR	0.884	0.718
ED	0.866	0.764
GV	0.852	0.540
HP	0.912	0.776
KB	0.902	0.821
Mİ	0.789	0.662

Yakınsak geçerliliği için aynı zamanda faktör yüklerine bakılmaktadır. PLS-SEM’de ölçeğin güvenilirlik ve geçerliliğinin sağlanması için faktör yüklerinin 0,60’dan yüksek olması gerekmektedir (Hulland, 1999). Tablo 4’de verilen faktör yükleri incelendiğinde, faktör yükü 0,60’ın altında kalan AF’den 1, AD’dan 1 ve GV’dan 1 ifade çıkarılmıştır.

Tablo 4: Faktör yükleri

	AD	AF	AR	ED	GV	HP	KB	Mİ
AD1	0.807							
AD2	0.812							
AD3	0.555							
AF1		0.598						
AF2		0.885						
AF3		0.741						
AR1			0.823					
AR2			0.867					
AR3			0.851					
ED1				0.813				
ED2				0.932				
GV1					0.528			
GV2					0.738			
GV3					0.806			
GV4					0.794			
GV5					0.770			

HP1	0.848	
HP2	0.905	
HP3	0.888	
KB1		0.919
KB2		0.893
Mİ1		0.967
Mİ2		0.624

Tablo 5’de modelden çıkarılan ifadeler sonrasında değişkenlere ait Cronbach Alfa, CR ve AVE değerleri verilmiştir. Tablo 5 incelendiğinde, $CR > 0,70$, $AVE > 0,50$ ve aynı zamanda $CR > AVE$ olduğundan yapıların yakınsak geçerliliği tatmin edici düzey olduğu söylenebilir. Faktörlerdeki ifadelerin güvenilirliğini test etmek için hesaplanan rho_A değerleri tüm faktörler için 0.70’in üzerinde bulunmuştur.

Tablo 5: Yapı güvenilirliği ve geçerliliği

Faktör	Madde	Standartlaştırılmış Madde Yükleri	rho_A	Cronbach Alfa (CA)	Birleşik Güvenilirlik (CR)	Çıkarılan Ortalama Varyans (AVE)
Algılanan Değer (AD)	AD1	0.794	0.703	0.710	0.830	0.711
	AD2	0.889				
Algılanan Fayda (AF)	AF2	0.895	0.709	0.705	0.869	0.768
	AF3	0.857				
Algılanan Risk (AR)	AR1	0.810	0.838	0.805	0.883	0.715
	AR2	0.860				
	AR3	0.866				
Etkileşime Devam (ED)	ED1	0.813	0.817	0.706	0.866	0.764
	ED2	0.932				
Güven (GV)	GV2	0.752	0.826	0.815	0.877	0.641
	GV3	0.820				
	GV4	0.834				
	GV5	0.793				
Hiper-kişiselleştirme Uygulamaları (HP)	HP1	0.842	0.861	0.855	0.912	0.776
	HP2	0.905				
	HP3	0.894				
	KB1	0.920	0.792	0.783	0.902	0.821

Kişisel Bilginin Kullanımı (KB)	KB2	0.892				
Mahremiyet İhlali (Mİ)	Mİ1	0.966	0.889	0.713	0.790	0.663
	Mİ2	0.726				

Ayrışma geçerliliği için Fornell ve Larcker (1981) kriterleri ile Henseler vd., (2015) tarafından PLS-SEM için önerilen Heterotrait-Monotrait (HTMT) değerleri test edilmiştir. Tablo 6’da Fornell-Larcker kriterleri verilmiştir. Wong (2013)’a göre Fornell Larcker değerlerinin gizil değişkenlere ait satırlardaki ve sütunlardaki korelasyon değerlerinden daha yüksek olması koşulunun sağlanması gerekmektedir. Tablo 6’ daki değerlere göre ayrışma geçerliliği sağlanmaktadır.

Tablo 6: Ayrışma geçerliliği (Fornell-Larcker kriterleri)

	AD	AF	AR	ED	GV	HP	KB	Mİ
AD	0.843							
AF	0.438	0.876						
AR	0.192	-0.008	0.846					
ED	0.157	0.364	-0.142	0.874				
GV	0.203	0.37	-0.191	0.409	0.800			
HP	0.114	0.31	0.19	0.081	0.247	0.881		
KB	0.479	0.406	-0.185	0.427	0.44	0.15	0.906	
Mİ	0.145	0.005	0.107	0.077	0.119	0.004	0.14	0.814

Ayrışma geçerliliğini sağlanmasındaki bir kriter olan HTMT kriterine ait değerler Tablo 7’de sunulmuştur. Henseler vd. (2015), HTMT değerinin 0,85’in altında olması gerektiğini belirtmişlerdir.

Tablo 7: Heterotrait-Monotrait Oranı (HTMT)

	AD	AF	AR	ED	GV	HP	KB	Mİ
AD								
AF	0.662							
AR	0.380	0.077						
ED	0.230	0.499	0.191					
GV	0.261	0.472	0.220	0.539				
HP	0.152	0.391	0.216	0.146	0.294			
KB	0.658	0.548	0.244	0.550	0.537	0.190		
Mİ	0.227	0.141	0.162	0.135	0.255	0.222	0.148	

Ayrışma geçerliğinin sağlanabilmesi için ayrıca çapraz yüklere bakılmıştır. Belirli bir ifadenin çalışmadaki diğer yapılara kıyasla kendi ana yapısında daha yüksek yüklere sahip olması gerekmektedir (Chin, 1998).

Tablo 8: Çapraz yükler

	AD	AF	AR	ED	GV	HP	KB	Mİ
AD1	0.795	0.284	0.401	0.020	0.035	0.022	0.263	0.173
AD2	0.889	0.438	-0.017	0.219	0.276	0.153	0.515	0.084
AF2	0.362	0.895	-0.018	0.323	0.305	0.357	0.347	0.008
AF3	0.410	0.857	0.006	0.315	0.348	0.174	0.366	-0.001
AR1	0.139	-0.026	0.810	-0.020	-0.147	0.122	-0.130	0.069
AR2	0.152	-0.065	0.86	-0.224	-0.190	0.123	-0.199	0.114
AR3	0.187	0.050	0.866	-0.11	-0.151	0.215	-0.143	0.087
ED1	0.105	0.251	-0.146	0.813	0.357	0.035	0.275	0.111
ED2	0.161	0.367	-0.113	0.932	0.366	0.095	0.443	0.042
GV2	0.243	0.303	-0.171	0.429	0.752	0.162	0.351	-0.049
GV3	0.115	0.247	-0.102	0.351	0.820	0.143	0.309	0.109
GV4	0.118	0.204	-0.068	0.255	0.834	0.220	0.270	0.179
GV5	0.155	0.380	-0.225	0.269	0.793	0.249	0.430	0.147
HP1	0.082	0.285	0.107	0.157	0.331	0.842	0.166	0.087
HP2	0.104	0.240	0.201	0.006	0.179	0.905	0.138	-0.065
HP3	0.113	0.292	0.189	0.057	0.154	0.894	0.097	-0.008
KB1	0.563	0.386	-0.059	0.384	0.335	0.091	0.919	0.166
KB2	0.289	0.348	-0.291	0.391	0.472	0.187	0.894	0.084
Mİ1	0.155	-0.036	0.095	0.074	0.082	-0.061	0.162	0.966
Mİ2	0.044	0.123	0.093	0.051	0.172	0.197	0.007	0.627

Tablo 8'deki çapraz yükler incelendiğinde her bir ifadenin ilgili olduğu faktörle en yüksek korelasyona sahip olduğu, dolayısıyla ayrışma geçerliğinin sağlandığı görülmektedir.

Yapısal Model

Yapısal model aşamasında model bir bütün olarak değerlendirilerek hipotez testleri yapılmıştır. Çalışmanın hipotezlerini test etmeden önce, eş doğrusallık olup olmadığını araştırmak için VIF değerleri kullanılmıştır. VIF değerinin 5'ten büyük olması durumunda, regresyon modelinin çalışmasında eş

doğrusallık sorunları olduğu varsayılmaktadır (Hair vd., 2017). Tüm dışsal gizil değişkenler için VIF değerleri 1 ile 1.059 arasında değişmektedir. Dolayısıyla $VIF < 5$ olduğundan değişkenler arasında eş doğrusallık bulunmamaktadır.

