

**T.C.
MANİSA CELAL BAYAR ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ**

**YÜKSEK LİSANS TEZİ
EKONOMİ VE FİNANS ANABİLİM DALI
EKONOMİ VE FİNANS PROGRAMI**



**ELEKTRONİK ÖDEME YÖNTEMLERİNE YÖNELİK
TÜKETİCİNİN GÜVENLİK VE GÜVEN ALGISININ
İNCELENMESİ**

Helin ASLAN

**Danışman
Dr. Öğr. Üyesi Asiye Ayben ÇELİK**

MANİSA-2021

**T.C.
MANİSA CELAL BAYAR ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ**

**YÜKSEK LİSANS TEZİ
EKONOMİ VE FİNANS ANABİLİM DALI
EKONOMİ VE FİNANS PROGRAMI**

**ELEKTRONİK ÖDEME YÖNTEMLERİNE YÖNELİK
TÜKETİCİNİN GÜVENLİK VE GÜVEN ALGISININ
İNCELENMESİ**

Helin ASLAN

**Danışman
Dr. Öğr. Üyesi Asiye Ayben ÇELİK**

MANİSA-2021

YEMİN METNİ

Yüksek lisans tezi olarak sunduğum “Elektronik Ödeme Yöntemlerine Yönelik Tüketicinin Güvenlik ve Güven Algısının İncelenmesi” adlı çalışmanın, tarafımdan bilimsel ahlak ve geleneklere aykırı düşecek bir yardıma başvurmaksızın yazıldığını ve yararlandığım eserlerin bibliyografyada gösterilen eserlerden oluştuğunu, bunlara atıf yapılarak yararlanmış olduğumu belirtir ve bunu onurumla doğrularım.

28/05/2021

Helin Aslan

İmza

ÖZET

ELEKTRONİK ÖDEME YÖNTEMLERİNE YÖNELİK TÜKETİCİNİN GÜVENLİK VE GÜVEN ALGISININ İNCELENMESİ

Günümüz iletişim teknolojilerindeki gelişmeler, çevresel etkenler, akıllı telefon sahipliğinin artması, internete erişim olanaklarının gelişmesi ve pandemi gibi olağanüstü durumlar, tüketicinin geleneksel alışveriş yöntemlerinden çevrimiçi alışverişe yönelmesine neden olmaktadır. Bu doğrultuda tüketicilerin elektronik alışverişlerinde ödeme konusu kaygı yaratan bir sorun olarak gündeme gelmektedir.

Bu çalışma, tüketicilerin elektronik ortamda yaptığı alışverişlerde kendilerine sunulan ödeme alternatiflerine yönelik güvenlik ve güven algılarını tespit etmek amacıyla yapılmıştır. Bu bağlamda oluşturulan modelde tüketicilerin elektronik ödeme yöntemlerine yönelik güvenlik ve güven algısı ile çeşitli parametreler çerçevesinde ödeme araçlarının kullanımı arasındaki ilişki değerlendirilmiştir.

Çalışmada veriler, Manisa Celal Bayar Üniversitesi'nde lisans eğitimi görmekte olan 503 öğrenciden anket yoluyla toplanmıştır. Verilerin analizinde SPSS ve AMOS programları kullanılmıştır. Ölçeklerin güvenilirliğini test etmek amacıyla “Güvenilirlik Analizi”, “Madde Toplam Puan Korelasyonu”, yapı geçerliliği test etmek için “Açıklayıcı Faktör Analizi (AFA)”, ve “Doğrulamalı Faktör Analizi (DFA)” yapılmıştır. Model kapsamında öne sürülen hipotezler test edilirken yapısal eşitlik modelinden (YEM) faydalanılmıştır.

Çalışma sonucunda da yapısal eşitlik modeli ile elde edilen genel uyum değerleri incelendiğinde modelin kabul edilebilir düzeyde uyum gösterdiği görülmüştür. Aynı şekilde yol analizi sonuçları da araştırmada yer alan 9 hipotezin desteklendiğini ortaya koymuştur. Bu doğrultuda teknik koruma, işlem prosedürleri, güvenlik bildirimleri, güvenlik algısı ve duyulan güven değişkenlerinin tüketicilerin elektronik ödeme yöntemlerini kullanma üzerinde anlamlı bir etkisi olduğu tespit edilmiştir.

Anahtar kelimeler: E-ticaret, elektronik ödeme yöntemleri, güven, güvenlik

ABSTRACT

INVESTIGATION OF THE CONSUMER'S PERCEPTION OF SECURITY AND TRUST FOR ELECTRONIC PAYMENT METHODS

The developments in today's communication technologies, environmental factors, the increase of smartphone ownership, the development of internet access facilities and the pandemic caused the consumer to turn to online shopping from traditional shopping methods. In this subject the issue of payment in the electronic purchases of consumers is a problem that creates anxiety.

This study was carried out to determine the perceptions of security and trust regarding the payment alternatives offered to consumers in their electronic shopping. In the model created in this context, the relationship between consumers' perception of security, trust in electronic payment methods and the use of payment instruments within the framework of various parameters was evaluated.

In the study, data were collected through questionnaires from 503 undergraduate students at Manisa Celal Bayar University. SPSS and AMOS programs were used in the analysis of the data. In order to test the reliability of the scales, “Reliability Analysis”, “Item Total Score Correlation”, “Explanatory Factor Analysis (EFA)” and “Confirmatory Factor Analysis (CFA)” were performed to test construct validity. While testing the hypotheses put forward within the scope of the model, the structural equation model (SEM) was used.

As a result of the study, when the general fit values obtained with the structural equation model were examined, it was seen that the model showed an acceptable level of fit. Likewise, the results of the path analysis revealed that 9 hypotheses in the research were supported. In this respect, it has been determined that the variables of technical protection, transaction procedures, security notifications, security perception and trust have a significant effect on consumers' use of electronic payment methods.

Keywords: E-commerce, electronic payment methods, trust, security

TEŞEKKÜR

Çalışmamın her aşamasında bana destek olan, bilgi ve tecrübesi ile lisans ve lisansüstü öğrenim hayatımın tüm zorlu aşamalarında bana yol gösteren, akademik olarak kendimi geliştirmeme büyük katkısı olan ve kendisiyle bu zorlu süreçte beraber çalışmış olmaktan onur duyduğum danışman hocam Sayın Dr. Öğr. Üyesi Asiye Ayben ÇELİK'e, bilgi ve deneyimi ile tez sürecimin zorlu aşamalarında her yönden yardımcı olan, desteğini hiç eksik etmeyen hocam Sayın Araş. Gör. Gencay TEPE'ye, çalışmalarım sırasında manevi desteklerini her zaman hissettiğim arkadaşlarıma, öğrenim hayatım boyunca beni maddi manevi her yönden destekleyen ve yanımda olan, en zorlu anlarımda bile beni hep motive eden yol arkadaşım, kıymetli eşim Murat'a ve beni bugünlere getiren canım aileme yürekten teşekkür ederim.

Helin ASLAN
Manisa, 2021

İÇİNDEKİLER

TEZ SAVUNMA SINAVI TUTANAĞI.....	iii
TEZ VERİ GİRİŞ VE TEZ YAYINLAMA İZİN FORMU.....	iv
YEMİN METNİ.....	v
ÖZET.....	vi
ABSTRACT.....	vii
TEŞEKKÜR.....	viii
İÇİNDEKİLER	ix
KISALTMALAR	xii
TABLolar LİSTESİ.....	xiv
ŞEKİLLER LİSTESİ	xv
EKLER LİSTESİ	xvi
GİRİŞ	1

BİRİNCİ BÖLÜM

ELEKTRONİK TİCARET VE ELEKTRONİK ÖDEME YÖNTEMLERİ

1.1. ELEKTRONİK TİCARET KAVRAMI VE GÖSTERDİĞİ GELİŞİM SEYRİ ..	6
1.2. ELEKTRONİK TİCARETTEN MOBİL TİCARETE GEÇİŞ	17
1.3. E-TİCARETTE KULLANILAN ELEKTRONİK ÖDEME YÖNTEMLERİ....	20
1.4. ELEKTRONİK ÖDEME ARAÇLARI.....	24
1.4.1. Kredi Kartı.....	24
1.4.2. Temassız Ödeme	27
1.4.3. Doğrudan Borçlandırma (Mail Order)	28
1.4.4. Banka Kartı.....	28
1.4.5. Elektronik Fon Transferi	29
1.4.6. Elektronik Çek.....	30

1.4.7. Ticari Banka Paraları	31
1.4.8. Elektronik Cüzdan	31
1.4.9. Sanal Kart	32
1.4.10. Akıllı Kart.....	32
1.4.11. Mobil Ödeme.....	33
1.4.12. Pay Pal	35
1.4.13. BKM Ekspres.....	36
1.4.14. Türk Ödeme Yöntemi (TROY)	37
1.4.15. Elektronik Para (Kripto Para).....	37
1.5. ELEKTRONİK ÖDEME YÖNTEMLERİNİN SINIRLAMALARI	41
1.6. ELEKTRONİK ÖDEME YÖNTEMLERİNİN AVANTAJLARI	42
1.7. ELEKTRONİK ÖDEME YÖNTEMLERİNİN SORUNLARI	42
1.8. ELEKTRONİK ÖDEME YÖNTEMLERİNDE YENİ TRENDLER.....	43

İKİNCİ BÖLÜM

E-ÖDEME YÖNTEMLERİNE YÖNELİK GÜVEN VE GÜVENİLİRLİĞE DAİR KAVRAMSAL ÇERÇEVE, GELİŞTİRİLEN HİPOTEZLER VE MODEL ÖNERİSİ

2.1. E-ÖDEME YÖNTEMLERİNDE KULLANILAN GÜVENLİK SİSTEMLERİ	45
2.2. ELEKTRONİK ÖDEME YÖNTEMLERİNE DUYULAN GÜVEN	53
2.3. E-ÖDEME YÖNTEMLERİNE YÖNELİK GÜVEN VE GÜVENİLİRLİĞE DAİR LİTERATÜR TARAMASI VE BİBLİYOMETRİK ANALİZ	60
2.3.1. Bibliyometrik Analiz	66
2.4. ARAŞTIRMA HİPOTEZLERİ VE MODEL ÖNERİSİ	71
2.4.1. Araştırma Modeli	71
2.4.2. Araştırma Hipotezleri	72
2.4.2.1. Elektronik Ödeme Yöntemlerinde Teknik Korumalar	72
2.4.2.2. Elektronik Ödeme Yöntemlerinde İşlem Prosedürleri.....	73

2.4.2.3. Elektronik Ödeme Yöntemlerinde Güvenlik Bildirimleri	75
2.4.2.4. Elektronik Ödeme Yöntemlerinde Algılanan Güvenlik	76
2.4.2.5. Elektronik Ödeme Yöntemlerine Duyulan Güven	77

ÜÇÜNCÜ BÖLÜM
ELEKTRONİK ÖDEME YÖNTEMLERİNE YÖNELİK TÜKETİCİLERİN
GUVENLİK VE GÜVEN ALGISININ İNCELENMESİNE DAİR ALAN
ARAŞTIRMASI

3.1. ARAŞTIRMANIN AMACI VE KAPSAMI	79
3.2. ARAŞTIRMANIN YÖNTEMİ.....	80
3.3. ARAŞTIRMANIN KISITLARI	81
3.4. VERİ ANALİZİ VE BULGULAR	82
3.4.1. Katılımcılara İlişkin Demografik Veri ve Özellikleri	83
3.4.2. Verilerin Analizi	85
3.4.3. Ölçüm Modeli, Geçerlilik ve Güvenilirlik	88
3.5. BULGULAR VE TARTIŞMA	90
SONUÇ VE ÖNERİLER	96
KAYNAKÇA	100
EKLER	

KISALTMALAR

ATM Otomatik Para Çekme Makinesi

B2B Firmadan Firmaya Ticaret

B2C Firmadan Tüketiciciye Ticaret

B2E Firmadan Çalışanına Ticaret

B2G Firmadan Devlete Ticaret

BKM Bankalararası Kart Merkezi

C2B Tüketiciden Firmaya Ticaret

C2C Tüketiciden Tüketiciciye Ticaret

C2G Tüketiciden Devlete Ticaret

EDI Elektronik Veri Değişimi

EFT Elektronik Fon Transferi

ETTK Elektronik Ticaret Koordinasyon Kurulu

FTP Dosya Aktarım Protokolü

G2B Devletten Firmaya Ticaret

G2C Devletten Tüketiciciye Ticaret

G2G Devletten Devlete Ticaret

GSM Mobil İletişim İçin Küresel Sistem

HTTPS Köprü Metin Aktarma Protokolü

OECD Ekonomik İşbirliği ve Kalkınma Örgütü

POS Satış Noktası

SET Güvenli Elektronik İşlem

SMS Kısa Mesaj Servisi

SPSS Sosyal Bilimler İçin İstatistik Programı

SSL Güvenli Giriş Katmanı

TCMB Türkiye Cumhuriyeti Merkez Bankası

TTP Güvenilir Üçüncü Taraf

TÜİK Türkiye İstatistik Kurumu

UN- CEFAC Birleşmiş Milletler İdari Ticari ve Ulaşım İlgili Uygulama ve Usulleri Kolaylaştırma Merkezi

UNCTAD Birleşmiş Milletler Ticaret ve Kalkınma Konferansı

WTO Dünya Ticaret Örgütü

WWW Dünya Çapında Ağ



TABLÖLAR LİSTESİ

Tablo 1: Geleneksel Ticaret-Elektronik Ticaret Karşılaştırılması

Tablo 2: Elektronik Ticaretin Araçları

Tablo 3: En Üretken Yazarlar

Tablo 4: Elektronik Ödeme Yöntemlerinde Güvenlik ve Güven Algısı Üzerine En Çok Araştırma Yapılan Disiplinler

Tablo 5: En Üretken Ülkeler

Tablo 6: En Çok Atıf Alan Yayınların Yıllara Göre Atıf Dağılımı (Scopus)

Tablo 7: En Çok Atıf Alan Yayınların Yıllara Göre Atıf Dağılımı (Wos)

Tablo 8: Demografik Özellikler

Tablo 9: Araştırmaya Katılan Katılımcıların Özelliklerine Göre Dağılımı

Tablo 10: Araştırmaya Kullanılan Ölçeklerin Normallik Analizi Sonuçları

Tablo 11: Araştırmada Kullanılan Ölçeğin Açıklayıcı Faktör Analizi

Tablo 12: Ölçüm Modeline İlişkin Sonuçlar

Tablo 13: Yapısal Modelin Uyum İyiliği Değerleri

Tablo 14: Yol Analiz Sonuçları

ŞEKİLLER VE GRAFİKLER LİSTESİ

Şekil 1: İnternetin ve E-Ticaretin Evriminde Kilometre Taşları

Şekil 2: E-Ticarette Sistemin İşleyişi

Şekil 3: İnternet Üzerinden E-Ticaretin Çalışma Yapısı

Şekil 4: Bir Mobil Ödeme Sisteminin Tipik Varlıkları ve Mobil Ödeme İşlemi Sırasında Etkileşimleri

Şekil 5: COVID-19 Sırasında Çevrimiçi Satın Alımlar için Ödeme Yöntemlerinin Kullanımı

Şekil 6: Araştırma Modeli ve Hipotezler

Şekil 7: Ölçeğinin Birinci Düzey Çok Faktörlü Doğrulayıcı Faktör Analizine İlişkin Model

Şekil 8: Yapısal Eşitlik Modelinin Sonuçları

Grafik 1: COVID-19'un Ortaya Çıkmasıyla Birlikte Eskisinden Daha Sık Çevrimiçi Alışveriş Yapma Sıklığı Anket Sonuçları

Grafik 2: COVID-19 Sonrası Farklı Satın Alma Kararları İçin Tercihler

Grafik 3: 2020 Yılı E-Ticaret Hacmi

Grafik 4: Ödeme Yöntemleri İtibariyle 2020 E-Ticaret Hacmi

Grafik 5: Scopus ve WoS Veri Tabanlarında 1995-2020 Yılları Arasındaki Yayın Sayıları

EKLER LİSTESİ

EK1: Anket Formu

EK2: Ölçek Kullanım İzni

EK3: Etik Kurul Onayı



GİRİŞ

Ticaret, insanlık tarihi kadar eski bir kavramdır. Binlerce yıl önce insanların gıda, barınma ve silah gibi temel ihtiyaçlarını gidermek için birbirleriyle yaptıkları takas usulü alışverişle birlikte ticaret kavramı ortaya çıkmıştır. Takas usulü alışverişin verimsizliği, ticarete sorunlara neden olmuştur. Milattan önce 5. yüzyılda Lidyalılar tarafından icat edilen para ile eski usuller terk edilmeye başlanmıştır (Yükçü ve Atağan, 2014: 28). Para kelimesi Latince pecus veya sığır kelimesinden gelmektedir. İlk zamanlar tahıl, kil, midye, kahve çekirdeği gibi dönemin ve coğrafyanın değerli nesneleri para olarak kullanılmıştır (Angel ve McCabe, 2014: 604). Kahve çekirdeklerinin bozulduğunda değerinin azalması gibi zorluklar, medeniyetleri bu nesneler yerine daha dayanıklı ve pek çok coğrafyada kabul edilen ortak bir nesneye yöneltmiştir. Toplamlar artık altın ve gümüş gibi madeni paralar kullanarak ticaretlerini gerçekleştirmeye başlamışlardır. Daha sonra değerli madenlerden yapılan paralar 18. ve 19. yy'da taşınması kolay kâğıt paralara yerini bırakmıştır. 20.yy'da kredi kartlarıyla alışveriş imkânı yaygınlaşmış, teknolojinin ve internetin gelişimiyle beraber para transferleri internet üzerinden yapılmaya başlanmıştır. Bu gelişmelerin sonucunda nakit para kullanımı giderek azalmış ve elektronik ödeme yöntemleri kullanılmaya başlanarak e-ticaret kavramı ortaya çıkmıştır (Pirinççi, 2018: 48-52; Sönmez, 2014: 2).

Tarihsel süreç içinde paranın tanımı yıllara, coğrafyaya ve medeniyetlere göre değişiklik göstermektedir. Para genel bir ifadeyle ürünün, hizmetin, emeğin ve borçların ödenmesinde kullanılan, başka bir araca dönüştürülebilen genel kabul gören her şey olarak tanımlanabilmektedir (Günel, 2010: 282). Bir araca para diyebilmemiz için beş temel özelliğe sahip olması gerekmektedir (Öztürk ve Koç, 2006: 228-229):

- Taşınabilirlik: Mübadele aracı olan paranın fiziksel olarak kolay taşınabilir olması gerekir. Ayrıca farklı ödeme noktalarına transfer edilebilmesini mümkün kılan kullanım kolaylığı sağlamalıdır.
- Dayanıklılık: Para olarak kullanılan malın fiziksel olarak dayanıklı olması gerekir. Çünkü dayanıksız maddelerden yapılmış bir ödeme aracı, alışveriş işlemlerinde kullanılması olası değildir.
- Bölünebilirlik: Paranın her türlü satın alma işlemini yürütecek şekilde bölünebilmesi gerekir.

- Standardizasyon: Paranın nitelik olarak tek biçimde, homojen olması gerekir.
- Taklit edilememe: Para olarak kullanılan ödeme araçlarının herkes tarafından tanınabilir olması ve sahte ödeme araçlarına izin vermemesi gerekir.

Bir aracın para özelliği taşıyabilmesi için belli fonksiyonları yerine getirmesi gerekmektedir (Dinler, 2015: 430-431; Alptekin, 2016: 458-460):

- Mübadele fonksiyonu: Paranın icadından önceki çağlarda ticaret trampa denilen değiş-tokuş(takas) sistemi ile gerçekleşmekteydi. Zamanla mal ile malın değiştirilmesinde yaşanan güçlüklerin ortadan kaldırılması için herkesçe kabul edilen bir mübadele aracı olan para ile malın değiştirilmesi yoluna gidilmiştir. İnsanlar ilk önce altın, gümüş, buğday, tuz, hayvan gibi mal para kullanmaya başlamışlardı. Daha sonra siyasi iktidarların ticareti düzenlemesiyle beraber resmi paralar, mal paranın yerini almıştır. Bu ilerlemeyi temsili kâğıt para ve itibari kâğıt para takip etmiştir. Teknolojinin ekonomide kullanılması ve ekonomide yaşanan hacimsel gelişmeler paranın fiziki bir biçimde değil de elektronik bir biçimde kullanılmasına neden olmuştur. Günümüzde elektronik paralar mübadele aracı olarak ticarete büyük bir payı oluşturmaktadır.
- Hesap birimi olma fonksiyonu: Ticarete trampa sisteminin kullanıldığı dönemlerde değiş-tokuş söz konusu iken bu değiş-tokuş piyasada alım satıma konu olan tüm mal ve hizmetler arasında geçerli olmaktaydı. Bu yüzden bir mal veya hizmetin diğer mallar ve hizmetler açısından bir karşılığı bulunduğundan ekonomide çok karmaşık bir fiyat sistemi ortaya çıkmaktaydı. Herkesçe kabul edilen mübadele aracı olan paranın icadıyla trampa sistemi terk edilerek, alım satıma konu olan mal ve hizmetlerin fiyatları tek birime indirgenmiştir. Paranın ortak değer ölçüsü olma fonksiyonu doğru bir şekilde sağlayabilmesi için zaman içinde kendi değerinin değişmemesi gerekmektedir. Eğer paranın kendi değeri sık sık değişirse para hesap birimi olma fonksiyonunu yerine getirmekte zorlanır.
- Tasarruf yapabilme fonksiyonu: Mal veya hizmetlerin tek bir para birimi cinsinden ticarete konu olması ekonomik birimlerin elde ettikleri paranın bir kısmını harcayıp bir kısmını tasarruf etmeleri sonucunu doğurmuştur. Böylece insanlar parayı değer biriktirme aracı olarak kullanmışlardır. Tasarruf aracı olma fonksiyonunda paranın her an kullanılabilme özelliği (likidite) parayı

diğer mallara göre daha avantajlı kılmaktadır. Ancak paranın tasarruf aracı olma fonksiyonunu sağlayabilmesi için değerinin istikrarlı olması gerekmektedir. Eğer paranın değeri düşüyorsa kimse elinde para tutmak istemez. Paradan kaçış başlar. Böyle durumlarda kişiler tasarruf etme yerine borçlanmayı tercih etmektedirler.

Gelişen teknoloji, artan bilgi birikimi, eğitim seviyesinin yükselmesi, refah düzeyinin artması gibi nedenlerle insanların beklentileri farklılaşmaktadır. Bu durum para üzerinde de etkisini göstermeye başlamıştır. Geçmişten günümüze evrim geçiren para, teknolojik gelişmeyle uyumlu olarak elektronik para olarak karşımıza çıkmaktadır. 20. yüzyılın ikinci yarısı teknoloji bakımından önemli gelişmelerin yaşandığı dönem olarak bilinir. Bu dönemde para, fiziksel boyuttan sanal boyuta geçiş sürecini yaşamıştır. 1975 yılında Amerika Birleşik Devletleri'nde ilk otomatik para çekme makinesi kullanılmaya başlanmıştır. 1980'lerin sonunda Avrupa'da benzin istasyonlarını hırsızlığa karşı korumak amacıyla akıllı kartlara para yüklenmesi ve bu paralarla yakıt alınabilir olması elektronik ödemenin ilk örnekleri arasında gösterilmektedir. Dünyada ilk kez Amerikan bankaları paranın elektronik yöntemler ile transferini (EFT- elektronik para transferi) gerçekleştirmiştir. Kredi kartlarının Amerika'da kullanılmaya başlamasıyla kredi kartları, giderek artan bir hızla tüm dünyada yaygınlaşmıştır. 1990'lı yıllarda da özellikle bankalar tarafından yeni ödeme yöntemlerine yönelik ürünler geliştirilmiştir (Yüksel ve Bozkurt, 2015: 176).

Ayrıca geçtiğimiz on yılda tüketicilerin, bir hizmet sunumunda geleneksel bir hizmet çalışanı rolünü üstlenmelerine olanak tanıyan self servis uygulamasında hızlı bir büyüme gerçekleşmiştir. Self-servis teknolojileri, müşterilerin, herhangi bir hizmet personeliyle etkileşime girmeden hizmetlerini almalarını sağlayan araçlardır. Bilgi teknolojilerindeki gelişmelerden de yararlanılarak self servis teknolojisinde verimlilik artmıştır. Bilgisayar kullanılarak havayolu yolcuları uçuşlarına check-in yapabilir; internette tüketiciler, bir satış temsilcisiyle hiç konuşmadan ürün satın alabilir ve bir cep telefonu kullanarak müşteriler banka bakiyelerini kontrol edebilir ve para transfer edebilirler. Bunların hepsi self servise birer örnektir. Yeni ödeme yöntemleri self servis teknolojisinin temelini kullanarak geliştirilmiş ve böylelikle verimlilik arttırılmış, maliyetler ciddi oranda düşürülmüş ve işlem kolaylığı sağlanmıştır. (Castro vd., 2010: 4-5).

Görülen o dur ki bilgi ve iletişim teknolojisinin gelişimi, ticari işlemler nakit temelli işlemlerden elektronik tabanlı işlemlere yöneltmiştir. E-ticaretin ortaya

çıkışıyla beraber geleneksel ödeme yöntemleri, ihtiyaçları karşılayamaz hale gelmiş ve bunun sonucunda finansal ihtiyaçların giderilmesi için elektronik ödeme yöntemleri geliştirilmiştir. Elektronik ödemeler, nakit içermeyen elektronik araçları kullanan bir ödeme mekanizması olarak anlaşılabılır. Elektronik ödeme yöntemleri, ticaretin önemli bir yönünü oluşturmaktadır. Verimli ve güvenilir bir e-ödeme yöntemi, daha hızlı ödeme, daha iyi takip, şeffaf işlemler, daha az zaman kullanımı, maliyet tasarrufu ve satıcılar ile alıcılar arasında artan güven sağlamaktadır (Wibowo vd., 2018: 2).

Elektronik ödeme yöntemleri; kredi kartları, banka kartları, elektronik para ve çek sistemleri, akıllı kartlar, dijital cüzdanlar temassız ödeme yöntemleri ve mobil ödemeler gibi birçok yenilik getirmiştir. Özellikle günümüzde akıllı telefonların geliştirilmesi ve yaygınlaşmasıyla beraber mobil ödeme yöntemlerinin kullanımı artış göstermektedir. Bununla birlikte ticaretin elektronik ticaret yoluyla hızlı genişlemesi ve teknolojik ilerleme, sürekli gelişen ödeme hizmetlerine neden olan ve ödeme sistemlerinin hızla gelişmesine yol açan faktörler arasında yer almaktadır. Çevrimiçi işletmelerin ise sürekli büyümesi, çevrimiçi ödeme sisteminin de yükselmesine neden olmuştur (Suwunniponth, 2016: 3915).

Online ödeme sistemi aynı zamanda işlem sırasında oluşabilecek birçok finansal riski de içinde barındırmaktadır. Artarak devam eden yeni ödeme yöntemleri, internet üzerinde gerçekleştirilen alışverişin yaygınlaşmasıyla kişisel bilgilerinin çalınma riski bakımından tüketicilerin gözünde güven ve güvenlik algısı konusunda bir takım soru işaretlerini barındırmaktadır. Çevrimiçi ödemelerin olumsuz etkileri birçok nedenden dolayı ortaya çıkabilmektedir. İnternetin doğası gereği, ödemelerin gerçekliği ve güvenliği, e-ticaret için tasarlanmamış teknolojiler tarafından garanti edilemez. Sadece güvenli ödeme sistemi sağlamakla kalmayan, aynı zamanda çevrimiçi müşteriler ve satıcı kimlik doğrulaması, müşteriler tarafından hem satıcılara hem de bankalara yetkilendirilmiş işlemlerin kanıtı, müşteri gizliliği ve işlemsel veri güvenliği gibi özelliklere sahip olması gereken bir elektronik ödeme (e-ödeme) sistemine ihtiyaç vardır (Zengin ve Güngördü, 2013: 131).

Bu araştırma, internetin gelişmesiyle birlikte oluşan elektronik ödeme araçlarına dair tüketicinin duyduğu güven ve güvenlik algısını incelemek amacıyla yapılmıştır. Araştırma üç bölümden oluşmaktadır. Birinci bölümde e-ticaretin gelişim seyri, sistemin işleyişi ve e-ticaretin içinde doğan mobil ticaret (m-ticaret) kavramları üzerinde durulmuş, elektronik ödeme yöntemleri detaylandırılarak avantajları, sorunları, sınırlamaları ve e-ödeme yöntemlerinde ortaya çıkan yeni trendlerden

bahsedilmiştir. İkinci bölümde elektronik ödeme yöntemlerinin güvenlik sistemleri ve elektronik ödeme yöntemlerine duyulan güven konuları detaylandırılarak elektronik ödeme yöntemlerine dair literatür taraması ve bibliyometrik analiz sunulmuştur. Analiz sonrası araştırma hipotezleri oluşturularak model önerisine yer verilmiştir. Üçüncü ve son bölümde ise araştırmanın amacı, kapsamı, yöntem ve kısıtları belirtilerek elektronik ödeme yöntemlerine yönelik tüketicinin güvenlik ve güven algısının incelenmesi amacıyla Manisa Celal Bayar Üniversite’nde lisans eğitimini sürdürmekte olan öğrencilerden anket yoluyla veri toplanmış, yapılan anketin sonuçlarından çıkan veriler, yapısal eşitlik modellemesine göre analiz edilmiştir. Bu verilere bağlı 9 adet hipotez test edilerek analizin yorumlanması ve elde edilen bulgulara yer verilmiştir. Sonuç bölümünde ise çalışma boyunca elde edilen verilerin kapsamlı bir şekilde değerlendirilmesi yapılarak önermeler sunulmuştur.

BİRİNCİ BÖLÜM

ELEKTRONİK TİCARET VE ELEKTRONİK ÖDEME YÖNTEMLERİ

Bu bölümde internetin ortaya çıkmasıyla birlikte oluşan e-ticaret ve mobil ticaret (m-ticaret) kavramları, elektronik ödeme yöntemleri, elektronik ödemenin sınırlamaları, elektronik ödeme yöntemlerinin avantajları ile dezavantajları ve e-ödemeye yöntemlerindeki yeni trendler anlatılmaktadır.

