ÇEVRİMİÇİ DAVRANIŞSAL REKLAMCILIKTAN KAÇINMADA GİZLİLİK ENDİŞESİNİN ROLÜ: KORUMA MOTİVASYONU TEORİSİ ÇERÇEVESİNDE BİR ARAŞTIRMA

Doktora Tezi

ŞADUMAN ŞEYDA GÖKDEMİR

Eskişehir 2023

ÇEVRİMİÇİ DAVRANIŞSAL REKLAMCILIKTAN KAÇINMADA GİZLİLİK ENDİŞESİNİN ROLÜ: KORUMA MOTİVASYONU TEORİSİ ÇERÇEVESİNDE BİR ARAŞTIRMA

Şaduman Şeyda GÖKDEMİR

DOKTORA TEZİ

Halkla İlişkiler ve Reklamcılık Anabilim Dalı

Danışman: Prof. Dr. R. Ayhan YILMAZ

Eskişehir

Anadolu Üniversitesi

Sosyal Bilimler Enstitüsü

Aralık 2023

JÜRİ VE ENSTİTÜ ONAYI

Şaduman Şeyda Gökdemir'in "Çevrimiçi Davranışsal Reklamcılıktan Kaçınmada Gizlilik Endişesinin Rolü: Koruma Motivasyonu Teorisi Çerçevesinde Bir Araştırma" başlıklı tezi **22 Aralık 2023** tarihinde, aşağıdaki jüri tarafından değerlendirilerek "Anadolu Üniversitesi Lisansüstü Eğitim-Öğretim ve Sınav Yönetmeliği'nin ilgili maddeleri uyarınca, **Halkla İlişkiler ve Reklamcılık** Anabilim Dalında, **Doktora** tezi olarak değerlendirilerek kabul edilmiştir/edilmemiştir.

		İmza
Üye (Tez Danışmanı)	**: Prof. Dr. R. Ayhan YILMAZ**	……...
Üye	**: Prof. Dr. N. Bilge İSPİR**	……
Üye	**: Doç. Dr. F. Zeynep ÖZATA**	……
Üye	**: Doç. Dr. Emre Ş. ASLAN**	……
Üye	**: Doç. Dr. Fatma YASA**	……

ÖZET

ÇEVRİMİÇİ DAVRANIŞSAL REKLAMCILIKTAN KAÇINMADA GİZLİLİK ENDİŞESİNİN ROLÜ: KORUMA MOTİVASYONU TEORİSİ ÇERÇEVESİNDE BİR ARAŞTIRMA

Şaduman Şeyda GÖKDEMİR

Halkla İlişkiler ve Reklamcılık Anabilim Dalı

Anadolu Üniversitesi, Sosyal Bilimler Enstitüsü, Aralık 2020

Danışman: Prof. Dr. R. Ayhan YILMAZ

Bu çalışmanın amacı, tüketicinin gizliliğini korumaya yönelik motivasyonları çerçevesinde çevrimiçi davranışsal reklamcılıktan kaçınmada etkili olan faktörleri belirlemektir. Bu amaç doğrultusunda çalışmada, koruma motivasyonu teorisi bağlamında tüketicilerin çevrimiçi davranışsal reklamcılığa yönelik, tehdit ve başa çıkma değerlendirmeleri, gizlilik endişesi ve gizlilik kontrolü algıları ve reklamdan kaçınma niyetleri olarak üç ana yapı oluşturulmuştur. Çalışmada bu ana yapıların doğudan ve dolaylı ilişkilerini ortaya koyan kavramsal bir model önerisi sunulmuştur. Önerilen model ile çalışmanın hipotezlerini test etmek için ise, Yapısal Eşitlik Modellemesi (YEM) analiz yöntemi kullanılmıştır. YEM analizi sonucunda önerilen modelin örneklemle iyi bir uyum gösterdiği kanıtlanmıştır. Elde edilen bulgulara göre, gizlilik endişesi ve gizlilik kontrolünün reklamdan kaçınma üzerinde pozitif etkisi olduğu görülmüştür. Ayrıca gizlilik endişesinin algılanan savunmasızlık ve algılanan ciddiyet değişkenlerinin reklamdan kaçınma üzerindeki etkisinde aracı bir role sahip olduğu ancak algılanan fayda üzerinde aracı bir etkisinin olmadığı görülmüştür. Gizlilik kontrolünün öz yeterlilik ve tepki yeterliliği değişkenlerinin reklamdan kaçınma üzerindeki etkilerinde aracılık etkisinin olduğu ancak tepki maliyeti üzerinde aracı bir etkisinin olmadığı sonucuna ulaşılmıştır.

Anahtar Sözcükler: Çevrimiçi Davranışsal Reklamcılık, Gizlilik Endişesi, Gizlilik Kontrolü, Reklamdan Kaçınma

ABSTRACT

THE ROLE OF PRIVACY CONCERN IN THE AVOIDANCE OF ONLINE BEHAVIOURAL ADVERTISING: A STUDY WITHIN THE FRAMEWORK OF THE PROTECTION MOTIVATION THEORY

Şaduman Şeyda GÖKDEMİR

Department of Public Relations and Advertising

Anadolu University, Graduate School of Social Sciences, December 2023

Supervisor: Prof. Dr. R. Ayhan YILMAZ

The purpose of this study is to identify the factors that are effective in the avoidance of online behavioural advertising in the context of consumer privacy motivation. In line with this purpose, three main constructs, namely consumers' threat and coping appraisals, perceptions of privacy concern and control, and intentions to avoid online behavioural advertising, were created in the context of protection motivation theory. The study proposes a conceptual model that identifies the direct and indirect relationships between these main constructs. The structural equation modelling (SEM) analysis method was used to test the hypotheses of the study with the proposed model. As a result of SEM analysis, the proposed model showed good fit with the sample. According to the results, privacy concerns mediated the effect of perceived vulnerability and perceived severity on ad avoidance, but did not mediate the effect of perceived benefit. It was concluded that privacy control mediates the effects of self-efficacy and response efficacy variables on ad avoidance, but not response cost.

Keywords: Online Behavioural Advertising, Privacy Concern, Privacy Control, Advertising Avoidance

……/……/…….

ETİK İLKE VE KURALLARA UYGUNLUK BEYANNAMESİ

Bu tezin bana ait, özgün bir çalışma olduğunu; çalışmanın hazırlık, veri toplama, analiz ve bilgilerin sunumu olmak üzere tüm aşamalarında bilimsel etik ilke ve kurallara uygun davrandığımı; bu çalışma kapsamında elde edilen tüm veri ve bilgiler için kaynak gösterdiğimi ve bu kaynaklara kaynakçada yer verdiğimi; bu çalışmanın Anadolu Üniversitesi tarafından kullanılan "bilimsel intihal tespit programı"yla tarandığını ve hiçbir şekilde "intihal içermediğini" beyan ederim. Herhangi bir zamanda, çalışmamla ilgili yaptığım bu beyana aykırı durumun saptanması durumunda, ortaya çıkacak tüm ahlaki ve hukuki sonuçları kabul ettiğimi bildiririm.

……..

Şaduman Şeyda Gökdemir

İÇİNDEKİLER

Sayfa

TABLOLAR DİZİNİ

Sayfa

ŞEKİLLER DİZİNİ

Sayfa

SİMGELER VE KISALTMALAR DİZİNİ

α : Alpha

ß : Beta

ω : Omega

N : Birey Sayısı

$\bar{x}$: Ortalama

x^2 : Ki-kare

p : Anlamlılık Düzeyi

r : Korelasyon Katsayısı

R^2 : Belirleme katsayısı

Sd : Serbestlik Derecesi

Ss : Standart Sapma

DFA : Doğrulayıcı Faktör Analizi

CFI : Comparative Fit Index (Karşılaştırmalı Uyum İndeksi)

DFA : Doğrulayıcı Faktör Analizi

GFI : Goodness of fit index (İyilik Uyum İndeksi)

IFI : Bollen's Incremental Fit Index (Bollen Artan Uyum İndeksi)

KMO : Kaiser-Meyer-Oklin Testi

NNFI : Bentler-Bonett Non-normed Fit Index (Normlaştırılmamış Uyum İndeksi)

RMSEA: Root Mean Square Error of Aproximation (Tahmin Hatalarının Ortalamasının Karekökü)

SRMR : Standardized Root Mean Square Residual (Standartlaştırılmış Hata Kareleri Ortalamasının Karekökü)

TLI : Tucker-Lewis Index (Tucker-Lewis İndeksi)

1. GİRİŞ

1.1. Problem

Teknoloji kullanımının hızla benimsenmesiyle birlikte pazarlamacılar geleneksel reklamcılıktan dijital reklamcılığa geçmeye başlamıştır. Günümüzün en hızlı büyüyen reklam formatı olan dijital reklamcılık, pazarlamacıların müşterileriyle her zaman ve her yerde bağlantı kurmasına olanak tanımaktadır (Sharma vd., 2022). Dünya çapında interneti kullanan insan sayısı arttığı için bu ortama yapılan reklam yatırımlarının miktarı da her geçen gün artmaktadır.

İnteraktif Reklamcılık Bürosunun (IAB) raporuna göre internet reklam gelirleri son yıllarda geleneksel mecranın önüne geçerek 2022 yılında %10,8'lik bir artışla büyümeye devam etmektedir. Türkiye reklam harcamalarının %69'u en büyük payla yine dijital medyaya aittir (IAB, 2022). Ancak dijital reklam kullanımının giderek artması nedeniyle kullanıcılar çok fazla reklama maruz kalmakta ve bunun sonucunda reklamdan rahatsız olma (iritasyon) ve reklamdan kaçınmak gibi olumsuz tutum ve davranışlar sergilemektedirler (Dodoo ve Wen, 2019; Sharma vd., 2022).

Reklamdan kaçınma, medya kullanıcılarının, reklam içeriğine maruz kalma oranlarını farklı şekilde azaltan duygusal, bilişsel ve davranışsal tüm eylemlerini ifade eder (Speck ve Elliott, 1997a; Tellis, 2004) Dijital bağlamda reklamlardan kaçınma, reklama maruz kalmayı azaltan reklamdan rahatsız olma, reklamı görmezden gelme, reklamı kapatma, web sitesinden ayrılma, hedefleme sisteminden çıkma gibi herhangi bir eylemin gerçekleştirilmesi olarak tanımlanır (Cho ve Choen, 2004; Kelly vd., 2021). Özellikle daha amaç odaklı olarak bilinen internet ortamında kullanıcılar, reklamlardan kaçınmak veya daha az reklam görmek için çeşitli stratejiler kullanmaktadır. 2021 yılında yapılan bir araştırmaya göre 530 milyon kişi varsayılan olarak reklamları engelleyen mobil tarayıcılar kullanmakta, 290 milyon kişi de masaüstü bilgisayarlarında karşılaştıkları reklamları engellemektedir (Blockthrough, 2022). We Are Social ve Hootsuite'in raporuna (2022) göre, bugün internet kullanıcılarının %37'si çevrimiçi etkinliklerinin en azından bir kısmında reklamları engellemek için araçlar kullanmaktadır. Yapılan araştırmalar dijital reklamcılıktan kaçınmanın markaların tüketicileri etkileme hedefini sekteye uğratarak reklam sektörüne zarar vermesi nedeniyle pazarlamacılar için önemli bir sorun haline geldiğini göstermektedir (Kelly vd., 2010; Beak ve Morimoto, 2012; Tran vd., 2017; Ham, 2017; Youn ve Kim, 2019a; Kelly vd., 2020; Kelly vd., 2021; Aiolfi vd., 2021; Wang vd., 2022; Ho, 2021; Çelik vd., 2023).

Dijitalleşmenin ve internet kullanımının artmasıyla bireyler giderek zamanlarının daha büyük bir kısmını çevrimiçi olarak geçirmekte ve gitgide daha fazla kişisel veriyi çevrimiçi ortamda görünür kılmaktadır (Boerman vd., 2018). Çoğu kişi internette bilgi elde edebilmek, sosyal bağlantılar oluşturmak, ücretsiz hizmetlere ve medya içeriğine erişmek (Bateman vd., 2011), kişiselleştirilmiş ürün tekliflerine ve önerilere, fiyat indirimlerine, ücretsiz hizmetlere ve daha alakalı pazarlama iletişimlerine sahip olmak (Martin ve Murphy, 2017), bir web sitesinin kullanılabilirliğini, rahatlığını ve verimliliğini artırabilmek (Boerman vd., 2018) gibi faydalardan ötürü kişisel verilerini paylaşabilmektedir. Tüketici verilerinin internetteki yaygın erişimi sayesinde birçok marka reklam mesajlarını doğru hedef kitleye uygun maliyette sunmak ve onların satın alma kararını etkilemek için tüketici verilerini kullanan hedefleme stratejilerinden yararlanma imkânı bulmuştur (Aguirre vd., 2015, 34). Reklamların hedeflenmesi, internet reklam ağı şirketlerinin tüketicilerin özel ilgi alanlarını ve tercihlerini zamanında tahmin etmelerine ve sonuç olarak tüketicilere özel olarak hazırlanmış reklamlar sunmalarına olanak tanır (Shelton 2012).

Reklamverenler tüketicilerin demografik, web sitesinin ziyaret geçmişi, anahtar kelime aramaları, çevrimiçi alışveriş kayıtları, coğrafi konum ve video izleme kayıtları gibi bilgilerine dayalı olarak belirli bir tüketici grubunu hedefleyebilir. Bu ise reklamverenlerin tüketici verisini kullanarak arzu edilen kitleyi daha iyi hedefleme olanağı kazanmasına yardım etmektedir (Gordon vd., 2021; Wang vd., 2022; Núnez-Barriopedro vd., 2023). Literatürde veriye dayalı bu reklamcılık türü internet ortamında tüketicinin çevrimiçi davranışlarının izlenmesi ve elde edilen verilerin reklamları hedeflemek için kullanılmasını ifade eden çevrimiçi davranışsal reklamcılık olarak adlandırılır (Boerman vd., 2017; Varnalı, 2021). Çevrimiçi davranışsal reklamlar hem tüketici hem de reklamveren için belirli faydalar sağlamaktadır. Örneğin tüketiciler kendileri ile daha alakalı reklam mesajları ilettiği ve ilgisiz reklamların sayısını azalttığı için bu reklamları faydalı bulmaktadır. Aynı şekilde reklamverenler tarafından da sadece hedeflediği guruba reklamlarını gösterdiği için hem reklam harcamalarının azalmasına olanak sağladığından hem de reklam etkililiğini arttırdığından dolayı çevrimiçi davranışsal reklamlar faydalı görülmektedir (Segijn ve Ooijen, 2022).

Hedefli reklam gelirleri dünya üzerinde geçen yıla göre 10,4 milyar dolar artarak %10,5 artışla toplam 109,4 milyar dolara ulaşmıştır (IAB, 2022). IAB Türkiye raporuna göre 2022 yılında Türkiye reklam harcamalarının en büyük çoğunluğu ise %75'lik bir

oranla hedefli reklamcılığa aittir (IABTR, 2022). Ayrıca davranışsal reklamcılık için tıklama oranının (kullanıcının görüntülenen bir reklamı tıklama olasılığı) 5,3 kat olduğu ve daha önce bir ürüne ilgi göstermiş olan yeniden hedeflenen tüketiciler için tıklama oranının 10,8 kat daha yüksek olduğu tahmin edilmektedir. (Fourberg vd., 2021, s. 19).

Çevrimiçi davranışsal reklamcılık etkili ve faydalı bulunmasının yanı sıra kişisel veri gizliliğine yönelik riskleri de beraberinde getirmektedir. Veriye yönelik gizlilik, kişiye ait bilgilerin başkalarına ne zaman, nasıl ve ne ölçüde iletileceği üzerinde kontrol sahibi olması anlamına gelmektedir (Westin, 1967). Reklam şirketleri çevrimiçi olarak dijital davranışları izleyip kişisel verileri topladıkça, kullandıkça ve paylaştıkça tüketiciler genellikle kişisel verileri üzerindeki kontrollerini kaybetmektedirler. Bu kontrol kaybı ise çevrimiçi davranışsal reklamcılığın tüketicide gizlilik endişesi yaratmasına neden olmaktadır (Turow vd., 2009; McDonald ve Cranor, 2010b; Smit vd., 2014; Boerman vd, 2017; Varnalı, 2021). Sonuç olarak çevrimiçi gizliliğin kişisel olarak yönetilmesi ve korunması, günlük yaşamın önemli bir parçası haline gelmiştir (Büchi vd., 2017). We Are Social ve Hootsuite'in raporuna (2022) göre, reklamdan kaçınmanın en önemli üçüncü nedeni %41 oranında gizlilik endişelerinden kaynaklanmaktadır. Bu sonuçlar bize internette zaten çok fazla sevilmeyen reklamların bir de gizlilik boyutuyla kaçınmaya neden olduğunu göstermektedir.

Gizliliğe yönelik tartışmaların artması hukuk ve reklamcılık sektörü öz-düzenlemelerinde gizliliğe yönelik çalışmaların da artmasına neden olmuştur. Federal Ticaret Komisyonu[1] (FTC) tarafından çevrimiçi davranışsal reklamlara yönelik 2009 ve 2012 yıllarında iki önemli rapor hazırlanmış ve tüketiciye belli kontrollerin verilmesinin önü açılmıştır. Ayrıca Avrupa Genel Veri Koruma Yönetmeliği (GDPR) tarafından 2018 yılında veri toplamada kullanılan çerezlerin kişisel veri olarak sayılması ve şirketlere çerezleri kabul etmeleri için tüketiciden onay alma zorunluluğu getirilmiştir (Rustad ve Koenig, 2018). Dijital Reklamcılık Ajansı (DAA), Ağ Reklamcılığı Girişimi (NAI) gibi sektör kuruluşları da çevrimiçi davranışsal reklamlara yönelik bazı öz-düzenlemeler hazırlayarak tüketiciye belirli kontrollerin verilmesine çalışmıştır (Balebako vd., 2012).

Bu durum şüphesiz akademinin de ilgisini çekmiş ve çevrimiçi davranışsal reklamcılık literatüründe gizlilik ve gizlilik endişesine yönelik çalışmalar yoğun ilgi görmeye başlamıştır (El Hana vd., 2023; Im vd., 2023; Smullen vd, 2021; Kim vd., 2019;

[1]Federal Ticaret Komisyonu (Federal Trade Commision-FTC) Amerika Birleşik Devletleri Federal Hükûmetine bağlı ve tüketici hakları konularında çalışan bağımsız bir kurumdur.

Boerman vd., 2017; Varnalı, 2021; Ham, 2017; Boerman vd., 2017; Lambrecht ve Tucker, 2013; McDonald ve Cranor, 2010a; Turow vd., 2009). Literatürdeki gizlilik çalışmalarının çoğunlukla yasal ve öz düzenlemelere yönelik etik boyutta ele alınan çalışmalar ve çevrimiçi davranışsal reklamcılığa yönelik tüketicinin tutum ve algılarına dayanan çalışmalar olduğu görülmüştür (Varnalı, 2021).

Tüketici gizlilik endişesi çalışmalarının çoğu fayda maliyet analizine dayanan gizlilik muhasebesi (privacy calculus) kavramsal çerçevesi ile ele alınmıştır. Bu bakış açısıyla fayda maliyetten daha yüksekse kişisel verilerin internette paylaşılma olasılığının artacağı varsayımı farklı bağlamlarda ölçülmüştür. Ancak tüketicide gizliliği korumaya yönelik motivasyonların ne olduğu hala belirsizdir (Boerman vd., 2017). Literatürde gizliliği korumaya yönelik motivasyonları ele alan sınırlı sayıda çalışamaya ulaşılmıştır (Boerman vd., 2018; Mousavi vd., 2020). Bu sonuçlar literatürde tüketici gizliliğini korumaya yönelik motivasyonların ne olduğunu açıklayan daha fazla çalışmaya ihtiyaç duyulduğunu göstermektedir.

Çevrimiçi ve mobil reklamlara yönelik olumsuz inançlar, algılar ve duyguların, reklam engelleme davranışının benimsenmesinde önemli bir rol oynağı bilinmektedir (Brinson ve Britt, 2021; Tudoran, 2019). Bu durum özellikle çevrimiçi davranışsal reklamlardan kaçınmada gizlilik endişesinin rolünü göstermektedir. Dijital reklamdan kaçınmaya yönelik literatür taraması çalışmasının sonucuna göre dijital reklamlardan kaçınma ve gizlilik endişesi ilişkisine odaklanan çalışmalarda farklı sonuçlar olduğu görülmüştür. Bu da alanda daha fazla çalışmaya ihtiyaç olduğunu göstermektedir (Çelik vd., 2023). Üstelik dijital reklamcılık literatüründe çevrimiçi davranışsal reklamcılıktan kaçınmaya yönelik yeterince çalışma olmadığı söylenebilir (Beak ve Morimoto, 2012; Li ve Huang, 2016; Aiolfi vd., 2021). Reklamdan kaçınma dijital reklamcılığın yükselmesi ile birlikte öne çıkan bir pazarlama olgusu olup, markaların tüketicileri etkileme hedefini sekteye uğratarak reklam sektörüne zarar vermesi nedeniyle pazarlamacılar için önemli bir sorundur. Bu nedenle literatürde kaçınmaya yönelik daha fazla çalışmaya ihtiyaç vardır (Çelik vd., 2023).

Tüm bu sorunlardan hareketle çalışmanın temel problemini tüketicinin gizliliği korumaya yönelik motivasyonları çerçevesinde çevrimiçi davranışsal reklamcılıktan kaçınmada etkili olan faktörlerin neler olduğu sorusu oluşturmaktadır.

1.2. Araştırmanın Amacı

Problem bölümünde bahsedilen gerekçeler doğrultusunda bu çalışma, tüketicinin gizliliğini korumaya yönelik motivasyonları çerçevesinde çevrimiçi davranışsal reklamcılıktan kaçınmada etkili olan faktörleri belirlemeyi amaçlamaktadır. Bu amaç doğrultusunda çalışmada, koruma motivasyonu teorisi bağlamında tüketicilerin çevrimiçi davranışsal reklamcılığa yönelik (1) tehdit ve başa çıkma değerlendirmeleri, (2) gizlilik endişesi ve gizlilik kontrolü algıları ve (3) reklamdan kaçınma niyetleri olarak üç ana yapı oluşturulmuştur. Çalışmada bu ana yapıların ilişkilerini ortaya koyan bir model önerisi sunulmuş ve önerilen bu modelin test edilmesiyle bu yapılar arasındaki ilişkilerin anlaşılması amaçlanmıştır. Bu amaç doğrultusunda aşağıdaki araştırma sorularına cevap aranmaktadır:

1. Tüketicilerin çevrimiçi davranışsal reklamlara yönelik gizlilik endişesi algısını hangi faktörler etkilemektedir?
2. Tüketicilerin çevrimiçi davranışsal reklamlara yönelik gizlilik kontrolü algısını hangi faktörler etkilemektedir?
3. Tüketicilerin çevrimiçi davranışsal reklamlardan kaçınma niyetlerini hangi faktörler etkilemektedir?

1.3. Araştırmanın Önemi

Bu çalışmanın problem kısmında belirtilen literatür boşluklarına hem teorik hem uygulama açısından önemli katlılar sağlaması beklenmektedir.

Öncelikle çevrimiçi davranışsal reklamcılık kavramının tanımı hala net değildir (Boerman vd., 2017; Varnalı, 2021). Kavram farklı tanımlamalarla da ele alınmaktadır ve reklamın işleyiş şekline yönelik (davranışsal veri ve çerez sistemi) farklı bakış açıları söz konusudur. Bunun yanı sıra gizlilik endişesi kavramı özellikle 2010'lu yıllardan sonra çok fazla gündeme alınan bir kavramdır. Hem çevrimiçi davranışsal reklamcılık kavramının hem de reklamcılık bağlamında gizlilik endişesi kavramının detaylı bir şekilde açıklanması özellikle Türkçe literatürdeki sonraki çalışmalar için bir zemin hazırlayacaktır.

Literatürde koruma motivasyonu bağlamında çevrimiçi davranışsal reklamcılıktan kaçınmaya yönelik sınırlı sayıda çalışma söz konusudur (Ham, 2017; Strycharz vd., 2019). Bu çalışmalarda odak noktası tüketicinin ikna bilgisi olup teorinin belirli kısımları araştırmaya dâhil edilmiştir. Bu anlamda koruma motivasyonu teorisinin tüm

değişkenleri incelenerek teorinin test edilmesi ile bu çalışmanın hem kavramsal hem uygulamalı sonuçları ile alana katkılar sağlayacağı düşünülmektedir.

Çevrimiçi davranışsal reklamcılık ve gizlilik endişesi ilişkisi (Varnalı, 2021) ile gizlilik endişesi ve reklamdan kaçınma ilişkisini (Çelik vd., 2023) inceleyen çalışma sonuçlarında farklılıklar söz konusudur. Bu sonuçlar kavramlar arasındaki ilişkilerin daha iyi anlaşılabilmesi açısından farklı kültür ve farklı bağlamlarda çalışmalara ihtiyaç olduğunu göstermektedir. Bu açından çalışma sonuçlarının alana katkı yapacağı düşünülmektedir.

Ayrıca literatürde özellikle gizlilik endişesine yönelik çalışmaların Avrupa ve Amerika tüketicilerine dayalı sonuçlar verdiği bu nedenle de diğer kültürlere ait daha fazla çalışmaya ihtiyaç duyulduğu bilinmektedir (Martin ve Murphy, 2017). Farklı kültürlerde tüketicinin gizliliğe bakış açısı net değildir. Kolektif toplumlarda gizliliğin bireysel batı toplumlarına oranla daha az önemsendiği varsayılır. Bu açıdan çalışmanın sonuçları bu varsayımı destekleyip desteklemeyeceği açısından önemli görülmektedir.

Türkçe literatürde çevrimiçi davranışsal reklamcılığa yönelik sınırlı sayıda çalışmaya ulaşılmıştır (Kırlıdoğ, 2013; Karabıyık ve Armağan, 2017; Akdağ ve Akan, 2017; Taşdelen ve Şentürk, 2018; Gökdemir ve Akıncı, 2019; Akan ve Tanyeri, 2020). Ayrıca çevrimiçi davranışsal reklamcılıktan kaçınmaya yönelik sınırlı sayıda çalışma olduğu görülmektedir (Akın, 2020). Üstelik gizlilik endişesi ve koruma motivasyonu bağlamında konuyu ele alan bir çalışmaya rastlanmaması bu anlamda literatüre katkı sağlayacaktır.

1.4. Araştırmanın Varsayımları

- Bu çalışmada gizlilik endişesi, gizlilik kontrolü ve çevrimiçi davranışsal reklamcılıktan kaçınma arasında bir ilişki olduğu varsayılmaktadır. Bu ilişkiler üzerinde ise koruma motivasyonunun bir etkisi olduğu varsayılmaktadır.
- Bu çalışmada veri toplama aracı olarak anket yöntemi kullanıldığından katılımcıların anket sorularını doğru anladığı ve samimi bir şekilde cevapladığı varsayılmaktadır.

1.5. Araştırmanın Sınırlılıkları

- Reklamdan kaçınma ve gizlilik endişesini etkileyen farklı yapılar olmasına karşın bu çalışmada reklamdan kaçınma, koruma motivasyonu teorisi kapsamında ele alınan değişkenlerle sınırlandırılmıştır.
- Çalışma çevrimiçi anket uygulaması ile kolayda örnekleme ulaştığından sonuçlar sadece bu çalışmadan elde edilen veriler ile sınırlıdır.

1.6. Tanımlar

Bilimsel araştırmalarda iki tür tanım bulunmaktadır. Bunlar kavramsal ve operasyonel tanım olarak ifade edilmektedir. Kavramsal tanım literatürde ele alınan konuların hangi bağlamda ve yaklaşımla ele alındığını ifade eden kavramsallaştırmaları ifade ederken operasyonel tanım ise bu kavramsallaştırmaların ölçümlemesine ait tanımlamaları içermektedir (Rubin ve Babbie, 2011). Bu çalışmada ele alınan kavramsal ve operasyonel tanımlar ise aşağıda açıklanmıştır.

Tehdit değerlendirmesi: Tehdittin ne kadar ciddi olduğu ve tehditte karşı savunmasızlığın içsel ve dışsal ödüllere oranı ile ölçülen değerlendirmeyi ifade eder (Rogers, 1975). Buradaki tehdit veri gizliliğine yönelik risklerdir.

Algılanan ciddiyet: Bireyin riskin yol açabileceği zararın ciddiyetine ilişkin inancıdır (Boerman vd., 2018). Bu çalışmadaki riskin ciddiyeti, bireyin çevrimiçi davranışsal reklamcılığın kişisel verileri izlemesi, toplaması, kullanması ve paylaşmasından doğabilecek gizlilik risklerinin ne kadar ciddi olduğuna yönelik inançlarını ifade eder.

Algılanan savunmasızlık: Bireyin riskli durumun getireceği olası olumsuz sonuçları deneyimleme ihtimaline olan inancıdır (Boerman vd., 2018). Bu çalışmada savunmasızlık kişinin veri gizliliğine yönelik risklere karşı ne kadar savunmasız olduğuna dair inançlarını ifade eder.

Algılanan fayda: Riskli durumun getirdiği içsel ve dışsal ödülleri ifade eder (Ham, 2017). Çevrimiçi davranışsal reklamlara yönelik fayda kişisel verilerin kullanılmasının getireceği ilgi alanına yönelik reklam, içerik ve ürün tekliflerinin alınmasıdır.

Başa çıkma değerlendirmesi: Tehditle başa çıkma konusunda kişinin öz-yeterlilik ve tepki yeterliliği ile algılanan maliyetlerin oranı ile ölçülen değerlendirmeyi ifade eder (Rogers, 1975).

Öz-yeterlilik: Bireyin bir davranışı başarılı bir şekilde gerçekleştirme becerisine ilişkin inancı olarak tanımlanmaktadır (Maddux vd., 1982). Bu çalışmada öz-yeterlilik çevrimiçi davranışsal reklamların kişisel verileri kullanmasını önlemede ve bu reklamlardan kaçınmada kişinin kendi becerilerine olan inancını ifade eder.

Tepki yeterliliği: Bireyin bir tepkinin tehdidi etkili bir şekilde önleyip önlemediğine dair inancıdır (Witte, 1992). Çevrimiçi davranışsal reklamcılığın kişisel verileri izlemesi, toplanması ve kullanmasını önleyen bazı uygulamaların (çerezleri engelleme, AdBlock-Ghostery gibi uygulamalar kullanma, youronlinechoices gibi araçları kullanarak reklam izleme sistemlerinden çıkma vb.) işe yarayıp yaramadığına yönelik kişinin inancını ifade eder.

Tepki maliyeti: Bireyin önerilen başa çıkma davranışını gerçekleştirmesi sırasında maruz kalacağı kayıplar/maliyetler olarak tanımlanır (Chenoweth vd., 2009). Kişisel verilerin reklam amaçlı kullanılmasını önlemenin getireceği olumsuz sonuç ve yükleri ifade eder. Bu çalışmada maliyetler, çevrimiçi davranışsal reklamların faydasından yararlanamamak, kişisel verilerin korunmasının zamansal ve zihinsel zorluklarını kapsamaktadır.

Gizlilik endişesi: Kişisel bilgilerin başkalarına ifşa edilmesini önleme hakkının potansiyel olarak işgal edilmesinden duyulan endişe derecesi olarak tanımlanır (Beak ve Morimoto, 2012). Bu çalışmada gizlilik endişesi çevrimiçi reklam şirketlerinin kişisel verileri izlemesi, toplaması, kullanması ve paylaşması sonucunda veriler üzerindeki kontrol kaybından doğan endişeleri ifade eder.

Gizlilik kontrolü: Bireyin kişisel bilgilerinin açıklanmasını ve yayılmasını yönetme becerisine ilişkin inançları olarak tanımlanır (Xu vd., 2011). Kişisel veriler üzerinde kişinin kontrol sahibi olup olmamasına yönelik inançlarını ifade eder.

Reklamdan kaçınma: Medya kullanıcılarının, reklam içeriğine maruz kalma oranlarını bilişsel, duygusal ve davranışsal şekilde azaltmaya çalıştıkları eylemlerdir (Cho ve Cheon, 2004). Bu çalışmada reklamdan kaçınma, çevrimiçi davranışsal reklamlara maruz kalmayı engelleyecek bilişsel (örn: görmezden gelme), duygusal (örn: hoşlanmama) ve davranışsal (örn: izleme sisteminden çıkma) kaçınma olarak tanımlanmıştır.

2. ALANYAZIN

Tezin alanyazın bölümü dört temel bölümden oluşmaktadır. Birinci bölümde, çevrimiçi davranışsal reklamın tanımlanmasına ve bu reklamların nasıl çalıştığını ifade eden izleme ve hedefleme kavramlarına yer verilmiştir. Tezin ikinci bölümünde ise gizlilik ve gizlilik endişesi kavramlarına değinilmiştir. Üçüncü bölümde reklamdan kaçınma konusu ele alınmış ve reklamdan kaçınmanın nedenleri ve boyutları incelenmiştir. Tezin son bölümünü oluşturan dördüncü bölümde ise araştırmanın kavramsal çerçevesini oluşturan koruma motivasyonu teorisine odaklanılmış, bu bağlamda gizlilik endişesinin çevrimiçi davranışsal reklamcılıktan kaçınma üzerindeki olası nedenleri incelenmiştir.

2.1. Çevrimiçi Davranışsal Reklamcılık

İnternetin modern anlamda 1990'lı yıllarda gelişmesiyle birlikte internet reklamcılığının da gelişmeye başladığını söylemek mümkündür. 1994 yılında ortaya çıkan banner ve pop-up reklamlar ile birlikte internet reklamcılığının ilk örnekleri oluşmaya başlamıştır. Şirketlerin insanların çevrimiçi davranışsal verilerine dayanarak reklamları hedeflemeye başlaması ise (Bennett, 2011, s. 899-901) dijital reklamcılık faaliyetlerinde yeni bir dönüşüm yaşanmasına yol açmıştır. Bu dönüşümün temelinde ise çevrimiçi davranışsal reklamcılık (ÇDR) yer almıştır. Çevrimiçi davranışsal hedefleme olarak da adlandırılan ÇDR'nin 1990'ların sonlarında DoubleClick şirketinin, kullanıcıları siteler arasında izlemek için 3. taraf çerezleri kullanması ve kullanıcının tarama modellerine göre reklamlar sunmasıyla ilk örnekleri kullanılmaya başlanmıştır. Google 2007 yılında DoubleClick'i satın aldıktan sonra Mart 2009'da AdSense hizmetinin reklamları kullanıcının göz atma davranışına göre hedeflemeye başlayacağını duyurmuştur (Toubiana vd., 2010, s. 1).

ÇDR başlarda daha çok hukuk alanında ve tüketici hakları odağında ele alınan bir kavram ve tartışma konusu olmuştur (örn: Kelley, 2007; Bennett, 2011). Bu doğrultuda kavramın ilk kez FTC raporlarında (FTC, 2007) geçtiğini söylemek mümkündür. Ardından kavramın reklamcılık alanında ve sektörün öz düzenleme raporlarında (örn: DAA) yer aldığı görülmektedir (DAA, 2009). Devam eden süreçte ÇDR artık hem akademinin hem de reklamcılık sektörünün hızla ilgi gösterdiği bir reklamcılık faaliyeti olmaya başlamıştır.

ÇDR'nin tam olarak ne olduğunu açıklamak için literatürde yer alan ÇDR tanımlarına bakmak faydalı olacaktır. Bu nedenle çalışmanın devamında literatürde yer alan farklı ÇDR tanımlarına yer verilerek kavram detaylı olarak açıklanmaya çalışılmıştır.

2.1.1. Çevrimiçi davranışsal reklamcılığın tanımlanması

ÇDR, uygulamacıların yanı sıra akademisyenlerin de ilgi odağı haline gelmiş bir kavram olmasına ve üzerinde çok fazla araştırma yapılmasına rağmen kavramın tanımlanması hala net değildir. Kavramın tanımlanmasında bir netliğin oluşmaması temelde iki nedene dayandırılabilir. Bunlardan ilki; ÇDR'nin çeşitli şekillerde tanımları yapılmış (veriye dayalı reklam, davranışsal hedefleme, ilgi alanına dayalı reklam, kişiselleştirilmiş, özelleştirilmiş reklam, yeniden hedefleme) ve bu da kavramı belirsiz hale getirmiştir. İkincisi ise, net bir bilgi birikimi olmadan çok çeşitli alanlarda ÇDR'ye yönelik nicel araştırmaların (bağımlı, aracı, düzenleyici ve bağımsız değişkenlerin incelenmesi) yapılmasıdır. Bu durum alanın reklamcılar, tüketiciler, bilgisayar bilimcileri ve politika yapıcıları da dahil olmak üzere çeşitli tarafları ilgilendiren disiplinler arası doğasından kaynaklanmaktadır. (Boerman vd., 2017, s. 364).

Günümüzün dijital dünyasında reklamverenler, reklamları kişiselleştirmek ve hedeflemek için tüketicilere yönelik çevrimiçi verileri kullanma fırsatını yakalamıştır. Bu verilere göre düzenlenen ÇDR, profilleme (profiling) ve davranışsal hedefleme (Bennett, 2011 s. 899), reklamları kişinin internetteki önceki gezinme davranışına (surfing behavior) göre ayarlama (Smit vd., 2014, s. 15), teknoloji odaklı (data-driven ad) bir kişiselleştirme yöntemi (Ham ve Nelson, 2016, s. 690), ilgi alanına dayalı (interest based ad) reklamcılık (IAB, 2014a; An vd., 2018, s. 270), davranışsal izleme ve hedeflemeye dayalı özelleştirilmiş (tailored) reklam (Turow vd., 2009; Backes vd., 2012, s. 257), bireyin çevrimiçi davranışlarına ve internet geçmişine dayalı özelleştirilmiş reklam türü (Balebako vd., 2012, s. 1) gibi birçok farklı şekilde tanımlanmıştır. Literatürde kullanılan bu farklı kavramsal tanımlamalar yukarıda da belirtildiği üzere ÇDR'nin tanımındaki belirsizliğin temel nedenini oluşturmaktadır. Yine de genel olarak ÇDR tanımlanırken tüketicinin çevrim içi davranışlarına göre düzenlenen kişiselleştirilmiş ve hedefli reklamın bir türü olduğu ifade edilebilir (McDonald ve Cranor, 2010a, s. 2; Agarwal vd., 2013, s. 1). Özetle bu reklam türü, tüketicilerin potansiyel ilgi alanları hakkında bilgi edinmek ve hem tüketici tercihleri hem de çevrimiçi davranışlarıyla ilgili kişiselleştirilmiş

reklamlar iletmek için kullanıcıları takip etmeye dayanmaktadır (Aiolfi vd., 2021, s. 1093).

ÇDR tanımlarında kullanılan hedefleme ve kişiselleştirme kavramları, ÇDR'ye göre daha geniş bir alanı ifade eder. Hedefli reklamcılığın literatürde zamana, coğrafi konuma, araca (telefon-bilgisayar) göre hedefleme gibi çeşitli sınıflandırmaları söz konusudur (Plummer vd., 2007: Gröne, 2011; Schlee, 2013). Bunlara ek olarak demografik, bağlamsal ve davranışsal hedefleme de hedefli reklamcılığın türleri arasında yer alır. ÇDR'nin anlaşılması için demografik, bağlamsal ve davranışsal hedefleme türleri arasındaki farklılıkları açıklamak doğru olacaktır.

Demografik hedefleme, tüketicileri yaş, cinsiyet, gelir, meslek gibi özelliklerine göre hedeflemeyi içerir (Plummer vd., 2007). Bağlamsal hedefleme, reklam ve tüketici uygunluğunu sağlamak için tüketici verisi yerine mecra verisinin kullanılmasını ifade eder. Teknoloji ile ilgili bir blog sayfasında bilgisayar reklamının yapılması mecraya uygun hedeflemeye örnek verilebilir (Goldfarb ve Tucker, 2011). Davranışsal hedefleme ise reklamların tüketicinin çevrimiçi davranışlarına göre iletilmesini kasteder (Boerman vd., 2017, s. 363). ÇDR bu anlamda hedefli reklamların sadece davranışsal hedefleme türüne karşılık gelir. Ancak bir tüketici, internet gezinme davranışı sonrası belirli ilgi gruplarına ayrılır ve aynı zamanda demografik kategoriler içerisine dâhil edilebilir. Bir tüketicinin ziyaret ettiği web siteleri, onun belirli bir demografik grubun üyesi olarak profillenmesine yol açar. Bu demografik grubu hedefleyen bir reklamın ise ÇDR olup olmadığı her zaman açık olmayabilir. Çünkü demografik veriler genellikle diğer verilerle birleşir. Bu nedenle de demografik hedeflemeyi davranışsal hedeflemeden ayırmanın zor olduğu söylenebilir (Balebako vd., 2012, s. 2).

Kişiselleştirme ise pazarlama (ürün ve hizmet tavsiyeleri), promosyon (örn: sadakat kartları) ve reklam (reklam mesajının kişiselleştirilmesi) gibi geniş bir alanı çevreleyen çevrimiçi ve çevrim dışı uygulamaları olan bir kavramdır (Beak ve Morimoto, 2012, s. 60). Reklam alanında kişiselleştirme ise kişi (isim, fotoğraf, e-posta bilgisi), grup (cinsiyet, etnik köken, meslek vb.) ya da davranış (satın alma geçmişi, ürün ya da marka tercihleri vb.) seviyesinde olabilir (Bang vd., 2019, s. 1116). ÇDR için kişiselleştirilmiş reklam ifadesi kullanıldığında ÇDR'nin sadece davranışsal veriyle sınırlı daha dar bir alanı ifade ettiği unutulmamalıdır (Boerman vd., 2017, s. 363). Literatürde yer alan farklı ÇDR tanımlarının bir özeti Tablo 2.1'de sunulmuştur.

Tablo 2.1. *Çevrimiçi davranışsal reklamcılık tanımları*

Kavram	**Yazarlar ve Yıl**	**Tanımlama**
Çevrimiçi Davranışsal Reklamcılık	FTC (2009)	Kişiye özel reklamların sunulması için tüketicilerin çevrimiçi etkinliklerinin izlenmesidir.
Davranışsal Reklamcılık	McDonald ve Cranor (2010a: s. 2)	Hedefli reklamcılığın bir türü olan davranışsal reklamcılık, hangi reklamın gösterileceğini seçmek için bir bireyin çevrimiçi etkinlikleri hakkında veri toplama uygulamasıdır.
Çevrimiçi Davranışsal Reklamcılık	Bennett (2011, s. 899)	ÇDR, çevrimiçi yayıncılar ve internet pazarlamacıları tarafından reklam kampanyalarının verimini ve etkinliğini artırmak için kullanılan profilleme ya da davranışsal hedefleme türüdür.
Çevrimiçi Davranışsal Reklamcılık	IAB (2014b)	ÇDR, belirli bir bilgisayardan veya cihazdan, zaman içinde kullanıcı tercihlerini veya ilgi alanlarını tahmin etmek üzere verilerin toplanması ve buna uygun reklam sunmak amacıyla Web görüntüleme davranışlarına ilişkin verilerin kullanılması anlamına gelir.
Çevrimiçi Davranışsal Reklamcılık	Smit vd. (2014, s. 15)	Reklamları önceki çevrimiçi gezinme davranışına göre ayarlamaya çevrimiçi davranışsal reklamcılık denir.
Çevrimiçi Davranışsal Hedefleme	Nill ve Aalbert (2014, s. 127)	Çevrimiçi davranışsal hedefleme, tüketicilerin çevrimiçi davranışlarının bir analizine dayanarak tüketicilere ilgili (relevant) mesajları iletmeye yönelik bir tekniktir.
Çevrimiçi Davranışsal Reklamcılık	Ham (2017, s. 634)	ÇDR, dijital medya şirketleri ve reklam ağlarının, tüketicilerin çevrimiçi davranışlarını izleme ve toplama, analiz etme ve ardından bireysel bir kullanıcının ilgi alanları, tercihleri, coğrafi konumları vb. hakkında çıkarımlarda bulunmasını sağlayan teknoloji odaklı bir reklam hedefleme yöntemidir.
Çevrimiçi Davranışsal Reklamcılık	Boerman vd. (2017, s. 364)	ÇDR, insanların çevrimiçi davranışlarını izleme ve toplanan bilgileri insanlara bireysel olarak hedeflenmiş reklamlar göstermek için kullanma uygulamasıdır.

Yukarıdaki tanımlamalara baktığımız zaman bazı tanımlar, tüketicilerin çevrimiçi etkinliklerinin izlenmesine vurgu yaparken (FTC, 2009; McDonald ve Cranor, 2010a; Smit vd., 2014;) bazıları ise (Nill ve Aalbert, 2014; IAB, 2014b; Ham, 2017; Boerman vd., 2017) tüketici verilerinin reklam amaçlı kullanılmasına vurgu yapmaktadır. Tüm tanımlamalardan hareketle Boerman vd. (2017, s. 364) ÇDR için iki basamak olduğunu ifade eder. Bunlardan ilki tüketicilerin çevrimiçi davranışlarının izlenmesi, ikincisi ise toplanan verilerin bireylere hedefli reklamları gösterilmek üzere kullanılmasıdır. Bir sonraki başlıkta ele alınacak olan izleme ve hedefleme kavramları ÇDR sisteminin nasıl çalıştığını anlamaya yardımcı olduğu için kavramın anlaşılmasında da önemli görülmektedir. İzleme ve hedefleme dışında ÇDR çalışmalarında kavram, ayrıca

davranışsal veriden ne kastedildiğinin belirtilmesi ile tartışılır ve böylece kavramın sınırları çizilmeye çalışılır.

ÇDR tanımlamasında vurgulanan davranışsal veri, ziyaret edilen web sitelerini, okunan makaleleri, izlenen videoları, reklam tıklama davranışlarını ve ayrıca bir arama motoruyla aranan her şeyi içerebilir (Boerman vd., 2017, s. 363). Aynı şekilde reklam ağı şirketleri, ÇDR'nin kişisel olarak tanımlanabilir bilgileri (örn: isim ve sosyal güvenlik numarası) izlemediklerini, yalnızca kişisel olmayan bilgileri (örn: belirli bir tüketicinin tanımlayıcı bilgisi olmayan çevrimiçi davranış verileri) izlediklerini belirtirler (Ham, 2017, s. 632). Bazı yazarlara göre ise bu veriler web tarama verilerini, arama geçmişlerini, medya tüketim verilerini (örn: video izleme, makale okuma), uygulama verilerini, satın alma verilerini, reklam tıklama verilerini içermenin yanı sıra kullanıcı tarafından üretilen verileri de (örn: e-posta, sosyal medya postları) içerebilir (Zuiderveen Borgesius, 2015). Hatta davranışsal verinin, web tarama verileri ve kullanıcı tarafından oluşturulan içeriğin yanı sıra mobil cihazlardaki sensörlerin kullanımı, robotik teknolojiler ve giyilebilir cihazlar tarafından izlenen biyometrik kullanıcı bilgileri tarafından üretilen verileri de içerdiği ifade edilmektedir. (Lamberton ve Stephen, 2016, s. 165). Bu durum ise davranışsal veri kavramının çok net çizgilerle ayrılamamasına neden olur.

ÇDR ile ifade edilen davranışsal verinin sadece arama motorlarında bir ürün ve hizmetle ilgili yapılan araştırma ve tıklama verisinden mi yoksa hem mobil hem de sosyal medyayı hatta giyilebilir teknolojiler gibi verileri de içeren daha geniş bir içeriği mi ifade ettiği belirsizdir. Buna ek olarak çevrimdışı ve çevrimiçi davranışı ayıran çizginin bulanıklaşması ile davranışsal verinin sadece tüketicinin çevrimiçi ortamda kasıtlı olarak yaptıkları mı (örn: video izlemesi, bir reklama tıklaması) yoksa bluetooth izleme teknolojileri aracılığıyla kaydedilen diğer çevrimdışı davranışları da içerdiği mi sorusu da gündeme gelebilir (Varnalı, 2021, s.106). Bu nedenle ÇDR'nin kavramsal sınırlaması Varnalı (2021) tarafından şöyle ifade edilir: "Bir davranış, bireysel bir profile bağlı bir veri olarak izlenebildiği, kaydedilebildiği ve çevrimiçi reklamları kişiselleştirebilmek için kullanılabildiği ölçüde çevrimiçi davranış olarak nitelendirilir." Bu şekilde ele alındığında ise ÇDR daha dar bir alandan çıkıp büyük veriye dayalı çevrimiçi reklamları ifade eden geniş bir kavrama dönüşmektedir. Fakat bu durumda ÇDR'nin kişiyi tanımlayan bilgileri içermediği davranışsal veri tanımı reddedilmiş olmaktadır. Bu durum bir sonraki bölümde ele alınacak olan gizlilik tartışmalarının da temel nedenlerinden biri sayılır. Ancak reklamcılık literatüründe ve sektördeki ÇDR tanımlarında davranışsal

veriden kastedilenin web tarayıcı aktiviteleri özelinde tüketicinin ürün ve hizmetlerle ilişkilendirilebilecek ve kişiyi tanımlamayan verileri içerdiği söylenebilir. Ayrıca bu davranışların web site ziyareti, arama terimleri (search terms) satın alma işlemleri, bir reklama tıklama ya da bir ürünü inceleme gibi daha dar ve basit bir çerçevede ele alındığı çevrimdışı veriler ya da bluetooth teknolojileri gibi diğer teknolojilerden bahsedilmediği görülmektedir. Buna dayanarak bu çalışmada ÇDR; "internet kullanıcılarının dijital ortamdaki davranışlarının (web sitesi ziyaretleri, tıklama, ürün inceleme vs.) takip edilerek, ilgi alanına uygun reklamlarla hedeflenmesi" şeklinde kişinin çevrimiçi davranışlarına göre düzenlenen internet reklamları olarak ele alınmıştır. Kavramın daha iyi anlaşılması için nasıl çalıştığını ifade eden izleme (tracking) ve hedefleme (targeting) kavramlarına değinmek yararlı olacaktır.

2.1.2. Çevrimiçi davranışsal reklamcılıkta veri izleme teknolojileri

Mevcut dijital ortam tüketici verisini web sitelerinde gezinirken, sosyal medya aracılığıyla iletişim kurarken ve arama motorlarında bilgi ararken kolayca çevrimiçi olarak erişilebilir hâle getirmiştir. Algoritmalar, reklamverenlerin bu verileri reklamları kişiselleştirmek, bireyleri hedeflemek ve fiyatları düzenlemek için kullanmasına yardımcı olmaktadır. Farklı pazarlama mesajlarıyla farklı segmentleri hedeflemek şu anda pazarlamanın merkezinde yer almakta ve çevrimiçi davranışsal reklamcılık bu manada hızla gelişmektedir. Reklamverenler, sosyal medya analitiği, coğrafi sınırlama, IP (internet protokolü) eşleştirme ve tüketicilerin söylediklerini, dinlediklerini veya izlediklerini dinleyen uygulamalar gibi farklı karmaşık tekniklerle tüketici verisini kullanabilmektedir (Boerman vd., 2021, s. 1).

Dijital ortamda; flash çerezler (flash cookie), web işaretleyicileri (web beacon), tarayıcı parmak izi gibi (browser fingerprint) farklı veri izleme teknolojileri bulunmaktadır (Sipior vd., 2011; Eckersley, 2010). Bu durum ise reklam sürecinin karmaşık ve kafa karıştırıcı bir hâl almasına neden olmaktadır. Ayrıca şirketlerin genellikle veri toplama yöntemlerini açık bir şekilde yayınlamadıklarından dolayı, veri toplamada kullandıkları algoritmalar hakkında tam bir bilgi sahibi olmak imkansızlaşmaktadır (Balebako vd., 2012, s. 1-2). Buna rağmen ÇDR literatüründe veri izleme ve toplama, çoğunlukla tarayıcı tabanlı izleme (Aalberts vd., 2016) olarak da ifade edilen çerezler ile anılmaktadır (Smit vd., 2014, s. 15; An vd., 2018, s. 270).

İlk olarak 1994 yılında Netscape Communications'dan Lou Montulli tarafından tasarlanan çerezler, "kaynak sunucu ile (bir web sitesi) kullanıcı arasında geçen ve kullanıcı tarafından depolanan durum bilgisi' olarak tanımlanmıştır (Bobev, 2021, s. 18). Kısaca çerezin, kişinin web tarayıcısına kaydedilen küçük bir metin dosyası olduğu söylenebilir. Kişi herhangi bir internet sayfasına girdiği zaman, çerezler kişinin web tarayıcısına yüklenir. İlk olarak web sitesinde kullanıcının daha kolay gezinmesine ve web deneyimlerinin kişiselleştirilmesine (örn: dil seçeneklerini hatırlama) olanak sağlamak için kullanılan çerezler (Sipior vd., 2011, s. 2), daha sonra reklam amaçlı veri toplamak için kullanılmaya başlanmıştır. Örneğin bir çerez, web sitelerinde hangi sayfalara ve içeriğe bakıldığı, web sitesinin ne zaman ziyaret edildiği ve web sitesinde bir reklama tıklanıp tıklanmadığı gibi tarama etkinliklerini kaydetmeye olanak tanıyabilir (http-1).

ÇDR sisteminde tüketicilerin internet gezinme davranışlarını izlenmek ve veri toplamak için kullanılan çerez teknolojisi birinci taraf (first-party cookie) ve üçüncü taraf (third-party cookie) çerezler olarak ikiye ayrılır. Birinci taraf çerezler; ziyaret edilen bir web sitesi tarafından doğrudan kullanıcının bilgisayarına yüklenen çerezleri ifade eder (Estrada- Jiménez vd., 2017, s. 37). Üçüncü taraf çerezler ise; reklam şirketleri tarafından birinci taraf olan web sitelerine yerleştirilmiş reklamlarla ilişkili çerezleri ayarlamak için kullanılan çerezlerdir (McDonald ve Cranor, 2010a, s. 7).

Bir web sitesine giriş yapıldığında, o site tarafından kullanıcının web tarayıcısına birinci taraf çerezler yüklenirken aynı zamanda site üçüncü taraf çerezler de kullanabilir. Böyle bir durumda reklam şirketlerinin bu çerezleri de kullanıcının web tarayıcısına yüklenmiş olur. Örneğin bir web sitesinde Facebook beğen butonu olduğunda, ya da bir reklam şirketinin (Oracle, Google Adsense vb.) çerezlerine izin verildiğinde, site aracılığıyla üçüncü taraf olarak adlandırılan bu reklam çerezleri de kullanıcının bilgisayarına yüklenebilir. Bu teknikle çerezler, tüketicilerin başka web sitelerine geçmesi durumunda tanınabilmesi için web tarayıcıyı işaretler. Bu ise reklamverenin çeşitli web sayfaları ve çevrimiçi oturumlar üzerinden veri toplamasına olanak tanır (Aalberts vd., 2016, s. 107). Çerezler yoluyla tüketicinin izlenmesi ve veri toplama aşamasından sonra reklam şirketleri artık tüketicileri uygun olan reklamlarla hedefler.

2.1.3. Çevrimiçi davranışsal reklamcılıkta hedefleme süreci

Tüketicinin çevrimiçi davranışları izlenip veri toplama işlemi sonrasında reklamların hedeflenerek yayınlanması söz konusudur. ÇDR hedeflemesinde, çerezlerle eş olarak birinci taraf ve üçüncü taraf reklamlar olmak üzere iki tür hedefli reklamdan söz edilmektedir. Birinci taraf ÇDR, ziyaret edilen web sitesi tarafından yüklenen birinci taraf çerezlerin aynı zamanda tüketiciye site içinde reklam gösterilmesi amacıyla da kullanılmasıdır (Bennett, 2011, s. 901). Örneğin bir e-ticaret sitesine ikinci kez giriş yapıldığında tüketicinin daha önceki gezinme davranışını birinci taraf çerezle hatırlayan sunucu tüketicinin ilgi alanına yönelik ürün önerileri sunabilir. Üçüncü taraf ÇDR ise birden fazla ve çeşitli web sitesinden bir reklam ağı şirketi gibi üçüncü taraf aracılığı ile veri toplanması ile hazırlanan reklamlardır (Bennett, 2011, s. 901). Örneğin bir web sitesine girdiğimizde bu sitedeki davranışlarımız üçüncü taraf olan aracı bir şirket tarafından da izlenebilir. Şirket birden fazla web sitesinden topladığı verilerle reklamveren için uygun reklamları birden fazla yayıncıya iletir. Reklamverenlerin büyük çoğunluğunun reklamları hedeflemek için bir reklam ağı şirketiyle çalıştığı bilinir (Agarwal vd., 2013, s. 1). Bu nedenle çalışmanın geri kalanında ÇDR olarak bahsedilen reklamlarla üçüncü taraf reklamlar kastedilmektedir.