SmartPLS programında hipotez testleri için bootstrapping (yeniden örnekleme) tekniği kullanılmaktadır. Yeniden örneklemede, orijinal örneklemden sürekli rasgele seçim yapılarak aynı boyutta yeni örneklem elde edilmekte ve seçilen örneklem her seferinde geri konmaktadır (Yıldız, 2021). Alt örneklem için 5.000 sayısı önerilmektedir (Hair vd. 2017). Yapılan yeniden örnekleme ile elde edilen hipotez testlerinin sonuçları Tablo 9’da verilmiştir.

Tablo 9: Hipotez testi sonuçları

Hipotezler	Yol Katsayısı(β)	Std.Sapma	t-değerleri	p-değerleri	Karar
H1	0.310	0.055	5.648	0.000*	Kabul
H2	0.189	0.062	3.071	0.002*	Kabul
H3	0.439	0.054	8.082	0.000*	Kabul
H4	0.195	0.065	2.988	0.003*	Kabul
H5	0.403	0.049	8.203	0.000*	Kabul
H6	0.106	0.058	1.824	0.068	Ret
H7	0.041	0.042	0.644	0.519	Ret
H8	0.353	0.044	8.363	0.000*	Kabul
H9	0.427	0.046	9.219	0.000*	Kabul

* $p < 0,05$

Tablo 9’daki bulgular değerlendirildiğinde hiper-kişiselleştirme uygulamalarının mahremiyet hesabı çerçevesinde algılanan fayda ($\beta = .310$, $p = .000$) ve algılanan risk ($\beta = .189$, $p = .002$) üzerinde pozitif yönde anlamlı bir etkisi olduğu görülmüştür. Algılanan faydanın algılanan değer üzerinde ($\beta = .439$, $p = .000$) ve algılanan riskin algılanan değer üzerinde ($\beta = .195$, $p = .003$) pozitif yönde anlamlı bir etkisi vardır. Algılanan değer kişisel bilginin kullanımına isteklilik üzerinde pozitif yönde anlamlı etkisi vardır ($\beta = .403$, $p = .000$). Modeldeki öncüllerden biri olan daha önce yaşanmış mahremiyet ihlali deneyiminin algılanan risk ve kişisel bilginin kullanımına isteklilik değişkenleri üzerinde bir anlamlı bir etkisinin olmadığı görülmüştür.

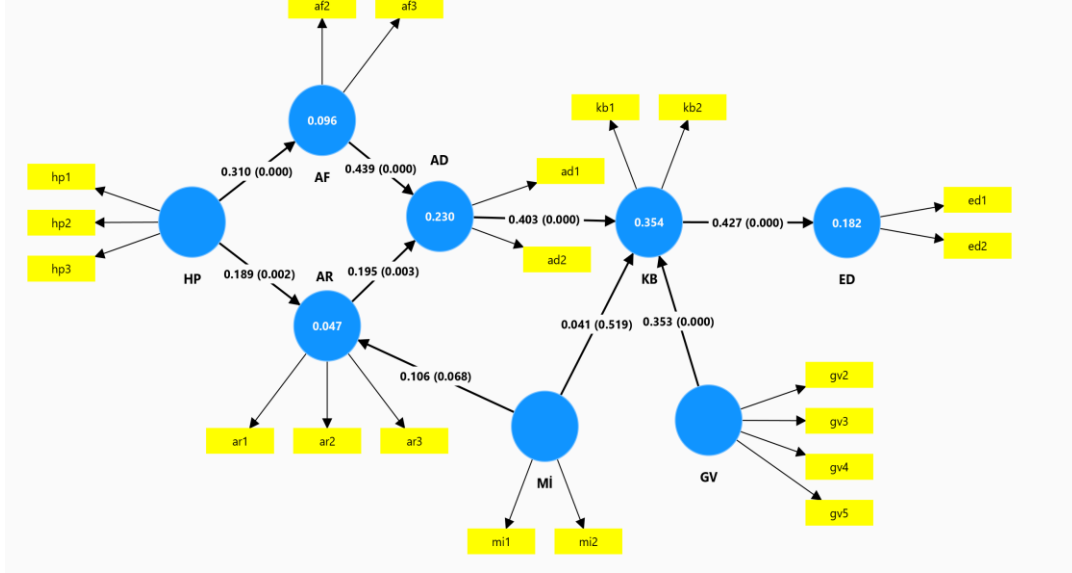
Modele dahil edilen bir diğer öncül olan firmaya ve/veya platforma duyulan güven unsurunun kişisel bilginin kullanımına isteklilik üzerinde pozitif yönde anlamlı bir etkisi vardır ($\beta = .353$, $p = .000$). Kişisel bilginin kullanımına istekliliğin ise etkileşime devam etme davranışı üzerinde pozitif yönde anlamlı bir etkiye sahip olduğu söylenebilir ($\beta = .427$, $p = .000$).

Yapısal modelin bir diğer değerlendirilmesi ise modelin tahmin yeteneğinin bir göstergesi olan Q^2 değeridir. Yapısal modelin tahmin geçerliliğinin sağlanabilmesi için Q^2 değerinin sıfırdan büyük olması yeterlidir (Chin, 1998). Yapılan analiz sonucunda çalışmanın bağımlı değişkenleri olan Kişisel Bilginin Kullanımına İsteklilik değişkenine ait Q^2 değeri 0,187 ve Etkileşime Devam Etme Davranışı değişkenine ait Q^2 değerinin 0,103 olduğunu görülmüştür. Q^2 değerlerinin sıfırdan büyük olması modelin tahmin geçerliliği için yeterlidir. Bir diğer ifadeyle model orijinal gözlenen değişkenleri iyi bir şekilde tahmin etmektedir.

Hem ölçüm modeli hem de yapısal modelin performansını belirlemek ve tüm modelin tahmin performansını için Tenenhaus vd. (2004) tarafından önerilen standart bir ölçü olan GoF uyum iyiliği indeksi kullanılmaktadır. GoF değeri, AVE'lerin ortalaması ile R^2 'lerin ortalamasının çarpımının karekökü ile hesaplanmaktadır ($GoF = \sqrt{AVE \times R^2}$). GoF değerinin değerlendirilmesi $GoF < 0,10$ (az), $0,10 < GoF < 0,25$ (orta) ve $0,25 < GoF < 0,36$ (iyi) şeklindedir (Wetzels, Odekerken-Schröder ve van Oppen, 2009). GoF değerinin 0.36'dan büyük olması modelin iyi uyuma sahip olduğunun bir göstergesidir. Araştırma modelimize ait GoF değeri 0,37 olarak bulunmuştur.

Modelin açıklayıcı gücü olan R^2 değeri, algılanan fayda değişkeni için .096, algılanan risk için .047, algılanan değer için .230, kişisel bilginin kullanımına isteklilik için .354 ve etkileşime devam etme davranışı için .182 olarak bulunmuştur. Tahmin edici PLS-SEM yaklaşımının dışsal gizil değişkenlerin varyansını açıklamak olduğundan anahtar hedef yapıların yüksek R^2 değerine sahip olması gerekmektedir (Hair vd. 2011:147). Ayrıca Hair vd. (2011), R^2 değerinin yüksek olduğuna dair kararın araştırma disiplinine bağlı olduğunu ve tüketici davranışı ile ilgili araştırmalarda 0.20'lik bir R^2 değerinin yüksek kabul edilebileceğini ifade etmişlerdir. Şekil 2'de görüldüğü gibi, mahremiyet hesabı teorisi çerçevesinde hiper-kişiselleştirme uygulamaları kişisel bilginin kullanımını %35,4 oranında açıklamaktadır.

