



Genç Tüketicilerin Elektronik Ödeme Yöntemi Kullanımlarının Belirleyicilerine Dair Alan Araştırması*

A Field Study on the Determinants of Young Consumers' Use of Electronic Payment Methods

Helin Tombaş¹ ID, Asiye Ayben Çelik² ID

Geliş Tarihi (Received): 22.06.2021

Kabul Tarihi (Accepted): 01.02.2022

Yayın Tarihi (Published): 31.03.2022

Öz: Tüketim pratiklerinin çevrimiçi platformlara artan bir ivmeyle kayıyor olması, beraberinde işletmelerin bu platformlardan yapılan alışverişlerde tüketicilerin olumlu bir deneyimle ayrılması hedefine odaklanmasına neden olmaktadır. Tüketicilere sunulan hizmetin tasarımında satın almanın kilit noktası olan ödeme süreçlerinin doğru şekilde yönetimi önemlidir. Bu bağlamda tüketicilere sunulan elektronik ödeme yöntemlerine dair tüketicinin duyduğu güven ve güvenlik algısı alışverişin satın almayla noktalanmasında belirleyici olacaktır. Çalışmada e-ödeme yöntemlerinin özelliklerinin, algılanan güven ve güvenlikle ilişkisinin sorgulandığı, ayrıca algılanan güven ve güvenliğin elektronik ödeme yöntemlerinin kullanımıyla ilişkisinin incelendiği kavramsal bir model ortaya konulmaktadır. 503 üniversite öğrencisinden anketle toplanan veri, yapısal eşitlik modellemesiyle analiz edilmiştir. Elde edilen bulgular, ödeme yöntemlerine dair güvenlik bildirimleri ve işlem prosedürlerinin algılanan güven ve güvenlik ile pozitif bir ilişkiye sahip olduğu ve algılanan güven ve güvenliğin elektronik ödeme yöntemlerinin kullanımında belirleyicisi olduğu sonucunu göstermektedir.

Anahtar Kelimeler: E-Ticaret, Elektronik Ödeme Yöntemleri, Güven, Güvenlik.

&

Abstract: The fact that consumption practices are shifting to online platforms with an increasing momentum causes businesses to focus on the goal of providing consumers positive experience when shopping from these platforms. In the design of the service offered to the consumer, the correct management of the payment processes, which is the key point of purchasing, is important. In this context, the trust and security perception of the consumer regarding the electronic payment methods offered to the consumer will be decisive in ending the shopping with the purchase. In the study, a conceptual model is presented in which the characteristics of e-payment methods are questioned and their relationship with perceived trust and security, and the relationship between perceived trust and security and the use of electronic payment methods is examined. The data collected by questionnaire from 503 university students were analyzed by structural equation modeling. The findings show that security notifications and transaction procedures for payment methods have a positive relationship with perceived trust and security, and that perceived trust and security are determinants of the use of electronic payment methods.

Keywords: E-Commerce, Electronic Payment Methods, Trust, Security.

Atıf/Cite as: Tombaş, H., Çelik, A. A. (2022). Genç tüketicilerin elektronik ödeme yöntemi kullanımlarının belirleyicilerine dair alan araştırması. *Abant Sosyal Bilimler Dergisi*, 22(1), 47 - 63. doi: <https://doi.org/10.11616/asbi.1025400>

İntihal-Plagiarizm/Etik-Ethic: Bu makale, en az iki hakem tarafından incelenmiş ve intihal içermediği, araştırma ve yayın etiğine uyulduğu teyit edilmiştir. / This article has been reviewed by at least two referees and it has been confirmed that it is plagiarism-free and complies with research and publication ethics. <https://dergipark.org.tr/tr/pub/asbi/policy>

Copyright © Published by Bolu Abant İzzet Baysal University, Since 2000 – Bolu

* Bu makale 2021 yılında Manisa Celal Bayar Üniversitesi Sosyal Bilimler Enstitüsü'nde Dr.Öğr.Üyesi Asiye Ayben Çelik'in danışmanlığında Helin (Aslan) Tombaş tarafından yazılan "Elektronik Ödeme Yöntemlerine Yönelik Tüketicinin Güvenlik ve Güven Algısının İncelenmesi" başlıklı tezden üretilmiştir.

¹ Bilim Uzmanı, Helin Tombaş, Manisa Celal Bayar Üniversitesi, 181188014@ogr.cbu.edu.tr (Sorumlu yazar).

² Dr. Öğr. Üyesi, Asiye Ayben Çelik, Manisa Celal Bayar Üniversitesi, ayben.celik@cbu.edu.tr.

1. Giriş

Günümüz iletişim teknolojilerindeki gelişmeler, internete erişim olanaklarının gelişmesi, akıllı telefon sahipliğinin artması, çevresel etkenler ve pandemi gibi olağanüstü durumlar, tüketicilerin geleneksel alışverişten online alışverişe yönelmesine neden olmuştur. Online satışların özellikle pandemiyle birlikte ciddi artış gösterdiğini Birleşmiş Milletler Ticaret ve Kalkınma Konferansı (United Nations Conference on Trade and Development-UNCTAD) tarafından yapılan 9 ülkeyi kapsayan araştırmada da görmek mümkündür. Araştırmada özellikle pandemiyle birlikte Türkiye ve Çin'in online alışveriş konusunda ciddi bir sıçrama yaşadığını ve araştırmaya katılan bireylerin gelecekte de online alışveriş yapmaya devam edecekleri dolayısıyla bu ivmenin katlanarak devam edeceği öngörülmektedir (bknkz: UNCTAD, 2021. Erişim Tarihi 08.05.2021).

Online alışverişin olumlu bir deneyim olarak tasarlanması ve tüketici memnuniyetini destekleyebilmesi için geliştirilen çok sayıda elektronik ödeme yöntemi mevcuttur. Ancak bu yöntemlerin yol açabileceği sorunlar dolayısıyla ödeme konusu, tüketicilerin elektronik alışverişlerinde kaygı duyduğu bir aşama olarak gündeme gelmektedir. Piyasada gerek online gerekse geleneksel alışverişte tüketicilerce kullanılmakta olan başlıca ödeme yöntemlerini; kredi kartı, temassız ödeme, banka kartı, eft, elektronik çek, elektronik cüzdan, sanal kart, akıllı kart, mobil ödeme, paypal ve bkm ekspres olarak sıralayabilmek mümkündür (Ooi ve Tan, 2016:36).

Çalışma, sözü edilen elektronik ödeme yöntemlerine dair tüketicilerin duyduğu güven ve güvenlik algısının ödeme yöntemlerinin kullanımıyla olan ilişkisini tespit etmeyi amaçlamaktadır. Bu bağlamda üniversite öğrencileri üzerinde gerçekleştirilen saha araştırması ve genç tüketicilere dair araştırma sonuçlarıyla hem literatüre katkı sağlamak hem de uygulayıcılara iş stratejilerinin isabetliliğini arttırmada bilimsel bilgi sunmak hedeflenmektedir.

Çalışmanın organizasyonunda giriş kısmını, literatür taraması üzerine inşa edilen kavramsal çerçevenin belirlenmesi ve bu doğrultuda geliştirilen hipotezler ve model önerisi izlemekte; ardından araştırmanın yöntemlerine yer verilmektedir. Daha sonra elde edilen verilerin analiz ve bulguları açıklanmaktadır. Çalışmanın son bölümünü ise sonuç ve öneriler kısmı oluşturmaktadır.

2. Kavramsal Çerçeve, Geliştirilen Hipotezler ve Model Önerisi

Kavramsal çerçeveyi oluşturmak üzere literatürü kapsamlı bir şekilde incelemek amacıyla, öncelikle çalışma kapsamında bibliyometrik analiz yöntemine başvurulmuş, konuyla ilgili dünya çapında ilgi çekmeyi başarmış yayınlar tespit edilmiş, ardından yapılan çalışmaların bulguları doğrultusunda; elektronik ödeme yöntemleri, e-ticarette güvenlik, elektronik ödeme yöntemlerine duyulan güven ve algılanan güvenlik konularına dair bilimsel bilgilere yer verilmiştir.

Çalışmada Scopus ve Web of Science veri tabanlarında, internet kullanımının yaygınlaştığı 1995 yılından itibaren, 1995-2020 yılları arasındaki döneme ait yayınlarda, "e-ödeme yöntemleri", "e-ödeme yöntemleri kullanımı", "elektronik ticaret", "güvenlik" ve "güven" anahtar kelimeleriyle bir tarama yapılmış ve ortaya çıkan çalışmalar incelenmiştir.

Toplamda 146 yayına ulaşılmış ve ağırlıklı olarak bilgisayar bilimleri, ardından telekomünikasyon, işletme ve ekonomi alanlarında araştırma konusu edilen bu kavramlara dair, Tablo 1'de Scopus ve Web of Science veri tabanlarında en çok atıf alan yayınların, atıf sayılarının yıllara göre dağılımına yer verilmiştir. Abrazhevich (2001), Bellare vd. (2000), Kim vd. (2010), Liebana-Cabanillas vd. (2017), Obaidat ve Boudriga (2007), Ooi ve Tan (2016), Smith (2005), Tan ve Thoen (2000) ve Tsiakis ve Sthephanides(2004) en çok atıf alan yayınlar arasında olduğu görülmektedir.