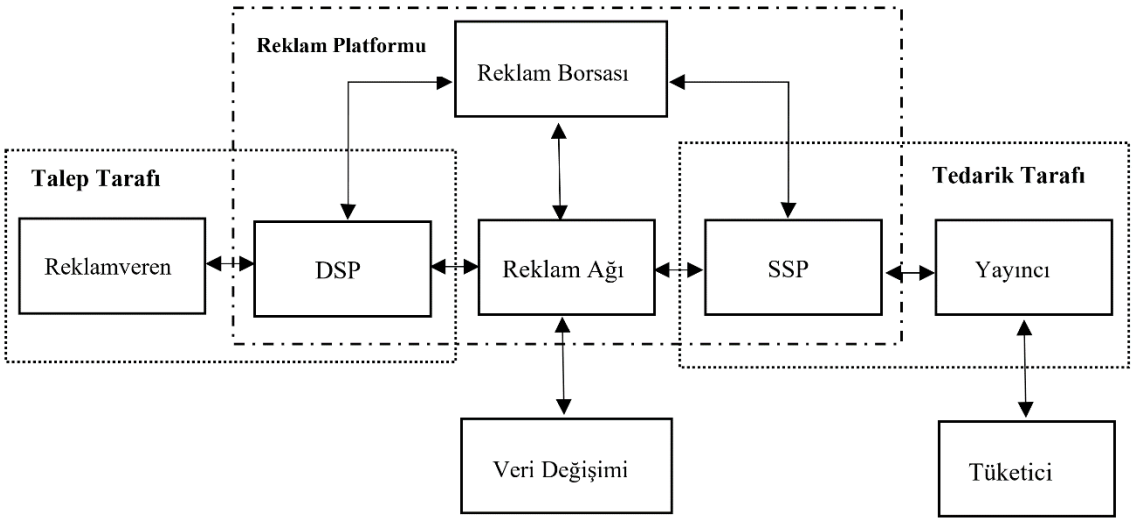
ÇDR'de hedefleme ile kastedilen aslında bu reklamların işleyiş süreci yani sistemin nasıl çalıştığıdır. ÇDR'de reklamverenler veya reklam ajansları, geniş bir profil elde etmek için bireysel bir tüketicinin internet faaliyetleri hakkında bilgi toplar. Toplanan bilgiler analiz edildikten sonra, tüketiciye ilgili (relevant) ve hedeflenmiş mesajlar iletilir. Örneğin, bir tüketici belirli bir hafta sonu için Las Vegas'a uçuş bilgisi arıyorsa bu kişinin otel ücretleriyle de ilgilenebileceği varsayılır ve bu yönde davranışsal veriye dayalı bir reklam iletilebilir (Nill ve Aalberts, 2014, s. 127). ÇDR'nin nasıl çalıştığı ile ilgili bir diğer basit örnek aşağıdaki gibidir:

> "Bir reklamcılık ağı (yani, binlerce web sitesinde reklam yayınlayan bir şirket), tüketicinin web sitesi ziyaretlerini izler. Örneğin, bir tüketici otomobillerle ilgili çeşitli web sitelerini ziyaret ederse, reklamcılık ağı tüketicinin otomobillerle ilgilendiğini varsaymaktadır. Ağ, daha sonra, yalnızca otomobillerle ilgilenen insanlara otomobil reklamları gösterebilir. Dolayısıyla, iki kişi aynı anda aynı web sitesini ziyaret ettiğinde, biri (örn: mobilyalarla ilgili web sitelerini ziyaret eden) mobilya reklamları görebilirken diğeri araba reklamları görebilmektedir" (Boerman vd., 2017, 363).

IAB ise ÇDR çalışma sistemini basit bir dille şöyle özetler: Bir arama motorunu kullandığınızda veya bir web sitesini ziyaret ettiğinizde, ziyaret ettiğiniz siteye ve yaptığınız aramalara bağlı olarak cihazınıza çerez adı verilen küçük bir dosya yerleştirilir.

Böylece beğendiğiniz şeyler hatırlanır, ancak kişisel bilgileriniz (isim, adres, e-posta, cep telefonu) toplanmaz. İlgi alanlarınız bir kitle segmentine eklenir ve bir reklamveren belirli bir kitle segmentini seçebilir. Örneğin bir seyahat şirketi, seyahat kitle segmentini seçebilir ve sizin ve aynı ilgi alanlarına sahip diğer kişilerin ilgisini çekebilecek bir reklam oluşturabilir. Bu reklam daha sonra ziyaret ettiğiniz web sitesine yerleştirilir (http-2).

Ancak üçüncü tarafların ve birden fazla teknolojinin işin içine girdiği ÇDR sistemi daha karmaşık bir yapıyı ifade eder. ÇDR sisteminde reklamveren, yayıncı, reklam ağları (ad network) ya da veri değişimi (ad exchange) sistemleri ile kullanıcılar olmak üzere temelde dört taraf vardır. Yayıncılar (reklamın yerleştirildiği web siteleri), web sayfalarına reklam ağı şirketi için bir bağlantı yerleştirir. Bu şirket bağlantılarının (üçüncü taraf çerez) tek amacı kullanıcı takibidir. Bir kullanıcı web sayfasını görüntülediğinde, kullanıcının web tarayıcısı reklam ağı şirketinin sunucularıyla bağlantı kurar ve bu da şirketin kullanıcıyı tüm ortak yayıncılar arasında izlemesine olanak tanır. Şirket daha sonra yayıncının sayfasında hangi reklamın sunulacağına karar vermek için izlenen veriler üzerinde kendi algoritmasını çalıştırır (Backes vd., 2012, s. 257). Böylece kullanıcılar ÇDR reklamları ile hedeflenmiş olup ilgilendikleri ürün ve hizmet reklamları ile karşılaşır.



Şekil 2.1. *Taraflar arasında etkileşimler ve reklam platformu şeması (Estrada-Jiménez vd., 2017, s. 35)*

Yukarıdaki şekilde çevrimiçi reklamlarda söz edilen birden fazla taraf ve birbiri ile olan etkileşimleri ayrıntılı olarak görülmektedir. Bu tarafların ilki olan reklamverenler, potansiyel müşterilere ilgili reklamları göstererek bir marka veya ürünü tanıtmakla

ilgilenen kuruluşlardır. Yayıncı, genellikle web sayfaları aracılığıyla çevrimiçi içerik (örn: gazeteler, arama motorları, bloglar, vb.) sağlayan bir kuruluştur. Bu kuruşlara reklamverenler, sayfalarında reklam yayınlamaları için ödeme yaparlar. Reklam ağları ise (ad network), yayıncılardan elde edilen toplu reklam envanterini reklamverenlere ve ilgili ajanslara yeniden satmakla ilgilenen GoogleAd- Sense, Media.net ve PulsePoint vb. gibi şirketlerdir. Veri değişimi (veri exchange), reklam ağları dışında veri toplayıcıları (data aggregators or data broker) olarak bilinen şirketlerin oluşturduğu DSP (demand-side platform) ve SSP (supply-side platforms) dışında reklam alışverişi sağlamanın bir başka yoludur (Estrada-Jiménez vd., 2017, s. 34-35). Bahsedilen reklam ağları ya da veri toplayıcı şirketlerin dışında hem yayıncının hem de reklamverenin işini kolaylaştıran iki taraf söz konusudur. Bunlardan ilki olan DSP yani talep tarafı platformu, reklamverenlerin yayıncı ile bağlantı kurmasını sağlayarak yeterli medyayı seçmelerine yardımcı olur. SSP yani satış tarafı platformu ise yayıncının sitesinde reklam satışından elde edilen gelirin en üst düzeye çıkarılmasına yardımcı olan platformdur. Reklam borsası (ad exchange) ise reklam alım ve satımı için açık bir pazar yeri olarak hareket eden platformu ifade eder (http-3). Bu sistem otomatik açık arttırmaya dayalı bir sistemdir ve tüm süreç saniyenin on da biri kadar sürebilir. Bu sistemde reklamveren ve yayıncı arasında reklam ağları gibi aracılar olmaz (Estrada-Jiménez vd., 2017, s. 34-35).

Literatürde aracısız reklam sistemi programatik reklamcılık olarak da bilinir. Programatik reklamlar da sosyal medya, haber siteleri, cep telefonları gibi farklı platform verileri ile reklamları hedefleyebilir. Sadece bir aracıya gerek duymadan reklamveren ve reklam yayıncısı arasında gerçek zamanlı teklif verme (real time biddig) ya da özel pazar yeri (private market place) gibi tekniklerle gerçekleşen otomatik satın alma üzerine kurulu bir sistemi ifade eder (Palos-Sanchez vd., 2019, s. 61-62). Tüm bu bilgiler bize veri sisteminin birçok tarafı olduğu için karmaşık ve tartışmalı olduğunu bu nedenle de ÇDR'nin reklamcılık literatüründe kavramsal olarak net bir zemine oturmadığını göstermektedir. Bu tartışmalar literatürde çoğunlukla ÇDR'nin gizlilik (privacy) konusu ile birlikte ele alınmasına neden olmaktadır. Bu nedenle çalışmanın devamında gizlilik kavramına değinilmiştir.

2.2. Gizlilik Kavramı

Genel olarak gizlilik çalışmaları fiziksel/genel gizlilik (physical privacy) ve bilgi gizliliği (information privacy) olarak iki alt kola indirgenebilir. Fiziksel gizlilik

çoğunlukla beden, özel alan, kamusal alan gibi konuları ele alır. Bilgi gizliliği ise bir kişi veya grubun bilgisine erişim ile ilgilidir. Gizlilik konusundaki ilk çalışmalar, fiziksel gizlilik alanındaki çalışmalardır. Bu temel üzerine bilgi gizliliği çalışmaları geliştirilir ve daha sonra kendi kuramsal yapısını oluşturur (Smith vd., 2011, s. 990). Bu anlamda bu bölümde genel olarak gizlilik kavramının kelime anlamına ve fiziksel gizlilik kavramına değinilerek bir sonraki başlıklarda bilgi gizliliği ve tüketici açısından gizlilik ve gizlilik endişesi kavramlarına değinilecektir.

Etimolojik olarak "*privacy*" kelimesi Latince "*privatus*"tan gelen "*private*" kelimesi kökenine dayanmaktadır. Private; kendine ait olma, paylaşılmamış, kişisel olma (halka açık değil), ayırt edici, kendine özgü (devlete değil), ayrı, mahrum, ayrıcalıklı, gibi anlamlara gelmektedir (http-4). Privacy ayrıca 14. yüzyılda eski Fransızca "*privaute*" kelimesine dayanır ve giz, yalnızlık anlamında kullanılır. 1590'larda özel mesele, giz, 1600'lerde izolasyon, inziva, 1814'te ihlal ya da izinsiz girişten özgür olma durumu anlamlarında kullanılmıştır (http-5). En güncel anlamıyla privacy; "diğer insanlar tarafından gözetlenmekten ya da huzursuz edilmekten özgür/muaf olma durumu" olarak tanımlanmaktadır (http-6). Türkçede ise privacy kelimesi mahremiyet olarak çevrilir. Arapça haram (mahrem) kelimesinin kökeninden gelen mahremiyetin (http-7) ise Türkçe eş anlamlı karşılığı gizlilik (http-8) olarak ifade edilmektedir. Mahremiyet kavramı daha çok beden, özel ya da kamusal alan tartışmalarının yapıldığı fiziksel gizlilik çalışmalarında kullanılmaktadır. Gizlilik kavramı ise daha çok bilgi gizliliği konularında tercih edilmektedir. Hukuk (gizlilik ihlali) ve reklamcılık (gizlilik politikası) alanlarında privacy kelimesinin Türkçe karşılığı olarak gizlilik kelimesinin kullanıldığı sıklıkla görülmektedir. Bu nedenle bu çalışmada da privacy kavramı gizlilik olarak kullanılmıştır.

Gizliliğin kökenleri insanın ve medeniyetin daha ötesinde tüm canlılarla ilişkili bir kavrama dayanır. Mesela hayvan davranışı ve sosyal organizasyon üzerine yapılan araştırmalar, insanın gizlilik ihtiyacının hayvan kökenlerinden kaynaklanabileceğini ve insanlarla hayvanların kendi türleri arasında gizlilik talebinde bulunmak için çeşitli temel mekanizmaları paylaştıklarını göstermiştir (Westin, 1967). Ancak modern yaşamda gizlilik kavramına yönelik tartışmaların ilk örnekleri Yunan siyaset felsefesine dayanır. Özellikle Aristo'nun siyaset felsefesinde kamusal (polis-politik alan) ve özel (oikos-ev içi alan) alan arasında yaptığı ayrımda sadece erkeklere ait olan politik alanı kamusal alan, ev ve aile alanını ise özel alan olarak ayırdığı bilinmektedir. Locke ise bu ayrımı mülkiyet üzerinden açıklar ve kişinin kendi bedenine sahip olduğunu (özel mülkiyet)

diğer mülklerin ise kamuya ait sayıldığını ileri sürer. Ancak kişinin kendi emeği ile elde ettikleri de (örn: balık tutma) kişinin özel mülkiyeti haline gelir (DeCew, 2015, s. 471-472). Hobbes ise gizliliği başkalarının müdahalesi olmadan özgür bırakılma düşüncesi olarak ifade eder. Bir devlet olması gerektiğini düşünür ancak kişilerin müdahaleden uzak özgür olabilecekleri alanların olması gerektiğini de savunur. Aynı şekilde Kant devlet müdahalesinin olmadığı özgür iradeyi gizlilik olarak açıklar. Gizliliğe yönelik bu ilk görüşler, gizliliği açıklayan liberal görüş yaklaşımını ifade eder. Liberal görüşün tersine kamusal alan görüşü ise daha çok gizlilik talep etmenin toplumu bireyselliğe iterek siyasi açıdan pasif hale getirdiğini iddia eder. Bu anlamda özel alan ya da özel mülkiyet gibi talepleri içeren gizlilik anlayışı sorunludur (Masur, 2018, s. 34-37). Aynı şekilde feminist görüş de özel ve kamusal alan ayrımında kamusal alanın erkeklere özgü olduğunu ve kadının ev içinde konumlandığını belirtir. Bu durumun ise genel anlamda gizlilik yaklaşımının toplumsal cinsiyet eşitsizliğini gösteren sorunlu tarafı olduğunu savunur (McClain, 1995; Masur, 2018). 19. yüzyılın sonlarından bu yana kişinin kendi bilgilerini kontrol etmesiyle ilgili olan bilgi gizliliği alanı gelişmiştir (Holvast, 2007, s. 740). Ancak 20. yüzyılın sonlarında meydana gelen bilgisayar teknolojilerindeki gelişmeler ile bilgi gizliliği tartışmaları özellikle son yirmi yılda daha çok kişisel veri gizliliğine yönelmiştir (Keulen ve Kroeze, 2018, s. 35). Bir sonraki başlıkta bu çalışmanın da kapsamında olan bilgi gizliliği konusu daha ayrıntılı ele alınmıştır.

2.2.1. Bilgi gizliliği kavramına yönelik yaklaşımlar

Gizlilik kavramının sosyal bilimler, sağlık bilimleri ve fen bilimleri de dâhil neredeyse bütün bilimsel alanlarda tartışıldığı bilinmektedir (Smith, 2011, s. 992). Özellikle hukuk, siyaset bilimi, sosyoloji ve psikoloji başta olmak üzere (Culnan, 1993, s. 344) birçok alanda uzun bir süredir araştırılmasına rağmen gizlilik kavramının tam olarak ne anlama geldiği hala tartışma konusudur (Solove, 2008, s. 1). Bu tartışmalar bilgi gizliliği kavramı için de geçerlidir.

En genel anlamıyla bilgi gizliliği, bireyin kendisi hakkındaki hangi bilgilerin başkaları tarafından bilinmesi gerektiğine karar verme hakkı olarak tanımlanır. Bu aynı zamanda bu tür bilgilerin ne zaman elde edileceğini ve başkaları tarafından ne şekilde kullanılacağını kontrol etmeyi de içerir (Westin, 2003, s. 431). DeCew (1997, s. 76), bilgi edinme veya edinmeye teşebbüs etme gibi bir bireye erişim sağlamayı içeren durumları bilgi gizliliği olarak ifade eder.

Kuramcılar sıklıkla bilgi gizliliğine konu olan "bireyin kendisi hakkındaki bilgilerin" özel olarak görünen bilgileri içerip içermediğini ve özel olarak görülmeyen bilgileri dışlayıp dışlamadığını incelemişlerdir. Sonuç olarak gizliliğe konu olan bu bilgilerin sadece özel sayılan (tıbbi, ev içi bilgiler vb.) bilgileri içerip diğer bilgileri dışarıda bırakmadığı kabul edilir (Solove, 2008 s. 14). Bu diğer taraftan da gizliliğin anonimlik, saklama, sınırlama, güvenlik gibi kavramlardan ayrılıp ayrılmadığı tartışmalarını gündeme getirir. Çoğu çalışma gizliliğin bu kavramları içinde barındırdığını ancak tamamen aynı şeyi ifade etmediğini belirterek gizliliği tanımlamaya çalışmıştır (örn: Margulis, 2003a; Margulis, 2003b; Tavani, 2008; Smith vd., 2011).

Anonimlik (Anonymity), bir kişinin gerçek kimliğini gizleme yeteneği olarak tanımlanabilir. Gerçek kimliği gizlendiğinde bilgiler bireye geri ilişkilendirilemediği için bu durum gizlilik kontrolünü mümkün kılabilir. Ancak bu kontrolün başka birçok yolu da mevcuttur. Bu nedenle anonimlik gizliliği sağlayabilen durumlardan birisidir. Saklama (Secrecy), kasıtlı olarak bilgilerin gizlenmesi ve genelde potansiyel olarak yanlış bilgi paylaşmak eğilimini ifade eder. Bir bilgiyi gizleme eğilimi, kişinin dışındaki kitle ya da toplum tarafından olumsuz değer verilen bir şeyin gizlenmesi anlamına gelir. Gizlilik ise tam tersine, ahlaki açıdan tarafsız (nötr) olan bilgileri de ifade eder ve toplum tarafından değer verilen davranışları korur. Sınırlama (Confidentiality), sınırlı ancak doğru bilgilerin dışa aktarılması anlamına gelir. Gizlilik, bir kişinin kişisel bilgilerin ifşasını kontrol etme arzusuna karşılık gelirken sınırlama, kişisel bilgilerin, bu bilgilerin kullanılabileceği veya daha fazla açıklanabileceği kapsam ve koşulları sınırlayan bir anlaşma kapsamında, bir bilgi saklayıcısına kontrollü olarak verilmesine karşılık gelir. Yani bir taraf kontrollü ve sınırlı bir şekilde/durumda bilgi paylaşmayı ifade eder. Gizlilik ise kişisel bilgilerin yayılmasını kontrol etme isteği ve hakkını anlatan daha geniş bir kavramdır. Güvenlik (Security) kavramı kişisel bilgilerin kurumlarca korunmasını ifade eder. Kuruluşlar kişisel bilgileri başarıyla güvence altına alabilir ancak yine de kişisel bilgilerin daha sonraki kullanımı konusunda kötü kararlar verebilir ve bu da bilgi gizliliği sorunlarına yol açabilir. Bu nedenle güvenlik gizlilik için gereklidir, ancak güvenlik daha sonraki kullanıma karşı koruma sağlamak, ifşa riskini en aza indirmek veya kullanıcılara güvence vermek için yeterli değildir (Smith vd., 2011, s. 996).

Bilgi gizliliği kavramı genel gizlilik literatüründe olduğu gibi farklı yaklaşımlarla ele alınmış ve tanımlanmaya çalışılmış bir konudur. Bazı görüşler gizliliği, bireyin kendisi veya kendisi hakkındaki hangi bilgilerin başkalarına iletilebileceğini belirleme

iddiası, yetkisi veya hakkı olarak görürken, bazıları kişinin kendisi hakkındaki bilgilerin kontrolü ya da bir kişiye sınırlı ya da koşullu erişimi olarak tanımlar (Schoeman, 1984, s. 2). Bu nedenle bilgi gizliliğinin kavramsallaştırmasını bu yaklaşımlar üzerinden açıklamak faydalı olacaktır.

2.2.1.1. *Hak olarak gizlilik yaklaşımı*

Gizliliğin bir hak olduğu yaklaşımı genel gizlilik tartışmalarında ele alınmış ve bilgi gizliliği tartışmalarının da temelini oluşturmuştur. Hukuk alanına dayanan gizlilik hakkı görüşü ilk kez Warren ve Brandeis tarafından yargıç Thomas Cooley'in 1880'de haksız fiiller üzerine yazdığı ünlü incelemesinden uyarlanan bir ifadeyle, "yalnız bırakılma hakkı" olarak tanımlanmıştır (Solove, 2008, s. 16). Warren ve Brandeis'in (1890) gizlilik hakkı isimli çalışmalarında, siyasi, sosyal ve ekonomik değişimlerin kişisel bilgilerin de korunmasını kapsayacak şekilde yasaların genişlemesine neden olduğunu dile getirilir. Yalnız bırakılma ise devlet veya kurumlar tarafından izinsiz erişim ve gözetimden (surveillance) korunma gibi iki temel hakka sahip olmayı ifade eder. Bu yaklaşım kişilerin sadece fiziki yaralanmalardan zarar görmeyeceğini ileri sürerek genel hukukun gizlilikten kaynaklanan psikolojik ve zihinsel zararları nasıl koruyacağı üzerinde durmuştur. Bu anlamda, edebiyat ve sanat eserleri, iyi niyet, ticari sırlar ve ticari markalar gibi zihnin ürünleri ve süreçlerini kapsayan gayri maddi haklar olarak mülkiyet kavramının sınırlarının genişlemesine olanak tanınmıştır. Ayrıca kişinin özel hayatına ilişkin kişisel bilgilerin kamuya açıklandığı gazete ve fotoğraf gibi teknolojik gelişmelere karşı gizlilik haklarının güvence altına alınmasını kapsamaktadır. Bu görüşün, ABD'de genel olarak "kendisi hakkındaki bilgilerin kontrolü" olarak tanımlanan gizlilik hakkı kavramının temelini attığı söylenebilir (Craig ve Ludloff, 2011, s. 16).

Gizlilik hakkına konu olan davaların ortak temaları arasında yasal uygulamalar (örn: aramalar ve el koymalar); genel kişisellik (örn: kürtajlar ve embriyolar); basın (örn: özel gerçeklerin ifşa edilmesi, şöhret kültürü, izinsiz giriş); röntgencilik (örn: izinsiz görüntüleme ve dinleme); ve işyerinde gizlilik (örn: psikolojik testler, yaşam tarzı izleme) konuları yer almaktadır (Alderman ve Kennedy, 2010). Ancak gizliliği yalnız bırakılma hakkı olarak tanımlayan bu görüş çok geniş kapsamlı olduğu için eleştirilmiştir (Gerety, 1977; Allen, 1988, s. 8). Örneğin Gerety (1977, s. 263) "yalnız bırakılma hakkı" tanımının gizlilikle ilgili her şeyi içinde barındıran ve anlaşılması zor bir arka plan yarattığını sadece hak bulma ve hak arama konularında diğer kavramları dışarıda

bırakabildiğini ve bu anlamda da çok fazla yardımcı olmadığını ifade eder. Ancak bu çalışmanın gizliliği tanımlamaktan çok gizlilik hakkının hukuki sınırlarını tartışmakla ilgili olduğu unutulmamalıdır. Warren ve Brandeis gizliliğin yalnızlık ve başkalarının kişinin özel düşüncelerine erişimi üzerindeki kontrolü gibi yönlerine değinse de makalelerinin asıl odak noktası, bir kişinin özel alanlarıyla ilgili bilgilerin yayınlanması ve bundan kaynaklanan gizlilik ihlalidir. Yazarlar, gizliliğin önemini savunurken hiçbir zaman gizliliğin ne olduğunu tanımlamasalar da onu, bireyin yalnız bırakılma hakkı ve bireyin dokunulmaz kişiliğine duyulan saygı gibi çeşitli diğer değerlerle ilişkilendirmişlerdir (Schoeman, 1984, s. 14).

Bazı yazarlar ise gizliliğin mutlak bir hak olduğu görüşünü eleştirir. Gizlilik mutlak bir haktan ziyade ekonomik bir değere sahiptir (Bennett 1995'ten aktaran Pavlou, 2011, s. 981). Özellikle internetin gelişmesi gizliliğin mutlak bir haktan ziyade maliyet-fayda analizine dayalı ekonomik bir mal (emtia) haline gelmesine etki etmiştir (Campbell ve Carlson, 2002; Davies 1997). Sonuç olarak gizliliğin tanımlanmasındaki ilk örneklerin gizlilik hakkıyla ilişkili olduğu söylenebilir.

2.2.1.2. *Sınırlı erişim yaklaşımı*

Sınırlı erişim teorisine göre kişi, başkalarının kendisi hakkındaki bilgilere erişimini sınırlandırabildiğinde veya kısıtlayabildiğinde bilgi gizliliğine sahip olur. Bu çerçevede, başkalarının kişinin kişisel bilgilerine erişimini sınırlamak veya kısıtlamak için gizlilik bölgeleri yani belirli bağlamlar oluşturulmalıdır (Tavani, 2008). Bu teori Bok (1989), Gavison (1980), Allen (1988) gibi yazarlar tarafından savunulmuştur.

Bok'a (1989, s. 25) göre gizlilik, "başkaları tarafından fiziksel erişim, kişisel bilgi veya dikkat gibi istenmeyen erişimlere karşı korunma durumudur". Yani kişiye hem fiziksel hem kişisel bilgi bağlamında erişimin sınırlanmasını ve bunun korunmasını ifade eder. Gavison (1980, s. 428) ise gizliliği, "başkalarının bir bireye erişiminin sınırlandırılması" olarak tanımlar. Mükemmel gizlilik, bir kişi hakkında bilgiye sahip olmama, ona dikkat etmeme ya da ona fiziksel olarak erişememe durumlarında sağlanır. Bu anlamda, gizlilik (secrecy), anonimlik ve yalnızlık olarak üç durumun varlığından söz edilebilir. Ancak toplumsal yaşamda mükemmel gizlilik ya da gizliliğin tamamen kaybı durumlarından söz etmek çok zordur. Bir kişi kendisi hakkında bilgi sahibi olundukça, ona ilgi gösterildikçe ve fiziksel olarak erişimi arttıkça gizlilik kaybı artar. Bunları sınırlandırdıkça gizliliğe yaklaşır. Allen (1988, s. 3) ise gizliliği, "kişilerin, zihinsel

durumlarına ve onlar hakkındaki bilgilerine başkaları tarafından erişilememe derecesi" olarak tanımlamaktadır. Bu görüş, kişinin kendine erişimi ne kadar sınırlanırsa gizliliğin o kadar artacağını ön görür. Sınırlı erişim üzerine çalışan bir başka yazar olan Moor (1997) ise kontrol odaklı yaklaşımla sınırlı erişim yaklaşımını birleştiren sınırlı erişim/kısıtlı kontrol (restricted access/limited control) teorisini ileri sürer. Moor'un bu yaklaşımında kişi ancak "diğerleri ile ilgili bir durum" söz konusu iken bu durumda izinsiz giriş, müdahale ve bilgi erişiminden korunuyorsa gizliliğe sahip olur. Yazara göre kişiler özellikle internet teknolojilerinin gelişmesiyle birlikte bilgileri üzerinde hiçbir zaman tam kontrole sahip olmazlar ve olmaları da gerekmez. Bilgi paylaşması gerekli ya da faydalı olduğu durumlarda kişi bilginin yayılması açısından korunuyorsa yine de gizliliğe sahiptir. Bu anlamda bilgileri özel bilgiler ve normatif olarak özel bilgiler şeklinde ikiye ayırır. Özel bilgi kişinin kendisine ait, özel olduğunu düşündüğü her türlü bilgiyi içerebilir. Normatif olarak özel olan bir bilgi ise kişinin tıbbi kayıtları, finansal durumu, oy verme tercihleri gibi yasal açıdan da korunması gereken bilgileri içerir. Mesela tıbbi kayıtlar yasal olarak korunan bilgilerdir ve bir hastanede bu kayıtlara sizinle ilgilenen doktor dışında kimsenin erişim izni yoktur. Örneğin evli bir çift ilişkilerindeki sorunlar hakkında tartışırken bu konuşma istenmeyen kişiler tarafından duyulduğunda kişi gizlilik kaybı yaşamış olur. Ancak tıbbi kayıtları başkalarının erişimine açıldığında bu gizlilik kaybının ötesinde gizlilik ihlalidir ve yasal bir soruna dönüşür. Bu anlamda gizlilik için kişisel bilgiler sınırlı bir kontrolde sınırlı bir erişim açısından korunmalıdır. Bu korumalar, kişiyi bilgilendirme (örn: gizlilik politikaları), açık rıza (örn: çerez onayı), ve yasal korumaları içerebilir.

Sınırlı erişimin önemi kabul edilse de bu teori en az üç farklı açıdan eleştirilir. İlk olarak, bazı eleştirmenler sınırlı erişim görüşünün, kişisel bilgilere erişimin kısıtlandığı "özel" ve "kamusal" bağlamlar veya bölgeler arasında yeterli bir ayrım çizmede başarısız olduğunu ileri sürmüştür. İkinci olarak, kısıtlı erişim teorisi gizlilik ile saklama (secrecy) kavramlarının birleştirilmesi olarak yorumlanabilir. Çünkü kişinin kişisel bilgileri başkalarından ne kadar çok saklanabilirse (veya gizli tutulabilirse), o kadar fazla gizliliğe sahip olunacağını öne sürer. Sınırlı erişim teorisinin bir sorunu da kişinin kişisel bilgileriyle ilgili gizlilikten yararlanabilmesi için gerekli olan kontrol veya seçim rolünü göz ardı etme veya en azından ciddi şekilde hafife alma eğiliminde olmasıdır (Tavani, 2008, s. 142). Kişinin kontrolünü ön plana alan bir diğer yaklaşım ise kontrol odaklı yaklaşım olmuştur.

2.2.1.3. *Kontrol odaklı yaklaşım*

Kontrol teorisine göre kişinin gizliliğe sahip olması, kişinin kendisi hakkındaki bilgiler üzerinde kontrole sahip olmasıyla doğrudan bağlantılıdır. Sınırlı erişim teorisini temel alan bu yaklaşım, kişinin kontrolünü ön plana çıkarır. Bu yaklaşım, Westin (1967), Miller (1971), Altman (1975), Rachels (1975), Petronio (2002), gibi yazarlar tarafından dile getirilmiş ve savunulmuştur.

Fried'a göre, gizlilik, "sadece başkalarının zihninde bizimle ilgili bilgilerin yokluğu değildir; daha ziyade kendimiz hakkında sahip olduğumuz bilgiler üzerindeki kontrolümüzdür" (Fried, 1990'dan aktaran Tavani, 2008, s.142). Yani Fried'e göre gizlilik sadece kimse bizim hakkımızda bilgi sahibi değilse ya da fiziksel erişimleri yoksa oluşmaz kendi bilgilerimiz üzerinde kontrol sahibi olduğumuzda oluşur. Benzer şekilde Rachels (1975, s. 297) gizliliği, "hakkımızda kimin bilgiye erişebileceğini kontrol etme yeteneğimiz ile farklı türde ilişkiler yaratma ve sürdürme yeteneğimiz" olarak tanımlar ve gizliliği yalnızlıktan ayırır. Kişinin sosyal ve yakın ilişkiler kurarken kişisel bilgileri üzerinde de kontrole sahip olduğu bir durumda gizliliğin var olduğunu ifade eder. Miller (1971, s. 25), gizliliği "bireyin kendisiyle ilgili bilgilerin dolaşımını kontrol etme yeteneği" olarak ifade eder. Miller ise bilgilere erişimden ziyade bilgilerin dolaşımı üzerine kontrole odaklanır. Kişiye özel bilgiler sosyal hayatta kişinin isteği ve kontrolüyle paylaşılabilir. Ancak özellikle teknolojik gelişmeler bu bilgilerin nasıl dolaşıma girdiği ve kimlerle paylaşıldığı üzerindeki kontrolün kaybedilmesine neden olabilmektedir. Bilgi gizliliği alanında önemli çalışmalara imza atan Westin (1967, s. 7) tarafından gizlilik "kişinin kendisi hakkındaki bilgilerin başkalarına ne zaman, nasıl ve ne ölçüde iletileceğini belirlemek" olarak tanımlanmıştır. Yazar daha önceki tanımlamaları biraz daha detaylandırmıştır. Kişisel bilgiler üzerindeki kontrolü, bu bilgilere kimlerin erişeceği üzerindeki kontrolün yanı sıra bilgilerin ne zaman, hangi yolla ve ne kadarının paylaşılacağı üzerindeki kontrol olarak genişletmiştir.

Gizlilik çalışmalarında ve kontrol teorisindeki bir diğer önemli isim olan Altman'a (1975) göre ise gizlilik, "kendine erişimin seçici kontrolüdür" (Altman, 1975'ten aktaran Margulis, 2003a, s. 418). Kontrol odaklı gizlilik yaklaşımında Westin, Altman ve Petronio'nun teorileri literatürde kabul görmüş ve birçok farklı çalışmada test edilmiş teoriler olarak ön plana çıkmaktadır (Margulis, 2011; Moloney ve Bannister, 2009). Bu nedenle bu teorilere ayrıntı olarak yer verilmiştir.

Gizlilik durumları teorisi

Westin'e (2003) göre bir toplumda gizlilik; politik düzey, sosyo-kültürel düzey ve bireysel düzey olmak üzere üç düzeyde var olur. Siyasi düzeyde gizlilik, bir toplumun siyasi felsefesine dayanmaktadır. Örneğin otoriter toplumlarla demokratik toplumlar arasında kamu düzeni açısından özel alana ne kadar değer verildiği konusunda bir fark vardır. Sosyo-kültürel düzeyde gizlilik, insanların başkalarının gözleminden özgürleşmek için sahip oldukları gerçek fırsatları ifade eder. Bu anlamda gizlilik sıklıkla bireyin gücü ve sosyal statüsü tarafından belirlenir. Bireysel gizlilik ise, bireylerin ilişkilerinin düzeyine odaklanır. Bireysel gizlilik dengeleri kişinin aile yaşamının, eğitiminin, sosyal sınıfının ve psikolojik yapısının bir fonksiyonudur. Gizliliğin bu boyutu, her bireyin özel ihtiyaçlarını ve arzularını yansıtır ve yaşam döngüsündeki ilerleme ve durumsal olaylar açısından sürekli olarak değişecektir. Westin (2003) gizlilik durumları teorisini bireysel düzeyde tanımlar ve bireyin kontrolünü merkeze alır.

Westin'in (1967) gizlilik durumları teorisine göre bireyin gizlilik arzusu asla mutlak değildir, çünkü topluma katılım da aynı derecede güçlü bir arzudur. Böylece her birey, içinde yaşadığı toplumun belirlediği çevresel koşullar ve sosyal normlar ışığında, gizlilik arzusunu, kendisini başkalarına açıklama ve iletişim arzusuyla dengelediği kişisel bir uyum süreciyle sürekli olarak meşgul olur. Birey bunu başkalarının merakından ve her toplumun kendi sosyal normlarını dayatmak için oluşturduğu gözetim süreçlerinden kaynaklanan baskılar karşısında yapar. Westin (1967) gizliliğin yalnızlık (solitude), yakınlık (intimacy), anonimlik (anonimity) ve sakınma (reserve) olarak dört durumda gerçekleştiğini söyler.

- Yalnızlık: Gizliliğin ilk halidir. Bireyin gruptan ayrı olması ve diğer kişilerin gözleminden uzaklaşması durumudur. Yalnızlık durumunda kişi fiziksel uyaranlara (örn: gürültü, koku) maruz kalabilir, iç huzuru bundan rahatsız olmaya devam edebilir ya da gizlice izlediğinden korkabilir. Ancak tüm bu fiziksel ve psikolojik müdahalelere rağmen yalnızlık, bireylerin elde edebileceği en eksiksiz gizlilik durumudur.
- Yakınlık: Gizliliğin ikinci durumu olan yakınlıkta birey, iki veya daha fazla kişi arasında yakın, rahat ve samimi bir ilişki kurabildiği küçük bir birimin parçası olarak hareket eder. Yakın ilişkilerin olduğu ortamda (evlilik, arkadaşlık vb.) kişi için gizlilik durumundan bahsedilebilir.

- Anonimlik: Gizliliğin üçüncü durumu olan anonimlik, bireyin halka açık yerlerde olması veya kamusal eylemlerde bulunması durumunda yine de kimlik tespitinden ve gözetimden uzak olma özgürlüğüdür. Tanınmama kişiye belli oranda gizlilik sağlar.
- Sakınma: Son gizlilik durumu olan sakınma, istenmeyen müdahalelere karşı psikolojik bir bariyerin yaratılmasıdır. Kişi yaşamı boyunca her zaman yalnızlık veya anonimlik durumlarında olmaz. Toplumsal yaşamda yakın ya da resmi ilişkiler kurar. Her iki ilişki durumunda da kişi kendisiyle ilgili her bilgiyi paylaşmayabilir. Bu, bireyin kendisiyle ilgili iletişimi sınırlama ihtiyacına etrafındakilerin katılması ve saygı duyması durumunda ortaya çıkar.

Ayrıca gizliliğin; kişisel özerklik, duygusal rahatlama, öz değerlendirme ve sınırlı-korumalı iletişim olarak dört işlevi de vardır:

- Kişisel özerklik (personal autonomy): Kişisel özerklik, başkaları tarafından manipüle edilmekten ve hükmedilmekten kaçınma arzusunu ifade eder. Gizlilik bireylere özerklik imkânı tanır.
- Duygusal rahatlama (emotional release): Duygusal rahatlama, kişinin toplumsal yaşamın getirdiği toplumsal rol gerilimlerinden kurtulmayı ifade eder.
- Öz değerlendirme (self-evaluation): Gizlilik bireylere bilgi akışını, olası sonuçları ve alternatifleri değerlendirme ve böylece mümkün olduğunca tutarlı ve uygun şekilde hareket etme olanağı sağlar.
- Sınırlı ve korumalı iletişim (limited and protected communication): Kişiler arası sınırları belirlemeyi ve kişisel bilgilerin güvenilen çevreyle paylaşılmasını ifade eder.

Westin gizliliği, toplumsal ve kişisel ilişkiler durumlarında kişinin kendisi hakkındaki bilgileri ne kadar paylaşacağını kontrol etme süreci olarak açıklar. Tüm bu durumlarda gizlilik kişiye özerklik, rahatlama, öz değerlendirme ve daha korunaklı bir iletişim sunar. Bilgi gizliliğinin temelini oluşturan Westin'in çalışmaları birçok araştırmada temel alınmıştır. Ancak yine de Westin'nin teorisi bazı yönlerden eleştirilir. Örneğin gizliliğin dört işlevi olduğunu ifade eden teoride bu işlevlerin birbiri ile bağlantılı mı yoksa bağımsız mı hareket ettikleri net değildir. Gizlilik durumları aslında gizliliğin belirli boyutlarını mı ifade etmektedir ya da teoride hiyerarşik bir yapı var mı gibi belirsizlikler bulunduğu söylenebilir (Margulis, 2011, s. 11).

Gizlilik düzenleme teorisi

Gizlilik tanımını kontrol üzerinden yapan bir diğer araştırmacı ise Irwin Altman'dır. İlk olarak 1975 yılında geliştirdiği teoride Altman gizliliği, kendine veya grubuna erişimin seçici kontrolü şeklinde tanımlar. Bu tanımdan da anlaşılacağı gibi Altman gizliliğe; birey, grup ve davranış boyutuyla odaklanır. Çevrenin gizliliği düzenleyen bir unsur olduğunu ifade eder ve ona göre gizlilik düzenlemesinin dört özelliği vardır (Altman, 1977):

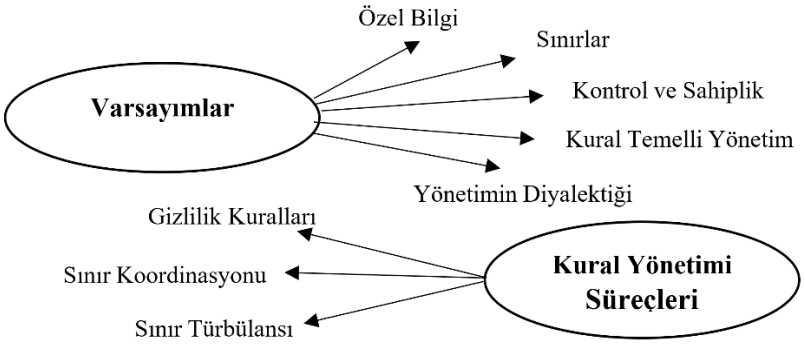
- Dinamik diyalektik bir süreç: Gizlilik tek yönlü bir uzak durma veya geri çekilme süreci değil başkalarıyla dinamik ve diyalektik bir etkileşimi ifade eder. Bu haliyle gizlilik, insanların bazen kendilerini başkalarına açık ve erişilebilir hale getirdiği, bazen de kendilerini başkalarına kapattığı bir sınır kontrol sürecidir. Zaman içinde ve koşullarla birlikte açık veya kapalı olmayı gerektirebilir.
- Bir optimizasyon süreci: Gizliliğe ilişkin geleneksel görüşler genellikle monotonik bir süreci ima eder; yani kişi ne kadar çok gizliliğe sahipse o kadar iyi durumdadır. Bu teoride ise çok az ya da çok fazla gizliliğin kişiyi memnun etmeyeceği, ortalama bir gizlilik seviyesinin olması gerektiği düşünülür. Bu yaklaşım kalabalıklaşma ve sosyal izolasyon kavramlarını gizlilik ile bütünleştirmektedir. Kalabalıklaşma, istenen etkileşim düzeyinden çok fazla yönde bir sapma, izolasyon ise çok az yönde bir sapmadır.
- Çok mekanizmalı bir süreç: Bir ben-öteki sınır kontrol süreci olarak gizlilik, insanların arzu edilen sosyal etkileşim seviyelerine ulaşmak için kullandıkları bir davranış mekanizmaları ağını içermektedir. Bu mekanizmalar arasında kişisel alan ve bölge belirleme gibi sözel ve sözsüz davranışlar ile kültürel olarak tanımlanmış yanıt verme tarzları yer almaktadır. Dolayısıyla gizlilik düzenlemesi, sosyal etkileşimin yönetiminde fiziksel çevreden çok daha fazlasını içerir. Dahası, bu davranışsal mekanizmalar bir sistem olarak işlemektedir. Bu nedenle, karşılıklı dayanışma içeren, dengeleyici ve ikame edilebilir eylem özelliklerini içerirler. Yani, bir kişi koşullara bağlı olarak istenen düzeyde bir gizlilik elde etmek için farklı davranış karışımları kullanabilir. Ya da farklı insanlar ve kültürler gizliliği düzenlemek için benzersiz mekanizma karışımlarına sahip olabilir.
- Gizlilik fonksiyonları: Gizlilik üç işleve hizmet eder: (a) sosyal etkileşimin yönetimi, (b) başkalarıyla etkileşim için plan ve stratejilerin oluşturulması ve (c) öz kimliğin geliştirilmesi ve sürdürülmesi.

Altman teorik çerçevesinde gizliliğin bir dizi önemli yönünü vurgular. Birincisi, gizlilik doğası gereği sosyal bir süreçtir. İkincisi, gizliliğin psikolojik yönlerinin doğru bir şekilde anlaşılması için kavram, insanların etkileşimini, sosyal dünyalarını, fiziksel çevreyi ve sosyal fenomenlerin zamansal doğasını içermelidir. Üçüncüsü, gizliliğin kültürel bir bağlamı vardır, psikolojik tezahürler kültüre özgüdür.

Altman'ın gizlilik kavramsallaştırması Westin ile pek çok yönden benzerlik gösterir. Her iki teori de sınırlı erişim ve kontrol yaklaşımlarını birleştirir. Her ikisi de gizlilik süreçlerini ve sınıflandırmalarını tartışır. Sadece Altman gizlilik süreçlerine öncelik verirken Westin gizlilik sınıflandırmalarına öncelik verir. Her iki yaklaşım birey ve grup düzeyinde gizliliği tartışırken kültürün etkisini de vurgular. Altman daha çok psikolojik süreçlere vurgu yaparken Westin politik sistemlerin etkisini tartışır. Bu nedenle Westin gizlilik ihlallerine daha çok atıfta bulunur. Farklılaştıkları bir diğer nokta ise Altman'ın teorik çerçevesinin daha kapsamlı olmasıdır (Margulis, 2011).

İletişim gizliliği yönetimi teorisi

Petronio'nun iletişim gizliliği yönetimi teorisinin temelleri, 1991 yılında iletişimin sınır yönetimi (communication boundary management) adlı çalışmasına dayanır. Bu çalışmada Petronio özel bilgilerin (private information) ifşa edilmesini (disclosure) düzenleyen bir dizi süreç sunmaktadır. Özel bilgilerin başkalarıyla paylaşılması birtakım riskleri barındırabilir. Kişinin bu riskleri yönetebilmesi için belli sınırlar koyması gerektiği üzerinde durulmaktadır (Petronio, 1991, s. 311). Daha sonra bu sınırları ve bu sınırların yönetilme süreçlerini iletişim gizliliği teorisinde (Şekil 2.2) birleştirmiştir.



Şekil 2.2. *İletişim gizliliği yönetimi teorisi (Petronio, 2022, s. 35)*

Teori iletişim sürecini, kişilerin özel bilgilerinin açıklanması ya da gizli kalması üzerindeki kararlarının bir dengesi olarak ifade eder. Bunu ise temel varsayımlar ve kural yönetimi süreçleri olarak iki kavramsal yapıyla ele alır. Söz konusu olan temel varsayımlar aşağıda listelendiği gibidir (Petronio, 2002):

1. **Özel bilgi:** Temel varsayımların ilk basamağı özel bilgilerin ifşasını kapsar. Özel ifşa ise başkalarına ve bize ait özel bilgilerin anlatılması süreciyle ilgilidir.
2. **Gizlilik sınırları:** Teori, özel bilgileri paylaşma sürecinde kişisel sınır ve kolektif sınır kavramlarına vurgu yapar. Özel bilgiler paylaşıldığında, bu paylaşım kolektif bir sınır oluşturur. Diğer yandan, özel bilgiler bir kişi tarafından saklandığında ve ifşa edilmediğinde, bu durum kişisel sınır olarak adlandırılır.
3. **Kontrol ve sahiplik:** Kişiler kendilerine ait özel bilgilere sahiptir. Bu nedenle birey kendi sahip olduğu bir bilgiyi kiminle paylaşacağını belirlerken kontrol yoluyla istenmeyen erişimlerden bilgiyi korur.
4. **Kural temelli yönetim sistemi:** Kural yönetim sistemi, üç yönetim sürecine bağlıdır. İlk süreç, kuralların gelişme şeklini ve özelliklerini temsil eden gizlilik kuralı temelleridir. İkincisi, sınır koordinasyon sürecidir. Bu süreç, insanlar kolektif sınırları yönetirken gizliliğin kurallar aracılığıyla nasıl düzenlendiğini yansıtır. Üçüncüsü, sınır türbülansı, koordinasyonun her zaman senkronize bir şekilde işlemediği varsayımını ifade eder. Sınır türbülansı, sınır koordinasyonunun ne zaman bozulduğunu ve kuralların senkronize olmadığını gösterir.
5. **Yönetimin diyalektiği:** Özel bilgileri ifşa etme veya gizleme kararının verildiği her yerde bir diyalektik söz konusudur.

İletişim gizliliği yönetimi teorisi içerisinde yer alan kural yönetimi süreçleri ise teoride aşağıda gösterildiği üzere üç süreç içerisinde ele alınmaktadır (Petronio, 2002):

1. **Gizlilik kuralları temeli:** Genel olarak, kural temelleri kavramı kuralın gelişimi ve özellikleri olarak iki noktaya odaklanır. Kuralların geliştirilmesi için bireyler kültürel beklentiler, cinsiyet, motivasyon, durumun bağlamı ve risk-fayda oranı gibi belirli kriterleri kullanırlar. İkinci boyut için, kuralların dört özelliği vardır. Birincisi, stabilize olabilirler ve insanlar için rutin hale gelebilirler. İkincisi, kurallar o kadar kalıcı hale gelebilir ki, gizlilik yönelimlerinin temelini oluştururlar. Üçüncüsü, kurallar da değişebilir. Dördüncüsü, kuralların kullanımını kontrol etmek için insanların kurduğu yaptırımlar söz konusu olabilir.

2. **Sınır koordinasyonu:** Kişisel bilgi sınırları; sınır bağlantısı ve sınır mülkiyet hakları ve sınır geçirgenliği olarak üç farklı şekilde düzenlenir. Sınır bağlantısı, sınır ittifaklarını oluşturan bağlantıları temsil eder. Sınır mülkiyeti ise bilgiye sahip olan tarafların algıladığı ayrıcalık ve hakları ifade eder. Sınır geçirgenliği, bilgiye açık ve kapalı erişimi ifade eder. Kişisel bilgileri ifşa etmede ne kadar esnek ya da katı olunmasıyla ilgilidir.
3. **Sınır türbülansı:** Sınır koordinasyonunda sorunlar olduğunda sınır türbülansı yaşanır. Örneğin taraflardan birinin gizliliği ihlal etmesi ya da kötüye kullanması, bir tarafın daha fazla risk hissetmesi gibi durumlarda sınır türbülansı gerçekleşmiş olur.

Gizliliği açıklamada kullanılan bu yaklaşımlar, gizlilik hakkına odaklananlar, gizliliğin sınırlı bir erişimle mümkün olduğunu ifade edenler ve bireyin kontrolünü ön plana alanlar olarak farklı şekillerde gizliliği tanımlamaya çalışmışlardır. Gizlilik hakkı daha çok hukuk alanında ele alınan bir yaklaşımdır. Gizlilikte sınırlı erişim ve kontrolü açıklayan dört temel teoride (Moon, Westin, Altman, Petronio) ise ortak nokta gizliliği kişisel bilgiler odağında, kültürel ve ilişkisel bağlamlarda ele almalarıdır. Altman ve Petronio'nun yaklaşımları daha çok kişiler arası ilişkilerde gizliliğin düzenlenmesine atıfta bulunurken Moor ve Westin ise daha çok gizlilikte veri kullanımında sınırlı erişim ve kontrole atıfta bulunur. Ancak Westin kişisel bilgiler üzerinde kişiye daha çok kontrol verilmesi gerektiğini savunurken Moor kişisel verilere sınırlı erişimi ve yasal olarak korunmayı ön plana almıştır.

Yukarıda ele alınan gizlilik çalışmalarının ilk örneklerinde gizlilik; hukuk, kişiler arası iletişim, siyasal iletişim gibi farklı alanlardaki çalışmaların bakış açısını yansıtmaktadır. Çoğu zaman kavramsal bütünlüğü aynı olsa da gizliliğe yönelik uygulamalarda konunun bağlamından kaynaklı farklılıkların görünmesi muhtemeldir. Özellikle teknolojinin getirdiği yenilikler ile birlikte gizlilik konularında ve korumaya yönelik uygulamalarda dönüşümlerin olması kaçınılmaz olmaktadır. Bu bakış açısıyla Nissenbaum, örneğin teknoloji tabanlı sistemlerin kullanımının neden gizlilik adına kaygıyı, korkuyu ve direnci tetikleyebileceğini açıklamaya yardımcı olmak için, bağlamsal bütünlüğe dayalı bir bilgi gizliliği teorisi ortaya koyar. Ona göre gizlilik hakkı "ne gizlilik hakkı ne de kontrol hakkıdır, ancak kişisel bilgilerin uygun şekilde akışı hakkıdır" (Nissenbaum, 2009'dan aktaran Bleier vd., 2020). Temelde fikir, başkası hakkında bilgi ileten birinin bu bilgiyi nasıl ve nereye iletebileceği konusunda

kısıtlanması gerektiğidir. Bu tür bilgi akışlarının uygunluğu, bilginin sağlık, eğitim, istihdam veya pazar gibi bir sosyal bağlamda nasıl paylaşılmasının beklendiğini tanımlayan bağlama bağlı bilgi normları tarafından yönetilir. Bilgi akışları yerleşik normlara bağlı kaldığında bağlamsal bütünlük bozulmaz, bilgi akışındaki kesintiler ise gizliliğin ihlaline yol açabilir (Nissenbaum, 2004'den aktaran Bleier vd., 2020).

İnternet teknolojilerindeki gelişmelerle birlikte gizliliğe konu olan kişinin kendisi hakkındaki bilgiler, kişisel veriler (personal data) olarak ifade edilmeye başlanmıştır. Bilgi gizliliği yaklaşımları reklamcılık ve pazarlama iletişimi bağlamında tüketici veri gizliliği ve gizlilik endişelerinin de konusu olmaktadır. Tüketici veri gizliliği ve gizlilik endişesi çalışmalarında daha çok tüketici verisinin kontrolü ön planda olduğundan bu çalışmada da gizlilik, kontrol odaklı yaklaşım perspektifinden ele alınmıştır. Bu nedenle bir sonraki başlıkta çevrimiçi ortamda tüketici veri gizliliği ve gizlilik endişeleri ele alınmıştır.

2.2.2. Tüketici bilgi gizliliği ve gizlilik endişesi

Bilgi gizliliği konusu tarihsel olarak sosyolojik ve teknolojik gelişmelerden etkilenerek dönüşüme uğramış ve bu dönüşümler kendi dönemlerine uygun yasal düzenlemeleri de beraberinde getirmiştir. Westin (2003) bilgi gizliliğinin gelişimini tarihsel olarak (Tablo 2.2'de gösterildiği gibi) dört ana döneme ayırmaktadır.

Tablo 2.2. *Gizlilik dönemleri (Westin, 2003, s. 435):*

Dönemler	Tanımlar
Gizliliğin Temel Çizgisi 1945-1960	Sınırlı bilgi teknolojisi gelişmeleri, iş ve hükümet sektöründe yüksek kamu güveni ve bunun getirdiği bilgi toplamada genel rahatlık söz konusu. Bu dönemde gizlilik üçüncü düzey bir sosyal mesele olarak görüldü.
İlk dönem: Çağdaş Gizliliğin Gelişimi 1961-1979	Bilgi gizliliğinin açık bir sosyal, politik ve yasal sorun olarak artması. Yeni teknolojilerin potansiyel karanlık taraflarının erken tanınması, Adil Bilgi Uygulamaları ve 1974 Gizlilik Yasası gibi kurulan hükümet düzenleyici mekanizmaların çerçevesinin oluşturulmasına etki etti. Gizlilik ikinci düzey sosyal ve politik bir mesele haline geldi.
Gizliliğin Gelişiminin İkinci Dönemi 1980-1989	Bilgisayar ve ağ sistemlerinin yükselişi, veri tabanı yetenekleri, 1980 Gizlilik Koruma Yasası, 1984 tarihli Kablolu İletişim Politikası Yasası, 1988 Video Gizlilik Koruma Yasası da dâhil olmak üzere yeni teknolojiler için tasarlanmış mevzuat gelişti. Avrupa ülkeleri hem özel hem de kamu sektörleri için ulusal veri koruma yasalarına geçti.
Gizliliğin Gelişiminin Üçüncü Dönemi 1990-2002	İnternet, mobil teknolojiler, veri madenciliği gibi teknolojilerin yükseldiği dönemi ifade eder. Web 2.0 ve 11 Eylül saldırısı gibi etkenler bilgi alışverişi ortamını önemli ölçüde değiştirdi. Dünya çapında iletişim, ticaret, seyahat ve pazarlama faaliyetlerinin artması sebebiyle gizlilik sorunları küreselleşti. Rapor edilen gizlilik endişeleri yeni seviyelere yükseldi.

Tablo 2.2'de yer alan gizlilik dönemlerine bakıldığında teknolojideki gelişmelerle birlikte kişisel verilerin gizliliği hem daha çok ihlal edilmeye başlanmış hem de artan gizlilik endişeleri gizliliği korumaya yönelik politikaların artmasına zemin hazırlamıştır. Ayrıca önceleri kamu ve devlet gözetimini içeren gizlilik konusunun gitgide pazarlamanın konusu haline gelmeye başladığı görülmektedir.