1.1. ELEKTRONİK TİCARET KAVRAMI VE GÖSTERDİĞİ GELİŞİM SEYRİ

İnsanlık tarihinin yaşadığı en önemli değişimlerden biri olan Sanayi Devrimi, yeni bir üretim tarzı yaratmanın yanında sosyal değişimleri de beraberinde getirerek toplumun yaşam biçimini belirlemiştir. Sanayi toplumu ile insanlığın geçirdiği değişim, dönüşüm ve gelişim süreci günümüzde de bilgi toplumuna dönüşüm şeklinde yaşanmaktadır. Geçtiğimiz 30 yıllık dönemde iletişim teknolojilerinde ortaya çıkan hızlı gelişmeler sonucunda, elektronik ticaret dünya ticaretinde egemen bir role sahip olmuştur. Teknolojinin hızla gelişen bir süreç olmasıyla beraber üretim faktörlerinde değişimler yaşanmakta ve üretim faktörleri arasındaki önem de değişmektedir. Bu süreçte gelişmiş teknoloji düzeyi rekabet üstünlüğü yaratmaktadır. Bilimsel araştırmalardan kazandıkları bilgi ve teknolojiyi ekonomiye uygulayan kesimler de uluslararası platformda rekabet üstünlüğüne sahip olmaktadır (Erbaşlar ve Dokur, 2016: 51).

20. yüzyılın sonlarında ortaya çıkan elektronik ticaret, yarattığı farklılıklarla ekonomik alanda dünya üzerindeki dengeleri değiştirmiştir. Elektronik ticaret, geleneksel ekonominin sıradan sistemlerinde kökten değişimlere sebep olmuş; sayısal hale çevrilmiş yazı metninin, ses ve video görüntülerinin hızlı bir şekilde işlenilmesine, iletilmesine ve depolanmasına, ticari işlemler için gerekli olan bilgi ve belgelerin elektronik ortama aktarılmasına ve işlemlerin aynı ortamda yapılmasına imkân sağlamıştır (Organ ve Çavdar, 2012: 65).

E-ticaretin yeni bir kavram olması ve sürekli olarak gelişiyor olması nedeniyle ortak bir tanımı yoktur. Bu yüzden farklı kuruluşların ve hükümetlerin e-ticaret

hakkında tanımları farklılık gösterebilmektedir. E-ticaret hakkındaki başlıca tanımlar şöyledir (Ekici: 2013: 39-40):

- Dünya Ticaret Örgütü'nün (WTO) tanımına göre; e-ticaret, mal ve hizmetlerin üretim, reklam, satış ve dağıtımlarının telekomünikasyon ağları üzerinden yapılmasıdır.
- Ekonomik İşbirliği ve Kalkınma Örgütü'nün (OECD) tanımına göre; e-ticaret, kurumların ve bireylerin katıldığı ve metin, ses ve görsel imaj gibi sayısallaştırılmış verinin işlenerek, açık veya kapalı ağlar üzerinden iletilmesine dayanan ticaretle ilgili işlemlerdir.
- Birleşmiş Milletler İdari, Ticari ve Ulaşım İlgili Uygulama ve Usulleri Kolaylaştırma Merkezi'nin (UN-CEFACT) tanımına göre; e-ticaret, iş, yönetim ve tüketim faaliyetlerinin yürütülmesi için, yapılanmış ve yapılanmamış iş bilgilerinin; üreticiler, tüketiciler ve kamu kurumları ve diğer organizasyonlar arasında elektronik araçlar (elektronik posta ve mesajlar, elektronik bülten panoları), world wide web (www) teknolojisi, akıllı kartlar, elektronik fon transferi, elektronik veri değişimi üzerinde paylaşılmasıdır.
- BM- Uluslararası Ticaret Hukuku Komisyonu (UNCITRAL) tanımına göre; e-ticaret, ticari aktiviteler kapsamında her türlü veri mesajının, Electronic Data Interchange (EDI), internet, e-mail gibi yöntemlerin yanında, telekopi ve fax gibi daha az karmaşık veri iletim yöntemleri kullanılarak elektronik ortamda değişimidir.
- Elektronik Ticaret Koordinasyon Kurulunun (ETKK), Mayıs 1998 tarihli Hukuk Çalışma Grubu raporunda e-ticaret; bireyler ve kurumların, açık ağ ortamında (internet) ya da sınırlı sayıda kullanıcı tarafından ulaşılabilen kapalı ağ ortamlarında (intranet) yazı, ses ve görüntü şeklindeki sayısal bilgilerin işlenmesi, iletilmesi ve saklanması temeline dayanan ve bir değer yaratmayı amaçlayan ticari işlemlerinin tümünü ifade etmektedir.

Yukarıda yapılan tanımlar dikkate alınarak ortak bir tanım yapmak gerekirse e-ticareti; "Bireyler, özel ve kamu kurumlarının birbirleriyle ve kendi bünyesindeki iş, yönetim, üretim ve tüketim faaliyetlerinin yürütülmesi için açık ve kapalı ağlar üzerinden elektronik araçlar kullanılarak metin, ses ve görüntü verilerinin elektronik olarak işlenmesi, iletilmesi ve saklanması

temeline dayanan ticari işlemler olarak betimlemek mümkündür (Özgener, 2004: 168).”

Bu tanımlardan yola çıktığımızda bir işlemin e-ticaret kapsamında değerlendirilmesi için aşağıdaki özelliklere sahip olması gerekmektedir (Ekici, 2013: 42):

- E-ticaret, sanal ortamda gerçekleştirilmelidir.
- Bir değer yaratmayı amaçlamalıdır.
- İki veya daha fazla taraf arasında mal veya hizmet alım satım işlemi gerçekleşmelidir.
- Ses, metin ve görüntü biçimindeki bilgilerin işlenmesi, iletilmesi ve saklanması temeline dayanmalıdır.
- Ticari nitelikte bir işlem olmalı veya ticari işlemi destekliyor olmalıdır.

Bu özelliklere göre e-ticaret kapsamında sayılabilecek iş ve ticaret işlemlerini şu şekilde sıralanabilir (Ekici, 2013:41-42):

- Mal (taşınır, taşınmaz) ve hizmetlerin (bilgi servisleri, danışmanlık, finans, hukuk, sağlık, eğitim, ulaştırma vb.) elektronik alışverişi
- Üretim planlaması yapma ve üretim zinciri oluşturma
- Tanıtım, reklam ve bilgilendirme
- Sipariş verme
- Anlaşma yapma
- Elektronik banka işlemleri ve fon transferi
- Gümrükleme
- Elektronik ortamda üretim izleme
- Elektronik para ile ilgili işlemler
- Elektronik hisse alışverişi ve borsa
- Ticari kayıtların tutulması ve izlenmesi
- Elektronik ortamda sevkiyat izleme
- Ortak tasarım geliştirme ve mühendislik
- Elektronik ortamda kamu alımları
- Doğrudan tüketiciye pazarlama
- Sayısal imza, elektronik noter vb. Güvenilir Üçüncü Taraf (TTP) işlemleri
- Anında bilgi oluşturma ve aktarma
- Elektronik ortamda vergilendirme

- Fikri mülkiyet haklarının transferi

İtici gücü internet olan, internet teknolojisinin gelişmesi ve yaygınlaşmasıyla yeni bir kavram olarak ortaya çıkan e-ticaret giderek geleneksel ticaretin yerini almayı başarmıştır. E-ticaretin, işlemlerin yürütülmesinde geleneksel ticarete göre yeni ve oldukça etkin yöntemleri vardır (Mathur, 2017: 1846). Geleneksel ticarete veri aktarımının sağlanması için birçok yöntem olmasına rağmen bu yöntemler elektronik ticarete e-posta ile diğer veri aktarım kanalları kadar hızlı olamazlar. Geleneksel ticarete göre elektronik ticaretin en önemli özelliği belirgin şekilde iletişim ve onay aşamasında ortaya çıkmaktadır (Erbaşlar ve Dokur, 2016: 53). Elektronik ticarete tüketiciler satın almak istedikleri mal ve hizmetler hakkında bilgilere internet ortamında ulaşırken, geleneksel ticarete satın alınacak ürün hakkında bilgi edinilmesi karşılıklı görüşmeler, dergilerin ve katalogların okunarak incelenmesi sonucu gerçekleşmektedir. Tüketici satın almaya karar verdiği malın siparişini firmaya giderek verirken elektronik ticarete bilgisayar ağları üzerinden siparişini verebilmektedir (Organ ve Çavdar, 2012: 70). Bu bağlamda e-ticaretin geleneksel ticarete üstün olduğu noktalar; “üretim, maliyet, pazar rekabeti, tedarik, uluslararası rekabet ve dağıtım” olarak sıralanabilir (Civelek ve Sözer, 2003: 117).

Satın alma işlemleri yürüten bir firmanın geleneksel (elektronik ticaretin sağladığı imkânlardan faydalanmadan yapılan ticaret) ve elektronik ortamlarda yapacağı ticaretin karşılaştırması Tablo 1’de gösterilmiştir.

Tablo 1: Geleneksel Ticaret- Elektronik Ticaret Karşılaştırılması

	Geleneksel Ticaret	Elektronik Ticaret
Satın Almayı Yürüten Firma		
Bilgi Edinme Yöntemleri	Görüşmeler, dergiler, kataloglar, reklamlar	Web sayfaları
Talep Belirtme Yöntemi	Yazılı form	Elektronik posta
Talep Onayı	Yazılı form	Elektronik posta
Fiyat Araştırması	Kataloglar, görüşmeler	Web sayfaları
Sipariş Verme	Yazılı form, fax	Elektronik posta, EDI
Tedarikçi Firma		
Stok Kontrolü	Yazılı form, fax, telefon	Online veri tabanı, EDI
Sevkiyat Hazırlığı	Yazılı form, fax, telefon	Elektronik veri tabanı, EDI
İrsaliye Kesimi	Yazılı form	Online veri tabanı, EDI
Fatura Kesimi	Yazılı form	Elektronik posta, EDI

Sipariş Yapan Firma		
Teslimat Onayı	Yazılı form	Elektronik posta, EDI
Ödeme Programı	Yazılı form	Online veri tabanı, EDI
Ödeme	Banka havalesi, posta, tahsil	İnternet bankacılığı, EDI, EFT

Kaynak: Erbaşlar ve Dokur, 2016: 53.

Elektronik ticarete bilgisayar, telefon, televizyon, faks, kredi kartları, elektronik veri değişimi (EDI), internet, gibi birçok elektronik araçtan yararlanılmaktadır (Canpolat, 2001: 11; Hasiloğlu, 2003: 22). E-ticaret Tablo 2’de detaylandırılan bu araçlarla sınırlı kalmamakla beraber sürekli gelişim göstermektedir.

Tablo 2: Elektronik Ticaretin Araçları

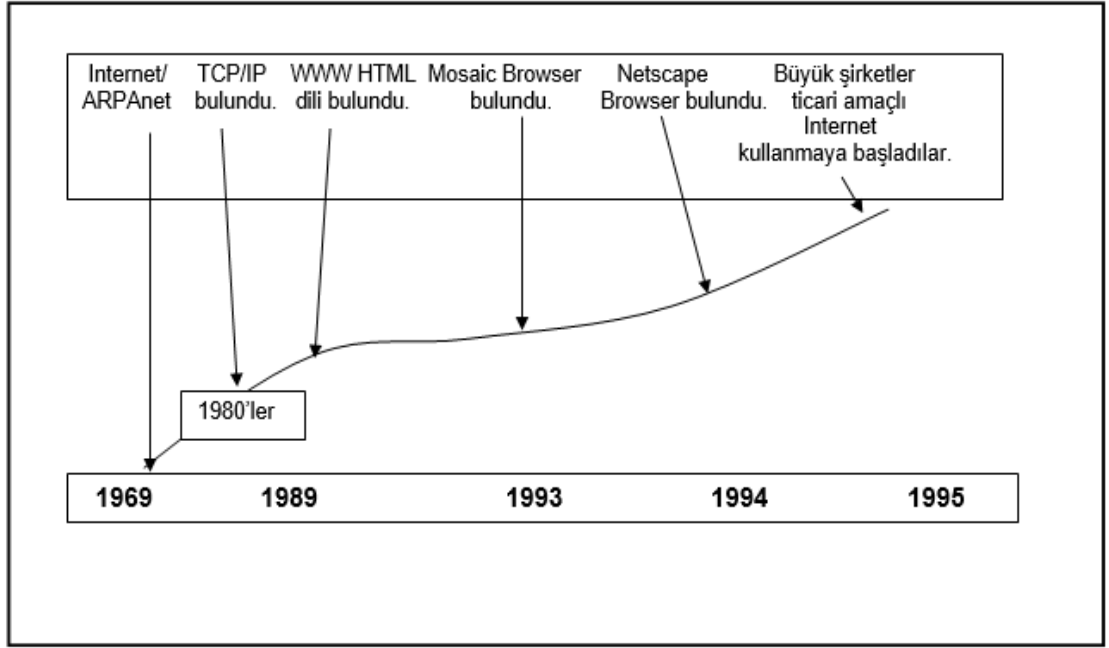
Bilgisayar	WWW (World Wide Web)
Radyo/ Televizyon	FTP
Telefon	Elektronik Posta
Faks	Sözlü Mesaj (Voice Mail)
Elektronik Ödeme ve Para Sistemleri; Bankamatik Makineleri (ATM) Kredi Kartları POS Makineleri	Konferans Sistemleri; Telekonferans Data Konferans Video Konferans
İntranet Kapalı Bilgisayar Ağları; Elektronik Fon Transferi (EFT) Elektronik Veri Değişimi (EDI)	Mobil İletişim İçin Küresel Sistem Teknolojisi(GSM) Kısa Mesaj Servisi(SMS) Telsiz Uygulama Programı Protokolü(WAP)

Kaynak: Hasiloğlu, 2003: 21.

1980’lerden beri elektronik iletişim teknolojilerinin ticari hayatta kullanılmasına rağmen internetin elektronik ticaret için kullanılmaya başlanması 1995’lere dayanmaktadır. İnternetin ekonomiye uyum sağlamasıyla beraber e-ticaret büyük bir sıçrama gerçekleştirmiştir. Amazon.com 1995 yılında ABD’de ilk ciddi e-ticaret sitesi olarak açılmış ve elektronik ticaretin faydalarından yararlanarak kısa sürede büyük ölçekte ticari işlemler yapan bir işletme haline gelmiştir. Türkiye ise 1994- 1995 yılları arasında e-ticaret kavramıyla tanışmıştır. Türkiye’de 1998 yılında infoshop.com adıyla ilk ciddi e-ticaret sitesi kurulmuştur. Aktif olarak günümüzde bu

site hepsiburada.com adıyla hala işleyişini sürdürmektedir. Büyük şirketlerin interneti ticari olarak kullanmaya başlaması e-ticarete küresel bir boyut kazandırmıştır. E-ticaretin üstünlüklerinden doğru bir şekilde yararlanan işletmeler de rekabet üstünlüğünü elde etmişlerdir. Şekil 1’de internetin ortaya çıkmasıyla gelişen e-ticaretin aşamaları gösterilmektedir (Erbaşlar ve Dokur, 2016: 11).

Şekil 1: İnternetin ve E-Ticaretin Evriminde Kilometre Taşları



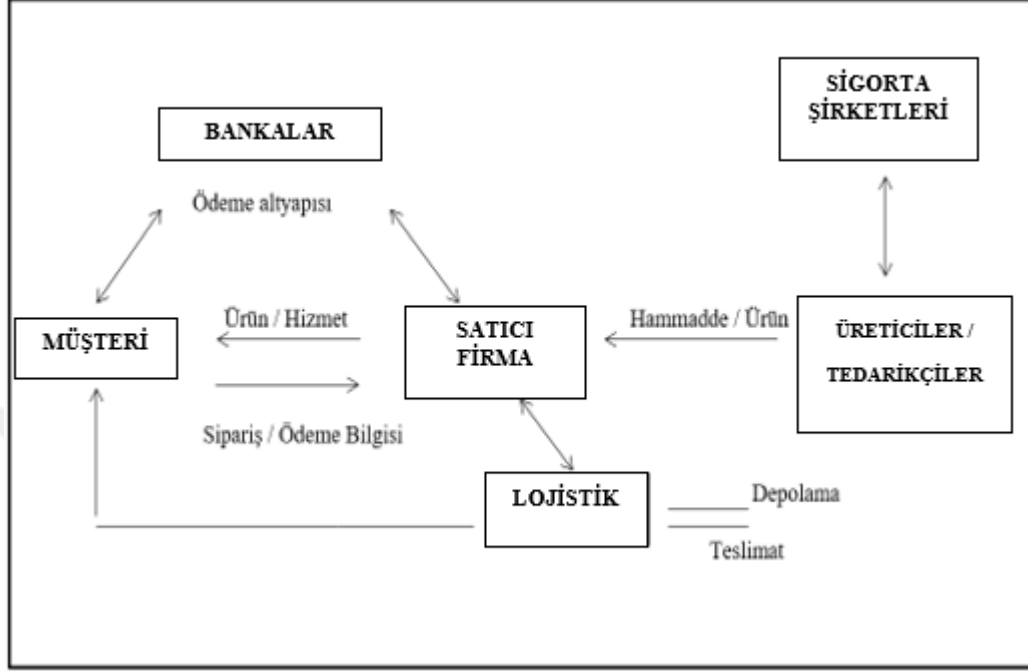
Kaynak: Erbaşlar ve Dokur, 2016: 11.

Elektronik ticaret, bilgisayar ağları sayesinde işlemlerin gerçekleştirilmesinde standardizasyon sağlamıştır. Buna ek olarak üreticiden tüketiciye kadar gelen zincirde tedarik aşamasında kolayca işlerin yürütülmesi, işlem maliyetlerinin düşüklüğü, tüketiciden gelen tepkilerin hızla alınabilmesi, ürün geliştirmenin hızlanması, sunulan ürün seçeneklerinin fazla olması, tüketicilerin aldıkları ürünleri evlerinde teslim alabilmeleri gibi özellikler e-ticaretin getirdiği avantajlardır (Sırma, 2002: 103).

Ticari işlemlerin gerçekleştirilmesi için gerekli bilgiler, işlemi başlatan kişi veya kurum tarafından, ticaret sürecinin parçası olan tüm tarafların (üretici, satıcı, alıcı, gümrük idareleri, sigortacı, nakliyeciler, bankalar, diğer kamu kurumları vb.) birbirine bağlı bilgisayarlarından birisine önceden belirlenmiş şekilde bir kez giriş yapıldığında, kısa süre içerisinde tüm tarafların bilgisayarlarına ulaşmaktadır. Gerekli belgeler elektronik ortamda hazırlanıp ilgililerin kullanımına sunulmaktadır. Belirtilen bu durum Şekil 2’de gösterilmektedir. Böylece işlemlerde hem hata oranı en aza

indirilir hem de işlem maliyetleri en düşük seviyede kalmaktadır (Erbaşlar ve Dokur, 2016: 50).

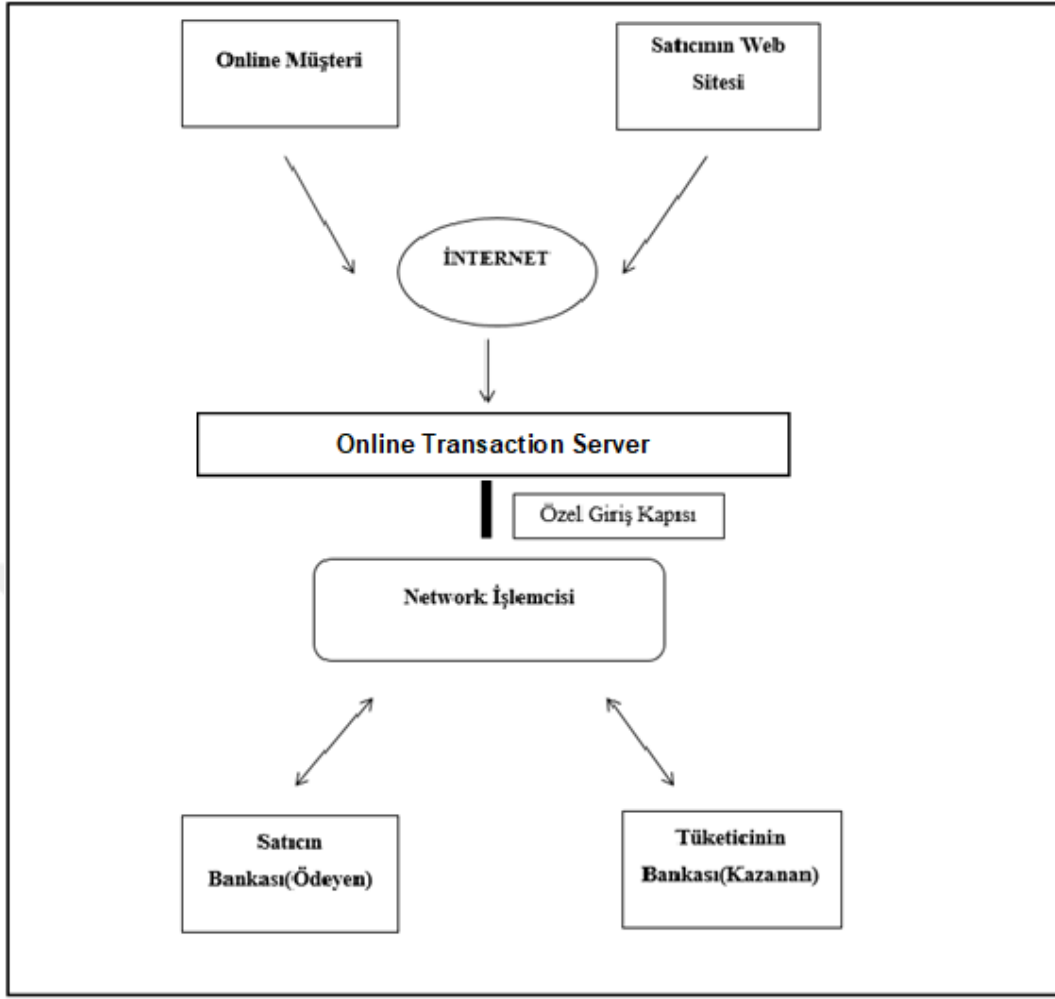
Şekil 2: E-Ticarete Sistemin İşleyişi



Kaynak: Ersoy, 1999.

İnternetin ticarete kullanılması ile çevrimiçi müşteri kavramı da ortaya çıkmıştır. Çevrimiçi müşteri, işlemlerini internet ortamında gerçekleştirerek mal ve hizmet satın alan kişi ve kurumlardır. Çevrimiçi müşteri, satın almak istediği ürüne internet aracılığıyla satıcının web sitesine giriş yaparak buradan karar verir. Çevrimiçi müşteri, kişisel bilgilerinin şifrelendiği 'Transaction Server'a yönlendirilir. Sipariş onaylandığı zaman bilgiler, internet aracılığıyla özel bir yöntemle ödemeyi yapan veya ödemeyi teslim alan bankaların bu işlemi onayladıkları veya reddettikleri Network işleme mekanizmasına gelir. Yapılan işlemlerin gerçekleşme zamanı gelişen teknolojiler sayesinde genelde 5-7 saniyenin üstüne çıkmaz. İnternet üzerinden e-ticaretin çalışma yapısı Şekil 3'te de gösterilmektedir (Erbaşlar ve Dokur, 2016: 13):

Şekil 3: İnternet Üzerinden E-Ticaretin Çalışma Yapısı



Kaynak: Erbaşlar ve Dokur, 2016:12.

İnternetin ticarete kattığı yararlar sayesinde ticaretin küresel çapta uygulanabilirlik derecesi artmıştır. Büyük bir kullanıcı kesimine ulaşabilen internet, işletmeleri sanal ortama taşımış ve elektronik ticaretin gelişmesinde büyük rol oynamıştır. Tasarım, kullanım kolaylığı, etkileşim ve teknoloji kullanımı, içerik, herhangi bir çevrimiçi perakende kuruluşunun web sitesi için önemli kriterler olsa da bunların tümü için güvenlik önlemlerinin alınması gerekmektedir (Tariq vb., 2017:1). Aynı zamanda işletmeler sanal ortamın getirdiği avantajlardan yararlanırken oluşturduğu dezavantajları da aşmak zorundadırlar. Bu dezavantajlardan bazıları şöyledir (Özgener, 2004: 170):

- Dağıtılan bilgi üzerindeki denetim yetersizliği; Bilgisayar korsanlarının hizmet sağlayıcılara, işletme bilgisayarlarına ve kişisel kullanıcılara müdahalesi nedeniyle internet üzerinden veri akışında tam denetimin sağlanamaması.

- Bilginin yayılması ve çalınması üzerindeki denetim yetersizliği; İnternet üzerinde kişiye, kurumlara ve işletmelere özel bilgi, program ve uygulamaların denetim dışı yayılması ve çalınması ile ilgili düzenlemelerin henüz tam anlamıyla yeterli olmaması.
- Bilgiye ulaşmada karşılaşılan sorunlar; İnternet ortamına sunulan bilgilerin kategorilere ayrılmasıyla ilgili çalışmaların yetersiz olması nedeniyle ulaşılmak istenen bilgiye kolay ve kısa bir şekilde ulaşamamak.

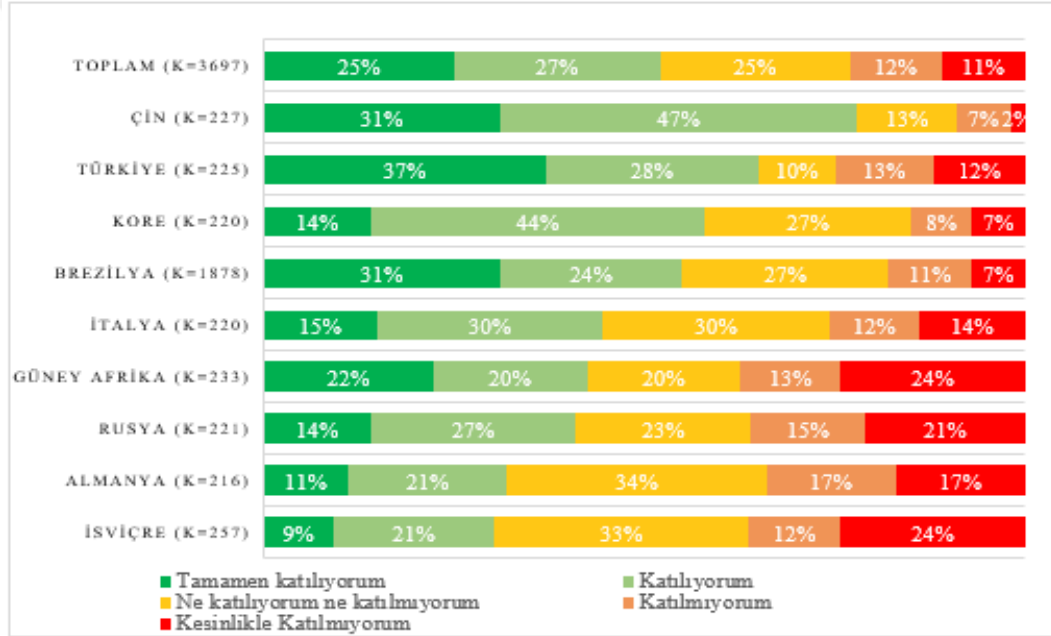
Elektronik ticareti; ticaretin gerçekleşme biçimine göre, ticaretin gerçekleştiği ortamın özelliğine göre ve ticareti gerçekleştiren katılımcılar şeklinde gruplandırmak mümkündür. Ticaretin gerçekleşme şekline göre elektronik ticaret; doğrudan e-ticaret ve dolaylı e-ticaret olarak ikiye ayrılmaktadır. Dolaylı e-ticarette malların siparişi elektronik ortamda yapılmakta ancak teslimat fiziki olarak yapılmakta ve geleneksel ticaret yollarından biri kullanılmaktadır. Doğrudan e-ticaret; siparişi, ödemesi, teslimi dijital ortamda yapılan mal ve hizmetleri kapsamaktadır (Akpınar, 2017: 24). Ticaretin dayandığı ortama göre elektronik ticaret, açık ağlar ve kapalı ağlar olmak üzere ikiye ayrılmaktadır. E-ticaret, internet gibi açık ağlarda gerçekleşebileceği gibi firmalar arasında kullanılan EDI sistemi kullanılarak kapalı ağda da gerçekleşebilmektedir (Organ ve Çavdar, 2012: 64). Elektronik ticaret, ticareti gerçekleştiren katılımcılara bağlı olarak değişik kişi ve gruplar arasında da gerçekleştirilebilmektedir. Günümüzde elektronik ticaret, internetin ve küreselleşmenin getirdiği yararlar sayesinde her kesim tarafından tercih edilmektedir. Elektronik ticaretin gerçekleştiği taraflar, B2C (Firmadan tüketiciye), B2B (Firmadan firmaya), C2B (Tüketiciden firmaya), C2C (Tüketiciden tüketiciye), B2E (Firmadan çalışanına), B2G (Firmadan devlete), G2B (Devletten firmaya), G2G (Devletten devlete), G2C (Devletten tüketiciye), C2G (Tüketiciden devlete) olarak sınıflandırılmaktadır (Tsiakis, T. ve Sthephanides, G. 2005: 11).

E-ticaretin günümüzde vardığı boyutlarla ilgili olarak, özellikle pandeminin dünya gündemine oturmasıyla e-ticarette yaşanan gelişmeler şöyledir. Birleşmiş Milletler Ticaret ve Kalkınma Birliği (UNCTAD) (2021) tarafından gelişmekte olan ve gelişmiş dokuz ekonomide (Brezilya, Çin, Almanya, İtalya, Kore, Rusya, Güney Afrika, İsviçre ve Türkiye) yaklaşık 3700 tüketicinin katıldığı “COVID -19¹ ve E-

¹ Covid 19, İlk olarak Çin’in Vuhan Eyaleti’nde aralık ayının sonlarında solunum yolu belirtileri (ateş, öksürük, nefes darlığı) gelişen bir grup hastada yapılan araştırmalar sonucunda 13 Ocak 2020 ‘de tanımlanan bir virüstür (T.C. Sağlık Bakanlığı,2020. Erişim Tarihi 09.05.2021).

Ticaret” başlıklı araştırmaya göre hem yükselen hem de gelişmiş ekonomilerdeki tüketicilerin çevrimiçi alışverişe yöneliminin yükselen bir ivmeyle arttığı belirlenmiştir. COVID-19 sırasındaki çevrimiçi alışveriş artışlarının ülkeler arasındaki farklılıklarında en güçlü artış Çin ve Türkiye’de gözlemlenirken, en zayıf ise daha fazla insanın e-ticaretle uğraştığı İsviçre ve Almanya olarak gözlemlenmiştir. Grafik 1’de görüldüğü üzere Çin, Türkiye ve Kore’den katılımcıların çoğu COVID-19’un ortaya çıkmasından bu yana eskisinden daha sık çevrimiçi alışveriş yaptıklarını belirtmiştir. Öte yandan, Almanya ve İsviçre’nin gelişmiş ekonomilerinde çok daha az sayıda tüketicinin, çevrimiçi satın alma faaliyetlerini arttırdığı gözlemlenmiştir (UNCTAD, 2021. Erişim Tarihi 08.05.2021).