Tablo 1: En Çok Atıf Alan Yayınların Yıllara Göre Atıf Dağılımı

Scopus							
Yayınlar/Yıl	<2017	2017	2018	2019	2020	>2020	Total
(Tan ve Thoen, 2000)	260	11	12	11	10	2	306
(Kim vd., 2010)	119	24	26	26	29	2	226
(Tsiakis ve Sthephanides, 2004)	46	14	8	7	12	1	88
(Obaidat ve Boudriga 2007)	30	2	10	9	16	2	69
(Smith, 2005)	61	3	0	0	2	1	67
Web of Science							
Yayınlar/Yıl	<2017	2017	2018	2019	2020	>2020	Total
(Kim vd., 2010)	87	16	21	14	18	2	158
(Ooi ve Tan, 2016)	0	9	20	38	46	6	119
(Bellare vd., 2000)	69	3	0	2	0	0	74
(Liebana-Cabanillas vd., 2017)	0	0	3	16	18	1	38
(Abrazhevich, 2001)	15	1	2	0	0	0	18

2.1. Kavramsal Çerçeve

Bibliyometrik analiz kapsamında karşılaşılan yayınlardan hareketle, literatürde konunun hangi açılardan, hangi değişkenler eşliğinde incelendiği araştırılmış ve şu bulgulara erişilmiştir:

Bellare vd. (2000), çalışmasında elektronik ödeme işlemlerinde oluşan güvenlik endişelerin giderilmesi amacıyla Güvenli Elektronik İşlem (Secure Electronic Transaction-SET) güvenlik katmanını incelemeye almıştır. SET aracılığıyla yapılan herhangi bir işlemin; satıcı, ödeme ağ geçidi ve müşteri olmak üzere üç ayağı içerdiğine vurgu yaparak sağladığı yararlar üzerinde durmuştur. Tan ve Thoen (2000), çalışmalarında elektronik ticaret için genel bir güven modeli oluşturmuşlardır. Model, "bir kişinin sahip olduğu işlem güveni seviyesi, kişisel eşliğinin üzerinde olmalıdır" ana fikrine dayanmaktadır. İncelenen çalışmada bu durumun, işlemin türüne ve işleme dâhil olan diğer taraflara bağlı olduğu belirtilmiştir. İşlem güveni düzeyinin iki temel bileşeninin, karşı tarafa duyulan güven ve kontrol mekanizmalarına olan güven olduğu ileri sürülmüştür. Güven ve kontrol arasındaki ilişki genellikle ikame veya tamamlayıcı bir ilişki olarak görülmüştür. Yani bu modele göre eğer güven seviyesi eşğin altında ise, o zaman güvenin eşik seviyesine ulaştırmak için kontrol tarafından tamamlanması gerektiği üzerinde durmuşlardır (Bellare vd., 2000: 611-627; Tan ve Thoen, 2000: 61-74).

Abrazhevich (2001), çalışmasında ödeme sistemlerinin kullanıcılar açısından önemli olan özelliklerinden güven, uygulanabilirlik, kullanım kolaylığı, güvenlik, verimlilik, izlenebilirlik ve güven yönünden inceleyip önemine vurgu yapmıştır. Smith (2005), çalışmasında elektronik ödeme ve çevrimiçi işlemlerde oluşan güvenlik endişelerini gidermek amacıyla tasarlanan SSL güvenlik katmanı üzerinde durmuştur. Bilgilerin daha güvenli paylaşılması ve ödeme bilgilerinin saklanması bakımından geliştirilmiş bu sistemin önemine değinmiştir (Abrazhevich, 2001: 81-90; Smith, 2005: 101-121).

Tsiakis ve Sthephanides (2005), çalışmalarında güvenlik ve güven kavramlarının elektronik ödeme yöntemlerinin ortak bir finansal işlem aracı olarak kabul edilmesi ve tesis edilmesi için gerekliliğine vurgu yaparak bu kavramlar üzerinde durmuşlardır. Güçlü ve uzun süreli iş ilişkilerinin güvene bağlı olduğunu belirterek elektronik ödeme yöntemlerinin güvenli kabul edilebilmesi için çeşitli gereksinimlerin (bütünlük, kimlik doğrulama, dolandırıcılığın önlenmesi ve gizlilik) karşılanması gerektiğine işaret etmişlerdir. Aynı zamanda güvenli işlem için yeni bir ödeme yöntemi veya güven altyapısı oluşturmak amacıyla çeşitli veri şifreleme tekniklerinden yararlanılması gerektiği sonucuna varmışlardır. Obaidat ve Boudriga (2007) ise, çalışmasında internetteki bilgisayar korsanları ve ağ saldırılarına karşılık e-güvenlikte bilgi ve ağ güvenliği üzerinde durmuştur. Bunun için güvenlik saldırıları, güvenlik mekanizmaları ve güvenlik servisi olmak üzere bilgi güvenliğinin üç yönünü incelemiştir (Obaidat ve Boudriga, 2007: 3-24).

Kim vd. (2010), çalışmalarında elektronik ödeme yöntemlerinin güvenliği ile ilgili sorunları tüketiciler açısından deneysel bir çalışma olarak anket yoluyla Kore'de incelemiştir. Elde edilen bulgularla hem e-ödeme yöntemlerine dair sahip olunan teknik korumaların hem de gerçekleştirilen güvenlik

bildirimlerinin, tüketicilerin algılanan güvenliği arttırmada önemli faktörler olduğunu belirtmişlerdir. Liebana-Cabanillas vd. (2017), geleneksel olarak kullanılan ödeme sistemlerinin internet, sosyal ağlar, mobil cihazlar vb. teknolojilerin ortaya çıkmasıyla oluşan mobil ödemenin avantajlarına değinmişlerdir. Makaleye göre kullanım kolaylığı ve zamandan tasarruf ettirmesi göz önüne alındığında teknolojik gelişmelerin kullanıcıların satın alma davranışını değiştirebileceğini göstermiştir (Liebana-Cabanillas vd., 2017:25-64).

Sonuç olarak çalışmalarda görüldüğü üzere, genel olarak elektronik ödeme yöntemlerinin ve e-ticaretin güvenilirliği araştırma konusu edilmiştir. Bu çalışma, mevcut literatürün çoğunluğundan farklı olarak, tüketicilerin bakış açısıyla güvenlik ve güveni ve bunların elektronik ödeme yöntemleri kullanımı üzerindeki etkilerini araştırmakta ve elektronik ödeme yöntemlerinde algılanan güvenlik ve duyulan güvenin öncüllerini anlamaya çalışmaktadır. Anket yoluyla elde edilen verilerle elektronik ödeme yöntemlerine yönelik tüketicilerin güven ve güvenlik algısına dair görüşleri hakkında kapsamlı bir araştırma sunulacaktır.

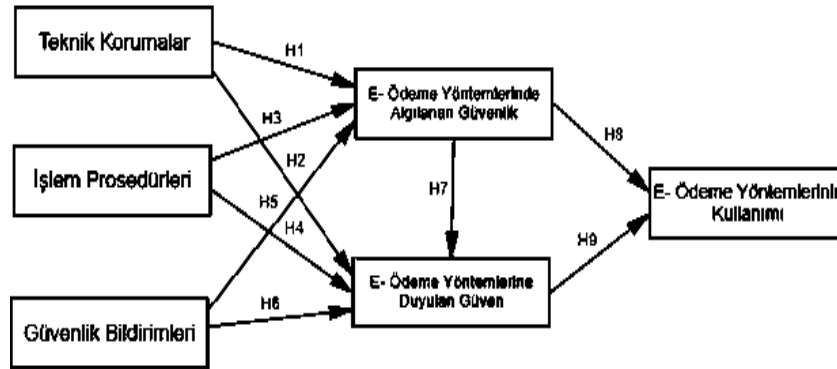
2.2. Araştırma Hipotezleri ve Model Önerisi

Araştırma kapsamında test edilmek istenen model için, bu alanda yayınlarıyla global ölçekte en fazla atıf almayı başarmış Kim vd.'nin (2010) çalışmasından yola çıkılmıştır. Bu kısımda araştırma modeline ve model kapsamında elektronik ödeme yöntemlerine ilişkin tüketicinin güven ve güvenlik algısıyla ilişkilendirilen değişkenlere, test edilecek hipotezlere ve model önerisine yer verilmektedir.

2.2.1. Araştırma Modeli

Bu çalışma, algılanan güvenlik ve duyulan güvenin tüketicilerin elektronik ödeme yöntemlerinin kullanımı üzerindeki etkisini test etmek için Kim vd.'nin (2010) çalışmalarında kullandıkları araştırma modeline dayanmaktadır. Daha önce belirtildiği gibi hem algılanan güvenlik hem de duyulan güven elektronik ödeme yöntemlerinin kullanımı için önemli birer ölçüttür. Algılanan güvenlik ve duyulan güven eksikliği, tüketicilerin elektronik ödeme yöntemlerini kullanma isteğini azaltabilmektedir (Linck vd., 2006: 3). Bu nedenle, algılanan güvenlik ve duyulan güveni etkileyen faktörleri incelemek bu açıdan önemli olmaktadır. Şekil 1 araştırma modelini özetlemektedir. Şekilde gösterildiği üzere teknik koruma, işlem prosedürleri ve güvenlik bildirimleri değişkenlerinin, tüketicinin elektronik ödeme yöntemleri kullanımındaki güvenlik ve güven ile ilişkili olduğu ve bu iki değişkenin de e-ödeme yöntemlerinin kullanımıyla ilişkili olduğu varsayımına dayanılarak model ortaya konmuştur.