19. yüzyılda başlayan ve 20. yüzyılda gelişen kitlesel pazarlama ile bilgi gizliliği konusu devlet ve kamu alanlarındaki gözetim ve bilgi toplamadan özellikle reklam ve pazarlama gibi alanlarda özel sektörde de kendini göstermeye başlamıştır. Tüketicilerin ürün hakkındaki görüşlerinin yanı sıra yaşam tarzları ve psikolojik veriler toplanarak hedefleme için kullanılmıştır. Hedefli pazarlamadaki gelişmeler ilk olarak doğrudan postalama yoluyla kendini göstermiş, 1970'li yıllarda ise tele-marketing (telefonla pazarlama) türü keşfedilmiştir. Geri dönüşlerin azlığı hedefleme tekniklerinin daha kesin hale getirilmesine neden olmuştur, ancak bunun için daha fazla tüketici verisinin toplanması, saklanması ve analiz edilmesi de söz konusu olmuştur. Önce demografik olarak 80'li yıllara doğru ise görüşler, tutumlar, inançlar ve yaşam tarzı gibi psikolojik özellikler hakkındaki psikografik verilerin analizleriyle tüketiciler hedeflenmeye başlanmıştır. Veriye dayalı pazarlamanın ilk örneklerini oluşturan bu yöntemleri e-posta ve sms reklamcılığı gibi uygulamalar izlemiştir. İnternet teknolojisindeki gelişmeler sayesinde tüketici verisinin toplanması ve analizindeki kolaylıklar çevrimiçi reklamcılıkta tüketici verisinin kullanılmasına zemin hazırlamıştır (Solove, 2000). Bu uygulamaların gelişmesi gizlilik konusunun reklamcılık alanında da ele alınmasına sebep olmuştur.

Culnan ve Bies'e (2003) göre tüketici gizliliği konusu literatürde, tüketici gizliliğine ilişkin kurumsal perspektif, aktivist perspektif ve merkezci perspektif olmak üzere üç farklı perspektifin merkezinde yer almaktadır. Kurumsal bakış açısına göre şirketler toplum için ekonomik büyüme ve kalkınmanın birincil yaratıcısıdır. Şirketin tüketicilere ilişkin kişisel bilgilere erişme becerisine getirilen herhangi bir kısıtlama yalnızca şirketin pazarda verimli bir şekilde faaliyet gösterme becerisini tehlikeye atmaz aynı zamanda sosyal sorumluluğunu yerine getirme becerisini de engeller. Bu görüşün aksine aktivist bakış açısı, eğer serbest piyasa güçleri ve teknolojideki ilerlemeler kontrol edilmezse, bilginin herhangi bir amaç için herkesin kullanımına açık olacağını, bunun da gizlilik hakkını ihlal edeceğini ve topluma zararlı sosyal maliyetler yükleyeceğini savunur. Merkezci perspektif ise kurumsal ve aktivist perspektifler arasında bir orta yol

getirir. Canlı bir ekonomide tüketicilerin seçimlere sahip olması gerektiğini ancak kişisel bilgilere makul bir oranda kurumsal erişime izin verilirse bu seçimlerin tüketiciyle daha alakalı olabileceğini savunur. Merkezcilere göre, kurumsal olarak kişisel bilgilere erişim, tüketicilerin meşru gizlilik haklarına karşı dengelenmelidir; bu hakların korunması öz denetim, yasalar ve teknoloji tarafından sağlanmaktadır.

Lanier ve Saini (2008) ise tüketici gizliliği literatürünü tüketici gizliliğinin kavramsallaştırılması, firma ile ilgili gizlilik, tüketici ile ilgili gizlilik olarak üç ana başlıkta inceler. Tüketici gizliliği; demografik bilgiler, arama geçmişi ve kişisel profil bilgileri de dahil ancak bunlarla sınırlı olmayan tüketici bilgilerinin yayılmasının ve kullanımının kontrolüyle ilgili gizlilik olarak tanımlanabilir (Campbell, 1997; Martin ve Murphy, 2017). Goodwin (1991) tüketici gizliliğini, tüketicinin (a) bir satın alma işlemi veya tüketim davranışı sırasında, ortamda bulunan diğer kişilerin varlığını ve (b) bu tür işlemler veya davranışlarla ilgili veya bu işlemler veya davranışlar sırasında sağlanan bilgilerin orada olmayan kişilere yayılmasını kontrol edebilme yeteneği olarak tanımlar. Foxman ve Kilcoyne (1993) ise tüketici gizliliği kavramını (a) tüketici verilerini kimin kontrol ettiği ve (b) tüketicilerin veri toplama ve gizlilik hakları konusunda bilgilendirilip bilgilendirilmediği şeklinde genişletir. Beke vd. (2018) bu tanımlardan hareketle tüketici gizliliğini, tüketicinin kendisine ait bilgilerin firma tarafından toplanması, saklanması ve kullanılmasının farkında olması ve kontrol edebilmesi olarak tanımlamıştır. Firma ile ilgili gizlilik konuları tüketici verisinin korunması, adil bilgi uygulamaları, gizlilik politikaları gibi daha çok yasal ve etik konuları kapsamaktadır. Tüketici ile ilgili gizlilik ise gizlilik endişesi konusunu içerir. Tüketici gizlilik endişelerine yönelik literatürde birçok kavramsal ve ölçümleme çalışmaları vardır. Özellikle bilgisayar teknolojilerinin gelişimi tüketici verilerinin depolanmasına imkân sağladığından bu veriler pazarlama amaçlı analiz edilip kullanılmaya başlanmıştır. Tüketiciler çevrimdışı ve çevrimiçi pazarlama faaliyetleri sırasında firmalarla kişisel verileri paylaşırlar. Bu verilerin reklam ve pazarlama amaçlı kullanılmaya başlamasıyla tüketici gizlilik endişeleri gündeme gelmiştir.

Bireyler sosyal medya ya da internette genellikle bilgi, fırsat ya da kaynak elde edebilmek, paylaşılan kimlikler oluşturmak ya da bir grubun parçası gibi hissetmek, sosyal bağlantılar oluşturabilmek ve kullanılan web sitesi ya da sosyal medya platformunun sunduğu fırsatlardan yararlanabilmek için profil oluşturmakta ya da kişisel bilgilerini paylaşmaktadırlar (Bateman vd., 2011). Tüketiciler ise genellikle

kişiselleştirilmiş ürün tekliflerine ve önerilere, fiyat indirimlerine, ücretsiz hizmetlere ve daha alakalı pazarlama iletişimlerine ve medya içeriğine sahip olmak için kişisel verilerinin kullanımına izin vermektedir. Tüketicilerin kişisel bilgilerine yaygın erişim, dolandırıcılığa karşı savunmasızlık, yüksek düzeyde hedeflenmiş, rahatsız edici pazarlama iletişimleri ve gizlilik ihlalleri gibi olumsuz sonuçlar doğurabilmektedir (Martin ve Murphy, 2017). Gizlilik endişesi; kişisel bilgilerin başkalarına ifşa edilmesini önleme hakkının potansiyel olarak işgal edilmesinden duyulan endişe derecesi olarak tanımlanabilir (Beak ve Morimoto, 2012). Diğer bir deyişle kişilerin kendi bilgileri üzerindeki kontrol eksikliğinden doğan rahatsızlık, gizlilik endişesi olarak ifade edilebilir (Dolnicar ve Jordan, 2007).

Tüketici gizlilik çalışmalarını inceleyen Lanier ve Saini (2008) literatürde yer alan tüketici gizlilik endişelerinin üç ana kategoride ele alabileceğini ifade etmişlerdir. Bunlar, bilgilendirme, kontrol ve güvenliktir. İlk olarak, pek çok tüketici, kişisel bilgilerinin firmalar tarafından toplanması ve kullanılması konusunda bilgilendirilmek ister. İkinci olarak, tüketiciler, toplama üzerinde bir miktar kontrole sahip olduklarını hissetmek isterler. Üçüncü olarak ise, çoğu tüketici firmalardan özellikle de çevrimiçi olarak sağladıkları kişisel bilgilerinin ve bu bilgilerin saklanmasının güvenli olduğuna dair bir miktar güvence ister. Bu anlamda tüketici gizlilik endişesi bilgilendirmenin, kontrolün ve güvenliğin azaldığı durumlarda ortaya çıkan rahatsızlıkları tanımlamaktadır.

Tüketici gizlilik endişesi çalışmalarının ilk örnekleri çevrimdışı ve çevrimiçi ortamda bilgi gizliliği endişesini kavramsallaştırmak ve ölçümlemek üzerinedir. Çoğu yazar için gizlilik endişesi çok boyutlu (Tablo 2.3) bir yapıya sahip olsa da kavramı tek boyutlu ele alan çalışmalar da mevcuttur.

Tablo 2.3. *Tüketici bilgi gizliliği endişeleri boyutu*

Yazarlar ve Tarih	Bağlam	Boyutlar
Culnan, (1993)	Doğrudan pazarlama (direct marketing)	Gizliliğe yönelik genel kaygı Gizlilik kontrolü İzinsiz ikincil kullanım
Smith, vd., (1996)	Genel olarak kurumların bilgi toplama ve kullanmalarına yönelik tüketici endişeleri.	Toplama İzinsiz ikincil kullanım Uygunsuz erişim Hatalar
Sheehan ve Hoy, (2000)	E-posta	Farkındalık Kullanım Bilgi hassasiyeti (information sensitivity) Aşinalık (familiarity) Tazminat/Karşılık (compensation)

Tablo 2.4. (Devam) *Tüketici bilgi gizliliği endişeleri boyutu*

Yazarlar ve Tarih	Bağlam	Boyutlar
Malhotra vd., (2004)	İnternet	Toplama Kontrol Farkındalık
Dinev ve Hart, (2006)	E-ticaret	Kötüye kullanım
Buchanan vd., (2007)	İnternet	Tutum

Örneğin Culnan (1993) gizlilik endişesini kişisel verilerin ikincil kullanımı üzerinden açıklar. Kişisel verilerin ikincil kullanımı bu çalışmada, (1) bilgi işleme faaliyeti (edinme, kullanma veya aktarma) ve (2) tüketici ile bilgiyi kullanan firma (mevcut müşteri veya potansiyel müşteri) arasındaki ilişki olarak iki boyutlu olarak kavramsallaştırılmıştır. Mevcut müşteriler için firma, organizasyon içindeki bilgileri ikincil olarak kullanabilir veya üçüncü taraflardan bilgileri edinip kullanabilir. Gizlilik endişesi ise gizliliğe yönelik genel kaygıları, kontrol kaybını ve kişisel verilerin izinsiz kullanımını içerir. Bu üç boyutlu kavramsal yapı için ise beş ifadeden oluşan tek boyutlu bir ölçüm aracı geliştirmiştir.

Gizlilik endişesini kavramsallaştırma ve ölçümle üzerine yapılan ilk çalışmalardan bir diğeri olan bilgi gizliliği endişe ölçeği (concern for information privacy-CFIP) çalışmasında Smith vd. (1996) gizlilik endişesi literatüründe endişeyi açıklayan altı boyut ortaya çıkarmışlardır. Bunlar; toplama, izinsiz ikincil kullanım (iç), izinsiz ikincil kullanım (dış), uygunsuz erişim, hatalar, azaltılmış yargı ve veri birleştirme olarak tanımlanır. Toplama, büyük miktarlarda kişisel olarak tanımlanabilir verilerin toplanması ve veri tabanlarında saklanması endişesi olarak tanımlanır. İzinsiz ikincil kullanım iç ve dış olarak iki farklı bakış açısıyla ele alınmıştır. İzinsiz ikincil kullanım (iç), bilgilerin bireylerden bir amaç için toplandığı ancak bireylerin izni olmadan tek bir kurum içinde başka bir ikincil amaç için kullanıldığından doğan endişedir. İzinsiz ikincil kullanım (dış) ise bilginin bir amaç için toplandığı ancak harici bir tarafa (toplayan kuruluşa değil) ifşa edildikten sonra başka ikincil bir amaç için kullanıldığı düşüncesinin yarattığı gizlilik endişesini tanımlar. Uygunsuz erişim, bireyler hakkındaki verilerin, bu verileri görüntüleme ya da bu verilerle çalışma yetkisine sahip olmayan kişiler tarafından kolayca erişilebilir olduğunu düşünür. Bu düşünceden doğan gizlilik endişeleri uygunsuz erişim boyutunu açıklamaktadır. Hatalar, kişisel verilerin korunmasında kasıtlı ve kazara oluşan hatalara karşı firmalar tarafından uygulanan korumaların yetersiz olduğu düşüncesinden

kaynaklanan endişelerdir. Azaltılmış yargı, karar verme süreçlerinin otomasyonunun aşırı olabileceği ve otomatik karar süreçlerinden ayrılma mekanizmalarının yetersiz olabileceği endişesidir. Veri birleştirme ise farklı veri tabanlarındaki kişisel verilerin daha büyük veri tabanlarında birleştirilebileceği ve böylece "mozaik etkisi" yaratılabileceği düşüncesinin yarattığı gizlilik endişesini tanımlamaktadır. Ölçümleme çalışmasının sonucunda gizlilik endişesinin boyutları toplama, izinsiz ikincil kullanım (tek boyut), uygunsuz erişim ve hatalar olmak üzere dört temel boyutta toplanmıştır. Azaltılmış yargı gizlilik endişesinin bir boyutu olarak zaten çok az çalışmada ele alındığından bu çalışmada da gizlilik endişesiyle bağlantısı çok zayıf bulunmuştur. Veri birleştirme ise izinsiz erişim ve toplama boyutlarıyla birleştiği görülmüştür. Bu sonuçlardan hareketle Smith vd., (1996) tüketici bilgi gizliliği endişesini kişisel verilerin toplanması, izinsiz kullanılması, uygunsuz erişimi ve korunmasına yönelik çok boyutlu bir yapı olarak tanımlar.

Sheenan ve Hoy (2000) tüketici gizlilik endişesini farkındalık, kullanma, duyarlılık aşinalık ve tazminat olarak beş boyutta tanımlar. Farkındalık, pazarlamacıların bir şekilde kendileri hakkında onların haberi veya izni olmadan bilgi elde ettiğinin farkına vardıkça artan gizlilik endişelerini tanımlar. Tüketiciler çoğu zaman firmalarla bilgi paylaşır. Bu bir alışveriş esnasında ya da bir web sitesine kayıt olduklarında verdikleri kişisel veriler olabilir. Daha sonra, örneğin bir e-posta reklamı aldıklarında kişisel verilerin toplandığının farkına varır ve gizlilik endişesi duyarlar. Endişenin bir diğer boyutu ise kişisel verilerin kullanımıdır. Kişisel verilerin reklam ve pazarlama amaçlı kullanımı arttıkça tüketicilerin kişisel veriler üzerinde kontrol kaybından doğan gizlilik endişeleri başlamaktadır. Gizlilik endişesine neden olan bir diğer konu ise bilgi hassasiyetidir. Kişisel verilerin mülkiyeti üzerinde bir tartışma söz konusudur. Tüketiciler kişisel verilerin kendilerine ait olduğunu düşünürken reklam ve pazarlama şirketleri belli bir işlem sırasında (örn: bir web sitesine üye olma) elde ettikleri verileri kullanma hakkına sahip olduklarını dile getirirler. Bu noktada hassas olan ve olmayan bilgi ayrımı meydana gelmiştir. Hassas veriye yönelik endişe “bir bireyin belirli bir durumda bir veri türü için hissettiği gizlilik endişesi düzeyi” olarak tanımlanmaktadır. Bu verilerin (finansal bilgiler, tıbbi kayıtlar, sosyal güvenlik numaraları vb.) kullanımı gizlilik endişesini artırır. Gizlilik endişesini tanımlayan bir diğer boyut, firma aşinalığıdır. Tüketicilerin tanıdıkları ve güvendikleri firmalarla bilgi paylaşma olasılığı daha yüksektir. Bu anlamda, bu firmalardan gelen reklamlara geri dönüş yapma olasılıkları daha fazla olur. Ancak aşina

olmadıkları firmalardan gelen pazarlama iletişimi faaliyetleri tüketicilerin gizlilik endişelerini arttırır. Bu durum üçüncü taraf veri toplamayla da ifade edilir. Birinci taraf tarafından hedeflenen reklamlar gizlilik endişesine çok fazla etki etmezken, üçüncü taraf hedeflemeler tüketicide verilerin izinsiz paylaşıldığı düşüncesine neden olmaktadır. Son boyut ise tazminat olarak ifade edilir. Bu durum kişisel verilerin belirli faydalar için paylaşılabileceği durumları ifade eder. Eğer bir firma web sitesine üye olunduğu takdirde indirim yapacağını açıklarsa, tüketici bilgi paylaşmaya daha istekli olur. Bunun sonucunda gelen bir iletişim çalışması ise önceden isteyerek bilgi paylaşan tüketicide daha az gizlilik endişesine neden olabilir.

Bir diğer gizlilik endişesi çalışması ise Malhotra vd. (2004) tarafından geliştirilen internet kullanıcılarının bilgi gizlilik endişesi (IUIPC) ölçek çalışmasıdır. İnternet bağlamında ele alınan bu çalışma ilk önemli çalışmalardan biri olarak görülmektedir. Bilgi gizliliği endişesi genellikle kurumların adil olup olmadığına dayandırılarak, bireyin bilgi gizliliği bağlamında adalete-adil olmaya (fairness) ilişkin öznel görüşlerini ifade eder. Ancak bu dış etkenlerin yanı sıra bu öznel görüşler kişinin karakter özelliklerine ve geçmiş deneyimlerine göre değişiklik gösterebilir. Bu nedenle insanlar, bir firmanın kişisel bilgilerinin toplanması ve kullanılmasıyla ilgili olarak neyin adil olduğu ve neyin adil olmadığı konusunda sıklıkla farklı görüşlere sahip olabilirler. Çevrimiçi ortamda tüketici gizlilik endişesini kavramsallaştırıp ölçümlemek için yapılan çalışmada gizlilik endişesi toplama, kontrol ve farkındalık olarak üç boyutlu bir yapıyı ifade eder. Toplama; bir kişinin, elde edilen faydaların değerine göre başkalarının sahip olduğu bireye özgü verilerin miktarıyla ilgilenme derecesi olarak tanımlanır. Yani kişi kendine ait verilerin başkaları tarafından ne kadar toplandığıyla ilgili bir endişe duyabilir, bunu ise elde edilen faydaların değerine göre belirler. Bir diğer boyut olan kontrol ise kişisel veriler üzerinde kontrol kaybının artması ile oluşan gizlilik endişesini ifade eder. Son boyut ise farkındalık olarak belirlenmiştir. Farkındalık, kişisel verilerin toplanması ve kullanılmasına yönelik kişinin farkındalığını ve bunu arttıracak kurumsal bilgilendirmeyi ifade eder. Kişinin kurumların şeffaf bir bilgilendirme yapıp yapmadığı ve kişisel verilerin kullanılması üzerinde bilgi sahibi olmasının önemini değerlendirmesi ile ilgilidir. Bu anlamda bireyin kişisel verilerinin nasıl toplandığı ya da kullanıldığına dair bilgisi ne kadar az olursa gizlilik endişesi o kadar artacaktır.

Bir diğer gizlilik endişesi tanımı ise kişilerin bilgisi olmadan kişisel verilerinin bir veri ağının parçası haline gelmesinden doğan endişelerdir. Kişisel verilerin bu şekilde

yayılması tüketicide verilerinin kötüye kullanılması ihtimalinden doğan endişelere neden olmaktadır. Gizlilik endişesi, interneti kullanırken ifşa edilen bilgilere kimin erişebileceğine ve bu bilgilerin nasıl kullanıldığına ilişkin inançlardır. Bu durum hakkindeki belirsizlik arttıkça gizlilik endişeleri de o derece artar (Dinev ve Hart, 2006).

Buchanan vd. (2007) internet gizlilik endişesi ve gizliliği korumaya yönelik davranışları araştırmıştır. Bu anlamda gizlilik, endişeye yönelik tutum ve koruma davranışı olarak iki boyutta incelenir. Gizlilik endişesi genel tutum olarak tek boyutta ele alınmasına rağmen yine kişisel verilerin toplanması, kullanılması ya da paylaşılmasından doğan belirli riskleri ele almaktadır. Bunların arasında kredi kartı kullanımı, virüs, e-postaların kullanımı, kimlik hırsızlığı gibi internet kullanımı sırasında doğabilecek risklerin endişesi yer alır.

Özetle yapılan çalışmalara bakıldığında tüketici açısından gizlilik endişesinin kişisel verilerin toplanması, kullanılması ve paylaşılması üzerinde duyulan endişeleri ifade ettiği söylenebilir. Tüketicinin gizliliğe yönelik endişelerinin, kişisel verilerin kullanımı üzerinde yeterince bilgi sahibi olamadıklarında, bu bilgilerin işlenmesi ve paylaşılması üzerinde (izinsiz kullanımlar, uygunsuz erişimler vb.) kontrol sahibi olamadıklarını ve kişisel verilerin firma tarafından güvenli bir şekilde saklanamayacağını düşündüklerinde ortaya çıktığı ya da arttığı söylenebilir. Tüketici gizliliği ile ilgili ilk çalışmalarda gizlilik endişesinin tanımlanmasının yanı sıra doğrudan pazarlama, telefonla pazarlama, e-posta, e-ticaret, internet gibi farklı bağlamlarda ve farklı teorik alt yapılarla (Tablo 2.4) gizlilik endişesinin nedenleri araştırılmıştır.

Tablo 2.5. *Tüketici gizlilik endişesi nedenleri*

Yazar ve Yıl	Bağlam	Teori	Öncüller
Culnan ve Armstrong (1999)	Bilgi gizliliği endişesi	Adalet teorii (Justice Theory) ve Gizlilik muhasebesi teorisi (Privacy calculus theory)	Risk Fayda Prosedüral adalet Güven
Sheehan ve Hoy (2000)	Doğrudan postalama (Direct mail)	FTC prensipleri	Bilgi toplama farkındalığı Bilginin kullanımı Bilginin hassasiyeti Firmaya aşinalık Ödül
Phelps vd. (2000)	Doğrudan pazarlama (Direct marketing)	Sosyal sözleşme teorisi (Social contract theory)	Bilgi türü Bilgi miktarı Risk/Fayda Kişisel Özellikler

Tablo 2.6. (Devam) *Tüketici gizlilik endişesi nedenleri*

Yazar ve Yıl	Bağlam	Teori	Öncüller
Phelps vd. (2001)	Doğrudan postalama (Direct mail)	Nedenli eylem teorsi (Theory of reasoned action)	Doğrudan postalamaya yönelik tutum Kontrol arzusu (desired control)
Dinev ve Hart (2004)	İnternet	Gizlilik muhasebesi teorisi (Privacy calculus theory)	Algılanan savunmasızlık Algılanan kontrol
Chellappa ve Shin (2005)	Çevrimiçi gizlilik	Sosyal Değişim Teorisi (Social Exchange Theory)	Algılanan kişiselleştirme
Lwin vd. (2007)	Tüketici online gizlilik endişesi	Güç-sorumluluk denge modeli (Power-Responsibility Equilibrium)	Gizlilik politikası Yasal/Öz düzenleme politikaları
Smith vd. (2011)	Bilgi gizliliği endişeleri	Gizlilik literatürü	Kişilik özelliği Demografik özellikler Kültürel özellikler Gizlilik deneyimi Gizlilik farkındalığı
Xu vd. (2011)	Tüketici gizlilik endişesi	İletişim gizliliği yönetim modeli (Communication privacy management theory)	Algılanan risk Güven Gizlilik değeri (value of privacy)
Mohamed ve Ahmad (2012)	Sosyal medya	Koruma motivasyonu teorisi (Protection motivation theory)	Algılanan ciddiyet Algılanan savunmasızlık Algılanan Fayda Öz yeterlilik Tepki yeterliliği
Xu vd. (2013)	Sosyal medya	Planlı davranış modeli (Theory of planned behavior)	Bilgi hassasiyeti Gizlilik riski Bilgi kontrolü Öznel norm
Chen vd. (2017)	İnternet	Öz-kontrol teori (Self-control theory) Rutin aktiviteler teorisi (Routine activity theory)	İnternet dolandırıcılığı mağduriyeti
Mpinganjira ve Maduku (2019)	Mobil	Etik teori (Ethical theory)	Algılanan kontrol Gizlilik beklentisi (desire for privacy)

Yukarıdaki çalışmalara bakıldığında gizlilik endişesine yönelik araştırmaların farklı teoriler ve farklı bağlamlarla ele alındığı görülmektedir. Çalışmaların bazıları (Culnan ve Armstrong, 1999; Phelps vd., 2000; Lwin vd., 2007; Mpinganjira ve Maduku, 2019) tüketici gizlilik endişesine kurum perspektifinden yaklaşmıştır. Kurumların adil, açık ve etik davranışlar sergileyip sergilemedikleri tüketicide gizlilik endişesine neden olan bir etmendir. Bu çalışmalar kurumsal sorumlulukların tüketicideki algısına odaklanmıştır. Çoğu çalışma (Culnan ve Armstrong, 1999; Dinev ve Hart, 2004;

Chellappa ve Shin, 2005) ise tüketici gizlilik endişesine risk-fayda teorileri üzerinden yaklaşmıştır. Burada önemli olan tüketicinin algısıdır. Tüketici riski faydadan daha fazla hissederse gizlilik endişesinin oluşacağı ön görülmektedir. Bunun dışında nedenli eylem, planlı davranış, iltişim gizliliği yönetimi gibi teorik altyapıları ele alan çalışmalar (Phelps vd., 2001; Xu vd., 2011; Xu vd., 2013) gizlilik endişesinin tüketici tutum ve algılarına bağlı olduğunu ele alarak tüketicinin davranışsal niyetlerini anlamaya çalışmışlardır. Tüketici gizliliği nedenlerine daha genel yaklaşan (Sheehan ve Hoy, 2000; Smith vd., 2011) çalışmalarda ise farkındalık, kişisel verilerin kullanımı, önceki deneyimler, bilginin türü gibi kişisel verilere yönelik farklı değişkenlerin yanı sıra kişisel ve kültürel özelliklerin de etkisi göz önüne alınmıştır. Tüm bu çalışmalardan haraketle tüketici gizlilik endişelerinin başta kişisel verilerin kullanımı ve paylaşılmasının farkında olması ve bu duruma yönelik risk, fayda vb. algılarının etkili olduğu söylenebilir. Ayrıca kurumlara duyulan güven, kontrolün kendinde olup olmadığına yönelik algılar, önceki olumsuz deneyimler gibi nedenler tüketicinin gizlilik endişesi duyup duymamasında etkili olan nedenlerin başında gelmektedir.

Çerez teknolojilerinin gelişmesiyle özellikle dijital reklamcılıkta davranışsal verilerin toplanmaya başlaması kişiyi tanımlayan verilerin dışında davranışsal verilerin izlenmesine dayanan gizlilik endişeleri konularının hızla gündeme gelmesine neden olmuştur. (Caudill ve Murphy, 2000, s. 9). ÇDR'ye yönelik gizlilik endişesi ve reklamdan kaçınma çalışmalarına tezin dördüncü bölümü olan kavramsal çerçeve içerisinde yer verilecektir. Bir sonraki başlıkta ise reklamdan kaçınma kavramına yönelik genel literatür ele alınmıştır.

2.3. Kaçınma Motivasyonu

Psikolojinin ilgilendiği en temel sorulardan biri de insan davranışlarının altında yatan motivasyonların ne olduğudur. İnsan bilinçli bir çıkarımla mı, geçmiş deneyimleriyle mi, otomatik dürtüsel tepkilerle mi ya da duygularıyla mı hareket etmektedir sorusu psikolojinin birçok alanında ele alınmıştır. Bu motivasyonlar sonucunda insanlar pek çok davranış gerçekleştirmektedir. Bu davranışlardan biri ise kaçınma davranışıdır. Elliot (2008), kaçınma davranışının altında yatan temel itici gücü anlamak için en başta yaklaşma-kaçınma motivasyonu arasındaki farkın anlaşılması gerektiğini ifade eder.

Yaklaşma-kaçınma ayrımının temelleri Antik Yunan Filozofları Demokritus ve Aristupus' un etik hazcılık düşüncelerinde görülür. Bu düşünceye göre insan davranışının temelleri hazza yaklaşma ve acıdan kaçınmaya odaklıdır (Elliot ve Covington, 2001, s. 74). Daha sonraları bilimsel psikoloji alanında da James ve Freud gibi bazı düşünürlerin acı ve hazzı, davranışa neden olan yegâne pekiştireç ve önleyici olarak ele aldığı görülür. Bu yazarlar yaklaşma ve kaçınmayı genel haz kavramının dışında yaklaşma ve kaçınma davranışlarının ürettiği ve düzenlediği belirli yollara odaklanarak ele almışlardır (Elliot, 2006, s. 111). Elliot'a (1999, s. 170) göre yaklaşma motivasyonunda davranış, olumlu veya arzu edilen bir olay veya olasılık tarafından teşvik edilir veya yönlendirilirken, kaçınma motivasyonundaki davranış ise olumsuz veya istenmeyen bir olay veya olasılık tarafından teşvik edilir veya yönlendirilir.

İnsan davranışını açıklamada yaklaşma ve kaçınma çalışmaları tüketici davranışını açıklamada da önemli görülmektedir. Bilişsel psikolojideki çalışmalar kaçınmanın bir uyarana verilen bilinç dışı bir refleks mi yoksa bir yorumlama sürecinden sonra verilen bir tepki mi sorusuna odaklanmıştır. Olumlu ve olumsuz olarak uyaranlara temel yaklaşma ve kaçınma hareketlerinin doğrudan (yani anlık, kasıtsız, örtük, otomatik ve uyarıcı temelli) veya dolaylı olarak (yani durumun bilinçli veya bilinçsiz yorumlanmasından sonra) olup olmadığına yönelik önemli tartışmalar vardır. (Phaf vd., 2014). Bir organizma bir uyaran tarafından yaklaşma ve kaçınma için motive edilebilir ancak bu her zaman davranışa dönüşmeyebilir. Örneğin örümcekten korkan bir insanın örümcek gördüğünde korku duygusu sebebiyle kaçması beklenirken, birey korkunun üstüne gitmek için kaçma davranışını göstermeyebilir (Elliot ve Covington, 2001, s. 84). Bu durumda duyguyla başa çıkmak (coping behavior) için bilinçli bir karar verilmiştir.

1970 ve 1980'lere kadar yaklaşma ve kaçınma arasındaki ayrım bilişsel psikoloji teorileriyle ele alınmaya çalışılmış ve motivasyon ile biliş arasında keskin bir ayrım çizilmiştir. Bu ayrımla davranışı açıklamada, duygu temelli olmayan açıklamalar üzerinde durulur (Elliot, 2006) ya da duyguların biliş tarafından yürütüldüğü ve bilişin önce geldiği savunulur (Lazarus, 1984'ten aktaran Yılmaz, 1999, s. 78). Bazı araştırmacılar ise çağdaş psikolojik kuramlar içinde duygunun biliş ötesi şeklinde ya da sadece bilişsel işlemlerden sonra oluştuğu görüşünü eleştirir. Aslında onlara göre duygusal değerlendirme tamamen bilişten bağımsızdır ve hatta bilişten önce gelir (Zajonc, 1980'den aktaran Yılmaz, 1999, s. 78). 1990'larda ise biliş ve motivasyonun

ayrılamayacağı ve duyguların da davranışları açıklamada gerekli olduğu düşüncesi yaygınlaşmıştır (Elliot, 2006, s. 112).

Sonuç olarak, duygu ve motivasyon önemli ölçüde bağlantılıdır ve bu ilişki, reklamcılığın nasıl işlediğini incelemek için reklam literatüründe de ele alınır (Percy, 2012). Ayrıca duygu, biliş ve davranış reklam uyaranının etkisini ortaya koyan çalışmalarda reklamdan kaçınmayı açıklamak için de kullanılmıştır. Duygu ve bilişin önceliği tartışmalarının yanı sıra ikisinin de davranışla beraber reklamdan kaçınmanın boyutlarını oluşturduğu bilinmektedir. Reklamcılıkla ilgili olarak, insanların eğlence veya bilgi gibi bir miktar ödül veya zevk sağlayan reklamlara yaklaşmayı; sıkıcı, güvenilmez veya yıkıcı olarak algılanan reklamlardan kaçınmayı seçecekleri düşünülür (Kelly vd., 2020, s. 489). Bir sonraki bölümde kaçınma motivasyonu bilişsel, duygusal ve davranışsal boyutlardan hareketle ve reklamcılık özelinde ele alınarak açıklanmıştır.

2.3.1. Reklamdan kaçınma kavramı

Reklamdan kaçınma, medya kullanıcılarının, reklam içeriğine maruz kalma oranlarını farklı şekilde azaltan eylemler (Speck ve Elliott, 1997a: 61) ve tüketicilerin bilinçli olarak reklamdan kaçındıkları durumlar (Tellis, 2004, s. 31) şeklinde tanımlanır. Biliş, duygu ve davranış ise tüketicinin reklam uyaranlarına yönelik tepkilerinin üç unsurunu oluşturmaktadır (Cho ve Cheon, 2004, s. 91). Bu nedenle reklamdan kaçınma, "medya kullanıcılarının, reklam içeriğine maruz kalma oranlarını farklı şekilde azaltmaya çalıştıkları eylemler ve tüketicilerin bilişsel, duygusal ve davranışsal olarak reklamdan kaçındıkları durumlar" şeklinde tanımlanmıştır.

2.3.1.1. *Davranışsal kaçınma boyutu*

Reklamdan kaçınmaya yönelik ilk çalışmalar geleneksel mecrayı, özellikle de televizyon reklamlarından kaçınmayı ele alan çalışmalarla ortaya konmuştur (Speck ve Elliott, 1997a, s. 61). Bu anlamda reklamdan kaçınma çalışmaları reklamı atlama (zapping) ya da ileri sarma (zipping) davranışı olarak reklama maruz kalmayı engellemeyi ifade eden mekanik kaçınma olarak kavramsallaştırılmıştır. Bu kaçınmada uzaktan kumanda ya da video kayıt cihazları gibi teknolojilerin kullanımı ile reklamı geçme, kaçınmanın mekanik boyutunu ifade eder (Kaplan, 1985; Heeter ve Greenberg, 1985; Yorke ve Kitchen, 1985; Lee ve Lumpkin, 1992; Moriarty ve Everett, 1994) ve bu durum belirli kontrollerin tüketicide reklamdan kaçınmaya etki ettiğini gösterir.

Televizyon izleyicilerinin kanal değiştirme davranışını inceleyen çalışmalar, kanal değiştirmenin reklamları geçmek ya da başka bir programa geçmek için yapıldığını göstermiştir (Ferguson ve Perse, 1993, s. 43). Bazı çalışmalar program alternatifi için yapılan kanal değiştirmenin (Zufryden vd., 1993, s. 61) reklamı atlama motivasyonundan daha fazla olduğunu; bazı çalışmalar ise (Kaplan, 1985, s. 10-11) reklam arasında kanal değiştirmenin daha fazla olduğunu gösterse de sonuç olarak bu çalışmalar, reklamdan kaçma davranışının mekanik olarak gerçekleştiğini ortaya koymaktadır.

Abernethy ise (1991a; 1991b) reklamdan kaçınmayı fiziksel ve mekanik eylemler olarak iki şekilde ifade eder. Televizyon ve radyo reklamları için yapılan çalışmalarında kişinin odayı terk etmesi fiziksel, kanalın değiştirilmesi ise mekanik kaçınmayı gösterir. Speck ve Elliott da (1997a) kanalı değiştirme davranışını mekanik kaçınma olarak ifade ederken, kişinin reklam süresince odayı terk etmesini davranışsal kaçınma olarak tanımlamıştır.

İnternet reklamcılığında ise mekanik olarak ele alınan kaçınma, davranışsal boyut olarak ifade edilmiştir. Bu anlamda reklamdan kaçınmanın davranışsal boyutu, kaçınma için tüketicinin gösterdiği eylemleri ifade eder (Cho ve Cheon, 2004). Bu eylemler basitçe reklamı atlama, reklamı kapatma, reklamın bulunduğu ortamı (web sitesi) terk etme, reklamı engelleme gibi davranışlar olabilir.

2.3.1.2. *Bilişsel kaçınma boyutu*

Bilişsel kaçınma, istenmeyen durum veya problemlerden kaçmayı amaçlayan bireyin dikkati dağıtma ya da dikkat etmeme, endişe ve düşünce bastırma gibi çeşitli stratejileri kullanmasını temsil eden bir terimdir (Sagui-Henson, 2017, s. 2). Düşünce bastırmaya yönelik kasıtlı girişimler olarak ifade edilen bilişsel kaçınma (Williams ve Moulds, 2007, s. 1142) reklamdan kaçınmanın en yaygın biçimini oluşturur (Bellman vd., 2010). Tüketicilerin bilinçli olarak düşünce bastırma yoluyla davranıştan kaçınmasının, reklamdan kaçınma davranışını da etkileyebileceği düşünülür (Baumeister vd., 2011).

Bilişsel olarak reklamdan kaçınma en temelde reklamı görmezden gelmeyi ifade eder (Speck ve Elliott, 1997a, s. 62). Televizyon izleyicileri için yapılan çalışmalar izleyicilerin televizyon açıkken yemek yeme, kitap okuma, ev işleriyle uğraşma gibi başka aktiviteler yaptığını göstermiştir (Clancey, 1994). Bu durum TV programlarını izlerken bile izleyicinin içeriğe dikkat etmediğini gösterir ki reklam aralarında bu durumun daha fazla olması muhtemeldir. Bu görmezden gelme internet reklamları için

de geçerlidir. Örneğin internet reklam türlerinden biri olan banner reklamlar için banner körlüğü şeklinde ifade edilen bir kavram söz konusudur. Banner körlüğü, tüketicilerin çevrimiçi reklam afişlerine bakmaktan kaçınabilecekleri bulgusuna karşılık gelir (Hervet vd., 2011). Banner körlüğüyle ilgili göz izleme araştırması, çevrimiçi reklamcılığın öngörülebilir doğası nedeniyle tüketicilerin beklenen alanlarda reklam görmeyi öğrendiklerini ve bu nedenle bilişsel olarak o alanları görmezden geldiğini kanıtlamıştır (Barreto, 2013).

Mecra ya da reklam formatının yanı sıra bilişsel kaçınma bir tüketicinin bir nesne hakkındaki inancından da etkilenir. Reklamla ilişkili olumsuz inançlar ne kadar fazla olursa, genel bilişsel bileşenin o kadar olumsuz olduğu varsayılır ve bu da tüketicinin reklamı görmezden gelmesi, reklamı bilerek tıklamaması, reklama dikkat etmemesi gibi bilişsel kaçınma tepkilerine yol açar (Cho ve Cheon, 2004, s. 91).

2.3.1.3. *Duygusal kaçınma boyutu*

Duygular, bireylerin fırsatlara ve sorunlara tepki vermesini yani bir duruma yaklaşmasını veya bir durumdan kaçınmasını sağlayan bir dizi tepkiyi (örn: fizyoloji, davranış, deneyim ve iletişim) tetikler. Tepkisellik, algılanan davranışsal özgürlüklere yönelik tehditlere yanıt olarak ortaya çıkar (Kelly vd., 2021). Bir tüketicinin bir nesneye (örneğin bir internet reklamına) karşı hissi veya duygusal tepkisi de reklamdan kaçınmanın duygusal bileşenini temsil eder (Cho ve Cheon, 2004).

Reklama yönelik duygusal kaçınma, tüketicilerin reklamdan kaçınmalarını teşvik eden olumsuz duyguları olduğunda ortaya çıkar (Alwitt ve Prabhaker, 1994; Cho ve Cheon, 2004). Bu olumsuz duygular reklamdan hoşlanmama, nefret etme, rahatsız olma, reklamın olmamasını tercih etme olarak ifade edilebilir. Reklamdan hoşlanmayan tüketicinin reklama yönelik olumsuz tutum ve bunun sonucunda da reklamdan kaçınma sergileyeceği düşünülür.

Reklamdan hoşlanmama nedenleri; reklamın hedefi engellemesi (Speck ve Elliott, 1997a), algılanan reklam fazlalığı (Ha ve McCann, 2008; Cho ve Cheon, 2004), reklam mesajına ya da mecraya duyulan güvensizlik (Kelly vd., 2010), reklamın yarattığı gizlilik endişesi (Beak ve Morimoto, 2012) gibi nedenler olabilir.

Bir içeriği izleme, okuma ya da dinleme davranışı sırasında araya giren, içeriyi engelleyen, ya da bu işlemler sırasında kişinin zarar görmesine (şüphe ve güven eksikliği)

neden olacağı düşünülen reklam, bireyin özgürlüğünü kısıtlayan, rahatsız edici ya da aldatıcı bir uyaran olarak algılanabilir ve duygusal kaçınmaya neden olabilir.

2.3.2. Reklamdan kaçınma nedenleri

Tellis (2004, s. 31) reklamdan kaçınmanın nedenlerini, reklamın verdiği bilgiyi almak istememek, reklamın dikkat dağıtıcı ya da rahatsız edici olması gibi nedenlerle açıklar. Çalışmalar genellikle mecraya yöneliktir ve geleneksel mecra ile internet temel iki ayrım noktasını oluşturur. Reklamdan kaçınma literatüründe iki temel makale göze çarpmaktadır. Bunlar geleneksel mecra içi Speck ve Elliot (1997a), internet reklamları için ise Cho ve Choen (2004) çalışmalarıdır. Speck ve Elliott (1997a, s. 62-63), televizyon ve basılı mecradaki reklamlardan kaçınma nedenlerini; demografik değişkenler, mecra ile ilgili değişkenler (kullanım genişliği, kullanım miktarı, tutum), reklama yönelik tutum ve iletişim problemleri olarak belirlemiştir. Cho ve Cheon (2004) ise internet reklamlarından kaçınma davranışlarını ele alır. İnternet reklamlarından kaçınma nedenlerini; algılanan hedef engeli, reklam kirliliği ve olumsuz deneyim olarak belirler. Bunların dışında Rojas-Méndez ve Davies (2005) zaman odaklılığın reklamdan kaçınmaya etkisini araştırır. Kişinin geçmiş, şimdiki ve gelecek zaman odaklı olmasının, o kişinin belli bir nesne hakkındaki inanışlarını etkilediğini, bu inanışların da reklama yönelik genel bir tutum oluşturduğunu ve bu üç değişkenin ise reklamdan kaçınmayı etkilediğini savunmaktadır. Prendergast vd., (2010) ise psikolojik bir faktör olan başkalarının varlığının, reklamdan kaçınmaya etki ettiğini ileri sürmüştür. Reklamdan kaçınmanın aktif ve pasif öncüllerinin olabileceğini varsayar. Yazarlara göre reklama yönelik tutum gibi önceden ele alınan değişkenler kişinin aktif olarak kontrol ettiği değişkenlerdir. Ancak kişi kendi kontrolü dışında olan iki faktör, başkalarının varlığı ve algılanan zaman baskısıdır. Başkalarının varlığı ve zaman baskısı pasif faktörler olarak tanımlanabilir, çünkü bu psikolojik değişkenler bir dereceye kadar reklam izleyicinin kontrolü dışındadır. Bu tür pasif faktörler etkili ise tüketiciler reklamdan ille de istedikleri için değil, çevreleri onları buna zorladığı için kaçınabilir. Li vd. (2002) ise bilgilendirici olmayan, sıkıcı ve müdahaleci (intrusiveness) reklamların rahatsız ediciliğe (iritasyon) ve kaçınmaya neden olduğunu belirtir. Çalışmalara bakıldığında reklamdan kaçınmada mecranın özelliği dikkate alınmıştır. Çalışmaların çoğu geleneksel mecrayı ve televizyonu ele alırken bazı çalışmalar (Cho ve Cheon, 2004) internet mecrasını ele almıştır. İnternet, geleneksel mecraya göre daha fazla amaç ve bilgi odaklı bir mecra olarak nitelendirilir. Bu nedenle

de reklamların amacı engellediği ve reklam kirliliği etkisinin bu mecrada daha fazla olduğu ileri sürülür.

Reklamdan kaçınmanın sebepleri farklı çalışmalarda farklı öncüllerle ele alınır. Bu farklılıklar reklamın yayınlandığı ortama (örn: geleneksel mecralar, internet, mobil, sosyal medya), reklam formatına (örn: video reklam, basılı reklam, banner, pop-up, doğal reklam, hedefli reklam) ya da çalışmalarda kullanılan teorik arka plana göre değişiklik gösterebilir. Bu değişiklerin örnekleri detaylı şekilde Tablo 2.5'te gösterilmektedir.

Tablo 2.7. *Farklı mecralara yönelik çalışmalarda reklamdan kaçınmanın öncülleri ve boyutları*

Reklam Alanı/Medya	**Yazar ve Yıl**	**Öncüller**	**Boyutlar**
Televizyon	Abernethy (1991a)	Reklam ve program izleme süreleri (tv programlarına maruz kalma ile reklama maruz kalma arasındaki fark)	Fiziksel Mekanik
	Stafford ve Stafford (1996)	TV izleme motivasyonu	Mekanik
	Phau ve Dix (2003)	Planlı-plansız TV izleme	Mekanik
	Rojas-Méndez ve Davies (2005)	Zaman odaklılık Reklama yönelik inanç Reklama yönelik genel tutum	Mekanik Davranışsal
	Rojas-Méndez, Davies ve Madran (2009)	Reklama yönelik genel tutum	Mekanik Davranışsal
	Dix ve Phau (2010)	Zapping/zipping (kanal değiştirme/reklamları ileri sarma)	Mekanik
	Rojas-Méndez ve Davies (2017)	Zaman baskısı	Davranışsal Mekanik
Radyo	Abernethy, 1991b	Kanal değiştirme (Switching)	Mekanik
	Michelon vd. (2020)	Günün saati Lokasyon (evde-dışarda) Format (müzik- sohbet)	Mekanik
Çoklu Medya	Speck ve Elliot (1997a)	Demografik değişkenler Medyayla ilişkili değişkenler Reklama yönelik algı İletişim problemleri	Bilişsel Davranışsal Mekanik
	Elliott ve Speck (1998)	Reklam kirliliği	Davranış
	Prendergast vd. (2010)	Başkalarının varlığı Zaman baskısı	Bilişsel Davranışsal
	Beak ve Morimoto (2012)	Gizlilik endişesi Algılanan kişiselleştirme Rahatsız edicilik Şüphe	Bilişsel Duygusal Davranışsal
	Kim ve Seo (2017)	Reklama yönelik biliş ve algılar Reklama yönelik tutum	Bilişsel Duygusal Davranışsal
	Van der Goot vd. (2018)	Medya kullanım sıklığı Tutum	Bilişsel Duygusal Davranışsal

Tablo 2.8. (Devam) *Farklı mecralara yönelik çalışmalarda reklamdan kaçınmanın öncülleri ve boyutları*

Reklam Alanı/Medya	Yazar ve Yıl	Öncüller	Boyutlar
İnternet	Edwards, Li ve Lee (2002)	Reklam değeri Bilişsel yoğunluk Kesintinin süresi Reklam-içerik uyumu Reklam müdahaleciliği Rahatsız edicilik	Davranış
	Li, Edwards ve Lee (2002)	Reklam müdahaleciliği Rahatsız edicilik	Bilişsel Davranışsal
	Cho ve Cheon (2004)	Hedef engeli Reklam kirliliği Önceki olumsuz deneyimler	Bilişsel Duygusal Davranışsal
	Jin and Villegas (2006)	Biliş İhtiyacı Risk alma eğilimi	Davranış
	Rachbini ve Hatta (2018)	E-yaşam tarzı	Bilişsel Duygusal Davranışsal
	Seyedghorban, Tahernejad ve Matanda (2016)	Hedef engeli Reklam kirliliği Önceki olumsuz deneyimler	Bilişsel Duygusal Davranışsal
	Söllner ve Dost (2019)	Karşılıklılık normu	Davranışsal
Mobil	Okazaki vd. (2012)	Gizlilik endişesi Her yerde bulunma (perceived ubiquity) Algılanan risk Algılanan güven	Davranışsal
	Nyheim vd. (2015) (lokasyon)	Endişe Algılanan kişiselleştirme Rahatsız edicilik Algılanan kontrol	Bilişsel Duygusal Davranışsal
	Shin ve Lin (2016) (lokasyon)	Hedef engeli Fedakârlık/sacrifice Algılana fayda Algılanan eğlence Mobil araçla geçirilen zaman	Bilişsel Davranışsal
	Brinson ve Britt (2021)	Reklam uygunluğu Reklam şüpheciliği Rahatsız edicilik Reklama yönelik tutum	Duygusal Bilişsel Davranışsal
E-posta	Morimoto ve Macias (2009)	Algılanan müdahalecilik Psikolojik tepki Tutum	Davranışsal
	Morimoto ve Chang (2009)	Algılanan müdahalecilik Rahatsız edicilik Reklama yönelik tutum Reklama yönelik şüphe	Davranışsal
Video reklam	Kim vd. (2013)	Reklam değeri Reklam müdahaleciliği Reklama yönelik tutum	Bilişsel Duygusal Davranışsal
	Hussain ve Lasange (2014)	İlgisiz reklam içeriği Algılanan özgünlük Etkileşimlilik	Davranışsal
	Li ve Yin (2021)	Algılanan kontrol Algılanan müdahalecilik	Davranış

Tablo 2.9. (Devam) *Farklı mecralara yönelik çalışmalarda reklamdan kaçınmanın öncülleri ve boyutları*

Reklam Alanı/Medya	Yazar ve Yıl	Öncüller	Boyutlar
Sosyal medya	Guardia (2015)	Reklam kirliliği Rahatsız edicilik Reklam müdahaleciliği	Bilişsel
	Jung (2017)	Reklam uygunluğu Gizlilik endişesi	Bilişsel Duygusal Davranışsal
	Tran (2017)	Algılanan kişiselleştirme Şüphe Güven	Bilişsel Duygusal Davranışsal
	Wei vd. (2019) (mobil sosyal medya)	Reklam müdahaleciliği Endişe Rahatsız edicilik	Bilişsel Davranışsal Mekanik
	Youn ve Kim (2019b)	Algılanan müdahalecilik Algılanan tehdit Negatif biliş Öfke	Bilişsel Davranışsal
	Chinchanachokchai ve Gregorio (2020)	Akran etkisi Sosyal medya etkisi Sosyal medya kullanımına yönelik tutum	Bilişsel Duygusal Davranışsal
	Chung ve Kim (2021)	Reklam müdahaleciliği Reklam değeri Akran etkisi Marka takip sayısı Şüphe	Bilişsel Duygusal Davranışsal
	Niu vd. (2021)	Psikolojik sahiplik Sosyal etki Reklam istilası (invasiveness) Rahatsız edicilik	Bilişsel Duygusal Davranışsal
	Kelly vd. (2021)	Gizlilik kontrolü Gizlilik endişesi Mecraya negatif tutum Reklam kirliliği Negatif WOM	Bilişsel Duygusal Davranışsal

Tablo 2.5'te gösterildiği gibi reklamdan kaçınma farklı mecralarda farklı öncüller içermektedir. Fakat her ne kadar farklı öncüller söz konusu olsa da geleneksel mecra ve internet reklamlarından kaçınmanın temel nedenleri veya öncüllerini reklamın kendisinden kaynaklanan faktörler ve tüketici algılarından kaynaklanan faktörler olarak iki temel kategoride ele almak mümkündür. Reklamın kendisinden kaynaklanan faktörler içerisinde reklam kirliliği ve hedef engeli yer alırken, tüketici algılarından kaynaklanan faktörler arasında olumsuz deneyimler ve reklama yönelik tutum yer alır (Speck ve Elliot, 1997a; Li vd., 2002; Cho ve Cheon, 2004) Başka bir ifade ile her mecrada söz konusu olan ve reklamdan kaçınmaya etki eden dört neden söz konusudur. Çalışmanın devamında bunlara yönelik bilgiler sunulmuştur.

2.3.2.1. *Reklam kirliliği*

Reklamdan kaçınmaya etki eden önemli faktörlerden biri reklamın yarattığı reklam kirliliğidir. Reklam kirliliğine yönelik ilk çalışmalar geleneksel mecra üzerindedir ve bir mecra üzerindeki reklam sayısının fazlalığı/aşırılığı olarak ele alınır (Elliott ve Speck, 1998; Ha 1996; James ve Kover 1992). Ancak reklam fazlalığı tüketicinin reklam miktarına yönelik objektif değerlendirmesinden ziyade algılarını ifade eder (Speck ve Elliot 1997b, s. 40). İlk çalışmalar daha çok reklam kirliliğini reklam miktarı olarak tek bir boyutta ve hatırlamaya etkisi üzerinden ele almıştır ve reklam miktarındaki artışın reklamın hatırlanması üzerinde olumsuz bir etki yarattığını ortaya koymuştur (Webb ve Ray, 1979; Mord ve Gilson 1985; Ray ve Webb, 1986).

Reklam kirliliğini, reklamın miktarından farklı boyutlarda ve hatırlamadan farklı sonuçlarla ele alan çalışmalar da vardır (Ha, 1996; Ha ve Litman, 1997; Kent ve Allen 1994; Cho ve Cheon, 2004; Riebe ve Dawes, 2006, Speck ve Elliott, 1997b; Elliott ve Speck, 1998).

Örneğin, Ha (1996, s. 77) dergi reklamlarının yarattığı reklam kirliliğini ele aldığı çalışmasında reklamın hatırlama üzerindeki bilişsel etkisinin yanı sıra tutumlara olan duygusal bir etkisinin de olduğunu belirtir. Reklam kirliliğini ise reklam miktarının (quantity-overload) yanı sıra reklam rekabeti (competitiveness-interference) ve reklamın müdahaleciliği (intrusiveness-reactance) olarak üç boyutta ele alır. Reklam rekabeti, reklamı yapılan ürünlerin benzerlik derecesi ve bir medya aracında aynı ürün kategorisindeki rakip markaların reklamları arasındaki yakınlık olarak tanımlanır. Birbirine benzer ürün ve reklamlar, tüketicinin ürünleri birbirine karıştırmasına neden olmaktadır. Reklam müdahaleciliği ise reklamın editoryal içeriğin akışını bozmasını ifade eder. Bu durum ise tepki teorisine (reactance theory) göre tüketicinin özgürlüğünün tehdit edilmesine ve tepki göstermesine neden olur. Özetle Ha (1996) reklam kirliliğinin iki şekilde müdahaleci olduğunu ileri sürer. Bunlardan ilki çok fazla reklamın yarattığı karışıklık, ikincisi içerik akışının bozulmasıyla meydana gelen psikolojik tepkidir. Çalışma, algılanan reklam müdahalesi ve reklam fazlalığının bir mecra üzerindeki reklama yönelik tutum üzerinde olumsuz etkisinin olduğunu göstermiştir.

Speck ve Elliott (1997b, s. 40) dergi ve televizyon reklamlarında algılanan reklam kirliliğinin nedenleri ve sonuçlarını ele aldıkları çalışmada iletişim problemlerinin algılanan reklam kirliliğini arttırdığını ve bunun sonucunda da reklama yönelik olumsuz tutum ve reklamdan kaçınmanın arttığını ortaya koymuştur. Reklam kirliliğini iletişim

teorisiyle açıklayan bu çalışmaya göre kullanıcıların sınırlı bilgi işleme kapasitesi vardır. Bu nedenle kaynak ve hedef arasına giren diğer unsurlar gürültü olarak algılanır. Reklam ise yarattığı iletişim problemleri ile gürültünün temel sebebi olarak görülür ve reklam kirliliğine yol açar.

Geleneksel medyaya kıyasla daha amaç odaklı olan internet mecrasında da reklam kirliliği reklamdan kaçınmanın bir öncülü olarak ele alınmıştır. Örneğin, Cho ve Cheon (2004) internet reklamları bağlamında reklam kirliliğini, internette yer alan reklam fazlalığı (excessiveness), internetteki reklam sayısından kaynaklanan rahatsız edicilik (iritasyon) ve internetin sadece bir reklam aracı olma algısı (ad exclusiveness) olarak ele almışlardır. Reklam kirliliğini ifade eden bu üç boyutun da internet reklamlarından kaçınmaya etki ettiği ortaya koyulmuştur.

Daha çok reklam fazlalığı olarak ele alınan reklam kirliliğinin dijital reklamcılık alanında yapılan farklı çalışmalarda da (örn: İspir ve Süher, 2009; Guardia, 2015; Seyedghorban vd., 2016; Li, 2019; Kelly vd., 2021) reklamdan kaçınmaya etki ettiği ortaya konmuştur.

2.3.2.2. *Hedef engeli ve reklam müdahaleciliği*

Reklamın çoğu zaman kişinin ulaşmak istediği içeriği engellemesi bazı çalışmalarda iletişim problemleri (Speck ve Elliot, 1997a-1998), bazı çalışmalarda hedef engeli (Cho ve Cheon, 2004), bazı çalışmalarda ise reklam müdahaleciliği (Ha, 1996; Li, Edwars ve Lee; 2002), olarak ele alınmıştır.