Grafik 1: COVID- 19’un Ortaya Çıkmasıyla Birlikte Eskisinden Daha Sık Çevrimiçi Alışveriş Yapma Sıklığı Anket Sonuçları



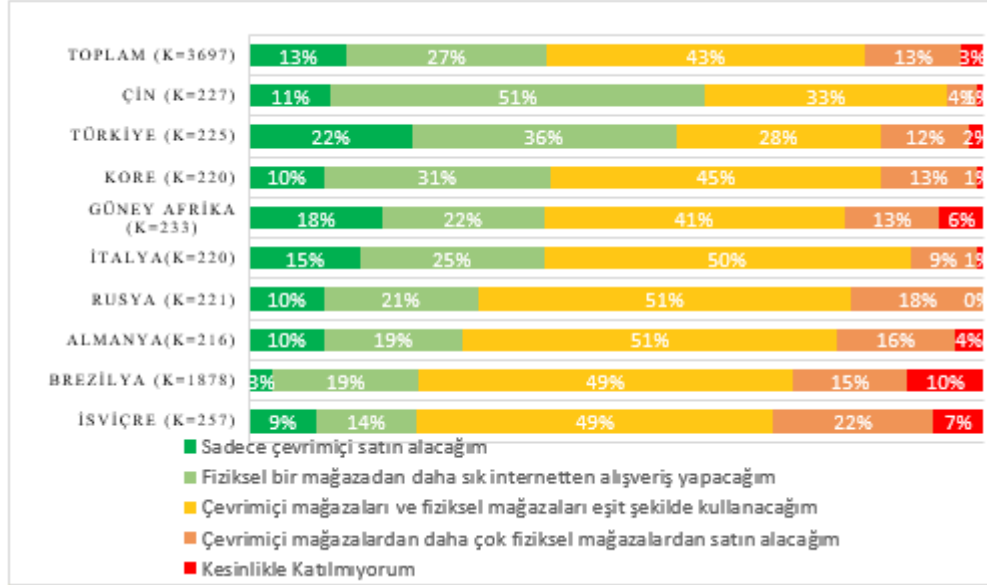
(K= Katılımcı sayısı)

Kaynak: UNCTAD, 2021. https://unctad.org/system/files/official-document/dtlstictinf2020d1_en.pdf
Erişim Tarihi 08.05.2021.

Anket sonuçlarına göre, Grafik 2’de COVID-19’dan sonra gelecekteki satın alma kanalları arasından, Çin ve Türkiye’deki tüketicilerin, çevrimiçi satın almayı fiziksel mağazalardan daha sık tercih ettikleri, İtalyan, Rus, Alman, Brezilyalı ve İsviçreli tüketicilerin ise dijital ve fiziksel perakendecilik arasında dengeli bir yaklaşım tercih ettikleri gözlemlenmiştir. Pandemiden önce İsviçre ve Almanya gibi daha yerleşik çevrimiçi alışveriş sektörlerine sahip ülkelere göre Çin ve Türkiye gibi çevrimiçi alışveriş sektörüne düşük katılım oranlarıyla başlayan ekonomilerde

çevrimiçi alışveriş yapan insan sayısında daha yüksek büyüme oranları bulunmuştur (UNCTAD, 2021. Erişim Tarihi 08.05.2021).

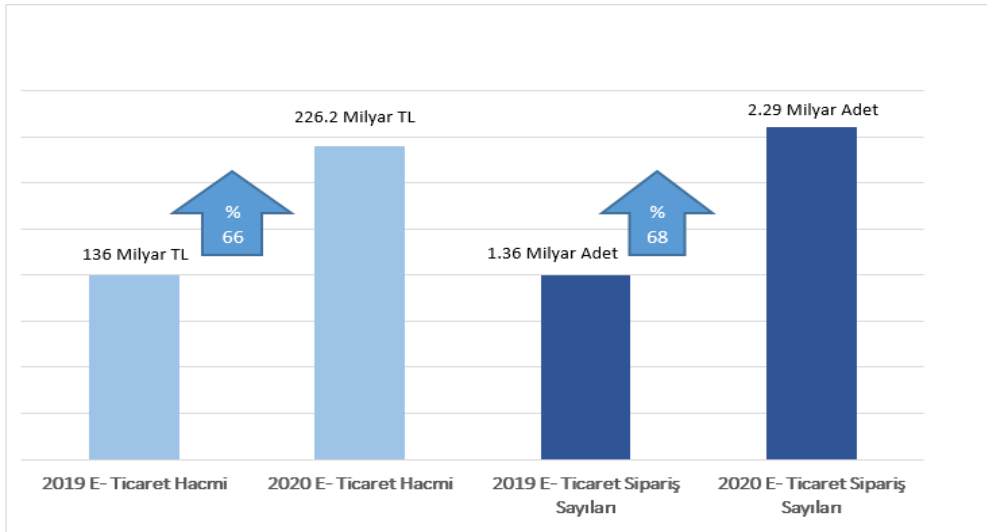
Grafik 2: COVID-19 Sonrası Farklı Satın Alma Kararları İçin Tercihler



Kaynak: UNCTAD, 2021. https://unctad.org/system/files/official-document/dtlstictinf2020d1_en.pdf
Erişim Tarihi 08.05.2021.

Pandemi sonrası e-ticaret işlemlerinin artışıyla birlikte T.C. Ticaret Bakanlığı (2021) tarafından yapılan araştırma verilerine göre Grafik 3'te de belirtildiği üzere 2019 yılına kıyasla 2020 yılında Türkiye'deki e-ticaret hacmi %66 artış gösterdiği görülmüştür. Aynı şekilde 2020 e-ticaret sipariş sayıları da 2019'a kıyasla %68 arttığı tespit edilmiştir. (E-Ticaret Bilgi Platformu, 2021. Erişim Tarihi 08.05.2021).

Grafik 3: 2020 Yılı E-Ticaret Hacmi



Kaynak: E- Ticaret Bilgi Platformu, 2021. Erişim Tarihi 08.05.2021.

1.2. ELEKTRONİK TİCARETTEN MOBİL TİCARETE GEÇİŞ

İnternetin dünya çapında yaygınlaşması ile birlikte elektronik ticaretin gelişmesi, uluslararası ticaret hacmini ve ticarete konu mal sayısını arttırmıştır. Aynı zamanda uluslararası şirketlerin yeni yönetim şekillerini keşfetmelerini, yeni finansal araçların bulunmasını ve yeni şirket kavramlarının ortaya çıkmasını sağlayarak ülkelerin ekonomik ve finansal sistemlerinde önemli etkiler yapmaya başlamıştır. Ekonominin son yıllarda yaşadığı hızlı küreselleşme hareketi, mal, hizmet, işgücü ve sermaye piyasalarının daha fazla bütünleşmiş ve rekabetçi olmalarını teşvik etmiştir (Mülküt, 2017: 9-10).

Geçmişte internete girebilmek için kullandığımız cihazlar insanlara mekân özgürlüğü sağlamayan statik cihazlardan oluşmaktayken, kablosuz teknoloji devrimiyle birlikte mobil cihazların, kullanıcıların hareket halindeyken işlemleri gerçekleştirdiği yeni dijital ekonominin kritik bir bileşeni haline gelmesini sağlamıştır. Mobil cihazları kullanmak, çevrimiçi ve güncel bilgilere erişimi kolaylaştırmıştır.

Taşınabilir cihazların tasarımındaki son teknolojik gelişmeler, artan yüksek hızlı internet erişimi ve mobil ağ teknolojileriyle birlikte, kullanıcıların bu tür cihazları her yerde, her zaman kullanmalarına ve internette gezinme ve e-posta okuma gibi işlemlere ek olarak e-ticaret işlemlerini gerçekleştirmelerine olanak sağlamıştır (Isaac ve Zeadally, 2014; Koenigstorfer ve Groeppel-Klein, 2012). Artık ticari faaliyetler zaman sınırlamasını ortadan kaldırarak, mekâna bağlı kalmadan 7/24 gerçekleştirilebilir hale gelmiş ve e-ticaretin bir parçası olmuştur.

Ticari faaliyetlerde yapılan işlemlerin kablosuz erişime sahip akıllı telefon, tablet gibi mobil cihazlar aracılığıyla gerçekleştirilmesi ise mobil ticaret (m-ticaret) olarak adlandırılmaktadır. Özellikle mobil cihazların büyük bir gelişim göstererek özelliklerinin artmasıyla beraber internete bu cihazlar üzerinden kolaylıkla her yerden bağlanılarak çevrimiçi alışveriş yapmalarına olanak tanıdığından mobil ticaretin gelişimine büyük katkıda bulunmaktadır (Wu vd., 2010: 531-532). Mobil ticaret, işletmeler için de olumlu bir gelişme olarak karşımıza çıkmaktadır. Her yerde bulunabilme, kişiselleştirme, esneklik gibi özelliklerinden dolayı işletmelere geniş çaplı pazar potansiyeli vaat etmektedir. Mobil kullanıcılar ise cihazlarını, hızlı ve kısa iletişim, fiyat kontrolü veya konumla ilgili hizmetler gibi çevrimdışı etkinliklerde kullanma bakımından avantajlı bir araç olarak görmektedirler. Her bir kişiye her yerden mobil cihazlarla yalnızca birkaç tıklamayla alışveriş yapma, bankacılık

işlemlerini yapma ve medya dosyaları indirebilme gibi işlemleri yapmayı sağlamaktadır. Whatsapp, Yahoo ve Gtalk gibi çeşitli mobil mesajlaşma programlarında ve diğer ağ platformlarında oturum açarak da çevrimiçi esnek erişilebilirlik imkânı sağlamaktadır. Şirketlerin ve satıcıların son kullanıcıya yaklaşma yolu olarak da belirtilebilir (Chung ve Holdsworth, 2012: 224).

Pek çok benzerlik olmasına rağmen, m-ticaret ile e-ticaret arasında pek çok fark vardır. Bunlardan aşağıdaki şekilde söz edilebilir (Niranjanamurthy vd., 2013: 2367):

- Bir e-ticaret müşteriyi takip ederken, fiyat ve ürün karşılaştırması, kullanıcı incelemeleri ve satın alma gibi tüm faaliyetler bilgisayar kullanılarak gerçekleştirilir.
- Karmaşık işlemler e-ticarete kolaydır ve yeterli zaman vardır. M-ticaret için ise fiziksel kaynaklar ve zaman çok daha önemlidir.
- M-ticarete kişiselleştirilmiş içerikler mevcuttur.
- M-ticarete sipariş verme süresi e-ticarete göre daha kısadır.
- M-ticaretin e-ticarete göre işlem maliyeti daha düşüktür.
- E-ticarete elektrik zorunlu unsurlardan biri olmasına karşılık m-ticarete böyle bir zorunluluk yoktur.
- E-ticaret açık internete dayanır, m- ticaret ise mobil iletişim ağı tabanlıdır yani m-ticarete ağ sinyali mevcut olduğu sürece, mobilden mobile ve hattan mobile diğer cihazlara bağlanabilir ve ticaret işlemleri yapılabilir.
- M-ticaret ödeme veya Wİ-Fİ bağlantı gerekliliğini ortadan kaldırır.

Mobil ticaretin avantajları olduğu gibi çoğu cihazın küçük ekranları, dosya ve veri aktarım türlerini sınırladığından, mobil ve kablosuz geniş bant altyapısı kurmanın maliyetli yapısından ve sınırlı grafik kullanım koşullarından kaynaklı dezavantajlarının da olduğunu söylemek mümkündür (Niranjanamurthy vd., 2013: 2368).

M-ticarete ele alınması gereken bazı temel sorunlar; güvenlik, gizlilik ve kullanılabilirliktir. Bunlardan birinin olmaması m-ticaret uygulamalarının büyük ölçüde kullanılmasını engellemektedir (Esparza vd., 2006: 2308). Güvenlik, m-ticaret ile ilgili önemli bir konudur. Mobil cihazlar mobil ticaret için giderek daha fazla kullanılıyor ve bu tür cihazlardaki kullanıcıların verilerinin güvenliğinin sağlanması

büyük önem taşımaktadır. Günümüzde mobil cihazları hem kişisel hem de profesyonel her türlü faaliyet için kullandığımızdan kişisel ve özel bilgilerimizin çoğunu içermektedir. Bu bilgiler her zaman güvenli bir şekilde ele alınmaz ve birçok uygulama bellekteki kişisel ve hassas verilere kötü davranma eğilimindedir. Perakendeciler, bankalar, ödeme hizmeti sağlayıcıları vb. için, mobil cihazlarında çevrimiçi ödeme yapan kullanıcılar için güvenli bir ortam oluşturmak ve aynı zamanda iyi bir kullanıcı deneyimi sürdürmek arasında iyi bir denge kurmak için birlikte çalışmak önemlidir (Licina vd., 2017:12-14; Gururajan, 2006: 3-4).

Mobil ticarete güvenlik riskleri, hem teknik riskler (doğrudan güvenlik tehditleri) hem de teknik olmayan riskler (dolaylı) olarak ikiye ayrılmaktadır (Licina vd., 2017:14): Doğrudan güvenlik riskleri; bir teknik, veri veya yazılım sorunları nedeniyle kullanıcıları doğrudan etkileyen risklerdir. Mobil bilgi işlem için daha özel olan güvenlik riskleri; kötü niyetli kullanıcılar, veri alışverişi ile ilgili güvenlik sorunları, küçük boyutlarından dolayı cihazın kaybolması veya çalınması veya konum tanımlamasından kaynaklanan güvenlik sorunlarıdır. Kötü niyetli kullanıcılar için, mobil ortam çok iyi bir koruma sağlamaktadır. Cep telefonları gibi kablosuz cihazlar, kablosuz bölgelerin içinde ve dışında dolaşır; belirli bir coğrafi noktaları yoktur ve kolayca çevrimiçi ve çevrimdışı olma becerisine sahiptirler. Bu, kullanıcıların ağ bağlantılarını hızla kesmelerini sağlar. Bu nedenle bir mobil kullanıcıyı izlemek zordur. Dolaylı güvenlik riskleri ise örneğin gizlilik sorunları, kişisel bilgiler ve devlet endişeleriyle ilgilidir. M-ticaret işlemleri genellikle alıcıların, bir satış işlemini tamamlamak amacıyla veya sadece şirket tarafından gerekli olduğu için ad soyad, e-posta, tc kimlik numarası gibi büyük miktarda kişisel bilgi girmesini gerektirir. Tüketiciler de genellikle bilgilerinin gerçekte ne kadar güvenli olduğu, bunlara kimin erişimi olduğu ve nasıl kullanılacağı konusunda fazla düşünmezler. Cep telefonlarının kullanımı hem kişisel hem de sosyal avantajlar sağlar. Bununla birlikte, bu avantajlar, kişisel bilgilerin yönetimiyle ilgili bir dizi tehdit ve sorunla birlikte gelir. Mobil ticaret söz konusu olduğunda, kullanılabilirlik de son kullanıcılar için önemli bir faktördür. Web sitesi geliştirmenin esasları ve belirli özellikleri, tasarımcılar için büyük bir zorluktur ve bu nedenle bu bileşen, geleneksel olarak farklı yönergeler olan kullanılabilirlik kalıpları kullanılarak belgelenebilir. Mobil cihazlar aracılığıyla web ara yüzlerinin kullanılabilirliğini anlamanın ve geliştirmenin ticari faydası büyüktür. Cep telefonları birçok yeni uygulamaya erişim sağlayabilir, ancak aynı zamanda küçük

ekran boyutu, sınırlı ekran çözünürlüğü ve daha zor giriş mekanizmaları gibi sınırlamalar da getirir (Licina vd., 2017:12-14; Gururajan, 2006: 3-4).

Mobil ticaret uygulamaları ise zaman açısından kritik olan ve görevlerin daha verimli bir şekilde gerçekleştirilmesine izin vererek hareket halindeki insanlara hitap eden hizmetler için kullanılmaya başlanmıştır. Günümüzde birçok mevcut m-ticaret uygulaması ve hizmeti bulunmaktadır. Bunlardan bazıları mobil bankacılık, fatura ödeme, konum haritaları ve çeşitli haberler, mobil alışveriş, bilet ve mobil dosya paylaşımıdır. Bu hizmetlerde m-ticaret sadece yaygın olarak kabul edilmekle kalmıyor, aynı zamanda daha popüler bir iş/ ticaret yöntemi olark da kullanılıyor. Belli başlı m-ticaret kullanım alanlarını, “finans, telekomünikasyon, bilgi ve iletişim, perakende, mobil komisyonculuk/satın alma/pazarlama ve reklamcılık” gibi sektörler olarak tarif etmek mümkündür (Niranjanamurthy vd., 2013: 2369).

1.3. E-TİCARETTE KULLANILAN ELEKTRONİK ÖDEME YÖNTEMLERİ

Hayatımızın vazgeçilmezi haline gelen internet, tüketim alışkanlıklarımızı da etkilemiş, online satın alma hacmini özellikle içinde bulunduğumuz pandemi dönemi içinde yukarı çekmiştir. Yapılan araştırmalar gelecekte de online alışverişin kazandığı ivmenin süreceğini göstermektedir (UNCTAD, 2021. Erişim Tarihi: 02.05.2021). Bu noktada internet bankacılığı hizmetleri de zaman ve mekân sınırı olmaksızın tüketicilere alışveriş yapmasına imkân sağlamıştır. Teknolojide yaşanan gelişmelerle beraber e-ticaretin yükselişi yeni ödeme yöntemlerinin de artan oranda kullanımını başlatmıştır.

Ödeme yöntemlerini açıklamadan önce ödeme kavramını tanımlamak gerekirse, en ilkel biçimde ödeme, “mal ve hizmetlerin diğer mal ve hizmetlerle doğrudan değişimini (takas sistemini) kapsamaktadır. Diğer bir deyişle ödeme kavramı, paranın veya parasal yükümlülüğün yerine getirilmesi amacıyla herhangi bir belgenin karşılıksız veya borç olarak verilmesi olarak tanımlanabilir. Ödeme sistemleri ödemenin gerçekleşmesini sağlayan mekanizmalardır (Brindle ve Cox, 2004: 320). Ödeme yöntemleri genel anlamıyla, ekonomik birimlerin kendi içinde mal veya hizmetlerin değişimini kolaylaştıran araçları, işletim süreçlerini, kuralları ve iletişim ağını kapsayan bir yapı olarak tanımlanmaktadır (Erdoğan, 2004: 80).

Günümüzde ödeme araçları oldukça gelişmiş ve çeşitlenmiştir. Ekonomide yer alan katılımcıların ihtiyaçlarını mümkün olduğunca daha iyi bir şekilde karşılamak

iin, teknolojinin geliřmelerden her geen gn deme mekanizmalarını kolaylařtırmak amacıyla yararlanılmaktadır (Abrazhevich, 2001: 81). Nakit deme bugn kullanılan para transferi trleri arasında en popleri olsa bile, daha byk miktarların sz konusu olması, para maliyetini ve mevcut deme sistemlerini azaltma ihtiyaı, kk satın alımlar ve anında demeler iin esnekliėin saėlanması, dolandırıcılık ve diėer su trlerine karřı gvenliėi ve korumayı arttırmak, e-ticaretin internette ve evrimii demelerde ortaya ıkması, insanların servetlerini daha az nakit biimde tutmak ve banka gibi finansal kuruluřların hizmetlerinden yararlanmak amacıyla kullanıcılar elektronik ortamda deme seeneklerini tercih edebilmektedir (Aliyev, 2019: 52; Liebana- Cabanillas, 2015: 421).

“Elektronik deme yntemleri, nc bir kuruluř aracılıėıyla iki kiřinin birbirine gvenli ve kolay bir řekilde para transferi yapmalarına olanak veren veya mal-hizmet alımlarının gerekleřtirmelerini internet zerinden yapmalarını saėlayan sistemlerdir (zbař, 2019: 87).” Bir bařka deyiřle “elektronik deme, belgelerin elektronik řekilde temsil edildiėi ve iřlemlerin elektronik olduėu bir deme yntemidir (Tsiakis vd., 2005: 147).”

Avrupa Merkez Bankası, elektronik ortamdaki demelerin sorunsuz bir řekilde gerekleřmesi ve deme iřlemlerine ait gvenliėin saėlanmasından bankaları sorumlu tutmaktadır (Erdoėdu, 2004: 80). lkemizde deme sistemlerinden Trkiye Cumhuriyet Merkez Bankası (TCMB) sorumludur. Buna gre TCMB, kurulmuř ve kurulacak olan deme sistemlerinin yapısındaki riskleri azaltacak dzenlemeleri yapmak, finansal ve parasal istikrarın saėlanması, para politikalarının etkili řekilde yrtlmesi iin deme sistemlerinde gnn kořullarına gre gerekli dzenlemeleri yapmak, sistemlerin etkinliėini ve gvenliėini etkileyebilecek geliřmeleri takip etmek gibi yetki ve sorumlulukları bulunmaktadır (Dndar ve Duramaz, 2014: 25).

“deme sisteminin kurulum, geliřim, iřletim ve denetim srelerinde merkez bankalarının doėrudan rol almasının nedeni; para politikalarının bařarı ile yrtlmesi iin saėlıklı iřleyen bir deme sistemine gereksinim duyulması, lke ekonomisi ynnden yksek stratejik nem tařıyan bu tr sistemlerde gvenlik ve denetimin saėlanması, yksek tutarlı fon demeleri ve menkul kıymet iřlemlerinin merkez bankaları nezdinde tutulan hesaplar zerinden yapılmakta olması, denetim yetkisi ve mevzuat belirleyici konumu nedeniyle merkez bankalarının kredi riskinin ve sistemik riskin azaltılmasında rol tařımaları olarak sayılabilir (TCMB, 2014. Eriřim tarihi 30.03.2020).”

Elektronik ödeme hizmeti, müşterilerin banka hesaplarına ve işlemlerine uzaktan erişmesine, bunları yönetmesine olanak tanıyan web tabanlı bir kullanıcı arayüzü ile birlikte gelmektedir. Genel olarak elektronik ödeme, internet üzerinden gerçekleştirilen e-ticaret / çevrimiçi işlemler bağlamında elektronik ödeme sürecini ifade eder (Shafie vd., 2018: 54). Elektronik ödemeler, kâğıtsız bir ödeme süreci olarak da tanımlanabilmektedir (Fatonah ve Wibowo, 2018: 2).

E-ödemeler, e-ticarete önemli bir rol oynar ve etkili bir e-ödeme yönteminin olmaması e-ticaret gelişimini engelleyebilecektir. E-ödeme yöntemlerinin kullanılması tüketicilerin bu yöntemlere güven duymasına bağlıdır. E-ticarete güven yaratmak için ilk olarak güveni anlamak gerekmektedir. E-ödeme yöntemlerinde tüketicilerin bu yöntemleri benimsemesini engelleyen birçok faktör bulunmaktadır (AL-Maaitah ve Shatat, 2011: 395). Bu faktörler güven eksikliği, kullanılabilirlik, güvenlik, algılanan avantaj eksikliği ve algılanan riskle ilgilidir. Özkan vd. (2010) bu faktörleri çalışmalarında şöyle değerlendirmişlerdir:

- E-ticarete “güven”, tüketicinin parasının ve kişisel bilgilerinin, diğer kişilerin çıkarları için kullanılmayacağına duyduğu güvendir. Kusurlu bir sistem kullanılsa bile tüketiciler; satıcıların, bankaların ve kredi kartı şirketlerinin kişisel bilgilerini kötüye kullanmayacağına inanmak istemektedirler. Tüketici güveni ne oranda yüksekse, tüketicilerin satın alma konusundaki niyetleri o oranda yüksek ve tüketicileri elde tutmak o kadar kolay olmaktadır.

- E-ödeme yöntemlerinin benimsenebilmesi için “kullanılabilir olması” gerekmektedir. Bu yöntemler tüketici için karmaşıklık yaratmamalı, kullanım kolaylığı olmalı ve kullanıcı dostu şeklinde tasarlanmalıdır. Ödeme süreci çok zaman alırsa ve karmaşıksa müşterinin motivasyonu düşer ve diğer web etkinliklerini kullanmaktan da kaçınır. Müşteriler çevrimiçi işlemlerinde daha fazla kolaylık algılayorsa büyük olasılıkla e-ödeme yöntemlerini benimseyecektir. Örneğin; Amazon, kimlik doğrulama sürecinde müşterilerin çabalarını azaltmak için ödemeleri tek tıklamayla gerçekleştirilebilir şekilde tasarlamıştır.

- “Güvenlik”, işlemlerin ve müşterilerin detaylarının dahili ve harici dolandırıcılık ve benzeri suç amaçlı kullanımlardan korunması olarak tanımlanmaktadır. İnsanlar, kişisel bilgilerinin çalınabileceğinden korkarak çevrimiçi işlem yapmaktan ve ödeme yapmaktan korkabilmektedirler. Satış işlemlerinde insan faktörü olmadığı ve sanal ortamda yapıldığı için insanlar şüphe duymaktadırlar. Bu nedenle çevrimiçi satışların geleneksel satışlar kadar güvenli olmadığı kabul

edilmektedir. Kullanıcıların güvenlik endişeleri, elektronik ödeme yöntemlerinin benimsenmesini etkilemektedir.

- E-ödeme sistemlerinde “algılanan avantaj”, müşteriler tarafından işlemlerin herhangi bir zamanda, konumdan bağımsız olarak, herhangi bir yerde kolayca gerçekleştirilebildiğinde fark edilir. Geleneksel ödeme yöntemlerinde ödemeler hem zaman hem de mekân kısıtlaması nedeniyle müşterilere zorluk çıkarmaktadır. E-ödeme yöntemlerindeki bu avantaj kullanıcıların bu sistemi benimsemesi için motive edecektir. Algılanan avantaj ayrıca bir e-ödeme yöntemini benimsemek için tüketicinin algıladığı fayda ve kullanım kolaylığı ile de açıklanmaktadır. Algılanan faydaya katkı sağlayan e-ödemelerin avantajı işlemlerin minimum zaman ve maliyetle tamamlanmasını sağlamasıdır.

- “Algılanan risk”, müşterilerin e-ödemelere olan güvenini etkileyen bir diğer önemli faktördür. Müşterilerin yeni ödeme yöntemlerini benimsemesi için algılanan riskin eski ödeme yöntemlerinden daha büyük olmaması gerekmektedir. Kişisel bilgilerin ifşa edilmesinin bir sonucu olarak müşteriler ekonomik risk ve gizlilik riskiyle karşı karşıya kalabilmektedir. Bir müşteri çevrimiçi ödeme yapmayı seçerken dolandırıcılık, hırsızlık, bilgisayar korsanlığı, şifre çalma gibi riskleri göz önünde bulundurmaktadır. Bu nedenle çevrimiçi ödeme yapıp yapmama kararı algılanan riskten etkilenir (Özkan vd., 2010: 305-306).

Elektronik ticarete kullanılan ödeme araçlarının büyük bir bölümünü, bu amaç için geliştirilmemiş geleneksel ödeme araçlarının elektronik olarak kullanılması oluşturur. Elektronik ticarete entegre edilen geleneksel ödeme araçları ile yalnızca elektronik ticarete kullanılması için geliştirilen ödeme araçları arasındaki ayrımı fark etmek gereklidir. Geleneksel ödeme araçlarının elektronik ticaret ile oluşturulan yeni piyasaya uyumunda, ödeme araçlarının işleyişinde çok küçük bir değişiklik olmaktadır. Müşteriler tarafından geçmişten beri geleneksel ödeme araçlarının kullanılması, e-ticaret ortamında da kullanımını kolaylaştırmış ve yaygınlaştırmıştır. Oysa ikinci gruptakiler sadece e-ticaret için kullanılan ödeme araçları oldukları için toplumun bu araçları benimsemesi ve güvenle kullanması hem hukukun desteğine hem de bu araçların sağlayacağı ek faydalara bağlı olmaktadır. Banka kartları, hesaptan havaleler ve borçlandırma araçları (doğrudan borçlandırma ve çekler) internet ve kablosuz ağlar aracılığıyla yapılan e-ticaret ödemelerinde kullanılan geleneksel ödeme araçlarının başında gelmektedir. Elektronik ticaret işlemlerinde kullanılan geleneksel ödeme yöntemleri ve hizmetlerinin yanı sıra yalnızca e-ticaret ödemeleri için

geliştirilmiş yeni ödeme araçları ve bu araçlarla verilen hizmetler de mevcuttur. Bunlardan bazıları; elektronik para, ticari banka paraları, ticari banka paraları, aracılar aracılığıyla yapılan ödemeler, toplu ödemeler, mobil ödemeler olarak sayılabilir. Bilgi ve iletişim teknolojilerinin sağladığı olanakların kullanılması da her iki yöntemin ortak özelliği olarak belirtilebilir (Erdoğan, 2004: 81-82).

Elektronik ödeme, tüketicilere temel olarak kolaylık açısından fayda sağlamak ve işlem maliyetini düşürmek için tasarlanmıştır. Bu gelişmeler sırasıyla telekomünikasyon şirketleri ve bankacılık kurumları tarafından internet ve mobil bankacılık hizmetlerinin sunulmasını sağlamıştır (Teoh vd., 2013: 467).

1.4. ELEKTRONİK ÖDEME ARAÇLARI

Piyasada gerek online alışverişte gerekse geleneksel alışverişte tüketicilerce kullanılmakta olan başlıca ödeme araçları şöyledir:

1.4.1. Kredi Kartı

Kredi kartı, parasal bir kuruluş tarafından kart sahibine verilen kartın, kâğıt para kullanmadan internet üzerinden veya elektronik bir cihaz aracılığıyla ödeme yapmak için kullanılan bir sistemdir (Masihuddin vd., 2017: 4). İnternet üzerinden yapılan alışveriş işlemlerinde en sık tercih edilen elektronik ödeme şeklidir. Kredi kartı, bir bankadan kredi alıyormuş gibi davranır. Harcanılan miktar bankadan gelir. İçindeki bakiyenin her biri belirli bir süre içinde kapatılması gerekir. Harcanılan bu bakiyenin belirtilen süre içinde ödenmemesi durumunda, harcanılan tutarla birlikte faiz de yansır (Krishna ve Shanmugam, 2018: 132). Kredi kartının uluslararası alanda genel kabul görmüş olması, büyük çapta müşteri kitlesine hitap etmesi, geniş pazar alanına sahip olması, kredi kartı kullanıcısına para taşıma şartını ortadan kaldırması, belirli limitler dâhilinde nakde ihtiyaç duyulmadan mal ile hizmet alımına ve aynı zamanda nakit çekimine imkân sağladığı için tercih edilme nedenleri arasında gösterilebilir (Yüksel ve Bozkurt, 2015:177). Birçok ülkede kredi kartı veren kuruluşlar ya da ticari işletmeler hileli kullanımlardan veya işlemlerden dolayı sorumlu tutulduğundan kredi kartı kullanıcıları kredi kartı kullanımını güvenilir kabul

etmektedir. Buna istinaden kredi kartı bilgilerinin güvenliğini sağlamak için işlemler sırasında çeşitli şifreleme teknikleri kullanılmaktadır(Ekici, 2013: 92).