Şekil 1: Araştırma Modeli ve Hipotezler



Kaynak: Kim, vd., (2010:92)

2.2.2. Araştırma Hipotezleri

2.2.2.1 Elektronik Ödeme Yöntemlerinde Teknik Korumalar

Teknik koruma, işlem sürecinde ödeme güvenliğini sağlamak için kullanılan gizlilik, bütünlük ve istikrarı içeren bir dizi özel teknik mekanizma olarak tanımlanmaktadır (Barkhordari vd., 2016: 95; Diep, 2020: 2).

Benzer şekilde Kim vd. (2010) ve Chellappa ve Pavlou (2002), teknik korumaların algılanan güvenlik ve duyulan güven üzerinde olumlu bir etkiye sahip olduğunu belirtmişlerdir (Chellappa ve Pavlou, 2002: 361; Kim vd., 2010: 88). Hazae vd. (2018)'ye göre internet, bireysel işlemler üzerinde doğrudan insan kontrolü olmayan açık bir ağ olduğundan elektronik ödeme yöntemlerini destekleyen teknik altyapının güvenlik saldırılarına karşı dirençli olması gerekmektedir. Bu riski azaltmak için tasarlanan teknik korumaların, tüketici güveni sorunu ele alınmadan önce dikkate alınması gerekmektedir (Hanzaee ve Alinejad, 2012: 1576). Şifreleme ve kimlik doğrulama teknikleri dahil elektronik ödeme yöntemleri için mevcut güvenlik teknolojilerini gözden geçiren bazı araştırmacılar, güvenli bir elektronik ödeme yönteminin dolandırıcılık faaliyetlerine karşı güvenlik sağlaması ve tüketicilerin gizliliğini koruması gerektiği sonucuna varmaktadırlar (Barkhordari vd., 2016: 95; Hanzaee ve Alinejad, 2012: 1576). Bu bulgulara dayanarak aşağıdaki hipotezler oluşturulmuştur:

H₁: Teknik korumalar ile tüketicilerin e-ödeme yöntemlerinde algıladığı güvenlik arasında pozitif bir ilişki vardır.

H₂: Teknik korumalar ile tüketicilerin e-ödeme yöntemlerine duyduğu güven arasında pozitif bir ilişki vardır.

2.2.2.2. Elektronik Ödeme Yöntemlerinde İşlem Prosedürleri

İşlem prosedürleri, tüketicilerin elektronik ödeme yöntemleri satıcıları ile işlemlerinin tamamlanmasına kadar gerçekleştirdikleri bir süreçtir (Diep, 2020: 2). Bir başka ifadeyle, tüketicilerin eylemlerini kolaylaştırmak ve güvenlik korkularını ortadan kaldırmak için tasarlanmış adımlardır (Hanzaee ve Alinejad, 2012: 1576). Kim vd. (2010), çalışmalarında iyi tanımlanmış işlem prosedürlerinin, tüketicilerin elektronik ödeme yöntemlerinin kullanımını kolaylaştırdığını ve tüketicilerin güvenlik endişelerini ortadan kaldırmalarına yardımcı olduklarını belirtmişlerdir (Kim vd., 2010: 88). Elektronik ödeme işlemleri sırasında genellikle üç ana işlem prosedürü uygulanmaktadır. Bu prosedürler şunlardır: (1) işlemden önce her katılımcıya kimlik doğrulaması yapmak; (2) tüketicilere ödemenin tanımlanmasına yönelik birkaç adım sunmak; (3) ödemenin tamamlanmasının ardından her katılımcıya onay mesajları göndermek (Öney vd., 2017: 400). Buna göre doğru işlem prosedürlerinin algılanan güvenlik ve duyulan güven üzerinde etkisi olacağına inanılmaktadır (Diep, 2020: 2). Söz konusu bulgular eşliğinde şu hipotezler oluşturulmuştur:

H₃: İşlem prosedürleri ile tüketicilerin e-ödeme yöntemlerinde algıladığı güvenlik arasında pozitif bir ilişki vardır.

H₄: İşlem prosedürleri ile tüketicilerin e-ödeme yöntemlerine duyduğu güven arasında pozitif bir ilişki vardır.

2.2.2.3. Elektronik Ödeme Yöntemlerinde Güvenlik Bildirimleri

Güvenlik bildirimleri, elektronik ödeme yöntemleri üzerindeki güvenlik konusunda satıcıların kesin beyanlarıdır. Bu ifadeler, tüketiciler için kamuya açık bir şekilde yayınlanmaktadır (Diep, 2020: 3). Araştırmacılar güvenlik özellikleri, veri koruma ve gizlilik, güvenlik politikaları ve güvenlik önlemleriyle ilgili diğer açıklayıcı içerikleri detaylandıran ifadelerin, kullanıcıların güvenli elektronik ödeme yöntemlerinin ne olduğuna dair daha doğru yorumlar oluşturmalarına yardımcı olarak internet üzerinden alışveriş yapma olasılığını arttıracaklarını belirtmişlerdir (Hanzaee ve Alinejad, 2012: 1576). Bu bulgulara dayanarak şu hipotezler oluşturulmuştur:

H₅: Güvenlik bildirimleri ile tüketicilerin e-ödeme yöntemlerinde algıladığı güvenlik arasında pozitif bir ilişki vardır.

H₆: Güvenlik bildirimleri ile tüketicilerin e-ödeme yöntemlerine duyduğu güven arasında pozitif bir ilişki vardır.

2.2.2.4. Elektronik Ödeme Yöntemlerinde Algılanan Güvenlik

Kim vd. (2010) algılanan güvenliği, “tüketicilerin e-ödeme yöntemlerinin güvenliğine ilişkin öznel değerlendirmesi” olarak tanımlamıştır. Benzer şekilde Halaweh (2017), güvenliği müşterilerin e-ticarete girmesini engelleyen bir sorun olarak belirtmiş, elektronik ödeme yöntemlerinde algılanan güvenliği, “tüketicilerin kişisel bilgilerinin taşıma ve saklama sırasında uygun olmayan taraflarca güvenli beklentilerine uygun şekilde görüntülenmeyeceğine, saklanmayacağına ve değiştirilmeyeceğine inandıkları öznel olasılık” olarak tanımlamıştır (Halaweh, 2017: 630). Tüketiciler farklı deneyim ve beklentilere sahip olduklarından, elektronik ödeme yöntemlerine yönelik farklı tutumlar benimseyebilmektedirler (Kim vd., 2010: 88). Bu nedenle, elektronik ödeme yöntemlerinin algılanan güvenliği kişiden kişiye değişebilir (Öney vd., 2017: 401). Bir elektronik ödeme yönteminde algılanan güvenlik seviyesi çok düşükse, tüketicilerin bir işleme girme olasılığı daha düşüktür (Kim vd., 2010: 88). Bu doğrultuda aşağıdaki hipotezler oluşturulmuştur:

H₇: Tüketicilerin e-ödeme yöntemlerinde algıladığı güvenlik ile e-ödeme yöntemlerine duyduğu güven arasında pozitif bir ilişki vardır.

H₈: Tüketicilerin e-ödeme yöntemlerinde algıladığı güvenlik ile e-ödeme yöntemleri kullanımı arasında pozitif bir ilişki vardır.

2.2.2.5 Elektronik Ödeme Yöntemlerine Duyulan Güven

Tsiakis ve Sthephanides (2005), duyulan güveni, “tüketicilerin elektronik ödeme işlemlerinin beklentilerine uygun olarak yürütüleceğine olan inancı” olarak tanımlamışlardır (Tsiakis ve Stephanides, 2005:11). Al-Dala’in vd. (2009: 3134)’ne göre tüketicilerin elektronik ödeme yöntemlerine olan güveni ne kadar yüksekse, satın alma niyetleri o kadar yüksek ve buna karşılık tüketicileri elde tutmak o kadar kolay olmaktadır. Mallat’a (2007) göre elektronik ödeme yöntemlerine duyulan güvenin müşteri sadakatine olumlu bir etkisi vardır (Mallat, 2007: 417). Kullanıcıların ve satıcıların, güvenilmeyen bir şirketin güvenli ödeme sisteminden çok, güvenilir bir şirketin güvensiz ödeme sistemini kullanma olasılığının yüksek olduğu iddia edilmektedir (Kniberg, 2002: 2). Sözü edilen bulgular doğrultusunda H₉ hipotezi kurulmuştur:

H₉: Tüketicilerin e-ödeme yöntemlerine duyduğu güven ile e-ödeme yöntemleri kullanımı arasında pozitif bir ilişki vardır.