Reklamla ilgili iletişim problemleri ya da hedef engeli, bilgi teorisiyle (information theory) açıklanır ve bilgi teorisi bunu reklamı bilgiye ulaşmayı engelleyen gürültü kaynağı olarak ele alır. Reklamla ilgili gürültüye neden olabilecek muhtemel üç iletişim sorunu olduğu ifade edilir. Reklamlar bir kişinin medya içeriğini aramasını engelleyebilir (search hinderence), reklamlar medya içeriğini tüketen bir kişinin dikkatini dağıtabilir (distract) ve reklamlar medya tüketimini tamamen kesintiye uğratabilir (disrupt) (Speck ve Elliot, 1997a; Cho ve Cheon, 2004).

İçeriğin engellenmesi geleneksel mecralarda reklamdan kaçınmayı etkilemektedir. İçeriği kesintiye uğratma ise yayın medyası olan televizyon ve radyo için kaçınmaya etki etmektedir. İzleme ve dinleme basılı mecraya göre daha pasif süreçlerdir. Reklamdan kaçınmak için ise kişiler pasif durumdan aktif duruma geçmelidir. Radyo ve televizyon reklamlarında ise kullanıcılar reklam zamanlaması ve uzunlukları üzerinde çok az

kontrole sahiptir. Bu nedenle reklamlar program içeriklerine ulaşmayı daha fazla kesintiye uğratabilir. Dikkatin dağılması ise sadece radyo reklamlarında kaçınmayı etkilemektedir. Radyoda kanal değiştirmek televizyona göre daha az düşünce gerektiren ve daha kolay bir eylemdir. Üstelik aynı ilginlikte başka bir radyo kanalı bulmak daha kolaydır. Televizyonda ise ilginliğin yüksek olduğu bir programı kaçırmak insanları kanal değiştirmekten alıkoyabilir (Speck ve Elliott, 1997a, s. 72-73).

İnternet ise geleneksel mecraya göre daha fazla amaç odaklı (goal-oriented) bir araç olarak görülmektedir. Bu nedenle internet reklamları geleneksel mecraya göre daha fazla amacı engelleyen reklamlar olarak algılanır. İnternet reklamları, tüketicinin web içeriğine göz atma çabalarını engelleyen önemli bir gürültü veya rahatsızlık kaynağı olduğunda, tüketicinin web sayfasını görüntülemesini bozabilir, izleyicileri web sayfasının editoryal bütünlüğünden uzaklaştırabilir ve istenen bilgiyi aramalarına müdahale edebilir. Örneğin, tüketiciler internette istenen içeriği bulmak için gezinme sürecinin zor olduğunu hissedebilirler çünkü internet reklamları istenen bilgi için genel aramayı kesintiye uğratır veya araya girer, bu da müdahale kaynağından uzaklaşmaya (yani reklamdan kaçınmaya) neden olabilir. Bu nedenle, tüketici arama engeli, kesinti ve dikkatin dağılmasıyla gösterilen algılanan hedef engelinin internette de reklamlardan kaçınmaya neden olabileceği düşünülmektedir (Cho ve Cheon, 2004, s. 90).

Li vd. (2002) ise kişilerin istenmeyen reklam içeriklerine maruz kaldığı anlarda ortaya çıkan negatif tutum (iritasyon gibi) ve davranışların (kaçınma) çalışmalarda odak noktası olurken çok az çalışmanın algılanan reklam müdahaleciliğine yer verdiğini ileri sürer. Reklama yönelik rahatsız edicilik ve kaçınmanın temel sebeplerinden biri olarak ele aldıkları reklam müdahaleciliğini Ha (1996) ve Speck ve Elliott'a (1997a) atıfta bulunarak genişletirler. Ha (1996) reklam müdahaleciliğini, bir medya aracındaki reklamların içerik akışını kesintiye uğratma derecesi olarak tanımlar. Speck ve Elliott (1997a) ise reklamları gürültü kaynağı olarak ele alır ve çeşitli iletişim sorunlarına neden olabileceğini açıklar.

Li vd., (2002, s. 39) ise psikolojik tepki teorisinden (psychological reactance theory) yola çıkarak insanların özgürlüklerinin kısıtlanması sonucu verilen tepki olarak reklam müdahaleciliğini; reklamın izleyicinin bilişsel sürecini kesintiye uğrattığında ortaya çıkan bir algı ve psikolojik durum olarak tanımlar. Bu nedenle reklamın kendisi değil izleyicinin hedeflerini kesintiye uğratması müdahaleci olarak algılanmalıdır. Müdahalecilik reklamın yarattığı rahatsız ediciliğin bilişsel bir süreci olarak düşünülse de

bu tarz ortaya çıkabilecek olumsuz duygulardan ayrı düşünülmelidir. Reklamdaki müdahalecilik algısı bu olumsuz duygular değil bu tepkileri uyandıran bir durum olarak ele alınır. Bu algı mecralara göre farklılaşabilir. Özellikle internet geleneksel mecraya göre farklı formatta ve beklenmedik anlarda reklam yayınlamanın yeni yollarını geliştirir. Tüketicinin beklemediği anlarda ve yerlerde reklamlarla karşılaşması algılanan müdahaleciliği dolayısıyla reklamın etkililiğini etkileyebilir. Bu anlamda reklam müdahaleciliği, tüketicinin devam eden bilişsel süreçlerine müdahale eden reklamlara verilen psikolojik bir tepki olarak tanımlanır. Reklamın hacim, uzunluk, boyut veya fazlalık (clutter) gibi özellikleri bu algıyı arttırabilir. Müdahalecilik algısını ise bağlamdan bağımsız olarak ölçmeye çalışırlar. Örneğin, bir dergi, televizyon programı arası ya da bir e-posta kutusunda çıkan bir reklam bilişsel işlemeye müdahale ettiği sürece reklamın müdahaleci olarak (intrusiveness) algılanması mümkündür. Çalışmada reklam müdahaleciliği; dikkat dağıtıcı, kesintiye uğratan, zorlayıcı, karışan, müdahaleci, istilacı ve rahatsız edici (Distracting, Disturbing, Forced, Interfering, Intrusive, Invasive, Obtrusive) olarak yedi kavramla ölçülür.

Reklam müdahaleciliği ve hedef engeli, internet reklamları (Cho ve Cheon, 2004; Li vd., 2002), mobil reklamlar (Shin ve Lin, 2016), e-posta reklamları (Morimoto ve Chang, 2009), video reklam (Kim vd., 2013), sosyal medya reklamları (Wei vd., 2019; Youn ve Kim, 2019b) ÇDR (Li ve Huang, 2016; Wijenayake ve Pathirana, 2019; Udadeniya vd., 2019) gibi birçok reklam çalışmasında kaçınmanın öncülü olarak ele alınmıştır.

2.3.2.3. *Önceki olumsuz deneyimler*

Tüketicinin seçim kararı önceki bilgilerinden ve deneyimlerinden etkilenmektedir (Bettman vd., 1980). Deneyimlerden öğrenilen bilgilerin reklamdan alınan bilgiye nazaran tutumlar ve davranışlar üzerinde güçlü ve doğrudan bir etkisi olduğu da bilinmektedir (Smith ve Swinyard, 1982). Ayrıca tüketicinin deneyim sonucu elde ettiği bilgiyi daha güvenilir bulduğu görülmüştür (Hoch ve Deighton, 1989, s.16). Bu anlamda tüketiciler reklamla etkileşime girdiği önceki deneyimlerine dayanarak sonraki reklamlara nasıl tepki vereceğine karar verebilir. Cho ve Choen (2004) deneyimden öğrenme teorisine dayanarak, internet reklamlarıyla ilgili olumsuz deneyimler arttıkça, reklamlardan kaçınma eğiliminin de arttığını varsayar. İnternet reklamlarından kaçınmada, önceki olumsuz deneyimler, bir reklamı tıklamada yaşanan

memnuniyetsizlik, fayda ve teşvik eksikliği olarak üç grupta ele alınmıştır. ÇDR bağlamında ise önceki olumsuz deneyimler gizliliğiye yönelik olumsuz deneyimleri de ifade etmektedir (Xu vd., 2012).

Reklama yönelik olumsuz deneyim birçok çalışmada (Cho ve Cheon; 2004; Kelly vd., 2010; Seyedghorban vd., 2016; Li vd., 2017; Van den Broeck vd., 2018; Li, 2019) reklamdan kaçınmaya etki eden nedenlerin başında yer almıştır.

2.3.2.4. *Reklama yönelik tutum*

Reklamdan kaçınmadaki temel sebeplerden biri reklama yönelik algı ve tutumlardır. Ancak yapılan araştırmalarda her mecra için reklama yönelik algı ve kaçınma arasında farklı sonuçlar olduğu görülür. Bu durum ise reklama yönelik genel tutumlardan ziyade bir reklama yönelik tutum ile açıklanır. Belirli bir mecradaki, formattaki ya da farklı içeriğe sahip olan reklamlara yönelik farklı inanç yapıları mümkündür. Bir reklama yönelik tutum, belirli bir maruz kalma süresinde belirli bir reklam uyaranına olumlu veya olumsuz bir şekilde yanıt verme eğilimi olarak tanımlanmaktadır. Bir reklama yönelik tutumu; reklam güvenilirliği, reklam algıları, reklam verene yönelik tutum, reklama yönelik genel tutum ve ruh hali (mood) belirler (MacKenzie ve Lutz, 1989, s. 49). Ducoffe (1996) ise kullanımlar ve doyumlar teorisine dayanan reklam değeri teorisiyle internet reklamlarına yönelik tutumun öncülleri olarak bilgilendirici, eğlendirici ve rahatsız edici olarak üç değişken belirlemiştir. Brackett ve Carr (2001), ise reklam değerinde yer alan üç öncüle, güvenilirlik öncülünü eklemiştir.

Reklamdan kaçınma çalışmalarında ise tutum, reklamdan kaçınmaya neden olan bir değişken olarak ele alınır. Speck ve Elliot (1997a) çalışmasında bir reklama yönelik tutum, reklama yönelik algı olarak ifade edilmiştir. Bu algıları yazarlar faydalı, ilgi çekici, aşırı (reklam fazlalığı), can sıkıcı, inandırıcı ve zaman kaybı olarak ele almıştır. Bazı kaçınma çalışmalarında ise (örn: Süher ve İspir, 2010) bu algı değişkenleri, bir reklama yönelik tutum olarak ele alınmıştır. Bir reklama yönelik tutumu eğlendirici, bilgilendirici, faydalı, güvenilir gibi olumlu ve rahatsız edici, aşırı, can sıkıcı vb. olumsuz birçok özellik belirlemektedir. Tutumun davranışın öncülü (Fishbein ve Ajzen, 1975) olduğu temel yaklaşımla, bir reklama yönelik tutum birçok araştırmada (Morimoto ve Chang, 2009; Morimoto ve Macias, 2009; Kim vd., 2013; Van der Goot vd., 2018) reklamdan kaçınmanın öncülü olarak ele alınmış, bazı çalışmalar (Tran, 2017; Chung ve Kim, 2021)

ise güven, rahatsız edicilik, fayda gibi olumlu ya da olumsuz reklam algılarının tek başına bir değişken olarak kaçınmaya etkisini incelemiştir.

Bir sonraki bölümde tezin kavramsal çerçevesini oluşturan koruma motivasyonu bağlamında ÇDR'den kaçınmaya etki eden motivasyonlara yer verilmiştir.

2.4. Kavramsal Çerçeve: Koruma Motivasyonu Bağlamında ÇDR'den Kaçınmada Etkili Olan Motivasyonlar

Bu bölümde tezin kavramsal çerçevesini oluşturan koruma motivasyonu teorisi ve bu teori bağlamında ÇDR'den kaçınmaya etki eden değişkenlere yer verilmiştir. İlk bölümde koruma motivasyonu teorisinin ne olduğuna dair kavramsal bir çerçeve sunulmuştur. Daha sonra koruma motivasyonu bağlamında ÇDR'ye yönelik tehdit ve başa çıkma değerlendirmelerine yer verilerek koruma motivasyonlarının gizlilik endişesi ve gizlilik kontrolü üzerindeki etkilerine değinilmiştir. Son olarak ise ÇDR'den kaçınma çalışmaları ve gizlilik endişesinin ÇDR'den kaçınma üzerindeki etkileri açıklanmıştır.

2.4.1. Koruma motivasyonu teorisi

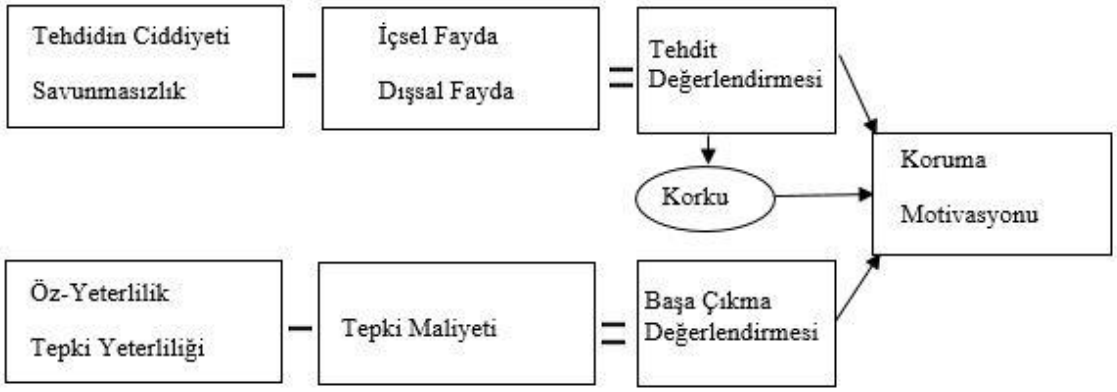
Koruma motivasyonu teorisinin (KMT) temelleri, Yale İletişim ve Tutum Değişimi Araştırma Programı'nda yürütülen korku çekiciliklerinin tutum ve davranışları değiştirebileceği yol ve koşullara ilişkin sistematik çalışmalara dayanır (Norman vd., 2015). Beklenti değer teorisini temel alarak geliştirilen KMT, riskli bir durumda bireyin bilişsel süreçlerini açıklamaya çalışarak koruma motivasyonuna etki eden nedenleri bir araya getiren bir model ortaya koyar. Korku çekiciliği özelinde ele alınan çalışma KMT'nin aslında risk barındıran durumlarda koruma motivasyonlarını ortaya çıkarmak için farklı alanlarda da kullanılabileceğini önerir (Rogers, 1975, s. 95).

Rogers (1975) daha önce duygu teorileri ile çalışılan korku çekiciliğinin kişide koruma motivasyonuna ve kişinin davranışına nasıl etki ettiğini açıklayan teorik bir yapı kurmayı amaçlayarak KMT'yi geliştirir. KMT'ye göre bireyler bir korku uyaranı ile karşılaştığı zaman üç farklı değerlendirme süreci gerçekleştirir. Bunlardan ilki korkuya sebep olan durumun ne kadar ciddi olduğuna yönelik değerlendirmeyi kapsar. İkinci olarak birey korku uyaranının gerçekleşme olasılığına karşı savunmasız olup olmadığını değerlendirir. Son olarak ise korku uyaranını önleyeceği iddia edilen tepkinin yeterliliğini değerlendirilerek koruma motivasyonu geliştirir ve daha sonra davranış gerçekleşir. Örnek verilecek olursa korku çekiciliği (kanser) içeren sigara karşıtı bir reklam ile

karşılaşan birey ilk önce sigaranın kanser yapma tehlikesinin ciddi bir tehlike olup olmadığını değerlendirir. Daha sonra ise sigara içmenin kendisini kanser karşısında ne kadar savunmasız yaptığını ve son olarak sigarayı bırakmanın kanserden kendisini koruyup korumayacağını değerlendirmektedir. Eğer kanseri ciddi bir risk olarak düşünür ve kendini savunmasız hissederse ve sigarayı bırakmanın kanseri önlemede etkili bir davranış olduğuna ikna olursa sonunda koruma motivasyonu ve koruma davranışı olan sigarayı bırakma gerçekleşir.

İlk çalışmada teorik bir çerçeve çizen Rogers daha sonra iki bilişsel süreci başlatan faktörlerin de eklenmesi ile teoriyi geliştirip koruma davranışlarını tahmin etmek için bütünsel bir model öne sürmüştür. Genişletilen model, koruma motivasyonunun tehdit ve başa çıkma olarak iki bilişsel değerlendirme süreciyle başladığını varsayar. Bu iki sürecin başlamasında ise çeşitli bilgi kaynakları (çevresel, kişilik, önceki deneyimler vb.) etkili olur. Modelde tehdidi değerlendirmek için onun varlığından haberdar olunması bir ön koşul olarak kabul edilir.

Tehdit değerlendirmesi; tehdidin ciddiyeti (severity) ve tehdide karşı savunmasızlığın (vulnerability) zararlı davranışın getirdiği içsel ve dışsal ödüllere oranı ile ölçülür. Başa çıkma değerlendirmesi ise koruma davranışını gerçekleştirmeye yönelik öz yeterlilik (self-efficacy) ve tepki yeterliliğinin (responce efficacy) davranışı gerçekleştirme maliyetlerine (response costs) oranının değerlendirilmesi ile ölçülür. Tehdidin ciddiyeti ve tehdide karşı savunmasızlık korkuyu arttırır ancak başa çıkma değerlendirmesi yüksekse bireyin kontrol algısı yükselir ve istenilen davranış değişikliğine neden olur (Rogers, 1983).



Şekil 2.3. Koruma motivasyonu teorisi, Rogers (1983)

Kısaca teori risk altındayken bireylerde gerçekleşen davranışları araştırır. Buradaki risk kişiyi tehlike altına sokan ve korku uyandıran bir durumun koruma motivasyonunu

harekete geçirmesi ile ilişkilidir. Risk altındaki bireyin koruma davranışını gerçekleştirmesi aynı zamanda öz-yeterliliği ve tepki yeterliliğine yönelik algıları ile belirlenmektedir.

Çevrimiçi gizlilik bağlamında KMT değerlendirildiğinde, bireysel gizlilik kaygıları, bir tehdit olarak değerlendirilebilir. Bilgi gizliliğine yönelik tehditler, kişisel bilgilerin ifşa edilmesi, kişisel bilgilerin toplanması, ikincil kullanımı ve paylaşılmasıyla ilgili çeşitli tehditleri, yetkisiz kuruluşların uygunsuz erişimini ve bu tür bilgilerin şirketler tarafından saklanması sırasındaki hataları içermektedir (Ioannou vd., 2021). Bu anlamda genellikle sağlık iletişiminde kullanılan teori gizlilik araştırmalarında da (Ioannou vd., 2021; Mousavi vd., 2020; Park ve Lee, 2014; Mohamed ve Ahmad, 2012; Youn, 2009) sıklıkla kullanılmaktadır.

Bu çalışmada ÇDR'den kaçınma KMT kapsamında ele alınmıştır. Bu bağlamda tüketicinin ÇDR'yi gizliliğe yönelik bir tehdit olarak değerlendirip değerlendirmediği ve bunun sonucunda ÇDR'den kaçınma niyetinin olup olmadığı incelenmiştir. Çalışmada ÇDR'den kaçınma niyetini etkileyen iki bilişsel sürecin olduğu varsayılmıştır. Bu süreçlerden ilki tehdit değerlendirmesidir. Bu değerlendirme sonucu oluşan korku çalışmada gizlilik endişesi olarak ifade edilmiştir. Gizlilik endişesinin oluşması gizliliğe yönelik risklerin ciddiyeti, riske karşı savunmasızlık ve ÇDR'ye yönelik faydaların değerlendirilmesini içerir. Bu değerlendirmeler sonucu gizlilik endişesi yüksek olan bireyin ÇDR'den kaçınacağı varsayılmaktadır. İkinci süreç ise başa çıkma değerlendirmelerini kapsar. Bu süreçte birey gizliliği korumaya yönelik öz-yeterliliğini, gizliliği korumaya yarayan tepkilerin yeterliliğini ve bu tepkileri almasının getireceği maliyetleri değerlendirir. Modelin bu aşamasında başa çıkma değerlendirmelerinin ise gizlilik kontrolünü arttıracağı varsayılarak modele bu değişken eklenmiştir. Gizliliğe yönelik kontrol algısı yüksekse bireyin ÇDR'den kaçınacağı varsayılmaktadır.

Bu nedenle çalışmanın kavramsal çerçevesinde önce ÇDR'ye yönelik gizlilik endişesi ve gizlilik endişesine neden olan tehdit değerlendirmelerine daha sonra ise ÇDR'ye yönelik gizlilik kontrolü ve gizlilik kontrolünde etkili olan başa çıkma değerlendirmelerine yer verilmiş, son olarak da ÇDR ve kaçınma çalışmalarına değinilmiştir.

2.4.2. ÇDR'ye yönelik gizlilik endişesi ve tehdit değerlendirmeleri

Dijitalleşme süreci veri toplama, ayrıştırma ve depolama maliyetlerini azalttığından, pazarlamanın birçok alanında verilerin benzeri görülmemiş bir düzeyde

kullanılmasına olanak tanır. Tüketici verilerinin kullanımı firmaların sağlık, reklam, güvenlik, e-ticaret, ulaşım ve bankacılık gibi sektörlerde rekabet etmek için iş modellerini inşa ettikleri ve giderek kullanımı artan bir yöntem haline gelmiştir. Firmaların, ürün ve hizmetler için yeni fikirlerin geliştirilmesinden, bunları potansiyel hedef müşterilere satmaya kadar her şey için tüketici verilerini kullanması, pazarlamanın veriye dayalı olması gerekliliğinin savunulmasına neden olmaktadır. Örneğin Netflix müşterilerine kişiselleştirilmiş öneriler sunmak, Google yeni reklam uygulamaları geliştirmek için tüketici verilerini kullanmaktadır (Bleier vd., 2020).

Veriye dayalı reklam formatlarından biri olan ÇDR en temelde web sitelerinde tüketicinin göz atma geçmişinin izlenmesine dayanır (Im vd., 2023; Kim vd., 2019; Ham, 2017; Boerman vd., 2017; Bleier ve Eisenbeiss, 2015a; Bleier ve Eisenbeiss, 2015b; Lambrecht ve Tucker, 2013; McDonald ve Cranor, 2010a; Turow vd., 2009). ÇDR'nin dijital ortamlarda tüketicinin davranışlarını izlemesi ve bu verileri reklam amaçlı kullanması daha önce de bahsedildiği gibi karmaşık bir sistemdir. ÇDR uygulayıcıları kişiyi tanımlayan verileri kullanmadıklarını dile getirse de (Boerman vd., 2017) çalışmalar, izlenen bilgileri kişiyi tanımlayan bilgilerle ilişkilendirmenin genellikle kolay olduğunu göstermektedir (Backes vd., 2012). Bu nedenle etik ve yasal olarak da tartışma konusu olan ÇDR ve gizlilik endişesi ilişkisi, reklam literatüründe de reklamın etkililiği ya da reklama yönelik tepkiler bağlamında sıklıkla ele alınmaktadır.

Tüketici bağlamında gizlilik endişeleri bölümünde de açıklandığı üzere gizlilik endişesine yönelik çok sayıda tanım yapılmıştır. Bazıları (örn: Malhotra vd., 2004) gizlilik endişesini bilgi gizliliği bağlamında adalete ilişkin subjektif görüşler olarak daha geniş bir perspektiften tanımlarken bazı tanımlar (Dinev ve Hart, 2006) ise gizlilik endişesini internet üzerinden bilgi toplanmasına ilişkin algıları ifade eden daha dar bir perspektiften ele alır. Bu çalışmada ele alınan kontrol odaklı yaklaşıma göre gizlilik endişesi, bireylerin kişisel verilerinin bir kişi ya da kurum tarafından toplanmasını ve daha sonra kullanmasını kontrol etme kaygısı olarak tanımlanmıştır (Westin, 1967; Smith vd., 1996). Gizlilik endişesinin odak noktası, bireylerin kendi özel bilgilerine kimin erişimi olduğu ve bu bilgilerin nasıl kullanılacağıyla ilgili kontrol kaybı endişeleridir (Beak ve Morimoto, 2012). ÇDR'ye yönelik gizlilik endişesi ise internet ortamında dijital davranışların izlenmesi ile kişisel verilerin toplanması, kullanılması ve paylaşılması üzerindeki kontrol kaybından doğan endişeleri ifade etmektedir (Boerman vd., 2017; Ham, 2017).

Kişisel verilerin reklam amaçlı kullanımına yönelik gizlilik endişesi önceki çalışmalarda ortaya konmuştur (Dolnicar ve Jordan, 2007; Beak ve Morimoto, 2012). ÇDR ise dijital davranışların *izlenmesi* ve kişisel verilerin kullanılarak reklamların *hedeflenmesi* olarak iki süreçte gerçekleşir. Bu anlamda ÇDR ve gizlilik endişesine yönelik ilk çalışmalarda özellikle davranışsal izlemeye yönelik tüketici tutumlarına ve ÇDR'ye yönelik tüketici algılarına odaklanılmıştır. Bu tutumlar genellikle kişisel veriler üzerindeki kontrol kaybı ve gizlilik endişesi ile bağlantılıdır. Örneğin Turow vd. (2009) tarafından gerçekleştirilen çalışmaya göre Amerikan tüketicilerinin %84'ünün dijital davranışlarının üçüncü taraflarca izlenmesini istemedikleri ve %64'ünün kişisel veriye dayalı reklamlardan hoşlanmadıkları tespit edilmiştir. Aynı şekilde McDonald ve Cranor'un (2010b) Amerikan tüketicileri üzerinde yaptıkları araştırmada tüketicilerin %69'unun gizliliği bir hak olarak gördüğü ve %64'ünün ÇDR'yi istilacı olarak ifade ettiği sonucu çıkmıştır. Çoğu tüketici kişisel verilerin izlenmesi ve reklam amaçlı toplanmasını gizlilik ihlali olarak nitelemiş ve bu doğrultuda gerçekleştirilen çalışmalar ÇDR'nin gizlilik endişelerine sebep olduğunu ortaya konmuştur.

Çalışmalarda ayrıca ÇDR'ye yönelik tüketici algıları, gizlilik endişesine neden olan bir başka konu olarak ele alınmıştır. Çoğu tüketicinin, reklam şirketlerinin internet davranışlarını izlemesini gizlilik kaybına yol açan, istilacı ve ürkütücü (creepy) bulduğu görülmüştür. (Turow vd., 2009; McDonald ve Cranor, 2010a; Ur vd., 2012; Smit vd., 2014; Moore vd, 2015; Fachryto ve Achyar, 2018). ÇDR sisteminde çevrimiçi etkinliklerin izlenmesinin, davranışsal verilerin toplanmasının ve bilgilerin yayılmasının sıklıkla tüketicinin bilgisi olmadan gizlice gerçekleştiği (Ham ve Nelson 2016; Nill ve Aalberts, 2014) ve bu nedenle çoğunlukla ÇDR'nin örtülü (covert) bir reklam uygulaması olarak görülmesine neden olduğu bilinmektedir (Boerman vd., 2017; Aguirre vd., 2015). Bazı örnek olay çalışmaları da davranışsal hedeflemenin tüketici rızası dışında gerçekleştiğini kanıtlar niteliktedir (Dwyer, 2009). Kuruluşların çerezler gibi teknolojileri örtük bir şekilde kullanmasının güvene zarar verdiği ve satın alma niyetini azalttığı bilinmektedir (Martin ve Murphy, 2017). Tüketiciler firmaların açık izin almadan örtük bir şekilde bilgi topladıklarını fark ettiklerinde (Sheehan ve Hoy, 2000) ya da kişisel bilgi ihlallerine maruz kalıp veya mağdur olduklarında, kişilerin bilgi gizliliği konusunda daha güçlü endişelere sahip olduğu görülmüştür (Smith vd, 1996). Bu nedenle ÇDR'ye yönelik şüphenin fazla ve şirketlere yönelik güvenin az olduğu söylenebilir (Zarouali vd., 2017). Araştırmalar bu durumda güvenin ÇDR'nin etkisinde önemli rol oynadığını göstermiştir.

Örneğin, daha güvenilir perakendeciler, tüketicilerin ilgi alanlarını eksiksiz bir şekilde yansıtan reklamlar geliştirerek reklamlarının algılanan faydasını arttırabilmektedir (Bleier ve Eisenbeiss, 2015a).

Tüketicide gizlilik endişelerine sebep olan bir diğer neden, ÇDR'nin hedefleme türünü içeren üçüncü taraf çerez sistemidir. Önceden de bahsedildiği gibi üçüncü taraf çerezler, kullanıcı bilgisayarı ya da telefonuna, kullanıcıların etkileşim kurduğu internet sayfaları, mobil uygulamalar vs. dışında, bir reklam ya da veri şirketi tarafından yerleştirilmektedir. Ayrıca veri şirketleri birçok ayrı mecradan veri toplayıp bu verileri satan şirketler olduğundan bu durumda da veri dolaşımı üzerinde kontrol kaybı gittikçe artmakta (Beck, 2015) ve verilerin kötüye kullanımından doğan gizlilik tartışmalarına zemin hazırlamaktadır (El Hana vd., 2023). Buna ek olarak üçüncü taraf çerezlerin veri birleştirmeye olanak tanıması, tüketici anonimliğini sağlama ve böylece gizliliği koruma bakımından garanti sağlamamaktadır (Smullen vd., 2021). Bu nedenle hedefli reklamların etkililiği için güvenin önemli bir faktör olduğu söylenmektedir. (Leong vd., 2020; Wiese vd., 2020). Tüketicilerin kişisel verilerinin üçüncü taraflara aktarılmaması durumunda tüketicilerin gizlilikleri konusunda daha az endişe duyacağı ve ürünlerle ilgili içeriklerden daha fazla memnun kalacağı bilinmektedir (Sutanto vd., 2013). Tüketici verilerinin kimler tarafında ne amaçla kullanıldığına yönelik güven azaldıkça gizlilik endişelerinin arttığı da bir gerçektir.

ÇDR'ye yönelik tüketici algıları ayrıca, hedeflenen reklamlardaki kişiselleştirme seviyesine, tüketicinin demografik özelliklerine, kişilik özelliklerine ve kültürel özelliklere göre değişebilmektedir. Kişiselleştirme seviyesinin, reklamı hedeflemek için kullanılan kişisel veri türlerine göre düzenlendiği söylenebilir (Boerman, 2017). Birçok deneysel çalışmada kullanılan veri türleri arasında yaş, cinsiyet, konum, eğitim düzeyi, ilgi alanı, çevrimiçi alışveriş davranışı, arama geçmişi, çevrimiçi mesajlaşma gibi bilgiler yer almıştır. Sonuçlar, kişiselleştirme düzeyinin, müdahalecilik (Van Doorn ve Hoekstra 2013), savunmasızlık (Aguirre vd., 2015), reklama yönelik tepki (Bleier ve Eisenbeiss, 2015a) rahatsız edicilik (Goldfarb ve Tucker, 2011) gibi olumsuz tepkilere neden olduğu ve gizlilik endişelerini etkilediğini göstermektedir.

Gizlilik endişesini etkilediği düşünülen bir diğer neden ise tüketicinin demografik ve kişilik özellikleridir. Yaş, cinsiyet, eğitim gibi demografik özelliklerin gizlilik endişesi üzerinde etkili olduğu bilinmektedir (Lee vd., 2015; Smit vd., 2014; Turow vd., 2009; Youn, 2005). Ayrıca tüketici kişilik özelliğinin de reklama yönelik gizlilik endişelerinde

etkisi olduğu düşünülür. Mesela nevrotik kişilik tipinin daha kaygılı, güvenmeyen kişiler olarak gizliliğe daha fazla önem verdiği ve gizlilik endişesini daha fazla hissettiği görülmüştür (Bansal vd., 2010; Dodoo ve Wen, 2019). Ayrıca kültürel özelliklerin de gizlilik endişesinde etkili olduğu bilinmektedir. Bireysel kültüre sahip ülkelerde, kolektif kültürlere kıyasla gizliliğe daha fazla önem verildiği görülmüştür (Kim, 2014; Dinev vd., 2006). Buna ek olarak Avrupa ve Amerika'ya göre gelişmekte olan ya da daha az gelişmiş ülkelerde (örn: Pakistan) gizliliğe yönelik farkındalığın yanı sıra çerez gibi teknik bir sistemin anlaşılması da zordur. Bu durum ise ÇDR'ye yönelik olumsuz tutumların yanında kişisel verilerin kullanılmasından kaynaklanan risklere yönelik korku ve endişe duygularının sergilenmesine neden olmaktadır (Asgher vd., 2022; Gökdemir ve Akıncı, 2019).

Yukarıdaki açıklamalardan da anlaşılacağı gibi reklamın türü ve kişisel özelliklere vb. göre farklılık gösterebilen ÇDR'ye yönelik gizlilik endişeleri en temelde tüketicinin bu reklamları gizliliğe yönelik bir tehdit olarak görmesi ve riskli bulmasıyla ilgilidir. Bunun en temel nedeni ise ÇDR'nin çalışma sistemi olan üçüncü taraflarca davranışsal verilerin izlenmesi ve kullanılmasıdır. KMT bağlamında tehdidin değerlendirilmesi algılanan risk (riskin ciddiyeti ve savunmasızlık) ve algılanan faydanın değerlendirilmesini içermektedir.

Algılanan risk: Gizlilik tehditlerinin çoğu zaman iyi ifade edilmediği ve sonuç olarak, gizlilik tehdit edildiğinde neyin tehlikede olduğu ve bu sorunları çözmek için yasanın tam olarak ne yapması gerektiği konusunda sıklıkla ikna edici bir açıklamanın yapılamadığı düşünülmektedir (Solove, 2008, s. 2).

Algılanan risk; performans, zaman, gizlilik ve özgürlük riski olarak farklı boyutlarda da ele alınır ve ÇDR'den kaçınmada bu risklerin etkili olduğu görülmüştür (Wang vd., 2022). Gizliliğe yönelik riskler, önceki çalışmalarda gizlilik endişesi ölçümlemesinde ele alınan boyutlarla açıklanmaya çalışılmıştır. Bunlar kişisel verilerin izlenmesi, toplanması, kullanılması ve paylaşılmasından kaynaklanacak izinsiz erişim, ikincil kullanım, kötüye kullanım, kişisel verilerin depolanmasındaki güvenliğe yönelik riskleri kapsamaktadır (Culnan, 1993; Smith vd., 1996; Sheehan ve Hoy, 2000; Malhotra vd., 2004). Tüketicilerin ÇDR aracılığıyla kişisel bilgilerinin kaybolması durumunda bilgilerin kötüye kullanım riskinin ortaya çıkabileceği düşünülür (Alraja ve Mohammed, 2015). Örneğin internet kullanıcıları kişisel bilgilerinin sızdırılması, ihlal edilmesi, çalınması (Pavlou, 2003) kimlik hırsızlığı (Saunders ve Zucker, 1999) dolandırıcılık

(Chen vd., 2017) gösterilen ürün ya da fiyatta ayrımcılık (Wachter vd., 2021) gibi güvenlik riskleri ile de karşılaşabilir. Bu durum kişisel verilerin kötüye kullanımı ve güvenliğinin sağlanamamasından doğan risklere örnektir. Mesela Facebook Cambridge Analytica skandalı, kişisel verilerin izinsiz paylaşılması, güvenliğinin sağlanmaması ve kişisel verilerin ikincil bir amaç (oy verme davranışına yönelik ikna) için kullanılmasını kapsayan gizlilik riskine örnek olarak verilebilir.

Tüketici araştırmalarında, algılanan risk ise genellikle bir bireyin bazı işlemsel durumlarla ilgili olarak sergilediği belirsizlik, rahatsızlık ve/veya endişe duyguları ile ilişkilendirilir (Dowling ve Staelin, 1994). Kişisel veriler bağlamında algılanan risk, internet kullanıcılarının çevrimiçi şirketlere ve pazarlamacılara kişisel bilgi sağlamanın olumsuz sonuçlarından emin olmadıkları bir belirsizlik olarak tanımlanabilir (Okazaki vd., 2009; Pavlou, 2003). Algılanan gizlilik riski de benzer şekilde, bir bireyin yüksek bir kayıp potansiyelinin kişisel bilgilerin açığa çıkmasıyla ilişkili olduğuna inanma derecesi olarak ifade edilir (Smith vd., 2011, s. 1001). Sonuç olarak algılanan gizlilik riski, kişisel verilere (1) başkaları tarafından fırsatçı davranış ve (2) kişisel verilerin firmalar tarafından kötüye kullanılması ihtimallerine yönelik algılardır (Dinev ve Hart, 2006). ÇDR sisteminde özellikle çerezlere ilişkin gizlilik endişesi, verilerin, bilgiyi toplayan tarafça veya onu satın alan veya başka bir şekilde elde eden üçüncü bir tarafça ikincil kullanımı ve kötüye kullanılması riskine dayanmaktadır (Sipior ve vd., 2011, s.5). Birçok çalışmada algılanan risk, gizlilik endişesinin öncülü olmuştur (Dinev ve Hart, 2004; Dinev ve Hart, 2006; Xu vd., 2011; Xu vd., 2013; Ham, 2017).

KMT bağlamında algılanan risk, tehdidin ciddiyeti ve tehdide karşı savunmasızlık olarak iki boyutta incelenir. *Algılanan ciddiyet,* kişinin riskin yol açabileceği zararın ciddiyetine ilişkin inancını ifade ederken; *algılanan savunmasızlık,* riskli durumun getireceği olası olumsuz sonuçları deneyimleme ihtimaline olan inancını ifade eder (Witte, 1992; Salleh vd., 2012; Boerman vd., 2018). ÇDR açısından riske karşı savunmasızlık, tüketici verisinin ÇDR aracılığıyla bireysel bir tüketicinin gizliliğine zarar gelmesi ihtimaline yönelik inancı anlamına gelmektedir. Bir riskin ciddiyeti ise, ÇDR aracılığı ile tüketicinin gizliliğine yönelik herhangi bir zararın algılanan önemini ifade eder (Ham, 2017).

KMT bağlamında yapılan gizlilik araştırmalarında algılanan riskin gizliliği korumaya yönelik davranışları artırdığı ortaya konmuştur. Örneğin tehdidin algılanan şiddeti ve tehdide yönelik algılanan savunmasızlığı ne kadar büyük olursa, çevrimiçi

tüketicilerin koruma davranışını benimseme olasılığı da o kadar artmaktadır (LaRose vd., 2005). Bilgi gizliliğini korumaya yönelik önceki araştırmalar, algılanan gizlilik risklerine yönelik ciddiyetin ve savunmasızlığın, bilgisayardaki bilgileri yedekleme davranışlarını (Crossler, 2010), casus yazılımları önleme programı kullanma konusundaki davranış niyetlerini (Chenoweth vd., 2009) kablosuz ağ kullanıcılarının güvenlik önlemlerini uygulama kararlarını (Woon vd., 2005) arttırdığı, bir web sitesinde bilgi paylaşma istekliliğini ise azalttığını (Youn, 2005) göstermektedir. Bazı çalışmalarda (Woon vd., 2005; Strycharz vd., 2019) ise riske yönelik algılanan ciddiyet koruma davranışını etkilerken savunmasızlığın koruma davranışına bir etkisi bulunamamıştır. Woon vd. (2005) tarafından gerçekleştirilen araştırmaya göre kablosuz ağ kullanıcılarının güvenlik önlemlerini uygulama kararlarını riskin ciddiyeti etkilerken savunmasızlığın bu kararlara bir etkisi bulunamamıştır. Strycharz vd. (2019) tarafından gerçekleştirilen ve kişiselleştirilmiş reklamlara yönelik koruma motivasyonlarının belirlendiği çalışmada, riske yönelik algılanan ciddiyetin fazla olması, koruma motivasyonu ve davranışında etkiliyken riskin olma ihtimalinin yani riske karşı savunmasızlığın bunlarda bir etkisinin olmadığı tespit edilmiştir. Teknik olarak bilgi sahibi olan tüketicilerin kendilerini savunmasız görmemesi bu durumun nedeni olarak ifade edilmiştir.

KMT bağlamında tüketici gizliliğine yönelik çalışmalarda algılanan riskin ayrıca endişeyi artırdığı bilinmektedir (Lwin vd., 2007; Youn, 2009; Mohamed ve Ahmad, 2012; Aguirre vd., 2015; Ham, 2017; Mousavi vd., 2020). Örneğin Lwin vd. (2007), çalışmalarında özellikle hassas verilere (finans, sağlık vb.) yönelik algılanan riskin gizlilik endişesini arttırdığını söyler. Ancak bu verilerin yapılan işlemlerle uygun olması, gizlilik endişesini azaltmıştır. Bu, bir tüketicinin satın alma bilgilerini bir süpermarketin web sitesine açıklarken, ilgisiz bir çevrimiçi işletmeye kıyasla daha az endişe duyacağı anlamına gelir. Bu anlamda ÇDR özellikle üçüncü taraf çerezleri ifade ettiği için tüketicide algılanan risk ve endişeyi artıracağı ön görülebilir. Youn (2009) ergenler üzerinde yaptığı çalışmada pazarlama şirketlerinin veri toplama uygulamalarına yönelik algılanan savunmasızlığın gizlilik endişesini arttırdığını ortaya koymuştur. Mohamed ve Ahmad (2012) sosyal medya bağlamında gizlilik riskine yönelik algılanan ciddiyet ve savunmasızlığın gizlilik endişesini arttırdığı sonucuna ulaşmıştır. Aguirre vd. (2015) tarafından yürütülen ve sosyal medya bağlamında yapılan deneysel çalışmada, sosyal medya mesaj verilerinin reklam amaçlı kullanılması örtük bilgi toplama olarak tüketicinin savunmasızlık algılarını artırdığını ve reklamı tıklama niyetlerini azalttığını ortaya

koymuştur. Yine sosyal medya bağlamında Mousavi vd. (2020) risk algısının gizlilik endişesini arttırdığını ve koruma motivasyonuna etki ettiğini ortaya koymuştur. ÇDR bağlamında da algılanan risk (ciddiyet ve savunmasızlık) tüketici gizlilik endişelerinin artmasına neden olmaktadır (Ham, 2017). Bu araştırmalar sonucunda ÇDR'ye yönelik algılanan riskin ciddiyeti ve algılanan savunmasızlığın ÇDR'ye yönelik gizlilik endişesine neden olduğu düşünülmektedir.

Algılanan fayda: ÇDR bağlamında algılanan fayda literatürde, reklamın kullanışlılığı (usefulness), algılanan kişiselleştirme (perceived personalization) ve reklamın algılanan faydası (perceived benefit) olarak üç şekilde ele alınır. Reklamın algılanan kullanışlılığı, alışveriş deneyimini iyileştirme ve etkinliği arttırma, satın alma işlemlerini daha hızlı ve kolay yapmaya yardımcı olma olarak ifade edilir (Tam ve Ho, 2006; Aiolfi vd., 2021). Algılanan kişiselleştirme ise daha çok kişiselleştirilmiş reklama yönelik olumlu algıları ifade eder. Bu algılar reklamın tüketiciye ihtiyacı olan bilgiyi ve satın alma tavsiyelerini iletmesi, ilgi alanına yönelik ürünleri elde etmede sağladığı kolaylık ve kişiselleştirmenin tüketiciyi tek ve benzersin bir müşteri olarak hissettirmesini içerir (Li ve Huang, 2016). Algılanan kullanışlılık daha çok teknoloji kabul modeli perspektifinden reklamın sağladığı yarara odaklanırken, algılanan kişiselleştirme ise tüketicinin hedefli reklamı nasıl algıladığına odaklanır.

KMT bağlamında fayda, riskli durumun getirdiği ödülleri ifade eder (Rogers, 1975). Önceden de bahsedildiği gibi belirli pazarlama ödüllerini almak için tüketiciler kişisel bilgilerini paylaşmayı kabul edebilir. Bu ödüller kişiselleştirilmiş ürün teklifleri ve öneriler, fiyat indirimleri ve kuponlar, ücretsiz hizmetler ve daha alakalı pazarlama iletişimleri ve medya içeriği olarak tanımlanabilir (White, 2004; Jin vd., 2012; Martin ve Murphy, 2017). Bu çalışmada ise algılanan fayda, davranışsal hedeflemenin getirdiği faydaları ifade eder. Davranışsal hedeflemenin tüketicilere iki şekilde faydalı olması muhtemeldir. Birincisi, tüketiciler muhtemelen ilgilendikleri ürün ve hizmet ile ilgili reklamları alırlar. İkincisi, internetteki çok sayıda ücretsiz içeriğe erişim elde ederler (Aalbert vd., 2016). Bu nedenle ÇDR bağlamında algılanan fayda, kişisel verilerin kullanılmasının tüketiciye daha alakalı, bilgilendirici ve eğlenceli içeriklerin yanı sıra ilgi alanına uygun reklam mesajları, ürün teklifleri sağlamasıyla ilişkilendirilir (Ham, 2017).

ÇDR bağlamında hedeflemenin olumlu etkileri, tüketiciler tarafından algılanan yüksek alaka düzeyiyle (relevance information) açıklanmaktadır (de Groot 2022; De Keyzer vd., 2022; Kim ve Huh, 2017). ÇDR, insanların çevrimiçi davranışlarını ve kişisel

verilerini kullandığından, reklamın içeriğinin tüketiciler tarafından daha alakalı olarak algılanması muhtemeldir ve bu da sonuç olarak reklamdan beklenen etkiyi artırabilir (De Keyzer vd., 2022; Özçelik ve Varnalı, 2019; Jung, 2017) ve reklamdan kaçınmayı azaltabilir (Ham, 2017; Youn ve Shin, 2020). Son çalışmalar ÇDR'nin hedeflenmemiş reklamlara oranla daha olumlu tutuma neden olduğunu ancak gizlilik endişesinin bu olumlu tutumu azalttığını göstermektedir (Zhang vd., 2023). Bazı yazarlara göre ise reklamverenler ve markalar tüketicilerin kişiselleştirilmiş reklamları yararlı bulduklarını düşünmek isterler. Ancak yapılan tutum araştırmalarında tüketici "ilgi alanıma yönelik reklamları yararlı bulurum" demesine rağmen gizlilik endişelerini de beraberinde taşıdıkları gerçeği göz ardı edilmemelidir. Yapılan etki araştırmaları sadece kişiselleştirilmiş reklamlara yönelik tutumları içeren sorulara yer vermektedir ve kişisel verilerin ihlali kısmını bildiğinde çoğu tüketicinin gizlilik endişeleri de ortaya çıkacaktır (Marshall, 2014'ten aktaran Gökdemir ve Akıncı, 2019).

Sonuç olarak çoğu tüketici kişisel reklamları yararlı bulurken aynı zamanda verilerinin bunun için kullanılmasını istememektedir (McDonald ve Cranor, 2010a; Ur vd., 2012; Smit vd., 2014). Literatürde gizlilik paradoksu (Aguirre vd., 2015) olarak ifade edilen bu durum tüketicinin ÇDR algısında hem risk hem de fayda olduğunu ortaya koymaktadır. Aynı anda hem olumlu hem olumsuz algıların olması ÇDR etki çalışmalarında farklı sonuçlarla karşılaşılmasındaki nedenlerden biridir. Bu durum KMT ile ele alındığında tüketicinin gizlilik endişesine neden olan iki değerlendirmesi yani risk ve fayda değerlendirmesi söz konusudur. Eğer algılanan fayda algılanan riskten daha fazla ise gizlilik endişesinin azalacağı varsayılmaktadır.

2.4.3. ÇDR'ye yönelik gizlilik kontrolü ve başa çıkma değerlendirmeleri

Bilgi gizliliği kavramı çoğunlukla bireyin kişisel bilgileri üzerindeki kontrolü perspektifinden tanımlanır. Gizlilik endişesi tanımlarının temelinde de insanların kişisel bilgileri üzerinde kontrol kaybı (loss of control) hissetmelerinden doğan endişe yer alır. (Westin, 1967; Altman, 1975; Dolnicar ve Jordan, 2007). Bu perspektifte algılanan kontrol, bireyin kişisel bilgilerinin açıklanmasını ve yayılmasını yönetme becerisine ilişkin inançları olarak tanımlanır (Xu vd., 2011). Bu çalışmada ise gizlilik kontrolü reklam şirketleri tarafından toplanan ve kullanılan kişisel veriler üzerinde kontrole sahip olup olmama inancı olarak tanımlanmıştır.

KMT, tüketici tepkisini azaltmada gizlilik kontrollerinin rolüne vurgu yapmaktadır (Feng ve Xie, 2019, s. 48). ÇDR literatüründe gizliliği koruma motivasyonu, riski azaltıcı davranışlar yani kontroller üzerinden tanımlanmıştır (Ur vd., 2012; Chen vd., 2016; Ham, 2017; Boerman vd., 2018; Okazaki vd., 2020). KMT bağlamında ise kişinin öz-yeterliliği, tepkinin yeterli olduğuna dair inancı ve tepkinin getireceği maliyetler algılanan gizlilik kontrolünü belirlemektedir.

Algılanan öz-yeterlilik (self-efficacy): KMT bağlamında öz yeterlilik kişinin bir davranışı başarılı bir şekilde gerçekleştirme becerisine ilişkin inancı olarak tanımlanmaktadır (Maddux vd., 1982). Başa çıkma değerlendirmesi içinde ele alınan öz-yeterlilik ile bireyin tehdidi önlemeye yönelik kontrolleri gerçekleştirmesine olan inancı yüksek olduğunda koruma motivasyonu ve davranışının da artacağı varsayılır (Rogers, 1975) Gizlilik literatüründe ise öz yeterlilik, insanların internette gizliliklerini koruma konusunda kendi yeteneklerine olan inançları olarak tanımlanmaktadır (Ham, 2017; Boerman vd., 2018). Bu çalışmada öz-yeterlilik kişinin ÇDR'den kaçınmaya yönelik yeterliliklerine olan inançlarını ifade eder.

Örneğin LaRose vd. (2005) çalışmasında çevrimiçi güvenlik önlemlerini alabilme konusundaki öz-yeterliliğin bu önlemleri alma davranışını arttırdığını göstermiştir. Rifon vd. (2005) öz-yeterliği yüksek bireylerin kişisel bilgilerini bir web sitesine verme konusunda öz-yeterliği düşük olanlara göre daha az istekli olduklarını tespit etmişlerdir. Aynı şekilde Chai vd. (2009) çalışmalarında öz-yeterliliğin internette sınırlı bilgi paylaşımına yol açtığı sonucuna ulaşmıştır. Boerman vd. (2018) ise öz-yeterliliğin internette gizliliği koruma davranışları üzerinde etkisi olmadığını tespit etmiştir. Çalışmada tüketicinin çerezlere yönelik düşük bilgisinin öz-yeterliliklerinin de düşük olmasına etki edebileceği sonucuna varılmıştır.

Bazı çalışmalarda ise öz-yeterlilik ve koruma davranışı arasında gizlilik endişesi aracı değişken olarak ele alınmıştır. Youn (2009) ergenlerin gizliliği korumaya yönelik davranışları üzerinde yaptığı çalışmada öz yeterliliğin gizlilik endişesini etkilemediği sonucuna ulaşmıştır. Çalışmaya göre öz-yeterliliği yüksek olan bireylerin koruma davranışı gerçekleştirebileceklerine olan inançları yüksek olduğu için gizlilik endişeleri düşüktür. Mohamed ve Ahmad (2012) ise sosyal medyada gizliliği koruma motivasyonlarını inceledikleri çalışmada gizlilik endişesinin öz-yeterlilik ve koruma davranışı üzerinde aracılık etkisinin olduğunu bulmuştur. Bu çalışmaya göre kişilerin öz-yeterliliği arttıkça gizliliğe yönelik endişeleri de artacak ve koruma davranışı

gerçekleşecektir. Zhang vd. (2018) ise bilgi gizliliğini korumaya yönelik öz-yeterlilikleri yüksek olan bireylerin sağlık verileri bağlamında gizlilik endişelerinin düşük olduğu sonucuna varmıştır. Mousavi vd. (2020) sosyal medyada gizliliği koruma motivasyonlarını incelediği çalışmada gizlilik endişesinin tehdit ve başa çıkma değerlendirmesi arasında aracılık etkisinin olduğunu ortaya koymuştur. Çalışmaya göre tehdit değerlendirmesi yüksek olan kişiler gizlilik endişesine kapılırlar ve yüksek gizlilik endişesi öz-yeterlilik gibi başa çıkma değerlendirmelerine yönelik inançların düşük çıkmasına etki eder. Bu durum duygunun bilişi ön yargılı bir şekilde etkilediğini göstermektedir. Kişiler yüksek düzeyde endişe duyduklarında onla başa çıkamayacakları inancına kapılabilir. Ham (2017) ise ÇDR'ye yönelik ikna bilgisinin yüksek olduğu durumlarda öz-yeterliliğe yönelik inancında yüksek olduğu ve öz yeterliliğinde gizlilik endişesini pozitif yönde etkileyeceğini ileri sürer.

Çalışmalara bakıldığında öz-yeterliliğin koruma davranışına pozitif bir etkisi olduğu söylenebilir. Ancak gizlilik endişesi bağlamında öz-yeterlilik ve gizlilik endişesi arasındaki ilişkide farklı sonuçlar olduğu görülmektedir. Bu farklılıkların nedeni temelde kişilerin gizliliği korumaya yönelik algılarından ziyade gizliliğe yönelik bilgileri tarafından açıklanmaktadır. Kişinin teknik bilgisi öz-yeterlilik inancına da etki edebilir. Bu nedenle bu çalışmada öz-yeterliliğin tehdit değerlendirmesinin bir sonucu olan gizlilik endişesinin değil başa çıkma değerlendirmesi olarak ele alınan gizlilik kontrolünün bir öncülü olduğu düşünülmektedir.

Algılanan tepki yeterliliği (response efficacy): Tepki yeterliliği, bir tepkinin tehdidi etkili bir şekilde önleyip önlemediğine dair bireyin inancı olarak tanımlanır (Witte, 1992). KMT'ye göre insanların koruma davranışını gerçekleştirmeye motive olmaları için tepkilerinin etkili olduğuna inanmaları gerekmektedir. Birinci bölümde de bahsedildiği gibi ÇDR bağlamında tüketici verisinin kullanılmasından doğan endişeler hem hukuk alanında (örn: FTC, GDPR) hem de reklamcılık öz düzenlemeleri alanında (örn: DAA, IAB) tüketicilere belli kontrollerin verilmesiyle sonuçlanmıştır ancak, kullanıcıların bu araçları kullanarak izleme taktiklerini ve ÇDR'yi etkili bir şekilde kontrol edip edemediği hala belirsizdir (Cranor, 2012, s. 93).

Tepki yeterliliğine ait kontroller arasında tüketicinin çerezlerin kabulü için açık rıza, ÇDR için tanımlayıcı ikonların (AdChoices) oluşturulması, ÇDR sisteminden çıkmak için (örn: youronlinechoses) bazı yolların geliştirilmesi, internet tarayıcılarında üçüncü taraf çerezlerin takibini engelleyebilme (do not track) sekmelerinin yerleştirilmesi

yer almaktadır (Cranor, 2012). Ayrıca tüketicinin gizliliği korumak ve reklamları engellemek için çeşitli yazılımları (örn: Ghostery, Adblock) kullandığı bilinmektedir (Ikram ve Kaafar, 2017; vd., 2021).

KMT bağlamında tepki yeterliliği çok az çalışmada incelenmiştir (Boerman vd., 2018, s. 7). Önceki internet gizliliği ve güvenliğine yönelik çalışmalarda tepki yeterliliğinin, virüs koruma önlemlerinin alınmasında (Lee vd., 2008; Chenoweth vd., 2009), güçlü şifreler oluşturulmasında (Zhang ve McDowel, 2009), kablosuz ağ kullanıcılarının güvenlik önlemlerini uygulama kararlarında (Woon vd., 2005), bilgisayar yedekleme davranışlarında (Crossler, 2010) etkili olduğu doğrulanmıştır. Boerman vd. (2018) çevrimiçi gizliliği korumaya yönelik tepki yeterliliğinin koruma davranışlarını etkilediğini kanıtlamıştır.

ÇDR'den kaçınma bağlamında ise kişilerin hangi tepkileri verdiğinde gizliliklerini koruyacağı ve reklamdan kaçınacağı belirsiz olduğundan tepki yeterliliğini ölçmenin zor olacağı düşünülür (Smit vd., 2014; Ham, 2017). Strycharz vd. (2019) ise ÇDR sisteminden çıkma uygulamalarının reklamdan kaçınmada bir etki yaratmadığını ortaya koymuştur. Mohamed ve Ahmad (2012) ise sosyal medya kullanıcılarının gizlilik endişelerine yönelik yaptığı çalışmada tepki yeterliliğinin gizlilik endişesi üzerinde bir etkisi olmadığı sonucuna ulaşmıştır.