Kredi kartı, tüketiciye borç veren bir hesaptır, yani tüketicilerin krediyle mal veya hizmet satın almalarına izin verilir. Bir güven belirteci olan kredi kartı, bir satıcıdan kredi verme riskini kartı veren bankaya aktarır. Bu açıdan hem tüketiciler hem de tüccarlar bir bankaya kaydolmalıdır. Kredi kartı sisteminde kredi kartı çıkaran kart firmaları, kart kullanıcıları, kart kullanıcılarına hizmet sunanlar veya mal satanlar(tüccarlar) ve banka olarak dörtlü bir ilişkinin varlığından söz edilebilir. Tarafların arasındaki ilişkiler ve sözleşmeler birbirinden farklıdır (Aigbe ve Akpojaro, 2014: 11).

Kredi kartı ile ödeme şeklinde genellikle POS(Point of Sale veya Point of Service) yani kelime olarak satış veya servis noktası anlamına gelen cihazın kullanıldığı görülür. Mal veya hizmet satın almak isteyen kişi POS cihazına kredi kartını yerleştirerek ödemeyi gerçekleştirir. Kredi kartı POS cihazına yerleştirildiğinde, kartın içindeki bütün bilgiler okunarak alıcının bankasındaki hesabı arasında bağlantı kurulmuş olur. Bağlantının kurulmasıyla birlikte alıcının bankadaki hesabına ürün ve hizmetin maliyetinin satıcının hesabına ödendiği bilgisi gider. Satıcının hesabına para aktarımı ise kart şirketi ile üye iş yeri sahibi arasındaki sözleşmeye istinaden gerçekleşir (Yüksel ve Bozkurt, 2015: 177). POS, özel bir bilgisayar terminali olup satışla ilgili bütün bilgileri kredi kartını çıkaran banka bilgisayarına aktarmakta, kaybedilen, çalınan, sahte olarak düzenlenen ve çeşitli nedenlerle iptal edilen geçersiz kredi kartlarının denetimini yapmakta, işlemle ilgili olarak bankadan karşılık almaktadır. Kredi kartı firmaları, tüketicileri için bir dizi farklı işlem için geniş bir kullanıcı tabanı sağlayan geniş bir ağ kurmuş, ancak küçük işletmeler ve yüksek kredi kartı ücretleri nedeniyle küçük ödeme yapmak zorunda kalan müşteriler için daha az uygun bir yöntem olarak kabul edilmektedir (Bezhovski, 2016: 128).

Kredi kartlarının en önemli avantajlarından biri, anında ve her yerden çevrimiçi işlem yapabilmeleri için kullanımı kolaylığı/işlevselliğidir (Asokan vd., 2000: 2). Kullanıcıların kart kullanımı konusunda ek yazılım veya donanım satın almaları gerekmediği için kart sahibi olmak kolaydır. Kredi kartı kullanımı kimlik doğrulama prosedürü, bir ad, kredi kartı numarası ve son kullanma tarihinin sağlanmasıyla beraber kullanımı basittir (Bezhovski, 2016: 128). Kredi kartı geleneksel ödeme aracı

olarak kabul edilse de çevrimiçi olarak işlem gördüğünden elektronik ödeme sistemleri kategorisinde değerlendirilir.

Bir kart sahibi, tarayıcı aracılığıyla bir siteyi ziyaret eder. Satın alınacak ürünleri seçtikten sonra müşteri (çevrimiçi alışveriş yapan) bir ödeme talebi doldurarak kullanmak istediği kredi kartlarından seçim yapar ve müşteri ödeme talebini ödeme ağ geçidine (veya satıcının web sunucusuna) iletir. Ödeme ağ geçidinde alıcının bilgileri internetten satıcıya gönderilir. Satıcı, kart sahibinin finans kurumundan bir ödeme talebi yetkisi oluştur. Dijital imzası, işlem tanımlayıcısı ve ödeme talimatları şifrelenmiş talebe dâhil edilir ve şifresinin çözüldüğü, işlendiği ve doğrulandığı bir ödeme kartı işleme merkezine veya alıcı kuruluşun ödeme ağ geçidine iletilir. İşlem doğrulandıktan sonra, ödeme kartı işleme merkezi, yetkilendirme talebini finansal ağlar tarafından kullanılan biçime dönüştürür ve ardından onay için yetkilendirme işlemini, kart sahibinin bankasına (düzenleyici) iletir. Kartı veren banka, yetkilendirme talebine yanıt olarak ödeme ağ geçidine bir onay veya ret cevabı gönderir. Ödeme ağ geçidi bu yanıtı (yetkilendirme veya hata) satıcıya gönderir. Banka yetkilendirmeye onay verirse ödeme ağ geçidi dijital olarak imzalanmış şekilde bildirim gönderir. Daha sonra satıcı, ödeme ağ geçidinin dijital imzasını aldıktan sonra, müşteri işleminin onaylandığını bilerek malları kart sahibine gönderir. Satıcı, alıcı aracılığıyla ödeme ağ geçidi aracılığıyla ihraççıdan ödeme talep eder (Aigbe ve Akpojar, 2014: 11). Ancak bu durumda kredi kartı bilgilerinin üçüncü kişilerin eline geçme riski ortaya çıkar. Çünkü tüketicilerin işlem kayıtları kredi kartıyla izlenilebilmektedir. Bu nedenle internette gerçekleştirilen kredi kartı kullanımında en önemli sorunların başında kredi kartı bilgilerinin çalınması gelmektedir (Kim vd., 2010: 86). Söz konusu riskin önüne geçebilmek için bu sorunla ilgili birçok prosedür ve protokol geliştirilmiştir.

Kredi kartı bilgilerinin, üçüncü kişiler tarafından banka veya şirketlerin internet sitelerinden ele geçirilmesini önlemek için kullanılan protokollerin başında kredi kartı bilgilerinin şifrelenmesini içeren SET (Secure Electronic Transactions) ve SSL (Secure Socket Layer) protokolleri gelmektedir. Bu sayede alışveriş güvenliği kolaylıkla sağlanmaktadır. 1996 yılında kredi kartı şirketleri Visa ve MasterCard tarafından oluşturulan, güvenli elektronik işlem anlamında gelen SET protokolü, özellikle internet gibi güvenlik açığının oluşabileceği ağlarda kredi kartı bilgilerinin güvenliğini sağlamak için kullanılır. Günümüzde SET protokolünün yerini üç boyutlu (3D) güvenlik şeması (3D security scheme) sistemi almıştır. Banka, bu sistem

sayesinde kartın sahibinden kart şifresini isteyerek kimlik doğrulamasını gerçekleştirmektedir. Böylece şifreyi bilmeyen kişilerin işlem yapması engellenerek kart sahteciliğinin önüne geçilmiş olur. Bir diğer güvenlik protokolü ise güvenli giriş katmanı anlamına gelen SSL protokolüdür. Bu protokol; Opera, Google Chrome, Explorer gibi bir web tarayıcısının web sunucusuna internet üzerinden güvenli veri iletişimini gerçekleştirir. Eğer web tarayıcısında bir asma kilit resmi varsa SSL protokolünden söz etmek mümkündür. Bazı durumlarda ise adres çubuğunda asma kilit yeşil renkle birlikte görülür (Yüksel ve Bozkurt, 2015: 179-180). Bahsedilen bu sistemler, kullanıcıların kredi kartları aracılığıyla çevrimiçi alışveriş yaparken bir şifre oluşturmaya ve kullanmaya olanak tanımaktadır (Bezhovski, 2016: 129).

Türkiye’de kredi kartlarının kullanımı ise “Servis Turistik AŞ.” adlı firma aracılığıyla olmuştur. Yurtiçi Kart çıkartma yetkisini Amerika Birleşik Devletleri (ABD)’den alan firma, “Diners Club” adlı kredi kartlarını 1968 yılında piyasaya sunmuştur. Hemen ardından da “Amerikan Ekspres” kartları Türkiye’de kullanılmaya başlanmıştır. 1983 yılından itibaren Master Card ve Visa kredi kartlarının da ülkemizde sisteme girmesiyle, kredi kartları çok daha geniş kitleler tarafından benimsenip hızlı bir gelişme göstermeye başlamıştır (Kaya, 2009: 9-12). 1990 yılında ise Bankalararası Kart Merkezi (BKM), 13 kamu ve özel türk bankalarının ortaklığıyla kurulmuştur (Dündar ve Duramaz, 2014: 26).

1.4.2. Temassız Ödeme

Temassız ödeme, satıcı ile müşterilerin birbirleriyle fiziksel şekilde temasa geçmeden mal veya hizmet alımını mümkün hale getiren ödeme yöntemidir. (Eren, 2020: 109). Temassız ödeme uygulaması, tüketicilerin alışveriş anında hayatını kolaylaştırmak ve nakit para ile yapılan ödemeler sonucu oluşan zaman kayıplarını ortadan kaldırmak için geliştirilmiştir (Polasik vd., 2012: 12). Bu ödeme şeklinde kartların kart okuyucusuna dokunmasına gerek yoktur (Turban ve Brahm, 2000: 283).

Son dönemde yaşanan pandemi sebebiyle günümüzde tüketiciler tarafından kredi kartı, banka kartı ve akıllı telefon aracılığıyla en çok kullanılan yöntemlerden biri haline gelen temassız ödeme, POS makinelerinden çip veya manyetik şerit okuma ve şifre doğrulama işlevini ortadan kaldırarak, POS cihazı ile ödeme aracı arasında hiçbir şekilde dokunma olmadan yalnızca cihaza yaklaştırılarak işlemlerin çok daha hızlı, hijyenik ve uzun kuyruklar yaşanmadan ödeme yapılmasını sağlamıştır (Wang,

2008: 687). Temassız ödeme uygulamasında tüketiciler, düşük tutarlı işlemlerde harcamalarını nakit problemi yaşamaksızın uyumlu cihazlara kartını veya akıllı telefonunu yaklaştırarak ödemelerini saniyeler içinde gerçekleştirmektedir. Temassız ödeme, bireylere kullanım kolaylığı, zamandan tasarruf sağlamış ve bireylerin şifre hatırlama gereksinimini ortadan kaldırmıştır (Eren, 2020: 109). Temassız ödemeyi kabul eden iş yerlerinin POS cihazlarının üstünde ise temassız dalga işareti veya contactless (temassız) ifadesi bulunmaktadır (İyzico, 2020. Erişim Tarihi 30.03.2021).

1.4.3. Doğrudan Borçlandırma (Mail Order)

“Ödeyen kişi, hesap bilgilerini ödemenin yapılacağı bankaya veya ödeme yapılacak kişiye göndermekte ve ödeme alacaklı banka tarafından gelen istek üzerine kişinin hesabından havale yoluyla yapılmaktadır. Fatura, vergi, maaş, emeklilik aylıkları ve primleri ve periyodik ödemeler bazı ülkelerde doğrudan borçlandırma yöntemleri olarak kullanılmaktadır (Erdoğan, 2004: 82).”

1.4.4. Banka Kartı

Bir diğer adı debit kart olan banka kartı, ön ödemeli bir kart olan ATM kartı olarak da kullanılabilir (Krishna ve Shanmugam, 2018: 131). Bankalar, müşterilerine daha hızlı ve kolay hizmet verebilmek amacıyla koydukları ATM (Otomatik para çekme makinesi) makinelerinden müşterilerin para çekebilmeleri için banka kartlarını tasarlamışlardır. Müşteriler banka kartıyla kendilerinin belirlediği bir şifreyle ödeme yaptıklarında işlem otomatik olarak bankacılık sistemine ulaşır. Daha sonra sistem şifreyi kontrol eder ve kullanıcı hesabında sahip olduğu tutardan fazla olan miktarı işlemeyeceği için işlemin devam edip etmeyeceğini onaylar. Banka kartları müşterilere banka ile kredi ilişkisi oluşturmaz (Reisoğlu, 2004: 101). Kredi kartlarının aksine, banka kartları ile yapılan ödemeler, aracı hesap yerine doğrudan tüketicinin kişisel hesabından çekme imkânı sağlama özelliği ile kredi kartlarından ayrılmaktadır (Kim vd., 2010: 86). Borç ödemeleri için fiziki kart veya kart numarası üretmeye gerek kalmadan hesap numarasının verilmesi yeterlidir. Aynı zamanda banka kartı ödemelerinin genel güvenliğinin, bankalar tarafından talep edilen kapsamlı

kimlik gereksinimleri ile kredi kartı ödemelerine göre daha yüksektir. (Bezhovski, 2016).

Banka kartları, doğrudan borçlandırma sistemi gibi işlemektedir. Ancak kartın bizzat kendisi kullanıldığından daha fazla güvenlik olanakları sunması, doğrudan borçlandırma yönteminden farklı olmasına neden olmaktadır. Güvenlik olanakları sayesinde kart sahibi bilgisayara bağlı bir kart okuyucu aracılığıyla kendi kimliğini doğrulamakta ve onay vermektedir (Erdoğan, 2004: 83).

1.4.5. Elektronik Fon Transferi

Teknolojide yaşanan gelişmeler, bankacılık sektöründeki işlemlerin giderek artması ve elektronik bankacılık hizmetlerinin yaygınlaşmasıyla ortaya çıkan elektronik fon transfer sistemi, banka hesabında bulunan paraların elektronik ortamda ve tam zamanlı olarak diğer bir banka hesabına aktarılmasına olanak veren ve karşılıklı mutabakatı sağlayan 1960'ların sonlarından beri kullanılmakta olan bir sistemdir (Dündar ve Duramaz, 2014: 28). Elektronik fon transferi ve elektronik kontrol eş anlamlıdır. Kavramsal olarak, elektronik kontrol ve neredeyse tüm elektronik ödemeler alıcı, satıcı ve aracı olarak üç tarafı içermektedir. Alıcı, satıcı ile işlem başlatır ve satıcı ödeme talep eder. Alıcı daha sonra aracından elektronik biçimde bir ödeme sertifikası alır. Bu sertifika, alıcının aracındaki hesabına borç kaydeder. Alıcı daha sonra sertifikayı satıcıya verir ve satıcı sertifikayı aracıya verir. Sertifika, satıcının aracındaki hesabına kredi verir. İncelendiği zaman işlem geleneksel bir kontrol işlemi gibidir. Ancak elektronik olarak yürütüldüğünde, sertifika aracı tarafından belgelenen elektronik bir akıştır. Sertifikanın teslimi, sertifikanın devri ve hesapların borçlandırılması ve kredilendirilmesi kısa bir zamanda gerçekleşmektedir. Alıcı ve satıcı aynı aracıyı kullanmazsa, araçlar arasında genellikle ülkenin merkez bankası (yurtiçi işlemler için) veya üçüncü bir ülke (uluslararası işlemler için ve üçüncü ülkenin merkez bankası) aracılığıyla düzen ve uyumu sağlayan bazı standartlaşmış takas odası sistemi kullanılmaktadır. Elektronik kontrol yoluyla yapılan ödemeler geleneksel kontrol (kâğıt üzerinde kontrol) gibi nakit ve kâğıt olmadan yapılması bakımından çeşitli avantajlar sağlar (Panurach, 1996: 46):

Zamandan tasarruf: Hesap bakiyelerinin anlık olarak güncellenmesi, tüm finansal oyunculara daha fazla finansal esneklik sağlamaktadır. İşlemlerin bitirilmesi için bir takas süresi yoktur, bu da büyük tutarlı işlem durumlarında büyük maliyet

indirimleri ve daha fazla fırsata izin verirken, tüketicilere ve tasarruf sahiplerine büyük bir mali özgürlük ve zamandan tasarruf sağlamaktadır.

Geri dönen kontrol yok: Eş zamanlı olarak, onay alınması ve hesapların borçlandırılması ve kredilendirilmesi, onu destekleyecek fonlar olmadan onay yapılmamasını sağlar. Bu tür ödemeler, sertifika verilmeden önce hesap durumunun otomatik olarak onaylanması yoluyla yapılabilir.

Esneklik: Elektronik fon transferi, dünya çapında çeşitli şekillerde kullanılan son derece geniş ve genel bir alandır. İşlemler, ATM ağları aracılığıyla perakende düzeyinde düşük değerli para çekme işlemlerinden, şu anda en büyük New York ticari bankalarından bazıları tarafından kurulan uluslararası bir ödeme takas sistemi olan Clearing House Bankalararası Ödemeler Sistemi (CHIPS) gibi uluslararası büyük ciro lu ağlara kadar uzanmaktadır.

İnternet üzerinden gerçekleştirilen kredi kartı ödemeleri, ATM ağı üzerinden üniversite ücretlerinin ödenmesi ve POS cihazıyla yapılan ödemeler kâğıt kullanılmadan ve elektronik ortamda gerçekleştiği için elektronik fon transfer modeli olarak görülebilir. İnternet ortamında EFT işlemini gerçekleştirebilmek için banka hesabı bulunan kişinin bankaya bu konuda talimat vermiş olması gerekir ya da bilgisayarı ile bu işlemi gerçekleştirir (Özbaş, 2019: 89).

1.4.6. Elektronik Çek

Elektronik çek, sanal çek biçiminde de nitelendirilen ve EFT prensibiyle çalışan ödeme yöntemidir. Elektronik ticaret yapan sitelerin, ödemeleri çek şeklinde kabul etmelerin, mümkün kılan bir sistemdir (Ekici, 2013: 93). Kâğıt çekte bulunan bilgileri taşır. Bu anlamda elektronik çek, kâğıt çek ile neredeyse aynı özelliklere sahiptir. Elektronik çek, elektronik çeki ödeyenin hesap numarasını, alıcı adını, çek tutarını ve ödeme tarihini tanımlamak için rastgele büyük ve benzersiz bir numara olan çek numarası gibi önemli alanlara sahiptir (Yahid vd., 2013: 88). Kâğıt ve elektronik çekler arasındaki tek fark, internet gibi bilgisayar ağları aracılığıyla aktarılan ödeme aracının fiziki olarak basılmadan aynı nitelik ve hakları taşıyacak şekilde elektronik ortamda kayıtlanarak izlenmesidir (AL-Maaitah vd., 2011: 394). Çeki düzenleyen kişi, elektronik ortamda çeki doldurduktan sonra elektronik imza ile imzalar ve internet aracılığıyla alacaklıya çeki elektronik ortamda sunar. Alacaklı bu çeki yine internet ortamında kendi bankasına göndererek kendi bankasının borçlunun bankası ile irtibata

geçmesini sağlar. Borçlunun hesabı çek bedelini ödemeye yeterli gelirse alacaklının bankasına çekin değeri kadar para aktarılır ve alacaklının hesabına aynı miktarda değer artışı kaydedilir (Yüksel ve Bozkurt, 2015: 181). Bu işlemler takas merkezi olarak tanımlanan finansal kurumlar aracılığıyla da yürütülebilir (Ekici, 2013: 93).

Elektronik çek, normal çekten farklı olarak ödeme emri elektronik form aracılığıyla verilmektedir. Islak imzanın olmaması, yasal geçerlilik bakımından bu ödeme aracının farklı sınıflandırılmasına neden olmaktadır. Elektronik çek, PIN ve dijital imza ile korunur. Bu, ödeme işlemi sırasında kullanıcıları doğrulamak için iki faktörlü bir kimlik doğrulama mekanizmasından yararlandığı anlamına gelmektedir. Bu kimlik doğrulama mekanizması, bir kullanıcının kimliğini iki veri ögesiyle kanıtlamasını gerektirmektedir (Aigbe ve Akpojar, 2014: 11). Elektronik çek altyapısını oluşturan sistemlerin (sertifika otoriteleri, hukuk kuralları vb.) finans sektörü tarafından kabul görmesi daha yaygın kullanımı için gereklidir (Erdoğan, 2004: 83).

1.4.7. Ticari Banka Paraları

Çevrimiçi kişisel ödemeler olarak da adlandırılan bu sistemler banka hesapları gibi işlemektedir. Bu ödeme yönteminde müşteri, ödeme hizmet sağlayıcısına ayrılmış hesaplar açmakta ve bu hesaplardaki fonlar internet üzerinde yapılan ödemelerde kullanılmaktadır. Bu ödeme şeklindeki en önemli yenilik elektronik posta ile birlikte servis sağlayıcıya ait web sitesinin kullanıcılar ve hizmet sağlayıcı arasında bir iletişim platformu olarak kullanılmasıdır. Bir diğer yenilik de, yeni hesap açmadaki kolaylık olarak görülmesidir (Erdoğan, 2004: 85).

1.4.8. Elektronik Cüzdan

Elektronik cüzdanlar, internet ortamında alışveriş yaparken kullanabilmek amacıyla geliştirilmiş, kredi kartı numaraları, e-nakit, sahibinin kimliği ve adres gibi diğer ilgili bilgileri veya o sırada gerekli olan diğer bilgileri saklamak için kullanılan yazılım türleridir (Krishna ve Shanmugam, 2018: 130). Alışveriş yapabilmek gerekli bilgiler bir defa olmak üzere e-cüzdan yazılımları kullanıcı bilgisayarına yüklendikten

sonra tanımlanır. Bu sayede internet ortamında gereken işlemler için bilgilerin tekrarlanmasına ihtiyaç duyulmaz. Her seferinde bilgilerin tekrar girilmesine zaman kazandırır. Kullanıcı, e-cüzdanı kişisel bilgisayarından kullanabileceği gibi üretici firmanın internet sitesinden de işlemlerini yürütebilir (Aytekin ve Yücel, 2017: 98).

1.4.9. Sanal Kart

Sanal kart, basılı olmayan, fiziki bir yapısı olmayan ve internet üzerinden güvenli alışveriş yapılmasına imkân tanıyan bir ödeme aracıdır (Kalyoncuoğlu, 2018: 198). Kart sahibinin üzerinde taşınması gereken bir kart değildir. Bu kartlar aracılığıyla yalnızca kart numarası, son kullanma tarihi ve güvenlik kodu ile işlem gerçekleştirilir. Sanal kart bilgileri, asıl kart bilgilerinden farklılık gösterir. Bu durum hiçbir şekilde asıl kart bilgilerinin internette paylaşılmasını sağlar. Kart kullanıcısının, kredi kartları veya banka hesapları limitlerine bağlı olarak oluşturulduğu için sanal kartın bir limiti yoktur (Konuk ve Yıldırım, 2012: 86). Ek olarak sanal kartların yıllık üyelik ücreti, sanal kart oluşturma ve kullanma ücreti bulunmamaktadır. Aynı zamanda sanal kart üzerinden de taksit yapma imkânı bulunur (Bankacılık Düzenleme ve Denetleme Kurulu (BDDK), Erişim Tarihi: 30 Mart 2021). Online alışverişler dışında kullanılması, fiziksel bir kart olmadığı için mümkün değildir. Dolayısıyla kayıp veya çalıntı riski taşımazlar. Müşterilerin yüklediği kadar bulunan sanal kart limiti, online alışveriş sonrası kalan tutar tekrar hesaba aktararak sıfırlanabilir. Böylece güvenlik konusunda olası bilgi hırsızlığının önüne geçilebilir (Kalyoncuoğlu, 2018: 198).

1.4.10. Akıllı Kart

Akıllı kartlar, üzerinde veya içinde mikroçip olan genellikle banka tarafından verilen kişiye özel şifrelenmiş seri numarası ile onaylı çipli kart olarak da adlandırılan yüklenmiş, kredi kartı boyutunda, plastik bir karttır (Şeker, 2011: 65; Turban ve Brahm, 2000: 282). Farklı tanımlama araçları için kullanılan plastik ve manyetik kartları içeriğindeki çip nedeniyle birden çok hizmete, ağa ve internete erişebilen tek bir kartta birleştirir. Hem kişisel hem de finansal gibi tüm bilgileri saklayabilir (Krishna ve Shanmugam, 2018: 131). Bu nedenle çip, kart sayısını azaltır ve bir kartı birden çok hesaba erişim anahtarı yapar. Bir ödeme aracı olarak akıllı kart sistemi

birden fazla işlev veya uygulama için kullanılmasına olanak tanıyan işlem gücüne sahiptir. Para, akıllı karta elektronik olarak kopyalanır (Aigbe ve Akpojar, 2014: 11). Akıllı kart uygulamaları sadece finans alanında değil ulaşım, telekomünikasyon, eğitim ve sağlık gibi sektörlerde de karşımıza çıkmaktadır. Son dönemlerde akıllı kimlik kartı olarak adlandırılan yeni nüfus cüzdanları da buna örnek verilebilir (Yüksel ve Bozkurt, 2015: 182). Bununla beraber içerdiği çip sayesinde kopyalanan bilgilerin elde edilmesine, çoğaltılmasına vb. haksız müdahalelere karşı koruyucu özelliğe sahiptir. Akıllı kartlar, e-cüzdan olarak kullanırken para, kartın üzerindeki çipe yüklendiği için kart okuyucuları internet bağlantısı olmaksızın çalışabilmektedir. Karttaki çip, para transfer işlemlerinde dijital imza yaratarak kullanıcıya özel olmaktadır. Akıllı kart teknolojisi 1993 yılında MasterCard, Visa ve Euro Pay ortaklığında debit kart ve kredi kartına bağlanmıştır (Kaya, 2009: 84).

1.4.11. Mobil Ödeme

İletişim teknolojilerinin hızla yükselmesi nedeniyle zamandan ve konumdan bağımsız olan mobil ödeme sistemi, popüler bir yöntem olarak karşımıza çıkmaktadır (Ting vd., 2016: 369). Bu yöntem, cep telefonlarının çok büyük kullanıcı tabanı nedeniyle çevrimiçi satıcılar için çekici bir uygulama haline gelmiştir. Kullanıcıların ödeme yapmak için mobil ödeme yöntemini benimsemelerinin en önemli yönü, sistemlerin tüketicilerin günlük yaşamlarına kolayca entegre edilebilecekleri esnekliğidir. Yapılan çalışmalarda; sinema biletleri, mobil oyunlar ve çevrimiçi içerik satın almak için yapılan küçük ödemeler için daha çok mobil ödeme yöntemini kullandıkları belirlenmiştir.

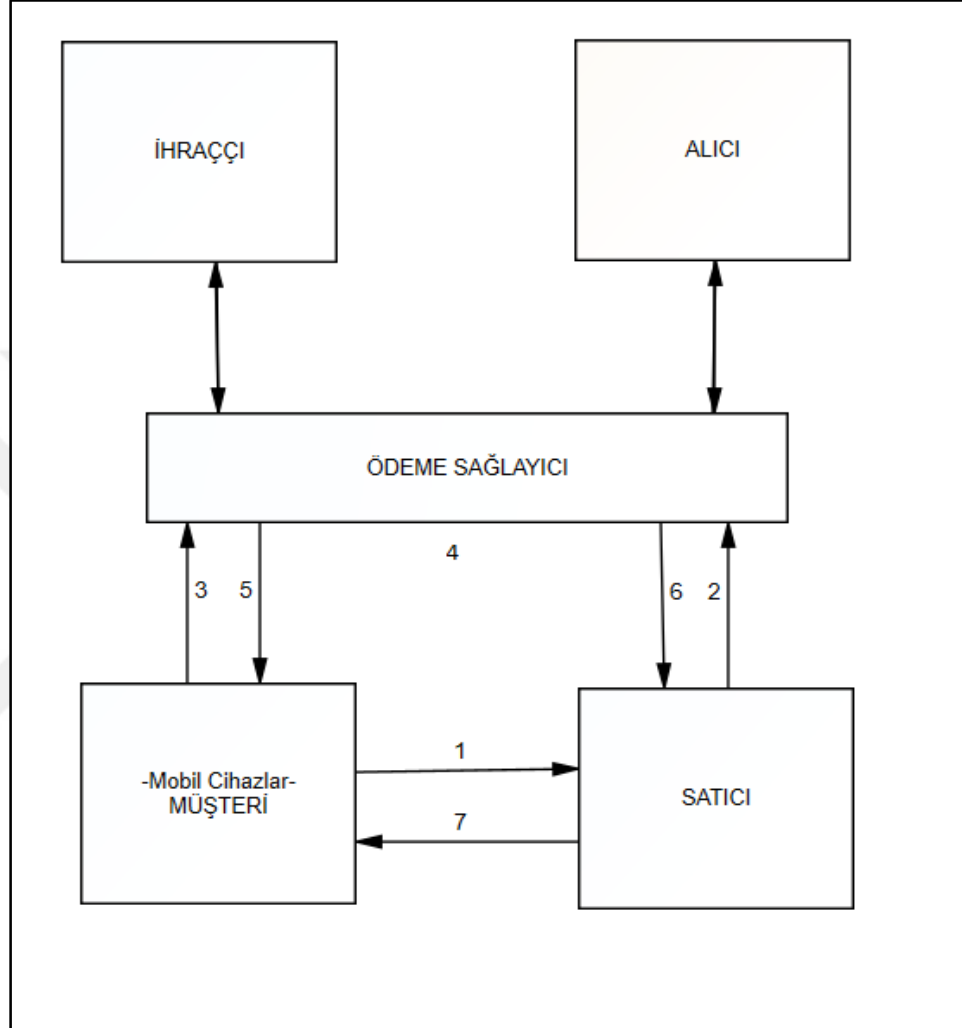
Mobil ödeme, alışveriş yaparken cep telefonu operatörlerinin anlaşmalı üye iş yerlerindeki yerlere cep telefonuna gelen mesajı veya cep telefon numarasını verme sonucunda, yapılan alışverişin cep telefonu faturasına yansıma ve lira bakiyesinden düşmesiyle gerçekleşen ödeme aracıdır (Dündar ve Duramaz, 2014: 31). Mobil ödeme ile ödeme yapabilmek için işlemin bir SMS aracılığıyla başlatılması ya da tamamlanabilmesi için bir onay SMS'i gönderilmesi gerekir. Dolayısıyla işlemin gerçekleşmesi ödeme miktarının onaylanmasına bağlıdır. Mobil telefon aracılığıyla ödeme yapılmasında kaynaklı m-ödeme olarak da adlandırılır. Mobil ödeme yöntemi ile cep telefonuna inen bir uygulama sayesinde nakit para veya kredi kartı olmaksızın mal veya hizmet alımının hızlı ve güvenilir bir şekilde yapılmasına imkân verir (Ooi

ve Tan, 2016: 36). Türkiye’de cep telefonlarının kredi kartı olarak da kullanabileceği mobil ödeme sistemine Garanti Bankası ve Turkcell’in ortaklığı sonucunda ortaya çıkan Paycell uygulamasını örnek vermek mümkündür (Kaya, 2009: 158). Mobil telefonların kişiye özel olması, kolay ve sürekli taşınabilmesi, işlem ücreti azaltıcı özellikleri nedeniyle kişisel bilgisayarlara oranla ödeme aracı olarak kullanım oranı daha fazladır. Mobil ödeme hizmetinin kullanılması yalnızca işlemin toplam maliyetini azaltmakla kalmaz, aynı zamanda daha iyi bir ödeme güvenliği de sağlar (Liebana-Cabanillas, 2017: 27). Mobil ödeme yönteminin geliştirilmesiyle birlikte çeşitli yerlerde hızlı, kolay ve güvenli bir ödeme yöntemi sunan giyilebilir teknolojileriyle de popüler hale gelmeye başlamıştır. Giyilebilir ödeme teknolojisi akıllı saatler, yüzükler, bilek bantları ve bir dizi Android ve İos akıllı telefon uygulamasını içerir (Bezhovski, 2016: 130). Bununla birlikte mobil ödeme sistemleri, gizlilik sorunları ve uluslararası ödemeleri karşılayamamaları da dâhil olmak üzere birçok nedenden dolayı önemli bir tüketici tabanı elde etmekte bazı zorluklarla karşılaşmıştır. Bu açıdan mobil ödeme pazarının geleceği için cep telefonu üreticileri, telekomünikasyon şirketleri ve ödeme endüstrisi, çevrimiçi ödeme işlemleri için en güvenli ortamı sağlayan bir platform geliştirebilmeleri için birbirleriyle işbirliği yapmalıdır. Mobil ödeme sistemlerinin güvenliğini ve verimliliğini arttırmak için biyometrik kimlik doğrulama gibi en son teknolojiler kullanılmalıdır. Bu teknolojiler ilerledikçe ve pazar tabanı genişledikçe, mobil ödemelerin benimsenmesinin önündeki tüm engellerin ortadan kalkacağı öngörülmektedir (Hoofnagle vd., 2012: 5).