3. Araştırmanın Yöntemi

Nicel araştırma deseni çerçevesinde gerçekleştirilen bu çalışmada anket yoluyla veri toplanmıştır. Anket formunun oluşturulmasında elektronik ödeme yöntemlerine yönelik güvenlik ve güven algısı ile ilgili literatür detaylı şekilde incelenerek bu alanda en fazla atıf alma başarısını gösteren Kim vd. (2010) tarafından yazılan “An Empirical Study of Customers’ Perceptions of Security and Trust” adlı çalışmada oluşturulan ölçek maddelerinden yararlanılmıştır. Ölçeklerin yapı geçerliliğini test etmek için “Açıklayıcı Faktör Analizi (AFA)” ile “Doğrulayıcı Faktör Analizi (DFA)” ve ölçeklerin güvenilirlik durumunu test etmek amacıyla da “Güvenilirlik Analizi” ve “Madde Toplam Puan Korelasyonu” yapılmıştır. Model kapsamında öne sürülen hipotezler test edilirken yapısal eşitlik modelinden (YEM) faydalanılmıştır.

Araştırma için iki bölümden oluşan bir anket düzenlenmiştir (Ek: 1). Ankettin birinci bölümünde, lisans eğitimi sürdürmekte olan öğrencilerin cinsiyeti ile katılımcıların, internet sitesinden alışveriş yapma sıklığı ve internet alışverişlerinde en çok kullandığı ödeme yöntemlerinin tespitine dair sorular yer almaktadır. İkinci bölümde ise bağımlı ve bağımsız değişkenlere yönelik 5’li likert tipi ölçeğe göre toplam 29 ifade için katılımcıların değerlendirme yapması istenmiştir.

Saha araştırması, Manisa Celal Bayar Üniversitesi’nde yapılmış olup, Etik Kurul izni alındıktan sonra, 17.01.2021 –10.03.2021 tarihleri arasında lisans öğrenimi görmekte olan 503 öğrenciden anket yoluyla veri toplanmıştır. Çalışmada anket “Google Forms” aracılığıyla online platformda düzenlenmiş ve kolayda ve kartopu örnekleme yöntemlerinden yararlanılarak veri toplanmıştır. Araştırma modeli kapsamında

kurulan hipotezlerin testi için yapısal eşitlik modellemesinden faydalanılmıştır. Veri analizi yapılırken ise AMOS 23.0 ve SPSS 25.0 ve programları kullanılmıştır.

4. Veri Analizi ve Bulgular

4.1. Veri Analizi

YEM'in yapılabilmesi için veri setinin çok değişkenli normal dağılımı ve çoklu normallik varsayımını sağlaması gerekmektedir (Byrne, 2001: 98). Bu bağlamda kullanılan verilerin normal dağılıma uygunluğu, çarpıklık ve basıklık değerlerine bakılarak test edilmiştir. Bahsedilen değerlerin ise ± 3 yer alması veri setinin normal dağılım sağladığını göstermektedir (Demirağ ve Durmaz, 2019: 707). Yapılan analizde de tüm değişkenler için bu koşul sağlanmış ve bu sayede verilerin normal dağılım gösterdiği tespit edilmiştir. Sağlanması gereken diğer bir varsayım olan çoklu normallik varsayımı ise Mahalanobi yöntemiyle test edilmiştir. Bu doğrultuda aykırı-uç değerlerin varlığı incelenip eğer aykırı-uç değer varsa çıkarma işlemi yapılmıştır (Esen ve Timor, 2019: 268). Anketi dolduran 503 katılımcıdan toplanan veri setinde yer alan aykırı-uç değerlerin çıkarılması sonucunda veri seti 490'a düşürülmüş ve nihayetinde çoklu normallik varsayımı sağlanmıştır.

4.1.1 Katılımcılara İlişkin Demografik Veri ve Özellikleri

Katılımcıların demografik özelliğine Tablo 2'de yer verilmektedir. Ankette yer verilen sorular Manisa Celal Bayar Üniversitesi'ndeki lisans eğitimini sürdürmekte olan öğrencilere yönlendirildiği için yaş, eğitim seviyesi ve aylık gelir gibi demografik özelliklerini belirleyici sorular çıkartılarak yalnızca cinsiyet durumu incelemeye alınmıştır.

Tablo 2: Katılımcılara İlişkin Demografik Veri ve Özellikleri

Değişkenler		n	%	
Cinsiyet	Kadın	284	58.0	
	Erkek	206	42.0	
İnternet Alışveriş Sıklığı	Hemen hemen her gün	13	2.7	
	Haftada Bir Kere	97	19.8	
	Ayda Bir Kere	202	41.2	
	2-3 Ayda Bir Defa	128	26.1	
	Yılda Bir, İki Defa	47	9.6	
	Hiç	3	0.6	
Alışverişlerde Kullanılan Ödeme Yöntemi	Sanal Kart	Evet	102	20.8
		Hayır	388	79.2
	Kredi ya da Banka Kartı	Evet	430	87.8
		Hayır	60	12.2
	Nakit	Evet	60	12.2
		Hayır	430	87.8
	EFT ve Havale	Evet	47	9.6
		Hayır	443	90.4
	E-cüzdan	Evet	32	6.5
		Hayır	458	93.5
	Sanal Para	Evet	5	1.0
		Hayır	485	99.0
Paypal	Evet	9	1.8	
	Hayır	481	98.2	
Toplam		490	100.0	

Yapılan anketten değerlendirmeye alınan verilere göre elde edilen sonuçlar tabloda incelendiğinde, katılımcıların %60'ından fazla internet alışverişini tercih ederken, ödeme yöntemi olarak e-cüzdan, sanal kart, eft, havale ve paypal gibi alternatif e-ödeme yöntemleri yerine bireylerin yaklaşık %90'lık kısmı en klasik ödeme yöntemlerinden olan kredi kartı ya da banka kartı kullandıklarını ifade etmişlerdir. %20,8 olarak sanal kart ile ödeme şekli de en çok tercih ettikleri ikinci sık kullanılan yöntem olmuştur. Dolayısıyla lisans öğrencilerine uyguladığımız anket sonuçlarına göre bu yaş aralığındaki bireylerin genel olarak online alışveriş yapmayı tercih edebildiklerini ve bunu yaparken geleneksel ödeme araçlarını kullandıkları sonucuna ulaşılmıştır.

4.1.2. Analiz Sonuçları

Açımlayıcı faktör analizi yapılmadan önce örneklem büyüklüğünün faktör analizi yapmaya yeterli olup olmadığını test etmek için Kaiser-Meyer-Olkin (KMO) test değerleri ile korelasyon matrisindeki ilişkilerin analizine uygunluğunu tespit etmek için Bartlett küresellik testi sonuçlarına bakılmıştır. Yapılan analizde KMO değerinin 0.899 olduğu belirlenmiştir ve kabul edilebilir değer aralığında olduğu görülmüştür (Altunışık vd., 2010: 266). Ayrıca yapılan Bartlett küresellik testi sonuçlarına bakıldığında, elde edilen ki kare değerinin kabul edilebilir bir değerde olduğu tespit edilmiştir ($\chi^2(406) = 8172.925$; $p < 0,05$) (Kaya, 2013: 180).

Yapılan açımlayıcı faktör analizi sonucunda ise maddelerin faktör yüklerinin 0.40'ın üzerinde olduğu ve kabul edilebilir düzeyde olduğu görülmektedir (Acaroğlu, 2014: 12). Ayrıca yapılan açımlayıcı faktör analizi sonucunda 29 maddelik ölçeğin 6 alt boyutu olduğu belirlenmiştir. Bu faktörler toplam varyansın %65.725'ini açıklamaktadır. Açımlayıcı faktör analizinde açıklanma oranının %50'nin üzeri olması yeterli kabul edilmektedir (Büyüköztürk, 2002: 477; Tavşancıl, 2005: 48). Yapılan analizde faktörler, toplam varyansın %65.725'ini açıkladığından yeterli kabul edildiği görülmektedir.

Ek olarak ölçeğinin ve boyutlarının güvenilirlikleri ayrı ayrı değerlendirilmiştir. Tabloda görüldüğü üzere hepsi güvenilir ölçek olarak değerlendirilmiştir (Anderson ve Gerbing, 1988: 417). Bu araştırmada ölçeğin

açımlayıcı analizine istinaden ele alınan değişkenlerin açıklanan varyans değerleri, güvenilirlik katsayıları, öz değerleri ve toplam madde korelasyon değerleri Tablo 3'te verilmektedir.