Çalışmalara bakıldığında tepki yeterliliğinin hem koruma davranışı hem de gizlilik endişesi üzerindeki etkilerine odaklanıldığı ve farklı bağlamlarda farklı sonuçlarla karşılaşıldığı görülmektedir. Bu çalışmada ise algılanan tepki yeterliliği, ÇDR bağlamında gizliliği korumaya yönelik kontrollerin (çerezleri reddetme, AdBlock kullanma, ÇDR sisteminde çıkma vb.) gizliliği korumada etkili olup olmadığına dair tüketici inançlarını ifade eder. Eğer algılanan tepki yeterliliği yüksekse gizlilik kontrolüne yönelik algılarında yüksek olacağı düşünülmektedir.

Algılanan tepki maliyeti (response cost): Tepki maliyeti, bir kullanıcının önerilen başa çıkma davranışını gerçekleştirmesi sırasında maruz kalacağı kayıplar/maliyetler olarak tanımlanır (Chenoweth vd., s. 4). ÇDR bağlamında tepki maliyeti, reklamdan kaçınma davranışının tüketiciye getireceği maliyetler şeklinde tanımlanmıştır. Bu çalışma açısından tepki maliyetleri, ÇDR'nin getirdiği faydalardan mahrum kalma, gizliliği koruma davranışının zaman alması ve zihinsel olarak yorucu olması olarak ifade edilir.

ÇDR tüketiciye ilgi alanına yönelik içerik ve reklam mesajları sunması bakımından bilgilendirici olarak görülmektedir (Ham, 2017). ÇDR'yi engelleme sonucunda tüketici

ilgi alanına yönelik reklamlar yerine daha ilgisiz reklamlar görmeye başlayacağından ÇDR'yi faydalı bularak tercih edebilmektedir. Bu durum reklamın etkisi üzerinde de etkili olmaktadır (De Keyzer vd., 2022).

Gizlilik kontrolü ve tepki yeterliliği başlığında da açıklandığı gibi tüketiciye gizliliklerini korumaları için belirli kontroller verilmiştir. Ancak bu kontroller tüketici açısından zor ve zaman alıcı olarak görülebilir. Önceki çalışmalar tüketicinin ÇDR sistemini anlamada zorlandığını kanıtlamıştır (McDonald ve Cranor, 2010a; Ur vd., 2012). Bu nedenle kişisel verilerin gizliliğini korumak, tüketici için karmaşık ve zahmetli bir süreç olarak ifade edilebilir. Üstelik kişisel verileri korumaya yönelik tepki yeterlilikleri belirli teknik bilgileri (çerezleri silme, gizlilik ayarlarını düzenleme, gizlilik için özel yazılımlar kullanma vb.) gerektirir (Nelson ve Ham, 2016; Boerman vd., 2018; Strycharz vd., 2019). Bu nedenle de korumaya yönelik davranışlar bazı tüketiciler için zihinsel bir çaba ve bu çabanın getireceği zorluklar olarak algılanabilir.

Ayrıca korumaya yönelik davranışlar tüketici için bir zaman alıcı faaliyet olarak ifade edilebilir. Örneğin önceki çalışmalar gizlilik politikalarının çok uzun olmasının tüketicilerin bu metinleri okumakta ve anlamlandırmakta zorlandığını göstermiştir (Cranor 2003; McDonald, vd., 2008; Milne ve Culnan 2004). Bu anlamda tüketicilerin gizliliğe yönelik bazı koruma davranışlarını gerçekleştirmesi bir zaman maliyeti yaratabilmektedir.

Bu tür maliyetler tüketicinin gizliliğe yönelik kontrolleri yerine getirmeyi zor ve karmaşık bir süreç olarak algılamasına neden olabilir. Bu nedenle ÇDR'ye yönelik tepki maliyetinin gizlilik kontrolü üzerinde olumsuz bir etki yaratacağı düşünülmektedir.

2.4.4. Koruma motivasyonu olarak ÇDR'den kaçınma niyeti

Literatürde ÇDR'ye yönelik kaçınma çalışmaları az olmakla birlikte çalışmalara bakıldığında bazı çalışmalar reklama yönelik tüketici algılarına (Beak ve Morimoto, 2012; Li ve Huang, 2016; Aiolfi vd., 2021) bazıları ikna bilgisi ve başa çıkma davranışlarına (Smit vd., 2014; Ham, 2017) bazılarının ise koruma motivasyonlarına (Strycharz vd., 2019; Cho vd., 2020) odaklandığı görülmektedir.

Beak ve Morimoto (2012) tarafından gerçekleştirilen çalışma, kişisel verilerin kullanımına yönelik (e-posta, doğrudan postalama ve sms) reklamlardan kaçınma üzerine yapılmış ilk çalışmalar arasında yer alır. Çalışmaya göre bu tür reklamlara yönelik

rahatsız edicilik, algılanan kişiselleştirme ve gizlik endişesi reklama yönelik şüpheye ve reklamdan kaçınmaya neden olmaktadır.

Li ve Huang (2016) ÇDR'den kaçınmayı etkileyen faktörleri araştırdıkları çalışmalarında hedef engeli, algılanan kişiselleştirme, olumsuz deneyim ve gizlilik endişesinin ÇDR'den kaçınmada etkili olduğunu ortaya koymuştur.

Aiolfi vd. (2021) ÇDR ye yönelik farklı algıların reklam kabulü ve reklamdan kaçınma üzerindeki etkisini incelemişlerdir. Çalışma ÇDR uygunluğu, güvenilirliği ve faydasının reklam kabulünde etkili olurken gizlilik endişesinin ise reklamdan kaçınmayı etkilediğini ifade eder.

İkna bilgisine odaklanan Smit vd. (2014), çalışmasında ÇDR'ye yönelik ikna bilgisinin gizlilik endişesi ve ÇDR ile başa çıkma tutumları üzerindeki etkisini incelemiştir. Çalışmada ikna bilgisi ÇDR'nin çalışma sistemi ve çerez bilgisi olarak iki boyutta ele alınmış ve tüketicilerin bilgi seviyeleri ölçülmüştür. İkna bilgisi yüksek olan grubun gizlilik endişesinin de düşük olduğunu ve daha az gizliliği koruma davranışlarını sergilediklerini açıklayan çalışma bunun daha az bir grubu ifade ettiğini göstermiştir. Tüketicilerin çoğu ÇDR taktiklerini anlamadığı için gizlilik endişesi duymakta ve bu reklamları istememektedir. Aynı şekilde Ham (2017) ÇDR'ye yönelik gizlilik endişeleri ve ÇDR'den kaçınma niyetlerini ikna bilgisi ve koruma motivasyonu teorileriyle inceler. ÇDR taktiklerine yönelik ikna bilgisi yüksekse hem algılanan risk hem de öz-yeterlilik yüksek olmaktadır. Tüketicinin koruma motivasyonlarına yönelik bu algıları ise gizlilik endişesini belirlemektedir ve gizlilik endişesi yüksek olan tüketicilerin reklamdan kaçınmaları da yüksektir.

Strycharz vd. (2019) ÇDR sisteminden çıkma (opt-out) davranışında etkili olan faktörleri koruma motivasyonu çerçevesinde incelemiştir. Sonuçlar, algılanan ciddiyetin ve tepki yeterliliğinin sistemden çıkma motivasyonunu artırdığını, kişiselleştirmeye yönelik olumlu tutumun ve algılanan öz yeterliliğin ise bunu azalttığını göstermektedir.

Cho vd. (2020) tüketicilerin Facebook reklamlarına yönelik başa çıkma taktiklerini araştırmıştır. Çalışmanın sonuçlarına göre tehdit ve başa çıkma değerlendirmeleri tüketicide öfke, endişe, korku gibi duyguları tetiklemekte ve bu duygular reklamdan kaçınma ve gizlilik önlemlerini etkinleştirme gibi başa çıkma davranışlarına (coping behavior) yol açmaktadır.

KMT bağlamında reklamdan kaçınma bireyin tehdit ve başa çıkma değerlendirmesinin bir sonucudur. Bu bağlamda gizlilik endişesi (tehdit değerlendirmesi)

ve gizlilik kontrolünün (başa çıkma değerlendirmesi) bir koruma motivasyonu olarak ÇDR'den kaçınmada etkili olduğu düşünülmektedir.

Gizliliğe yönelik önceki araştırmalar gizlilik endişesinin gizliliği korumaya yönelik davranışları arttırdığını göstermiştir (Turow vd., 2009; McDonald ve Cranor, 2010a; Ur vd., 2012; Smit vd., 2014; Moore vd, 2015; Phelan vd., 2016; Boerman vd., 2017; Ham, 2017; Boerman; 2018; Varnalı, 2021; Aiolfi vd., 2021; Zhang vd., 2023). Ayrıca internet (Li ve Huang, Ham, 2017; Strycharz vd., 2019; Aiolfi vd., 2021) ve sosyal medya (Kelly vd., 2021; Morimoto, 2021; Singaraju; vd., 2022) bağlamında gizlilik endişesinin hedefli reklamlardan kaçınma üzerindeki etkisi kanıtlanmıştır. Bu nedenle bu çalışmada da ÇDR'ye yönelik gizlilik endişesinin reklamdan kaçınmayı etkilediği düşünülmektedir.

KMT bağlamında ÇDR'den kaçınmayı etkilediği düşünülen bir diğer değişken ise gizlilik kontrolüdür. Reklamdan kaçınmanın önceki literatürü (tv reklamları) tüketiciye belirli kontroller sağlandığında reklamdan kaçındığını göstermiştir (örn: Moriarty ve Everett, 1994). ÇDR bağlamında ise kontrol, gizliliğe yönelik kontroller olarak ele alınmıştır. Bu sebeple algılanan gizlilik kontrolü kişisel verilerin kullanılması ve yayılması üzerindeki kontrolleri ifade etmektedir.

Bazı çalışmalarda algılanan kontrolün reklama yönelik olumsuz algıların önüne geçtiği ve bu nedenle reklamdan kaçınmayı azalttığı sonucuna ulaşılırken (Morimoto, 2021; Youn ve Kim, 2019b) bazı çalışmalarda ise kontrolün kaçınmayı pozitif yönde etkilediği sonucuna ulaşılmıştır (Wohn vd., 2015; Youn ve Kim, 2019a; Kelly vd., 2021).

Literatürde gizlilik kontrolü ve gizlilik endişesi ilişkisine bakıldığında, tüketicilere hangi bilgilerin toplandığı ve nasıl kullanıldığını açıklamak (örn; gizlilik politikaları ile); reklam çerezlerini kabul etmemek, ya da çerez sisteminden çıkmak gibi kontroller verildiğinde endişenin azalacağı düşünülür. Bu düşünce çalışmalarda algılanan kontrol ve gizlilik endişesi arasında negatif bir ilişkisi olduğu sonuçlarıyla desteklenmiştir (Xu vd., 2011; Dinev ve Hart, 2004; Morimoto, 2021). Reklam mecralarında gizlilik kontrollerinin belirginleştirilmesi sonucunda tüketicilerin yüksek bir gizlilik kontrolü algıladıklarını ve bunun sonucunda hedeflenen reklamı daha etkili, ikna edici ve güvenilir olarak değerlendirdiklerini bilinmektedir (Zarouali vd., 2018).

Bu sonuçlardan hareketle bu çalışmada algılanan gizlilik kontrolünün gizlilik endişesini azaltacağı ancak tüketicilerin koruma motivasyonları bağlamında gizlilik kontrollerini almaya daha yatkın olacaklarından algılanan gizlilik kontrolü ile ÇDR'den kaçınma arasında pozitif yönde bir ilişki olduğu varsayılmıştır. Kavramsal çerçevede

tartışılan tüm bu araştırmaların sonuçlarından hareketle tehdit değerlendirmesinin gizlilik endişesi üzerinde ve gizlilik endişesinin de reklamdan kaçınma üzerinde doğrudan etkilere sahip olduğu söylenebilir. Buna ek olarak gizlilik endişesinin tehdit değerlendirmesi ve reklamdan kaçınma üzerinde bir aracılık etkisine sahip olabileceğini de söylemek mümkündür. Ayrıca başa çıkma değerlendirmesinin gizlilik kontrolü üzerinde ve gizlilik kontrolünün de reklamdan kaçınma üzerinde doğrudan bir ilişkisi söz konusudur. Bu durumda gizlilik kontrolünün başa çıkma değerlendirmesi ve reklamdan kaçınma arasındaki ilişkide de aracılık rolünden bahsedilebilir.

3. YÖNTEM

Bu çalışmanın temel amacı, tüketicilerin ÇDR'den kaçınmasında etkili olan faktörlerin belirlenmesidir. ÇDR'den kaçınma konusu ise gizlilik endişesi bağlamında ele alınmış ve koruma motivasyonu teorisi çerçevesinde belirlenen faktörlerle incelenmiştir. ÇDR'den kaçınmada etkili olduğu düşünülen faktörler önerilen bir yapısal eşitlik modeli ile test edilmiştir. Bu amaç doğrultusunda bu bölümde öncelikle araştırmada kullanılan yöntemlere, kavramsal model ve hipotezlere ait bilgilere araştırma modeli başlığı altında yer verilmiştir. Daha sonra araştırmanın evren ve örneklem bilgisi ve veri toplama aracının belirlenmesini kapsayan ölçeklerin belirlenmesi, uzman paneli, pilot çalışma, öntestin sunulduğu geçerlik ve güvenirlik sonuçlarına değinilmiştir.

3.1. Araştırma Deseni

Bir araştırmanın kavramsal ve yöntemsel alt yapısı araştırmacının hangi araştırma felsefesini benimsediği ile derinden ilişkilidir. Sosyal bilimlerde araştırmalar genel anlamda pozitivist, yorumlayıcı, eleştirel, feminist ve postmodern olmak üzere beş farklı bilim felsefesine dayandırılabilir. Bu çalışmada bilim felsefesi olarak pozitivizm yaklaşımı belirlenmiştir. Pozitivist yaklaşım, doğa bilimlerine benzer şekilde sosyal bilimlerde de nedensellik ve genelleme kaygısı taşımaktadır. Genellikle niceliksel olarak kurgulanan deneysel ve tarama modellerini benimser ve hipotez testlerine dayanır (Neuman, 2017, s. 120). Araştırma felsefesinin benimsenmesi aynı zamanda araştırmada kullanılacak yöntem yaklaşımının da belirlenmesini ifade etmektedir.

Bir çalışmanın araştırma deseni ayrıca araştırmanın amacı bakımından ele alınan farklı yöntemlerden uygun olanın belirlenmesi ile ilişkilendirilir. Sosyal bilimler alanında yapılan çalışmalarda keşfedici, tanımlayıcı, açıklayıcı ve değerlendirici olmak üzere dört temel amaçtan söz edilebilir (Rubin ve Babbie, 2011, s. 133). Bu araştırma amacı bakımından açıklayıcı araştırma desenine sahiptir. Açıklayıcı araştırmalar, bir değişkendeki varyasyonun başka bir değişkendeki farklılıkları açıklamak için nasıl varsayıldığına dair geçici ifadeler olan hipotezlerin test edilmesini ifade eder (Rubin ve Babbie, 2011, s. 135). Kısacası açıklayıcı araştırmalar özellikle bir kuramsal alt yapıyla oluşturulan hipotezler arasındaki nedensellik ilişkilerinin test edilmesini amaçlamaktadır.

Sosyal bilimlerde araştırma yöntemleri en temelde nitel, nicel ve karma olmak üzere üç farklı araştırma yaklaşımına sahip olmaktadır. Nitel araştırma, bireylerin veya grupların sosyal veya insani bir soruna yükledikleri anlamı keşfetmeye ve anlamaya

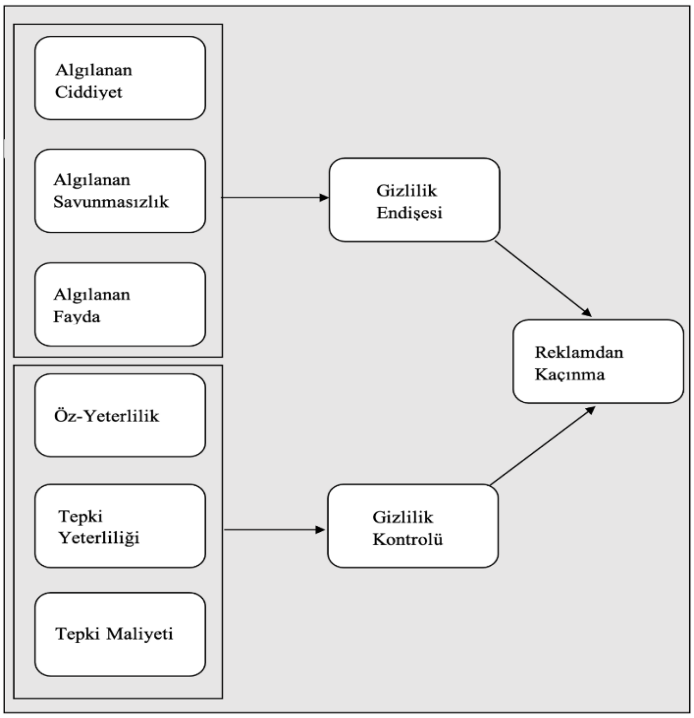
yönelik bir yaklaşımdır. Araştırma süreci, ortaya çıkan soruları ve prosedürleri, tipik olarak katılımcının ortamında toplanan verileri, ayrıntılardan genel temalara tümevarımsal olarak oluşturulan veri analizini ve araştırmacının verilerin anlamına ilişkin yorumlar yapmasını içerir. Nitel araştırmalar en geniş ifadeyle bir araştırma sorusunun herhangi bir hipotez ve istatistiksel test kullanmadan cevaplandığı araştırma tasarımını tanımlamaktadır. Pozitivist araştırma felsefesinde sıklıkla kullanılan nicel araştırmalar ise araştırma sorusunda hipotez testlerini ve istatistiki testleri kullanan araştırmalardır. Nicel araştırma, değişkenler arasındaki ilişkiyi inceleyerek nesnel teorileri test etmeye yönelik bir yaklaşımdır. Bu değişkenler de tipik olarak belirli araçlarla (örn: anket) ölçülebilir, böylece numaralandırılmış veriler istatistiksel prosedürler kullanılarak analiz edilebilir. Nicel araştırmalar, teorileri tümdengelimli olarak test etme, önyargıya karşı koruma oluşturma, alternatif açıklamaları kontrol etme ve bulguları genelleştirip tekrarlayabilme konusunda varsayımları içermektedir. (Creswell, 2014). Bu araştırmada nicel araştırma yöntemi benimsenmiştir. Literatürde farklı sınıflandırmalar olmasına rağmen nicel araştırma yönteminin, tarama modelleri ve deneysel araştırmalar olmak üzere iki temel araştırma modelinden oluştuğu söylenebilir. Bu çalışmada kullanılan araştırma modeli tarama modellerinden ilişkisel tarama modelidir. Tarama modeli bir araştırma evreni hakkında yargıya varabilmek için evrenin tamamına ya da evrenden alınan bir grup örneklem üzerinde yapılan araştırmalardır. İlişkisel tarama ise iki veya daha çok değişken arasında birlikte değişimi ya da değişimin derecesini belirlemeyi amaçlayan araştırma modelidir (Karasar, 2003, s. 81).

Sosyal bilimlerde araştırmalar ayrıca süreleri bakımından kesitsel ve boylamsal araştırmalar olarak ikiye ayrılmaktadır. Verilerin belirli bir sürede toplanıp bitirildiği araştırmalar kesitsel, verilerin bir süre boyunca farklı zamanlarda toplanıldığı araştırmalar ise boylamsal araştırma olarak ifade edilmektedir (Gürbüz ve Şahin, 2018, s. 113). Bu çalışmada veriler tek bir zamanda toplandığından araştırma süresi bakımından kesitsel bir araştırmadır. Araştırmanın desenini oluşturan araştırma yaklaşımları sırayla amaç bakımından açıklayıcı, yöntem bakımından nicel araştırma yöntemi olan ilişkisel tarama, süre bakımından ise kesitsel bir araştırmadır.

3.2. Araştırma Modeli ve Hipotezler

Bu çalışmada ÇDR'den kaçınma niyeti KMT üzerinden açıklanarak bir model geliştirilmiş ve bu modelin test edilmesi amaçlanmıştır. Geliştirilen kavramsal model

tüketicinin ÇDR'ye yönelik tehdit ve başa çıkma değerlendirmeleri, gizlilik endişesi ve gizlilik kontrolü algıları ve reklamdan kaçınma niyetlerinin ölçüldüğü üç yapıyı içermektedir. Bu yapılar içerisinde belirlenen değişkenler ve bu değişkenler arasındaki ilişkilerin gösterildiği kavramsal model Şekil 3.1'de gösterilmektedir.



Şekil 3.1. *Araştırmanın kavramsal modeli*

Araştırma modelinde görüldüğü gibi tüketicinin tehdide yönelik değerlendirmeleri; algılanan ciddiyet, algılanan savunmasızlık ve algılanan fayda olarak üç boyutta ele alınmaktadır. Başa çıkma değerlendirmeleri de yine öz-yeterlilik, tepki yeterliliği ve tepki maliyeti olarak üç boyuttan meydana gelmektedir. Bunun dışında gizlilik endişesi, gizlilik kontrolü ve reklamdan kaçınma niyeti olarak üç diğer değişkenin var olduğu modelde bu değişkenler arasında ilişkileri ifade eden 20 farklı hipotez kurulmuştur. Araştırma hipotezleri aşağıda açıklanmaktadır.

- H1 Algılanan ciddiyet ve gizlilik endişesi arasında pozitif bir ilişki vardır.
- H2 Algılanan savunmasızlık ve gizlilik endişesi arasında pozitif bir ilişki vardır.
- H3 Algılanan fayda ve gizlilik endişesi arasında negatif bir ilişki vardır.
- H4 Öz yeterlilik ve gizlilik kontrolü arasında pozitif bir ilişki vardır.
- H5 Tepki yeterliliği ve gizlilik kontrolü arasında pozitif bir ilişki vardır.
- H6 Tepki maliyeti ve gizlilik kontrolü arasında negatif bir ilişki vardır.

- H7 Gizlilik endişesi ve reklamdan kaçınma arasında pozitif bir ilişki vardır.
- H8 Gizlilik kontrolü ve reklamdan kaçınma arasında pozitif bir ilişki vardır.
- H9 Algılanan ciddiyet ve reklamdan kaçınma arasında pozitif bir ilişki vardır.
- H10 Algılanan savunmasızlık ve reklamdan kaçınma arasında pozitif bir ilişki vardır.
- H11 Algılanan fayda ve reklamdan kaçınma arasında negatif bir ilişki vardır.
- H12 Öz yeterlilik ve reklamdan kaçınma arasında pozitif bir ilişki vardır.
- H13 Tepki yeterliliği ve reklamdan kaçınma arasında pozitif bir ilişki vardır.
- H14 Tepki maliyeti ve reklamdan kaçınma arasında negatif bir ilişki vardır.
- H15 Algılanan ciddiyet ve reklamdan kaçınma arasındaki ilişkide gizlilik endişesinin aracılık rolü vardır.
- H16 Algılanan savunmasızlık ve reklamdan kaçınma arasındaki ilişkide gizlilik endişesinin aracılık rolü vardır.
- H17 Algılanan fayda ve reklamdan kaçınma arasındaki ilişkide gizlilik endişesinin aracılık rolü vardır.
- H18 Öz yeterlilik ve reklamdan kaçınma arasındaki ilişkide gizlilik kontrolünün aracılık rolü vardır.
- H19 Tepki yeterliliği ve reklamdan kaçınma arasındaki ilişkide gizlilik kontrolünün aracılık rolü vardır.
- H20 Tepki maliyeti ve reklamdan kaçınma arasındaki ilişkide gizlilik kontrolünün aracılık rolü vardır.

3.3. Araştırma Kümesi

Bilimsel çalışmalarda örnekleme yöntemleri olasılıklı örnekleme ve olasılıklı olmayan örnekleme olarak ikiye ayrılmaktadır. Olasılıklı örnekleme çalışma evreninin belli olduğu durumlarda her bir bireyin araştırmaya dâhil edilmesinde eşit şansa sahip olmasını ifade etmektedir. Bu ise örneklemin evreni temsil etme gücünü arttırarak evren genellemesi yapmaya imkân tanır. Bu tür avantajlarının olmasına rağmen sosyal bilimlerde her zaman olasılıklı örneklem kullanılması zordur. Bunun temel nedenlerinden biri çalışma evreninin sınırlarının çizilmesindeki zorluk ya da evrenin geniş olduğu durumlarda herkese eşit şans verilmesinin imkânsızlaşması ile ilişkilendirilir. Bu

durumda çalışmacı olasılıklı olmayan örneklem yöntemlerini seçebilir (Rubin ve Babbie, 2011, s. 335-359).

Bu çalışmanın araştırma kümesini 18 yaş üstü internet kullanıcıları oluşturmaktadır. Çalışma evreninin çok geniş olması evrenin tamamına ulaşma ve evrenden seçilecek örneklemde herkese eşit şans verme olasılığını zorlaştırmaktadır. Bu sebeple bu çalışmada olasılıklı olmayan örnekleme yöntemlerinden kolayla örneklem tercih edilmiştir. Kolayda örnekleme tekniğinde temel nokta, ulaşılabilen herkesin araştırmaya dâhil edilmesidir (Altunışık vd., 2012, s. 142). Bu örnekleme türü, evren genellemesine imkân tanımamaktadır (Cohen, vd., 2000). Fakat kolayda örnekleme; kolay, hızlı ve ekonomik bir şekilde katılımcılara ulaşmayı sağladığından (Malhotra ve Dash, 2016) sosyal bilimler araştırmalarında çoğunlukla tercih edilmektedir.

Çalışmaya dâhil edilecek örneklem sayısının büyüklüğünü belirlemede araştırmada kullanılan istatistiksel yöntemler önemli olmaktadır. Bu çalışmada 9 gizil değişken arasındaki ilişkiyi ölçmek üzere bir kavramsal model geliştirilmiştir. Bu model testi için ise YEM analizi kullanılmıştır. YEM, terimi tek bir istatistiksel tekniği tanımlamak yerine bir dizi ilişkili işlemler dizisine işaret etmektedir (Kline, 2019, s. 9). YEM, sürekli ya da süreksiz ve bir ya da daha fazla bağımsız değişken ile sürekli ya da süreksiz bir ya da daha fazla bağımlı değişken arasındaki ilişkiyi test eden istatistiksel teknikler topluluğu olarak tanımlanabilir (Ullman, 2015, s. 681). YEM, bazı olgulara dayanan yapısal bir teorinin analizine doğrulayıcı bir yaklaşım getiren istatistiksel bir metodolojidir (Byrne, 2016, s. 3).

YEM analizinde örneklem büyüklüğünün belirlenmesinde literatürde farklı bakış açıları söz konusudur. Kline (2019, s. 15) örneklem büyüklüğünün çalışmadaki YEM modelinin türüne ve karmaşıklığına, ölçekte yer alan değişken ve madde sayılarına, değişkenlerin türüne (sürekli, nominal vb.) ölçeğin normal dağılım gösterip göstermediğine ve kayıp veri ihtimaline göre değişebileceğini belirtir. Tüm bu etkiler göz önüne alınmakla beraber bir YEM analizi için ortalama 100 ile 200 gibi bir örneklemin gerekli olduğu söylenebilir. Tabachnick ve Fidell (2015, s. 618) örneklem büyüklüğünün çalışmalardaki değişken ve faktör sayısına göre değişebileceğini ancak düşük ortak varyans, az sayıda faktör ve her bir faktörün sadece üç veya dört göstergesi olduğu durumlarda faktör analizi için en az 300 katılımcının analize dâhil edilmesi gerektiğini ifade eder.

Bu genel görüşlerin dışında örneklem hesaplama için genel olarak temel kuralın, ölçekte yer alan ifade başına en az 10 katılımcının araştırmaya dâhil edilmesi olduğu söylenebilir (Field, 2009, s.647). Hair vd., (2019) ise farklı modellere göre örneklem büyüklüğünün belirlenmesi için bazı ölçütler sunmaktadır. Bu ölçütlere göre yedi veya daha fazla örtük değişkene sahip, bazı örtük değişkenlerde gözlenen değişkenlerin sayısı üçten az ve faktör yüklerinin bir kısmı 0.05'ten düşük olduğu modeller için en az 500 örneklem büyüklüğü önermektedir.

Çalışmada 9 örtük değişken ve kullanılan ölçeklerde toplam 42 ifade yer almaktadır. Madde çarpı 10 oranı ile (Field, 2009, s.647) çalışmada en az 420 örnekleme ulaşılması ideal görünmektedir. Ayrıca örtük değişken ve gözlenen değişken sayısı ile 500 örneklem sayısına ulaşmanın (Hair, 2019, s. 633) bu çalışmada YEM analizi için daha etkili olduğu söylenebilir. Bu bilgiler ışığında en az 500 örneklem sayısına ulaşmak hedeflenmiştir.

3.4. Ölçüm Araçlarının Geliştirilmesi

Çalışmada kullanılan ölçekler, literatürde daha önceden yapılmış, güvenirliği ve geçerliği yine aynı çalışmalarda test edilmiş olan araştırmalardan elde edilmiştir. Bu araştırmalar içerisinde öncelikle KMT bağlamında ÇDR'ye yönelik gizlilik endişesi ve reklamdan kaçınmanın incelendiği çalışmalardan yararlanılmıştır. Bu bağlamda çalışmanın kavramsal çerçevesinde açıklanan 9 farklı gizil değişken belirlenmiştir. Bu değişkenlere ait ölçeklerden üç faktörlü Tehdit Değerlendirmesi Ölçeği Ham, (2017) ve Boerman vd., (2018); yine üç faktörlü Başa Çıkma Değerlendirmesi Ölçeği Ham (2017), Boerman vd., (2018), Crossler, (2010); Gizlilik Endişesi Ölçeği Aiolfi vd., (2021); Gizlilik Kontrolü Ölçeği Kelly vd., (2021); Reklamdan Kaçınma Ölçeği Beak ve Morimoto (2012) tarafından yapılan çalışmalardan alınarak ifadeler çalışmaya uygun bir şekilde uyarlanmıştır.

Orijinal çalışmalardaki ölçeklerin çoğunda 5'li Likert tasarımı kullanıldığı için bu çalışmada da anket tasarımı 1. Kesinlikle Katılmıyorum … 5. Kesinlikle Katılıyorum şeklinde 5'li Likert yapıda hazırlanmıştır.

Ölçeklerin orijinal ifadesi İngilizce olduğundan çeviri işlemi gerçekleştirilmiştir. Ölçeklerin Türkçeye uyarlanması sürecinde; orijinal ölçekler, 1 dil uzmanı 1 alan uzmanı ve araştırmacının kendisi olmak üzere üç uzman tarafından çevrilme yöntemi izlenmiştir (Coster ve Mancini, 2015, s. 52). Elde edilen çeviriler üç uzmanın bir araya gelmesiyle

değerlendirilmiş ve farklılıklar üzerine uzlaşı yoluna gidilerek ilk taslak çeviri ölçek elde edilmiştir.

Ölçekler belirlendikten sonra ölçeklerin son hali için sırasıyla uzman görüşü, pilot çalışma ve ana çalışma öncesi ön-test işlemleri gerçekleştirilmiştir.

3.4.1. Uzman görüşü ve pilot çalışma

İlk taslak çeviri ölçeğin hem anlaşılırlığını test etmek hem de kapsam geçerlik oranını değerlendirilmek üzere 5 alan uzmanına (2 Profesör Dr., 2 Dr. Öğr. Üyesi 1 Dr.) 3 dereceli uzman form ile ölçek iletilmiştir. Yine eş zamanlı olarak ölçek ifadelerinin anlaşılırlığını test etmek için öğrenciler üzerinde pilot uygulama (*N*=50) gerçekleştirilmiş olup, ifadelerin anlaşılırlığına yönelik katılımcı görüşleri yüz yüze toplanmıştır. Hem uzman görüşleri hem de pilot çalışmada yüz yüze alınan geribildirimler sonucunda ilk çeviri taslak ölçekte anlaşılmayan ve problemli olduğu ifade edilen iki temel unsur ortaya çıkmıştır.

Bu unsurlardan ilki ölçek ifadelerinde yer alan *kişisel davranışsal veri* (personal behavioral data) ifadesi ve ÇDR kısaltmasının okumayı ve anlaşılırlığı zorlaştırdığıdır. İkincisi ise algılanan fayda ölçeğinde yer alan *sosyal imaj* ifadesinin anlaşılır olmadığı üzerinedir. Problemlerin tespiti araştırmacıyı taslak form üzerinde düzeltme yapmaya yönlendirmiştir. Uzman tavsiyeleri üzerine kişisel davranışsal veri ifadesi yerine kişisel veri ifadesinin kullanılmasına karar verilmiştir. Uzman görüşleri tarafından ayrıca çevrimiçi davranışsal reklamcılık ifadesinin de uzun ve okumayı zorlaştıran bir ifade olduğundan yerine daha anlaşılır bir kelime grubunun kullanılması tavsiye edilmiştir. Bunun üzerine ÇDR kısaltması ya da çevrimiçi davranışsal reklamcılık ifadesi yerine hedefli reklam ifadesinin kullanılmasına karar verilmiştir. Son olarak algılanan fayda ölçeğinde yer alan "*.....sosyal imajımı geliştiririm"* ifadesinin ölçekten çıkarılmasına karar verilmiştir.

Yapılan değişikliklerin ardından çevrilen taslak ölçek için tekrar uzman görüşü almak ve düzenlenen ölçek kapsam ve görünüş geçerliğini test etmek için aynı 5 alan uzmanına iletilmiştir. Uzman değerlendirilmesi sonucunda düzenlenen ölçekte herhangi bir problem olmadığı ve ölçeğin kapsam geçerlik oranı (KGO) değerinin kabul edilebilir değerde olduğu (.99) tespit edilmiştir (Veneziano ve Hooper, 1997).

Ayrıca ifadelerin anlaşılırlığını yeniden değerlendirmek üzere ölçek tekrar değerlendirmeye sunulmuştur. Farklı yaş ve meslek gruplarını içeren N=20 (Tablo 3.1.)

kişiye ulaşılmış ve ölçeğin anlaşılır olduğuna dair tekrarlı geri bildirimler alındığından görüşmeler sonlandırılmıştır.

Tablo 3.1. *Pilot çalışma araştırma kümesi bilgisi*

Yaş	Meslek	Eğitim	Kişi Sayısı
18-24	Öğrenci	Öğrenci	5
25-45	Kamu ve özel sektör çalışanı	Lisans ve lisansüstü	10
35-45	Çalışan (işçi vb.)	Lise	5

Ölçeğin anlaşılırlığı için yapılan pilot çalışmalar ve uzman görüşleri sonucunda hazırlanan taslak form için ayrıca ana çalışmadan önce bir ön test analizi gerçekleştirilmiştir

3.4.2. Ön test geçerlik ve güvenirlik analizleri

Yapısal eşitlik analizinden önce çalışmanın geçerlik ve güvenirliğini görmek için ön test uygulaması yapılmıştır. Ön test çalışmasında güvenilirlik için Cronbach Alfa analizinden yararlanılmıştır. Ölçeklerin geçerliği için ise faktör analizi yapılmıştır. Literatürde açımlayıcı ve doğrulayıcı olmak üzere iki tür faktör analizi mevcuttur. Açımlayıcı Faktör Analizi (AFA), teori üretmek ve yapının içerisinde var olan; fakat bilinmeyen temel boyutlar keşfedilmek istendiğinde gerçekleştirilen bir yöntemdir. Doğrulayıcı Faktör Analizi (DFA) ise önceki çalışmalara veya ilgili teoriye dayanarak belirlenen değişkenlerin birbiri ile olan ilişkisinin test edilmesinde kullanılan bir yöntemdir (Kline, 1994, s. 7-10). Önceden de açıklandığı gibi YEM analizleri bir kuramsal at yapıya dayalı ve bu kuramdan hareketle gerçekleştirilen modelin doğrulanmasına imkân sağlamaktadır (Byrne, 2016, s. 3). Bu doğrultuda çalışma önceden belirlenmiş bir kuramsal alt yapıya dayandığı için DFA yapılması uygun görülmüştür. Ön test için iki hafta sürede veri toplanmıştır. Toplamda 150 anket elde edilmiştir. Kayıp ve tekrarlanan veriler çıkarıldığında ise 139 veri üzerinden analizler gerçekleştirilmiştir.

Güvenilirlik analizlerinden en çok kullanılanlardan biri Cronbach Alfa katsayısıdır. Bu katsayı 0-1 arasında değişir ve katsayı 1'e yaklaştıkça güvenirliliğin yüksek olduğu sonucuna varılmaktadır (İslamoğlu, 2011, s. 134). Alfa katsayısı olarak da bilinen bu yöntemde kabul edilen güvenilir değerin 0.70 ile 1 arasında olması beklenmektedir (Altunışık vd., 2010). Bu doğrultuda 139 kişi ile yapılan ön test uygulamasında ölçeğin

güvenirliliğini belirmek için Cronbach Alfa katsayıları hesaplanmıştır. Yapılan analiz sonuçlarına göre tepki maliyeti ölçeğinin dışında tüm ölçeklerin alfa katsayılarının .70'den büyük olduğu görülmüştür. Tepki maliyeti ölçeğinin alfa kat sayısı .51 madde atıldığındaki alfa kat sayısı .66 olarak belirlenmiştir. Alfa katsayıları .40 altındaki ölçekler güvenilir bulunmazken .40 ve .60 arasındaki ölçekler ise düşük güvenirlilik olarak kabul görmektedir (Karagöz, 2019). Bu nedenle tüm ölçeklerin güvenilir olduğu kabul edilmiştir.

Güvenirlik analizi sonrası geçerlilik için DFA analizi yapılmıştır. Ölçeklerin DFA analizine uygunluğu için de Kaiser-Meyer-Olkin (KMO) örneklem yeterliliği ve Bartlett Küresellik Testi yapılmıştır. Kaiser-Meyer-Olkin (KMO) değerinin 0,60 ve üstünde olması örneklemin faktör analizi için yeterli olduğunu göstermektedir (Tabachnick ve Fidell, 2015). Bartlett küresellik testinin $p<0,05$ olması değişkenler arası ilişkilerin oluşturduğu matrisin faktör analizi için anlamlı olduğunu ve faktör analizi yapılabileceği anlamına gelmektedir (Gürbüz ve Şahin, 2018: 319). Test sonuçları tüm ölçeklerin KMO değeri 0.70 üstündedir. Bartlett küresellik testinin sonuçları ise 0,05 düzeyinde anlamlı ($p=000 <0.05$) olarak belirlenmiştir. Bu sonuçlar bize verilerin faktör analizi için uygun olduğunu göstermektedir. Son olarak DFA analizinden önce ölçeklerin normal dağılımına bakılmıştır. Normal dağılım için literatürde çarpıklık ve basıklık değerinin +1 -1 ya da +2 -2 arasında olması gerektiği ifade edilir (George ve Mallery, 2016). Normallik testi sonucunda ölçeklerin tamamı +1 ve -1 arasında bir değerde bulunmuştur. Normallik varsayımı sağlandığı için DFA analizine geçilmiştir.

3 alt boyut ve toplam 13 maddeden oluşan algılanan tehdit ölçeğinin birinci düzey üç faktörlü yapısı DFA ile test edilmiştir. İncelenen yapıda algılanan ciddiyet için 4, algılanan savunmasızlık için 4 ve algılanan fayda için 5 madde ölçekte yer almaktadır. Araştırma kapsamında yapılan DFA analizi sonucunda elde edilen değerler CMIN: 120,467, DF:62, p=,000, CMIN/DF= 1,943, RMSEA=0,08; SRMR=0,05; GFI=,887; CFI=,931 olarak belirlenmiştir. Elde edilen uyum iyiliği değerleri literatürde kabul edilen düzeydedir.

3 alt boyut ve toplam 16 maddeden oluşan başa çıkma ölçeğinin birinci düzey üç faktörlü yapısı DFA analizi ile test edilmiştir. İncelenen yapıda öz yeterlilik için 4, tepki yeterliliği için 9 ve maliyet için 3 madde ölçekte yer almaktadır.

Araştırma kapsamında yapılan DFA analizi sonucunda elde edilen değerler CMIN: 223,825; DF:101; p=,000; CMIN/DF=2,216; RMSEA=0,09; SRMR=0,08; GFI=,839;

CFI=,846 olarak belirlenmiştir. Bazı değerlerin istenilen uyum indekslerini karşılamaması ve p değerlerinin anlamsız olması nedeniyle faktör yükleri düşük olan MA1 ve TY9 maddeleri analizden çıkarılarak model yeniden test edilmiştir. Analiz sonucunda CMIN: 199,191; DF:74; p=,000; CMIN/DF=2,692; RMSEA=0,111; SRMR=0,843; GFI=,836; CFI=,843 bulunmuştur. Tekrarlanan test sonuçlarında bazı uyum indeksleri karşılanmadığından önerilen modifikasyon işlemlerinin yapılmasına karar verilmiş böylece TY2-TY3; TY4-TY5 ve TY6-TY7 maddelerine kovaryans atılmıştır. Analiz sonucunda CMIN:143,641, DF:71, p=,000, CMIN/DF=2,023; RMSEA=0,086; SRMR=0,070; GFI=,871; CFI=,909 sonucuna ulaşılmıştır. Uyum indeksleri istenilen düzeydedir.

Tek boyutlu ve 5 maddeli gizlilik endişesi ölçeği için DFA analizi yapılmıştır. DFA analizi sonucunda elde edilen değerler CMIN: 56,015, DF:5, p=,000, CMIN/DF=11,203, RMSEA=0,27; SRMR=0,04; GFI=,853; CFI=,903 olarak belirlenmiştir. Araştırma sonuçlarına göre istenilen uyum indekslerinin karşılanmadığı görülmüştür. Bunun üzerine modelde önerilen şekliyle GE4-GE5 maddelerinin arasına kovaryans bağlantısı çizilerek analiz tekrar edilmiştir. Bunun sonucunda elde edilen değerler CMIN:3,135, DF:4, p=,000, CMIN/DF= 0,784, RMSEA=0; SRMR=0,01; GFI=,99; CFI=,1 sonuçlarına ulaşılmıştır. Sonuçlar istenilen uyum değerlerindedir.

3 ifadeli gizlilik kontrolü ölçeği için DFA analizi yapılmıştır. Bu ölçek 3 ifadeden oluşan tek bir ölçek olduğu için uyum değerleri hesaplanamamıştır. Çünkü uyum değerlerinin hesaplanabilmesi için ölçeğin en az 4 ifadeden oluşması gerekmektedir. Bu bağlamda sadece faktör yükleri kontrol edilmiştir (Çelik ve Yılmaz, 2016, s. 58).

5 maddeden oluşan reklamdan kaçınma ölçeği için DFA analizi yapılmıştır. DFA analizi sonucunda elde edilen değerler CMIN:0,78, DF:4, p=,000, CMIN/DF=0,195, RMSEA=0,09; SRMR=0,04; GFI=,99; CFI=1 olarak belirlenmiştir. Araştırma sonuçlarına göre istenilen uyum indekslerinin karşılanmadığı görülmüştür. Bunun üzerine modelde önerilen şekliyle RK1-RK2 maddelerinin arasına kovaryans bağlantısı çizilerek analiz tekrar edilmiştir. Bunun sonucunda elde edilen değerler CMIN:3,135, DF:4, p=,000, CMIN/DF=0,784, RMSEA=0; SRMR=0,01; GFI=,99; CFI=,1 sonuçlarına ulaşılmıştır. Sonuçlar istenilen uyum değerlerindedir.

Ölçek ifadelerinde yer alan faktör yükleri .40 ve üzeri anlamlı kabul edilmektedir (Hair vd., 2019). Analiz sonuçlarına göre iki ifade dışında tüm faktör yükleri kabul edilir

seviyededir. Yapılan DFA analizi sonuçlarına göre ana çalışmaya geçmeden önce aşağıda sıralanan değişiklikler gerçekleştirilmiştir:

- Faktör yükü kabul edilebilir seviyenin altında olan MA1 *"Hedefli reklamlar kullanan şirketlerin kişisel verilerime ulaşmasına izin vermemek, bana daha uygun içeriklerden mahrum kalmama neden olur"* maddesi daha anlaşılır olması açısından "*Hedefli reklamlardan kaçınırsam ilgilendiğim ürün/hizmet reklamlarıyla daha az karşılaşırım"* şeklinde yeniden düzenlenmiştir.
- Faktör yükü kabul edilebilir seviyenin altında olan olan TY9 örneklem büyüklüğünden etkilenme ihtimaline karşı ifadesinin ana çalışma için tutulmasına karar verilmiştir.
- Faktör yükü düşük olan (0.44) AS4 *Kişisel verilerimin bilgim dışında bilinmeyen şirketler tarafından kullanılacağını düşünüyorum* ifadesinin daha anlaşılır olması için *Kişisel verilerimin bilmediğim şirketlerle izinsiz paylaşılacağını düşünüyorum* şeklinde yeniden düzenlenmesine karar verilmiştir.

3.5. Verilerin Toplanması ve Analizi

Ek-1'de yer alan ölçeklerin son hali belirlendikten sonra ana çalışma için verilerin toplanması aşamasına geçilmiştir. Verilerin toplanması 25 Nisan 2023 - 25 Haziran 2023 tarihleri arasında Google Formlar üzerinden çevrimiçi olarak gerçekleştirilmiştir. Veri toplama işlemi anketlere son bir hafta içerisinde yanıt gelmediği sürede sonlandırılmıştır. Bu süre sonunda 704 kişi araştırmaya katılım göstermiştir. Bu örneklem sayısı YEM analizi için önerilen büyüklüğe uygun bulunmuştur.

Verilerin analiz sürecindeki testler için IBM SPSS 24, IBM SPSS Amos 24 ve 'lavaan' paketi üzerinden işlem gerçekleştiren JASP programlarından yararlanılmıştır. Çalışma içerisinde katılımcılardan elde edilen verilerin YEM analizine uygunluğunu kontrol etmek için öncelikle kayıp veri kontrolü gerçekleştirilmiş, uç değerler ve verilerin normal dağılım sınırları içerisinde olup olmadığı tespit edilmiştir. Ardından tek değişkenli ve çok değişkenli normallik, doğrusallık, çoklu doğrusallık ve eşvaryanslılık varyasımlarının kontrolü gerçekleştirilmiştir. Devamında DFA gerçekleştirilerek ölçeklerin uyum indeksleri hesaplanmış, geçerlikleri ve güvenirlikleri sınanmıştır. Son olarak da DFA modelinin geçerliği sınanmış, araştırma modelinin uyum indeksleri hesaplanmış ve hipotez testleri gerçekleştirilmiştir. Bu işlemlere ve sonuçlara ait bulgular çalışmanın devamında sunulmuştur.

4. BULGULAR

4.1. Verilerin İncelenmesi

Çalışmada herhangi bir analiz gerçekleştirilmeden önce 704 katılımcıdan elde edilen veriler içerisinde herhangi bir kayıp verinin olup olmadığına bakılmış ve herhangi bir kayıp verinin olmadığı tespit edilmiştir. Daha sonra verilerde yer alan uç değerleri tespit edebilmek için ölçeklerde yer alan maddelerin kritik ki-kare değeri ve Mahalanobis uzaklığı hesaplanmıştır (Karagöz, 2019, s. 378). Mahalanobis uzaklığına ilişkin sonuçlarda kritik ki-kare değerlerini ($p<0,001$) aşan verilerin kesme noktası 26,125 olarak belirlenmiştir. Araştırma kümesi içerisinde yer alan 10 katılımcının bu kesme noktasından yukarıda bir değere sahip olduğu görülmüş ve bu katılımcılar araştırmadan çıkarılmıştır. Çalışmaya 694 katılımcı ile devam edilmiş ve öncelikle betimsel analizler gerçekleştirilmiştir.

Betimsel istatisikler değerlendirildiğinde örneklemin % 69,5'i kadın (482 kişi), 30,5'i erkek (212 kişi) katılımcılardan oluşmaktadır. Katılımcıların yaş gruplarına göre dağılımı, % 26,9'u 18-24 yaş (187 kişi), % 26,2'si 25-34 yaş (182 kişi), % 30,1'i 35-44 yaş (209 kişi), % 13,5'i, 45-54 yaş (94 kişi), % 3,2'si 55 yaş ve üzeri (22 kişi) yaş aralığında yer almaktadır. Katılımlımcıların eğitim durumları ise % 52,4'ü lisans (364 kişi), % 25,9'u lisansüstü (180 kişi), % 12'si, önlisans (83 kişi) son olarak % 9i7'si lise mezunu (67 kişi) şeklinde dağılım göstermiştir.

4.2. Normallik Testi

YEM modelini test edebilmek için bazı varsayımların doğrulanmış olması gerekir. Bunlardan biri verilerin normal dağılım sağlamasıdır. Çok değişkenli analizlerin hemen hepsinde sürekli değişkenlerin normalliğe sahip olup olmadığını kontrol etmek ilk önemli adımlardan birisidir. Normallik varsayımı tek değişkenli ve çok değişkenli normallik olmak üzere iki başlıkta incelenebilir. Tek değişkenli normallik, veri setindeki her bir değişkene yönelik verilerin normal dağılım göstermesi durumu olarak tanımlanır. Çok değişkenli normallik ise verilerin ve değişkenlerin tüm kombinasyonları açısından normal dağılım göstermesini ifade etmektedir (Çokluk vd., 2016, s. 15-16).

Tek değişkenli normal dağılım, istatistiksel ve grafiksel olarak farklı yöntemlerle kontrol edilebilir. Ancak en çok kullanılan yöntem çarpıklık ve basıklık değerlerinin kontrolüdür (Tabachnick ve Fidell, 2015, s. 79). Bu nedenle de çalışmada tek değişkenli normallik için her bir madde özelinde çarpıklık ve basıklık değerlerinin kontrolü

gerçekleştirilmiştir. Tablo 4.1'de veri setindeki tüm maddeler için basıklık ve çarpıklık değerleri gösterilmektedir.

Tablo 4.1. *Gözlenen değişkenlerin çarpıklık ve basıklık değerleri*

Değişken	Maddeler	Çarpıklık	Basıklık
Algılanan Ciddiyet (ALC)	**AC1**	-1,192	0,691
	AC2	-1,438	1,343
	AC3	-1,627	1,824
	AC4	-1,374	1,207
Algılanan Savunmasızlık (ALS)	**AS1**	-1,108	0,439
	AS2	-0,723	-0,284
	AS3	-0,767	-0,242
	AS4	-1,271	1,058
Algılanan Fayda (ALF)	**AF1**	-0,457	-0,641
	AF2	-0,217	-0,887
	AF3	-0,727	-0,25
	AF4	-0,563	-0,54
	AF5	-0,509	-0,586
Öz Yeterlilik (AOY)	**OY1**	-0,011	-0,907
	OY2	0,213	-0,893
	OY3	0,297	-0,822
	OY4	0,419	-0,699
Tepki Yeterliliği (ATY)	**TY1**	-0,092	-0,054
	TY2	-0,17	-0,204
	TY3	-0,353	-0,422
	TY4	-0,246	-0,341
	TY5	-0,076	-0,513
	TY6	-0,01	0,596
	TY7	-0,109	0,092
	TY8	-0,048	0,321
	TY9	0,031	-0,768
Tepki Maliyeti (ATM)	**MA1**	-0,564	-0,362
	MA2	-0,294	-0,676
	MA3	-0,016	-0,882
Gizlilik Endişesi (AGE)	**GE1**	-1,145	0,663
	GE2	-1,331	1,36
	GE3	-1,474	1,937
	GE4	-1,346	1,563
	GE5	-1,395	1,697
Gizlilik Kontrolü (AGK)	**GK1**	0,228	-0,691
	GK2	0,243	-0,772
	GK3	0,173	-0,814
Reklamdan Kaçında (RKN)	**RK1**	-0,55	-0,567
	RK2	-0,48	-0,791
	RK3	-0,582	-0,726
	RK4	-0,399	-0,598
	RK5	-0,264	-0,651

Literatürde farklı bakış açıları olmasına rağmen sosyal bilimler araştırmalarında -2 ile +2 arasındaki çarpıklık ve basıklık değerleri, normallik varsayımı için kabul edilebilir değerler olarak görülmektedir (George ve Mallery, 2010). Yapılan normallik testi

sonucunda ise her bir maddenin istenilen aralıkta olduğu gözlemlenmiştir. Bu sayede tek değişkenli normallik varsayımının sağlandığı söylenebilir.

Çalışma tek değişkenli normallik varsayımını sağladığı gibi çok değişkenli normallik varsayımını da sağlamaktadır. Çok değişkenli normallik için önerilen yöntemlerden biri ölçekteki maddelere yönelik kritik ki-kare değeri ve Mahalabobis uzaklığının hesaplanmasıdır (Arifin, 2015). "Verilerin İncelenmesi ve Uç Değerlerin Tespiti" başlığı altında uç değerlerin tespiti için yapılan işlem aynı zamanda çalışmanın çok değişkenli normallik varsayımını sağladığını da ortaya koymuştur.

4.3. Doğrusallık, Çoklu Doğrusallık ve Eşvaryanslılık

YEM modelini test edebilmek için normallik varsayımına ek olarak doğrulanması gereken diğer varsayımlar doğrusallık, çoklu doğrusallık ve eşvaryanslılık varsayımlarıdır.

Doğrusallık varsayımı iki değişken arasında düz çizgi halinde bir ilişki olduğunu ifade eder ve değişkenler arasındaki korelasyon (Pearson r) üzerinden yorumlanır (Tabachnick ve Fidell, 2015, s. 83). Çalışmada da korelasyon analizi gerçekleştirilerek doğrusallık varsayımı kontrol edilmiştir. Tablo 4.2'de değişkenler arası korelasyon değerlerine yönelik bulgular sunulmaktadır.

Tablo 4.2. *Değişkenler arası korelasyon değerlerine yönelik bulgular*

	ALC	**ALS**	**ALF**	**AOY**	**ATY**	**ATM**	**AGE**	**AGK**	**RKN**
ALC	1								
ALS	,693**	1							
ALF	-,115**	-,090**	1						
AOY	-,085*	-,065*	,223**	1					
ATY	0,024	0,042	,258**	,548**	1				
ATM	,137**	,141**	,091**	0,004	,132**	1			
AGE	,562**	,568**	-,133**	-,147**	0,015	,212**	1		
AGK	0,013	0,034	,221**	,442**	,355**	0,051	-,099**	1	
RKN	,490**	,458**	-,232**	0,002	,086*	,197**	,511**	,094**	1

**. Correlation is significant at the 0.01 level (1-tailed).
*. Correlation is significant at the 0.05 level (1-tailed).

Literatürde değişkenler arasındaki korelasyon değerlerinin ,80 üzerinde olmaması istenmektedir. Tablo 4.2'den de görüleceği üzere değişkenler arası korelasyon değerlerinin tamamının 0,80 altında olduğu tespit edilmiştir. Bu bulgulardan hareketle çalışmanın doğrusallık varsayımını sağladığı söylenebilir.

YEM modelindeki bir diğer varsayım olan çoklu doğrusallık ise iki veya daha fazla değişkenin çok yüksek düzeyde ilişkili olduğu ve her ikisinin de temelde aynı temel yapıyı temsil ettiği durumlarda ortaya çıkmaktadır (Bryne, 2016, s. 191). Bu durumda ele alınan değişkenlerin çok yüksek korelasyonda ilişki göstermemesi beklenir. Doğrusallığın ölçülmesinde korelasyon sonuçlarının yanı sıra Tolerans ve Varyans Artış Faktörü (VIF) değerlerine bakmak gerekir. Literatüre göre VIF değeri 10 altında olması kabul edilebilir bir göstergeyken bu değerin 4'in altında olması ise çoklu doğrusallık probleminin olmadığının göstergesidir. Tolerans değerinin ise 0,10'dan (0,1) büyük olması beklenir (Hair vd., 2019). Tablo 4.3'te çalışmanın VIF ve Tolerans testi sonuçları yer almaktadır.

Tablo 4.3. *VIF ve Tolerans testi sonuçları*

Bağımlı Değişken	**Bağımsız Değişkenler**	**Tolerans Değeri**	**VIF**
Reklamdan Kaçınma	Gizlilik Endişesi	0,585	1,71
	Gizlilik Kontrolü	0,762	1,313
	Algılanan Ciddiyet	0,476	2,102
	Algılanan Savunmasızlık	0,47	2,127
	Algılanan Fayda	0,886	1,129
	Öz Yeterlilik	0,61	1,641
	Tepki Yeterliliği	0,648	1,544
	Tepki Maliyeti	0,927	1,079

Tablo 4.3'te yer alan sonuçlara bakıldığında VIF değerlerinin 4'ün altında Tolerans değerlerinin ise .10'un üstünde olduğu görülmektedir. Bu sonuçlara göre çalışmada çoklu doğrusallık problemi olmadığı ve çalışma özelinde çoklu doğrusallık varsayımının karşılandığı söylenebilmektedir.