Bir m-ödeme sisteminin ana varlıkları ve bir m-ödeme işlemi sırasındaki etkileşimleri Şekil 4’te gösterilmektedir. Genel olarak, bir m-ödeme sistemi müşteri, tüccar, tüccarın finans kurumu ve müşterinin finans kurumu olarak dört ana varlıktan oluşur. Bu varlıklar, m-ödeme gerçekleşirken aşağıdaki sırada işlemlerini tamamlarlar (Isaac ve Zeadally, 2014: 37):

1. Müşteri, mobil cihaz ile satıcıya ödeme yapma talebini iletir.
2. Satıcı, müşteriden istenen tutarı hesabına yatırılmasını ister.
3. Müşteri, paranın hesabından düşürülmesini talep eder.
4. Ödeme takası gerçekleşir
5. Müşterinin talebinin onaylandığına veya reddedildiğine dair bildirim iletilir.
6. Satıcının talebine ilişkin alındı makbuzu oluşturulur.
7. Mal teslimatını onaylamak için ödeme makbuzu verilir.

Şekil 4: Bir Mobil Ödeme Sisteminin Tipik Varlıkları ve Mobil Ödeme İşlemi Sırasında Etkileşimleri



Kaynak: Isaac ve Zeadally, 2014: 38.

1.4.12. Pay Pal

PayPal, e-posta adresi bulunan kişilerin kredi kartıyla ya da kredi kartı olmadan güvenli bir biçimde para gönderip alabilmesine imkân veren bir ödeme şekli seçeneğidir (Erden, 2014: 61). E-posta adresi sisteme kaydedilerek üyelik işlemleri tamamlandığında PayPal tarafından sanal cüzdan açılır. Oluşturulan sanal cüzdanı kullanabilmek için öncelikle bir kredi kartı veya debit kartı(banka kartı, ATM kartı)nın PayPal hesabına kaydedilmesi gerekir. Kartlardan birinin sisteme kaydedilmesiyle

birlikte hesap aktif hale getirildikten sonra e-posta adresiyle giriş yapılarak PayPal üyesi olan kişi veya şirkete ödeme yapılabilir (Gökgül, 2014: 58-59). PayPal, ödeme yapabilmek için çeşitli alternatifler geliştirmiştir. PayPal üyeleri, www.paypal.com adresinden e-posta adresi bilinen herhangi bir kullanıcıya para gönderimini gerçekleştirebilir. Eğer para gönderilen kişi bir PayPal üyesi değilse gönderilen iletide kişiye nasıl üye olacağını ve hesabındaki parayı nasıl alabileceğine dair bilgilere de yer verilir. PayPal kullanıcıları, PayPal ödeme sistemini destekleyen bir e-ticaret sitesinden alışverişlerini tamamlamak istediklerinde PayPal ödeme seçeneğine tıkladıklarında PayPal hesaplarına ait e-posta adresi ve şifrelerini girerek ödeme işlemini gerçekleştirebilirler. Kullanıcılar, PayPal hesabı açarken kart bilgilerini sadece bir kez sisteme girerler. Daha sonra PayPal ile yaptıkları alışverişlerde kart bilgilerini tekrar sisteme girmeksizin PayPal 'da kayıtlı olan e-posta adresleri ile şifrelerini kullanarak hızlı ve kolay bir şekilde ödemelerini gerçekleştirirler. Ödeme yaparken her seferinde kart bilgilerinin siteye yüklenmesini önlemesi PayPal sisteminin en avantajlı yönüdür. Bu sayede kredi kartı bilgileri gizli tutulur, hesap verilerinin paylaşılması konusunda endişelenme ortadan kalkar (Niranjanamurthy, 2014: 673).

1.4.13. BKM Ekspres

BKM (Türkiye Bankalararası Kart Merkezi), kart ödemeleri açısından güçlü altyapıya ve yenilikçi ürünlere sahip 13 kamu ve özel Türk bankasının sahip olduğu Türkiye'nin iç bankalar arası takas ve değişim kuruluşudur. “Nakitsiz Toplum” planının bir parçası olarak BKM, 2012 yılında dünyanın ilk ulusal ağ geçidi BKM Expressi tanıtmıştır (Kayalıderen ve Çetiner, 2018: 73).

BKM Express, internet ortamında alışveriş yaparken müşterilerin kart bilgilerini işyerleri ile paylaşmadan işlem yapılmasını sağlayan bir ödeme sistemi olarak tanımlanır. BKM Ekspres sistemi üzerinden internette alışveriş yapabilmek için öncelikle BKM Ekspres sitemine üye olunması ve yalnızca bir defalık kart bilgilerinin girilmesi gereklidir. Böylece internette yapılan alışverişlerde her defasında kart bilgilerinin girilmesi sorunu ortadan kaldırılır, kart taşımaya gerek kalmadan hızlı işlem yapılır, müşterinin oluşturacağı kişisel şifresi ile alışveriş güvenli tamamlanır ve taksit imkânı sağlanır. İşlem dört aşamadan oluşur. İşyerinin ödeme sayfasında bulunan “BKM Ekspres İle Öde” seçeneği seçildikten sonra açılan BKM

Express sayfasına üye girişi yapılır. Ardından daha önce sisteme kaydedilen ödeme yapılacak kart seçilerek taksit seçenekleri belirlenir. Son aşama olarak da bankanın sms ile gönderilen doğrulama kodunu ekrana girerek alışveriş tamamlanır (Bankalararası Kart Merkezi, 2020. Erişim Tarihi 3.04.2020). Yurtdışında kullanılmakta olan PayPal sisteminin ülkemizdeki örneği olarak da gösterilebilir (Dündar ve Duramaz, 2014: 33).

1.4.14. Türk Ödeme Yöntemi (TROY)

Troy, Türkçe kelimeler Türkiye (TR), Ödeme ve Yöntem (Y)kelimelerin kısaltmasıdır. Troy, kartlı ödemeler sektöründe yaşanan artışla birlikte 2014 yılında yerli bir ödeme yöntemi hazırlamaya karar verilerek oluşturulan bir yöntemdir. 2015 yılının ekim ayında BKM iş birliğiyle Türkiye'nin ilk ve tek yerli ödeme yöntemi olan TROY kartın çıkarılmasında Türkiye'nin yurtiçi işlemlerin çok fazla gerçekleştiği bir ülke olması, sektörün kartlı ödeme konusunda iyi bir altyapı ve bilgi birikimine sahip olması ve sektörde yerel bir ödeme aracına ihtiyaç duyulması etkin bir rol oynamıştır. Kredi kartı, banka kartı ve ön ödemeli kartların sağ alt köşesinde milli ve yerli ödeme yöntemi olarak piyasaya sunulmuştur (Bankalararası Kart Merkezi, 2018b. Erişim Tarihi 3.04.2020).

1.4.15. Elektronik Para (Kripto Para)

Elektronik ödeme yöntemlerinin gelişmesiyle birlikte yeniliklerin hızla devam etmesi sonucunda elektronik para olgusu ortaya çıkmıştır (Özbaş, 2019: 90-91). Elektronik para (e-para), üreticisi dışındaki işletmelere yapılacak ödemelerde kullanılmak üzere önceden bedeli ödenerek elektronik ortamda depolanan parasal bir değer olarak tanımlanabilir (Abrazhevich, 2001: 87). Elektronik para, mali bir değeri olan elektronik verilerin çip karta veya bilgisayara kopyalanması sonucu oluşan sanal ödeme yöntemidir (Şeker, 2011: 67-68). Diğer bir ifade ile elektronik para, internet ortamında para transferini mümkün kılan ödeme yöntemine verilen bir addır (Ekici, 2013: 94). Elektronik para, benzersiz bir kimlik numarasının belirli bir miktar para ile ilişkilendirildiği bir ödeme yöntemidir. Elektronik paraya genellikle e-para, kripto para, sanal para ya da siber para da denmektedir. Bu yöntem, mal ve hizmetlerin

internet alımlarında kredi kartlarının kullanımına alternatif olarak geliştirilmiştir. Banka hesapları kullanımı, e-paranın aracı olarak kullanıldığı ödemelerde gerekli değildir(Erdoğdu, 2004: 84). Bu ödeme sistemini kullanmak için müşteriler, satıcı şirketten elektronik dijital para satın alırlar. Nakit daha sonra bilgisayarlar veya diğer telekomünikasyon kanalları aracılığıyla transfer edilebilmektedir (Kim vd., 2010: 85). Dolayısıyla elektronik paraları akıllı kartlarda veya kişisel bilgisayar sürücülerinde saklanan ve internetten alışveriş yapmaya imkân veren ve kullandıkça hesapta bulunan bakiyeyi eksiltten bir sistem olarak tanımlayabilmek mümkündür (Özbaş, 2019: 91).

Elektronik paranın kullanıcılar tarafından nakit para gibi benimsenmesi için aşağıdaki koşulları sağlaması gerekir (Ekici, 2013: 94-95):

- Kullanıcı Memnuniyeti: Ödemelerin özel bir bilgiye sahip olmaksızın kolaylıkla yapılabilmesi gerekir.
- Çevrimdışı İşleyiş: Para kullanılmak istendiğinde herhangi bir bilgisayar bağlantısı kurmaya gerek olmamalıdır.
- Güvenlik: Ödeme gerçekleştirirken veya ödemeyi kabul ederken üçüncü kişilerin müdahalelerine karşı güvenli olması ve gerekli önlemlerin alınması gerekir.
- Güvenilirlik/İşlemin Takip Edilememesi: Nakit parada olduğu gibi işlemler yapılırken hiç kimsenin kimin hangi para birimini ne zaman ve nerede harcadığını tespit edememelidir. İşlemlerin güvenilirliği sağlanmalıdır.
- Bölünebilirlik: Para, ihtiyaç duyulduğu zaman en küçük değer birimlerine ayrılabilmesi gerekir.

Elektronik para, nakit para ve kredi ile banka kartının avantajlarını içinde barındırmaktadır. Gün içinde yapılan işlemlerden doğabilecek herhangi bir gecikme veya hatalı işlemlerde ortaya çıkabilecek finansal riskleri azaltması ya da ortadan kaldırması en önemli avantajları arasında sayılabilir. Ayrıca çeşitli ödeme seçenekleri sunarak ödemenin yüz yüze gerçekleşme zorunluluğunu ortadan kaldırması ve bu sayede de kişilerin daha çok miktarda alım yapması elektronik paranın bir diğer avantajı olarak gösterilebilir. Elektronik para aynı zamanda ödeme aracı olarak e-parayı kabul eden kuruluşlara da birçok avantaj sağlamaktadır. Buna göre kişiler ödemeyi gerçekleştirirken e-para sayesinde zamanında işlemlerini yaptıklarından kuruluşlar da alacaklarını gecikmeye düşmeksizin kolay tahsil edebilmektedir.

Dolayısıyla kuruluşların vergi, sigorta ödemeleri gibi yasal yükümlülüklerini yerine getirmede kolaylık sağlamaktadır. Bu sayede zamanında bu işlemlerin yapılmasına katkıda bulunur. Kullanım süresi açısından da e-para diğer ödeme yöntemlerine göre daha uzun ömürlüdür. Aynı zamanda para taşıma zorunluluğunu ortadan kaldırır. Böylece nakit paranın kirlenmesi ve belirli aralıklarla yeniden basılmasından kaynaklı maliyeti ortadan kaldırmaktadır (Öztürk ve Koç, 2006: 232-233; Çağlar, 2007: 182).

Elektronik paranın avantajlarının yanı sıra dezavantajları da bulunmaktadır. Bunlardan en önemlisi her para sisteminde olduğu gibi güvenlik riski sorunudur. Özellikle diğer para sistemlerinden ayıran en önemli güvenlik sorunu teknoloji ağırlıklı güvenlik sorunlarıdır. Paranın çalınması, kopyalanması gibi risklere karşı diğer ödeme yöntemlerinde olduğu gibi elektronik ödeme yöntemlerinde de birçok güvenlik önlemlerinin alındığını görmek mümkündür. Nitekim bilişim, elektronik ve şifreleme gibi teknolojik gelişmeler güvenilirliği arttırmada önemli rol almaktadır (Çağlar, 2007: 182).

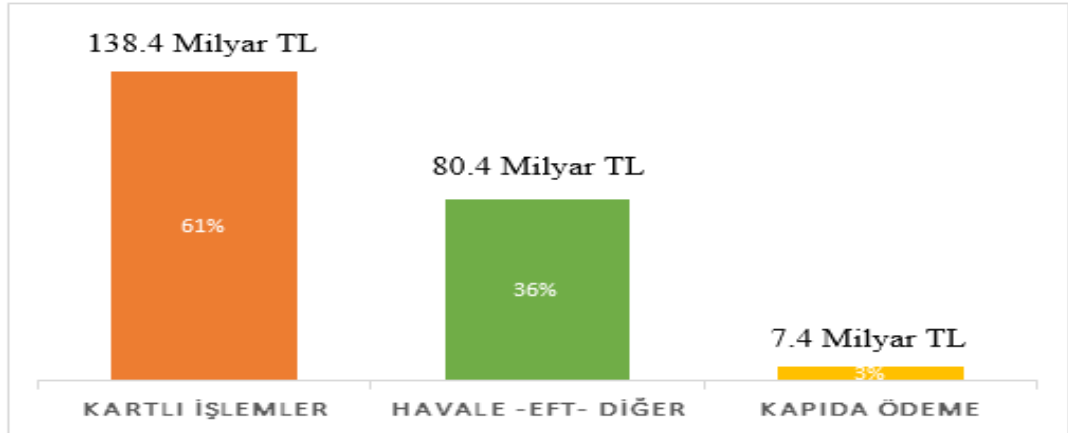
Elektronik para, bir diğer adıyla sanal para fikri 2009 yılında Satoshi Nakamoto isimli kimliği henüz bilinmeyen kişi ya da kuruluş tarafından “Bitcoin” para birimi kavramı dile getirilmiştir. Bu sanal para birimi için “ dijital imzalardan oluşan bir zincir” tanımı kullanılmıştır (Nakamoto, 2008). Bitcoin, üçüncü bir aracı kişi veya kuruma gerek kalmadan, elektronik para transferini mümkün kılan dijital bir para birimidir. Bununla birlikte aracı kuruluşların kaldırılması hem işlemlerin gönderi ile alıcı arasında gerçekleşmesini sağlayacak hem de aracılardan kaynaklı işlem maliyetlerini de düşürecektir (Bilir ve Çay, 2016: 22-24; Avunduk ve Aşan, 2018: 370-372). Üretilen ve satın alınan bitcoinler dijital cüzdanlarda tutulmaktadır. Dolar ve Euro gibi para birimlerden farklı olarak herhangi bir kalıp üzerine basılamazlar. Bilgisayarların matematiksel problemleri çözen bir yazılım aracılığıyla milyonlarca kişi tarafından elektronik ortamda basılmaktadır. Teknolojinin hızla gelişmesini sürdürmesiyle beraber bitcoinden ilham alınarak farklı elektronik para birimlerinin oluştuğunu görmek de mümkündür. Ethereum, Ripple ve Litecoin de kullanılan diğer para birimleri olarak gösterilebilir (Aytekin ve Yücel, 2017: 98-99). Bahsedilen sanal para birimlerinin tümü devletler ile bağlantısı olmayan kişiler, örgüt ya da şirketler tarafından üretilir ve normal para işleyişi gibi banka hesabında da tutulması gerekli değildir. Merkezi bir otoritenin onayı olmadan internet üzerinden haka açık işlem yapılmasını sağlar (Rehman vd., 2019: 1). Ayrıca merkez bankası gibi para

birimlerinin kontrolünü elinde bulunduran bir kurumu sanal para ortamında görmemiz mümkün değildir (Bilir ve Çay, 2016: 22-24).

Görüldüğü gibi tüketicilerin ve işletmelerin nasıl ödeme yapacaklarına ve hangi ödeme türlerini kabul edeceklerine dair seçenekleri vardır. Farklı ödeme biçimleri, ödeyen ve alacaklıya farklı düzeylerde maliyet ve fayda getirir. Ödemeler teknolojisindeki devam eden evrim, işletmeler için olduğu kadar kamu politikası konuları için de ilginç etik soruları gündeme getirmektedir. Ödeme yöntemlerinin kullanıcıları, seçimlerinin etik sonuçlarını dikkate almalıdır (Angel ve McCabe, 2014: 610).

T.C. Ticaret Bakanlığı (2021) tarafından yapılan çalışmalarda pandemi sonrası e-ticaret işlemlerinin artışıyla birlikte ödeme yöntemleri arasında karşılaştırma yapıldığında 2020 verilerine göre e-ticaret hacminde en çok pay alan yöntemin kartlı işlemler olduğu belirtilmiştir (%61). Havale- eft ve diğer işlemler kartlı işlemten sonra en çok tercih edilen yöntem olduğu belirtilip (%36), kapıda ödeme (%3) en az tercih edilen yöntem olarak tespit edilmiştir. 2020 yılının ödeme yöntemlerine göre e-ticaret hacimleri Grafik 4'teki gibidir (E-Ticaret Bilgi Platformu, 2021. Erişim Tarihi 08.05.2021):

Grafik 4: Ödeme Yöntemleri İtibariyle 2020 E-Ticaret Hacmi



Kaynak: E-Ticaret Bilgi Platformu, 2021. Erişim Tarihi 08.05.2021.

1.5. ELEKTRONİK ÖDEME YÖNTEMLERİNİN SINIRLAMALARI

E-ticaret bağlamında elektronik ödeme yöntemlerinin çeşitli sınırlamaları vardır. Aşağıdaki gibi sıralamak mümkündür (AL-Maaitah, M. ve Shatat, A., 2011: 394-395; AL-Maaitah, 2015: 824-825):

Kullanılabilirlik Eksikliği: İnternet için erişilebilir ödeme yöntemleri, son kullanıcının büyük miktarda bilgi sunmasına veya karmaşık ayrıntılı internet sitesi ara yüzlerini kullanarak ödeme yapmasına ihtiyaç duyar. Örneğin, bir internet sitesi aracılığıyla yapılan kredi kartı ödemeleri, ödeme yapmanın en kolay yolu değildir. Çünkü bunlar bir web formuna çok miktarda kişisel veri ve iletişim bilgileri girmeyi gerektirir.

Güvenlik Eksikliği: İnternet için sunulan ödeme yöntemleri, para ve kişisel bilgileri çalmak için kolay bir hedeftir. Tüketiciler, kredi kartı veya ödeme hesabı ayrıntılarını ve diğer kişisel bilgilerini çevrimiçi olarak vermek zorundadır. Bu veriler bazen güvenli olmayan bir şekilde, Güvenli Yuva Katmanı gibi güvenli işlem mekanizmalarının kullanılmasına rağmen gerçekleşir. Bu ayrıntıların posta yoluyla veya telefonla sağlanması da güvenlik risklerini beraberinde getirir.

Güven Eksikliği: Tüketiciler; sahtekârlık, kötüye kullanım veya düşük güvenilirlik geçmişine sahip sunulan yöntemlere karşı uzun bir süredir güvenmeme eğilimindedir. Mevcut durumda, internet ödemeleri için kredi kartları gibi mevcut ödeme yöntemlerini kullanırken müşteriler tarafından para kaybı oldukça olasıdır. Potansiyel müşteriler genellikle bir ödeme hizmetine güvenmemelerinin ve bu nedenle internet siparişleri vermemelerinin ana nedeni olarak bu riski belirtmektedir.

Uygulanabilirlik Eksikliği: Bazı internet siteleri belirli bir ödeme yöntemini desteklemez, bu nedenle müşterinin ödeme kabiliyetini sınırlar. Kredi kartları yalnızca ilgili kredi kartı şirketinin hizmetlerine kaydolun ve doğrudan işten işletmeye veya kişiler arası ödemeleri desteklemeyen satıcılarla çalışır.

Verimlilik Eksikliği: İnternet üzerinden yapılan ödemeler, ödemelerin ve işlemlerin işlenmesine dâhil edilen harcamalar nedeniyle mevcut ödeme yöntemleri tarafından işlenemeyecek kadar küçük olabilir. Kredi kartları küçük ödemeleri eklemek için çok pahalıdır ve küçük işlemler için uygun değildir.

1.6. ELEKTRONİK ÖDEME YÖNTEMLERİNİN AVANTAJLARI

Elektronik ödeme yöntemleri, para transfer işlemlerini elektronik ortamda yapması, para transferinin daha hızlı, güvenilir ve düşük maliyetle gerçekleştirmesi, bankaların fon yönetimlerini daha kolay ve etkin biçimde gerçekleştirmesi, insan gücü ve kâğıda dayalı işlemlere olan ihtiyacın azalması, ödeme hizmetlerinin çeşitlenmesine fırsat verecek bir altyapı sunması gibi özellikleri ile klasik ödeme yöntemlerinden daha avantajlıdır (TCMB, 2014. Erişim tarihi 30.03.2020). Bunlardan bazıları geleneksel ödeme yöntemleriyle sağlanamaz. Artan güvenlik seviyeleri ve tüketicinin güçlendirilmesi, daha fazla ekonomik şeffaflık, artan ekonomik canlanma, bankacılık sistemine genişletilmiş katılım, işlem verimliliğini arttırmak ve ödeme kanallarının genişletilmesi faydaları ekonomik büyümeyi desteklemektedir (Masihuddin vd., 2017: 5).

Ek olarak, elektronik iş başarısının dayandığı e-ticarete en büyük kolaylaştırıcı araç haline gelmiştir. Elektronik ödeme yöntemi aynı zamanda dünya ödeme sisteminde verimlilik, dolandırıcılık azaltma ve yenilikçilik getirmiştir (Fan ve Huang, 2010: 569). Ayrıca elektronik ödeme yöntemi, finansal kuruluşların müşterilerine kredi kartları, banka kartları, çevrimiçi bankacılık ve mobil bankacılık gibi farklı e-ödemeye fırsatları ve hizmetleri sunduğu birçok elektronik ödeme şekli oluşturma eğilimindedir (Kabir vd., 2015: 114).

1.7. ELEKTRONİK ÖDEME YÖNTEMLERİNİN SORUNLARI

Elektronik ödeme yöntemlerinin avantajlarına rağmen, günümüzün teknolojik olarak gelişmişlerine paralel kendi içinde zorlukları da vardır. Önceki araştırmacılar tarafından belirlenen zorluklar altyapı, düzenleyici, yasal konular ve sosyo-kültürel konulardır (Masihuddin vd., 2017: 7:

* Altyapı: Elektronik ödemelerin etkili bir şekilde yürütülmesi için altyapıesastır. Elektronik ödemelerin verimli olabilmesi için, halkın baskın kesimi tarafından yararlanılabilecek mali açıdan bilgili ve güvenilir bir altyapıya sahip olması gerekir. Gelişmekte olan ülkelerde, ülkenin büyük bir bölümünde bankalar bulunmaz ve elektronik ödemeleri yönlendiren temel altyapıya erişimleri yoktur. Bu da elektronik ödemelerin ilerlemesini tersine etkilemektedir.

* **Düzenleyici ve Yasal Konular:** Ulusal, bölgesel veya küresel yasaların, standartların ve diğer yönlerin düzenlenmesi, elektronik ödeme planlarının etkin bir şekilde uygulanması için zorunlu ön koşullardır. Bileşenlerin önemli bir kısmı, vergi kaçakçılığı, e-para kuruluşlarının ve ticari bankaların denetim uzmanları tarafından denetimi; merkez bankaları ödeme sistemleri, alıcı ve bilgi koruma, katılım ve rekabet konuları üzerinde gözetim altında bulundurulmalıdır.

* **Sosyo-Kültürel Zorluklar:** Sosyo-kültürel farklar ve çeşitli nakit türlerinin kullanımı(örneğin, Kuzey Amerika’da kredi kartlarının kullanılması ve Avrupa’da banka kartlarının kullanılması), küresel düzeyde bir elektronik ödeme sistemi oluşturmada karmaşık hale gelmektedir. Çeşitli toplumlardaki bireyler arasında gerekli güvenlik ve üretkenlik düzeyindeki ve ilerleme derecesindeki tutarsızlık sorunu durumu daha da kötüleştirmektedir. Alıcının geleneksel ödeme yöntemlerine duyduğu güven, müşterileri yenilikleri benimseme konusunda daha isteksiz kılar. Müşteriler, gizliliklerinin sağlandığından ve güvenliğin tatmin edici şekilde onaylandığından emin olana kadar yenilikler piyasaya hâkim olamaz. Kullanımı daha basit ve yerleşik tekniklerden daha ucuz olsa da insanların güvenliğini sağlamak için yeni ilerlemelerin de aynı şekilde zamana karşı ayakta durması gerekir.

1.8. ELEKTRONİK ÖDEME YÖNTEMLERİNDE YENİ TRENDLER

Bankaların değişen müşteri alışkanlıklarına uyum sağlayabilmeleri için özellikle tüketicinin zamandan tasarruf etmelerini sağlamak amacıyla yaptığı yeniliklerle birlikte dijital ve mobil ödeme sistemlerinde de yepyeni gelişmeler karşımıza çıkmaktadır. Bu gelişmelere paralel olarak ödeme yöntemlerinde yeni trendleri Erbaşlar ve Dokur, (2016) şöyle açıklamaktadır:

* **Mobil Deneyimlerin Kişiselleşmesi:** Tüketicilerin dijital kanalları daha fazla kullanmaya başlamasıyla ilgili birimler daha fazla veri üretmeye başladı. Oluşan bu veriler ile tüketicilerin mobil deneyimleri kişiselleştirilmeye başlandı. Mobil bankacılık, bilet alımı, park hizmetleri gibi pek çok servis buna örnek verilebilir.

* Self Servis Ödeme Yöntemlerinde Artış: Tüketicilere her durumda 24 saat hizmet veren self servis ödeme terminallerinden kioks² ve vending (satış makinesi) gibi makineler geliştirilmiştir. Bu makineler sayesinde tüketicilere tek başlarına ödeme yapma imkânı verir, maliyetleri azaltır, verimliliği arttır. Tek başına ödeme yapılmasını sağlayan bu cihazlar araba park etme, oyun makinelerinde kullanım, müze, film, konser bileti alma, perakende satışlarında self servis gibi hizmetlerde gelişim göstermektedir. Özellikle alışverişlerde tüketicinin kendi kendine ödeme yapmasına imkân veren bu cihazlar sayesinde alışverişlerde oluşan uzun kuyrukların oluşması önlenmektedir.

* Alternatif Mobil Ödeme Çözümlerinin Sunumu: Şirketler ve markalar, daha iyi bir hizmet sunabilmek ve daha çok müşteriye ulaşmak için geliştirilmiş alternatif mobil ödeme yöntemleri tasarlamışlardır. Buna örnek olarak Apple'ın pazara sunmuş olduğu kapalı alanlarda mobil kullanıcıların nerede olduğunu belirlemesini sağlayan iBeacon gösterilebilir. Bu az maliyetli konumlandırma hizmeti, herhangi bir yere yerleştirilmiş kablosuz sensörleri sayesinde yakınlarda bulunan İOS cihazlara bildirimler yollayarak içinde olduğumuz mağazada bulunan ürünler hakkında bilgi aktarılmasının yanı sıra kuponlar, promosyonlar ve fırsatlar hakkında da bilgi alınmasını sağlamaktadır. Aynı zamanda geliştirilen iBeacon uygulaması kasa kuyruğu beklemeye gerek kalmaksızın ödeme yapabilme imkânı sunmaktadır (Erbaşlar ve Dokur, 2016: 115-117).

² Kioks sistemleri, kabin içinde gizlenmiş bir bilgisayar, dokunmatik bir ekrandan oluşan, tanıtım, bilgilendirme, yönlendirme amaçlı kullanılan interaktif tanıtım ve hizmet terminalidir. Sistem tamamen dokunmatik olarak çalışmakta, ekranda işlem sırasında dinamik olarak beliren butonlara dokunularak istenilen bilgilere ulaşılmaktadır (Diostech, 2021. Erişim Tarihi: 19.05.2021).

İKİNCİ BÖLÜM

E-ÖDEME YÖNTEMLERİNE YÖNELİK GÜVEN VE GÜVENİLİRLİĞE DAİR KAVRAMSAL ÇERÇEVE, GELİŞTİRİLEN HİPOTEZLER VE MODEL ÖNERİSİ

Bu bölümde teknolojinin ilerlemesiyle birlikte gelişen e-ödeme yöntemlerindeki güvenlik ve e-ödemeye karşı duyulan güven dört bölümde incelenmiştir. Birinci kısımda e-ödeme yöntemlerinin güvenlik sistemleri tanıtılmakta, ikinci kısımda e-ödeme yöntemlerine duyulan güven üçüncü kısımda elektronik ödeme yöntemlerine dair literatür taraması ve bibliyometrik analiz yapılarak dördüncü kısımda elde edilen bilgilerle geliştirilen hipotezler ve model önerisi detaylandırılarak anlatılmaktadır.