Şekil 2: Yapısal model



f^2 değerleri bağımsız değişkenlerin bağımlı değişken üzerindeki etkisini açıklamaktadır (Yıldız, 2021). Cohen vd. (2003) f^2 ile ilgili olarak .02 ise düşük, .15 ise orta, .35 ise yüksek şeklinde bir değerlendirme yapmıştır. f^2 değerleri incelendiğinde kişisel bilginin kullanımına isteklilik değişkeni üzerinde en yüksek etkiye algılanan fayda değişkeni olduğu görülmektedir. Kişisel bilginin kullanımına isteklilik değişkeninin etkileşime devam etme davranışı üzerindeki etkisi ise yüksek düzeydedir. Araştırma modeli etki gücüne ait f^2 değerleri Tablo 10’da verilmiştir.

Tablo 10: f^2 değerleri

AD -> KB	0.724
AF -> AD	0.868
AR -> AD	0.147
GV -> KB	0.333
HP -> AF	0.187
HP -> AR	0.053
KB -> ED	0.392
MI -> AR	0.013
MI -> KB	0.000

SmartPLS programında modelin uyum değerleri olarak SRMR (Standartized Root Mean Square Residual) ve NFI (Normed Fitted Index) değerleri raporlanmaktadır. Hu ve Bentler (1999), SRMR için 0,080’in altında ve NFI içinde 0,80’in üzerindeki değerleri iyi uyum değerleri olarak tanımlamaktadır.

Yapılan analiz sonucunda $SRMR=0,072<0,080$ ve $NFI=0,828>0,80$ hesaplandığından yapısal modelin yeterli uyuma sahip olduğu görülmektedir.

SONUÇ ve ÖNERİLER

Bu çalışmada hiper-kişiselleştirme uygulamalarının çevrimiçi mahremiyet ile ilişkisi, mahremiyet hesabı teorisi çerçevesinde incelenerek tüketicilerin çevrimiçi etkileşime devam etme davranışına etkisi araştırılmıştır. Araştırma kapsamında geliştirilen model, çevrimiçi tüketicilerin hiper-kişiselleştirme uygulamaları karşısında algıladıkları fayda, risk ve değer muhakemesinin, etkileşime devam etme davranışını nasıl etkilediğini incelemiştir. Çalışmanın sonuçları, hiper-kişiselleştirme uygulamalarının, bilgi ifşasının algılanan fayda ve risk ve değeri üzerinde anlamlı bir etkisi olduğunu göstermiştir. Bu veriler mahremiyet hesabı teorisinin öngördüğü rasyonel akıl yürütme sürecine ilişkin çalışma sonuçları ile uyumludur (Al-Jabri vd., 2019; Baek vd., 2014; Belanger ve James, 2020; Bleier ve Eisenbeiss, 2015; Culnan ve Armstrong, 1999; Culnan ve Bies, 2003; Dinev ve Hart, 2006; Kim vd., 2019; Princi ve Krämer, 2020; Tang vd., 2022; Tian vd., 2022; Wang vd., 2022; White, 2004). Rasyonel akıl yürütme sürecinde bilgi ifşasının algılanan değerinin kişisel bilginin kullanımına isteklilik üzerinde anlamlı bir etki yaptığına ve bunun da etkileşime devam etme davranışı üzerinde anlamlı bir etki oluşturduğuna dair hipotezler araştırma sonuçlarıyla desteklenmiştir. Bu, yapılan literatür taraması sonucu işaret edilen araştırmaların (Ferreya vd., 2020; Van Der Schyff vd., 2023) sonuçlarıyla uyumludur.

Ayrıca işletmeye/platforma duyulan güven faktörünün müşterinin kişisel bilgilerinin kullanılmasına istekliliği üzerinde pozitif yönde anlamlı etkisi vardır. Çalışma sonuçları, çevrimiçi güven faktörünün kişisel bilginin kullanılmasına isteklilik üzerinde pozitif yönde anlamlı bir etkisi olduğunu ortaya koymuştur. Bu bulgu, tüketicilerin güven duydukları platformlarda kişisel bilgilerini paylaşma konusunda daha rahat olduklarını vurgulayan araştırma sonuçları (Bansal vd., 2016; Chen vd., 2024; Craig vd., 2006; Malhotra vd., 2004; McKnight vd., 2002; Osatuyi vd., 2018; Sun vd., 2023; Veltri vd., 2020; Wang vd., 2024) ile uyumludur.

Araştırma hipotezleri içinde desteklenmeyen iki hipotez bulunmaktadır; daha önce tüketicinin yaşamış olduğu çevrimiçi mahremiyet ihlali deneyimi tüketicinin bilgi ifşasına dair algıladığı riski artırmamakta, ayrıca kişisel bilginin kullanılmasına isteklilik üzerinde de anlamlı bir etki yapmamaktadır. Daha önce yaşanmış mahremiyet ihlali deneyimlerinin, kişisel bilgilerinin kullanımına isteklilik üzerinde anlamlı bir etkisinin olmadığı bulgusu, bu deneyimlerin her zaman doğrudan müşteri davranışlarına doğrudan etki etmediğini ortaya koymaktadır. Bu veriler ışığında, daha önce yaşanmış mahremiyet ihlali deneyiminin müşteri algıları üzerindeki etkilerini anlamaya yönelik farklı araştırmalar yapılabilir. Rasyonel

akıl yürütmede yaşanan sınırlamalar, iyimserlik önyargısı, riskle başa çıkma becerilerine duyulan aşırı güven gibi unsurlar daha önce de birçok araştırma kapsamında (Baek vd., 2014; Boerman vd., 2018; Helweg-Larsen ve Shepperd, 2001; Jensen vd., 2005; Klein ve Helweg-Larsen, 2002) incelenmiştir. Gelecekte bu unsurların hiper-kişiselleştirme ve mahremiyet algısı üzerindeki etkilerini anlamaya yönelik çalışmaların daha da önem kazanacağı öngörülmektedir. Acquisti, Brandimarte ve Loewenstein (2015), bireylerin her zaman kendi çıkarları doğrultusunda mahremiyetle ilgili karmaşık dengelemeleri yönetemeyeceğini vurgularlar. Çoğu zaman, bireyler hangi bilgileri paylaştıklarının farkında olmazlar, bu bilgilerin nasıl kullanılabileceğini bilmezler ve nadiren tüm sonuçları bildiklerinde bile, kendi tercihleri hakkında kararsız olabilirler. Öte yandan, daha önce yaşanmış mahremiyet ihlali deneyiminin algılanan risk üzerinde doğrudan bir etkisinin olmaması literatürdeki bazı çalışmalarla (Baek vd., 2014; Klein ve Helweg-Larsen, 2002) örtüşmekle birlikte, bu konuda daha fazla araştırma yapılması gerektiği sonucuna varılmıştır.

SINIRLILIKLAR ve GELECEKTE YAPILACAK ÇALIŞMALAR İÇİN ÖNERİLER

Bu araştırmanın örneklemini Türkiye’de yaşayan 18 yaş üstü bireylerle sınırlıdır. Bu nedenle, daha geniş ve farklı demografik özelliklere sahip bir örnekleme yapılacak araştırmalar literatüre önemli katkılar sağlayabilir. Ayrıca, çalışmanın tasarımında yalnızca belirli değişkenlerin ele alınmış olması, diğer potansiyel etkileyici faktörlerin göz ardı edilmesine neden olmuştur. Gelecekte yapılacak araştırmalarda, tüketici kişilik özellikleri, internet kullanım alışkanlıkları ve sosyal çevre gibi faktörlerin de modele dahil edilmesi önerilmektedir. Gelecekte yapılacak çalışmalarda hiper-kişiselleştirme uygulamaları ve mahremiyet paradoksu ilişkisi daha hassas bilgiler içeren banka, sağlık ve e-devlet gibi uygulamalar özelinde ele alınabilir.