Çalışmada YEM varsayımlarının sonuncusu olarak eşvaryanslılık kontrol edilmiştir. Eşvaryanslılık, bir sürekli değişkenin puanlarındaki değişkenliği diğer sürekli

değişkenin tüm puanlarında kabaca aynı olması durumudur. Eşvaryanslılık aslında normallik varsayımı ile ilişkilidir. Çok değişkenli normallik sağlandığında eşvaryanslılığın da sağlandığı kabul edilir. Bunun dışında ise eşvaryanslılık varyansların homojenliği olarak bilinir. Literatürde ANOVA homojenlik testinin eşvaryanslılığı ölçümleme konusunda etkin bir analiz olduğu kabul edilmektedir (Tabachnick ve Fidell, 2015, s. 85). Bu bağlamda çalışmada eşvaryanslılık testi için varyansların homojenliği testi yapılmıştır. Tablo 4.4.'te eşvaryanslılığa yönelik bulgular yer almaktadır.

Tablo 4.4. *Eşvaryanslılık homojenlik testi*

	Levene İstatistiği	**df1**	**df2**	**Anlamlılık**
Algılanan Ciddiyet	0,539	1	692	0,463
Algılanan Savunmasızlık	0,258	1	692	0,612
Algılanan Fayda	0,397	1	692	0,529
Öz Yeterlilik	2,349	1	692	0,126
Tepki Yeterliliği	0,714	1	692	0,398
Tepki Maliyeti	0,424	1	692	0,515
Gizlilik Endişesi	0,085	1	692	0,771
Gizlilik Kontrolü	3,577	1	692	0,059
Reklamdan Kaçınma	0,859	1	692	0,354

Eşvaryanslılık varsayımının sağlanabilmesi için Levene değerinin 0,01 değeri üzerinde bir değere sahip olması gerekmektedir (Tabachnick ve Fidell, 2015). Tablo 4.4.'ten de görüleceği üzere Levene değerleri 0,085 ile 3,577 arasında değişmektedir. Bu doğrultuda çalışmada eşvaryanslılık varsayımının sağlandığı söylenebilir.

Toparlamak gerekirse YEM modelini test edebilmek için öncelikle normallik, doğrusallık, çoklu doğrusallık ve eşvaryanslılık varsayımlarının doğrulanması gerekmektedir. Yapılan analizler sonucunda elde edilen bulgular, çalışmada bu varsayımların doğrulandığını göstermektedir. Bu sonuçların elde edilmesinin ardından çalışmaya ölçeklerin geçerliğinin ve güvenirliğinin sınanmasıyla devam edilmiştir.

4.4. Ölçeklerin Geçerlik ve Güvenirlik Analizleri

Çalışmanın bu bölümünde Tehdit Değerlendirmesi Ölçeği, Başa Çıkma Değerlendirmesi Ölçeği, Gizlilik Endişesi Ölçeği, Gizlilik Kontrolü Ölçeği ve

Reklamdan Kaçınma Ölçeğinin geçerliği ve güvenirliği sınanmıştır. Bunun için öncelikle her bir ölçeğin DFA aracılığıyla uyum iyiliği indeksleri hesaplanmıştır. DFA temelde geçerlik analizleri ve önceden belirlenmiş olan bir yapının doğrulanması amacıyla kullanılmaktadır (Yaşlıoğlu, 2017, s. 78). Bu çalışmada da DFA'dan yararlanarak hem model uyum iyiliği indekslerini hesaplanmış hem de her bir ölçeğin geçerliğine yönelik bulgular tespit edilmiştir. Geçerlik kısaca ölçülmek istenen şeyin ne derece ölçülebildiğidir (Pallant, 2005, s. 6; Côté vd., 1988, s. 262). Yakınsama ve ayırt edici geçerlik ise yapı geçerliğinin iki temel yönüdür. Yakınsama geçerliği aynı şeyi ölçmesi gereken göstergelerin birbirleriyle ilişkili olup olmadığı anlamına gelir. Ayrıt edici geçerlik ise farklı şeyleri ölçen göstergelerin çok güçlü bir şekilde korelasyon gösterip göstermediği ile ilgilidir (Campbell ve Fiske, 1959) ve bir yapının, ilişkili diğer yapılardan farklı olma derecesi anlamına gelir (Hair vd., 2019, s. 659). Literatür yakınsama geçerliğin sağlanabilmesi için standardize edilmiş faktör yüklerinin ve Açıklanan Ortalama Varyans (AVE) değerlerinin 0,50'den, Birleşik Güvenirlik (Composite Reliability – CR) değerlerinin ise 0,70'ten büyük olmasını önerir. Yine literatür ayırt edici geçerlik için Paylaşılan Varyansın Karesinin Ortalaması (Avarage Shared Square Variance – ASV) ve Maksimum Paylaşılan Varyansın Karesi (Maximum Squared Variance – MSV) değerlerinin hesaplanması gerektiğini, fakat bu değerlerin hesaplanması içinse ölçeklerde en az 2 faktörün bulunması gerektiğini belirtir (Hair vd., 2019, s. 776). Bu doğrultuda çalışmada üçer faktörden oluşan Tehdit Değerlendirmesi Ölçeği ile Başa Çıkma Değerlendirmesi Ölçeği için ayırt edici geçerlik hesaplanmıştır. Ayırt edici geçerlilik koşulu için MSV ve ASV değerlerinin AVE değerinden küçük olması koşuluna (Hair vd., 2019) dikkat edilmiştir. Çalışmada tek faktörlü ölçekler içinse ölçeklerin sadece yakınsak geçerlikleri incelenmiştir. Çalışmanın devamında her bir ölçeğin geçerlik ve güvenirliklerine yönelik bulgular sunulmuştur.

4.4.1. Tehdit Değerlendirmesi Ölçeğine yönelik bulgular

13 madde ve 3 faktörlü bir yapıdan oluşan Tehdit Değerlendirmesi Ölçeğine yönelik yapılan ilk DFA sonucunda yapının bazı uyum iyiliği indekslerinin ideal olanın biraz altında olduğu görülmüştür (x2/df=5,309; CFI=,949, RMSEA=,790, SRMR=,040, GFI=,930). Bu nedenle çalışma içerisinde modifikasyon indisleri incelenerek AF1 ve AF2 maddeleri arasında kovaryans eklenmiş ve test tekrar edilmiştir. Yapılan ikinci test

sonucunda ise uyum iyiliği indekslerinin Tablo 4.5'te de gösterildiği üzere ideal düzeyde olduğu tespit edilmiştir.

Tablo 4.5. *Tehdit Değerlendirmesi Ölçeğinin DFA uyum iyiliği indekslerine yönelik bulgular*

DFA Uyum İndeksleri	Mevcut Değer	Kabul Edilir Değer	Kaynak	Kabul Edilebilirlik
X^2 /df	3,897	X^2 /df ≤ 5	Hair, Black, Babin ve Anderson (2019)	Kabul Edilebilir
Tahmin Hatalarının Ortalamasının Karekökü (RMSEA)	0,064	RMSEA ≤ .08	Hu ve Bentler, 1999	Kabul Edilebilir
Karşılaştırılmalı Uyum İndeksi (CFI)	0,994	.90 ≤ CFI	Brown, 2015	Kabul Edilebilir
İyilik Uyum İndeksi (GFI)	0,930	.90 ≤ GFI	Hu ve Bentler, 1999	Kabul Edilebilir
Standartlaştırılmış Hata Kareleri Ortalamasının Karekökü (SRMR)	0,037	SRMR ≤ .08	Hu ve Bentler, 1999	Kabul Edilebilir

Tehdit Değerlendirmesi Ölçeğinde hata kovaryansının yapılması ile iyi uyum değerlerine sahip olduğunun tespitinden sonra ölçek içerisinde yer alan maddelerin faktör yükleri, standardize edilmiş faktör yükleri, R^2 değerleri, anlamlılık düzeyleri ve z değerleri hesaplanmıştır. Tablo 4.6'da ölçeğe yönelik bu genel bulgular yer almaktadır.

Tablo 4.6. *Tehdit Değerlendirmesi Ölçeğine ilişkin genel bulgular*

Faktör	***Madde***	***Faktör Yükü***	***S. Faktör Yükü***	***R²***	***Standart Sapma***	***Mean***	***z değerleri***	***p***
ALC	AC_1	0,865	0,847	0,718	1,022	4,193	26,826	< .001
	AC_2	0,821	0,891	0,793	0,922	4,369	28,923	< .001
	AC_3	0,499	0,708	0,502	0,705	4,586	20,632	< .001
	AC_4	0,684	0,727	0,529	0,940	4,327	21,320	< .001
ALS	AS_1	0,752	0,713	0,508	1,056	4,146	20,421	< .001
	AS_2	0,858	0,808	0,653	1,063	3,934	24,509	< .001
	AS_3	0,893	0,848	0,719	1,054	3,973	26,271	< .001
	AS_4	0,598	0,660	0,436	0,906	4,313	18,581	< .001
ALF	AF_1	0,815	0,690	0,476	1,182	3,507	19,963	< .001
	AF_2	0,843	0,695	0,483	1,214	3,229	20,109	< .001
	AF_3	0,854	0,737	0,543	1,159	3,700	21,844	< .001
	AF_4	1,057	0,894	0,799	1,184	3,516	29,194	< .001
	AF_5	1,039	0,886	0,785	1,174	3,477	28,809	< .001

Tablo 4.6'dan da anlaşılacağı üzere maddelerin standardize edilmemiş faktör yükleri ,499 ile 1,057 arasında, standardize edilmiş faktör yükleri 0,660 ile 0,894 arasında R^2 değerleri ise 0,436 ile 0,799 arasında değişmektedir. Söz konusu olan bu değerlerin tamamının yeterli büyükte olduğunu söylemek mümkündür. Buna ek olarak standardize edilmiş faktör yüklerinin 0,50 ve üzerinde olması yakınsama geçerliğinin sağlandığına yönelik bir kanıt oluşturmaktadır. Tablo 4.7'de ise Tehdit Değerlendirmesi Ölçeğinin geçerliğine yönelik diğer bulgular sunulmuştur.

Tablo 4.7. *Tehdit Değerlendirmesi Ölçeğinin CR, AVE, MSV ve ASV değerleri*

Faktör	**CR**	**AVE**	**MSV**	**ASV**
Algılanan Ciddiyet	0,873	0,635	0,581	0,300
Algılanan Savunmasızlık	0,845	0,579	0,581	0,297
Algılanan Fayda	0,888	0,617	0,019	0,016

Tablo 4.7'de yer aldığı üzere Tehdit Değerlendirmesi Ölçeğine ait faktörlerin AVE değerleri 0,538 ile 0,777 arasında değişmektedir. CR değerleri ise 0,845 ile 0,888 arasında değişmektedir. Elde edilen bu bulgular (AVE > 0,50, CR > 0,70) ve standardize edilmiş faktör yüklerinin 0,50 ve üzerinde olması analize tabi tutulan ölçeğin yakınsama geçerliğini sağladığını göstermektedir.

Tablo 4.7'de Tehdit Değerlendirmesi Ölçeğinin ayırt edici geçerliği sağladığına yönelik bulgular da söz konusu olmaktadır. Algılanan Ciddiyet faktörünün MSV değeri ,581, ASV değeri ise ,300 düzeyindedir. Her iki değerin de aynı faktörün AVE değerinden (.635) küçük olduğu anlaşılmaktadır. Bir diğer faktör olan Algılanan Savunmasızlık faktörünün ise MSV değeri 0,581, ASV değeri ise 0,297'dir. Yine bu değerlerin faktöre ait olan AVE değerinden (.579) küçük olduğu görülmektedir. Tehdit Değerlendirmesi Ölçeğinin sonuncu faktörü olan Algılanan Fayda faktöründe de benzer durumlar söz konusudur. Faktörün MSV değeri 0,019'ken ASV değeri 0,016'dır. Faktörün AVE değeri (,617) ise bu iki değerden daha fazladır. Söz konusu olan tüm bu bulgular ise Tehdit Değerlendirmesi Ölçeğinin ayırt edici geçerliği sağladığını ortaya koymaktadır. Ölçeğin hem yakınsama hem de ayırt edici geçerliği kontrol edildikten sonra çalışmaya ölçeğin güvenirliğinin analizi ile devam edilmiştir. Güvenirlik analizleri için Cronbach alfa ve

McDonald’s ω değerleri incelenmiştir. Tablo 4.8’de ölçeğin güvenirliğine yönelik bulgular yer almaktadır:

Tablo 4.8. *Tehdit Değerlendirmesi Ölçeğinin güvenirliğine yönelik bulgular*

Faktör	***Maddeler***	***Toplam madde r***	***Madde silindiğinde Cronbach alfa***	***Cronbach alfa***		***Madde silindiğinde McDonald's ω***	***McDonald's ω***
ALC	AC_1	0,756	0,816	0,867		0,824	0,878
	AC_2	0,803	0,793			0,804	
	AC_3	0,669	0,855			0,862	
	AC_4	0,678	0,846			0,873	
ALS	AS_1	0,616	0,822	0,839		0,836	0,847
	AS_2	0,731	0,770			0,781	
	AS_3	0,754	0,759			0,768	
	AS_4	0,597	0,828			0,833	
ALF	AF_1	0,715	0,880	0,896		0,880	0,895
	AF_2	0,726	0,878			0,880	
	AF_3	0,709	0,881			0,879	
	AF_4	0,786	0,864			0,865	
	AF_5	0,785	0,865			0,865	

Tehdit Değerlendirmesi Ölçeğinin güvenirliğine ilişkin bulgulara bakıldığında her bir faktörün yüksek düzeyde güvenirlik değerlerine sahip olduğu görülmektedir. Bu doğrultuda en düşük Cronbach alfa katsayısı 0,839 ile algılanan savunmasızlık faktörüne aitken, en düşük McDonald’s ω değeri ise 0,847 ile aynı faktöre aittir. Bu değerler ise ölçeğin oldukça güvenilir olduğunu ortaya koymaktadır.

Tehdit Değerlendirmesi Ölçeği özelinde gerçekleştirilen tüm işlemler sonucunda ölçeğin iyi uyum değerlerine sahip olduğu ve aynı zamanda geçerli ve güvenilir bir ölçek olduğu çalışmada ortaya konmuştur.

4.4.2. Başa Çıkma Değerlendirmesi Ölçeğine yönelik bulgular

16 madde ve 3 faktörlü bir yapıdan oluşan Başa Çıkma Değerlendirmesi Ölçeğine yönelik yapılan ilk DFA sonucunda yapının bazı uyum iyiliği indekslerinin ideal olanın biraz altında olduğu görülmüştür (x2/df=5,250; CFI=,908, RMSEA=,780, SRMR=,0750, GFI=,911). Hata kovaryansları gerçekleştirmeden önce ve yapılan incelemelerden sonra Tepki Maliyeti faktörü içerisinde yer alan MA1 (*Hedefli reklamlardan kaçınırsam*

ilgilendiğim ürün/hizmet reklamlarıyla daha az karşılaşırım) maddesinin standardize edilmiş faktör yükünün 0,120 gibi oldukça düşük bir yüke sahip olduğu, ayrıca yine MA1 maddesinin R^2 değerinin 0,009 düzeyinde olduğu görülmüştür. Bu değerler kabul edilebilir seviyede değildir. MA1 maddesindeki problemin bir diğer göstergesi maddenin ölçeğin güvenirliğine zarar veriyor olmasıdır. Yapılan analizlerde MA1 maddesinin yer aldığı Tepki Maliyeti faktörünün Cronbach alfa katsayısı 0,496 gibi düşük bir değere sahip olduğu görülmüştür. MA1 maddesinin ölçekten çıkarılmasıyla birlikte bu faktörün Cronbach alfa katsayısının 0,729 seviyesine çıktığı tespit edilmiştir. Tüm bu bulgular ve pilot çalışmada da problemli olmasına yönelik ipuçları sunması nedeniyle MA1 maddesinin ölçekten çıkarılmasına ve analizlere bu şekilde devam edilmesine karar verilmiştir. Yukarıda yer alan açıklamalardan hareketle MA1 maddesi ölçekten çıkarılmış, ayrıca modifikasyon indisleri incelenerek TY2 ve TY3 maddeleri arasında kovaryans eklenerek çalışmada tekrar DFA gerçekleştirilmiştir. Yapılan bu ikinci test sonucunda ise uyum iyiliği indekslerinin Tablo 4.9'da da gösterildiği üzere ideal düzeyde olduğu tespit edilmiştir.

Tablo 4.9. *Başa Çıkma Değerlendirmesi Ölçeğinin DFA uyum iyiliği indekslerine yönelik bulgular*

DFA Uyum İndeksleri	Mevcut Değer	Kabul Edilir Değer	Kaynak	Kabul Edilebilirlik
X^2 /df	4,531	X^2 /df ≤ 5	Hair, Black, Babin ve Anderson (2019)	Kabul Edilebilir
Tahmin Hatalarının Ortalamasının Karekökü (RMSEA)	0,071	RMSEA ≤ .08	Hu ve Bentler, 1999	Kabul Edilebilir
Karşılaştırılmalı Uyum İndeksi (CFI)	0,934	.90 ≤ CFI	Brown, 2015	Kabul Edilebilir
İyilik Uyum İndeksi (GFI)	0,928	.90 ≤ GFI	Hu ve Bentler, 1999	Kabul Edilebilir
Standartlaştırılmış Hata Kareleri Ortalamasının Karekökü (SRMR)	0,051	SRMR ≤ .08	Hu ve Bentler, 1999	Kabul Edilebilir

Başa Çıkma Değerlendirmesi Ölçeğinde hata kovaryansının yapılması ile iyi uyum değerlerine sahip olduğunun tespitinden sonra ölçek içerisinde yer alan maddelerin faktör yükleri, standardize edilmiş faktör yükleri, R^2 değerleri, anlamlılık düzeyleri ve z değerleri hesaplanmıştır. Tablo 4.10'da ölçeğe yönelik bu genel bulgular yer almaktadır.

Tablo 4.10. *Başa Çıkma Değerlendirmesi Ölçeğine ilişkin genel bulgular*

Faktör	*Madde*	*Faktör Yükü*	*S. Faktör Yükü*	R^2	*Standart Sapma*	*Mean*	*z değerleri*	*p*
AOY	OY_1	0,790	0,650	0,423	1,216	2,988	18,564	< .001
	OY_2	0,986	0,818	0,668	1,207	2,741	25,396	< .001
	OY_3	1,120	0,929	0,864	1,206	2,640	30,921	< .001
	OY_4	0,939	0,775	0,600	1,213	2,555	23,505	< .001
ATY	TY_1	0,705	0,699	0,334	0,971	3,293	15,765	< .001
	TY_2	0,699	0,637	0,489	1,009	3,216	20,036	< .001
	TY_3	0,768	0,727	0,406	1,098	3,267	17,713	< .001
	TY_4	0,790	0,718	0,528	1,058	3,291	21,180	< .001
	TY_5	0,629	0,696	0,515	1,102	2,990	20,824	< .001
	TY_6	0,680	0,717	0,484	0,904	3,092	19,967	< .001
	TY_7	0,600	0,671	0,514	0,949	3,235	20,770	< .001
	TY_8	0,563	0,480	0,450	0,895	3,297	19,012	< .001
	TY_9	0,776	0,690	0,229	1,177	2,909	12,638	< .001
ATM	MA_2	0,995	0,833	0,476	1,125	3,442	4,048	< .001
	MA_3	0,790	0,650	0,693	1,196	3,066	4,079	< .001

Tablo 4.10'dan da görüleceği üzere maddelerin standardize edilmemiş faktör yükleri ,563 ile 1,120 arasında, standardize edilmiş faktör yükleri 0,480 ile 0,929 arasında değişmektedir. Standardize edilmiş faktör yüklerinin 0,50 ve üzerinde olması iyi değer olarak ele alınırken ölçekte sadece TY_8 maddesine ait olan değerin (0,48) beklenen değerin (0,50) çok ufak bir farkla altında olduğu görülmektedir. Ölçekte yer alan diğer tüm maddeler ise oldukça yüksek düzeyde standardize edilmiş faktör yüklerine sahiptir. Maddelerin R^2 değerleri ise 0,229 ile 0,864 arasında değişmektedir. Söz konusu olan bu değerlerin tamamının yeterli büyükte olduğunu söylemek mümkündür.

Buna ek olarak TY_8 hariç diğer tüm maddelerin standardize edilmiş faktör yüklerin .50 ve üzerinde olması yakınsama geçerliğinin sağlandığına yönelik bir kanıt olarak ele alınabilir. Geçerliğin sağlandığından emin olmak için diğer değerler de incelenmiştir. Tablo 4.11'de Başa Çıkma Değerlendirmesi Ölçeğinin geçerliğine yönelik diğer bulgular sunulmuştur.

Tablo 4.11. *Başa Çıkma Değerlendirmesi Ölçeğinin CR, AVE, MSV ve ASV değerleri*

Faktör	**CR**	**AVE**	**MSV**	**ASV**
Öz Yeterlilik	0,804	0,638	0,339	0,174
Tepki Yeterliliği	0,874	0,438	0,339	0,169
Tepki Maliyeti	0,736	0,584	0,008	0,004

Tablo 4.11'de yer aldığı üzere Başa Çıkma Değerlendirmesi Ölçeğine ait faktörlerin AVE değerleri 0,438 ile 0,638 arasında değişmektedir. CR değerleri ise 0,736 ile ,874 arasında değişmektedir. Öz Yeterlilik ve Tepki Maliyeti faktörlerinin AVE değeri 0,50 üzerindeyken, Tepki Yeterliliği faktörünün AVE değeri olması gereken değerin biraz altındadır. Böyle bir durumda Literatürde, AVE değeri 0,40 düzeyindeyse bu değerin geçerlilik için yeterli olduğunu anlamak için CR değerine bakılması ve CR değeri ,60'ın üzerindeyse yakınsama geçerliğinin sağlandığı belirtilir (Fornell ve Larcker, 1981). Tablo 4.11 üzerinden de görüleceği üzere Tepki Yeterliliği faktörünün AVE değeri ,40 üzerindedir ve faktörün CR değeri ise 0,874'tür. Yapılan tüm bu açıklamalardan hareketle Başa Çıkma Ölçeğinin yakınsama geçerliğini sağladığını söylemek mümkündür.

Ayrıca Öz Yeterlilik faktörünün MSV değeri 0,339, ASV değeri ise 0,174 düzeyindedir. Her iki değerin de aynı faktörün AVE değerinden (.638) küçük olduğu anlaşılmaktadır. Bir diğer faktör olan Tepki Yeterliliği faktörünün ise MSV değeri 0,339, ASV değeri ise 0,169'dur. Yine bu değerlerin faktöre ait olan AVE değerinden (.438) küçük olduğu görülmektedir. Tehdit Değerlendirmesi Ölçeğinin sonuncu faktörü olan Tepki Maliyeti faktöründe de aynı durum söz konusudur. Faktörün MSV değeri 0,008, ASV değeri 0,004'tür. Faktörün AVE değeri (.584) ise bu iki değerden daha fazladır. Söz konusu olan tüm bu bulgular ise Başa Çıkma Ölçeğinin ayırt edici geçerliği sağladığını ortaya koymaktadır. Ölçeğin güvenirliğine yönelik bulgular ise Tablo 4.12'de yer almaktadır:

Tablo 4.12. *Başa Çıkma Ölçeğinin güvenirliğine yönelik bulgular*

Faktör	***Maddeler***	***Toplam madde r***	***Madde silindiğinde Cronbach alfa***	***Cronbach alfa***		***Madde silindiğinde McDonald's ω***	***McDonald's ω***
AOY	OY_1	0,610	0,874	0,868		0,879	0,872
	OY_2	0,744	0,821			0,830	
	OY_3	0,830	0,785			0,787	
	OY_4	0,700	0,839			0,847	
ATY	TY_1	0,526	0,864	0,871		0,866	0,873
	TY_2	0,684	0,850			0,852	
	TY_3	0,625	0,856			0,858	
	TY_4	0,672	0,851			0,853	
	TY_5	0,669	0,851			0,853	
	TY_6	0,638	0,855			0,858	

Tablo 4.13. (Devam) *Başa Çıkma Ölçeğinin güvenirliğine yönelik bulgular*

Faktör	*Maddeler*	*Toplam madde r*	*Madde silindiğinde Cronbach alfa*	*Cronbach alfa*		*Madde silindiğinde McDonald's ω*	*McDonald's ω*
	TY_7	0,647	0,854			0,857	
	TY_8	0,615	0,857			0,860	
	TY_9	0,435	0,876			0,878	
ATM	MA_2	0,579	--------	0,729		--------	--------
	MA_3	0,579	--------			--------	

Başa Çıkma Değerlendirmesi Ölçeğinin güvenirliğine ilişkin bulgulara bakıldığında hem ölçek içerisindeki maddelerin hem de her bir faktörün kabul edilebilir güvenirlik değerlerine sahip olduğu görülmektedir. Bu doğrultuda en düşük Cronbach alfa katsayısı 0,729 ile Tepki Maliyeti faktörüne aittir.

Başa Çıkma Değerlendirmesi Ölçeği özelinde gerçekleştirilen tüm işlemler sonucunda ölçeğin iyi uyum değerlerine sahip olduğu ve aynı zamanda geçerli ve güvenilir bir ölçek olduğu çalışmada ortaya konmuştur.

4.4.3. Gizlilik Endişesi Ölçeğine yönelik bulgular

5 madde ve tek faktörlü bir yapıdan oluşan Gizlilik Endişesi Ölçeğine yönelik yapılan ilk DFA sonucunda yapının bazı uyum iyiliği indekslerinin ideal olanın biraz altında olduğu görülmüştür (x2/df=15,960; CFI=,966, RMSEA=,147, SRMR=,034, GFI=,954). Model uyumunun iyileşmesi için modifikasyon indisleri incelenerek G4 ve G5 maddeleri arasında kovaryans eklenerek tekrar test yoluna gidilmiştir. İkinci test sonucunda uyum iyiliği indekslerinin Tablo 4.13'te gösterildiği üzere ideal düzeyde olduğu tespit edilmiştir.

Tablo 4.14. *Gizlilik Endişesi Ölçeğinin DFA uyum iyiliği indekslerine yönelik bulgular*

DFA Uyum İndeksleri	Mevcut Değer	Kabul Edilir Değer	Kaynak	Kabul Edilebilirlik
X^2 /df	1,250	X^2 /df ≤ 5	Hair, Black, Babin ve Anderson (2019)	Kabul Edilebilir
Tahmin Hatalarının Ortalamasının Karekökü (RMSEA)	0,019	RMSEA ≤ .08	Hu ve Bentler, 1999	Kabul Edilebilir

Tablo 4.15. **(Devam)** *Gizlilik Endişesi Ölçeğinin DFA uyum iyiliği indekslerine yönelik bulgular*

DFA Uyum İndeksleri	Mevcut Değer	Kabul Edilir Değer	Kaynak	Kabul Edilebilirlik
Karşılaştırılmalı Uyum İndeksi (CFI)	1	.90 ≤ CFI	Brown, 2015	Kabul Edilebilir
İyilik Uyum İndeksi (GFI)	0,997	.90 ≤ GFI	Hu ve Bentler, 1999	Kabul Edilebilir
Standartlaştırılmış Hata Kareleri Ortalamasının Karekökü (SRMR)	0,008	SRMR ≤ .08	Hu ve Bentler, 1999	Kabul Edilebilir

Gizlilik Endişesi Ölçeğinde hata kovaryansının yapılması ile iyi uyum değerlerine sahip olduğunun tespitinden sonra yine ölçek içerisinde yer alan maddelerin faktör yükleri, standardize edilmiş faktör yükleri, R^2 değerleri, anlamlılık düzeyleri, z değerleri, CR ve AVE değerleri hesaplanmıştır. Tablo 4.14'te ölçeğe yönelik bu genel bulgular yer almaktadır.

Tablo 4.16. *Gizlilik Endişesi Ölçeğine ilişkin genel bulgular*

Ölçek	*Madde*	*Faktör Yükü*	*S. Faktör Yükü*	*R^2*	*Standart Sapma*	*Mean*	*z değerleri*	*p*	*CR*	*AVE*
AGE	GE_1	0,766	0,746	0,545	1,027	4,128	22,311	< .001	0,899	0,643
	GE_2	0,846	0,887	0,764	0,955	4,238	28,868	< .001		
	GE_3	0,805	0,883	0,766	0,913	4,300	28,664	< .001		
	GE_4	0,704	0,785	0,665	0,898	4,288	23,956	< .001		
	GE_5	0,639	0,690	0,536	0,927	4,265	19,976	< .001		

Tablo 4.14'ten de anlaşılacağı üzere maddelerin standardize edilmemiş faktör yükleri 0,639 ile 0,846 arasında, standardize edilmiş faktör yükleri 0,690 ile 0,887 arasında R^2 değerleri ise 0,536 ile 0,766 arasında değişmektedir. Söz konusu olan bu değerlerin tamamının yeterli büyükte olduğunu söylemek mümkündür. Buna ek olarak standardize edilmiş faktör yüklerin 0,50 ve üzerinde olması yakınsama geçerliğinin sağlandığına yönelik bir kanıt oluşturmaktadır.

Gizlilik Endişesi Ölçeğinin geçerliliği sınanırken tek faktörlü yapısından dolayı CR ve AVE değerlerinden yararlanılmış ve böylece ölçeğin yakınsama geçerliği sağlayıp sağlamadığı incelenmiştir. Bu durum çalışmanın devamında yer alan ve tek faktörlü yapıya sahip olan diğer ölçekler için de geçerli olmuştur.

Tablo 4.14'ten de görüleceği üzere Gizlilik Endişesi Ölçeğinin CR değeri 0,899, AVE değeri ise 0,643 olarak tespit edilmiştir. Elde edilen bu bulgular (AVE > 0,50, CR > 0,70) ve standardize edilmiş faktör yüklerinin 0,50 ve üzerinde olması analize tabi tutulan ölçeğin yakınsama geçerliğini sağladığını ortaya koymuştur. Ölçeğin güvenirliğine yönelik bulgular ise Tablo 4.15'te sunulmuştur:

Tablo 4.17. *Gizlilik Endişesi Ölçeğinin güvenirliğine yönelik bulgular*

Ölçek	***Maddeler***	***Toplam madde r***	***Madde silindiğinde Cronbach alfa***	***Cronbach alfa***		***Madde silindiğinde McDonald's ω***	***McDonald's ω***
Gizlilik Endişesi	GE_1	0,689	0,896	.902		0,897	.903
	GE_2	0,813	0,867			0,868	
	GE_3	0,812	0,868			0,869	
	GE_4	0,777	0,876			0,879	
	GE_5	0,696	0,892			0,894	

Gizlilik Endişesi Ölçeğinin güvenirliğine ilişkin bulgulara bakıldığında ölçek içerisindeki maddelerin her birinin yüksek düzeyde güvenirlik değerlerine sahip olduğu görülmektedir (α = 0,902, ω = 0,903). Yapılan işlemler sonucunda ölçeğin iyi uyum değerlerine sahip olduğu ve aynı zamanda geçerli ve güvenilir bir ölçek olduğu tespit edilmiştir.

4.4.4. Gizlilik Kontrolü Ölçeğine yönelik bulgular

Gizlilik Kontrolü ölçeği 3 maddeden oluşan tek faktörlü bir ölçektir. Ölçeğin bu yapısından dolayı model uyumu sınanmamıştır. Çünkü madde sayısı 4 altında olan ölçeklerde uyum indeksi hesaplanması söz konusu değildir (Çelik ve Yılmaz, 2016, s.58). Bu nedenle çalışmaya uyum indekslerinin hesaplanması yerine doğrudan ölçek içerisinde yer alan maddelerin faktör yükleri, standardize edilmiş faktör yükleri, R^2 değerleri, anlamlılık düzeyleri ve z değerlerinin hesaplanmasıyla başlanmış ve CR ile AVE değerlerinin hesaplaması yapılmıştır. Tablo 4.16'da ölçeğe yönelik bu genel bulgular yer almaktadır.

Tablo 4.18. *Gizlilik Kontrolü Ölçeğine ilişkin genel bulgular*

Ölçek	Madde	Faktör Yükü	S. Faktör Yükü	R^2	Standart Sapma	Mean	z değerleri	p	CR	AVE
AGK	GK_1	0,928	0,793	0,630	1,171	2,756	23,954	< .001	0,881	0,713
	GK_2	1,048	0,874	0,764	1,200	2,764	27,319	< .001		
	GK_3	1,037	0,865	0,747	1,200	2,793	26,899	< .001		

Tablo 4.16'da yer alan bulgulara bakıldığında maddelerin standardize edilmemiş faktör yüklerinin 0,928 ile 1,048 arasında, standardize edilmiş faktör yüklerinin 0,793 ile 0,874 arasında R^2 değerlerinin ise 0,630 ile 0,764 arasında değiştiği görülmektedir. Söz konusu olan bu değerlerin tamamının yeterli büyükte olduğunu söylemek mümkündür. Buna ek olarak yapılan analiz sonucunda Gizlilik Kontrolü Ölçeğinin CR değeri 0,881, AVE değeri ise 0,713 olarak tespit edilmiştir. Elde edilen bu bulgular (AVE > 0,50, CR > 0,70) ve standardize edilmiş faktör yüklerinin 0,50 ve üzerinde olması analize tabi tutulan ölçeğin yakınsama geçerliğini sağladığını ortaya koymuştur. Ölçeğin güvenirliğine yönelik bulgular ise Tablo 4.17'de sunulmuştur:

Tablo 4.19. *Gizlilik Kontrolü Ölçeğinin güvenirliğine yönelik bulgular*

Ölçek	Maddeler	Toplam madde r	Madde silindiğinde Cronbach alfa	Cronbach alfa		Madde silindiğinde McDonald's ω	McDonald's ω
Gizlilik Kontrolü	GK_1	0,736	0,861	,881		--------	,882
	GK_2	0,790	0,814			--------	
	GK_3	0,784	0,819			--------	

Gizlilik Kontrolü Ölçeğinin güvenirliğine ilişkin bulgulara bakıldığında ölçeğin yeterli düzeyde güvenirlik değerlerine sahip olduğu görülmektedir (α = ,881, ω = ,882). Yapılan işlemler sonucunda elde edilen tüm bulgular ölçeğin iyi uyum değerlerine sahip olduğunu ve aynı zamanda geçerli ve güvenilir bir ölçek olduğunu ortaya koymuştur.

4.4.5. Reklamdan Kaçınma Ölçeğine yönelik bulgular

Reklamdan Kaçınma Ölçeği 5 madde ve tek faktörden oluşan bir ölçektir. Yapılan ilk DFA sonucunda uyum iyiliği indeksleri CMIN/df=29,5 p=.000, RMSEA=.203, CFI=.883, GFI=.924 SRMR= .076 olarak bulunmuştur. Bu değerler kabul edilebilir değerlerin dışında kalmaktadır. Bu nedenle model uyumunun iyileşmesi için modifikasyon indisleri incelenerek RK_4 ve RK_5 maddeleri arasına kovaryans eklenmiş ve test tekrarlanmıştır. Fakat yine elde edilen uyum iyiliği indekslerinin istenen düzeyde olmadığı görülmüş, bundan dolayı RK_1 ve RK_4 maddeleri arasında bir kez daha kovaryans eklenerek test tekrarlanmıştır. Yapılan bu test sonucunda uyum iyiliği indeksleri istenen düzeye ulaşmıştır. Tablo 4.18'de Reklamdan Kaçınma Ölçeğinin uyum iyiliği indeksleri yer almaktadır.

Tablo 4.20. *Reklamdan Kaçınma Ölçeğinin DFA uyum iyiliği indekslerine yönelik bulgular*

DFA Uyum İndeksleri	Mevcut Değer	Kabul Edilir Değer	Kaynak	Kabul Edilebilirlik
X^2 /df	3,987	X^2 /df ≤ 5	Hair, Black, Babin ve Anderson (2019)	Kabul Edilebilir
Tahmin Hatalarının Ortalamasının Karekökü (RMSEA)	0,066	RMSEA ≤ .08	Hu ve Bentler, 1999	Kabul Edilebilir
Karşılaştırılmalı Uyum İndeksi (CFI)	0,993	.90 ≤ CFI	Brown, 2015	Kabul Edilebilir
İyilik Uyum İndeksi (GFI)	0,993	.90 ≤ GFI	Hu ve Bentler, 1999	Kabul Edilebilir
Standartlaştırılmış Hata Kareleri Ortalamasının Karekökü (SRMR)	0,016	SRMR ≤ .08	Hu ve Bentler, 1999	Kabul Edilebilir

Çalışmada DFA sonucu uyum iyiliği indekslerinin incelenmesinin ardından ölçek içerisinde yer alan maddelerin faktör yükleri, standardize edilmiş faktör yükleri, R^2 değerleri, anlamlılık düzeyleri, z değerleri, CR ve AVE değerleri hesaplanmıştır. Tablo 4.19'de ölçeğe yönelik bu genel bulgular yer almaktadır.

Tablo 4.21. *Reklamdan Kaçınma Ölçeğine ilişkin genel bulgular*

Ölçek	*Madde*	*Faktör Yükü*	*S. Faktör Yükü*	*R^2*	*Standart Sapma*	*Mean*	*z değerleri*	*p*	*CR*	*AVE*
RKN	RK_1	0,612	0,561	0,315	1,091	3,731	14,976	< .001	0,790	0,446
	RK_2	0,989	0,868	0,753	1,140	3,761	25,213	< .001		
	RK_3	0,929	0,833	0,694	1,117	3,863	23,974	< .001		

Tablo 4.22. (Devam) *Reklamdan Kaçınma Ölçeğine ilişkin genel bulgular*

Ölçek	Madde	Faktör Yükü	S. Faktör Yükü	R^2	Standart Sapma	Mean	z değerleri	p	CR	AVE
	RK_4	0,561	0,502	0,252	1,120	3,563	13,080	< .001		
	RK_5	0,520	0,467	0,218	1,115	3,487	12,108	< .001		

Tablo 4.19'da yer alan bulgulara bakıldığında maddelerin standardize edilmemiş faktör yüklerinin 0,520 ile 0,989 arasında, standardize edilmiş faktör yüklerinin 0,467 ile 0,868 arasında R^2 değerlerinin ise 0,218 ile 0,753 arasında değiştiği görülmektedir. Söz konusu olan bu değerlerin tamamının yeterli büyükte olduğunu söylemek mümkündür. Buna ek olarak yapılan analiz sonucunda Reklamdan Kaçınma Ölçeğinin CR değeri 0,790, AVE değeri ise 0,446 olarak tespit edilmiştir. AVE değeri 0,40'ın üzerinde CR değerinin de 0,60'ın üzerinde olmasından dolayı (Fornell ve Larcker, 1981) hem de standardize edilmiş faktör yüklerinin 0,50 ve üzerinde bir değere sahip olmasından dolayı ölçeğin yakınsama geçerliğini sağladığı söylenebilir. Ölçeğin güvenirliğine yönelik bulgular ise Tablo 4.20'de sunulmuştur.

Tablo 4.23. *Reklamdan Kaçınma Ölçeğinin güvenirliğine yönelik bulgular*

Ölçek	Maddeler	Toplam madde r	Madde silindiğinde Cronbach alfa	Cronbach alfa		Madde silindiğinde McDonald's ω	McDonald's ω
Reklamdan Kaçınma	RK_1	0,507	0,794	.806		0,791	.806
	RK_2	0,676	0,742			0,745	
	RK_3	0,673	0,743			0,744	
	RK_4	0,581	0,772			0,789	
	RK_5	0,523	0,789			0,799	

Reklamdan Kaçınma Ölçeğinin güvenirliğine ilişkin bulgulara bakıldığında ölçeğin yeterli düzeyde güvenirlik değerlerine sahip olduğu görülmektedir (α = ,806, ω = ,806). Yapılan işlemler sonucunda elde edilen tüm bulgular ölçeğin iyi uyum değerlerine sahip olduğunu ve aynı zamanda geçerli ve güvenilir bir ölçek olduğunu ortaya koymuştur.

"Ölçeklerin Geçerlik ve Güvenirlik Analizleri" başlığı altında Tehdit Değerlendirmesi Ölçeği, Başa Çıkma Değerlendirmesi Ölçeği, Gizlilik Endişesi Ölçeği, Gizlilik Kontrolü Ölçeği ve Reklamdan Kaçınma Ölçeğinin geçerlikleri ve güvenirlikleri

sınanmış hem ölçeklere hem de maddelere yönelik çeşitli bulgular sunulmuştur. Sunulan tüm bulgulardan hareketle söz konusu ölçeklerin tamamının geçerli ve güvenilir ölçekler olduğu tespit edilmiştir. Yapılan bu tespitin ardından çalışmaya araştırma modelinin test edilmesiyle devam edilmiştir.

4.5. Araştırma Modelinin Test Edilmesi

Hair vd. (2019) YEM gerçekleştirmek için iki aşama ileri sürer. İlk aşama ölçüm modelinin değerlendirilmesidir. İkinci aşama ise yapısal modeli değerlendirmektir. Başka bir ifade ile yapısal modeli değerlendirmek için öncelikle ölçüm modelini değerlendirmek gerekmektedir. Buradan hareketle de çalışmada ölçüm modelinin değerlendirilmesi için çeşitli analizler gerçekleştirilmiş bunun ardından ve son olarak da yapısal modelin değerlendirilmesi gerçekleştirilmiştir. Çalışmanın devamında bu değerlendirme süreçlerinde gerçekleştirilen işlemlere yönelik bulgular yer almaktadır.

4.5.1. Ölçüm modelinin değerlendirilmesi

Ölçüm modelinin değerlendirilmesi aynı zamanda yapı geçerliğinin sınanması anlamına gelir. Çalışmada da bu bağlamda ölçüm modelinin yapı geçerliğini sağlayıp sağlamadığını tespit etmek adına yakınsama ve ayırt edici geçerlilikler model özelinde değerlendirilmiştir. Tablo 4.21'de ölçüm modelinin geçerliğine yönelik bulgulara yer verilmiştir.

Tablo 4.24. *Ölçüm modelinin geçerliğine yönelik bulgular*

	CR	AVE	MSV	ASV	AGE	ALC	ALS	ALF	AOY	ATY	ATM	AGK	RKN
AGE	0,900	0,645	0,392	0,154	**0,803**								
ALC	0,874	0,636	0,585	0,169	0,613	**0,797**							
ALS	0,845	0,580	0,585	0,166	0,626	0,760	**0,761**						
ALF	0,889	0,618	0,097	0,042	-0,120	-0,137	-0,119	**0,786**					
AOY	0,875	0,640	0,348	0,084	-0,162	-0,085	-0,071	0,224	**0,800**				
ATY	0,874	0,439	0,348	0,075	0,015	0,029	0,048	0,298	0,590	**0,662**			
ATM	0,744	0,597	0,075	0,030	0,274	0,187	0,209	-0,016	-0,088	-0,023	**0,773**		
AGK	0,882	0,714	0,220	0,056	-0,113	0,022	0,053	0,224	0,469	0,395	0,029	**0,845**	
RKN	0,795	0,451	0,334	0,141	0,578	0,573	0,533	-0,312	-0,068	0,017	0,273	0,039	**0,672**

Köşegenlerde yer alan koyu değerler, AVE değerlerinin kareköklerini ifade eder.

Tablo 4.21 incelendiğinde ATY ve RKN değişkenleri hariç diğer tüm değişkenlerin AVE değerlerinin 0,50 ve üzerinde olduğu görülmektedir. AVE değerleri 0,50 altında olan değişkenlerin CR değerleri kontrol edildiğinde ise her iki değişkenin CR değerinin ise 0,80 ve üzerinde olduğu görülmektedir. Tüm bu bulgulardan hareketle ölçüm modelinin yakınsak geçerliği sağladığını söylemek mümkündür. Yine Tablo 4.21 incelendiğinde AVE değerlerinin kareköklerinin yapılar arasındaki korelasyon değerlerinden yüksek olduğu görülmektedir. Bu durum ölçüm modelinin ayırt edici geçerliği sağladığına dair kanıt oluşturmaktadır (Hair vd., 2019). Buna ek olarak çalışmada ölçüm modelinin yapı geçerliğini değerlendirmek için Heterotrait-Monotrait (HTMT) oranı hesaplanmıştır. Tablo 4.22'de bulgulara yer verilmiştir.

Tablo 4.25. *Ölçüm modelinin HTMT oranları*

	ALC	**ALS**	**ALF**	**AOY**	**ATY**	**ATM**	**AGK**	**AGE**	**RKN**
ALC									
ALS	0,809								
ALF	0,125	0,103							
AOY	0,098	0,078	0,252						
ATY	0,026	0,043	0,292	0,631					
ATM	0,216	0,22	0,027	0,099	0,004				
AGK	0,013	0,037	0,248	0,506	0,404	0,029			
AGE	0,633	0,657	0,145	0,166	0,017	0,281	0,112		
RKN	0,577	0,555	0,272	0,002	0,099	0,294	0,112	0,597	

Kline (2011) ayırt edici geçerliğin sağlanması için 0.85'lik bir eşik önerir. Yazara göre HTMT oranları 0,85 ve üzeri olmadığı sürece ayırt edici geçerlikten bahsedilebilir. Tablo 4.22 incelendiğinde ise hiçbir oranın bu eşik değerden daha yukarıda olduğu görülmemektedir. Böylece ölçüm modelinin ayırt edici geçerlilik sağladığına yönelik bir başka bulgu ortaya konmuştur. Modelin uyum indeksleri ise Tablo 4.23'te gösterilmektedir.

Tablo 4.26. *Ölçüm modelinin uyum iyiliği indekslerine yönelik bulgular*

DFA Uyum İndeksleri	Mevcut Değer	Kabul Edilir Değer	Kaynak	Kabul Edilebilirlik
X^2 /df	2,347	X^2 /df ≤ 5	Hair, Black, Babin ve Anderson (2019)	Kabul Edilebilir
Tahmin Hatalarının Ortalamasının Karekökü (RMSEA)	0,044	RMSEA ≤ .08	Hu ve Bentler, 1999	Kabul Edilebilir
Karşılaştırılmalı Uyum İndeksi (CFI)	0,937	.90 ≤ CFI	Brown, 2015	Kabul Edilebilir
İyilik Uyum İndeksi (GFI)	0,890	.90 ≤ GFI	Hu ve Bentler, 1999	Kabul Edilebilir
Tucker-Lewis İndeksi (TLI)	0,930	.90 ≤ TLI	Hu ve Bentler, 1999	Kabul Edilebilir
Bollen's Artan Uyum İndeksi (IFI)	0,937	.90 ≤ IFI	Hu ve Bentler, 1999	Kabul Edilebilir

Tablo 4.23'te de görüleceği üzere GFI hariç diğer tüm değerler kabul edilebilir seviyededir. GFI değerinin düşüklüğünün en önemli sebebi bu değerin örneklem büyüklüğünden etkileniyor olmasıdır. Örneklem büyüklüğü arttıkça, GFI değerinin de artması söz konusu olacaktır (Jöreskog ve Sörbom, 1993; Bollen, 1990). Bu nedenle hem GFI değerinin olması gereken değere oldukça yakın olması (.89) aynı zamanda bu değerin sadece örneklem büyüklüğünden etkileniyor olması, mevcut değerden kaynaklı modelin olumsuz etkilenmeyeceğini düşündürtmüştür.

Toparlamak gerekirse "Ölçüm modelinin değerlendirilmesi" başlığı altında gerçekleştirilen tüm işlemlerle ölçüm modelinin benzeşim ve ayırt edici geçerliği sağladığı ortaya konmuş, bu nedenle de yapı geçerliliğinde herhangi bir problemin olmadığı tespit edilmiştir. Bu tespitin ortaya konmasının ardından çalışmaya yapısal modelin değerlendirilmesiyle devam edilmiştir.

4.5.2. Yapısal modelin değerlendirilmesi

Yapısal modelin değerlendirilmesi için önce modelin iyi uyum değerleri incelenmiştir. Yapısal modelin uyum iyiliği indekslerine yönelik sonuçlar ise Tablo 4.24'te gösterilmektedir. Yapısal modelin değerlendirilmesindeki bir sonraki aşama ise modele yönelik doğrudan ve dolaylı etkilere ait sonuçların incelenmesini kapsamaktadır. Yapısal modele ait doğrudan ilişki sonuçları Tablo 4.25'te ve dolaylı ilişki sonuçları ise

Tablo 4.26'da paylaşılmıştır. Bir sonraki adımda ise hipotez testlerinin sonuçlarına yer verilmiştir. Hipotez testlerine ait sonuçlar ise Tablo 4.27'da gösterilmiştir.

Tablo 4.27. *Yapısal modelin uyum iyiliği indekslerine yönelik sonuçlar*

Uyum İndeksleri	Mevcut Değer	Kabul Edilir Değer	Kaynak	Kabul Edilebilirlik
X^2 /df	2,392	$x^2/df \leq 5$	Hair, Black, Babin ve Anderson (2019)	Kabul Edilebilir
Tahmin Hatalarının Ortalamasının Karekökü (RMSEA)	0,045	RMSEA ≤ .08	Hu ve Bentler, 1999	Kabul Edilebilir
Karşılaştırılmalı Uyum İndeksi (CFI)	0,934	.90 ≤ CFI	Brown, 2015	Kabul Edilebilir
İyilik Uyum İndeksi (GFI)	0,887	.90 ≤ GFI	Hu ve Bentler, 1999	Kabul Edilebilir
Tucker-Lewis İndeksi (TLI)	0,927	.90 ≤ TLI	Hu ve Bentler, 1999	Kabul Edilebilir
Bollen's Artan Uyum İndeksi (IFI)	0,934	.90 ≤ IFI	Hu ve Bentler, 1999	Kabul Edilebilir
Standartlaştırılmış Hata Kareleri Ortalamasının Karekökü (SRMR)	0,048	SRMR ≤ .08	Hu ve Bentler, 1999	Kabul Edilebilir

Tablo 4.24'te görüldüğü üzere yapısal modele ait uyum indeksleri GFI değeri haricinde literatürde yer alan (Hair, 2019; Hu ve Bentler, 1999; Brown, 2015; Hu ve Bentler, 1999; Hu ve Bentler, 1999; Hu ve Bentler, 1999) kabul edilebilir değerleri içermektedir. Önceden de ifade edildiği gibi GFI değeri örneklem büyüklüğünde etkilenebilmektedir (Jöreskog ve Sörbom, 1993; Bollen, 1990). Buna rağmen değerin kabul edilebilir değere çok yakın olduğunu söylemem mümkündür. Bu sonuçlara göre yapısal modelin kabul edilebilir olduğu sonucuna varılmıştır. Bir sonraki adımda yapısal modele ilişkin doğrudan ve dolaylı etki sonuçları değerlendirilmiştir. Bu sonuçlar Tablo 4.25'te gösterilmektedir. Tablolarda yer alan kısaltmalar ise yapısal modele yönelik standardize edilmemiş beta katsayılarına (B), standardize edilmiş beta katsayılarına (ß), standart hatalara (SE), kritik oranlara (CR), anlamlılığa (p) işaret etmektedir.

Tablo 4.28. *Yapısal modele ilişkin doğrudan etkilere ait sonuçlar*

	İlişkiler	B	ß	S.H	CR	*p*
Doğrudan Etkiler	ALC ➔ AGE	0,351	0,317	0,07	5,029	***
	ALS ➔ AGE	0,486	0,383	0,083	5,865	***
	ALF ➔ AGE	-0,023	-0,032	0,025	-0,95	0,342
	AOY ➔ AGK	0,339	0,366	0,047	7,194	***
	ATY ➔ AGK	0,34	0,185	0,096	3,545	***
	ATM ➔ AGK	0,083	0,069	0,051	1,634	0,102
	ALC ➔ RKN	0,224	0,259	0,057	3,941	***
	ALS ➔ RKN	0,064	0,065	0,066	0,975	0,330
	ALF ➔ RKN	-0,149	-0,26	0,023	-6,554	***
	AOY ➔ RKN	0,008	0,015	0,025	0,322	0,747
	ATY ➔ RKN	0,036	0,034	0,05	0,723	0,470
	ATM ➔ RKN	0,088	0,127	0,028	3,119	0,002
	AGE ➔ RKN	0,255	0,327	0,041	6,214	***
	AGK ➔ RKN	0,055	0,095	0,024	2,332	0,020

p<0,05

Tablo 4.29. *Yapısal modele ilişkin dolaylı etkilere ait sonuçlar*

	Yapılar	B	ß	Alt Limit	Üst Limit	p
Dolaylı Etkiler	ALC ➔ AGE➔RKN	0,089	0,104	0,056	0,177	0,001
	ALS ➔ AGE ➔ RKN	0,124	0,125	0,071	0,201	0,000
	ALF ➔ AGE ➔ RKN	-0,006	-0,010	-0,03	0,007	0,339
	AOY ➔ AGK ➔ RKN	0,019	0,035	0,009	0,067	0,027
	ATY ➔ AGK ➔ RKN	0,019	0,018	0,005	0,041	0,016
	ATM ➔ AGK ➔ RKN	0,005	0,007	0,000	0,022	0,080

p<0,05

Tablo 4.25'te ve Tablo 4.26'da yer alan doğrudan ve dolaylı ilişkilere ait sonuçlar üç başlıkta ifade edilebilir:

- Doğrudan ilişkilere ait sonuçlara bakıldığında tehdit değerlendirmelerini içeren algılanan ciddiyet (ß=0,317; p<0,000) ve algılanan savunmasızlık (ß=0,383; p<0,000) ile gizlilik endişesi arasında pozitif ve anlamlı bir ilişki olduğu görülmüştür. Ancak algılanan faydanın ve gizlilik endişesi arasında (ß=-0,032; p<0,342) anlamlı bir ilişki bulunamamıştır. Öte yandan başa çıkma değerlendirmelerinde öz yeterlilik (ß=0,366; p<0,000) ve tepki yeterliliği (ß=0,185; p<0,000) ile gizlilik kontrolü arasında pozitif yönlü anlamlı bir ilişki söz konusuyken tepki maliyeti ile gizlilik kontrolü arasında (ß=0,069; p<0,102) anlamlı bir ilişki bulunamamıştır. Tehdit değerlendirmelerinden algılanan ciddiyet ile reklamdan kaçınma arasında pozitif yönlü (ß=0,259; p<0,000),

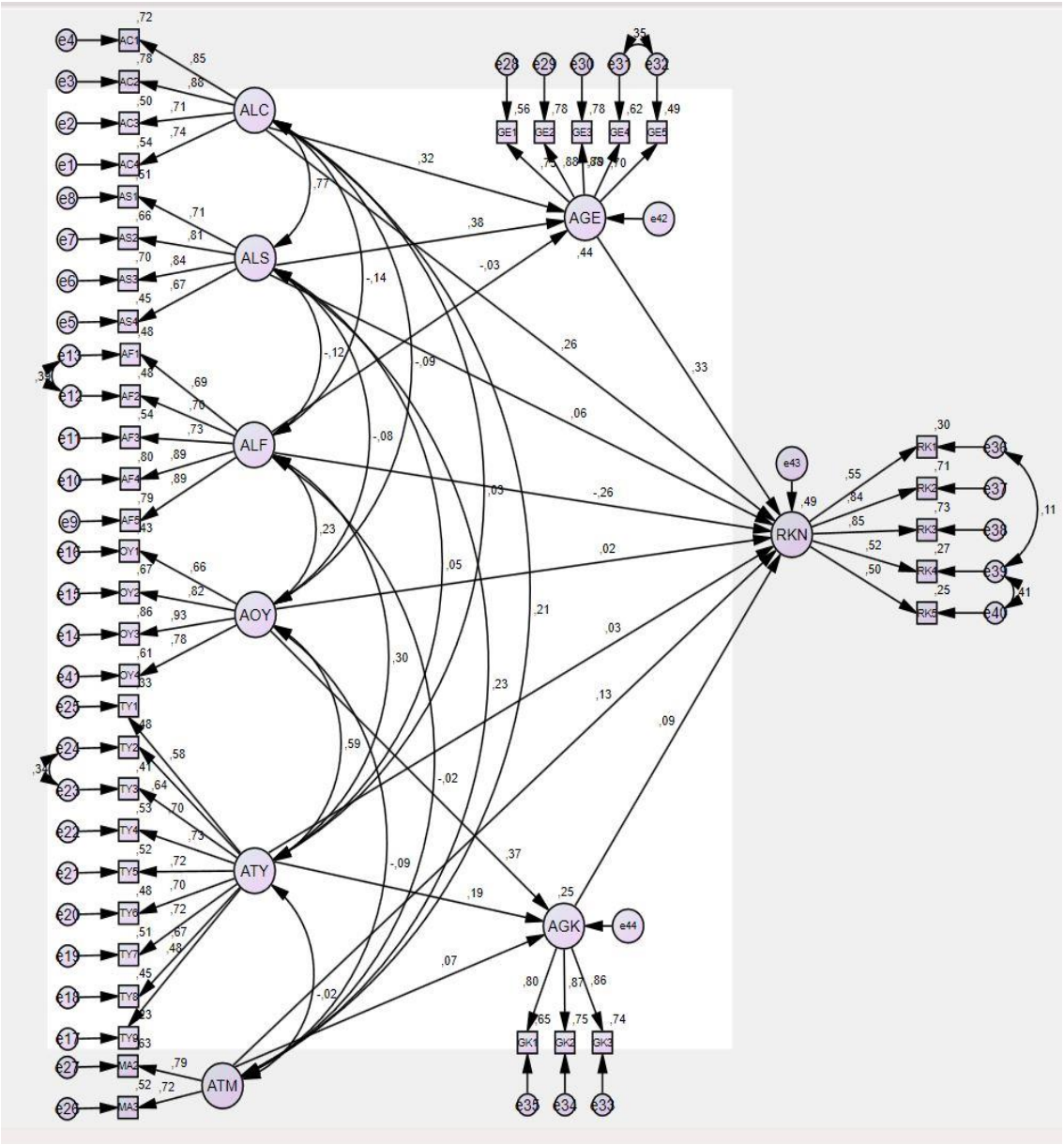
algılanan fayda ile reklamdan kaçınma arasında ise (ß=-0,26; p<0,000) negatif yönlü anlamlı bir ilişki bulunmuştur. Algılanan savunmasızlık ve reklamdan kaçınma arasında ise (ß=0,065; p<0,33) anlamlı bir ilişkinin olmadığı tespit edilmiştir. Başa çıkma değerlendirmelerinden öz yeterlilik (ß=0,015; p<0,747) ve tepki yeterliliği (ß=0,034; p<0,47) ile reklamdan kaçınma arasında anlamlı bir ilişki bulunamamış, tepki maliyeti ise reklamdan kaçınma arasında (ß=0,127; p<0,002) ise pozzitif yönlü anlamlı bir ilişki olduğu tespit edilmiştir. Gizlilik endişesi (ß=0,327; p<0,000) ve gizlilik kontrolünün (ß=0,095; p<0,02) ise reklamdan kaçınma üzerinde pozitif yönle anlamlı bir ilişkiye sahip olduğu görülmektedir.