2.1. E-ÖDEME YÖNTEMLERİNDE KULLANILAN GÜVENLİK SİSTEMLERİ

Elektronik ticaretin yaygınlaşması bankacılık sektörünün aracılık ettiği elektronik ödeme sistemi kullanımını arttırmıştır. Ancak bununla birlikte yeni güvenlik tehlikeleri ortaya çıkmıştır. Elektronik ödemelerde yoğun kişisel ve finansal bilgilerin kullanılması kötü niyetli kişilerin ve kurumların odak noktası haline gelerek virüs, hacker, hırsızlık ve siber saldırı olayları artmaya başlamıştır (İşler ve Gülaç, 2017: 82; Obaidat, 2007: 9). İnsanlar, kişisel bilgilerinin çalınabileceğinden korktukları için bir işlem yapmaktan ve çevrimiçi ödeme yapmaktan korkabilmektedir (Mukherjee ve Nath, 2003: 13). Özellikle kişisel verilerin depolandığı ortamlar saldırganların en çok ulaşmayı istediği bölgeler olduğu için en riskli unsurdur. Bu verileri saklayan kurumlar sistemin güvenliğini sağlamak zorundadırlar (Ayhan, 2018: 41). Elektronik ortamda gerçekleşen ödemelerin sorunsuz bir şekilde gerçekleşebilmesi ve ödeme işlemlerinin güvenliğinin sağlanması için bankalar bu anlamda büyük sorumluluk sahibidir. Elektronik ödeme yöntemlerinde ortaya çıkan güvenlik sorunlarını en aza indirmek için bankalar yeni girişimler başlatmıştır. Bir finansal işlemin güvenliği, özellikle internet üzerinden birçok tarafla iş yaparken son derece önemlidir. Tüketiciler, finansal bilgilerini, üçüncü kişilerce elde edilme korkusu olmadan çevrimiçi bir satıcıya gönderebilmelidir. Ayrıca satıcının

kimliğinden, siber satıcının güvenilir olduğundan ve sahte bir kimlik taşımadığından emin olmalıdır. Güvenlik gereksinimlerini karşılamak için şifreleme tekniklerin kullanılması, ilgili tarafların güvenli anahtar depolamaya erişime sahip olması istenir. Örneğin, aynı mesajları iki farklı alacaklıya göndererek aynı parayı iki kez harcamak mümkün olmamalıdır. Bütün bunlar, dürüst ödeyenlerin ve alacakların mahremiyetini ihlal etmeyecek şekilde yapılmalıdır (Rob ve Opara, 2003: 140). Ödemeler çevrimiçi olarak, her ödemede bir kimlik doğrulama veya çevrimdışı yani ödeme sırasında üçüncü bir tarafla iletişime geçmeden gerçekleştirilebilir olmalıdır (Asokan vd., 2000: 7-8).

Elektronik ödeme yöntemleri, müşteri bilgilerini korumak ve güvence altına almak ve finansal işlemi doğrulamak için koruma mekanizmasına ihtiyaç duymaktadır (Ardiansah vd., 2020: 1474-1475). Güvenli olmayan bir e-ödeme yöntemine müşterileri güvenmeyecektir. Bu bakımdan güven, müşterilerin kabulünü garantilemek için son derece önemlidir. Elektronik ödemelerde ve çevrimiçi işlemlerde sistemin güvenli kabul edilmesi için aşağıdaki hizmetlerin sağlanması gerekir (Singh vd., 2012: 238; Masihuddin vd., 2017: 9; Asokan vd., 2000: 4-5; Obaidat, 2007: 10-11):

- Anonimlik, mahremiyet: Kullanıcıların gizliliklerini, kimliklerini ve kişisel bilgilerini koruma arzusunu yansıtır. Bazı işlemlerde tarafların kimlikleri anonim olarak korunabilir. Anonimlik, bir kişinin kimliğini keşfetmenin veya bir bireyin harcama modellerini izlemenin mümkün olmadığını gösterir.

- İzlenebilirlik: İzlenebilirlik, bir ödeme yönteminden geçen ve satın alımlar için kullanılan para akışlarını ve fon kaynaklarını izlemenin ne kadar kolay olduğunu gösterir. Elektronik ödeme yöntemlerinde para, bir ödeme faaliyetini tutan kayıtlarla izlenebilir. Örneğin, kredi kartı ödemeleri ile ilgili bilgiler bankalar ve kredi kartı şirketleri tarafından saklanır ve paranın ne için kullanıldığını ve nereden geldiğini öğrenmek mümkündür.

- Erişilebilirlik/Kullanılabilirlik Kontrolü: Bir kaynağın yetkisiz kullanımının engellenmesi anlamına gelir. Diğer bir deyişle bir kaynağa kimin erişebileceğini, hangi koşullar altında erişimin gerçekleşebileceğini ve kaynağa erişenlerin ne yapmasına izin verildiğini kontrol eder. Ayrıca müşteriler istedikleri zaman işlemlerini yapabilmeli, sistemler yeterli performans ve kapasiteyi içinde barındırmalı ve sistemlerde oluşabilecek arızaların giderilmesiyle yeniden çalışılabilir hale getirilmesi kabul edilebilir bir süreçte gerçekleşmelidir. Ödeme

işlemleri atomik olmalıdır. Yani ödeme yapan kişi, bir ağ çökmesi nedeniyle, alacaklının sunucusunun çökmesiyle, site arızalarında, tek taraflı işlem iptallerinde ve hileli davranışlarda bir para kaybı yaşamamalıdır (Katsaros, 2009: 237). Elektronik ödeme yöntemleri, kullanıcı merkezli bir bakış açısı ve çevrimiçi ödeme yapmak karmaşık bir işlem olmasının aksine kolay ve kullanıcı dostu bir şekilde yapılmalıdır. Buna göre ödeme sürecinde, kullanıcılar ödemeyi karmaşık hale getiren veya dikkatlerini dağıtan minimum faktörlere sahip olmalıdır. Elektronik ödeme yöntemlerinde aşırı karmaşık bir ödeme süreci, müşterileri bir finansal işlemden ve gelecekte olabilecek e-ticaret faaliyetlerinden uzaklaştırabilir. Örneğin isim, adres bilgileri, 16 haneli kredi kartı numarası ve son kullanma tarihi içeren uzun bir formun doldurulması gerektiğinden ödeme süreçlerinin nakit ödemelerle karşılaştırıldığından kolay bir işlem olarak adlandırılmaz (Abrazhevich, 2004: 33-38; Abrazhevich, 2001:85-86).

- Kimlik Doğrulama ve Yetkilendirme: “Kimlik doğrulama, bir prosedürün veya belki de cihazın kimliğini doğrulama prosedürüdür (Hassan vd., 2020: 8).” İşlemlere başlamadan önce kullanıcılar birbirlerinin kimliklerini teyit etmeli ve işlem yapan müşteriler izin verilen ölçüde işlemlerini gerçekleştirmelidir. Her iki taraf da karşı tarafla iletişim kurarken kendilerini rahat hissedebilmelidir. Bu açıdan kimlik doğrulama faktörleri, bir iletişimin gerçek olmasını sağlamayı amaçlar. Aigbe ve Akpojaro (2014), kimlik doğrulama faktörlerini şu şekilde değerlendirmişlerdir: Kimlik doğrulama faktörlerinin katmanlarının değiştirilmesi, daha fazla veya daha az güvenlik sağlar ve herhangi bir kimlik doğrulama faktörü katmanının doğruluğu, çevrimiçi kullanıcıların ödeme bilgilerinin ve tüm sistemin bütünlüğünden ödün vermeden yeterince somut olmalıdır. Farklı elektronik ödeme yöntemleri, farklı doğrulama faktörleri seviyeleri sergilemektedir. Doğrulama faktörü, bir elektronik ödeme yönteminin ne ölçüde güvence altına alınacağını belirler. Tek faktörlü bir kimlik doğrulama mekanizması, bir kullanıcının kimliğini yalnızca bir veri ögesiyle kanıtlamasını kullanır. Bu, tek kimlik doğrulama faktörü başarısız olursa elektronik ödeme yöntemlerinin kolayca tehlikeye atılacağı anlamına gelir. İki faktörlü kimlik doğrulama, tek bir sürecin iki tutarlı ve bağımlı adımında iki bağımsız bilgi parçası sunarken, üç faktörlü doğrulama, tek bir sürecin üç tutarlı ve bağımlı adımında üç bağımsız bilgi parçası sunar. Birden çok bağımsız faktörle kimlik doğrulama, talepte bulunan kişinin birden çok bağımsız ancak tutarlı süreçte kimliğine ilişkin doğru kanıt sunmasını sağlar. Faktörlerin sayısı ve

bağımsızlığı önemlidir. Çünkü daha bağımsız faktörler daha yüksek olasılıklar anlamına gelir. Dolayısıyla iki veya daha fazla kimlik doğrulama faktörünü içeren kimlik doğrulama mekanizmalarına sahip sistemler daha güvenli olma, dolandırıcılık açıklarını azaltma ve kullanıcıların elektronik ödeme sistemlerinin kullanma güvenliğini artırma eğiliminde olduğu söylenebilir (Aigbe ve Akpojaro, 2014: 12). Yetkilendirme, bir ödeme açıkça yetkilendirilmedikçe bir taraftan para alınmaması anlamına gelir. Ayrıca kullanıcılar, açık rızaları olmadan para almamayı isteyebilir. Bu, bir kullanıcı istenmeyen tahsilattan kaçınmak istediğinde istenir. Teknik olarak, yetkilendirme genellikle para transferine neden olan mesajların doğrulanmasıyla elde edilir yani işlemlerin geçerliliği üzerinde bir kontrol biçimi olarak tanımlanır (Abrazhevich, 2004: 33-38; Abrazhevich, 2001:85-86).

- Bütünlük: “Alınan verilerin tam olarak yetkili bir kuruluş tarafından herhangi bir ekleme, silme veya tekrarlama olmadan gönderildiği gibi olduğuna dair güvencedir (Masihuddin vd., 2017: 9)”. Verilerin silinmesi/ imhası da bu hizmet tarafından kontrol edilir. Bütünlük, işin niteliklerine ve isteklerine göre verilerin geçerliliği, doğruluğu ve eksikliği olarak nitelendirilebilir. Elektronik ödeme işlemlerinde verilerin bütünlüğü korunmalı, saklanan veya transfer edilen bilgiler üzerinde değişiklik yapılmamalı ve silinmemelidir (Hassan vd., 2020: 8).

- İnkâr Edilememe: İletişimin tamamına veya bir kısmına katıldığına dair bir iletişimde yer alan kuruluşlardan birinin inkâr etmesine karşı koruma sağlar. Ne bir mesajın göndericisinin mesajın iletimini reddedemeyeceğini, ne de bir mesajın alıcısının mesajın alımını reddedemeyeceğini garanti eder. Bu nedenle bir mesaj gönderildiğinde alıcı mesajın aslında söz konusu gönderen tarafından gönderildiğini kanıtlayabilir. Benzer şekilde, bir mesaj alındığında, gönderen, mesajın gerçekte meşru alıcı tarafından alındığını kanıtlayabilir. Bir başka deyişle çevrimiçi işlemlerin bilgi akışının doğru kişiler arasında yapıldığını kanıtlayan özelliklere sahip olmalıdır.

- Bilgilerin Gizliliği: Bilgisayar korsanlarının hassas bilgileri ele geçirme olasılığı nedeniyle, e-ticaret dünyasında gizlilik son derece önemlidir (Hassan, 2020: 9). Gizlilik, özel ve hassas verilerin yetkisiz açığa çıkarılmasına karşı korunması anlamına gelmektedir. Aynı zamanda bir işlemle ilgili ödeyen, alacaklı, satın alınan içerik, miktar vb. hakkındaki bilgilerin kısıtlanması olarak da tanımlanabilir. Gizlilik, kullanıcı gizliliğinin yanı sıra özel bilgilerin korunmasında

ve bilgi hırsızlığına karşı caydırıcı bir unsurdur. Genel bir ağda gizliliği sağlamanın yolu güçlü şifrelemedir. Veriler, güvenli olmayan bir ortamdan geçse bile uygun kimlik bilgileri olmayanlardan gizli tutulur. Taraflar arasındaki işlemlerin üçüncü kişilerce görüntülenmesi ve paylaşılması engellenir, ödeme bilgilerinin detayları üçüncü kişilerden korunur. Tüm ödeme sistemleri, ödeyen ve alacaklı arasındaki tüm akışlar şifrelenerek yabancılar tarafından izlenemez ve gerçek kimlikler yerine takma adlar kullanılarak alacaklı için anonim hale getirilebilir.

- Güvenlik: Genel olarak güvenlik, “bilgi kaynağının kimliğini doğrulamak ve bu durumdan kaçınmak için verilerin bütünlüğünü ve gizliliğini garanti etmek için bir dizi prosedür ve mekanizmadır (Tsiakis ve Sthephanides, 2004: 12)”. Güvenlik, ödeme sistemlerine yapılan saldırıları ve dolandırıcılık girişimlerini önler ve tespit eder ve makul ödeme bilgilerini korur. Güvenlik, internette dolandırıcılık yapmak için bir ödeme sistemini kötüye kullanma girişimleri yaygın olduğu için gereklidir (Abrazhevich, 2004:36). Güvenlik öznel bir kavramdır. Her kullanıcı tarafından farklı şekilde hissedilir. Bir yandan, kullanıcılar çevrimiçi ödeme yaparken paraların güvende olduğundan emin olmak isterler. Diğer yandan, bankalar ve ödeme hizmetleri kuruluşları da hiçbir para, mali veya kişisel bilginin çalınmaması veya kötüye kullanılmaması için kendilerini korumak istemektedir. (Párhonyi vd., 2006: 3).

Herhangi bir çevrimiçi ödeme işlemi döngüsünde gizli tutulması gereken hedef bilgi, kullanıcının ödeme (finansal) bilgisidir. Elektronik ödeme ve çevrimiçi işlemlerde oluşan güvenlik endişeleri nedeniyle de bir yetkili tarafından kullanıcının kimliğini doğrulamak için bir yöntem ve sistemin birden fazla koruma katmanından yararlanması gereklidir. En yaygın kabul edilen stratejiler arasında biyometrik kimlik doğrulama, dijital imzalar, şifreleme teknikleri, SSL ve SET gibi güvenlik katmanları ve teknolojik olarak alınan önlemler gibi oluşturulan mekanizmalarla güvenlik endişeleri giderilebilir (Serhateri, 2015: 229; Meng ve Xiong, 2004: 597). Bilgilerin daha güvenli paylaşılması ve ödeme bilgilerinin saklanması bakımından geliştirilmiş sistemlerin bir kısmını incelemek mümkündür (Masihuddin vd., 2017: 9):

* Akıllı Kart Güvenliği: Akıllı karta yerleştirilen bilgiler, kodlanmıştır ve PIN/şifre olmadan kullanılamaz ve bu nedenle iyi bir güvenlik sağlanır. Akıllı kartlar, manyetik şeritleri, yani kredi kartları, banka kartları vb. içeren devreden çıkarılmış kartlardır.

* Kriptografi (Şifreleme): Bu yöntemde müşterinin kredi/banka kartı ayrıntıları gibi hassas bilgileri, çeşitli ağ saldırganlarından korunmasını sağlamak için ödeme ağ geçidi tarafından herkesin bildiği bir genel anahtarla şifrelenir. Ancak, alıcı banka tarafından gizli tutulan ağ geçidinin özel anahtarı kullanılarak şifresi çözülebilir. Bu durum yetkisiz tarafların şifrelenmiş biçimdeki verilerin şifresini çözmesini engellemektedir.

Şifreleme mekanizmaları, karmaşık matematiksel algoritmalar ve anahtarların bir eşleşmesidir. Web’de şifreleme işlemi, web sunucuları ve tarayıcılar kullanılarak gerçekleştirilebilir. Böyle bir teknoloji uygulandığında, tüketici web sunucusu ile iletişim kurmak için kullanılan geleneksel http protokolü yerine https protokolünü kullanır. Web siteleri “güvenli işlem için buraya tıklayın” gibi ifadeler içeriğiyle veya tarayıcıların sunduğu işlemin güvenli olduğunu belirten iletişim kutuları aracılığıyla tüketici de bu mekanizmaya dahil edilir. Ayrıca, bir tarayıcının altındaki kırılmamış bir anahtar ve kilit görüntüsü, işlemin şifreli olduğunu gösterir. İşlem güvenliğinde şifreleme tekniği kullanıldığı gibi şifresiz işlem ve açık anahtarlı dijital imza şeklinde güvenlik mekanizmaları da şifreleme güvenlik mekanizmasının alt başlığı olarak incelenebilmektedir (Asokan vd., 2000: 15-16).

* Şifresiz İşlemler: Hiçbir şekilde kriptografi kullanmamak anlamına gelir. Örneğini elektronik olarak sipariş verilen mallar, siparişi onaylayan ödeyenden bir telefon görüşmesi, faks veya mail gelmeden önce teslim edilmez. Bu tür sistemlere örnek olarak First Virtual verilebilir. Bu işlemde kullanıcının bir hesabı vardır ve bir kredi kartı numarası karşılığında bir şifre alır. İnternet üzerinden işlem yaparken şifre korumalı değildir. Bu nedenle, bu sistemler gizli işlemlere karşı savunmasızdır. First Virtual bu anlamda sözde ödeyen kişiden mail yoluyla her ödemenin onayını isteyerek bir miktar koruma sağlar, ancak ödeyenin her bir ödemeyi belirli bir süre içinde iptal etme yetkisi bulunur. Bu sürenin sonuna kadar alacaklı tüm riski üstlenir.

* Açık Anahtarlı Dijital İmzalar: Açık anahtar şifrelemesine dayalı kimlik doğrulaması için, kanıtlayıcı, iyi bilinen bir yetkili tarafından verilen bir gizli imza anahtarına ve buna karşılık gelen genel imza doğrulama anahtarı için bir sertifikaya sahip olunması gerekir. Dijital imzalar, imzalı bir iletinin göndereni ve alıcısı arasındaki anlaşmazlıkların çözülebilmesi için kolaylık sağlar. Ödeyen, en azından yüksek değerli ödemeler için sahte ödeme riskini taşıyorsa bu zorunlu olmalıdır. Açık anahtar şifreleme kullanan WWW(İnternet Dünya Çapında Ağ üzerinde geliştirilen SHTTP ve SSL şemalar örnek gösterilebilir. SSL, iki tarafın güvenli bir şekilde

iletiřim kurmasını saęlayan bir internet soket katmanı iletiřim ara yzudur. SHTTP ise WWW üzerinde kullanılan http protokolünün gvenli bir uzantısıdır. SHTTP, imzalama ve řifreleme gibi çeřitli gvenlik teknikleri sunmaktadır (Asokan vd., 2000: 15-16; Chellappa ve Pavlou, 2002: 361; Singh vd., 2012: 240-241).

* Biyometrik Kimlik Doęrulama: Biyometrik kimlik doęrulaması, e-ticaret iřlemlerinde kullanıldığında çevrimiçi iřlemlerde gvene yol aabilen bir gvenlik teknolojisidir. Elektronik ödeme iin biyometrik kimlik doęrulaması, genellikle çevrimiçi ödeme iin kullanıcıları tanımlamak ve doęrulamak iin daha hızlı, kullanışlı ve daha gvenli bir ara olarak gvrulmektedir. Biyometrik kimlik doęrulaması, bir kiřinin ozelliklerinin biyometrik verilerinin depolanmış bir kopyasıyla olvlmesini ve karřılařtırılmasını ierir. Biyometrik kimlik doęrulamanın amacı, kimlik doęrulama noktasında yakalanan biyometrik verilerin önceden depolanan svrümle eřleşmesini saęlamaktır. Akıllı telefonlar ve akıllı saatler tarafından popler hale getirilen ödeme iin biyometrik kimlik doęrulamasının yukseliři, daha dűřuk gvenlik endiřeleri (orneęin kimlik hırsızlıęını onlemek) ve artan kolaylık ile iliřkilendirilmiřtir (Ogbanufe ve Kim, 2018: 9-10).

* 3D Gvenlięi (3D Secure): 3 boyutlu gvenlik sistemi (3D Secure), Visa ve MasterCard tarafından e-ticaret iřlemlerinin gvenlięinin arttırılması amacıyla oluřturulmuş bir sistemdir (Masihuddin vd., 2017: 9). 3D Secure, internet alıřveriřlerinde; műřteri, kartı oluřturan banka ve iřyeri arasındaki bilgi akıřını gvenli gerekleřtirmeye olanak saęlar. İnternet alıřveriři sırasında; műřteri, banka ve iřyeri arasındaki bilgi akıřı ozel řifre ve anahtarlar ile saęlanır. Bu sistemi kullanan iřyerlerinden alıřveriř yapan kart sahipleri iřlem sırasında kiřisel gvenlik mesajını doęrularak ve cep telefonuna iletilen tek kullanımlık akıllı sms řifresini sisteme girerek alıřveriři gvenle tamamlamaktadırlar (Yapı Kredi Bankası, 2021. Eriřim Tarihi 23.04.2021).

* Gvenli Soket Katmanı (SSL): Gvenli bir aę protokolű olan Secure Socket Layer (SSL), sunucularda ve web tarayıcılarında kullanılır. Benzersiz řekilde řifrelenmiş bir kanal oluřturarak ozel verileri gvenli bir řekilde aktarmak iin sertifika kimlik doęrulamasını kullanır. SSL'nin iletiřim kuran taraflar arasında hareket eden verileri řifreleyerek gizlilięi saęlamak ve tarafların kimlik doęrulamasını saęlamak olmak uzere iki ana hedefi bulunmaktadır (Serhateri, 2015: 229). Bu sistemlerde kimlik bilgileri doęrulama ařamasında katılımcılardan genellikle ek bir řifre istenmektedir (Mukherjee ve Nath, 2003: 7).

İletişim kuran tarafların (istemci yani tarayıcı ve sunucu), kendi kimliklerini doğruladıkları ve bir şifreleme anahtarı üzerinde anlaştıkları el sıkışma prosedürü olarak da adlandırılır. Bir SSL işlemi, istemcinin sunucuya bir el sıkışma göndermesiyle başlar. Sunucunun yanıtında sertifikasını gönderir. Sertifika, sunucuyla ilişkili bir genel anahtarı ve sertifikanın sahibi, sona erme tarihi ve sunucuyla ilişkili tam nitelikli alan adı gibi diğer bilgileri içeren bir veri parçasıdır (Smith, 2005: 142).

* Güvenli Elektronik İşlem (SET): Güvenli elektronik işlem (Secure Electronic Transaction (SET)), kredi kartlarını içeren çevrimiçi ödeme sistemi için güvenlikle ilgili sorunlara yanıt vermek için Visa ve MasterCard tarafından oluşturulan açık bir standarttır. SET, satıcılar ve alıcılar arasındaki ve tüketiciler ile bankalar arasındaki mevcut ilişkileri koruyarak internet üzerinden güvenli elektronik işlemlerin kolay ve hızlı bir şekilde dijital imza kullanılarak yapılmasını sağlayan bir sistemdir (S.M.Furnell ve Karweni, 1999: 374). Bu, hem müşteriye hem de bayiye bir dijital sertifika verilerek gerçekleştirilir. SET aracılığıyla yapılan herhangi bir işlem; satıcı, ödeme ağ geçidi ve müşteri olmak üzere üç varlığı içerir. SET, bir tüketici ile bir alıcı ağ geçidi arasında mevcut finansal altyapıya ara yüz oluşturan güvenli bir şekilde kredi kartı numaraların iletilmesine yardım eder. SET, katılımcı varlıklar arasında dijital imzalar kullanarak güvenli bir iletişim kanalı ve hassas bilgileri yalnızca yetkili taraflarla sınırlayarak gizlilik sağlamaktadır (Bellare vd., 2000: 613). İlk anlaşmada satıcı, tüketiciye kendini doğrular ve tüm teklif ve ödeme verileri sabitlenir. Tüketici daha sonra kredi kartı numarası gibi hassas ödeme bilgilerini koruyan, ihracat onayını kolaylaştırmak için şifrelemeyi seçilen alanlarla sınırlayan, sipariş bilgilerini kriptografik olarak bağlayan ve kullanıcının gizliliğinin açığa çıkmasını en aza indiren gelişmiş bir şifreleme şeması kullanarak bir ödeme makbuzu oluşturur. Bu fiş daha sonra ödeme yetkisi vermek için tüketici tarafından imzalanır ve ödemeyi onaylamak ve kaydetmek için alıcı ağ geçidine gönderen satıcıya gönderilir. Alıcı, tüm imzaları ve fişi kontrol eder, mevcut ağ üzerinden tüketicilerin doğrular ve bu işlemin sonucuna bağlı olarak satıcı ve tüketiciye olumlu ya da olumsuz imzalı bir alındı bildirimini gönderir. İşlemleri başarılı bir şekilde gerçekleştirmek adına SET için temel gereksinimler şunlardır (Asokan vd., 2000: 15-16; Chellappa ve Pavlou, 2002: 361):

- Ödeme bilgilerinin ve ödeme bilgileriyle birlikte iletilen sipariş bilgilerinin gizliliği sağlanmalıdır.
- İletilen tüm verilerin bütünlüğü sağlanmalıdır.

- Kart sahibinin markalı bir ödeme kartı hesabının meşru bir kullanıcısı olduğuna dair kimlik doğrulaması sağlanmalıdır.
- Bir satıcının, satın alan bir finans kurumu ile ilişkisi yoluyla markalı ödeme kartı işlemlerini kabul edebileceğine dair doğrulama sağlanmalıdır.
- Bir elektronik ticaret işleminde tüm meşru tarafları korumak için en iyi güvenlik uygulamalarının ve sistem tasarım tekniklerinin kullanıldığına emin olunmalıdır.
- Taşıma güvenlik mekanizmalarına bağlı olmayan ve bunların kullanımını engellemeyen bir protokol oluşturulmalıdır.
- Yazılım ve ağ sağlayıcıları arasında birlikte çalışabilirlik kolaylaştırılmalı ve teşvik edilmelidir.

SET'in amacı, ödeme sürecini özel, kullanışlı ve en önemlisi her şeyden güvenli olmasını sağlamaktır. SET, müşterilerinin sipariş ve ödeme bilgilerinin gizli tutulmasını sağlar. SET, kredi kartını müşterinin verdiği bilgilere göre doğrular ve ardından online mağaza olan üye iş yeri sipariş detaylarını bankaya gönderir. Satın alınan onaylanması işlemi ikisi arasında gerçekleşir. Onaylandığında, banka dijital olarak imzalayacak ve daha sonra siparişi işleyebilecek olan satıcıya yetki vererek sipariş tamamlanma işlemini gerçekleştirecektir (İsmaili vd., 2015: 78).

2.2. ELEKTRONİK ÖDEME YÖNTEMLERİNE DUYULAN GÜVEN

Elektronik ticaret, elektronik ödeme yöntemleri üzerine inşa edilmiştir, dolayısıyla e-ticarete ödeme yöntemlerine duyulan güven online platformda bir ticari işlemin satın almayla sonlanabilmesi açısından son derece önemlidir. Güven faktörü e-ticarete tüketicilerin elektronik ödeme yöntemlerinin kullanımını etkileyen önemli bir konudur. Çünkü gerçek dünya işlemlerinden farklı olarak, perakendeci işlem sırasında şahsen bulunmaz ve tüketici gerçek bir kişi ile muhatap olmaz. Sadece bir arayüzle uğraşır. Bir kuruluşun web sitesi ve elektronik ödeme işleme sistemi kurması, gerçek bir vitrinden çok daha kolaydır. Daha ucuz, daha hızlı ve daha şeffaftır. Ancak müşterilerin web sitelerinin gerçekliğinin belirlenmesi çok daha zordur. Bu durum perakendecilerin iddia ettikleri kişi olduğuna güvenmeyi çok zorlaştırır. Güven, tüketicilerin e-ticaret pazarındaki işlemlerin ve ilişkilerin belirsizliğini ve

karmaşıklığını azaltmaya çalışırken kullanabilecekleri zihinsel bir kısayoldur. (Gupta ve Dubey, 2016: 231). E-ticaret güvenliği ise, “e-ticaret varlıklarının yetkisiz erişim, imha, değişiklik ve kullanımdan korunması” olarak tanımlanır (Tariq vb., 2017: 1). Elektronik ödeme yöntemleri bu anlamda kullanıcıların, kredi kartı numarası, telefon numarası, adres, isim gibi kişisel bilgilerinin güvende tutulmasını ve transferlerin hızlı ve güvenilir olmasını sağlamalıdır (Öney vd., 2017: 408).

Güven, bir kişinin isteyerek birine karşı sahip olduğu inancı ifade eder. Bu, uzun vadede müşterilerle iş ilişkileri kurmada önemli bir araçtır. Güven eksikliği, tüketicilerin çevrimiçi mağazalardan alışveriş yapmasına engel olarak e-ticaret işletmelerinin başarısızlığına neden olur. Tüketiciler ve ürün-hizmet sağlayıcıları, elektronik iletişim ve işlemlerin gizli olacağından, mesajların kaynağının doğrulanabileceğinden ve kişisel mahremiyetin korunabileceğinden emin olmadıkça geniş ölçüde elektronik ticaret uygulamalarını kullanmaları beklenmez (Tsiakis vd., 2005: 149).

Güven aynı zamanda tüketicinin yeni teknolojileri kabul etmesini etkiler ve tüketicinin ürünlere olan güvenini belirler. Böylelikle sitenin güvenlik koruması, mahremiyeti ve güven işareti ile etkili e-ödeme sistemi, sistem kullanıcılarına güven oluşturabilir. Müşteri güveni, müşterinin sitenin ürün ve hizmetlerinin sunulmasına yönelik tutumuna, sistem kalitesine, veri kalitesine ve hizmet kalitesine dayanır. Müşteri güveninin, sitenin sahibi olan kuruluşun ödeme sistemlerinin etkin ve güvenilir bir şekilde yönetilmesine bağlıdır. Bunlar, e-iş yönetiminde müşteri güvenini oluşturmanın yanı sıra, kulaktan kulağa iletişimin etkisi ve ürün satın alma kararı da dahil olmak üzere e-ticaret yoluyla satın alma ve ödeme yapma konusunda önemli rol oynar (Suwunniponth, 2016: 3927).