Bu çalışmadan elde edilen bulgular, çevrimiçi pazarlama stratejilerini şekillendiren işletmeler için önemli bilgiler sunmaktadır. İşletmeler, tüketicilerin güvenini kazanarak kişisel verilerin toplanması konusunda daha başarılı olabilirler. Ayrıca, hiper-kişiselleştirme uygulamalarını kullanırken tüketicilerin fayda algılarını artırmaya yönelik stratejiler geliştirmeleri önerilmektedir. En çok kullanılan e-ticaret siteleri ve sosyal medya platformları müşterilerinin kişisel bilgilerin kullanımı üzerindeki kontrollerini artıran seçenekler sunmaktadır. Bu ve benzeri düzenlemelerin müşterilerin mahremiyet endişeleri üzerindeki etkileri birçok araştırmaya (Brandimarte vd., 2013; Martin vd., 2017; Mousavi vd., 2020) konu olmuştur. Türkiye’deki e-ticaret siteleri ve sosyal medya platformlarının benzer düzenlemelerinin mahremiyet endişesi üzerindeki etkileri derinlemesine araştırılabilir. Kişisel Verileri Koruma Kurumu’nun (KVKK), kişisel veri toplama süreçlerinde mahremiyet endişelerini gidermek için daha şeffaf politikalar geliştirmeleri konusunda işletmeleri yönlendirmesi ve özellikle Türkiye bağlamında, kişisel bilgilerin kullanımında

mahremiyetin korunması ile ilgili düzenlemelere uyumun sağlanması yönündeki çalışmalara öncelik vermesi önem arz etmektedir.

Sonuç olarak, önerilen modelin genişletilmesi ve farklı coğrafyalarda ve demografik gruplar arasında test edilmesi, hiper-kişiselleştirme ve çevrimiçi mahremiyet üzerine literatüre önemli katkılar sağlayabilir. Gelişen teknolojik araç ve uygulamalar karşısında tüketicilerin çevrimiçi ortamdaki tecrübeleri de gün geçtikçe biçim değiştirmektedir. Bu nedenle tüketicilerin fayda, risk ve değer algılarının da süreç içinde değişime uğrama olasılığı vardır. Tüketicilerin çevrimiçi platformlara yönelik algılarının zaman içerisindeki değişimini inceleyen boylamsal araştırmalar, bu alandaki bilgi birikimini derinleştirecektir.

YAZAR BEYANI / AUTHOR STATEMENT

Araştırmacılar makaleye ortak olarak katkıda bulunduğunu bildirmiştir. Araştırmacılar herhangi bir çıkar çatışması bildirmemiştir. Bu çalışma için Anadolu Üniversitesi Etik Kurulu'nun 30/05/2023 tarihli toplantısında 524149 nolu kararı ile etik kurul onayı alınmıştır. Bu çalışma Anadolu Üniversitesi Bilimsel Araştırma Projeleri Koordinasyon Birimi Koordinatörlüğü'nün SBA-2023-1880 numaralı projesi ile desteklenmiştir.

Researchers have jointly contributed to the article. Researchers have not declared any conflict of interest. For this study, ethics committee approval was obtained from the Ethics Committee of Anadolu University, based on Decision No. 524149 taken at the committee meeting dated 30 May 2023. This study was supported by the Anadolu University Scientific Research Projects Coordination Unit Coordinatorship with the project numbered SBA-2023-1880.

KAYNAKÇA

- Ackermann, K. A., Burkhalter, L., Mildenerger, T., Frey, M. & Bearth, A. (2022). Willingness to share data: Contextual determinants of consumers' decisions to share private data with companies. *Journal of Consumer Behaviour*, 21(2), 375–386. <https://doi.org/10.1002/cb.2012>
- Acquisti, A. (2004). Privacy in electronic commerce and the economics of immediate gratification. In *Proceedings of the 5th ACM Electronic Commerce Conference* (pp. 21-29). New York, NY: ACM. <http://dx.doi.org/10.1145/988772.988777>
- Acquisti, A., Brandimarte, L. & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, 347(6221), 509–514. <https://doi.org/10.1126/science.aaa1465>
- Aguirre, E., 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. <https://doi.org/10.1016/j.jretai.2014.09.005>

- Aguirre-Urreta, M. I., & Hu, J. (2019). Detecting common method bias: Performance of the Harman's single-factor test. *Data Base for Advances in Information Systems*, 50(2), 45–70. <https://doi.org/10.1145/3330472.3330477>
- Aldoseri, A., Al-Khalifa, K. N. & Hamouda, A. M. (2024). AI-Powered Innovation in Digital Transformation: Key Pillars and Industry Impact. *Sustainability*, 16(5), 1790. <https://doi.org/10.3390/su16051790>
- Al-Jabri, I. M., Eid, M. I. & Abed, A. (2019). The willingness to disclose personal information. *Information and Computer Security*, 28(2), 161–181. <https://doi.org/10.1108/ics-01-2018-0012>
- Amin, M. a. S., Johnson, V. L., Prybutok, V. & Koh, C. E. (2024). An investigation into factors affecting the willingness to disclose personal health information when using AI-enabled caregiver robots. *Industrial Management & Data Systems*, 124(4), 1677–1699. <https://doi.org/10.1108/imds-09-2023-0608>
- Ampong, G., Mensah, A., Adu, A., Addae, J., Omoregie, O. & Ofori, K. (2018). Examining Self-Disclosure on Social Networking Sites: A Flow Theory and Privacy Perspective. *Behavioral Sciences*, 8(6), 58. <https://doi.org/10.3390/bs8060058>
- Anderson, C. L. & Agarwal, R. (2011). The digitization of healthcare: boundary risks, emotion, and consumer willingness to disclose personal health information. *Information Systems Research*, 22(3), 469–490. <https://doi.org/10.1287/isre.1100.0335>
- Arora, N., Dreze, X., Ghose, A., Hess, J. D., Iyengar, R., Jing, B., Joshi, Y., Kumar, V., Lurie, N., Neslin, S., Sajeesh, S., Su, M., Thomas, J. & Zhang, Z. J. (2020). Putting one-to-one marketing to work: Personalization, customization, and choice. *Marketing Letters*, 31(3), 367-380. <https://doi.org/10.1007/s11002-008-9056-z>
- Bandara, R., Fernando, M. & Akter, S. (2020). Explicating the privacy paradox: A qualitative inquiry of online shopping consumers. *Journal of Retailing and Consumer Services*, 52. <https://doi.org/10.1016/j.jretconser.2019.101947>
- Bansal, G., Zahedi, F. M. & Gefen, D. (2016). Do context and personality matter? Trust and privacy concerns in disclosing private information online. *Information & Management* 53(1), 1–21. <https://offcampus.anadolu.edu.tr:2206/10.1016/j.im.2015.08.001>
- Baek, Y. M., Kim, E. M. & Bae, Y. (2014). My privacy is okay, but theirs is endangered: Why comparative optimism matters in online privacy concerns. *Computers in Human Behavior*, 31, 48-56. <https://doi.org/10.1016/j.chb.2013.10.010>
- Barnes, S. B. (2006). Privacy paradox: Social networking in the United States. *First Monday*, 11(9). <https://doi.org/10.5210/fm.v11i9.1394>
- Bastos, J. A., & Bernardes, M. I. (2024). Understanding online purchases with explainable machine learning. *Information*, 15(10), 587. <https://doi.org/10.3390/info15100587>
- Beke, F. T., Eggers, F., Verhoef, P. C. & Wieringa, J. E. (2022). Consumers' privacy calculus: The PRICAL index development and validation. *International Journal of Research in Marketing* (39)1, 20-41. <https://doi.org/10.1016/j.ijresmar.2021.05.005>