- Dolaylı ilişkileri tespit edebilmek amacıyla Amos 24 üzerinde 5000 bootstrap örneklem seçme tekniği kullanılmıştır (Hair vd., 2019). Sonuçlara bakıldığında gizlilik endişesinin algılanan ciddiyet (ß=0,104; p<0,001) ve algılanan savunmasızlık (ß=0,125; p<0,000) ile reklamdan kaçınma arasındaki ilişkide dolaylı bir ilişki söz konusu olduğu görülmektedir. Algılanan fayda ve reklamdan kaçınma arasında ise gizlilik endişesinin (ß=-0,010; p<0,339) aracı bir rolü bulunamamıştır. Ayrıca gizlilik kontrolünün öz yeterlilik (ß=-0,035; p<0,027) ve tepki yeterliliği (ß=-0,018; p<0,016) ile reklamdan kaçınma arasındaki dolaylı bir ilişkiye sahip olduğu tespit edilmiştir. Gizlilik kontrolünün ise tepki maliyeti ve reklamdan kaçınma (ß=-0,007; p<0,080) arasındaki ilişkide dolaylı etkileri görülmemiştir.

Yukarıda ifade edilen bulgular ışığında hipotez testlerinin sonuçları Tablo 4.27'de gösterilmiştir.

Tablo 4.30. *Hipotez testine ait sonuçlar*

Hipotezler	**Sonuç**
H1 Algılanan ciddiyet ve gizlilik endişesi arasında pozitif bir ilişki vardır.	Kabul
H2 Algılanan savunmasızlık ve gizlilik endişesi arasında pozitif bir ilişki vardır.	Kabul
H3 Algılanan fayda ve gizlilik endişesi arasında pozitif bir ilişki vardır.	Ret
H4 Öz yeterlilik ve gizlilik kontrolü arasında pozitif bir ilişki vardır.	Kabul
H5 Tepki yeterliliği ve gizlilik kontrolü arasında pozitif bir ilişki vardır.	Kabul
H6 Tepki maliyeti ve gizlilik kontrolü arasında pozitif bir ilişki vardır.	Ret
H7 Gizlilik endişesi ve reklamdan kaçınma arasında pozitif bir ilişki vardır.	Kabul
H8 Gizlilik kontrolü ve reklamdan kaçınma arasında pozitif bir ilişki vardır.	Kabul
H9 Algılanan ciddiyet ve reklamdan kaçınma arasında pozitif bir ilişki vardır.	Kabul
H10 Algılanan savunmasızlık ve reklamdan kaçınma arasında pozitif bir ilişki vardır.	Ret
H11 Algılanan fayda ve reklamdan kaçınma arasında negatif bir ilişki vardır.	Kabul
H12 Öz yeterlilik ve reklamdan kaçınma arasında pozitif bir ilişki vardır.	Ret
H13 Tepki yeterliliği ve reklamdan kaçınma arasında pozitif bir ilişki vardır.	Ret
H14 Tepki maliyeti ve reklamdan kaçınma arasında negatif bir ilişki vardır.	Ret
H15 Algılanan ciddiyet ve reklamdan kaçınma arasındaki ilişkide gizlilik endişesinin aracılık rolü vardır.	Kabul
H16 Algılanan savunmasızlık ve reklamdan kaçınma arasındaki ilişki üzerinde gizlilik endişesinin aracılık rolü vardır.	Kabul
H17 Algılanan fayda ve reklamdan kaçınma arasındaki ilişki üzerinde gizlilik endişesinin aracılık rolü vardır.	Ret
H18 Öz yeterlilik ve reklamdan kaçınma arasındaki ilişki üzerinde gizlilik kontrolünün aracılık rolü vardır.	Kabul
H19 Tepki yeterliliği ve reklamdan kaçınma arasındaki ilişki üzerinde gizlilik kontrolünün aracılık rolü vardır.	Kabul
H20 Tepki maliyeti ve reklamdan kaçınma arasındaki ilişki üzerinde gizlilik kontrolünün aracılık rolü vardır.	Ret



Şekil 4.1. *Yapısal modelin testine ilişkin diyagram*

5. SONUÇ, TARTIŞMA VE ÖNERİLER

Çalışmanın son bölümü olan bu bölümde, araştırma bulgularına ait sonuçlar tartışılmış ve yeni çalışmalar için araştırma önerilerine yer verilmiştir.

5.1. Sonuç ve Tartışma

Özellikle son yirmi yıldaki dijital dönüşüm ile teknoloji ve internet kullanımı günlük yaşamın vazgeçilmez bir parçası haline gelmiştir. İnsanlar günlük aktivitelerinin çoğunu dijital araçlar aracılığı ile gerçekleştirmektedir. Bunlar arasında bilgi alma ve bilgi paylaşma, eğlence, sosyalleşme, alışveriş yapma gibi pek çok aktiviteyi saymak mümkündür. Dijital kullanımlar en başta bilgiye ulaşmada hem çok hızlı hem de ücretsiz alternatifler sunmaktadır. Ancak markalar açısından tüketici konumunda olan birey internet kullanımı sonucu elde ettiği faydaların yanı sıra dijital ayak izlerini bırakarak markaların ve reklam şirketlerinin tüketici profillerini daha kusursuz çıkarmalarına dolaylı da olsa katkı sağlamaktadır. İnternet kullanımındaki artış reklam yatırımlarının da geleneksel mecralardan internet mecrasına yönelmesine neden olmuştur. Tüketici verisinden de yararlanma imkânı yakalayan markalar reklamları artık daha fazla kişiselleştirilmiş olarak hazırlamaktadır. Tüketici verisine dayanan bu kişiselleştirilmiş reklamlar literatürde ÇDR olarak ifade edilmektedir.

ÇDR, bireysel internet kullanıcılarının hangi web sitelerini ziyaret ettikleri, orada ne kadar kaldıkları ve ne yaptıkları (ör: alışveriş; arama; gezinme) gibi çevrimiçi davranışsal verilerini izleyen ve derleyen bir tür dijital reklam hedefleme yöntemidir. Bu yöntem sayesinde internet reklam ağı şirketleri bireysel tüketicilerin özel ilgi alanlarını ve tercihlerini zamanında tahmin edebilmekte ve bunun sonucunda tüketicilere özel olarak hazırlanmış reklam mesajları iletebilmektedir (Ham, 2017).

ÇDR'nin etkilerine yönelik sonuçlar pazarlamacıları reklamları hedeflemeye ve kişiselleştirmeye daha fazla yatırım yapmaya teşfik etmektedir. Aynı zamanda akademik araştırmalar kişiselleştirilmiş reklamların dikkat, tutum, satın alma ve tıklama oranlarını olumlu yönde etkileyebileceğini göstermektedir. ÇDR'ye yönelik tutum araştırmaları insanların kişiselleştirilmiş reklamcılığın faydalı olabileceğini ve kişisel olarak daha alakalı ve bilgilendirici reklamlar görmenin özellikle satın alma deneyimindeki kolaylığı artırma ve daha fazla ekonomik fayda sağlayacağını düşündüklerini göstermiştir (Boerman vd., 2021). Bununla birlikte, insanlar gizliliğin ihlali, gözetim, kişisel verilerin kötüye kullanılması, ayrımcılık ve kontrol kaybı konusunda da endişe duymaktadır ve

bunun sonucunda ÇDR'nin tepkiye, reklamdan kaçınmaya, reklamı engellemeye ve daha az güvene yol açtığı gösterilmiştir (Varnalı, 2021).

ÇDR'ye yönelik bu iki keskin uç tüketicinin özellikle gizlilik endişeleri bağlamında hedafli reklamdan kaçınmada hangi motivasyonlarla hareket ettiğini anlamanın önemine işaret etmektedir. Bu nedenle bu çalışma ÇDR'den kaçınmada etkili olan faktörleri gizlilik endişesi ve gizliliği koruma motivasyonu çerçevesinde açıklamayı amaçlamaktadır. Bu amaç doğrultusunda KMT çerçevesinde geliştirilen araştırma modelinin sınanması ile elde edilen sonuçlar tehdit ve başa çıkma değerlendirmelerinin reklamdan kaçınma üzerindeki doğrudan ve dolaylı etkileriyle açıklanmaya çalışılmıştır.

Tüketicinin gizliliğe yönelik tehdit değerlendirmelerinin gizlilik endişesi üzerindeki doğrudan etkileri

Çalışma sonuçlarına göre tüketicinin ÇDR'ye yönelik tehdit değerlendirmelerinden algılanan ciddiyet (ß=0,317; p<,000) ve algılanan savunmasızlığın (ß=0,383; p<,000) gizlilik endişesi üzerinde doğrudan pozitif bir etkiye sahip olduğu ortaya konmuştur. Dolayısıyla ilgili hipotezler (H1 ve H2) kabul edilmiştir. Ancak tehdit değerlendirmelerinden algılanan faydanın gizlilik endişesi üzerinde bir etkiye sahip olmadığı görülmüştür (ß=-0,032; p<,342). Bu sonuç karşısında kurulan hipotez (H3) reddedilmiştir.

Tüketicinin kişisel verilerin gizliliğine yönelik algıladığı riskler gizlilik endişesini doğrudan arttırmaktadır. KMT'ye göre tüketici öncelikle kişisel verilerin kullanılmasından doğacak risklerin ciddiyetini yani önem derecesini değerlendirir. Eğer tüketici bu riskleri önemli bir risk olarak algılar ve bu risklerden doğacabilecek bir zarara karşı kendini savunmasız hissederse gizlilik endişesi oluşacaktır. Kişisel verilerin kullanılmasından doğacak riskler genellikle belirsizdir ve bu belirsizlik tüketicide gizliliğe yönelik endişeleri tetiklemektedir. Önceden de ifade edildiği gibi ÇDR'nin kişiyi tanımlayan bilgileri toplamadığı sadece davranışsal verileri kullandığı ifade edilmektedir. Ancak çok fazla verinin toplanması kişiyi tanımlanabilir hale getirmektedir. Bu durumda kişi kendini riskler karşısında savunmasız hissedebilir. ÇDR bu nedenle kişisel verileri izleyen, toplayan, kullanan ve paylaşan bir reklam sistemi olarak algılandığında tüketicide gizliliğe yönelik endişeleri açığa çıkarmaktadır. Bu endişeler dijital davranışların izlenmesinden doğan anonimliğin kaybolması, çok fazla kişisel veririnin toplanmasından kaynaklanan kişiyi tanımlanabilir hale getirme olasığının kesinleşmesi,

kişisel verilerin kötüye kullanılma ihtimali ve kişisel verilerin paylaşılmasından kaynaklanan gizlilik ihlalleri olarak ifade edilebilir. Literatürdeki çalışmalar riske yönelik algılanan ciddiyet ve algılanan savunmasızlığın gizlilik endişesini arttırdığını göstermektedir (Lwin vd., 2007; Youn, 2009; Mohamed ve Ahmad, 2012; Aguirre vd., 2015; Ham, 2017; Mousavi vd., 2020). Bu araştırmanın sonuçları da literatürde belirtilen çalışma sonuçlarıyla örtüşmektedir.

ÇDR'ye yönelik algılanan faydanın ise gizlilik endişesi üzerinde negatif bir etkisi bulunamamıştır. ÇDR'ye yönelik algılanan fayda reklamın tüketicinin ilgi alanına yönelik iletilmesini ifade eder. ÇDR, dijital ortamda tüketiciyi takip ettiği ve kişisel verilerini kullandığından, reklamın içeriğinin tüketiciler tarafından daha alakalı olarak algılanması muhtemeldir ve bu da sonuç olarak reklamdan beklenen etkiyi arttırmaktadır (De Keyzer vd., 2022; Özçelik ve Varnalı, 2019; Jung, 2017). Reklamı daha etkili ve faydalı gören tüketicinin ÇDR'ye yönelik gizlilik endişelerinin azalacağı varsayılmıştır. Bu sonuç literatürdeki bazı çalışmalarla (Ham, 2017; Youn, 2009) benzerlik göstermezken bazı çalışmalarla (Mohamed ve Ahmad, 2012) benzerlik göstermektedir. Tüketicinin reklamı faydalı bulmasının reklam etkinliğini arttırdığı ve kaçınmayı azalttığı bilinmektedir. Bu çalışmada da algılanan faydayla reklamdan kaçınma arasında negatif bir ilişki olduğu tespit edilmiştir (ß=-0,260, p<,000). Bu sonuç ile ilgili hipotez (H11) kabul edilmiştir. Bu durumda tüketicinin reklamı faydalı bulması kaçınma davranışına doğrudan etkiliyken gizlilik endişesini etkilememektedir. Literatüre tüketicinin reklama yönelik olumlu ve olumsuz tutumları bir arada hissediği ifade edilmektedir. ÇDR'ye yönelik tüketici tutumları araştırmalarında reklamı faydalı bulan tüketicinin reklamı kabul davranışlarında olumlu sonuçlar olduğu görülmüştür (Smit vd., 2014; Aguirre vd., 2015). Bu durumda tüketicinin reklamdan kaçınma üzerindeki etkisi sadece gizlilik endişesi ile değil aynı zamanda reklama yönelik fayda ile de ilgilidir. Gizlilik literatürüne göre kişisel verinlerin reklam şirketlerinin kullanımına izin verilmesi sonucu tüketici bazı faydalar elde ettiğine inanıyorsa gizliliği korumaya yönelik motivasyonları azalacaktır (Phelps vd., 2000; Sheehan ve Hoy, 2000) ancak gizlilik endişesinin artması ya da azalması söz konusu olmayabilir. Sonuç olarak tüketici koruma motivasyonlarını harekete geçirirken ÇDR'yi hem risk hem de fayda açısından değerlendirmektedir. ÇDR bir tüketici için hem faydalı hem de riskli algılanabilir ancak reklamdan kaçınma niyetlerini riskin faydadan daha yoğun bir şekilde hissedilmesi belirlemektedir. Yapısal modelin sonuçlarına bakıldığında tehdit değerlendirmelerini ifade eden bütün

değişkenlerin gizlilik endişesine yönelik R^2 katsayısı 0,44 olarak hesaplanmıştır. Bu sonuçla tehdit değerlendirmelerini oluşturan değişkenlerin gizlilik endişesini % 44 düzeyinde açıkladığı görülmektedir.

Tüketicinin gizliliğe yönelik başa çıkma değerlendirmelerinin gizlilik kontrolü üzerindeki doğrudan etkileri

KMT'ye göre koruma motivasyonunun davranışa dönüşmesi için bireyin riski önlemeye yönelik bazı yeterlilikleri değerlendirmesi gerekmektedir. Gizlilik endişesi bağlamında bunlar çevrimiçi gizliliği korumaya yönelik öz yeterlilikler, önerilen tepkinin yeterliliği ve bu tepkiyi göstermenin getireceği maliyetler olarak belirtilmiştir. KMT aynı zamanda tehdit değerlendirmelerini korku, başa çıkma değerlendirmelerini ise kontrol süreçleri olarak ifade eder. Bu durumda bireyin başa çıkmaya yönelik değerlendirmeleri algılanan kontrolü belirlemektedir. ÇDR bağlamında öz yeterliliğin gizlilik kontrolünü pozitif yönde etkilediği tespit edilmiş (ß=0,366; p<,001) ve ilgili hipotez (H4) kabul edilmiştir. KMT bağlamında ele alınan çalışmalarda öz yeterlilik çoğunlukla gizlilik endişesinin bir öncülü olarak ele alınmıştır. Bazı çalışmalar öz yeterlilik ve gizlilik endişesi arasında pozitif bir ilişki olduğu sonucuna ulaşırken (Mohamad ve Ahmad; Ham), bazı çalışmalar ise öz yeterliliğin gizlilik endişesi arasında negatif bir ilişki olduğunu (Youn, 2009; Zhang vd., 2018) tespit etmişlerdir. Öz yeterliliğin gizlilik endişesi üzerindeki farklı sonuçları kaçınma üzerindeki ilişkisinin farklı değişkenlerle açıklanabileceğini gösterebilir. KMT bağlamında öz yeterlilik korku süreçleri yerine kontrol süreçlerinin bir parçasıdır. Öz yeterliliğin yüksek olması koruma davranışının gerçekleşmesine neden olur. Bu durumda öz yeterliliğin artması algılanan gizlilik kontrolünün de artmasına sebep olacaktır. Bu sonuçlar teori ile örtüşmektedir (Roger, 1975; Roger, 1983). Koruma motivasyonları bağlamında bir tüketicinin ÇDR'den kaçınma niyetlerinde ele alınan öz yeterlilik, tüketicinin gizliliği korumaya yönelik başa çıkma değerlendirmelerinden birini ifade etmektedir. Bu sonuçlara göre gizliliği bir tehdit olarak algılayan tüketicinin reklamdan kaçınmaya yönelik öz yeterliliği olduğuna dair inançları arttırkça reklamların kişisel verilerini kullanmasını önlemeye yönelik kontrollerin kendisinde olduğunu düşünmektedir.

Başa çıkma değerlendirmelerinden tepki yeterliliği ve gizlilik kontrolü arasında pozitif yönlü bir ilişki olduğu (ß=0,185; p<,001) tespit edilmiştir. Bu durumda ilgili hipotez (H5) kabul edilmiştir. ÇDR bağlamında tepki yeterliliği, reklamların dijital

davranışları izlemesi ve kişisel verileri reklam amaçlı kullanmasını önlemeye yarayan araçların ne derece etkili olduğuna dair inançları ifade eder. Çerezleri engelleme, reklamları engelleyen araçlar kullanma (örn: AdBlock), gizliliği arttıran bazı yazılımları kullanma (örn: Ghostery) ya da reklam şirketlerinin dijital davranışları izlemesini önlemek için ÇDR sisteminden çıkma seçeneklerini kullanma gibi çeşitli araçların varlığı tüketicide algılanan gizlilik kontrolünü arttırmaktadır. Literatürde gizlilik kontrolü ve gizlilik endişesi ilişkisine bakıldığında, tüketicilere hangi bilgilerin toplandığı ve nasıl kullanıldığını açıklamak (örn; gizlilik politikaları ile); reklam çerezlerini kabul etmemek, ya da çerez sisteminden çıkmak gibi kontroller verildiğinde endişenin azalacağı düşünülür. Bu düşünce çalışmalarda algılanan kontrol ve gizlilik endişesi arasında negatif bir ilişkisi olduğu sonuçlarıyla desteklenmiştir (Xu vd., 2011; Dinev ve Hart, 2004; Morimoto, 2021). Bu sonuç bize tepki yeterliliklerine olan inancın gizlilik kontrolü algısını arttırdığını göstermektedir.

Son olarak tepki maliyeti değişkeni ile gizlilik kontrolü arasında negatif yönlü anlamlı bir ilişki bulunamamış (ß=0,069; p<,102) ve ilgili hipotez reddedilmiştir (H6). Gizliliği korumaya yönelik tepkilerin alınması zaman ve bilinç düzeyi açısından tüketiciye zorluk yaratabilmektedir. Öncelikle bu kontrollerin alınabilmesi çeşitli teknik bilgilerin gerekliliğine işaret eder. Üstelik internet üzerinde gizliliği korumaya yönelik her araç ya da platform için farklı uygulamalar söz konusu olabilmektedir. Bu durumda tüketici zihinsel bir yorgunluk olarak bu işlemleri yapmayı maliyetli görebilir. Ayrıca gizlilik politikaları gibi uygulamalar çok uzun ve karmaşık olduğundan her bir kullanımda bunların okunması zamansal açıdan bir maliyet yaratmaktadır (Milne ve Culnan, 2004). Bu durumda tüketicilerin maliyet algısı ile gizlilik kontrolü algısı arasında negatif bir ilişki olacağı varsayılmıştır. KMT bağlamında maliyetler doğrudan davranışla ilişkilendirilir. Bu durumda maliyetin kontrol üzerinde bir etkisi yerine doğrudan davranış üzerine bir etkisinin olması söz konusu olabilir. Ancak tepki maliyeti ve reklamdan kaçınma arasındaki doğrudan ilişkiye bakıldığında (ß= 0,127; p<,002) bu ilişkinin anlamlı ancak pozitif bir ilişki olduğu görülmüştür. Bu durumda ilgili hipotez (14) reddedilmiştir. Bunun nedeni tepki maliyeti arttıkça reklamdan kaçınma niyetlerinin de artmasında tepki maliyetlerinin olumsuz bir tutuma neden olma ihtimali olabilir. Bu durumda tepki maliyeti reklamdan bilişsel ya da duygusal kaçınma sonuçları ile örtüşmüş olabilir. Algılanan maliyetler arttıkça kişinin reklamdan hoşlanmaması ve onu görmezden gelmesi mümkün olabilir. Ancak davranışsal kaçınma ile arasında negatif bir ilişki

beklenmektedir. Bu durumda algılanan maliyetlerin reklamdan kaçınma boyutlarıyla farklı ilişkilerinin olabileceğinden söz etmek de mümkündür. Ayrıca burada karşılaşılan alfa hatasının (Tip 1) örneklem büyüklüğünden de kaynaklanması muhtemeldir.

Yapısal modelin sonuçlarına bakıldığında başa çıkma değerlendirmelerini ifade eden bütün değişkenlerin gizlilik kontrolüne yönelik R^2 katsayısı 0,25 olarak hesaplanmıştır. Bu sonuçla başa çıkma değerlendirmelerini oluşturan değişkenlerin gizlilik kontrolünü % 25 düzeyinde açıkladığı görülmektedir.

Gizlilik endişesinin reklamdan kaçınma üzerindeki doğrudan ve dolaylı etkileri

ÇDR'ye yönelik literatürün çok büyük bir kısmını gizlilik ve gizlilik endişesine yönelik tartışmalar oluşturmaktadır. Çoğu çalışmada ÇDR'nin tüketiciler için faydalı olarak algılansa da çoğunlukla gizlilik endişelerini beraberinde getirdiği ve tüketicide negatif tepkilere yol açtığı görülmüştür (Turow vd., 2009; McDonald ve Cranor, 2010a; Ur vd., 2012; Smit vd., 2014; Moore vd, 2015; Fachryto ve Achyar, 2018; Boerman vd., 2017; Varnalı, 2021). Bu çalışmada özellikle gizlilik endişesinin reklamdan kaçınma ile olan iliksini açıklamak için endişeye neden olan değişkenlerin belirlenmesi ve bu değişkenlerle reklamdan kaçınma arasında gizlilik endişesinin nasıl bir rolü olduğunu anlamak amaçlanmıştır. Bu durumda gizliliği önemli bir sorun olarak görmek ve gizlilik risklerine karşı savunmasızlık hissi tüketicideki gizlilik endişelerini açıklayan iki değişken olarak görülmektedir. Bunun sonucunda doğan endişesi ise tüketicide reklamdan kaçınma niyetlerini pozitif yönde arttırmaktadır (ß=0,327; p<,000). Bu durumda ilgili hipotez (H7) kabul edilmiştir. Gizlilik endişesinin reklamdan kaçınma üzerindeki pozitif etkisi literatürdeki çalışmalarla (Baek ve Morimoto, 2012; Li ve Huang, 2016; Ham, 2017; Cho vd., 2020; Aiolfi vd., 2021) benzerlik göstermektedir.

Literatürde ÇDR'ye yönelik tepkiler genellikle gizlilik muhasebesi teorisi üzerinden açıklamaktadır (Dinev ve Hart, 2004; Dinev ve Hart, 2006; Youn ve Shin, 2020). Bu bakış açısı ile risk ve fayda analizi yapan tüketici reklamı kabul ya da ret davranışına karar vermektedir. KMT bağlamında ise ÇDR'ye yönelik risklerin reklamdan kaçınma üzerindeki etkisi gizlilik endişesinin aracılık rolü ile açıklanmaktadır. Gizlilik endişesinin tehdit değerlendirmeleri ve reklamdan kaçınma arasındaki aracılık etkisinin incelenmesi sonucunda elde edilen bulgulara göre gizlilik endişesinin algılanan ciddiyet ve reklamdan kaçınma arasında aracılık etkisi olduğu tespit edilmiştir (ß=0,104; alt limit=,056; üst limit=,177; p<,001). Bu sonuca göre ilgili hipotez (H15) kabul edilmiştir.

Algılanan ciddiyetin reklamdan kaçınma üzerinde ise pozitif bir etkiye sahip olduğu (ß=0,259; p<,000) tespit edilmiştir. Bu sonuca göre ilgili hipotez (H9) kabul edilmiştir. Algılanan ciddiyetin reklamdan kaçınma üzerindeki doğrudan etkisi ise bize gizlilik endişesinin bu ilişkide kısmı bir aracılık etkisine sahip olduğunu göstermektedir.

Literatürde gizliliğe yönelik algılanan ciddiyet ile kaçınma davranışı arasında pozittif bir ilişki olduğunu gösteren çalışmalar söz konusudur (LaRose vd., 2005; Crossler, 2010; Youn, 2005; Strycharz vd., 2019). Ayrıca riske yönelik algılanan ciddiyet gizlilik endişesini arttırmaktadır (Mohamed ve Ahmad, 2012; Ham, 2017). Bu durumda çalışmada elde edilen bulguların ilgili literatürle örtüştüğü görülmektedir. Riske yönelik algılanan ciddiyet reklamdan kaçınmayı arttırmakta ve bu durum aynı zamanda gizlilik endişesi üzerinden gerçekleşmektedir.

Riske yani tehdide yönelik bir diğer değerlendirme olan algılanan savunmasızlığın reklamdan kaçınma niyeti üzerindeki etkisinde gizlilik endişesinin aracılık rolü olduğu tespit edilmiştir (ß=0,125; alt limit=,060; üst limit=,218; p<,000). Bu sonuç ile ilgili hipotez (H16) kabul edilmiştir. Algılanan savunmasızlığın reklamdan kaçınma üzerinde ise pozitif bir etkiye sahip olmadığı (ß=0,065; p<,330) tespit edilmiştir. Bu sonuca göre ilgili hipotez (H10) reddedilmiştir. Bu sonuç bize gizlilik endişesinin algılanan savunmasızlık ve reklamdan kaçınma arasında tam aracılık etkisine sahip olduğunu göstermektedir. Literatürde algılanan savunmasızlığın gizlilik endişesini arttırdığı görülmüştür (Youn, 2009; Mohamed ve Ahmad, 2012, Ham, 2017; Mousavi vd., 2020). Bu çalışmada elde edilen sonuçlar literatürü destekler niteliktedir. Algılanan savunmasızlığın reklamdan kaçınma üzerindeki etkisi ise gizlilik endişesinin aracılık etkisiyle açıklanmıştır.

Son olarak algılanan fayda ile reklamdan kaçınma niyeti arasında gizlilik endişesinin aracı bir etkisi olmadığı tespit edilmiştir (ß=-0,010; alt limit= -,030; üst limit=,007; p<,339). Bu sonuç karşısında ise ilgili hipotez (H17) reddedilmiştir. Bu durum daha öncede ifade edildiği gibi tüketicinin gizliliğe yönelik endişesi olsa bile reklamın faydalarından dolayı reklamdan kaçınma niyetinin azalması ile açıklanabilir.

Gizlilik kontrolünün reklamdan kaçınma üzerindeki doğrudan ve dolaylı etkileri

Algılanan gizlilik kontrolü, bireyin kişisel bilgilerinin açıklanmasını ve yayılmasını yönetme becerisine ilişkin inançları olarak tanımlanır (Xu vd., 2011). KMT bağlamında bu inançlar ne kadar yüksekse koruma motivasyonları ve davranışları da o kadar yüksek

olmaktadır. ÇDR bağlamında tüketicinin gizliliği korumaya yönelik kontroller üzerindeki algısı ile reklamdan kaçınma arasında pozitif bir ilişki olduğu varsayılmıştır. Gizlilik kontrolü ve reklamdan kaçınma arasındaki ilişkiye bakıldığında (ß=0,095; p<,020) anlamlı ve pozitif yönlü bir ilişkinin varlığı tespit edilmiştir. Bu sonuç doğrultusunda ise ilgili hipotez (H8) kabul edilmiştir. Bu sonuç literatürdeki ilgili bazı çalışmalarla (örn: Whon vd., 2015; Youn ve Kim, 2019a; Kelly vd., 2021) benzerlik göstermektedir. Literatürde gizliliğe yönelik kontrollerin artması koruma davranışının azalttığını ifade eden çalışmalarlar da söz konusudur. Bireyler belirli kontrollere sahip olduğunda gizlilik endişeleri azalacağıdan korumaya yönelik davranışları azaltarak kişisel verileri paylaşmaya daha yatkın olmaktadır (örn: Morimoto, 2021). Bu araştırmanın sonuçları bu araştırmaladan farklı olarak kontrolün reklamdan kaçınmayı arttırdığını göstermiştir.

Gizlilik kontrolünün başa çıkma değerlendirmeleri ve reklamdan kaçınma arasındaki dolaylı etkilerine bakıldığında öz yeterlilik ve reklamdan kaçınma arasında arcılık etkisi olduğu (ß=0,035; alt limit=,009; üst limit=,067;p<0,02) görülmüştür. Bu sonuç üzerine ilgili hipotez (H18) kabul edilmiştir. Öz yeterliliğin reklamdan kaçınma arasındaki doğrudan etkisinin ise (ß=0,015; p<,747) anlamsız olması sonucu ilgili hipotez (H12) reddedilmiştir. Öz yeterlilik ve reklamdan kaçınma arasındaki doğrudan ilişkinin anlamsız olması ise bize gizlilik kontrolünün bu ilişkide tam aracı rolü olduğunu göstermektedir. ÇDR literatüründe öz yeterlilik gizlilik endişesinin bir öncülü olarak ya da kaçınma davranışına doğrudan etkileri ile incelenmiştir. KMT bağlamında öz yeterliliğin reklamdan kaçınma ile ilişkisinde gizlilik kontrolünün aracı etkisine bakan bir çalışmaya rastlanmamıştır. Önceden de bahsedildiği gibi öz yeterlilik çoğunlukla doğrudan davranış üzerindeki etkisi ya da gizlilik endişesi üzerindeki etkisiyle ele alınmıştır. Örneğin, Boerman vd. (2018) öz yeterliliğin internette gizliliği koruma davranışları üzerinde etkisi olmadığını tespit etmiştir. Bu durumda öz yeterlilik ve kaçınma arasındaki ilişki gizlilik kontrolü ile açıklamak bu literatür ile örtüşmektedir.

Gizlilik kontrolünün tepki yeterliliği ve reklamdan kaçınma üzerindeki dolaylı etkisine bakıldığında (ß=0,018; alt limit=,005; üst limit=,041;p<0,01) bir aracılık etkisinin olduğu tespit edilmiştir. Bu sonuç üzerine ilgili hipotez (H19) kabul edilmiştir. Tepki yeterliliğinin reklamdan kaçınma üzerindeki doğrudan etkisi ise anlamsızdır (ß=0,034; p<0,47). Bu durumda ilgili hipotezin (H13) reddedilmesi gizlilik kontrolünün tepki yeterliliği ve reklamdan kaçınma arasındaki ilişkiye tam aracılık ettiğini göstermektedir. KMT bağlamında tepki yeterliliği çok az çalışmada incelenmiştir

(Boerman vd., 2018, s. 7). Çalışmalarda genellikle tepki yeterliliği koruma davranışına etkisi üzerinden açıklanmıştır (Lee vd.,2008; Chenoweth vd., 2009; Boerman vd., 2018). Bir riske yönelik tepkilerin yeterliliğine olan inanç yüksekse kişinin o davranışı gerçekleştirmesi de yüksektir. ÇDR'den kaçınma bağlamında ise kişilerin hangi tepkileri verdiğinde gizliliklerini koruyacağı ve reklamdan kaçınacağı belirsiz olduğundan tepki yeterliliğini ölçmenin zor olacağı düşünülür (Smit vd., 2014; Ham, 2017). KMT bağlamındaki çalışmalarla bu sonuçlar örtüşmektedir. Bu çalışmada ise tepki yeterliliğinin davranışa etkisi gizlilik kontrolü üzerinden doğrulanmıştır.

Son olarak ise tepki maliyeti ve reklamdan kaçınma niyeti arasında gizlilik kontrolünün aracılık etkisine rastlanmamıştır. Dolaylı ilişkilerin anlamsız olması (ß=0,007; alt limit=,000; üst limit= ,022; p<0,080) sonucunda ilgili hipotez (H20) reddedilmiştir. KMT bağlamında tepki maliyetleri artarsa korumaya yönelik davranışlar azalacaktır. Bu durumda tepki maliyeti arttıkça algılanan kontrollerin düşmesi ve reklamdan kaçınma niyetinin azalması beklenmektedir. Bu durumun bir sebebi tüketicinin tepki maliyetlerine yönelik algısının gizlilik kontrolü ile birlikte gizlilik endişesini tetiklediği ve reklamdan kaçınma arasında pozitif bir ilişkiye sebep olabileceğini gösterebilir. Araştırma hipotezlerinin sonuçları yukarıda belirtilen açıklamaların dışında örneklem türü ve sayısından, kültürel özelliklerden, katılımcıların konuya yönelik bilgi seviyelerinden ve de demografik ve kişilik özelliklerinden etkilenmiş olabilir.

Sonuç olarak ÇDR'den kaçınmayı etkileyen faktörleri belirlemek adına KMT bağlamında oluşturulan yapısal modelin bu fenomeni açıklamada iyi uyum değerlerine sahip olduğu ve çalıştığı görülmüştür. ÇDR'den kaçınmada etkili olduğu düşünülen gizlilik endişesi ve gizlilik kontrolünün reklamdan kaçınma ile pozitif yönlü anlamlı etkileri doğrulanmıştır. Bu iki değişkenin reklamdan kaçınma üzerindeki etkileri için hesaplanan R^2 katsayısı 0,494 olarak tespit edilmiştir. Bu sonuç bize gizlilik kontrolü ve gizlilik endişesinin ÇDR'den kaçınmanın % 49'unu açıkladığını göstermektedir.

Literatüre bakıldığında araştırma sonuçlarının üç önemli bulgusundan söz edilebilir. Bunlardan ilki gizlilik endişesi ve gizlilik kontrolünün reklamdan kaçınma üzerindeki doğrudan ve dolaylı etkilerinin KMT bağlamında kanıtlanmasıdır. İkinci önemli sonuç ise başa çıkma değerlendirmelerinin KMT bağlamındaki işleyiş sürecinin gizlilik kontrolü değişkeni üzerinden açıklanmasıdır. Genel ÇDR literatüründe önceden de bahsedildiği gibi tüketicinin başa çıkma değerlendirmelerini ölçmek genellikle zordur

ve bu nedenle ölçülmemiştir. Ancak reklamdan kaçınma bağlamında bu çalışmada bu değişkenler gizlilik kontrolü üzerinden ele alınmış ve gizlilik kontrolünün aracılığı ile reklamdan kaçınmaya etkisi kanıtlanmıştır. KMT'nin bilişsel süreçlerine eklenen gizlilik kontrolü değişkeni sonuç olarak başa çıkma değişkenlerinin davranışa yönelik motivasyonları açıklamada başarılı olduğunu gösterir. Kısacası tüketicinin ÇDR'den kaçınmada iki bilişsel süreçle hareket ettiğini söylemek mümkündür. Bu süreçler korku ve kontrol süreçleri olarak ifade edilebilir. Eğer bir tüketici gizliliğe yönelik endişelere sahipse korku süreçlerini harekete geçirmektedir. Aynı şekilde gizliliği korumaya yönelik yeterliliklere sahip olduğunu düşünürse de kontrol süreçlerini harekete geçirerek ÇDR'den kaçınma niyetlerini oluşturacaktır. Son olarak ise ÇDR literatüründe tüketicilerin gizlilik endişesi bağlamında ÇDR'den kaçınma niyetlerinin kültürel faktörlerden de etkilendiği ve bu bağlamda bireysel kültüre sahip batı toplumlarında kolektif kültüre sahip olan doğu toplumlarına göre gizliliğe daha fazla önem verdiğine yönelik çıkarımlar söz konusudur. Bu araştırmanın sonuçları kültürel bağlamda kollektif bir toplum olan ülkemizde de tüketicilerin gizliliklerine önem verdiğini ve gizlilik endişesinin reklamdan kaçınma niyetlerini pozitif yönde etkilediğini göstermektedir.

Kişisel verilere dayalı hedefleme son yıllarda reklamcılık alanında sıkça kullanılmaktadır. Reklam görüntüleme ya da tıklama sonuçlarındaki olumlu geri dönüşler markaları bu reklam türüne daha fazla yönlendirmektedir. Ancak aynı zamanda gizlilik üzerinde daha fazla bilinçlenmeye başlayan tüketicinin gizliliği koruma motivasyonlarının da arttığı görülmektedir. Tüketiciler reklamların gizliliği tehdit ettiğini hissediklerinde gizliliği korumaya yönelik motivasyonları harekete geçirmeye ve reklamdan kaçınmaya daha fazla yaklaşmaktadır.

5.2.Öneriler

Bu çalışmanın amacı gizlilik endişesi bağlamında ÇDR'den kaçınmada etkili olan koruma motivasyonlarının etkisinin incelenmesidir. Bu bağlamda yararlanılan KMT ile yapısal bir model oluşturularak test edilmiş ve elde edilen araştırma sonuçlarının hem teorik hem de niceliksel bağlamda literatüre katkı sağlaması amaçlanmıştır.

Öncelikle çalışmanın bulguları gizlilik endişesi ve gizlilik kontrolünün reklamdan kaçınma üzerindeki etkilerini desteklemiştir. Bunun yanı sıra tehdit değerlendirmelerinden algılanan ciddiyet ve algılanan savunmasızlığın gizlilik endişesi üzerinde doğrudan bir etkisi olduğu aynı zamanda da aracılık etkisine sahip olduğu tespit

edilmiştir. Ancak algılanan fayda değişkenin kaçınma üzerinde sadece doğrudan bir etkisi vardır. Başa çıkma değerlendirmelerinden öz yeterlilik ile tepki yeterliliğinin ise gizlilik kontrolü üzerinde doğrudan bir etkisi olduğu ancak tepki maliyetlerinin gizlilik kontrolü üzerinde bir etkisi olmadığı görülmüştür. Bunun yanı sıra öz yeterlilik ve tepki yeterliliği ile reklamdan kaçınma ilişkisinde gizlilik kontrolünün aracı etkileri söz konusuyken tepki maliyetinin aracı etkisine rastlanmamıştır. Korku ve kontrol süreçleri olarak bilinen KMT'nin iki bilişsel süreci ÇDR bağlamında reklamdan kaçınmanın etkisini ölçmek için uyarlanmıştır. Bu sonuçlar bize tüketicinin iki bilişsel süreci değerlendirerek reklamdan kaçınmaya karar verdiğini öne süren araştırma yapısını doğrulamaktadır.

Bu araştırma belirli sınırlılıklara sahiptir. Bu nedenle hem bu sınırlılıklar hem araştırma sonuçları dahilinde sonraki araştırmalara bazı önerilerde bulunulmuştur. Bunlardan ilki araştırmanın ÇDR'den kaçınmayı gizlilik endişesi özelinde KMT bağlamında incelemesidir. Gizlilik endişesi ve reklamdan kaçınma ilişkisi farklı teorilerle de incelenebilir. Farklı teorik yaklaşımlar konunun daha ayrıntı anlaşılmasına katkı sağlayacaktır.

Bu modelin farklı örneklem üzerinde ve farklı kültürlerde test edilmesi sonuçların karşılaştırılmasına katkı sağlayacaktır. Bunun yanı sıra algılanan fayda ve algılanan maliyet değişkenlerinin aracı etkisi yerine moderatör etkisine bakılarak model yeniden test edilebilir. Bu çalışmada kolayda örneklem yöntemi kullanılmıştır. Bu nedenle daha homojen ve spesifik örneklem yöntemleri kullanmak çalışmanın genellenebilirliğini sağlamak açısından önemli görülmektedir. Ayrıca bu çalışmada elde edilen sonuçlar davranışsal niyetleri içermektedir. Deneysel çalışmalarla tüketicinin gerçek davranışlarının incelenmesi fenomenin daha iyi anlaşılmasına fayda sağlayacaktır. Literatürde tüketicinin gizliliğe yönelik algıları ile reklama yönelik gerçek tepkilerinin aynı olmadığı gizlilik paradoksu olarak ifade edilmektedir. Araştırma modelinin gerçek davranışların incelendiği bir araştırmada yeniden test edilmesi gizlilik paradoksu bağlamında davranışsal niyetlerle gerçek davranışların karşılaştırılmasına olanak tanıyacaktır.

KMT'nin reklamdan kaçınma üzerindeki etkilerinin daha iyi anlaşılması için değişkenler arasındaki ilişkiye bakılabilir. Özellikle kontrol ve endişe süreçlerinin birbiri ile olan ilişkisi sonucunda kaçınma davranışına yönelik daha net bilgilere ulaşılabilir. Bunun yanı sıra ÇDR ve gizlilik endişesi arasındaki ilişkinin davranışlara olan yansımasını daha net anlayabilmek için daha fazla nitel çalışmanın yapılması yararlı

görülmektedir. Nitel çalışmalar araştırmacıya yeni nedensel ilişkiler kurması için öncülük edebilir ya da nicel araştırmaların sonuçlarının daha iyi anlaşılmasına olanak tanır.

Bu çalışmada ÇDR'ye yönelik kaçınma genel bir çerçeveden ele alınmıştır. Daha sonraki araştırmalarda bir reklama yönelik kaçınma davranışı deneysel olarak test edilebilir. Bu durumda farklı reklam türlerine yönelik ve farklı mecralar üzerinde araştırmalar (sosyal medya, mobil vb.) ve karşılaştırmalı analizler reklamdan kaçınmada koruma motivasyonlarının nasıl çalıştığını anlamamıza yardımcı olacaktır.

Bu çalışmada tüketicilerin özellikle öz yeterlilik ve tepki yeterliliği bağlamında gerçek bilgilerine değil algılarına odaklanılmıştır. Literatürde bilginin gizlilik endişesi ve davranışsal tepkilerle olan ilişkisi net değildir. Reklama yönelik ikna bilgisi, koruma motivasyonlarına yönelik bilgiler, çerez vb. konulara yönelik teknik bilgi, gizlilik ve internet okuryazarlığı gibi birçok bilgi yapısından söz etmek mümkündür ancak bu yapılar ile reklama yönelik tepkiler arasındaki ilişkiler bulanıktır (Brough ve Martin, 2020). Bu nedenle farklı bilgi yapılarının reklamdan kaçınma üzerindeki etkilerini içeren çalışmalar alana katkı sunacaktır. Özellikle koruma motivasyonları kapsamında farklı seviyelerdeki koruma bilgisinin (protection knowlenge) reklamdan kaçınma üzerindeki aracı ve düzenleyici rollerinin ölçülmesi başa çıkma değerlendirmelerinin daha iyi anlaşılmasına imkân verebilir. Son olarak demografik, kişilik özellikleri, gizliliğe verilen değer gibi farklılıkların KMT bağlamında reklamdan kaçınmayı açıklamada düzenleyici etkilerinin incelenmesi teorinin sınırlarının çizilmesine yardımcı olabilir.

Teknolojinin sürekli gelişip değiştiği unutulmamalıdır. Bu anlamda hedefli reklamcılığa yönelik çerez teknolojilerinin yerini başka teknolojilere bırakması muhtemeldir. Özellikle gizliliğe yönelik tepkilerin artması üçüncü taraf teknolojilerden vazgeçileceğini göstermektedir. Reklam ağı şirketlerinin davranışsal hedefleme yerine grup hedefleme ya da bağlamsal hedefleme gibi farklı tekniklere yöneleceği ön görülmektedir (El Hana, vd., 2023). Bu durum tüketicinin tepkilerinin bir baskı unsuru yarattığının göstergesi olabilir. Bu nedenle dijital ortamda kişisel verilerin korunması ve gizlilik ihllallerini önlemek için tüketicilerin özellikle gizlilik okuryazarlığı, dijital okuryazarlık ve bir kullanıcı olarak belirli teknik bilgilere sahip olması önemli görülmektedir. Bu nedenle hem iletişim eğitiminde hem de farklı alanlarda bireylerin bu yeterlilikleri için çaba sarfedilmesi önemli görülmektedir.

Ayrıca tüketiciyi korumaya yönelik öz düzenlemeler ve yasal düzenlemeler daha kapsamlı hale getirilmelidir. Örneğin Avrupa birliği üyesi olmayan ülkelerde GDPR

yasası kullanılmadığından çoğu şirketin bu ülkelerde tüketici gizliliğine yönelik daha esnek yaklaşımları söz konusu olabilir. Çevrimiçi ortam şirketlerin ve kullanıcıların ortak faydalara sahip oldukları ve birbirlerine bu anlamda ihtiyaç duydukları ortamlardır. Bireyler özellikle ücretsiz içeriklere erişim sağladığından internetin reklam gelirleri ile desteklenmesi önemlidir. Ancak bu iki grup arasında fayda dengelerinin eşit gitmediği ve bu dengenin sağlanmasının hem kullanıcılar hem de markaların yararına olacağı düşünülmektedir. Özellikle Facebook gizllik krizinden sonra tüketicinin haklarına daha fazla önem veren markaların ve mecraların daha çok tercih edilmesi git gide daha fazla yaygınlaşırken tüketici gizliliğine saygı duymak, markaların güvenilirlik ve itibarlarını koruması açısından da önemli görülmektedir.

Tüketicilerin gizliliği korumaya yönelik kontrolleri etkinleştirmesi reklamdan kaçınmayı artırırken reklama yönelik olumsuz tutumların önüne geçmektedir. Bu nedenle tüketiciye belirli kontrollerin verilmesi reklamın etkililiği açısından önemli görülmektedir. Bunun yanı sıra belirli kontrollerin gizlilik endişesini de azaltacağı unutulmamalıdır. Reklama yönelik şüphenin azalması ve reklama duyulan güvenin artması tüketicide reklama yönelik olumlu tutumların oluşmasın için önemlidir. Ancak bu durumda reklama yönelik faydanın arttırılması söz konudur. Araştırma sonuçları tüketicinin aynı zamanda ÇDR'yi faydalı bulduğunu da göstermektedir. Gizliliğe yönelik endişelerin en aza indirilmesi reklamın iletişim etkisinin de artmasına neden olacaktır. Bu anlamda markaların tüketici gizliliğine önem verilmesini desteklemesi hem reklamların başarısını artıracak hem de marka imajına ve güvenilirliğine olumlu katkı sağlayacaktır.

KAYNAKÇA

Aalberts, R. J., Alexander Nill, A., ve Poon, P. S. (2016). Online behavioral targeting: What does the law say? *Journal of Current Issue & Research in Advertising*, 37(2), 95-112.

Abernethy, A. M. (1991a). Television exposure: Programs vs. advertising. *Current Issues and Research in Advertising*, 13(1-2), 61-77.

Abernethy, A. M. (1991b). Differences between advertising and program exposure for car radio listening. *Journal of Advertising Research*, 31(2), 33–42.

Agarwal, L., Shrivastava, N., Jaiswal, S., ve Panjwani, S. (2013, July). Do not embarrass: Re-examining user concerns for online tracking and advertising. *In Proceedings of the Ninth Symposium on Usable Privacy and Security* (pp. 1-13).

Aguirre, E., Mahr, D., Grewal, D., de Ruyter, K., ve 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.

Akan, N. ve Tanyeri, E. (2020). Reklamın Değişen Yüzünde Çevrim İçi Davranışsal Reklamcılık: İnternet Kullanıcıları Perspektifinden Bir Araştırma. *Erciyes İletişim Dergisi*, 7 (2) , 1453-1479.

Akdağ, M., ve Akan, N. A. (2017). Dijital Reklamcılık Bağlamında Çevirimiçi Davranışsal Reklamcılık ve Üniversite Gençliğinin Çevirimiçi Rekam Algısı. *Avrasya Sosyal ve Ekonomi Araştırmaları Dergisi*, 4(11), 1-10.

Akın, G. (2020). Reklamdan kaçınma davranışı çerçevesinde çevrimiçi davranışsal reklam ve marka imajı ilişkisi. *Ege Üniversitesi İletişim Fakültesi Medya ve İletişim Araştırmaları Hakemli E-Dergisi*, (7), 59-86.

Alderman, E., ve Kennedy, C. (2010). The right to privacy. New York: Vintage Books.

Allen, A. L. (1988). Uneasy access: Privacy for women in a free society. United States of America: Rowman & Littlefield Publishers.

Alraja, M. N., ve Mohammed, A. (2015). Customer Acceptance of E-commerce: Integrating Perceived Risk with TAM. *International Journal of Applied Business and Economic Research*, 13(5).

Altman, I. (1975). The environment and social behavior: privacy, personal space, territory, and crowding. California: Brooks/Cole Publishing Company.

Altman, I. (1977). Privacy regulation: Culturally universal or culturally specific?. *Journal of Social Issues*, 33(3), 66-84.

Altunışık, R., Coşkun, R., Bayraktaroğlu, S., ve Yıldırım, E. (2010). *Sosyal bilimlerde araştırma yöntemleri: SPSS uygulamalı.* Sakarya Yayıncılık.

Altunışık, R., Coşkun, R., Bayraktaroğlu, S., Yıldırım, E. (2012). *Sosyal bilimlerde araştırma yöntemleri: SPSS uygulamalı*. (7. Baskı). Sakarya: Sakarya Yayıncılık.

Alwitt, L. F., ve Prabhaker, P. R. (1994). Identifying who dislikes television advertising: Not by demographics alone. *Journal of Advertising Research*, 34(6), 17-29.

Aiolfi, S., Bellini, S., ve Pellegrini, D. (2021). Data-driven digital advertising: benefits and risks of online behavioral advertising. International *Journal of Retail & Distribution Management*, 49(7), 1089-1110.

An, S., Kang, H., ve Jin, H. S. (2018). Self-regulation for online behavioral advertising (OBA): Analysis of OBA notices. *Journal of Promotion Management*, 24(2), 270-291.

Arifin, W. N. (2015). The graphical assessment of multivariate normality using SPSS. *Education in Medicine Journal*, *7*(2), 71-75.

Asgher, S., Latif, F., ve Tahir, N. (2022). Online Behavioral Advertising: Do Awareness and Privacy Concerns Protect the Users. *Journal of Development and Social Sciences*, 3(4), 165-174.

Backes, M., Kate, A., Maffei, M., ve Pecina, K. (2012, May). Obliviad: Provably secure and practical online behavioral advertising. *In 2012 IEEE Symposium on Security and Privacy* (pp. 257-271). IEEE.

Beak, T. H. ve Morimoto, M. (2012), "Stay away from me: Examining the determinants of consumer avoidance of personalized advertising," *Journal of Advertising*, 41 (1), 59–76.

Balebako, R., Leon, P., Shay, R., Ur, B., Wang, Y., ve Cranor, L. (2012, May). Measuring the effectiveness of privacy tools for limiting behavioral advertising. In Web 2.0 Security and Privacy Workshop.

Blockthrough Report (2022). https://blockthrough.com/blog/2022-pagefair-adblock-report/ (Erişim Tarihi: 10.11.2023).

Bang, H., Choi, D., Wojdynski, B. W., ve Lee, Y. I. (2019). How the level of personalization affects the effectiveness of personalized ad messages: The moderating role of narcissism. *International Journal of Advertising*, 38(8), 1116-1138.

Bansal, G., Zahedi, F. M., ve Gefen, D. (2010). The Impact of Personal Dispositions on Information Sensitivity, Privacy Concern and Trust in Disclosing Health Information Online, Decision Support Systems 49(2), 138-150.

Barreto, A. M. (2013). Do users look at banner ads on Facebook?. *Journal of Research into Interactive Marketing*, 7, 119-139.

Bateman, P. J., Pike, J. C., ve Butler, B. S. (2011). To disclose or not: Publicness in social networking sites. *Information Technology & People*, 24(1), 78-100.

Baumeister, R. F., Masicampo, E., ve Vohs, K. D. (2011). Do conscious thoughts cause behavior? *Annual review of psychology*, 62, 331-361.

Beck, E. N. (2015). The invisible digital identity: Assemblages in digital networks. *Computers and Composition*, 35, 125-140.

Beke, F. T., Eggers, F., ve Verhoef, P. C. (2018). Consumer informational privacy: Current knowledge and research directions. *Foundations and Trends® in Marketing*, 11(1), 1-71.

Bellman, S., Schweda, A., ve Varan, D. (2010). The residual impact of avoided television advertising. *Journal of Advertising*, Spring 39(1), 67-81.

Bennett, Steven C. (2011), "Regulating online behavioral advertising," *John Marshall Law Review*, 44, 899–962.

Bettman, James R., ve C. Whan Park (1980), "Effects of Prior Knowledge and Experience and Phase of the Choice Process on Consumer Decision Processes: A Protocol Analysis," *Journal of Consumer Research*, 7 (December), 234–248.

Bleier, A., Goldfarb, A., ve Tucker, C. (2020). Consumer privacy and the future of data-based innovation and marketing. *International Journal of Research in Marketing*, *37*(3), 466-480.

Bleier, A., ve Eisenbeiss, M. (2015a). The importance of trust for personalized online advertising. *Journal of Retailing*, *91*(3), 390-409.

Bleier, A., ve Eisenbeiss, M. (2015b). Personalized online advertising effectiveness: The interplay of what, when, and where. *Marketing Science*, *34*(5), 669-688.

Bobev, T. T. (2021). Track or treat: Personal data protection and behavioural targeting in web advertising. Yayınlanmamış Yüksek Lisans Tezi. Oslo: Oslo Üniversitesi.

Boerman, S. C., Kruikemeier, S., ve Zuiderveen Borgesius, F. J. (2017). Online behavioral advertising: A literature review and research agenda. *Journal of Advertising*, 46(3), 363-376.

Boerman, S. C., Kruikemeier, S., ve Zuiderveen Borgesius, F. J. (2018). Exploring motivations for online privacy protection behavior: Insights from panel data. *Communication Research*, 48(7), 953-977.

Boerman, S. C., Kruikemeier, S., ve Bol, N. (2021). When is personalized advertising crossing personal boundaries? How type of information, data sharing, and personalized pricing influence consumer perceptions of personalized advertising. *Computers in Human Behavior* Reports, 4, 100144.

Bok, S. (1989). Secrets: On the Ethics of Concealment and Revelation. New York: Vintage Books.

Bollen, K.A. (1990). Overall fit in covariance structure models: Two types of sample size effects. *Psychological Bulletin*, 107 (2), 256-259.