Tablo 3: Araştırmada Kullanılan Ölçeğin Açımlayıcı Faktör Analizi

İfadeler	Faktörler						Toplam Madde Korelasyonu
	F1: Güvenlik Bildirimleri	F2: İşlem Prosedürleri	F3: Duyulan Güven	F4: Teknik Koruma	F5: Algılanan Güvenlik	F6: Kullanım	
M15	0.793						0.784
M17	0.785						0.685
M16	0.763						0.723
M18	0.755						0.683
M13	0.721						0.698
M14	0.721						0.726
M4		0.820					0.705
M5		0.805					0.701
M6		0.782					0.610
M2		0.703					0.649
M1		0.587					0.460
M3		0.573					0.516
M25			0.764				0.826
M24			0.733				0.852
M26			0.731				0.773
M23			0.670				0.688
M9				0.748			0.660
M8				0.667			0.604
M12				0.618			0.499
M7				0.603			0.528
M10				0.592			0.581
M11				0.577			0.529
M20					0.772		0.764
M21					0.762		0.692
M19					0.706		0.979
M22					0.653		0.462
M28						0.860	0.788
M29						0.818	0.649
M27						0.714	0.591
Güvenirlilik	0.893	0.824	0.901	0.807	0.800	0.806	0.919
Açıklanan Varyans (%)	14.228	12.349	10.268	10.252	10.139	8.490	65.725
Öz Değer (Λ)	9.401	3.163	2.228	1.744	1.332	1.193	

KMO= 0.899; $\chi^2(406) = 8172.925$; Bartlett Küresellik Testi (p) = 0.000

4.1.2.1. Ölçüm Modeli, Geçerlilik ve Güvenirlilik

Açımlayıcı faktör analizinde 29 ölçeğin 6 alt boyut altında toplanan yapı modelinin uyumunun tespit edilebilmesi amacıyla doğrulayıcı faktör analizi yapılmıştır. Yapılan analizde ölçüm modeline ilişkin sonuçlar da aşağıdaki tabloda yer almaktadır.

Ölçüm modelinin güvenilirliği test eden iki değerden daha bahsetmek mümkündür. Bunlar ortalama açıklanan varyans (AVE) ve bileşik güvenilirlik (CR) değerleridir. Bunlar hem geçerliliği hem de güvenilirliği test eden iki değerdir. Bu doğrultuda AVE değerleri eşik değer olan 0.40'ın üzerinde, CR değerleri ise eşik değer olan 0.70 değerinin üzerinde olmalıdır (Dubihlela ve Dhurup, 2014: 36-37). Tablo 4'te yer alan ölçüm modeli sonuçları incelendiğinde bu değerlerin kabul edilebilir düzeyde olduğu

görülmektedir. Değişkenler arası faktör yükleri incelendiğinde ise maddelerin faktör yüklerinin 0.40'ın üzerinde olduğu ve kabul edilebilir düzeyde olduğu görülmektedir (Acaroğlu, 2014: 12).

Tablo 4: Ölçüm Modeline İlişkin Sonuçlar

Faktörler	İfadeler	Faktör Yükleri	Standart Hata	t Değerleri	P Değerleri	AVE	CR
F1: Güvenlik Bildirimleri	M15	0.862	-	-	-	0.57	0.89
	M17	0.677	0.050	16.280	***		
	M16	0.783	0.041	19.981	***		
	M18	0.700	0.053	17.030	***		
	M13	0.724	0.048	17.731	***		
	M14	0.766	0.046	19.257	***		
F2: İşlem Prosedürleri	M4	0.838	-	-	-	0.48	0.84
	M5	0.827	0.051	20.573	***		
	M6	0.773	0.055	18.675	***		
	M2	0.648	0.060	14.946	***		
	M1	0.437	0.079	9.509	***		
	M3	0.539	0.073	11.734	***		
F3: Duyulan Güven	M25	0.913	-	-	-	0.70	0.90
	M24	0.878	0.034	27.927	***		
	M26	0.855	0.036	26.620	***		
	M23	0.686	0.050	17.753	***		
F4: Teknik Koruma	M9	0.725	-	-	-	0.42	0.81
	M8	0.690	0.077	13.809	***		
	M12	0.551	0.071	11.136	***		
	M7	0.614	0.068	12.370	***		
	M10	0.676	0.074	13.539	***		
	M11	0.604	0.065	12.158	***		
F5: Algılanan Güvenlik	M20	0.887	-	-	-	0.59	0.85
	M21	0.800	0.037	21.620	***		
	M19	0.844	0.040	23.403	***		
	M22	0.490	0.074	11.176	***		
F6: Kullanım	M28	0.961	-	-	-	0.65	0.85
	M29	0.774	0.041	18.749	***		
	M27	0.657	0.059	15.541	***		

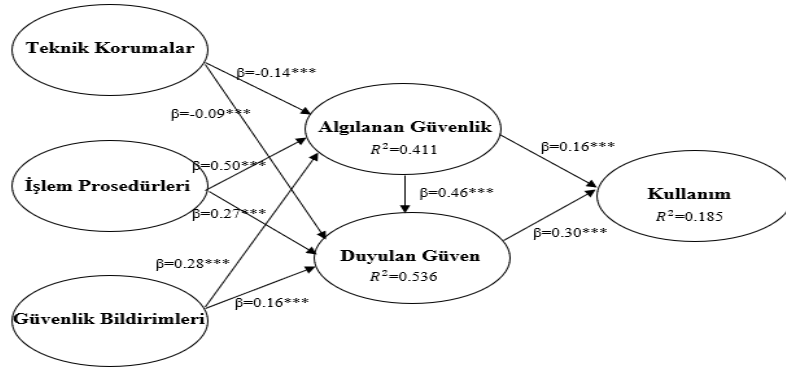
***p<0.05

4.2. Bulgular ve Tartışma

Bu çalışmada öne sürülen hipotezler test edilirken araştırma modeli ve veri uyumunu gösteren yapısal eşitlik modelinden (YEM) faydalanılmıştır. YEM, araştırma modelinin geçerliliğinin bütün olarak değerlendirilmesine ve değişkenler arasında ilişkinin gücünü ve yönünün belirlenmesine olanak sağlamaktadır.

Yapısal eşitlik modellemesi yapılırken Amos 23.0 programından faydalanılmıştır. YEM bulguları Şekil 2'de yer almaktadır.

Şekil 2: Yapısal Eşitlik Modelinin Sonuçları



Yapısal eşitlik modeli ile elde edilen genel uyum değerleri ve tavsiye edilen uyum iyiliği değerleri incelendiğinde; Tablo 5'te görüldüğü üzere modelin kabul edilebilir uyum gösterdiği görülmektedir. Tavsiye edilen uyum iyiliği değerleri Schermelleh-Engel ve Moosbrugger'ın (2003) çalışmasından alınmıştır (Schermelleh-Engel ve Moosbrugger, 2003:52).

Tablo 5: Yapısal Modelin Uyum İyiliği Değerleri

Yapısal Modelin Değerleri		Tavsiye Edilen Değerler
χ^2/df	2.870	≤ 5
RMSEA	0.062	≤ 0.08
GFI	0.870	≥ 0.80
AGFI	0.841	≥ 0.80
CFI	0.916	≥ 0.80
NFI	0.878	≥ 0.80
IFI	0.917	≥ 0.80
TLI	0.904	≥ 0.80
SRMR	0.063	≤ 0.10

$\chi^2: 1021.887, df: 356, p:0,000$

YEM'de değişkenlerin aralarındaki ilişkileri değerlendirmeyi sağlayan yol analizi bulguları Tablo 6'da yer almaktadır. Tabloda yer alan tahminler katsayıları, analize alınan değişkenlerin aralarındaki ilişkileri göstermektedir. Yapılan analiz sonucunda, p değerlerine bakarak bağımsız değişkenlerin bağımlı değişkenler üzerinde istatistiksel olarak anlamlı bir ilişkinin varlığı dikkat çekerken, beta değerinin negatif olması negatif yönlü bir ilişkisi olduğunu, pozitif olması pozitif yönlü bir ilişkisi olduğunu göstermektedir. Yol analizi sonuçlarına göre araştırmada yer alan hipotezler incelendiğinde de ilişki yönlerinin negatif olması gerekçesiyle H₁ ve H₂'nin desteklenmediği görülmektedir.

Tablo 6: Yol Analiz Sonuçları

Etki	Tahmin	Standart Hata	t	p	Std. Tahmin (β)	Sonuç
Teknik Korumalar Algılanan Güvenlik	-0.176	0.067	-2.624	0.009*	-0.140	H ₁ Desteklenmedi
Teknik Korumalar Duyulan Güven	-0.125	0.062	-2.018	0.044*	-0.096	H ₂ Desteklenmedi
İşlem Prosedürleri Algılanan Güvenlik	0.731	0.108	6.765	0.000*	0.502	H ₃ Kabul
İşlem Prosedürleri Duyulan Güven	0.407	0.102	4.006	0.000*	0.270	H ₄ Kabul
Güvenlik Bildirimleri Algılanan Güvenlik	0.300	0.058	5.168	0.000*	0.289	H ₅ Kabul
Güvenlik Bildirimleri Duyulan Güven	0.174	0.054	3.249	0.001*	0.162	H ₆ Kabul
Algılanan Güvenlik Duyulan Güven	0.481	0.057	8.360	0.000*	0.463	H ₇ Kabul
Algılanan Güvenlik Kullanım	0.161	0.066	2.430	0.015*	0.163	H ₈ Kabul
Duyulan Güven Kullanım	0.287	0.065	4.422	0.000*	0.302	H ₉ Kabul

Uyum İndeksleri:

$\chi^2/df: 3.146, RMSEA: 0.066, GFI: 0.852, AGFI: 0.823,$
CFI: 0.902, NFI: 0.863, IFI: 0.902, TLI: 0.890, SRMR: 0.074

*p<0.05

Teknik korumalar ile tüketicilerin e-ödeme yöntemlerinde algıladığı güvenlik arasındaki ilişki incelendiğinde, teknik korumaların tüketicilerin e-ödeme yöntemlerinde algıladığı güvenlik üzerinde istatistiksel olarak anlamlı ve fakat negatif yönde bir ilişki olduğu görülmektedir ($\beta = -0.140$, $p < 0.05$). Bu nedenle öne sürülen H_1 hipotezi desteklenmemektedir. Yine teknik korumalarla ilgili kurulan ikinci hipotezde, teknik korumalar ile tüketicilerin e-ödeme yöntemlerine duyduğu güven arasındaki ilişkiye bakıldığında istatistiksel olarak anlamlı ve fakat negatif yönde bir ilişki olduğu görülmektedir ($\beta = -0.096$, $p < 0.05$). Bu nedenle öne sürülen H_2 hipotezi de desteklenmemektedir. Bu sonuçlar mevcut literatür incelendiğinde Barkhordari vd. (2016), Diep (2020), Hanzaee ve Alinejad (2012), Kim vd. (2000) ve Öney vd. (2017) tarafından yapılan çalışmaların sonuçlarıyla farklılık göstermiştir. Yaptığımız bu çalışmada elde edilen analiz sonuçlarının literatürle uyumsuzluğunun nedenini pandemiyle birlikte tüketicilerin e-ticarete daha fazla yönelmeleri ve e-ödeme yöntemlerinde algıladığı güvenlik üzerindeki tutumlarında belirli değişiklikler yaşatabildiğini ve teknik korumaların daha çok bilgi istemesinden kaynaklı risk içeren unsurlar olarak düşünebilecekleri, bu nedenle tüketicilerin güvenlik aşamalarını tamamlama isteksizliğine yol açabileceği ve bilgi girişi konusunda isteksiz davranabilecekleri şeklinde yorumlamak mümkündür. Öte yandan anketi cevaplayanların genç kitle olmasından dolayı ödeme yöntemlerinin herkes tarafından kullanılıyor olduğu için bir sorun oluşturmayacağı, çoğunlukla ebeveynlerinin hesaplarına ait kartları kullanıyor olmaları veya ödeme araçlarındaki limitlerinin az olduğu varsayımıyla teknik korumaları çok fazla dikkate almayabilecekleri düşünülebilir.

İşlem prosedürlerinin tüketicilerin e-ödeme yöntemlerinde algıladığı güvenlik üzerindeki ilişkisi incelendiğinde, analiz sonuçları istatistiksel olarak anlamlı ve pozitif yönde bir ilişkisi olduğu görülmektedir ($\beta = 0.502$, $p < 0.05$). Buna göre öne sürülen H_3 hipotezi kabul edilmektedir. Yine İşlem prosedürleri ile tüketicilerin e-ödeme yöntemlerine duyduğu güven arasındaki ilişki incelendiğinde, işlem prosedürlerinin tüketicilerin e-ödeme yöntemlerine duyduğu güven üzerinde istatistiksel olarak anlamlı ve pozitif yönde bir etkisi olduğu görülmektedir ($\beta = 0.270$, $p < 0.05$). Buna göre öne sürülen H_4 hipotezi de kabul edilmektedir. Bu sonuçlar mevcut literatürün bir kısmı ile uyum göstermekte (Barkhordari vd., 2016; Diep, 2020; Hanzaee ve Alinejad, 2012), ancak bu çalışmada bulunan bulguyla Kim vd. (2000) ile Öney vd. (2017) tarafından elde edilen bulgular arasında farklılık gözlemlenmiştir. Yaptığımız analizde elde edilen sonuçlarla birlikte işlem prosedürlerinin, tüketicilerin elektronik ödeme yöntemlerini güvenli ve verimli kullanabilmeleri için kritik bir öneme sahip olduğunu yorumlamak mümkündür. Dolayısıyla online alışveriş sırasında ödeme aşaması için giriş yapıldığında bireylere kullanıcı adı ve şifre sorulması, ödeme sürecinin son adımını tamamlamadan önce ödeme bilgilerini değiştirme fırsatı sunması, sitenin ödemeyi tamamlamadan önce ödemeyi doğrulamak için veya ödemenin gerçekleştiğine emin olmak adına sms ve e- posta gibi yöntemlerle onay istemesi ve bu işlemlerin dijital çağa uyumlu bir şekilde geliştirilmesi, tüketicilerin algıladığı güvenlik seviyesini ve duyduğu güven arttırarak e- ticaretin gelişimine katkı sağlayacağı beklenebilir.

Güvenlik bildirimlerinin tüketicilerin e-ödeme yöntemlerinde algıladığı güvenlik üzerindeki ilişkisi incelendiğinde, istatistiksel olarak anlamlı ve pozitif yönde bir ilişki olduğu görülmektedir ($\beta = 0.289$, $p < 0.05$). Buna göre H_5 hipotezi kabul edilmektedir. Yine güvenlik bildirimleri ile tüketicilerin e-ödeme yöntemlerine duyduğu güven ilişkisi incelendiğinde, istatistiksel olarak anlamlı, pozitif yönde bir ilişki olduğu görülmektedir ($\beta = 0.162$, $p < 0.05$). Buna göre öne sürülen H_6 hipotezi de kabul edilmektedir. Bu sonuçlar mevcut literatür incelendiğinde Barkhordari vd. (2016), Diep (2020) ile Kim vd. (2000) tarafından yapılan çalışmaların sonuçlarıyla uyumlu iken, Hanzaee ve Alinejad (2012) ile Öney vd. (2017) tarafından elde edilen bulgu arasında farklılık gözlemlenmiştir. Çalışmanın bulguları doğrultusunda online alışveriş sitelerinde bir ödemenin nasıl gözden geçirileceği, iptal edileceği veya kaydedileceği hakkında ayrıntılı bilgiler vermek, sitede güvenlikle ilgili açıklamaların çok fazla teknik kelime içermeden kullanılması, e-ödeme aşamasında güvenlik bildirimlerine kolay erişilmesi ve sitede güvenlikle ilgili açıklamaların dikkati çekecek şekilde hazırlanarak tüketiciye sunulması gibi oluşturulan güvenlik bildirimleri tüketicilerin elektronik ödeme yöntemlerinde algıladığı güvenliği ve duyulan güvende artışa yol açacağı ve bu bağlamda e-ticaretin gelişmesine ivme kazandırması beklenebilir.

Algılanan güvenlik ile tüketicilerin e-ödeme yöntemlerine duyduğu güven arasındaki ilişkiye bakıldığında, sonuçlar istatistiksel olarak anlamlı ve pozitif yönde bir etkisi olduğu görülmektedir ($\beta=0.463$, $p<0.05$). Buna göre H_7 hipotezi kabul edilmektedir. Yine algılanan güvenliğin tüketicilerin e-ödeme yöntemleri kullanımı üzerindeki ilişkisi incelendiğinde, algılanan güvenliğin tüketicilerin e-ödeme yöntemleri kullanımı üzerinde istatistiksel olarak anlamlı ve pozitif bir ilişkisi olduğu görülmektedir ($\beta=0.163$, $p<0.05$). Buna göre H_8 hipotezi de kabul edilmektedir. Bu sonuçlar mevcut literatür ile uyum göstermektedir (Barkhordari vd., 2016; Diep, 2020; Hanzaee ve Alinejad, 2012; Kim vd., 2000, Öney vd., 2017). Çalışmanın bulguları doğrultusunda tüketicilerin elektronik ödeme yöntemlerinde algıladığı güvenlik ne kadar artarsa buna bağlı olarak tüketicinin ödeme yöntemlerine duyduğu güveni de olumlu yönde etkileyerek, e-ödeme yöntemlerinin kullanımını arttıracığı öngörülebilir. Bu bağlamda özellikle gizliliğin ihlali, bilgisayar korsanlarının saldırılarına karşı korunmasız kalma gibi hassas konularda algılanan güvenlik ne kadar artarsa buna paralel olarak tüketicilerin de e-ödeme yöntemlerine duyduğu güvenin o derece artacağı beklenebilecektir. Aynı zamanda elektronik ödeme yöntemlerine karşı algılanan güvenliğin artması, tüketicilerin kişisel bilgilerinin görüntülenmeyeceği, saklanmayacağı ve değiştirilmeyeceği gibi hususlarda korundukları algısını da güçlendirebilecek, bu bağlamda artan güvenlik algısı tüketicilerin elektronik ödeme yöntemleri kullanımını arttırarak e-ticaretin gelişimini desteklemesi beklenebilecektir.

Duyulan güvenin tüketicilerin e-ödeme yöntemleri kullanımı ile ilişkisi incelendiğinde, duyulan güvenin tüketicilerin e-ödeme yöntemleri kullanımı üzerinde istatistiksel olarak anlamlı ve pozitif yönde bir etkisi olduğu görülmektedir ($\beta=0.302$, $p<0.05$). Buna göre öne sürülen H_9 hipotezi kabul edilmektedir. Bu sonuçlar mevcut literatür ile uyum göstermektedir (Barkhordari vd., 2016; Diep, 2020; Hanzaee ve Alinejad, 2012; Kim vd., 2000; Öney vd., 2017). Yaptığımız çalışmada elde edilen sonuçlarla birlikte anlamlı ve pozitif bir etkisi çıkan duyulan güven unsurunun, aynen algılanan güvenlikte olduğu gibi, tüketiciler için elektronik ödeme yöntemlerindeki işlemler sırasında sunulan bilgilere karşı güvenin sağlanması halinde e-ödeme yöntemlerinin kullanımının ve buna bağlı olarak e-ticaretin de artacağı beklenmektedir.