- Bélanger, F. & James, T. L. (2020). A Theory of Multilevel Information Privacy Management for the Digital Era. *Information Systems Research* 31(2), 510-536. <https://doi.org/10.1287/isre.2019.0900>
- Bilgihan, A., Kandampully, J. & Zhang, T. (2016). Towards a unified customer experience in online shopping environments: Antecedents and outcomes. *International Journal of Quality and Service Sciences*, 8(1), 102–119. <https://doi.org/10.1108/IJQSS-07-2015-0054>
- Bitkina, O. V., Jeong, H., Lee, B. C., Park, J., Park, J. & Kim, H. K. (2020). Perceived trust in artificial intelligence technologies: A preliminary study. *Human Factors and Ergonomics in Manufacturing & Service Industries*, 30(4), 282–290. <https://doi.org/10.1002/hfm.20839>
- Bleier, A. & Eisenbeiss, M. (2015). The Importance of Trust for Personalized Online Advertising. *Journal of Retailing*, 91(3), 390-409. <https://doi.org/10.1016/j.jretai.2015.04.001>
- Bleier, A., Goldfarb, A. & Tucker, C. (2020). Consumer privacy and the future of data-based innovation and marketing. *International Journal of Research in Marketing*, 37(3), 466–480. <https://doi.org/10.1016/j.ijresmar.2020.03.006>
- Boerman, S. C., Kruikemeier, S. & Borgesius, F. J. Z. (2018). Exploring Motivations for Online privacy Protection Behavior: Insights from panel data. *Communication Research*, 48(7), 953–977. <https://doi.org/10.1177/0093650218800915>
- Brown, B. (2001). Studying the internet experience. *HP laboratories technical report HPL*, 49. <https://shiftleft.com/mirrors/www.hpl.hp.com/techreports/2001/HPL-2001-49.pdf> (Erişim tarihi: 15.03.2024).
- Bornschein, R., Schmidt, L. & Maier, E. (2020). The Effect of Consumers' Perceived Power and Risk in Digital Information Privacy: The Example of Cookie Notices. *Journal of Public Policy & Marketing*, 39(2), 135–154. <https://doi.org/10.1177/0743915620902143>
- Brandimarte, L., Acquisti, A. & Loewenstein, G. (2013). Misplaced Confidences: Privacy and the Control Paradox. *Social Psychological and Personality Science* 4(3), 340–347. <https://doi.org/10.1177/1948550612455931>
- BTK. (2021). Bilgi ve İletişim Teknolojilerinde Gelişmeler, Yenilikler ve Örnek Çalışmalar. 01.06.2023 tarihinde <https://www.btk.gov.tr/uploads/pages/gelismeler-yenilikler-ve-ornek-calismalar-bulteni/belgev2-21-04.pdf> adlı adresten alınmıştır.
- Budak, H. & Gümüştaş, E. (2022). Kişiselleştirilmiş ürün öneri sistemi için kullanıcı bazlı işbirlikçi filtreleme ve kümeleme kullanan hibrit bir yaklaşım. *İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi*, 21(43), 253-268. <https://doi.org/10.46928/iticusbe.1055162>
- Chaudoir, S. R. & Fisher, J. D. (2010). The disclosure processes model: Understanding disclosure decision making and postdisclosure outcomes among people living with a concealable stigmatized identity. *Psychological Bulletin*, 136(2), 236–256. <https://doi.org/10.1037/a0018193>
- Chen, M., Huang, X. & Qi, X. (2024). To disclose or to protect? Predicting social media users' behavioral intention toward privacy. *Industrial Management & Data Systems*, 124(6), 2091–2119. <https://doi.org/10.1108/imds-05-2023-0337>

- Chen, Y., Prentice, C., Weaven, S. & Hisao, A. (2022). The influence of customer trust and artificial intelligence on customer engagement and loyalty – The case of the home-sharing industry. *Frontiers in Psychology*, 13, 912339. <https://doi.org/10.3389/fpsyg.2022.912339>
- Chin, W. W. (1998). The Partial Least Squares Approach to Structural Equation Modelling. G. A. Marcoulides (Ed.), *Modern Methods for Business Research* (s. 295-336) içinde. London: Lawrence Erlbaum Associates.
- Choi, H., Park, J. & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. *Computers In Human Behavior*, 81, 42-51. <https://doi.org/10.1016/j.chb.2017.12.001>
- Chiasson, S., Abdelaziz, Y. & Chanchary, F. (2018). Privacy concerns amidst OBA and the need for alternative models. *IEEE Internet Computing*, 22(2), 52–61. <https://doi.org/10.1109/mic.2017.3301625>
- Cohen, J., Cohen, P., West, S. G. & Aiken, L. S. (2003). *Applied Multiple Regression/Correlation Analysis for the Behavioral Sciences*. Hillsdale, NJ: Erlbaum.
- Craig, V. S., Shim, J. T., Johnson, R. & Jiang, J. (2006). Concern for information privacy and online consumer Purchasing. *Journal of the Association for Information Systems*, 7(6), 415-431, 433-443. <https://doi.org/10.17705/1jais.00092>
- Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness and impersonal trust: an empirical investigation. *Organization Science* 10(1), 104–115. <https://doi.org/10.1287/orsc.10.1.104>
- Culnan, M. J. & Bies, R. J. (2003). Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues*, 59(2), 323-342. <https://doi.org/10.1111/1540-4560.00067>
- Çakır, F. S. (2019). Kısmi En Küçük Kareler Yapısal Eşitlik Modellemesi (PLS-SEM) ve Bir Uygulama. *Sosyal Araştırmalar ve Davranış Bilimleri Dergisi*, 5(9), 111-128.
- Davenport, T., Guha, A., Grewal, D. & Bressgott, T. (2020). How artificial intelligence will change the future of marketing. *Journal of the Academy of Marketing Science*, 48, 24–42. <https://doi.org/10.1007/s11747-019-00696-0>
- Deloitte. (2020). Connecting with Meaning-Hyper Personalizing the Customer Experience Using Data, Analytics and AI. 27.05.2020 tarihinde <https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/deloitte-analytics/ca-en-omnia-ai-marketing-pov-fin-jun24-aoda.pdf> adlı adresten alınmıştır.
- Dienlin, T. & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology*, 45(3), 285–297. <https://doi.org/10.1002/ejsp.2049>
- Dinev, T. & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, 17(1), 61–80. <https://doi.org/10.1287/isre.1060.0080>
- Do, Q. & Trang, T. (2020). An approach based on machine learning techniques for forecasting Vietnamese consumers' purchase behaviour. *Decision Science Letters*, 9(3), 313-322. <http://dx.doi.org/10.5267/j.dsl.2020.5.004>

- Doğan K. & Arslantekin S. (2016). Büyük veri: önemi, yapısı ve günümüzdeki durum. *Ankara Üniversitesi Dil ve Tarih-Coğrafya Fakültesi Dergisi*, 56(1), 16. https://doi.org/10.1501/Dtcfder_0000001461
- Dotcms. (2018). Hyper-Personalization: It's Time to Truly Meet Your Customers. 27.05.2023 tarihinde <https://www.dotcms.com/reports/hyper-personalization-it-s-time-to-truly-meet-your-customers> adlı adresten alınmıştır.
- Dunakhe, K. & Panse, C. (2022). Impact of digital marketing – a bibliometric review. *International Journal of Innovation Science*, 14(3/4), 506-518. <https://doi.org/10.1108/IJIS-11-2020-0263>
- Dwivedi, Y. K., Hughes, L., Ismagilova, E., Aarts, G., Coombs, C. & Crick, T. (2019). Artificial Intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management*. <https://doi.org/10.1016/j.ijinfomgt.2019.08.002>
- Estrada-Jiménez, J., Parra-Arnau, J., Rodríguez-Hoyos, A. & Forné, J. (2016). Online advertising: Analysis of privacy threats and protection approaches. *Computer Communications*, 100, 32–51. <https://doi.org/10.1016/j.comcom.2016.12.016>
- Fayyaz, Z., Ebrahimian, M., Nawara, D., Ibrahim, A. & Kashef, R. (2020). Recommendation Systems: Algorithms, Challenges, Metrics, and Business Opportunities. *Applied Sciences*, 10(21):7748. <https://doi.org/10.3390/app10217748>
- Ferreira, N. E. D., Kroll, T., Aïmeur, E., Stieglitz, S. & Heisel, M. (2020). Preventative Nudges: Introducing risk cues for supporting online Self-Disclosure decisions. *Information*, 11(8), 399. <https://doi.org/10.3390/info11080399>
- Fornell, C. & Larcker, D.F.(1981). Structural equation models with unobservable variables and measurement error: algebra and statistics. *Journal of Marketing Research*,18(3), 382–388. <https://doi.org/10.2307/3150980>
- Fu, J., Zhang, J. & Li, X. (2023). How do risks and benefits affect user' privacy decisions? An event-related potential study on privacy calculus process. *Frontiers in Psychology*, 14. <https://doi.org/10.3389/fpsyg.2023.1052782>
- Gudivada, V., Apon, A. & Ding, J. (2017). Data quality considerations for big data and machine-learning: Going beyond data cleaning and transformations. *International Journal on Advances in Software*, 10(1), 1–20.
- Hair, J. F., Ringle, C. M. & Sarstedt, M. (2011). PLS-SEM: Indeed a Silver Bullet. *Journal of Marketing Theory and Practice*, 19(2), 139-152. <https://doi.org/10.2753/MTP1069-6679190202>
- Hair, J. F., Hult, T., Ringle, C., & Sarstedt, M. (2014). *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*. Thousand Oaks, CA: Sage Publications, Inc.
- Hair, J. F., Hult, G. T. M., Ringle, C. M., Sarstedt, M., & Thiele, K. O. (2017). Mirror, mirror on the wall: a comparative evaluation of compositebased structural equation modeling methods. *Journal of the Academy of Marketing Science*, 45(5), 616–632. <https://doi.org/10.1007/s11747-017-0517-x>