Brackett L K ve Carr B N Jr. (2001). Cyberspace Advertising vs. Other Media: Consumer vs. Mature Student Attitudes. *Journal of Advertising Research*, 45(5), 23-32.

Brinson, N. H., ve Britt, B. C. (2021). Reactance and turbulence: Examining the cognitive and affective antecedents of ad blocking. *Journal of Research in Interactive Marketing*, 15(4), 549-570.

Brough, A. R., ve Martin, K. D. (2020). Critical roles of knowledge and motivation in privacy research. *Current opinion in psychology*, *31*, 11-15.

Brown, T. A. (2015). *Confirmatory factor analysis for applied research*. The Guilford Press.

Buchanan, T., Paine, C., Joinson, A. N., ve Reips, U. D. (2007). Development of measures of online privacy concern and protection for use on the Internet. *Journal of the American society for information science and technology*, *58*(2), 157-165.

Büchi, M., Just, N., ve Latzer, M. (2017). Caring is not enough: the importance of Internet skills for online privacy protection. *Information, Communication & Society*, 20(8), 1261-1278.

Byrne, B. M. (2016). *Structural equation modeling with AMOS: Basic concepts, applications, and programming*. London: Routledge.

Campbell, A. J. (1997). Relationship marketing in consumer markets: A comparison of managerial and consumer attitudes about information privacy. *Journal of Direct Marketing*, 11(3), 44-57.

Campbell, D. T., ve Fiske, D. W. (1959). Convergent and discriminant validation by the multitrait-multimethod matrix. *Psychological bulletin*, *56*(2), 81.

Campbell, J. E., ve Carlson, M. (2002). Panopticon. com: Online surveillance and the commodification of privacy. *Journal of Broadcasting & Electronic Media*, 46(4), 586-606.

Caudill, E. M., ve Murphy, P. E. (2000). Consumer online privacy: Legal and ethical issues. *Journal of Public Policy & Marketing*, 19(1), 7-19.

Chai, S., Bagchi-Sen, S., Morrell, C., Rao, H. R., ve Upadhyaya, S. J. (2009). Internet and online information privacy: An exploratory study of preteens and early teens. *IEEE Transactions on Professional Communication*, 52(2), 167-182.

Chellappa, R. K., ve Sin, R. G. (2005). Personalization versus privacy: An empirical examination of the online consumer's dilemma. *Information technology and management*, *6*, 181-202.

Chen, H., Beaudoin, C. E., ve Hong, T. (2017). Securing online privacy: An empirical test on Internet scam victimization, online privacy concerns, and privacy protection behaviors. *Computers in Human Behavior*, 70, 291-302.

Chen, H., Beaudoin, C. E., ve Hong, T. (2016). Protecting oneself online: The effects of negative privacy experiences on privacy protective behaviors. *Journalism & Mass Communication Quarterly*, *93*(2), 409-429.

Chenoweth, T., Minch, R., ve Gattiker, T. (2009, January). Application of protection motivation theory to adoption of protective technologies. *In 2009 42nd Hawaii International Conference on System Sciences* (pp. 1-10). IEEE.

Chinchanachokchai, S., ve de Gregorio, F. (2020). A consumer socialization approach to understanding advertising avoidance on social media. *Journal of Business Research*, 110, 474-483.

Cho, C. H., ve Cheon H. J. (2004). Why do people avoid advertising on the internet?. *Journal of Advertising*, 33(4), 89-97.

Cho, H., Li, P., ve Goh, Z. H. (2020). Privacy risks, emotions, and social media: A coping model of online privacy. *ACM Transactions on Computer-Human Interaction* (TOCHI), 27(6), 1-28.

Chung, Y. J., ve Kim, E. (2021). Predicting consumer avoidance of native advertising on social networking sites: A survey of Facebook users. *Journal of Promotion Management*, 27(1), 1-26.

Clancey, M. (1994). The television audience examined. *Journal of Advertising Research*, 34(4), 77-87.

Cohen, L., Manion, L. ve Morrison, K. (2000). *Research methods in education.* (5. Baskı). Londra ve New York: RoutledgeFalmer.

Craig, T. ve Ludloff, E. M. (2011). *Privacy an Big Data*. United States of America: O'Reilly Media.

Cranor, Lorrie F. (2003), “P3P: Making Privacy Policies More Useful,” *IEEE Security and Privacy,* 1 (6), 50–55.

Cranor, L. F. (2012). Can users control online behavioral advertising effectively?. *IEEE Security & Privacy*, 10(2), 93-96.

Creswell, W. J. (2014). *Research design: qualitative, quantitative and mixed methods approaches*. (4. Edition). London: SAGE Publications

Crossler, R. E. (2010). Protection Motivation Theory: Understanding Determinants to Backing Up Personal Data. In 2010 43rd Hawaii International Conference on System Sciences (pp. 1-10). IEEE.

Coster, W. J., ve Mancini, M. C. (2015). Recommendations for translation and cross-cultural adaptation of instruments for occupational therapy research and practice. Revista de Terapia Ocupacional da Universidade de São Paulo, 26(1), 50-57.

Côté, R., Battista, R.N., Wolfson, C.M., Hachinski, V. (1988). Stroke assessment scales: Guidelines for development, validation, and reliability assessment. *Canadian Journal of Neurological Sciences*, 15 (3), 261-265.

Culnan, M. J. (1993). " How did they get my name?": An exploratory investigation of consumer attitudes toward secondary information use. *MIS quarterly*, 341-363.

Culnan, M. J., ve Armstrong, P. K. (1999). Information privacy concerns, procedural fairness and impersonal trust: An empirical investigation. *Organization Science*, 10, 104–115.

Culnan, M. J., ve Bies, R. J. (2003). Consumer privacy: Balancing economic and justice considerations. *Journal of social issues*, 59(2), 323-342.

Çelik, F., Çam, M. S., ve Koseoglu, M. A. (2023). Ad avoidance in the digital context: A systematic literature review and research agenda. *International Journal of Consumer Studies*, 47 (6), 2071–2105.

Çelik, E. ve Yılmaz, V. (2016). Lisrel 9.1 ile yapısal eşitlik modellemesi temel kavramlar-uygulamalar-programlama. Ankara: Anı Yayınları

Çokluk, Ö., Şekercioğlu,G. ve Büyüköztürk,Ş. (2014). *Sosyal bilimler için çok değişkenli istatistik SPSS ve Lisrel uygulamaları*. (3.Baskı). Ankara: Pegem.

DAA, (2009). Self-regulatory principles for online behavioral advertising. https://digitaladvertisingalliance.org/sites/aboutads/files/DAA_files/seven-principles-07-01-09.pdf (Erişim Tarihi: 28.08.2022).

Davies, S. G. (1997). Re-Engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity. Agre, P. E. and Rotenberg, M. (eds.) Technology and Privacy: The New Landscape, içinde (s. 143-165). London: Cambridge, MA: MIT Press,

DeCew, J. W. (1997). In pursuit of privacy: Law, ethics, and the rise of technology. United States of America: Cornell University Press.

DeCew, J. W. (2015). Privacy and its importance with advancing technology. *Ohio NUL Review*, *42*, 471-492.

de Groot, J. I. M. (2022). "The Personalization Paradox in Facebook Advertising: The Mediating Effect of Relevance on the Personalization–Brand Attitude Relationship and the Moderating Effect of Intrusiveness." *Journal of Interactive Advertising*, 22 (1), 57–74.

De Keyzer, F., N. Dens, ve P. De Pelsmacker. (2022). "How and When Personalized Advertising Leads to Brand Attitude, Click, and WOM Intention." *Journal of Advertising*, 51 (1): 39–56.

Dinev, T. ve Hart, P. (2004). Internet privacy concerns and their antecedents – measurement validity and a regression model. *Behavior and Information Technology*, 23(6), 413–423.

Dinev, T., ve Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information systems research*, *17*(1), 61-80.

Dinev, T., Bellotto, M., Hart, P., Russo, V., ve Serra, I. (2006). Internet users privacy concerns and beliefs about government surveillance: An exploratory study of differences between Italy and the United States. *Journal of Global Information Management (JGIM)*, *14*(4), 57-93.

Dix, S., ve Phau, I. (2010). Television advertising avoidance: Advancing research methodology. *Journal of Promotion Management*, 16(1-2), 114-133.

Dodoo, N. A., ve Wen, J. (2019). A path to mitigating SNS ad avoidance: Tailoring messages to individual personality traits. *Journal of Interactive Advertising*, 19(2), 116-132.

Dolnicar, S., ve Jordaan, Y. (2007). A market-oriented approach to responsibly managing information privacy concerns in direct marketing. *Journal of Advertising*, *36*(2), 123-149.

Dowling, G. R., ve Staelin, R. (1994). A model of perceived risk and intended risk-handling activity. *Journal of Consumer Research*, 21(1), 119-134.

Ducoffe, R. H. (1996). Advertising value and advertising on the web. *Journal of Advertising Research*, 36(5), 21-21.

Dwyer, C. A. (2009). Behavioral targeting: A case study of consumer tracking on levis. com. Available at SSRN 1508496.

Eckersley, P. (2010). How unique is your web browser?. In Privacy Enhancing Technologies: 10th International Symposium, PETS 2010, Berlin, Germany, July 21-23, 2010. Proceedings 10 (pp. 1-18). Springer Berlin Heidelberg.

Edwards, S. M., Li, H., ve Lee, J. H. (2002). Forced exposure and psychological reactance: Antecedents and consequences of the perceived intrusiveness of pop-up ads. *Journal of Advertising*, 31(3), 83-95.

El Hana, N., Mercanti-Guérin, M., ve Sabri, O. (2023). Cookiepocalypse: What are the most effective strategies for advertisers to reshape the future of display advertising?. *Technological Forecasting and Social Change*, 188, 122297.

Elliot, A. J. (1999). Approach and avoidance motivation and achievement goals. *Educational Psychologist*, 34(3), 169-189.

Elliot, A. J ve Covington, M. V. (2001). Approach and Avoidance Motivation. *Educational Psychology Review*, 13(2), 73-92.

Elliot, A. J. (2006). The hierarchical model of approach-avoidance motivation. *Motivation and Emotion*, 30, 111-116.

Elliot, A. J. (2008). Handbook of approach and avoidance motivation. New York: Psychology Press.

Elliott, M. T., ve Speck, P. S. (1998). Consumer perceptions of advertising clutter and its impact across various media. *Journal of Advertising Research*, 38(1), 29-30.

Estrada-Jiménez, J., Parra-Arnau, J., Rodríguez-Hoyos, A., ve Forné, J. (2017). Online advertising: Analysis of privacy threats and protection approaches. *Computer Communications*, 100, 32-51.

Fachryto, T., ve Achyar, A. (2018). Effect of online behavioral advertising implementation on attitude toward ad and purchase intention in Indonesian E-marketplace. Sriwijaya international journal of dynamic economics and business, 2(2), 123-138.

Feng, Y., ve Xie, Q. (2019). Privacy concerns, perceived intrusiveness, and privacy controls: An analysis of virtual try-on apps. *Journal of Interactive Advertising*, *19*(1), 43-57.

Ferguson, D. A., ve Perse, E. M. (1993). Media and audience influences on channel repertoire. *Journal of Broadcasting & Electronic Media*, 37(1), 31-47.

Fishbein, Martin ve Icek Ajzen (1975), "Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research," Addison- Wesley, Reading, MA.

Field, A. (2009). Discovering statistics using SPSS. (3. Baskı). Kaliforniya: SAGE Publications Inc.

Fornell, C. ve Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39–50. https://doi.org/10.1177/002224378101800104

Fourberg, N., Taş, S., Wiewiorra, L., Godlovitch, I. (2021). Online advertising: the impact of targeted advertising on advertisers, market access and consumer choice, European Parliament. https://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2021)662913. (Erişim Tarihi: 17.09.2023).

Foxman, E. R., ve Kilcoyne, P. (1993). Information technology, marketing practice, and consumer privacy: Ethical issues. *Journal of Public Policy & Marketing*, 12(1), 106-119.

FTC, Online behavioral advertising moving the discussion forward to possible self-regulatory principles (2007). (Erişim Tarihi: 28.08.2022). https://www.ftc.gov/sites/default/files/documents/public_statements/online-behavioral-advertising-moving-discussion-forward-possible-self-regulatory-principles/p859900stmt.pdf.

FTC Self Report, (2009). Self-Regulatory Principles For Online Behavioral Advertising. Behavioral Advertising Traking, Targeting And Technology. (Erişim Tarihi: 12.08.2022). https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral advertising/p085400 behavadreport .pdf.

Gavison, R. (1980). Privacy and the limits of the law. Yale Law Journal, 89, 421–471.

George, D. ve Mallery, P. (2016). IBM SPSS statistics 23 step by step: A simple guide and reference. Boston, Munich: Pearson.

Gerety, T. (1977). Redefining privacy. Harv. CR-CLL Rev., 12, 233.

Goldfarb, A., ve Tucker, C. (2011). Online display advertising: Targeting and obtrusiveness. *Marketing Science*, 30(3), 389-404.

Goodwin, C. (1991). Privacy: Recognition of a consumer right. *Journal of Public Policy & Marketing*, 10(1), 149-166.

Gordon, B. R., Jerath, K., Katona, Z., Narayanan, S., Shin, J., ve Wilbur, K. C. (2021). Inefficiencies in digital advertising markets. *Journal of Marketing*, 85(1), 7-25.

Gökdemir, Ş. Ş., ve Akıncı, S. (2019). Çevrimiçi davranışsal reklamcılığa yönelik tüketici tutumları ve mahremiyet endişeleri. *Erciyes İletişim Dergisi*, (1), 21-38.

Gröne, N. (2011). Targeted advertising and consumer privacy concerns: experimental studies in an internet context. Göttingen: Cuvillier Press.

Guardia, F.R. (2015), "A generalization of advertising avoidance model on social network", available at: https://dee.uib.es/digitalAssets/312/312676_rejon.pdf (Erişim Tarihi: 15 Ekim 2023).

Gürbüz, S. ve Şahin, F. (2018). Sosyal bilimlerde araştırma yöntemleri: Felsefe, yöntem, analiz. (5.Baskı). Seçkin: Ankara.

Ha, L. (1996). Observations: Advertising clutter in consumer magazines: Dimensions and effects. *Journal of Advertising Research*, 36(4), 76-84.

Ha, L., ve Litman, B. R. (1997). Does advertising clutter have diminishing and negative returns?. *Journal of Advertising*, 26(1), 31-42.

Ha, L., ve McCann, K. (2008). An integrated model of advertising clutter in offline and online media. *International Journal of Advertising*, 27(4), 569-592.

Ham, C. D., ve Nelson, M. R. (2016). The role of persuasion knowledge, assessment of benefit and harm, and third-person perception in coping with online behavioral advertising. *Computers in Human Behavior*, 62, 689-702.

Ham, C. D. (2017). Exploring how consumers cope with online behavioral advertising. *International Journal of Advertising*, 36(4), 632-658.

Hair, J. F., Black, W. C., Babin, B. J. ve Anderson, R. E. (2019). *Multivariate data analysis*. (8. Baskı). Australia: Cengage.

Heeter, C., ve Greenberg, B. S. (1985). Profiling the zappers. *Journal of Advertising Research*. 25(2), 15–19.

Hervet, G., Guerard, K., Tremblay, S., ve Saber Chtourou, M. (2011). Is banner blindness genuine? Eye tracking Internet text advertising. *Applied Cognitive Psychology*, 25, 708-716.

Ho, V. T. (2021). Advertising avoidance: A literature review. *Independent Journal of Management & Production*, 12(1), 185–200.

Hoch, Stephen J., ve John Deighton (1989), "Managing What Consumers Learn from Experience," *Journal of Marketing*, 53 (April), 1–20.

Holvast, j. (2007). History of Privacy. De Leeuw, K. ve Bergstra, J. (Eds.). The history of information security: a comprehensive handbook içinde (s. 737-769). Netherlands: Elsevier.

Hu, L. ve Bentler, P.M. (1999) Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. Structural Equation Modeling: *A Multidisciplinary Journal*, *6*(1), 1-55. https://doi.org/10.1080/10705519909540118

Hussain, D., ve Lasage, H. (2014). Online video advertisement avoidance: can interactivity help?. *Journal of Applied Business Research* (JABR), 30(1), 43-50.

IAB, (2014a). Factsheet: Online Behavioural Advertising. https://www.iabuk.com/sites/default/files/IAB%20Fact%20Sheet%20May%202014%20-%20Online%20Behavioural%20Advertising.pdf (Erişim Tarihi: 18.10.2020).

IAB, (2014b). Self-Regulatory Principles for Online Behavioral Advertising. https://www.iab.com/news/self-regulatory-principles-for-online-behavioral-advertising/ (Erişim Tarihi: 18.10.2020).

IAB, (2022). İnternet Reklam Harcamaları Yıllık Raporu. https://www.iab.com/wp-content/uploads/2023/04/IAB_PwC_Internet_Advertising_Revenue_Report_2022.pdf (Erişim Tarihi: 02.11.2023).

IABTR (2022). İnternet Reklam Harcamaları Yıllık Raporu.

https://iabtr.org/UploadFiles/PageFiles/2022%20Medya%20ve%20Reklam%20Yat%C4%B1r%C4%B1mlar%C4%B1%20Raporu1142023094731.pdf (Erişim Tarihi: 02.11.2023).

Ikram, M., ve Kaafar, M. A. (2017, October). A first look at mobile ad-blocking apps. In 2017 IEEE 16th International Symposium on Network Computing and Applications (NCA) (pp. 1-8). IEEE.

Im, J., Wang, R., Lyu, W., Cook, N., Habib, H., Cranor, L. F., ... ve Schaub, F. (2023, April). Less is Not More: Improving Findability and Actionability of Privacy Controls for Online Behavioral Advertising. In Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (pp. 1-33).

Ioannou, A., Tussyadiah, I., ve Marshan, A. (2021). Dispositional mindfulness as an antecedent of privacy concerns: A protection motivation theory perspective. *Psychology & Marketing*, 38(10), 1766-1778.

İslamoğlu, H. (2011). *Sosyal bilimlerde araştırma yöntemleri.* (2. Baskı). İstanbul: Beta Yayınları.

İspir, N. B., ve Süher, H. K. (2009). Perceived ad clutter among young consumers: New media expansion. *Business Research Yearbook,* 16(1), 64-72.

James, W. L., ve Kover, A. J. (1992). Do overall attitudes toward advertising affect involvement with specific advertisements?. *Journal of Advertising Research*, 32(5), 78–83.

Jin, C. H., ve Villegas, J. (2006). Consumer responses to advertising on the internet: The effect of individual difference on ambivalence and avoidance. *CyberPsychology & Behavior*, 10(2), 258-266.

Jin, Y., Campbell, S. W., ve Kwak, N. (2012). Computers in Human Behavior Affect, cognition and reward: Predictors of privacy protection online. *Computers in Human Behavior*, 28(3), 1019–1027.

Jöreskog, K.G. ve Sörbom, D. (1993). LISREL 8*: Structural equation modeling with the SIMPLIS command language*. USA: Scientific Software International.

Jung, A. R. (2017). The influence of perceived ad relevance on social media advertising: An empirical examination of a mediating role of privacy concern. *Computers in Human Behavior*, 70, 303-309.

Karabıyık, B. K., ve Armağan, E. (2017). Tüketicinin çevrimiçi davranışsal reklamlara tıklama kararını etkileyen faktörler. *Yaşar Üniversitesi E-Dergisi*, 12(47), 202-215.

Karagöz, Y. (2019). *Bilimsel araştırma yöntemleri ve yayın etiği*. Ankara: Nobel Dağıtım.

Karasar, N. (2003). Bilimsel araştırma yöntemi. (12. Baskı). Ankara: Nobel Yayın Dağıtım.

Kaplan, B. M. (1985). Zapping—the real issue is communication. *Journal of Advertising Research*. 25(2), 9–12.

Keulen ve Kroeze, (2018). Privacy from a Historical Perspective. Sloot, B. ve de Groot, A. (Ed.) The Handbook of Privacy Studies içinde (s. 21-56). Amsterdam: Amsterdam University Press.

Kelley, B. (2007). Privacy and online behavioral advertising. *Journal of Internet Law*, 11(6), 24-26.

Kelly, L., Kerr, G., ve Drennan, J. (2010). Avoidance of advertising in social networking sites: The teenage perspective. *Journal of Interactive Advertising*, 10(2), 16-27.

Kelly, L., Kerr, G., ve Drennan, J. (2020). Triggers of engagement and avoidance: Applying approach-avoid theory. *Journal of Marketing Communications*, 26(5), 488-508.

Kelly, L., Kerr, G., Drennan, J., ve Fazal-E-Hasan, S. M. (2021). Feel, think, avoid: Testing a new model of advertising avoidance. *Journal of Marketing Communications*, 27(4), 343-364.

Kent, R. J., ve Allen, C. T. (1994). Competitive interference effects in consumer memory for advertising: The role of brand familiarity. *Journal of Marketing*, 58(3), 97-105.

Kırlıdoğ, M. (2013). Çevrimiçi Davranışsal Reklamcılık ve Kişisel Mahremiyet İhlalleri. Akademik Bilişim 2013.

Kim, E., Choi, S. M., Kim, S., ve Yeh, Y. H. (2013). Factors affecting advertising avoidance on online video sites. *The Journal of Advertising and Promotion Research*, 2(1), 87-121.

Kim, S. (2014). "Consumer Privacy Concerns and Responses to Online Behavioral Advertising: A Cross-Cultural Comparison of Americans and Koreans." Proceedings of the Conference - American Academy of Advertising, (s. 163-164). Atlanta.

Kim, J. K., ve Seo, S. H. (2017). An Exploration of Advertising Avoidance by Audiences across Media. *International Journal of Contents*, 13(1).

Kim, H., ve Huh, J. (2017). Perceived relevance and privacy concern regarding online behavioral advertising (OBA) and their role in consumer responses. *Journal of Current Issues & Research in Advertising*, 38(1), 92-105.

Kim, H.Y., Song, J.H. ve Lee, J.H. (2019). When are personalized promotions effective? The role of consumer control. *International Journal of Advertising* 38(4), 628–47.

Kline, P. (1994). *An easy guide to factor analysis*. New York: Routledge.

Kline RB 2011 Principles and Practice of Structural Equation Modeling Third Edition. New York: The Guilford Press.

Kline, R. B. (2019). Principles and practice of structural equation modeling. (Çeviri Editörü, Sedat Şen). (4. Baskı). New York: The Guilford Press.

Lamberton, C., ve Stephen, A. T. (2016). A thematic exploration of digital, social media, and mobile marketing: Research evolution from 2000 to 2015 and an agenda for future inquiry. *Journal of Marketing*, 80(6), 146-172.

Lambrecht, A., ve Tucker, C. (2013). When does retargeting work? Information specificity in online advertising. *Journal of Marketing research*, *50*(5), 561-576.

Lanier, C. D., ve Saini, A. (2008). Understanding consumer privacy: A review and future directions. *Academy of Marketing Science Review*, 12(2), 1-45.

LaRose, R., Rifon, N., Liu, S., ve Lee, D. (2005, May). Online safety strategies: a content analysis and theoretical assessment. In The 55th Annual Conference of the International Communication Association, New York City.

Lee, S., ve Lumpkin, J. R. (1992). Differences in attitudes toward TV advertising: VCR usage as a moderator. International *Journal of Advertising*, 11(4), 333-342.

Lee, D., Larose, R., ve Rifon, N. (2008). Keeping our network safe: a model of online protection behaviour. *Behaviour & Information Technology*, 27(5), 445-454.

Lee, Seungsin, Younghee Lee, Joing-In Lee, ve Jungkun Park (2015), "Personalized e-Services: Consumer Privacy Concern and Information Sharing," Social Behavior and Personality: *An International Journal*, 43(5), 729–40.

Leong, L. Y., Hew, T. S., Ooi, K. B., ve Dwivedi, Y. K. (2020). Predicting trust in online advertising with an SEM-artificial neural network approach. Expert Systems with Applications, 162, 113849.

Li, Y. (2019). User perception affects search engine advertising avoidance: Moderating role of user characteristics. Social Behavior and Personality: *An International Journal*, 47(4), 1–12.

Li, H., Edwards, S. M., ve Lee, J. H. (2002). Measuring the intrusiveness of advertisements: Scale development and validation. *Journal of Advertising*, 31(2), 37-47.

Li, W., ve Huang, Z. (2016). The research of influence factors of online behavioral advertising avoidance. *American Journal of Industrial and Business Management*, 6(09), 947.

Li, B., ve Yin, S. (2021). How perceived control affects advertising avoidance intention in a skippable advertising context: a moderated mediation model. *Chinese Journal of Communication*, 14(2), 157-175.

Lwin, M., Wirtz, J., ve Williams, J. D. (2007). Consumer online privacy concerns and responses: A power-responsibility equilibrium perspective. *Journal of the Academy of Marketing Science*, 35, 572-585.

MacKenzie, S. B., ve Lutz, R. J. (1989). An empirical examination of the structural antecedents of attitude toward the ad in an advertising pretesting context. *Journal of Marketing*, 53(2), 48-65.

Maddux, J. E., Sherer, M., ve Rogers, R. W. (1982). Self-efficacy expectancy and outcome expectancy: Their relationship and their effects on behavioral intentions. *Cognitive therapy and research*, 6, 207-211.

Malhotra, N. K., Kim, S. S., ve Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information systems research*, 15(4), 336-355.

Margulis, S. T. (2003a). On the status and contribution of Westin's and Altman's theories of privacy. *Journal of Social Issues*, 59(2), 411-429.

Margulis, S. T. (2003b). "Privacy as a Social Issue and Behavioral Concept," *Journal of Social Issues* 59(2), 243-261.

Margulis S. T. (2011). Three Theories of Privacy: An Overview. Trepte, S., & Reinecke, L. (Eds.). Privacy online: Perspectives on privacy and self-disclosure in the social web. İçinde (s. 9-18). Berlin: Springer.

Martin, K. D., ve Murphy, P. E. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science*, 45, 135-155.

Masur, P. K. (2018). Situational privacy and self-disclosure: Communication processes in online environments. Germany: Springer.

McClain, L. C. (1995). Inviolability and privacy: The castle, the sanctuary, and the body. *Yale JL & Human*, 7, 195.

McDonald, Aleecia M., ve Lorrie F. Cranor (2008), "The Cost of Reading Privacy Policies," Information System: *A Journal of Law and Policy for the Information Society*, 4 (3), 543–67.

McDonald, A. M., ve Cranor, L. F. (2010a). Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising. In Proceedings of the 2010 Research Conference on Communication, Information and Internet Policy, October 2010.

McDonald, A. M., ve Cranor, L. F. (2010b). Americans' attitudes about internet behavioral advertising practices. In Proceedings of the 9th annual ACM workshop on Privacy in the electronic society (pp. 63-72).

Michelon, A., Bellman, S., Faulkner, M., Cohen, J., ve Bruwer, J. (2020). A new benchmark for mechanical avoidance of radio advertising: Why radio advertising is a sound investment. *Journal of Advertising Research*, 60(4), 407-416.

Miller, A.R. (1971). The Assault on Privacy. Harvard University Press, Cambridge, MA.

Milne, G. R., ve Culnan, M. J. (2004). Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *Journal of Interactive Marketing*, 18(3), 15-29.

Mohamed, N., ve Ahmad, I. H. (2012). Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. *Computers in Human Behavior*, 28(6), 2366-2375.

Moloney, M., ve Bannister, F. (2009, January). A privacy control theory for online environments. In 2009 42nd Hawaii International Conference on System Sciences (pp. 1-10). IEEE.

Moor, J. H. (1997). Towards a theory of privacy in the information age. ACM Sigcas *Computers and Society*, 27(3), 27-32.

Moore, Robert S., Melissa L. Moore, Kevin J. Shanahan, ve Britney Mack (2015), "Creepy Marketing: Three Dimensions of Perceived Excessive Online Privacy Violation," *Marketing Management*, 25 (1), 42–53.

Mord, M. S., ve Gilson, E. (1985). Shorter units-risk responsibility reward. *Journal of Advertising Research*, 25(4), 9-19.

Moriarty, S. E., ve Everett, S. L. (1994). Commercial Breaks: A Viewing Behavior Study. *Journalism and Mass Communication Quarterly*, 71(2), 346.

Morimoto, M., ve Chang, S. (2009). Psychological factors affecting perceptions of unsolicited commercial e-mail. *Journal of Current Issues & Research in Advertising*, 31(1), 63-73.

Morimoto, M., ve Macias, W. (2009). A conceptual framework for unsolicited commercial e-mail: Perceived intrusiveness and privacy concerns. *Journal of Internet Commerce*, 8(3-4), 137-160.

Morimoto, M. (2021). Privacy concerns about personalized advertising across multiple social media platforms in Japan: The relationship with information control and persuasion knowledge. *International Journal of Advertising*, 40(3), 431-451.

Mousavi, R., Chen, R., Kim, D. J., ve 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.

Mpinganjira, M., ve Maduku, D. K. (2019). Ethics of mobile behavioral advertising: Antecedents and outcomes of perceived ethical value of advertised brands. *Journal of Business Research*, 95, 464-478.

Neuman, W. L. (2017). Toplumsal Araştırma Yöntemleri Nitel ve Nicel Yaklaşımlar 1. Cilt. (Çeviri: Sedef Özge). (9. Baskı). Ankara: Yayın Odası.

Nill, A. ve Aalberts, R. J. (2014). Legal and ethical challenges of online behavioral targeting in advertising. *Journal of Current Issues and Research in Advertising*, 35 (2), 126–46.

Niu, X., Wang, X., ve Liu, Z. (2021). When I feel invaded, I will avoid it: The effect of advertising invasiveness on consumers' avoidance of social media advertising. *Journal of Retailing and Consumer Services*, 58, 102320.

Norman, P., Boer, H., Seydel, E. R., ve Mullan, B. (2015). Protection motivation theory. Conner, M. and Norman, P. (Eds.). Predicting and changing health behaviour: Research and practice with social cognition models, 3 Edition, içinde, (s. 70-106). England: Open University Press.

Núnez-Barriopedro, E., Cuesta-Valiño, P., ve Mansori-Amar, S. (2023). The role of perceived usefulness and annoyance on programmatic advertising: the moderating effect of Internet user privacy and cookies. *Corporate Communications: An International Journal*, *28*(2), 311-324.

Nyheim, P., Xu, S., Zhang, L., ve Mattila, A. S. (2015). Predictors of avoidance towards personalization of restaurant smartphone advertising: A study from the Millennials' perspective. *Journal of Hospitality and Tourism Technology*, 6(2), 145-159.

Okazaki, S., Li, H., ve Hirose, M. (2009). Consumer privacy concerns and preference for degree of regulatory control. Journal of advertising, 38(4), 63-77.

Okazaki, S., Molina, F. J., ve Hirose, M. (2012). Mobile advertising avoidance: exploring the role of ubiquity. *Electronic Markets*, 22, 169-183.

Okazaki, S., Eisend, M., Plangger, K., de Ruyter, K., & Grewal, D. (2020). Understanding the strategic consequences of customer privacy concerns: A meta-analytic review. *Journal of Retailing*, 96(4), 458-473.

Özcelik, A. B., ve Varnalı, K. (2019). Effectiveness of online behavioral targeting: A psychological perspective. Electronic Commerce Research and Applications, 33, 100819.

Pallant, J. (2005). *SPSS Survival Manual: A step by step guide to data analysis using SPSS for Windows (Version 12).* Sydney: Allen & Unwin.

Palos-Sanchez, P., Saura, J. R., ve Martin-Velicia, F. (2019). A study of the effects of programmatic advertising on users' concerns about privacy overtime. *Journal of Business Research*, 96, 61-72.

Park, C., ve Lee, S. W. (2014). A study of the user privacy protection behavior in online environment: Based on protection motivation theory. Journal of Internet Computing and Services, 15(2), 59-71.

Pavlou, P. A. (2003). Consumer acceptance of electronic commerce—Integrating trust and risk, with the technology acceptance model. *Internat. J. Electronic Commerce,* 7(3) 69–103.

Pavlou, P. A. (2011). State of the information privacy literature: Where are we now and where should we go?. *MIS quarterly*, 977-988.

Percy, L. (2012). The Role of Emotion in Processing Advertising. Rodgers, S., & Thorson, E. (Eds.). Advertising theory içinde (s. 69-84). New York: Routledge.

Petronio, S. (1991). Communication boundary management: A theoretical model of managing disclosure of private information between marital couples. *Communication Theory*, 1, 311–335.

Petronio, S. (2002). Boundaries of privacy: Dialectics of disclosure. Albany: State University of New York Press.

Phaf, R. H., Mohr, S. E., Rotteveel, M., ve Wicherts, J. M. (2014). Approach, avoidance, and affect: a meta-analysis of approach-avoidance tendencies in manual reaction time tasks. *Frontiers in Psychology*, 5, 378.

Phau, I., ve Dix, S. (2003). The effect of planned versus impulse viewing on television advertising avoidance: An exploratory observer/survey approach. ANZMAC Conference Proceedings Adelaide 1-3 December.

Phelan, Chanda, Cliff Lampe, ve Paul Resnick (2016), "It's Creepy, But It Doesn't Bother Me," Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, New York: Association for Computing Machinery, 5240–51.

Phelps, J., Nowak, G., ve Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing*, 19(1), 27-41.

Phelps, J. E., D'Souza, G., ve Nowak, G. J. (2001). Antecedents and consequences of consumer privacy concerns: An empirical investigation. *Journal of Interactive Marketing*, 15(4), 2-17.

Plummer, J., Rappaport, S. D., Hall, T., ve Barocci, R. (2007). The online advertising playbook: Proven strategies and tested tactics from the advertising research foundation. New Jersey: John Wiley & Sons.

Prendergast, G., Cheung, W. L., ve West, D. (2010). Antecedents to advertising avoidance in China. *Journal of Current Issues & Research in Advertising*, 32(2), 87-100.

Rachels, J. (1975). Why privacy is important. *Philosophy and Public Affairs*, 4(4), 323–333.

Rachbini, W., ve Hatta, I. H. (2018). E-lifestyle and internet advertising avoidance. *Jurnal Manajemen*, 22(3), 435-448.

Ray, M. L., ve Webb, P. H. (1986). Three prescriptions for clutter. *Journal of Advertising Research*, 26(1), 69-76.

Riebe, E., ve Dawes, J. (2006). Recall of radio advertising in low and high advertising clutter formats. *International Journal of Advertising*, 25(1), 71-86.

Rifon, N. J., LaRose, R., ve Choi, S. M. (2005). Your privacy is sealed: Effects of web privacy seals on trust and personal disclosures. Journal of consumer affairs, 39(2), 339-362.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. *The Journal of Psychology*, 91(1), 93-114.

Rogers, R. W. (1983). Cognitive and physiological processes in fear-based attitude change: A revised theory of protection motivation. In J. Cacioppo & R. Petty (Eds.), Social psychophysiology. A sourcebook (pp. 153-176). New York. NY: Guilford.

Rojas-Méndez, J. I., ve Davies, G. (2005). Avoiding television advertising: Some explanations from time allocation theory. *Journal of Advertising Research*, 45(1), 34-48.

Rojas-Méndez, J. I., Davies, G., ve Madran, C. (2009). Universal differences in advertising avoidance behavior: A cross-cultural study. *Journal of Business Research*, 62(10), 947-954.

Rojas-Méndez, J. I., ve Davies, G. (2017). Time pressure and time planning in explaining advertising avoidance behavior. *Journal of Promotion Management*, 23(4), 481-503.

Rubin, A. ve Babbie, E. (2011*). Research methods for social work*. (7. Baskı). USA: Brook/Cole CENGAGE Learning.

Rustad, M. L., ve Koenig, T. H. (2018). Towards a global data privacy standard. *Florida Law Review*, 71, 18-16.

Sagui-Henson, S. J. (2017). Cognitive avoidance. Encyclopedia of personality and individual differences. Springer. https://doi. org/10.1007/978-3-319-28099-8_964-1.

Salleh, N., Hussein, R., Mohamed, N., Karim, N. S. A., Ahlan, A. R., ve Aditiawarman, U. (2012). Examining information disclosure behavior on social network sites using protection motivation theory, trust and risk. *Journal of Internet Social Networking & Virtual Communities*, 1.

Saunders, K., ve Zucker, B. (1999). "Contracting Identity Fraud in The Information Age: The Identity Theft and Assumption Deterrence Act," *International Review of Law, Computers and Technology* (13:2), pp.183–192.

Schlee, C. (2013). Targeted advertising technologies in the ICT Space: A use case driven analysis. Germany: Springer Science & Business Media.

Schoeman, F. (1984). Privacy philosophical dimensions of the literatüre. Schoeman, F. D. (Ed.), Philosophical dimensions of privacy: An anthology içinde (s. 56-74). New York: Cambridge University Press.

Segijn, C. M., ve Van Ooijen, I. (2022). Differences in consumer knowledge and perceptions of personalized advertising: Comparing online behavioural advertising and synced advertising. *Journal of Marketing Communications*, *28*(2), 207-226.

Seyedghorban, Z., Tahernejad, H., ve Matanda, M. J. (2016). Reinquiry into advertising avoidance on the internet: A conceptual replication and extension. *Journal of Advertising*, 45(1), 120-129.

Sharma, A., Dwivedi, R., Mariani, M. M., ve Islam, T. (2022). Investigating the effect of advertising irritation on digital advertising effectiveness: A moderated mediation model. *Technological Forecasting and Social Change*, 180, 121731.

Sheehan, K. B., ve Hoy, M. G. (2000). Dimensions of privacy concern among online consumers. *Journal of public policy & marketing*, *19*(1), 62-73.

Shelton, D. (2012). Online behavioral advertising Tracking users: Gold mine or land mine. Landslide, 5, 26.

Shin, W., ve Lin, T. T. C. (2016). Who avoids location-based advertising and why? Investigating the relationship between user perceptions and advertising avoidance. *Computers in Human Behavior*, 63, 444-452.

Singaraju, S. P., Rose, J. L., Arango-Soler, L. A., D'Souza, C., Khaksar, S. M. S., ve Brouwer, A. R. (2022). The dark age of advertising: An examination of perceptual factors affecting advertising avoidance in the context of mobile youtube. *Journal of Electronic Commerce Research*, *23*(1), 13-32.

Sipior, J. C., Ward, B. T., ve Mendoza, R. A. (2011). Online privacy concerns associated with cookies, flash cookies, and web beacons. *Journal of internet commerce*, 10(1), 1-16.

Smith, Robert E., ve William R. Swinyard (1982), "Information Response Models: An Integrated Approach," Journal of Marketing, 46 (Winter), 81–93.

Smit, Edith G., Guda Van Noort, ve Hilde A. Voorveld (2014). Understanding online behavioural advertising: user knowledge, privacy concerns, and online coping behaviour in europe. *Computers in Human Behavior*, 32, 15–22.

Smith, H. J., Milberg, S. J., ve Burke, S. J. (1996). Information privacy: measuring individuals' concerns about organizational practices. *MIS quarterly*, 167-196.

Smith, H. J., Dinev, T., ve Xu, H. (2011). Information privacy research: an interdisciplinary review. *MIS quarterly*, 35(4), 989-1016.

Solove, D. J. (2000). Privacy and power: Computer databases and metaphors for information privacy. Stan. L. Rev., 53, 1393.

Solove, D. J. (2008). Understanding Privacy. England: Harvard University Press.

Söllner, J., ve Dost, F. (2019). Exploring the selective use of ad blockers and testing banner appeals to reduce ad blocking. *Journal of Advertising*, 48(3), 302-312.

Speck, P. S., ve Elliott, M. T. (1997a). Predictors of advertising avoidance in print and broadcast media. *Journal of Advertising*, 26(3), 61-76.

Speck, P. S., ve Elliott, M. T. (1997b). The antecedents and consequences of perceived advertising clutter. *Journal of Current Issues & Research in Advertising*, 19(2), 39-54.

Stafford, M. R., ve Stafford, T. F. (1996). Mechanical commercial avoidance: A uses and gratifications perspective. *Journal of Current Issues & Research in Advertising*, 18(2), 27-38.

Strycharz, J., Van Noort, G., Smit, E., ve Helberger, N. (2019). Protective behavior against personalized ads: Motivation to turn personalization off. Cyberpsychology: *Journal of Psychosocial Research on Cyberspace*, 13(2).

Smullen, D., Yao, Y., Feng, Y., Sadeh, N., Edelstein, A., ve Weiss, R. (2021). Managing Potentially Intrusive Practices in the Browser: A User-Centered Perspective. *Proceedings on Privacy Enhancing Technologies*, 4, 500-527.

Sutanto, J., Palme, E., Tan, C. ve Phang, C.W. (2013), "Addressing the personalization–privacy paradox: an empirical assessment from a field experiment on smartphone users", *MIS Quarterly*, Vol. 37 No. 4, pp. 1141-1164.

Süher H. K. ve İspir, N. B. (2010). Televizyon ve gazetede reklamdan kaçınmayı etkileyen değişkenler. *Selçuk İletişim*, 6(2), 5-23.

Tabachnick, B. G. ve Fidell, L. S. (2015). *Çok değişkenli istatistiklerin kullanımı*. (Çev. B. Bıçak) Ankara: Nobel.

Tam, K. Y., ve Ho, S. Y. (2006). Understanding the Impact of Web Personalization on User Information Processing and Decision Outcomes. *MIS Quarterly*, 30(4), 865-890.

Taşdelen, H., ve Şentürk, Z. A. (2018). İnternet reklamcılığında davranışsal hedeflemenin tüketici satın alma davranışına etkisi. *İnönü Üniversitesi İletişim Fakültesi Elektronik Dergisi (İNİF E-Dergi)*, 3(2), 175-190.

Tavani, H. T. (2008). Informational Privacy: Concepts, Theories, and Controversies. Himma, K. E. ve Tavani, H. T (Eds), Informational Privacy: Concepts, Theories, and Controversies içinde (s. 131-164). New Jersey: John Wiley & Sons, Inc.

Tellis, G. L. (2004). Effective Advertising: Understanding when, how, and why advertising works. London: Sage Publicationd.

Toubiana, V., Narayanan, A., Boneh, D., Nissenbaum, H., ve Barocas, S. (2010, March). Adnostic: Privacy preserving targeted advertising. In Proceedings Network and Distributed System Symposium.

Tran, T. P. (2017). Personalized ads on Facebook: An effective marketing tool for online marketers. *Journal of Retailing and Consumer Services*, 39, 230-242.

Tudoran, A. A. (2019). Why do internet consumers block ads? New evidence from consumer opinion mining and sentiment analysis. Internet Research, 29(1), 144–166.

Turow, J., King, J., Hoofnagle, C. J., Bleakley, A., ve Hennessy, M. (2009). Americans reject tailored advertising and three activities that enable it. September 29. Accessed25 November 2019, doi: 10.2139/ssrn.1478214.

Udadeniya, U. P. R. P., Yalegama, M. M. H. H., Wickramasinghe, A. K. K. D., Mannapperuma, M. Y. S. S., ve Jayasuriya, K. K. N. A. (2019). Online Behavioral Advertising Avoidance in Online Retailing in Sri Lanka. *Global Journal of Management and Business Research*, *19*(4), 11-15.

Ur, Blase, Pedro G. Leon, Lorrie F. Cranor, Richard Shay, ve Yang Wang (2012). "Smart, Useful, Scary, Creepy: Perceptions of Online Behavioral Advertising," Proceedings of the Eighth Symposium on Usable Privacy and Security, art. 4.

Van den Broeck, E., Poels, K., ve Walrave, M. (2018). An experimental study on the effect of ad placement, product involvement and motives on Facebook ad avoidance. *Telematics and Informatics*, 35(2), 470–479.

Van der Goot, M. J., Rozendaal, E., Opree, S. J., Ketelaar, P. E., ve Smit, E. G. (2018). Media generations and their advertising attitudes and avoidance: a six-country comparison. *International Journal of Advertising*, 37(2), 289-308

Van Doorn, J., ve Hoekstra, J. C. (2013). Customization of online advertising: The role of intrusiveness. *Marketing Letters*, 24, 339-351.

Varnalı, K. (2021). Online behavioral advertising: An integrative review. *Journal of Marketing Communications*, 27(1), 93-114.

Veneziano L ve Hooper, J. (1997). A method for quantifying content validity of health-related questionnaires. *American Journal of Health Behavior*, 21 (1), 67-70.

Wachter, S. (2021). Affinity Profiling and Discrimination By Association in Online Behavioral Advertising. *Berkeley Technology Law Journal*, 35, 367.

Wang, H. J., Yue, X. L., Ansari, A. R., Tang, G. Q., Ding, J. Y., ve Jiang, Y. Q. (2022). Research on the Influence Mechanism of Consumers' Perceived Risk on the Advertising Avoidance Behavior of Online Targeted Advertising. *Frontiers in Psychology*, 13, 878629.

Warren, S. D., ve Brandeis, L. D. (1890). Right to privacy. *Harvard Law Review*, 4(5), 193-220.

Webb, P. H., ve Ray, M. L. (1979). Effects of TV clutter. *Journal of Advertising Research*, 19(3), 7-12.

Wei, X., Ko, I., ve An, N. (2019). An exploratory study for perceived advertising value in the relationship between irritation and advertising avoidance on the mobile social platforms. Proceedings of the 52nd Hawaii International Conference on System Sciences.

We Are Social, ve Hootsuite. (2022). Digital 2022 Global Overview Report. Retrieved from https:// www.hootsuite.com/resources/digital-trends.

Westin, A. (1967). Privacy and freedom. New York: Ig Publishing.

Westin, A. F. (2003). Social and political dimensions of privacy. *Journal of social issues*, 59(2), 431-453.

White, T. B. (2004). Consumer disclosure and disclosure avoidance: A motivational framework. *Journal of Consumer Psychology*, 14(1-2), 41-51.

Wohn, D. Y., Solomon, J., Sarkar, D., ve Vaniea, K. E. (2015, April). Factors related to privacy concerns and protection behaviors regarding behavioral advertising.

In *Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems* (pp. 1965-1970).

Wiese, M., Martínez-Climent, C., ve Botella-Carrubi, D. (2020). A framework for Facebook advertising effectiveness: A behavioral perspective. *Journal of Business Research*, 109, 76-87.

Williams, A. D., ve Moulds, M. L. (2007). Cognitive avoidance of intrusive memories: Recall vantage perspective and associations with depression. *Behaviour Research and Therapy*, 45(6), 1141-1153.

Wijenayake, S., ve Pathirana, I. (2019). A study on factors influencing online behavioral advertising avoidance (Oba): Special reference to Sri Lankan online advertising. *Management Science Letters*, *9*(8), 1281-1288.

Witte, K. (1992). Putting the fear back into fear appeals: The extended parallel process model. *Communication Monographs*, *59*, 329-349.

Wohn, D. Y., Solomon, J., Sarkar, D., ve Vaniea, K. E. (2015, April). Factors related to privacy concerns and protection behaviors regarding behavioral advertising. In Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems (pp. 1965-1970).

Woon, I., Tai, G. W., ve Low, R. A. (2005). Protection Motivation Theory approach to home wireless security. In Proceeding of 26th international conference on information systems. <http://aisel.aisnet.org/icis2005/31> Erişim Tarihi: 09.10.2023.

Xu, H., Dinev, T., Smith, J., ve Hart, P. (2011). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems*, 12(12), 798-824 .

Xu, H., Gupta, S., Rosson, M. B., ve Carroll, J. M. (2012). Measuring mobile users' concerns for information privacy. Thirty Third International Conference on Information Systems, Orlando.

Xu, F., Michael, K., ve Chen, X. (2013). Factors affecting privacy disclosure on social network sites: an integrated model. *Electronic Commerce Research*, 13(2), 151-168.

Yaşlıoğlu, M. M. (2017). Sosyal bilimlerde faktör analizi ve geçerlilik: Keşfedici ve doğrulayıcı faktör analizlerinin kullanılması. *İstanbul Üniversitesi İşletme Fakültesi Dergisi*, *46*, 74-85.

Yılmaz, R. A. (1999). Duygusal Çekicilikli Reklamların İletişim Etkileri. Yayınlanmamış Doktora Tezi. Eskişehir: Anadolu Üniversitesi Sosyal Bilimler Enstitüsü.

Yorke, D. A., ve Kitchen, P. J. (1985). Channel flickers and video speeders. *Journal of Advertising Research*, 25(2), 21–25.

Youn, S. (2005). Teenagers' perceptions of online privacy and coping behaviors: a risk–benefit appraisal approach. *Journal of Broadcasting & Electronic Media*, 49(1), 86-110.

Youn, S. (2009). Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. *Journal of Consumer Affairs*, 43(3), 389-418.

Youn, S., ve Kim, S. (2019a). Newsfeed native advertising on Facebook: Young millennials' knowledge, pet peeves, reactance and ad avoidance. *International Journal of Advertising* 38(5), 651–83.

Youn, S., ve Kim, S. (2019b). Understanding ad avoidance on Facebook: Antecedents and outcomes of psychological reactance. *Computers in Human Behavior*, 98, 232-244.

Youn, S., ve W. Shin. (2020). Adolescents' responses to social media newsfeed advertising: The interplay of persuasion knowledge, benefit-risk assessment, and ad scepticism in explaining information disclosure. *International Journal of Advertising* 39, no. 2: 213–31.

Zarouali, B., Ponnet, K., Walrave, M., ve Poels, K. (2017). "Do you like cookies?" Adolescents' skeptical processing of retargeted Facebook-ads and the moderating role of privacy concern and a textual debriefing. *Computers in Human Behavior*, 69, 157-165.

Zarouali, B., Poels, K., Ponnet, K., ve Walrave, M. (2018). "Everything under control?": Privacy control salience influences both critical processing and perceived

persuasiveness of targeted advertising among adolescents. Cyberpsychology: *Journal of Psychosocial Research on Cyberspace*, 12(1).

Zhang, L., ve McDowell, W. C. (2009). Am I really at risk? Determinants of online users' intentions to use strong passwords. *Journal of Internet Commerce*, 8(3-4), 180-197.

Zhang, X., Liu, S., Chen, X., Wang, L., Gao, B., ve Zhu, Q. (2018). Health information privacy concerns, antecedents, and information disclosure intention in online health communities. *Information & Management*, 55(4), 482-493.

Zhang, D., Voorveld, H., ve Boerman, S. C. (2023). Privacy Concerns Matter, Knowledge Does Not: Investigating Effects of Online Behavioral Advertising among Chinese and Dutch Adults. *Journal of Current Issues & Research in Advertising*, 1-19.

Zufryden, F. S., Pedrick, J. H., ve Sankaralingam, A. (1993). Zapping and its impact on brand purchase behavior. *Journal of Advertising Research*, 33(1), 58-67.

Zuiderveen Borgesius, F.J. (2015). Improving privacy protection in the area of behavioural targeting. *Information Law Series*, 33, 1-14.

Http-1. NAI, (2021). https://thenai.org/glossary/cookie/ (Erişim Tarihi: 08.03.2022).

Http-2. https://www.youronlinechoices.com/tr/konu-hakkinda (Erişim Tarihi: 14.03.2022).

Http-3. https://www.youronlinechoices.com/tr/konu-hakkinda (Erişim Tarihi: 14.03.2022).

Http-4. https://www.etymonline.com/word/private (Erişim Tarihi: 22.09.2023).

Http-5. https://www.etymonline.com/word/privacy (Erişim Tarihi: 22.09.2023).

Http-6.https://www.oed.com/search/dictionary/?scope=Entries&q=privacy (Erişim Tarihi: 22.09.2023).

Http-7. https://www.etimolojiturkce.com/kelime/mahrem (Erişim Tarihi: 22.09.2023).

Http-8. https://sozluk.gov.tr/ (Erişim Tarihi: 22.09.2023).

Ek 1. Anket ifadeleri

Algılanan Ciddiyet
Hedefli reklamlar için kişisel verilerimin toplanması ciddi bir problemdir
Hedefli reklamlar için kişisel verilerimin kullanılması ciddi bir problemdir
Hedefli reklamlar için kişisel verilerimin paylaşılması ciddi bir problemdir
Hedefli reklamlar için internet davranış geçmişimin takip edilmesi ciddi bir problemdir
Algılanan Savunmasızlık
Hedefli reklamlar için kişisel verilerimin kullanılmasının benim için bir risk oluşturacağını düşünüyorum
Hedefli reklamlar için toplanan kişisel verilerimin kötüye kullanılacağını düşünüyorum
Kişisel verilerimin hedefli reklamlar için kullanılmasının beklenmedik problemlere yol açacağını düşünüyorum
Kişisel verilerimin bilmediğim şirketlerle izinsiz paylaşılacağını düşünüyorum
Algılanan Fayda
Hedefli reklamlar ilgi alanıma yönelik bilgilendirici içeriklere erişmemi sağlar
Hedefli reklamlar ilgi alanıma yönelik eğlenceli içeriklere erişmemi sağlar
Hedefli reklamlar ilgi alanıma yönelik reklam mesajlarıyla karşılaşmamı sağlar
Hedefli reklamlar ilgi alanıma yönelik teklifler (örn: ürün/hizmet önerisi, uygun fiyat teklifi) elde etmemi sağlar
Hedefli reklamlar ilgi alanıma yönelik ürün ve hizmetlerle ilgili yeni bilgilere ulaşmamı sağlar
Gizlilik Endişesi
Hedefli reklam şirketlerinin internet davranış geçmişimi takip ediyor olması beni rahatsız ediyor
Şirketlerin benim hakkımda çok fazla bilgiye sahip olması beni endişelendiriyor
Şirketlerin hakkımdaki bilgilere erişebilmesi beni rahatsız ediyor
Şirketlerin kişisel verilerimi öngöremeyeceğim şekillerde kullanabileceğinden endişeleniyorum
İnternet davranış geçmişimle başkalarının yapabileceği şeylerden (çevrimiçi kimlik hırsızlığı vb.) endişeleniyorum
Gizlilik Kontrolü
Hedefli reklam şirketleri tarafından paylaşılan kişisel verilerim üzerinde kontrol gücüm olduğunu düşünüyorum.
Hedefli reklamların kişisel verilerimi nasıl kullanacağı konusunda kontrol gücüne sahip olduğumu düşünüyorum.
Hedefli reklamların erişimine sunulan kişisel verilerim üzerinde kontrol gücüne sahip olduğumu düşünüyorum.

Öz Yeterlilik
Eğer istersem hedefli reklamlar kullanan şirketlerden kaçınabilirim
Hedefli reklamlardan kaçınacak yeterli bilgiye sahibim
Hedefli reklamlardan kolaylıkla kaçınabilirim
Başkasının yardımına ihtiyaç duymadan, hedefli reklamlar kullanan şirketlerin kişisel verilerime ulaşmasını engelleyebilirim
Tepki Maliyeti
Hedefli reklamlardan kaçınırsam ilgilendiğim ürün - hizmet reklamlarıyla daha az karşılaşırım
Hedefli reklamları engellemeye çalışmak oldukça zaman alıcıdır
Hedefli reklamları engellemeye çalışmak çok fazla zihinsel çaba gerektirir
Tepki Yeterliliği
Reklam engelleme eklentisi kurmak (örn: Adblock) hedefli reklamları önlemede etkili bir yöntemdir
Çerezleri temizlemek hedefli reklamları önlemede etkili bir yöntemdir
Çerezleri kabul etmemek hedefli reklamları önlemede etkili bir yöntemdir
Web tarayıcısını gizli modda kullanmak hedefli reklamları önlemede etkili bir yöntemdir
Web tarayıcı geçmişini temizlemek hedefli reklamları önlemede etkili bir yöntemdir
Kişisel verilere dayalı hedefli reklamların takibinden çıkmak için (www.youronlinechoices.com gibi) devre dışı bırakma sitelerini kullanmak hedefli reklamları önlemede etkili bir yöntemdir
Web tarayıcısında beni takip etme (Do Not Track) özelliğini aktifleştirmek hedefli reklamları önlemede etkili bir yöntemdir
Kişisel verilerin toplanmasını zorlaştıran özel yazılımlar kullanmak (örn: Ghostery) hedefli reklamları önlemede etkili bir yöntemdir
Kişisel veriler istendiğinde yanlış bilgi vermek (yanlış isin, yanlış mail adresi vb.) hedefli reklamları önlemede etkili bir yöntemdir
Reklamdan Kaçınma
İnternette gördüğüm hedefli reklamları kasıtlı olarak görmezden geliyorum
İnternetteki hedefli reklamlardan nefret ediyorum
Kişisel verilerime dayalı hedefli reklamlar hiç olmasaydı daha iyi olurdu
Kişisel verilerime dayalı hedefli reklamları almaktan kaçınırım
Hedefli reklam şirketlerinin izleme listelerinden çıkarım/çıkmayı planlıyorum