5. Sonuç

Bu araştırma online alışverişin satın almayla noktalanmasında önemli rolü olan elektronik ödeme yöntemlerine dair genç tüketicilerin duyduğu güveni ve bu ödeme yöntemlerine karşı sahip olduğu güvenlik algısını inceleyip, duyulan güven ve güvenlik algısının bu araçların kullanımıyla olan ilişkisini tespit etmeyi amaçlamaktadır. Dolayısıyla bu çalışmayla elde edilen sonuçlar hem teorik olarak hem de bu alanda hizmet veren firmalara yol gösterici olması bakımından önem taşımaktadır.

Araştırmada genç tüketiciler tarafından geleneksel e-ödeme yöntemlerinden biri olan kredi kartı/banka kartı kullanımının %90 oranında bir ağırlığa sahip olduğu, e-cüzdan, sanal kart, eft, havale ve paypal gibi alternatif e-ödeme yöntemlerinin sınırlı oranda tercih edildiği görülmüştür. Araştırma sonucunda e-ödeme yöntemlerine dair teknik koruma, işlem prosedürleri, güvenlik bildirimleri, güvenlik algısı ve duyulan güven değişkenlerinin tüketicilerin elektronik ödeme yöntemlerini kullanma üzerinde anlamlı bir etkisi olduğu tespit edilmiştir. Sadece teknik koruma değişkeninin algılanan güvenlik ve güven ile ilişkisine dair geliştirilen hipotezler desteklenmemiş, diğer tüm hipotezler tüketicinin e-ödeme yöntemlerine dair güvenlik ve güven algısı ile bunların kullanımı arasında pozitif ilişkinin var olduğu bulgularıyla, çalışmanın örneklemini doğrultusunda desteklenmiştir. Çalışma genç tüketicileri temsil etmesi açısından üniversite öğrencileri üzerinde gerçekleştirilmiştir. Bu açıdan üniversite öğrencilerinin çoğunlukla ebeveynlerinin hesaplarına bağlı kartları kullanmalarından ötürü, kredi kartına dair bilgilerin gizliliğinin ihlalinden doğabilecek sonuçlardan doğrudan sorumlu olmamalarının teknik korumalar ile algılanan güvenlik ve güven arasında beklenen pozitif ilişkiye rastlanmasının nedeni olduğu düşünülmektedir.

Çalışmadaki analiz verileri göz önüne alındığında yapılan araştırma, algılanan güvenlik ve duyulan güvenin yüksek olması e-ödeme yöntemlerinin kullanımını arttırdığını göstermektedir. Mevcut çalışma, genel olarak e-ödeme araçlarını oluşturan firmalar için birkaç önemli çıkarım da sağlamaktadır. Buna göre e-ödeme araçlarını oluşturan firmalar, elektronik ödeme yöntemlerini kullanımına yönelik tüketicilerin algılanan güvenliğini ve duyulan güvenini arttırmanın yollarını aramalı ve kullanıcıların kişisel bilgilerinin

(isim, adres, telefon numarası, kredi kartı numarası vb.) güvende tutulmasını sağlamalıdır. Bu anlamda farklı yöntemlerle örneğin; biyometrik kimlik doğrulama, dijital imzalar, şifreleme teknikleri, SSL ve SET gibi güvenlik katmanları ve teknolojik olarak alınan önlemler gibi nasıl bir önlem almaları gerektiği üzerinde yoğunlaşmalı ve gerekirse bu konuda dijital platformlardan bilgilendirici içerik düzenleyip tüketicilerin kişisel e-posta, telefon gibi iletişim kanallarından bunu aktarmalıdır (Asokan vd., 2000: 15-16; Masihuddin vd., 2017: 9; Serhateri, 2015: 229). Ayrıca sonuçlar, kullanıcıların kendilerini güvende hissetmeleri ve elektronik ödeme yöntemlerine güvenmeleri için kullanıcı dostu ve sorunsuz sistemlere ihtiyaç duyduklarını da göstermiştir.

Yapılan araştırma tüketiciler açısından önemli bulgular ortaya çıkarsa da tüketicilerin elektronik ödeme yöntemleri kullanımını etkileyen tüm faktörleri kapsamamaktadır. Belirli e-ödeme işlevleri gibi faktörler ve sosyal ve bireysel faktörler gelecekteki araştırmalarda dikkate alınabilir. Güvenlik risklerini önlemek için de insan faktörü, yönetim, eğitim farkındalık ve diğer teknoloji dışı faktörlere de özel dikkat gösterilmelidir. Örneğin, kimlik hırsızlığına karşı mücadele etmek için verilen eğitim, tüketicilerin kişisel verilerini fiziksel ve sanal dünyalarda güvende tutma konusundaki farkındalığını arttırmada rol oynayabilir. Gelecekte farklı yaş grupları/kuşaklar üzerinde çalışmanın gerçekleştirilmesi, farklı demografik özelliklere sahip tüketicilerin e-alışveriş sırasındaki yolculuklarını tasarlamada anlamlı çıktılar üretebilecektir.

Kaynaklar

- Abrazhevich, D. (2001), Classification and Characteristics of Electronic Payment Systems, *Lecture Notes in Computer Science*, 81-90.
- Acaroğlu, R. (2014), Revize Edilen Hemşirelerin Mesleki Değerleri Ölçeği Türkçe Formunun Güvenirlik ve Geçerliği, *Florence Nightingale Hemşirelik Dergisi*, 22(1), s.8-16.
- Altunışık, R, Coşkun, R., Bayraktaroğlu, S. ve Yıldırım, E. (2010), *Sosyal Bilimlerde Araştırma Yöntemleri*, Sakarya: Sakarya Kitabevi.
- Anderson, J. C. Ve Gerbing, D. W. (1988), Structural Equation Modeling in Practice: A review and Recommended two-step Approach, *Psychological Bulletin*, 103(3), s.411-423.
- Asokan, N., Janson, P., Steiner, M. ve Waidner, M. (2000), Electronic Payment Systems. Research Report, *IBM Research Division*, s.1-16.
- Barkhordari, M., Nourollah, Z., Mashayekhi, H., Mashayekhi, Y. Ve Ahangar, M. (2016), Factors Influencing Adoption of E-Payment Systems, *Inf Syst E-Bus Manage*. 15(1), s.89-116.
- Bellare, M., Garay, J., Hauser, R., Herzberg, A., Krawczyk, H., Steiner, M. ve Tsudik, G. (2000), Design, Implementation, and Deployment of the iKP Secure Electronic Payment System, *IEEE Journal On Selected Areas In Communications*, 18(4), s.611-627.
- Büyüköztürk, Ş. (2002), Faktör Analizi: Temel Kavramlar ve Ölçek Geliştirmede Kullanımı, *Kuram ve Uygulamada Eğitim Yönetimi Dergisi*, (32), s.470- 483.
- Byrne, B. M. (2001), *Structural Equation Modeling With Mplus*, New York: Rotledge Taylor & Francis Group.
- Chellappa, R. K. ve Pavlou, P. (2002), Perceived Information Security, Financial Liability and Consumer Trust in Electronic Commerce Transactions, *Logistics Information Management*, 15(5-6), s.358- 368.
- Demirağ, B. ve Durmaz Y. (2019), Algılanan Hizmet Kalitesinin Algılanan Değer ve Tutumsal Marka Sadakati Üzerindeki Etkisinin İncelenmesi: 5 Yıldızlı Sayfiye ve Şehir Otelleri Örneği, *Uluslararası Toplum Araştırmaları Dergisi*, 9(11), s.695- 726.
- Diep, L. T. (2020), Retention Using Electronic Payment Systems: An Empirical, *Journal of Physics: Conference Series*, (1793), s.1-9.