- Hallam, C. & Zanella, G. (2017). Online self-disclosure: The privacy paradox explained as a temporally discounted balance between concerns and rewards. *Computers in Human Behavior*, 68, 217-227. <https://doi.org/10.1016/j.chb.2016.11.033>
- Harris, L. C. & Goode, M. M. H. (2010). Online serviscapes, trust, and purchase intentions. *Journal of Service Marketing*, 24(3), 230-243. <https://doi.org/10.1108/08876041011040631>
- Hayes, J. L., Brinson, N. H., Bott, G. J. & Moeller, C. M. (2021). The influence of consumer-brand relationship on the personalized advertising privacy calculus in social media. *Journal of Interactive Marketing*, 55(1), 16–30. <https://doi.org/10.1016/j.intmar.2021.01.001>
- Helweg-Larsen, M. & Shepperd, J. A. (2001). Do moderators of the optimistic bias affect personal or target risk estimates? A review of the literature. *Personality and Social Psychology Bulletin*, 5(1), 75-95. https://doi.org/10.1207/S15327957PSPR0501_5
- Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, 43(1), 115–135. <https://doi.org/10.1007/s11747-014-0403-8>
- Ho, F. N., Ho-Dac, N. & Huang, J. S. (2023). The effects of privacy and data breaches on consumers' online Self-Disclosure, protection behavior, and message valence. *SAGE Open*, 13(3). <https://doi.org/10.1177/21582440231181395>
- Hoffmann, C. P., Lutz, C. & Ranzini, G. (2016). Privacy cynicism: A new approach to the privacy paradox. *Cyberpsychology Journal of Psychosocial Research on Cyberspace*, 10(4). <https://doi.org/10.5817/cp2016-4-7>
- Hu, L. T. & Bentler, P.M. (1999). Cutoff Criteria for Fit Indexes in Covariance Structure Analysis: Conventional Criteria Versus New Alternatives. *Structural Equation Modelling: A Multidisciplinary Journal*, 6(1), 1-55. <https://doi.org/10.1080/10705519909540118>
- Huang, M. & Rust, R. (2017). Technology-driven Service Strategy. *Journal of the Academy of Marketing Science*, 45(6), 906-924. <https://doi.org/10.1007/s11747-017-0545-6>
- Hulland, J. (1999). Use of Partial Least Squares (PLS) in Strategic Management Research: A Review of Four Recent Studies, *Strategic Management Journal*, 20(2), 195-204.
- Ioannou, A., Tussyadiah, I. & Lu, Y. (2020). Privacy concerns and disclosure of biometric and behavioral data for travel. *International Journal of Information Management*, 54, 102122. <https://doi.org/10.1016/j.ijinfomgt.2020.102122>
- Jahari, S. A., Hass, A., Hass, D. & Joseph, M. (2022). Navigating privacy concerns through societal benefits: A case of digital contact tracing applications. *Journal of Consumer Behaviour*, 21(3), 625–638. <https://doi.org/10.1002/cb.2029>
- Jensen, C., Potts, C. & Jensen, C. (2005). Privacy practices of Internet users: Self-reports versus observed behavior. *International Journal of Human-Computer Studies*, 63(1–2), 203-227, <https://doi.org/10.1016/j.ijhcs.2005.04.019>

- Kaplan, A. & Haenlein, M. (2019). Siri, Siri, in My Hand: Who's the Fairest in the Land? On the interpretations, illustrations, and implications of artificial intelligence. *Business Horizons*, 62(1): 15-25. <https://doi.org/10.1016/j.bushor.2018.08.004>
- Karim, M. & Rahman, R. (2013). Decision Tree and Naïve Bayes Algorithm for Classification and Generation of Actionable Knowledge for Direct Marketing. *Journal of Software Engineering and Applications*, 6(4), 196-206. <https://doi.org/10.4236/jsea.2013.64025>
- Kim, H. W., Chan, H. C. & Gupta, S. (2007). Value-based Adoption of Mobile Internet: An empirical investigation. *Decision Support Systems*, 43, 111-126.
- Kim, D., Park, K., Park, Y. & Ahn, J. (2019). Willingness to provide personal information: Perspective of privacy calculus in IoT services. *Computers in Human Behavior*, 92, 273-281. <https://doi.org/10.1016/j.chb.2018.11.022>
- Kim, S. & Baek, T. H. (2017). Examining the antecedents and consequences of mobile app engagement. *Telematics and Informatics*, 35(1), 148-158. <https://doi.org/10.1016/j.tele.2017.10.008>
- Klein, C. T. F. & Helweg-Larsen, M. (2002). Perceived control and the optimistic bias: A meta-analytic review. *Psychology and Health*, 17, 437-446. <https://doi.org/10.1080/0887044022000004920>
- Kock, F., Berbekova, A., & Assaf, A. G. (2021). Understanding and managing the threat of common method bias: Detection, prevention and control. *Tourism Management*, 86, 1-10. <https://doi.org/10.1016/j.tourman.2021.104330>
- Komiak, S. Y. & Benbasat, I. (2006). The effects of personalization and familiarity on trust and adoption of recommendation agents, *MIS Quarterly*, 941-960. <https://doi.org/10.2307/25148760>
- Kotler, P. (2021). *Pazarlama 5.0: İnsan için Teknoloji*. Nişantaşı Üniversitesi Yayınları.
- Krishnan, C., Gupta, A., Gupta, A. & Singh, G. (2022). Impact of Artificial Intelligence-Based Chatbots on customer engagement and business growth. In *Studies in big data* (pp. 195-210). https://doi.org/10.1007/978-3-031-10869-3_11
- 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>
- Lee, J. M. & Rha, J. Y. (2016). Personalization-privacy paradox and consumer conflict with the use of location-based mobile commerce. *Computers in Human Behavior*, 63, 453-462. <https://doi.org/10.1016/j.chb.2016.05.056>
- Leon, P. G., Ur, B., Shay, R., Wang, Y., Balebako, R. & Cranor, L. (2012). Why Johnny can't opt out: A usability evaluation of tools to limit online behavioral advertising. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp 589-598).
- Li, Y. (2012). Theories in online information privacy research: A critical review and an integrated framework. *Decision Support Systems*, 54(1), 471-481, <https://doi.org/10.1016/j.dss.2012.06.010>