Güven sorunu, ekonomik işlemler risk içerdiği için ortaya çıkmaktadır. Bu açıdan algılanan risk güven konusunda önemli bir rol oynamaktadır. Müşterilerin elektronik iletişim teknolojisine ve internete yönelmeleri, genellikle internet bankacılığına olan güvenlerin bir temsilcisidir. Elektronik sisteme ne ölçüde güvendikleri, internet bankacılığına girerken duydukları genel güven ile büyük olasılıkla ilişkili olacaktır. Müşteriler, elektronik işlemleri değerlendirmek için bir ağ ve indirme hızı, gezinebilirlik, güvenilirlik, bağlanabilirlik ve kullanılabilirlik gibi çeşitli performans ölçümlerini kullanır. Müşterilerin temel endişesi, ağın güvenirliliği olacaktır. Müşteriler, kişisel finansal verileri elektronik ağ üzerinden aktardığında yetkisiz kişilerin bu bilgileri ele geçirme riski vardır. Bu nedenle, müşterilerin

teknoloji yönelimi ve elektronik iletişim sisteminin teknolojik yetkinliği algısı, bilgi işleme davranışları ve algılanan güvenleri açısından önemlidir. Mukherjee ve Nath (2003) çalışmalarında tüketicilerin bir işletmeye güven duyabilmesi için aşağıdaki bazı öncüllerin oluşması gerektiğini vurgulamaktadır. Bunlar (Mukherjee ve Nath, 2003: 7-8):

- Paylaşılan Değer: Ortakların hangi davranışların, hedeflerin ve politikaların önemli veya önemsiz, uygun veya uygunsuz ve doğru veya yanlış olduğuna dair ortak inançların derecesidir. Çevrimiçi bankacılık bağlamında paylaşılan değer, banka ve müşterilerin etik, güvenlik ve mahremiyet gibi kritik değerlere ilişkin ortak inançları ne ölçüde paylaştığını sembolize eder. Paylaşılan değer, müşterilerin bağlılığının artmasına yol açar ve çağrışım duygusunu güçlendirir. Bir bağ geliştirir ve ilişkisel uzun vadeli bir ilişkiyi besler. Bu daha sonra güvenin doğmasına yol açar. Bu nedenle, güvene dayalı bir ilişki geliştirmek için müşteri mahremiyeti, güvenliği ve ahlaki kültürünü teşvik etmek ve ilişkide pozitif paylaşılan değeri telkin etmek için çaba gösterilmesi gerekir.

- İletişim: Bir internet sitesinin açıklık, yanıt hızı ve bilgi kalitesi açısından sosyal iletişimini ne ölçüde geliştirebileceği, sitenin çevrimiçi müşterilerin ihtiyaçlarını karşılama yeteneğini etkileyecek ve onlar da buna yanıt verecektir. Bu nedenle banka internet sitelerinde gösterilen sosyal iletişimde yanıt hızı, bilgi kalitesi ve açıklık derecesi ne kadar yüksek olursa, müşterilerin güveni üzerindeki etki ve çevrimiçi işlemleri de paralel olarak artar.

- Fırsatçı Davranış: Bilginin çarpıtılması, kural ve düzenlemelerin ihlali gibi özelliklerle ölçülür. Yeni ortaya çıkan ve yetersiz geliştirilmiş kurallar ve düzenlemeler nedeniyle çevrimiçi bankaların daha yüksek fırsatçı davranış riski nedeniyle, müşteriler genellikle çevrimiçi bankacılığa düşük düzeyde güven duymaktadır.

Ödeme kritik bir aşama olduğundan ve daha fazla güvenlik gerektirdiğinden, müşterilere ödeme konusunda en fazla güveni sağlayacak bir yönteme sahip olmalıdır. Kredi kartı ile ödemenin yaygın olduğu ve şu anda internetten yapılan ödemelerde kredi kartının popüler olarak kullanıldığı söylenebilir. Süreç, alıcının kredi kartı numarasının şifrelenmesi ve ardından kart numaralarını okumak için kodu çözülmek üzere satıcının web sitesine gönderilmesidir. Ancak, satıcılar tüm alıcıların kredi kartı numaralarına erişebildikleri ve bunları yetkisiz bir şekilde kullanabilecekleri için alıcılar risk altında olabilir veya bilgisayar korsanları satıcıların verimsiz ödeme

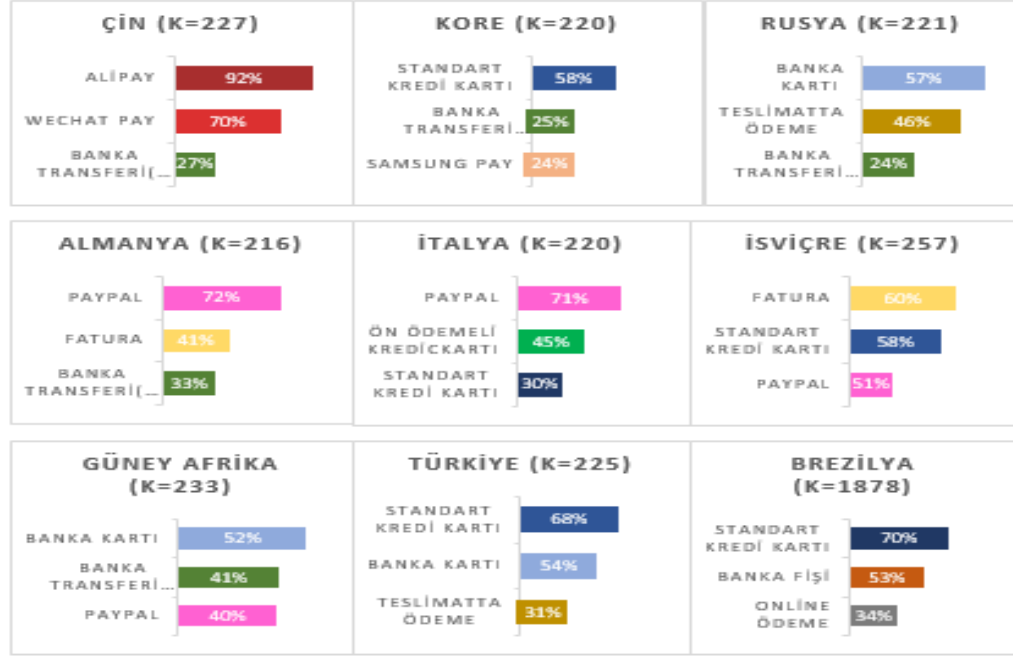
sistemini ele geçirebilir. Satıcının alıcının kredi kartı numarasını bilmediği güvenilir üçüncü şahıs hizmetleri aracılığıyla yapılan ödemeler ise müşterinin endişelerini azaltabilir. Çevrimiçi işlemlerin algılanan riski ile ilgili araştırmalar, internet kullanıcıların elektronik ticaret yoluyla ödeme hizmetlerini kullanma kararını etkileyen çevrimiçi ödeme yapmanın risklerinin ve güvenliğinin farkında olduklarını ortaya koymuştur. Elektronik ödeme için güven yaratmak önemli bir faktördür (Suwunniponth, 2016: 3926).

Tüketicinin web sitesinin bilgi kalitesine olan eğilimi, güven, gizlilik kaygıları, itibarı, güvenlik kaygıları ve şirketin itibarı, internet tüketicilerinin web sitesine olan güveni üzerinde güçlü etkilere sahiptir. Hem e-ticaret tüketicileri hem de siteler için en önemli iki sorun, gizlilik ve güvenliktir. Gizlilik, kişinin kişisel verileri üzerindeki kontroldür; güvenlik, yetkisiz kullanıcılar tarafından verilere erişilmeye çalışılmasıdır. Bu nedenle bilgi güvenliği, internet üzerinden her türlü verimli ve etkili ödeme işlemi etkinliği için temel bir yönetim ve teknik gerekliliktir (Gupta ve Dubey, 2016: 228). Tüketicilerin bir web sitesine güvenmesi için en önemli olan unsurlardan bazıları güvenlik sistemleri, şirketin itibarı, sunduğu ödeme yöntemleri, sağlanan müşteri hizmetleri, web sitesi tasarımı, teknoloji kontrolü ve kullanım kolaylığıdır. Dolayısıyla web tarayıcıları ile web siteleri güvenilir olmak için veri koruma ve güvenlik duvarları (koruma), kırılmamış bir kilit/ anahtar (şifreleme), güvenilir üçüncü şahıslardan dijital sertifikalar (kimlik doğrulama) ve tanıdık ve doğrulanabilir alan adları (doğrulama) ile ilgili ifadeler gibi görünür güvenlik mekanizmalarını gösterebilir olmalıdır (Gupta ve Dubey, 2016: 231). Bu doğrultuda müşterilerin gizlilik ve güvenlik konusundaki endişelerini azaltmak için çeşitli web güven mühürleri geliştirilmiştir. Güven mühürleri bankalar gibi üçüncü taraf sertifika kuruluşları tarafından onaylanmaktadır. Bu mühürler web sitelerinin prosedürleri, kontrollerinin onaylandığını belirten sosyal göstergelerdir. Güven mühürleri, satıcının güvenilir olup olmadığını doğrulayarak müşterilere güven sağlamaktadırlar (Özkan vd., 2010: 310).

Birleşmiş Milletler Ticaret ve Kalkınma Birliği (UNCTAD) (2021) tarafından hazırlanan “COVID-19 ve E-Ticaret” başlıklı anket çalışmasında pandemi sonrasında dijital ödemelerin kullanımındaki artışa istinaden UNCTAD’ın dokuz ülkeden oluşan tüketici anketi sonuçlarına göre ülkeler arasında çevrimiçi alışverişler için kullandıkları ödeme yöntemi tercihlerinde Şekil 5’te görüldüğü gibi önemli farklılık gözlemlenmiştir. Bu farklılık tüketicilerin elektronik ödeme yöntemlerine karşı duyduğu güvene bağlı olarak da değişiklik göstermektedir. Yapılan çalışmada banka

ve kredi kartlarının en çok Brezilya, Kore, Rusya, Güney Amerika ve Türkiye’de, Paypal’ın Almanya ve İtalya’da ve AliPay ile WeChatPay’in Çin’de popüler olduğu tespit edilmiştir (UNCTAD, 2021. Erişim Tarihi 08.05.2021).

Şekil 5: COVID- 19 Sırasında Çevrimiçi Satın Alımlar için Ödeme Yöntemlerinin Kullanımı



Kaynak: UNCTAD, 2021. Erişim Tarihi 08.05.2021.

Çevrimiçi işletmelerin güven inşa etme derecesi, müşterilerin e-ödeme yöntemlerini kullanma istekliliğini önemli ölçüde etkilemektedir. İşletmeler, müşterilerin güven derecesini anlamak için “gerekçeli eylem teorisi” modelini temel olarak hareket etmektedirler. Bu modele göre bir kişinin davranışı, davranışı gerçekleştirme niyetiyle ve öznel normlarıyla doğrudan ilişkilidir. Gerekçeli eylem teorisi modeli sosyal etkileri de göz önünde bulundurmaktadır (Özkan vd., 2010: 307-308). Örneğin; geleneksel kâğıt tabanlı kredi kartına güven, öncelikle toplum güvenine dayanmaktadır. Herkes kredi kartı kullandığı için kullanılan kontrol prosedürlerinin güvenliği çok az kişi tarafından sorgulanmaktadır. Ancak elektronik yeni ödeme sistemleri piyasaya sürüldüğünde bu ödeme sisteminin kabulü için yeni ödeme toplulukları oluşturulması gerekmektedir. Elektronik ödeme topluluğunda az sayıda kullanıcı varsa yeni kullanıcıların bu ödeme yöntemine güvenmeleri çok zor olmaktadır (Tan ve Thoen, 2000: 853). Elektronik ödemeleri güvence altına almak için kullanılan teknolojinin ayrıntısının açıklanması tüketici güveninde olumlu etki

yaratmaktadır. Uluslararası ticarete güven yaratmak için işletmeler, ticaret prosedürlerini kullanıcıların ayrıntılı şekilde anlamasını sağlamaktadırlar. Örneğin; elektronik ödemeler için SET protokolü ele alındığında yapılan çalışmalar, bu protokolü anlayan kullanıcıların ödeme yöntemine duyduğu güvenin arttığını tespit etmiştir. SET protokolünü anlayan kullanıcıların faydalı bilgiler edinip güven düzeyinin arttığı bu protokolün açıklanmadığı kullanıcıların ise ek bilgi edinemediği ve güven düzeylerinin minimum düzeyde kaldığı tespit edilmiştir. Müşterilerin bilgi güvenliğini algıladıklarında, e-ticarete olan güvenin arttığı ve satın alma niyetinin olumlu yönde etkilendiği tespit edilmiştir. Güvenlik, müşterilerin güvenilirliğe olan inançlarını arttırmaktadır. Böylece elektronik ödemeyi güvence altına almak için kullanılan teknolojinin detaylarını açık şekilde paylaşmak işletmeler için kaçınılmaz olmaktadır. Bu yaklaşımdaki sorun, teknolojinin (açık anahtar şifreleme, SET protokolü vb.) geniş bir kitleye açıklamak için çok karmaşık olmasından kaynaklanmaktadır (Tan ve Thoen, 2000: 853; Özkan vd., 2010: 309).

Elektronik ödeme yöntemleri birden çok bilgi güvenliği tehdidine tabidir. Elektronik ödeme işlemlerinde tüketici güveninin algılanan bilgi güvenliğinden etkilendiği ileri sürülür. Algılanan bilgi güvenliğinin öncülleri olarak şifreleme, koruma, kimlik doğrulama ve doğrulama mekanizmaları önerilir (Maqableh vd., 2015: 410). Bu mekanizmalar, tüketiciler tarafından görülebilen ve dolayısıyla gerçek tüketici algılarına katkıda bulunan güvenlik tehditlerine yönelik teknolojik çözümlerden türetilmiştir. Algılanan bilgi güvenliği, tüketicilerin kişisel bilgilerinin taşıma veya saklama sırasında uygun olmayan kişiler tarafından kendilerine güvenen beklentilerine uygun bir şekilde görüntülenmeyeceğine, saklanmayacağına veya manipüle edilmeyeceğine inandıkları bir olasılık olarak tanımlanmaktadır. Tüketiciler ve internet perakendecileri arasında güvenin geliştirilmesi, tüketici davranışını etkilemede önemli bir rol oynadığından elektronik ödeme yöntemlerinin sürekli büyümesi için kritiktir. Elektronik ödeme işlemlerinde tüketici güveni, tüketicilerin belirli bir işlemin kendilerine güvenen beklentileriyle tutarlı bir şekilde gerçekleşeceğine inandıkları öznel olasılık olarak tanımlanır. Algılanan bilgi güvenliği, elektronik ödeme yöntemlerine olan güven ile olumlu bir şekilde ilişkilidir (Gupta ve Dubey, 2016: 228).

Bu nedenle şifreleme, koruma, doğrulama ve kimlik doğrulama sistemleri aslında güven algılarını da etkiler. Pazar, ancak tüketiciler bu ortamda işlem yapma

konusunda güvendidiklerinde güvenilir olabilir. Sistemlerden bahsedecek olursak (Chellappa ve Pavlou, 2002: 361-362):

* Şifreleme: Şifreleme, bilgileri orijinal biçiminden kodlanmış, anlaşılmaz bir biçime çevirme işlemi olarak adlandırılır.

* Koruma: Koruma, müşterilerin kişisel bilgilerinin bilgileri toplayan işletme tarafından yeterince korunduğu gerçeğinden memnun oldukları süreç olarak tanımlanabilir. Koruma bilgisi, tüketiciye genellikle açıklama politikaları gibi birçok yolla bildirilir. Bu politikalar öncelikle gizliliğin korunmasına yönelik olsa da, verileri kimin topladığı, nasıl depolandığı ve ne kadar erişilemez olduğu konusunda güvence de içerir. İnternet perakendecileri, yetkisiz saldırıları veya izinsiz girişleri önlemek için tipik olarak gelişmiş güvenlik duvarı teknolojileri kullanır.

* Doğrulama: Elektronik ve geleneksel işlemler arasındaki en önemli fark, işlemle ilişkili örtük kimlik doğrulamasının olmamasıdır. Bir kişinin sahte bir web sayfası oluşturması oldukça kolaydır. Örneğin, tüm tüketiciler Citibank'ın "www.citibank.net" değil de "www.citibank.com" adresinde yer aldığının farkında olmazlar. Buna benzer birçok sayıda site örneği vardır. Kötü niyetli yazılımcılar tarafından bu şekilde sahte web siteleri oluşturmak son derece mümkündür. Bu nedenle, tüketiciler tam alan adının farkında olmadıklarında, Google gibi yerleşik portallara güvenebilirler. Doğrulamanın yaygın olarak karşılaşılan bir sorun olduğu düşünüldüğünde, kapsamın tüketici güven algılarını etkilemesi beklenmelidir.

* Kimlik Doğrulama: Kimlik doğrulama, bir internet perakendecisinin, perakendecinin gerçekten de iddia ettiği kişi olduğunu garanti eden güvenilir bir üçüncü taraf aracılığıyla kurulabildiği süreç olarak tanımlanır. Verisign.com gibi bağımsız üçüncü şahıslar bu garantileri sağlar. Kimlik doğrulamanın, bilgi güvenliği için örtük olarak algılanabilir başka bir mekanizma olduğu düşünüldüğünde, tüketici güvenlik algılarını da etkiler. (Chellappa & Pavlou, 2002).

Ödeme yöntemlerinin güvenliği ve güven algısı ile ilgili standartlar ve yasal düzenlemelerdeki eksiklikler e-ticaret satıcıları gerekli hassas gizlilik, güven ve güvenlik dengesine ulaşana kadar, etkili e-ticaret işlemleri bir sorun olmaya devam edecektir. Bu sistemlerden maksimum verim sağlamak amacıyla genel standartların ve kalıcı yasaların oluşturulup uygulanması gerekmektedir. Ayrıca ödeme yöntemlerinin güvenliğinin sağlanmak için altyapının sürekli olarak geliştirilmesi ve altyapı sağlayıcıları ile diğer paydaşların uygun iş birliği içinde çalışması gerekmektedir

(Erdođdu, 2004: 87). Bununla birlikte, müşteriye çevrimiçi olarak hassas bilgilerin gönderilmesi için güvenlik konularında daha fazla çalışma yapılmalıdır.

2.3. E-ÖDEME YÖNTEMLERİNE YÖNELİK GÜVEN VE GÜVENİLİRLİĞE DAİR LİTERATÜR TARAMASI VE BİBLİYOMETRİK ANALİZ

Literatür incelendiğinde; elektronik ödeme yöntemleri, e-ticarette güvenlik, elektronik ödeme yöntemlerine duyulan güven ve elektronik ödeme yöntemlerinde algılanan güvenlik konusuyla ilgili bir dizi bilimsel çalışmaya rastlanmıştır.

Mayer vd. (1995), çalışmalarında elektronik ticarette tüketicilerin satın alma davranışlarını etkileyen güven ve güvenilirlik kavramlarının üzerinde durmuşlardır. Güven kavramı, durumun ya da güvenen kişinin kendisini temsil ederken, güvenilirlik ise güvenilen kişinin özelliğini belirtmektedir, güven faktörünün uzun ve sürekli olması güvenilen kişi ya da kurumun güvenilirliğine bağlı olduğuna, bu sebeple işletmeler kendilerini birçok konuda güvenilir olarak görse bile son ölçüm tüketicinin algı ve davranışlarıyla gerçekleştiği için işletmelerin tüketici güvenilirliğine önem vermeleri gerektiği belirtilmiştir.

Sharma ve Patterson'ın (2000), çalışmalarında alıcı ile satıcının arasında uzun süreli ilişkiler oluşturma ve bu ilişkilerin sürdürülmesinde temel etmenlerden biri olarak güven gösterilmiştir.

Tan ve Thoen (2000), çalışmalarında elektronik ticaret için genel bir güven modeli oluşturulmuşlardır. Modelin temel fikrinde, bir kişinin sahip olduğu işlem güveni seviyesi, kişisel eşiğinin üzerinde olmalıdır. İncelenen çalışmada bu durum işlemin türüne ve işleme dâhil olan diğer taraflara bağlı olduğu belirtilmiştir. İşlem güveni düzeyinin de 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 eşiğin altında ise, o zaman güvenin eşik seviyesine ulaşmak için kontrol tarafından tamamlanması gerektiği üzerinde durmuşlardır.

Abrazhevich (2001), çalışmasında ödeme sistemlerinin kullanıcılar açısından önemli olan özelliklerinden güven, uygulanabilirlik, kullanım kolaylığı, güvenlik, verimlilik, izlenebilirlik ve güven yönünden inceleyip önemine vurgu yapmıştır.

McKnight ve Chervany (2001), çalışmalarında güven faktörünün kişiler arası ve ticari ilişkilerin merkezi olduğunu; özellikle riskin, belirsizliğin ve karşılıklı bağımlılığın olduğu elektronik ticarete tüketicilerin güven ihtiyacı büyüdüğünden dolayı teknik altyapı üzerine güvenin sağlanması için çalışmalar yapılması gerektiği vurgulanmıştır.

Balenger vd. (2002), çalışmalarında e-ticaretin büyümesinin temel koşulunu güvenliğin, gizlilik haklarına duyarlılığının ve güvenilirliğin teşviki ve maksimum kullanımının desteklenmesiyle mümkün olabileceğinin önemini vurgulamıştır (Belanger vd., 2002: 268).

Erdoğdu (2004), çalışmasında elektronik ödeme yöntemlerinin internet ve kablosuz ağlar üzerinden yapıldığı için ticaretin önemli bir noktasını oluşturduğu, bu nedenle sistemin kabul görmesinin ve yaygınlaşmasının elektronik ödemelerin güvenli bir şekilde gerçekleştirilmesiyle mümkün olabileceğinden bahsetmiştir.

Meng ve Xiong (2004), çalışmalarında e-ticaretin gelişmesiyle birlikte oluşturulan elektronik ödeme yöntemlerinin bazı güvenlik protokollerinden bahsetmektedirler. Aynı zamanda güvenlik protokollerinin ortak özellikleri olan anonimlik, inkart etmeme, izlenebilirlik, hesap verebilirlik ve adalet üzerinde durmuşlardır.

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) önemine vurgu yapmışlardır. Aynı zamanda güvenli işlem için yeni bir ödeme yöntemi veya güven altyapısı oluşturmak için çeşitli veri şifreleme tekniklerinden yararlanılması gerektiği sonucuna varmışlardır.

Obaidat (2007), 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.

Al- Dala'in vd. (2009), çalışmalarında mobil cihaz kullanımı ile çevrimiçi alışveriş yapan kişinin elektronik ödeme yöntemlerine olan güveni arasındaki ilişki üzerinde durmuşlardır. Buna göre elektronik ödeme yöntemlerine duyulan güven,

alışveriş yapan kişinin çevrimiçi satın alma niyetini arttırmaktadır. Ayrıca çalışmadan elde edilen sonuçlarla güvenliği etkin bir mobil cihaz kullanımının benimsenmesi, çevrimiçi alışveriş yapan kişilerin elektronik ödeme yöntemlerine olan güvenini arttırmada doğrudan etkiye sahip olduğu belirtilmiştir (Al-Dala'in vd., 2009: 3132).

Kim vd. (2010), Kim vd. (2010), çalışmalarında algılanan güvenliğin ve duyulan güvenin elektronik ödeme yöntemleri kullanımına etkilerinin yanı sıra, tüketicilerin algılanan güvenliğinin ve duyulan güveninin belirleyicilerini 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 güvenliğini ve duyduğu güveni arttırmada önemli faktörler olduğunu belirtmişlerdir. Aynı zamanda algılanan güvenlik ile duyulan güvenin elektronik ödeme yöntemi kullanımıyla da olumlu bir etkisi olduğu gözlemlenmiştir.

Özkan vd., (2010), çalışmalarında çevrimiçi işlemleri kolaylaştırmanın bir yolu olarak e-ödeme sistemlerinin benimsenmesini kolaylaştıran faktörlerin neler olduğuna dair inceleme yapmışlardır. İnceleme sonucunda güvenlik, güven, algılanan avantaj, güvence mühürleri, algılanan risk ve kullanılabilirliğin, müşterilerin e-ödemeyi benimsemesinde önemli etkenler olarak belirtilmiştir.

Ülgen (2010), çalışmasında elektronik paranın Türkiye ve dünya üzerindeki etkisini inceleyerek elektronik paranın gelecekte fiziki ve banka mevduatlarının yerini alma potansiyeli olduğunu öngörmüş ve elektronik ortamda gerçekleştirilen bankacılık dâhil olmak üzere tüm işlemlerin internet üzerinden kötü niyetli kişilerin mevduat sahiplerinin şifrelerine, hesap bilgilerine erişme gibi bir riskin her zaman göz önünde bulundurmaları gerektiğini belirtmiştir. Bu çerçevede bankacılık alanından inceleyen Ülgen, bankaların hesap sahiplerinin güvenli bir şekilde işlem yapabilmesi için ilgili hesapların sigortalanması gerektiği üzerinde durmuştur (Ülgen, 2010: 87-88).

Zengin ve Güngördü (2013), çalışmalarında elektronik paranın gelişmesinin önündeki en büyük engelin tüketiciler tarafından yeterince kullanılmaması, kullanımı sırasında çeşitli elektronik donanım gerektirmesi ve çeşitli güvenlik sorunlarının çözülememesi olduğunu tespit etmişlerdir. Bu sorunların aşılmasıyla gelecekte kâğıt paranın yerini alabileceğini öngörmüşlerdir.

Angel ve McCabe (2014), çalışmalarında ödeme teknolojisinin zaman içindeki gelişimini incelemişlerdir. Geçen zamanda ödemelerin çoğu ilk dönemlerde altın ve gümüşle yapılırken, gelişen teknolojiyle birlikte artık kâğıt tabanlı ödemelerin yerini

elektronik ödemelerin aldığını vurgulamışlardır. Ödemeler teknolojisindeki devam eden evrimle birlikte oluşan bitcoin'in etik veya etik olmayan kullanımının üzerinde durmuşlardır.

Aigbe ve Akporojo (2014), çalışmalarında güvenlik açığı ve güvenlik seviyesi arasındaki ilişkiyi ve bunların etkilerini inceleyen analiz yapmışlardır. Analiz sonucunda iki veya daha fazla kimlik doğrulama faktörünü içeren kimlik doğrulama mekanizmalarına sahip elektronik ödeme sistemlerinin daha güvenli olma, dolandırıcılık açıklarını azaltma ve kullanıcıların elektronik ödeme sistemlerini kullanma konusundaki güvenini artırma eğiliminde olduğunu belirtmişlerdir.

Duramaz ve Dünder (2014), çalışmalarında Türkiye ve İtalya'yı elektronik ödeme yöntemleri kullanımı bakımından karşılaştırarak Türkiye'deki kartların taksit imkânlarının çok olması ve Türkiye'nin tüketim alışkanlıklarından dolayı kredi kartı ile internet üzerinden yapılan ödemelerin Türkiye'nin İtalya'ya göre daha fazla olduğu üzerinde tespitte bulunmuşlardır. Bu durumda ise ödeme yöntemlerinin denetimi, işleyişi ve diğer düzenlemeler konusunda yetkili otorite olan merkez bankalarının güncel teknolojik gelişmelerle ve elektronik ödeme sistemlerinde ortaya çıkan yeniliklerle altyapılarını bu yeniliklere uydurma zorunluluğunu internet ortamında yapılan alışverişlerde güven ve güvenlik anlamında önemli olduğunu belirtmişlerdir.

Bilir ve Çay (2016), çalışmalarında elektronik para ve finansal piyasalar arasındaki bağlantıyı inceleyerek elektronik ödeme yöntemlerinin teknolojik gelişmelerle birlikte arttığını ve elektronik ödeme sistemlerinde yaşanan gelişim süreciyle oluşan bitcoin gibi, kripto para birimlerinin finansal piyasalar üzerindeki etkisini incelemişlerdir. Bunun sonucunda merkezi bir yapıya sahip olmayan bu para birimlerinin kontrolünü ve kullanımının engellenmesinin zor olduğu ve devletlerin bu para birimleriyle ilgili açık bir politikaya sahip olmamasının karışıklığa neden olabileceği sonucuna varmışlardır.

Bezhovski (2016), çalışmasında internetin gelişmesiyle birlikte oluşan çeşitli elektronik ödeme hizmetleri sistemlerini ve ilgili güvenlik sorunlarını analiz etmiştir. Yapılan araştırmada tüm dünyada yaygın olarak kabul gören ödeme yönteminin oluşabilmesi için elektronik ödeme sistemlerinin çevrimiçi işlemler için yüksek güvenlik sağlayan Güvenli Giriş Katmanı Protokolü (SSL) ve Güvenli Elektronik İşlem(SET) gibi verimli güvenlik protokollerinin izlenmesi gerektiğinin üzerinde durmuştur.

Ekşioğlu (2017), çalışmasında elektronik para kullanımının Türkiye ekonomisine etkilerini incelemiştir. Türkiye’de elektronik ödemelerin arttığını ve bu artışın zaman kaybını ortadan kaldırmakla birlikte internet erişimine zorunlu hale getirdiğini aynı zamanda bireylerin 24 saat alışveriş yapabilmesinin ekonomik yaşamı kolaylaştıran imkânları da beraberinde getirdiğini ve yeni kuşağın teknolojilere daha hızlı adapte olup daha aktif kullandığını belirtmiştir.

Ersoy (2017), çalışmasında çeşitli demografik özelliklere sahip tüketicilerin internet üzerinden alışveriş yapma nedenlerini 500 kişiye anket ileterek analiz gerçekleştirmiştir. Çalışma sonucunda kişinin yaş aralığı, cinsiyeti, gelir, meslek, medeni ve eğitim durumu gibi unsurları tüketim aşamasında farklı tercihler yapmasına neden olduğu görülmüştür.

Halaweh (2017), çalışmasında e-ticaret işlemleri için kullanılan kapıda ödeme modeli üzerinde durmuştur. Son yıllarda e-ticaret işlemleri için geleneksel elektronik ödeme yöntemlerinin aksine, müşterilerin bu yöntemi benimseme niyetini etkileyen faktörleri incelemiştir. Çalışma sonucunda, algılanan güvenlik, gizlilik ve güvenin müşterilerin kapıda ödeme sistemini benimsemeye önemli bir etkiye sahip olduğu sonucuna varılmıştır.

İşler ve Gülaç (2017), çalışmalarında gelişen teknoloji ile birlikte kullanımı artan mobil ödeme sistemindeki güvenlik riskleri üzerinde durmuşlardır. Çalışmada mobil ödemelerde yoğun kişisel ve finansal veri kullanmasından dolayı birçok tehdit ve güvenlik sorunlarıyla karşılaştıkları için internet ödemelerinde SSL ve SET gibi çeşitli güvenlik önlemleriyle korunması gerektiğini 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.