- Dubihlela, J. ve Dhurup, M. (2014), Modelling the Effects of Market Orientation Enablers on Business Performance among SMEs in a Developing Country, *Mediterranean Journal of Social Sciences*, 5(16), s. 33-41.
- Esen, M. F. ve Timor, M. (2019), Çok Değişkenli Aykırı Değer Tespiti İçin Klasik ve Dayanımlı Mahalanobis Uzaklık Ölçütleri: Finansal Veri ile Bir Uygulama, *Uluslararası İktisadi ve İdari İncelemeler (UIİİD) Dergisi*, (25), s.267-282.
- Halaweh, M. (2017), Intention to Adopt the Cash on Delivery (COD) Payment Model for E-commerce Transactions: An Empirical Study. International Conference on Computer Information Systems and Industrial Management, *Lecture Notes in Computer Science*, s.628-637.
- Hanzaee, K. H., & Alinejad, S. (2012), An Investigation about Customers Perceptions of Security and Trust in E-Payment Systems Among Iranian Online Consumers, *Journal of Basic and Applied Scientific Research*, 2(2), s.1575-1581.
- Kaya, M. F. (2013), Sürdürülebilir Kalkınmaya Yönelik Tutum Ölçeği Geliştirme Çalışması, *Marmara Coğrafya Dergisi*, (28), s.175- 193.
- Kim, C., Tao, W., Shin, N. ve Kim, K. S. (2010), An Empirical Study of Customers' Perceptions of Security and Trust, *Electronic Commerce Research and Applications*, 9(1), s.84-95.
- Kniberg, H. (2002), What Makes a Micropayment Solution Succeed. *Sweden: Kungliga Tekniska, Institution for Applied Information Technology Höskolan Masters Thesis*.
- Liebana-Cabanillas, F., Munoz-Leiva, F. ve Sanchez-Fernandez, J. (2017), A Global Approach To The Analysis of User Behavior in Mobile Payment Systems in The New Electronic Environment, *Service Business*. 12(1), s.25-64.
- Linck, K., Pousttchi, K. ve Wiedemann, D. (2006), Security Issues in Mobile Payment from the Customer Viewpoint. *Proceedings of the 14th European Conference on Information Systems (ECIS)*, Göteborg: Schweden, s.1-11.
- Mallat, N. (2007), Exploring Consumer Adoption of Mobile Payments – A Qualitative Study, *Journal of Strategic Information Systems*, 16(4), s.413-432.
- Masihuddin, M., Burhan Ul Islam Khan, M. Mueen Ul Islam Mattoo, ve Rashidah F. Olanrewaju. (2017), A Survey on E-Payment Systems: Elements, Adoption, Architecture, Challenges, *Indian Journal of Science and Technology*, 20(10), s.1-18.
- Obaidat, M. ve Boudriga, N. (2007), Introduction to E-Security, *Security of e-Systems and Computer Networks*, s. 3-24.
- Ooi, K.-B. ve Tan, G.-H. (2016), Mobile Technology Acceptance Model: An Investigation Using Mobile Users To Explore Smartphone Credit Card, *Expert Systems With Applications*, 56, s.33-46.
- Öney, E., Öksüzoğlu Güven, G. ve Rizv, W. (2017), The Determinants of Electronic Payment Systems Usage From Consumers' Perspective, *Economic Research-Ekonomiska Istraživanja*, 30(1), s.394-415.
- Schermelleh-Engel, K. Ve Moosbrugger, H. (2003), Evaluating the Fit of Structural Equation Models: Tests of Significance and Descriptive Goodness of Fit Measures, *Methods of Psychological Research Online*, 8(3), s.23-74.
- Serhateri, A. (2015), Elektronik Ticaret Güvenliğinin Tüketicilerin İnternet Üzerinden Alışveriş Yapma Tutumlarına Etkisi: Kocaeli Örneği, *Karedeniz Dergisi*, 27, s.227-249.
- Smith, S. W. (2005), *Trusted Computing Platforms: Design And Applications*, Boston: Springer Science Business Media, Inc.
- Tan, Y.-H. ve Thoen, W. (2000), Toward a Generic Model of Trust for Electronic Commerce, *International Journal of Electronic Commerce*, 5(2), s.61-74.

Tavşancıl, E. (2005), *Tutumların Ölçülmesi ve SPSS İle Veri Analizi*, Ankara: Nobel Yayıncılık.

Tsiakis, T. ve Sthephanides, G. (2005), The Concept of Security and Trust in Electronic Payments, *Computers&Security*, 24(1), s.10-15.

UNCTAD (2021), *Covid-19 and E-Commerce: A Global Review*. New York: United Nations Publications, *Finding From A Survey of Online Consumers in 9 Countries*, https://unctad.org/system/files/official-document/dtlstictinf2020d1_en.pdf, (Erişim Tarihi: 08.05.2021).

Ek 1: Anket Soruları

CİNSİYET	
<input type="checkbox"/> KADIN	<input type="checkbox"/> ERKEK
İNTERNET SİTESİNDEN ALIŞVERİŞ YAPMA SIKLIĞI	
<input type="checkbox"/> HEMEN HEMEN HER GÜN	<input type="checkbox"/> 2 3 AYDA BİR DEFA
<input type="checkbox"/> HAFTADA BİR KERE	<input type="checkbox"/> YILDA BİR İKİ DEFA
<input type="checkbox"/> AYDA BİR KERE	<input type="checkbox"/> HİÇ
İNTERNET ALIŞVERİŞLERİNDE EN ÇOK KULLANILAN ÖDEME YÖNTEMİ	
<input type="checkbox"/> KREDİ KARTI / BANKA KARTI	<input type="checkbox"/> E-CÜZDAN
<input type="checkbox"/> EFT VE HAVALE	<input type="checkbox"/> SANAL PARA
<input type="checkbox"/> SANAL KART	<input type="checkbox"/> PAYPAL
<input type="checkbox"/> NAKİT	

	SORULAR	Kesinlikle Katılmıyorum	Katılmıyorum	Kararsızım	Katılıyorum	Kesinlikle Katılıyorum
İŞLEM PROSÖDÜRLERİ	1. Elektronik ödeme sistemlerine giriş yaptığınızda her zaman kullanıcı adı ve şifre sorulur.					
	2. Kimlik doğrulaması için elektronik ödeme sistemleri tarafından bir takım önlemler alınmaktadır.					
	3.Site, ödeme sürecinin son adımını tamamlamadan önce ödeme bilgilerini değiştirme fırsatı sunar.					
	4.Site, ödemenin tamamlanmasından önce ödemeyi doğrulamak için bir adım sunar.					
	5.Site, ödeme bilgilerinin (maliyet, alacaklı ...) ve nihai ödeme tutarının bir özetini görüntüler.					
	6.Ödemenin gerçekleştirildiğinden emin olmak için size sms, e-posta gibi yöntemlerle onay mesajı gönderilir.					
TEKNİK KORUMA	7. Kişisel bilgileriniz (hesap bilgisi, iletişim bilgisi gibi) elektronik ödeme sistemi kullanılmasından dolayı daha önce hiç çalınmadı.					
	8. Kişisel bilgileriniz başka bir amaçla elektronik ödeme sistemlerinin servis sağlayıcıları tarafından diğer üçüncü taraflara açıklanmamıştır.					
	9. Elektronik ödeme sistemlerinde görüntülenen ödeme tutarı veya işlem verileri her zaman doğrudur.					
	10. İnternet üzerinden aktarılan elektronik ödeme sistemlerindeki işlem verilerinin güvenli bir şekilde korunduğunu düşünüyorsunuz.					
	11. Elektronik ödeme hizmetleri günün herhangi bir saatinde her zaman kullanılabilir.					

	12. Elektronik ödeme işlemi sırasında geçici veya sürekli hatayla sıklıkla karşılaşılmaz.						
GÜVENLİK BİLDİRİMLERİ	13. Site, bir ödemenin nasıl gözden geçirileceği, iptal edileceği veya kaydedileceği hakkında ayrıntılı açıklamalar sunmaktadır.						
	14. Site, güvenlik politikası, acil durumdaki iletişim bilgileri, teknik açıklamalar ve elektronik ödeme sistemlerinin işlevleri hakkında güvenlik bildirimleri sağlar.						
	15. Sitede güvenlikle ilgili açıklamaları bulmak için özel veya olağanüstü çaba sarf etmenize gerek yoktur.						
	16. Güvenlik sorunlarıyla ilgili endişelerinizi <i>Sık Sorulan Sorular</i> veya <i>Yardım</i> bölümünden kolayca bulabilirsiniz.						
	17. Güvenlikle ilgili açıklamalar, kolay anlaşılır bir şekilde hazırlanır ve büyük ölçüde teknik kelimeleri içermez.						
	18. Sitede güvenlikle ilgili açıklamalar dikkati çekecek şekilde hazırlanmıştır.						
	ALGILANAN GÜVENLİK	19. Elektronik ödeme sistemlerini güvenli buluyorum.					
20. Elektronik ödeme işlemlerine ve kullanıcıya ait bilgilerin güvence altında olduğu düşünüyorum.							
21. Elektronik ödeme sistemlerinde kullanıcıdan istenen bilgiler, ödeme işleminin güvenli şekilde yapılmasına yardımcı olur.							
22. Elektronik ödeme sistemlerine korsanların (Hacker) saldırmasından korkmuyorum.							
DUYULAN GÜVEN	23. Elektronik ödeme sistemlerinde yer alan her bir katılımcıya (satıcı ve alıcı gibi) güveniyorum.						
	24. Elektronik ödeme sistemlerindeki güvenlik mekanizmalarına güveniyorum.						
	25. Elektronik ödeme sistemlerinin hizmetlerine güveniyorum.						
	26. Elektronik ödeme sistemlerindeki işlemler sırasında sunulan bilgilere güveniyorum.						
KULLANIM	27. Elektronik ödemeyi diğer ödeme yöntemlerinden daha sık kullanıyorum.						
	28. Elektronik ödeme sistemlerini kullanıyorum ve gelecekte de kullanmaya devam edeceğim.						
	29. Elektronik ödeme sistemlerinin kullanımının artacağına inanıyorum.						