- Liu, Y., Zhao, H. & Yang, B. (2022). Research on customer churn prediction and model interpretability using GA-XGBoost algorithm. *PLOS ONE*, 17(8), e0289724. <https://doi.org/10.1371/journal.pone.0289724>
- Mach-Król, M. & Hadasik, B. (2021). On a certain research gap in big data mining for customer insights. *Applied Sciences*, 11(15), 6993. <https://doi.org/10.3390/app11156993>
- Maheswari, K. & Priya, P. P. A. (2017). Predicting customer behavior in online shopping using SVM classifier. In: *2017 IEEE International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS)*, Srivilliputtur, India. 1-5. <https://doi.org/10.1109/ITCOSP.2017.8303085>
- Malhotra, N. K., Kim, S. S. & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, 15(4), 336–355. <https://doi.org/10.1287/isre.1040.0032>
- Malle, B. F., Scheutz, M., Arnold, T., Voiklis, J. & Cusimano, C. (2015). Sacrifice one for the good of many? People apply different moral norms to human and robot agents. In: *10th ACM/IEEE international conference on human-robot interaction (HRI)*. Mart, 2015. pp. 117-124. IEEE.
- Martin, K. D., Borah, A. & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. *Journal of Marketing*, 81(1), 36–58. <https://doi.org/10.1509/jm.15.0497>
- Martin, K. D. & Murphy, P. E. (2017). The role of data privacy in marketing: A review and research agenda. *Journal of the Academy of Marketing Science*, 45(2), 135-155. <https://doi.org/10.1007/s11747-016-0495-4>
- Massara, F., Raggiotto, F. & Voss, W. G. (2021). Unpacking the privacy paradox of consumers: A psychological perspective. *Psychology and Marketing*, 38(10), 1814–1827. <https://doi.org/10.1002/mar.21534>
- McKnight, D. H., Choudhury, V. & Kacmar, C. (2002). Developing and Validating Trust Measures for e-Commerce: An Integrative Typology. *Information Systems Research*, 13(3), 334–359. <http://www.jstor.org/stable/23015741>
- Metzger, M. J. (2007). Communication Privacy Management in Electronic Commerce. *Journal of Computer-Mediated Communication*, 12(2), 335–361, <https://doi.org/10.1111/j.1083-6101.2007.00328.x>
- Milne, G. R., Rohm, A.J. & Bahl, S. (2004). Consumers' Protection of Online Privacy and Identity. *Journal of Consumer Affairs*, 38, 217-232. <https://doi.org/10.1111/j.1745-6606.2004.tb00865.x>
- Mousavi, R., Chen, R., Kim, D. J., & Chen, K. (2020). Effectiveness of privacy assurance mechanisms in users' privacy protection on social networking sites from the perspective of protection motivation theory. *Decision Support Systems*, 135, 113323. <https://doi.org/10.1016/j.dss.2020.113323>
- Nobile, T. H. & Kalbaska, N. (2020). An Exploration of Personalization in Digital Communication. Insights in Fashion. 456-473. In: Nah, FH., Siau, K. (eds) *HCI in Business, Government and Organizations*. HCII 2020. Lecture Notes in Computer Science, vol 12204. Springer, Cham. https://doi.org/10.1007/978-3-030-50341-3_35

- Norberg, P. A., Horne, D. R. & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, 41(1), 100–126. <https://doi.org/10.1111/j.1745-6606.2006.00070.x>
- Omarzu, J. (2000). A disclosure decision model: Determining how and when individuals will Self-Disclose. *Personality and Social Psychology Review*, 4(2), 174–185. https://doi.org/10.1207/s15327957pspr0402_05
- Osatuyi, B., Passerini, K., Ravarini, A. & Grandhi, S. A. (2018). “ Fool me once, shame on you . . . then, I learn.” An examination of information disclosure in social networking sites. *Computers in Human Behavior*, 83, 73–86. <https://doi.org/10.1016/j.chb.2018.01.018>
- Paschen, J., Kietzmann, J. & Kietzmann, T. C. (2019). Artificial intelligence (AI) and its implications for market knowledge in B2B marketing. *Journal of Business & Industrial Marketing*, 34(7), 1410–1419. <https://doi.org/10.1108/JBIM-10-2018-0295>
- Plangger, K., Grewal, D., de Ruyter, K. & Tucker, C. (2022). The future of digital technologies in marketing: A conceptual framework and an overview. *Journal of the Academy of Marketing Science* 50, 1125–1134. <https://doi.org/10.1007/s11747-022-00906-2>
- Princi, E. & Krämer, N. C. (2020). Out of control – Privacy calculus and the effect of perceived control and moral considerations on the usage of IoT healthcare devices. *Frontiers in Psychology*, 11, 582054. <https://doi.org/10.3389/fpsyg.2020.582054>
- Podsakoff, P., MacKenzie, S., & Podsakoff, N. (2012). Sources of method bias in social science research and recommendations on how to control it. *Annual Review Psychology*, 63, 539-569. <http://dx.doi.org/10.1146/annurev-psych-120710-100452>
- Punj, G. N. (2018). Understanding individuals’ intentions to limit online personal information disclosures to protect their privacy: implications for organizations and public policy. *Information Technology and Management*, 20(3), 139–151. <https://doi.org/10.1007/s10799-018-0295-2>
- Quinn, K. (2014). An ecological approach to privacy: “Doing” online privacy at Midlife. *Journal of Broadcasting & Electronic Media*, 58(4), 562–580. <https://doi.org/10.1080/08838151.2014.966357>
- Rust, R. T. & Huang, M. H. (2014). The service revolution and the transformation of marketing science. *Marketing Science*, 33(2), 206–221. <https://doi.org/10.1287/mksc.2013.0836>
- Sabharwal, R. & Miah, S. J. (2021). A new theoretical understanding of big data analytics capabilities in organizations: A thematic analysis. *Journal of Big Data*, 8(1), 1-17. <https://doi.org/10.1186/s40537-021-00543-6>
- Saponaro, M., Le Gal, D., Gao, M., Guisiano, M. & Maniere, I. C. (2018). Challenges and opportunities of artificial intelligence in the fashion world. In: *International Conference on Intelligent and Innovative Computing Applications (ICONIC)*. Aralık, 2018. pp. 1–5. IEEE. <https://doi.org/10.1109/ICONIC.2018.8601258>
- Shank, D. B., Graves, C., Gott, A., Gamez, P. & Rodriguez, S. (2019). Feeling our way to machine minds: people’s emotions when perceiving mind in artificial intelligence. *Computers in Human Behavior*, 98, 256–266. <https://doi.org/10.1016/j.chb.2019.04.001>

- Smit, E. G., Van Noort, G. & Voorveld, H. A. (2014). Understanding online behavioural advertising: User knowledge, privacy concerns and online coping behaviour in Europe. *Computers in Human Behavior*, 32, 15–22. <https://doi.org/10.1016/j.chb.2013.11.008>
- Smith, H. J., Milberg, J. S. & Burke, J. S. (1996). Information privacy: measuring individuals' concerns about organizational practices. *MIS Quarterly* 20 (2), 167–196. <https://doi.org/10.2307/249477>
- Smith, H. J., Dinev, T. & Xu, H. (2011). Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly*. 35, 989-1016.
- Sun, X., Pelet, J., Dai, S. & Ma, Y. (2023). The effects of trust, perceived risk, innovativeness, and deal proneness on consumers' purchasing behavior in the livestreaming social commerce context. *Sustainability*, 15(23), 16320. <https://doi.org/10.3390/su152316320>
- Tam, K. Y. & Ho, S. Y. (2006). Understanding the Impact of Web Personalization on User Information Processing and Decision Outcomes. *MIS Quarterly*, 30(4), 865–890. <https://doi.org/10.2307/25148757>
- Tang, J., Zhang, B. & Xiao, S. (2022). Examining the intention of authorization via apps: Personality traits and expanded privacy calculus perspectives. *Behavioral Sciences*, 12(7), 218. <https://doi.org/10.3390/bs12070218>
- Tenenhaus, M., Vinzi, V. E. Chatelin, Y-M. & Lauro, C. (2004). PLS Path Modeling. *Computational Statistics and Data Analysis*, 48(1), 159-205. <https://doi.org/10.1016/j.csda.2004.03.005>
- Tiago, M. T. P. M. B. & Veríssimo, J. M. C. (2014). Digital marketing and social media: Why bother? *Business Horizons, Elsevier*, 57(6), 703-708. <https://doi.org/10.1016/j.bushor.2014.07.002>
- Tian, X., Chen, L. & Zhang, X. (2022). The Role of Privacy Fatigue in Privacy Paradox: A PSM and Heterogeneity Analysis. *Applied Sciences*, 12, 9702. <https://doi.org/10.3390/app12199702>
- Tiihonen, J. & Felfernig, A. (2017). An introduction to personalization and mass customization. *Journal of Intelligent Information Systems*, 49, 1–7. <https://doi.org/10.1007/s10844-017-0465-4>
- Toch, E., Wang, Y. & Cranor, L. F. (2012). Personalization and privacy: a survey of privacy risks and remedies in personalization-based systems. *User Modeling and User-Adapted Interaction* 22(1-2), 203-220. <https://doi.org/10.1007/s11257-011-9110-z>
- Trepte, S. (2020). The social media privacy model: Privacy and communication in the light of social media affordances. *Communication Theory*, 31(4), 549-570.
- Tsohou, A. & Papaioannou, T. (2021). Impacts of information privacy violations. In *Springer eBooks* (pp. 1–4). https://doi.org/10.1007/978-3-642-27739-9_1614-1
- Tufekci, Z. (2008). Grooming, gossip, Facebook and MySpace: What can we learn about these sites from those who won't assimilate? *Information, Communication & Society*, 11, 544–564. <http://dx.doi.org/10.1080/13691180801999050>
- Tyrväinen, O., Karjaluoto, H. & Saarijärvi, H. (2020). Personalization and hedonic motivation in creating customer experiences and loyalty in omnichannel retail. *Journal of Retailing and Consumer Services*, 57, 102233. <https://doi.org/10.1016/j.jretconser.2020.102233>

- Unni, R. & Harmon, R. (2007). Perceived Effectiveness of Push vs. Pull Mobile Location-based Advertising, *Journal of Interactive Advertising* 7(2), 28-40.
- Van Der Schyff, K. & Flowerday, S. (2023). The mediating role of perceived risks and benefits when self-disclosing: A study of social media trust and FoMO. *Computers & Security*, 126, 103071. <https://doi.org/10.1016/j.cose.2022.103071>
- Veltri, G. A., Lupiáñez-Villanueva, F., Folkvord, F., Theben, A. & Gaskell, G. (2020). The impact of online platform transparency of information on consumers' choices. *Behavioural Public Policy*, 7(1), 55–82. <https://doi.org/10.1017/bpp.2020.11>
- Vimalkumar, M., Sharma, S. K., Singh, J. B. & Dwivedi, Y. K. (2021). 'Okay google, what about my privacy?': User's privacy perceptions and acceptance of voice based digital assistants. *Computers in Human Behavior*, 120, 106763. <https://doi.org/10.1016/j.chb.2021.106763>
- Wang, J., Cao, Q. & Zhu, X. (2024). Privacy disclosure on social media: the role of platform features, group effects, trust and privacy concern. *Library Hi Tech*. <https://doi.org/10.1108/lht-06-2023-0253>
- Wang, N., Zhao, Y., Zhou, R. & Li, Y. (2022). Factors influencing users' online information disclosure intention and the moderating effect of cultural background and platform type. *Aslib Journal of Information Management*, 75(6), 1178–1208. <https://doi.org/10.1108/ajim-04-2022-0218>
- Westin, A. F. (1967). *Privacy and Freedom*. Atheneum.
- Wetzels, M., Odekerken-Schröder, G., & van Oppen, C. (2009). Using PLS path modeling for assessing hierarchical construct models: Guidelines and empirical illustration. *MIS Quarterly*, 33(1), 177- 195. <https://doi.org/10.2307/20650284>
- White, T. B. (2004). Consumer Disclosure and Disclosure Avoidance: A Motivational Framework. *Journal of Consumer Psychology*, 14(1–2): 41–51. https://doi.org/10.1207/s15327663jcp1401&2_6
- Wilson, D. W. & Valacich, J. S. (2012). Unpacking the Privacy Paradox: Irrational Decision-Making within the Privacy Calculus. *Proceedings of the 33rd International Conference on Information Systems*, 41, 114–125.
- Wong, K. K. (2013). Partial least square structural equation modeling (PLS-SEM) techniques using SmartPLS. *Marketing Bulletin*, 24, 1-32.
- Wu X., Zhu X., Wu G. Q. & Ding W. (2014). Data mining with big data, *IEEE transactions on knowledge and data engineering*, 26 (1), 97-107. <https://doi.org/10.1109/TKDE.2013.109>
- Xu, H. (2007). The Effects of Self-Construal and Perceived Control on Privacy Concerns. In: *Twenty Eighth International Conference on Information Systems (ICIS)*.
- Xu, H., Luo, X. (Robert), Carroll, John M. & Rosson M. B. (2011). The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decision Support Systems* 51, 42-52. <https://doi.org/10.1016/j.dss.2010.11.017>
- Yıldız, E. (2021). *SmartPLS ile Yapısal Eşitlik Modellemesi, Reflektif ve Formatif Yapılar*. Seçkin Yayıncılık.

- Yılmaz, V. & Kınaş, Y. (2021). Kısmi En Küçük Kareler Yapısal Eşitlik Modellemesiyle Mobil Bankacılık Kullanımının Araştırılması, *Gazi İktisat ve İşletme Dergisi*, 7(2), 133-149. <https://doi.org/10.30855/gieb.2021.7.2.004>
- Young, A. & Quan-Haase, A. (2013). Privacy protection strategies on Facebook: The Internet privacy paradox revisited. *Information, Communication & Society*, 16, 479–500. <http://dx.doi.org/10.1080/1369118x.2013.777757>
- Zanker, M., Rook, L. & Jannach, D. (2019). Measuring the impact of online personalisation: Past, present and future. *International Journal of Human-Computer Studies*, 131, 160–168. <https://doi.org/10.1016/j.ijhcs.2019.06.006>
- Zhou H, Xiong, F. & Chen H. (2023). A Comprehensive Survey of Recommender Systems Based on Deep Learning. *Applied Sciences*, 13(20), 11378. <https://doi.org/10.3390/app132011378>
- Zhu, X., Cao, Q. & Liu, C. (2022). Mechanism of platform interaction on social media users' intention to disclose privacy: A case study of TikTok APP. *Information*, 13(10), 461. <https://doi.org/10.3390/info13100461>

EK 1: Tüketicilerin çevrimiçi alışveriş ve üyelik deneyimlerine ilişkin bilgiler

Çevrimiçi etkileşim	Haftada 6 defa veya daha az	78
	Günde 1-2 kez	83
	Günde 3 kez veya daha fazla	239
Çevrimiçi alışveriş deneyimi	Hiç deneyimim olmadı	1
	1 yıldan az	24
	1-3 yıl	127
	4-6 yıl	117
	6 yıldan fazla	131
Haftalık çevrimiçi alışveriş deneyimi süresi	1 saatten az	185
	1-2 saat arası	119
	2-3 saat arası	65
	4 saat ve üzeri	31
Günlük çevrimiçi sosyal ağlardaki etkileşim süresi	1 saatten az	55
	1-2 saat arası	97
	2-3 saat arası	157
	4 saat ve üzeri	91
Günlük eğlence ve kültür platformlarında geçirilen süre	1 saatten az	104
	1-2 saat arası	138
	2-3 saat arası	87
	4 saat ve üzeri	71
En çok tercih edilen 3 e-ticaret sitesi	Trendyol	379
	Hepsiburada	280
	Gittigidiyor	36
	Amazon	72
	Boyner Morhipo	12
	Aliexpress	7
	D&R	14
	İdefix	20
	Sahibinden.com	99
	Yemek Sepeti	145
	Diğer	64



En çok tercih edilen 3 sosyal ağ platformu

Twitter	178
Facebook	98
Instagram	378
TikTok	65
Pinterest	28
Linkedin	24
Spotify	118
Youtube	232
Wikipedia	7
Diğer	6

En çok kullanılan 3 eğlence/iletişim platformu

Netflix	299
PuhuTv	18
Amazon Prime	45
BluTv	80
Twitch	45
Whatsapp	362
Telegram	91
Skype	4
Zoom	72
Diğer	39