Masuhuddin vd. (2017), elektronik ödeme sistemlerinin avantajları, zorlukları ve güvenlik konuları dâhil olmak üzere çeşitli kavramlar hakkındaki farkındalığı araştırmayı ve arttırmayı amaçlamışlardır. Sundukları bu çalışma ile aynı zamanda elektronik ödeme sistemlerinin benimsenmesini ve bunun bir ulusun ekonomisi üzerindeki etkisini kapsamlı bir anket yaparak değerlendirmişlerdir. Elde edilen verilerde elektronik ödeme sistemlerinin kullanımının ortaya çıkardığı güvenlik sorunlarına rağmen küresel çapta bir ulusun ekonomik kalkınmasına yönelik olumlu

bir adım olarak tanımlamışlardır. Makalede ayrıca daha iyi bir müşteri anlayışı ve memnuniyeti sağlamak amacıyla elektronik ödeme sistemlerini benimsenebilirlik açısından incelemişlerdir.

Dal ve Şahin(2018), çalışmalarında güven faktörünün elektronik ticaretteki etkilerini ve güveni etkileyen faktörlerin satın alma niyetiyle ilişkisini, Trendyol sitesinden alışveriş yapan tüketicilere anket çalışması yaparak incelemiştir. Çalışma sonucunda güveni etkileyen faktörler ile satın alma niyeti ve güven arasında pozitif yönlü bir ilişki olduğu tespit edilmiştir (Dal ve Şahin , 2018: 257).

Ayhan (2018), çalışmasında elektronik ticarete güvenliği konu alarak alıcı ve satıcılar arasında oluşan güvensizliği elektronik ticaretin gelişimini engelleyen başlıca faktörlerden biri olarak görmüştür. Tüketiciler tarafından algılanan güvenlik riskinin en aza indirilmesi için kitle iletişim araçları kullanılarak elektronik ortamda bilinçli ve güvenli alışveriş yolları hakkında tüketiciye bilgi verilmesi elektronik ticaretin gelişmesi açısından önemli olduğu görüşünü belirtmiştir.

Özer vd. (2019), çalışmalarında elektronik ödeme araçlarının kabul düzeyini ve kullanım durumunu anket yoluyla veri toplayarak incelemişlerdir. Yapılan anket çalışmasıyla cinsiyet, yaş, eğitim, teknolojiyi kullanma ihtiyacı ve davranışa dönük niyet gibi faktörlerin elektronik ödeme araçlarını kullanım durumunu etkilediği sonucuna varmışlardır (Özer vd., 2019: 735).

Hassan vd. (2020), çalışmalarında “elektronik ödemelerin kullanımına ilişkin başlıca güvenlik sorunları nelerdir?” ve “güvenli elektronik ödemeler için hangi güvenlik özelliklerinin uyumlu olması gerekir? sorularına sistematik literatür incelemesi yaklaşımıyla elektronik ödemelerin artan kullanımları için güvenlik konularına odaklanmışlardır. Çalışmalardan elde ettikleri sonuçlara göre önemli boşlukların üstesinden gelmek için, elektronik ödemenin kullanılabilirlik, yetkilendirme, bütünlük, inkar etmeme, kimlik doğrulama ve gizlilik gibi bazı koruma özelliklerine sahip olması gerektiğini belirtmişlerdir.

Sonuç olarak araştırılan literatür çalışmalarında görüldüğü gibi genel olarak elektronik ödeme yöntemlerinin ve e-ticaretin güvenilirliği araştırma konusu edilmiştir. Bu tez çalışması ile daha önce literatür çalışmalarında bahsedilen elektronik ödeme yöntemlerindeki güven ve güvenlik algısı kavramları bir arada ele alınacak, anket yoluyla elde edilen verilerle elektronik ödeme yöntemlerine yönelik tüketicilerin güven ve güvenlik algısına dair görüşleri hakkında kapsamlı bir araştırma sunulacaktır.

2.3.1. Bibliyometrik Analiz

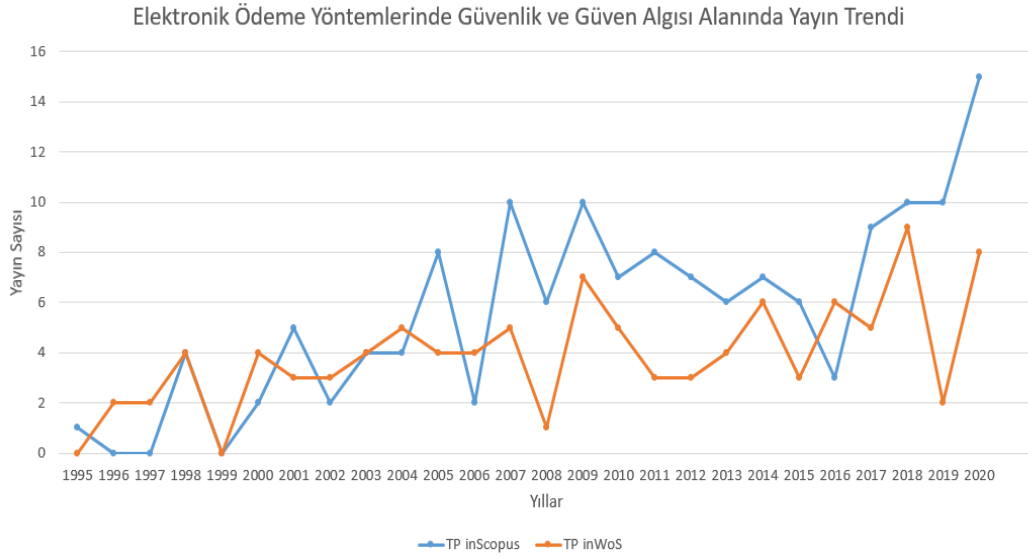
Tüketicilerin elektronik ödeme yöntemlerine yönelik güvenlik ve güven algısı üzerine literatür çalışmasının gerçekleştiği bu kısımda, bilimsel literatürün kapsamını belirlemek ve bu bağlamda global ölçekte konunun ne şekilde ele alındığını gözler önüne sermek için bibliyometrik analiz yapılmış ve bulgulara yer verilmiştir.

Bibliyometrik analiz, bir disipline ait akademik yayınları, anahtar kelimeleri, en üretken ve en çok alıntı yapılan yazarları, yazarların bağlı bulundukları kurumları, üretildikleri ülkeleri, atıfları, yayın yılları ve kaynakları gibi farklı ölçütleri kullanarak matematiksel ve istatistiksel yöntemlerle değerlendirme işlemidir (Pritchard, 1969: 348'den akt. Depren vd. 2018). Değerlendirme sonucunda elde edilen bulgular sayesinde yapılan akademik yayınlardaki gelişmelerin izlenmesi, ülkeler arasında karşılaştırma yapılması, dergilerin yıl bazlı incelenmesi açısından bibliyometrik analiz önem taşımaktadır (Depren vd., 2018: 5).

Çalışmada “e-ödeme yöntemleri”, “e-ödeme yöntemleri kullanımı”, “elektronik ticaret”, “güvenlik” ve “güven” anahtar kelimelerini içeren tüm yayınlar kapsanmıştır. En çok kullanılan iki veri tabanlarından Scopus ve Web of Science (WoS) veri tabanlarında, internet kullanımının 1995 yılından sonra artmasıyla elektronik ticaret ortaya çıktığı için 1995-2020 yılları arasındaki 25 yıllık süreçte yapılmış çalışmalar incelenmiştir. Ana kaynağın belirlenmesi ve literatürün nicel verilerle analizinin tespit edilmesi amacıyla detaylı bir bibliyometrik analiz çalışması yapılmıştır. Bu bölümde gerçekleştirilen analizlerin sonuçları, dönemleri, yayınları, yazarları ve diğer bilgiler yer almaktadır. Analiz için kullanılan verilerin tamamı 31.01.2021 tarihinde toplanmıştır.

Gerçekleştirilen çalışmada Scopus veri tabanında 146 adet yayın taranmıştır. Bu yayınların 69 tanesi makale, 67 tanesi konferans bildirileri, 7 tanesi kitap bölümü ve 3 tanesi basılmakta olan makedir. Web of Science veri tabanında ise 102 adet yayın taranmıştır. Bu yayınların 54 tanesi konferans bildirileri, 46 tanesi makale, 2 tanesi kitap bölümü olarak sunulmuştur. Çalışmada Grafik 5'te yıllara göre kapsama alınan yayın sayıları belirtilmiştir.

Grafik 5: Scopus ve WoS Veri Tabanlarında 1995-2020 Yılları Arasındaki Yayın Sayıları



Grafik 5’te elektronik ödeme yöntemlerinde güvenlik ve güven algısı konusuna yer verilen ilk yıl olan 1995’ten itibaren 2020 yılına kadar yayın sayılarında gerçekleşen gelişim gösterilmektedir. 1999 yılında hiç yayın yapılmamasına rağmen ve 2008 ile 2016 yıllarında çalışmalarda düşüş olsa da günümüze kadar yayın sayısında artış olduğu ve grafiksel eğilimin yukarı yönlü olduğunu söylemek mümkündür. Çalışmanın konusuyla ilgili en çok yayın yapılan yıl ise Scopus’ta 15 adet ve WoS’ta 8 adet olmak üzere toplam 23 adet yayın ile 2020 yılı olmuştur.

Tablo 3, Scopus ve Web of Science veri tabanlarında ayrı ayrı olmak üzere en üretken 10 yazarı göstermektedir. Tabloda bibliyometrik analiz için çeşitli performans göstergeleri çıkarılmıştır. Toplam yayın sayısı – TP (total publication), yayının aldığı toplam atıf sayısı - TC (total citation) ve yayın başına düşen atıf sayısı - CPP (citations per publication), yani toplam atıf sayısının toplam yayın sayısına bölümü şeklinde gösterilmiştir. “H- İndeks ise en az h sayıda atıf alan h sayıda yayını olduğu anlamına gelmektedir. Ayrıca tablolarda görülen R ifadesi sıralamayı belirtmektedir (Muhuri vd., 2019: 219).”

Tabloda görüldüğü üzere veriler toplam yayın sayısına göre sıralansa da ilk 10’da yer alan ve toplam yayın sayıları eşit olan yazarlar için sıralamada etkililik(TC) dikkate alınmış, bir başka deyişle atıf sayılarına göre sıralama yapılmıştır. Luo, S. ve Summons, P. Scopus veri tabanında en üretken yazarlar (TP=3, TC=9, CPP=3) olmalarına karşılık en etkili yazarın Tan, Y.H. olduğu görülmektedir (CPP= 167,5). Atıf sayısının diğer yayınlarla kıyaslandığında bu denli yüksek olmasının nedeni, Tan,

Y.H. (2000) yayınının elektronik ödeme yöntemlerindeki güvenlik ve güven algısı literatürünün ana kaynaklarından biri olmasıyla açıklanabilir. Bununla birlikte Xiong, Q., Web of Science veri tabanındaki en üretken yazardır (TP=4, TC=11, CPP=2,75). En etkili yazarın ise Munoz-Leiva, F. olduğu görülür (CPP=19). Ayrıca yayın sayısına göre yapılan sıralamada 1. sırada 4 yayınıyla Xiong, Q. görülse dahi 10.sırada olan Abrazhevich, D.'in 1 yayınıyla atıf sayısına göre daha etkin olmasını gözden kaçırmamak gerekir.

Tablo 3: En Üretken Yazarlar

Scopus						WoS				
R	Yazarlar	TP	TC	CPP	h- indeks	Yazarlar	TP	TC	CPP	h- indeks
1	Luo, S.	3	9	3	2	Xiong, Q.	4	11	2,75	2
2	Summons, P.	3	9	3	2	Liebana- Cabanillas, F.	3	46	15,33	2
3	Tan, Y.H.	2	335	167,5	2	Sanchez- Fernandez, J.	3	46	15,33	2
4	Tsiakis, T.	2	88	44	1	Yang, Jh.	3	28	9,33	3
5	Obaidat, M.S.	2	69	34,5	1	Chang, Cc.	3	17	5,66	3
6	Bindusara, G.	2	52	26	2	Munoz-Leiva, F.	2	38	19	1
7	Hackney, R.	2	52	26	2	Hassan, M.A.	2	11	5,5	2
8	Halaweh, M.	2	40	20	2	Meng, B.	2	11	5,5	2
9	Salah, K.	2	36	18	2	Brahm, J.	2	6	3	1
10	Al-Dala'in, T.	2	7	3,5	2	Abrazhevich, D.	1	18	18	1

Elektronik ödeme yöntemlerinde güvenlik ve güven algısı konusıyla ilgili yapılan çalışmaların disiplinlere göre her iki veri tabanında da ilk 10 konu alanı Tablo 4'te gösterilmektedir. Tabloya göre Scopus'ta en çok yayın bilgisayar bilimleri alanında yapılmış ve toplam yayınların %41,4'ü bu disiplin içerisinde yer almaktadır. İkinci en çok yayın yapılan alan ise 34 adet yayın ile işletme ve ekonomi alanıdır. Web of Science veri tabanında ise en çok yayın yine bilgisayar bilimleri alanında yapılmış (TP=48) ve tüm yayınların %47,06'sını oluşturmaktadır. Yapılan yayınların sayısında telekomünikasyon, mühendislik, işletme ve ekonomi gibi disiplinler takip etmektedir.

Her iki veri tabanı içinde % (katkı) sütunu %100'ü aşar. Çünkü bir makalenin birden fazla kategorilere ayrılabilmesi durumu mümkündür.

Tablo 4: Elektronik Ödeme Yöntemlerinde Güvenlik ve Güven Algısı Üzerine En Çok Araştırma Yapılan Disiplinler

Scopus			WoS		
Disiplin	TP	%	Disiplin	TP	%
Bilgisayar Bilimleri	106	41,4	Bilgisayar Bilimleri	48	47,06
İşletme ve Ekonomi	34	13.3	Telekomünikasyon	19	18,62
Mühendislik	23	9.0	Mühendislik	17	16,66
Sosyal Bilimler	22	8.6	İşletme ve Ekonomi	16	15,68
Matematik	21	8.2	Yönetim	7	6,8
Karar Bilimleri	16	6,3	Matematik	3	2,94
Ekonometri ve Finans	13	5.1	Sosyal Bilimler	3	2,94
Sanat ve Beşeri Bilimler	5	2,0	Ekonometri ve Finans	2	1,96
Malzeme Bilimi	3	1,2	Bilgi Bilimleri	2	1,96
Tıp Bilimleri	3	1,2	Eğitim Bilimi	2	1,9

Tablo 5'te en üretken ilk 10 ülkenin sıralamasına yer verilmektedir. Scopus veri tabanında Çin, konu ile ilgili 17 adet yayına sahiptir (TC=42, h-index=4). Çin'den sonra en üretken ülkeler olarak Malezya ve ABD gösterilir (TP=14). Ancak iki ülkenin de yayın sayısı eşit olduğundan sıralamada etkililik göz önünde bulundurulmuştur. Buna göre ABD'nin yayın sayısı 14 olsa da toplam atıf sayısına (TC=586) istinaden yayın başına düşen atıf sayısı (CPP=41,85) daha yüksek olduğu için sıralamada ikinci sıradadır, Scopus veri tabanında ABD'den sonra en etkili ülke ise Güney Kore (CPP=33,5) olmuştur. Web of Science veri tabanı incelendiğinde en üretken ülke 24 adet yayın sayısı ile Çin olmuştur (TC=29, h-indeks=3). İspanya ve ABD ise 11 adet yayın sayısı ile ikinci olmuşlardır. Ancak eşitliğin yaşandığı bu durumda etkililik göz önüne alınarak ABD (TC=260 CPP=23,64)'nin 2.sırada olduğu görülür Genel olarak WoS'ta ülkeler arasında inceleme yapıldığında en etkili ülkenin Güney Kore (CPP=33,8) olduğu görülür. Ayrıca yayın sayısı olarak 10.sırada olan Almanya'nın diğer ülkelerle karşılaştırıldığında, Güney Kore'den sonra en etkili 2.ülke konumunda olduğunu yorumlamak mümkündür (CPP=29).

Tablo 5: En Üretken Ülkeler

Scopus						WoS				
R	Ülke	TP	TC	CPP	h-İndeks	Ülke	TP	TC	CPP	h-İndeks
1	Çin	17	42	2,47	4	Çin	24	29	1,21	3
2	ABD	14	586	41,85	10	ABD	11	260	23,64	4
3	Malezya	14	64	4,57	3	İspanya	11	93	8,45	5
4	Avustralya	10	31	3,1	3	Tayvan	10	91	9,1	6
5	Hindistan	9	36	4	4	Hindistan	6	11	1,83	2
6	Birleşik Krallık	9	174	19,33	6	Malezya	5	119	23,8	1
7	İran	8	29	3,62	1	Güney Kore	5	169	33,8	3
8	Güney Kore	8	268	33,5	5	Avustralya	3	10	3,33	2
9	İspanya	6	54	9	2	İngiltere	3	16	5,33	2
10	Pakistan	5	18	3,6	3	Almanya	3	87	29	2

Tablo 6’de Scopus veri tabanında en çok atıf alan yayınların, atıf sayılarının yıllara göre dağılımına yer verilmiştir. Tan ve Thoen (2000), Kim vd. (2010), Tsiakis ve Sthephanides (2004), Obaidat (2007), Smith (2005), Cofta (2007), Özkan vd. (2010), Teoh vd. (2013), Angel ve McCabe (2014), Tan ve Thoen (2000) en çok atıf alan yayınlardır. Toplamda 1019 atıfa sahip yayınların CPP değeri 101,9 olarak gözlemlenmektedir.

Tablo 6: 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, 2007)	30	2	10	9	16	2	69
(Smith, 2005)	61	3	0	0	2	1	67
(Cofta, 2007)	37	7	2	5	1	1	53
(Özkan vd., 2010)	18	7	7	11	6	1	50
(Teoh vd., 2013)	12	9	3	10	13	0	47
(Angel ve McCabe, 2014)	3	3	2	14	12	2	36
(Tan ve Thoen, 2000)	24	2	1	1	1	0	29

Web of Science veri tabanında indekslenen yayınlar incelendiğinde en çok atıf alan yayınların yıllara göre aldığı atıf sayılarına Tablo 7’de yer verilmiştir. Kim vd. (2010), Ooi ve Tan (2016), Bellare vd. (2000), Liebana-Cabanillas vd. (2017), Fan ve Huang (2010), Katsaros (2009), (Abrazhevich (2001), Ogbanufe ve Kim (2018), Esparza vd. (2006), Liebana-Cabanillas vd. (2015) en çok atıf alan yayınlardır. Toplamda 491 atıfa sahip yayınların ortalaması 49,1 olarak gözlemlenmektedir.

Tablo 7: En Çok Atıf Alan Yayınların Yıllara Göre Atıf Dağılımı (Wos)

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
(Fan ve Huang, 2010)	10	0	4	2	3	0	19
(Katsaros, 2009)	13	2	2	1	0	0	18
(Abrazhevich, 2001)	15	1	2	0	0	0	18
(Ogbanufe ve Kim, 2018)	0	0	2	6	7	1	16
(Esparza vd., 2006)	16	0	0	0	0	0	16
(Liebana-Cabanillas vd., 2015)	0	3	5	3	4	0	15

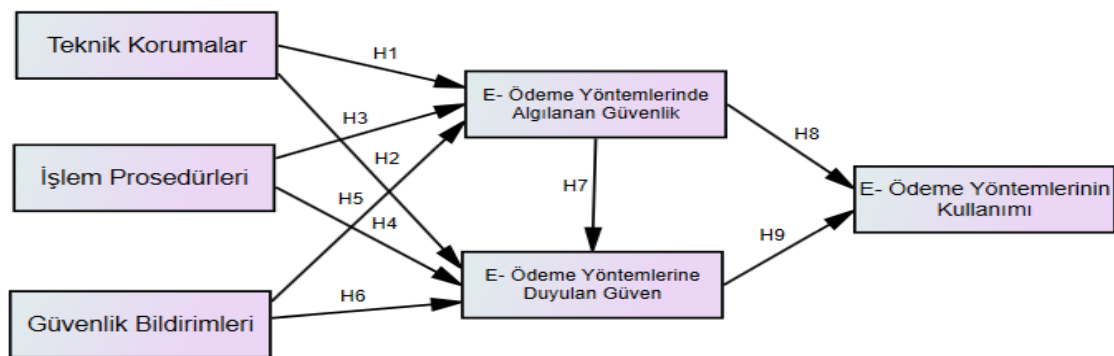
2.4. ARAŞTIRMA HİPOTEZLERİ VE MODEL ÖNERİSİ

Tez 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 yer verilecek, test edilecek hipotezlere ve model önerisine yer verilmektedir.

2.4.1. 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 modelinden yola çıkılmıştır. 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 istediğini azaltabilmektedir (Linck vd., 2006: 3). Bu nedenle, algılanan güvenlik ve duyulan güveni etkileyen faktörleri incelemek bu açıdan önemli olmaktadır. Şekil 6 geliştirilen 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.



2.4.2.1. Elektronik Ödeme Yöntemlerinde Teknik Korumalar

gizlilik, bütünlük ve istikrar ile ilgili bir garanti sunabiliyor olması tüketicilerin elektronik ödemeye olan algılanan güvenliğini seviyesi ve duyduğu güveni arttıracaktır (Lee ve Turban, 2001:78). Barkhordari vd. (2016)'ne göre iyi bir korumaya sahip çevrimiçi bir sistem, tüketicilere daha fazla rahatlık, güvenilirlik ve daha hızlı yanıtlar sağlayarak ödeme yöntemleri kullanımını da geliştirmektedir (Barkhordari vd., 2016: 95).

Hazaee 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). Literatürde araştırmacılar, elektronik ödeme yöntemlerinin güvenliği ile ilgili bazı sorunları değerlendirerek, elektronik ödeme yöntemlerinin güvenlik ihlallerine karşı sertleştirilmesi gerektiğini vurgulamaktadır. Elektronik ödeme işlemlerinin güvenliği, teknik altyapı ve uygulama gibi sistem faktörleri, belirli ve iyi tanımlanmış kurallara göre güvenli ödeme gibi işlem faktörleri ve elektronik işlemler için yasal çerçeve gibi yasal faktörler dahil olmak üzere bir dizi faktöre bağlı olmaktadır. 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.

2.4.2.2. 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).

İşlem prosedürleri, tüketicilerin elektronik ödeme yöntemlerini güvenli ve verimli bir şekilde kullanabilmeleri için kritik öneme sahiptir (Öney vd., 2017: 400). 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). Bu bağlamda, tüketicilerin güvenlik gereksinimlerini karşılamak için iyi tanımlanmış elektronik ödeme yöntem prosedürleri hazırlanmalıdır (Hwang vd., 2007: 184-185). 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 ayrı adım sunmak; (3) ödemenin tamamlanmasının ardından her katılımcıya onay mesajları göndermek (Öney vd., 2017: 400). Başka bir ifadeyle işlem sırasında kullanılan yaygın prosedürler arasında katılımcıların kimlik doğrulaması, işlem boyunca açık adımlar ve her adımın başarıyla sonlandırılmasının açık bir şekilde onaylanması yer almaktadır (Barkhordari vd., 2016: 95). Daha yüksek hizmet kalitesi seviyeleri, tüketicilerin sorunlarının daha hızlı çözülmesine yardımcı olmakta ve bu da çevrimiçi bankacılığın kullanımını kolaylaştırmaktadır (Ahn vd., 2007: 266). Doğru işlem prosedürlerinin algılanan güvenlik ve duyulan güven üzerinde etkisi olacağına inanılmaktadır (Diep, 2020: 2).

Elektronik ödeme çözümlerindeki prosedürler, geleneksel ödeme çözümlerindekilerden farklıdır. Çünkü işlem altyapıları temelde birbirinden farklı olmaktadır. Bu da yetkisiz kullanım ve işlem durumuyla ilgili endişeler dahil olmak üzere bir dizi yeni güvenlik sorunlarına yol açabilmektedir. Elektronik ödeme yöntemleri, geleneksel çevrimdışı işlemlere kıyasla zaman ve alan kısıtlamalarının üstesinden gelme avantajına sahip olsa da, tüketicilerin güvenlik algıları ve yöntemlere karşı duyulan güven, elektronik ödeme yöntemlerinin kullanımını arttırmak için büyük önem taşımaktadır. Bazı araştırmacılar, güvenlik gereksinimlerinin üstesinden gelmek için elektronik ödeme yöntemlerinde karmaşık prosedürlerin ve süreç etkileşimlerinin geliştirilmesi gerektiğini savunmaktadır (Hanzaee ve Alinejad, 2012: 1576). Bu bulgulara dayanarak aşağıdaki 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.

2.4.2.3. Elektronik Ödeme Yöntemlerinde Güvenlik Bildirimleri

Güvenlik bildirimi, elektronik ödeme yöntemleri üzerindeki güvenlik konusunda satıcıların en kesin beyanlarıdır. Bu ifadeler, tüketiciler için kamuya açık bir şekilde yayınlanmaktadır (Diep, 2020: 3). Bir başka ifadeyle, elektronik ödeme yöntemleriyle ilgili güvenlik bildirimlerinin, tüketicilerin elektronik ödeme yöntemlerine karşı duyduğu güveni etkileyen önemli bir faktör olduğu belirtilmektedir (Kim vd., 2010:88; Mukherjee ve Nath, 2003: 7). Kim vd. (2010)'ne göre tüketicileri ödeme seçeneklerinin güvenliği konusunda bilgilendirerek, tüketicilerin elektronik ödeme yöntemlerine dair güvenlik algısını ve duyduğu güveni etkilemek mümkün olmaktadır (Kim vd., 2010:88). Benzer şekilde Miyazaki ve Fernandez (2000), elektronik ödeme yöntemleri üzerine yayınlanan güvenlik bildirimlerinin tüketicilerin internet üzerinden alışveriş yapma olasılığını arttıracaklarını belirtmişlerdir (Miyazaki ve Fernandez, 2000:57). Araştırmacılar ayrıca 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 olduğunu öne sürmektedirler (Hanzaee ve Alinejad, 2012: 1576). Sanayei ve Noroozi (2009) de güvenlikle ilgili endişelere ilişkin açıklamaların ve elektronik ödeme yöntemlerinin web sitelerindeki görünürlüğünün çevrimiçi işlemlerin popülerliğini artırabileceğini belirtmektedir (Sanayei ve Noroozi, 2009: 6). Güvenlik bildirimlerine kolay erişim, elektronik ödeme yöntemlerinin web sitesinde bulunan bildirimler aracılığıyla güvenlik sorunlarının çözülmesi, güvenlik önlemlerinin anlaşılabilirliği ve elektronik ödeme yöntemleri hizmetlerinin günün her saati kullanılabilirliği, güvenlik bildirimlerine erişim noktasında dikkate alınan faktörler arasında yer almaktadır (Barkhordari vd., 2016: 95-96). Tüketicilerin herhangi bir e-ödeme yöntemini kullanma kararları, kendilerine sunulan güvenlik bildirimlerinin kalitesinden önemli ölçüde etkilenmektedir (Öney vd., 2017: 400). Bu bulgulara dayanarak aşağıdaki 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.

2.4.2.4. 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). Diep (2020) algılanan güvenliği, satıcının kimlik doğrulaması, bütünlük, şifreleme ve inkâr etmeme gibi güvenlik gereksinimlerini karşılayacağına dair bir tüketici algısı olarak tanımlamıştır (Diep, 2020: 3). Barkhordari vd. (2006) ise algılanan güvenliği, bir ödeme yönteminin güvenliğinin kişisel deneyimi ve değerlendirilmesi olarak tanımlamıştır (Barkhordari vd., 2016: 97). 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). Algılanan güvenlik seviyesi, tüketicilerin elektronik ödeme yöntemlerinin kullanımına ilişkin kararları üzerinde büyük bir etkiye sahiptir. Bir elektronik ödeme yöntemlerinde algılanan güvenlik seviyesi çok düşükse, tüketicilerin bir işleme girme olasılığı daha düşüktür (Kim vd., 2010: 88). Güvenlik, elektronik ödeme yöntemleri kullanımının önemli tetikleyicilerinden biridir. Güvenlik ve güven, elektronik ödeme yöntemlerini kullanan tüketiciler için ana endişelerdir ve birbirleriyle yakından ilişkilidir (Guan ve Hua, 2003: 516; Linck vd., 2006: 2). Güvenlik ve gizliliğin korunması, kullanıcıların bir teknolojiye olan güveninde büyük bir etkiye sahip olmaktadır. Bilgisayar korsanları ve gizlilik ihlali korkuları, çevrimiçi hizmetleri çevreleyen belirsizliği arttırmaktadır. Çevrimiçi bankacılık kullanımının önündeki en büyük engellerin başında da güvenlik sorunları gelmektedir (Salloum vd., 2019: 70). Elektronik ödeme yöntemleri bu bakımdan yapısal güvenceler sağlayarak tüketicilerin teknolojik altyapılarının ve hizmetlerinin güvenliği ve gizliliği konusunda belirsizliğini azaltabilmektedir (Barkhordari vd., 2016: 97). Bu bulgulara dayanarak 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.

2.4.2.5. 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). Duyulan güven, tüketicinin satıcının yükümlülüklerini iyi niyet olarak beklentilerine göre yerine getireceği inancıdır (Nguyen ve Huynh, 2018: 929). Güven, tüketicinin tedarikçinin belirli özelliklerine ve tedarikçinin gelecekteki olası davranışına ilişkin sahip olduğu bir dizi inanç olarak tanımlanmaktadır (Barkhordari vd., 2016: 97). Güven, tüketicilerin elektronik ödeme yöntemlerinin kullanımını etkileyen en önemli faktörlerden biri olarak tanımlanmıştır ve yüksek düzeyde güvene sahip tüketicilerin elektronik ödeme yöntemlerini kullanmaya daha yatkın olduğu bulunmuştur (Kim vd., 2010: 88). Benzer şekilde Kim vd. (2010) güven olmadan elektronik ödeme yöntemlerinin yaygın kullanım kazanmasının imkansız olduğunu belirtmişlerdir (Kim vd., 2010: 88). Linck (2006)'e göre güven daha yüksek kazanımlar sağlamaktadır (Linck vd., 2006: 8). Al-Dala'in vd. (2009)'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 (Al- Dala'in vd., 2009: 3134). Mallat (2007)'a göre elektronik ödeme yöntemlerine duyulan güvenin müşteri sadakatine olumlu bir etkisi vardır (Mallat, 2007: 417). Tüketicinin bir sistemi kullanma kararı, sistemin güvenilirliğinin kişisel olarak değerlendirilmesinin sonucudur. 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). Salloum vd. (2019)'ne göre elektronik ödeme yöntemlerine olan güven arttıkça, bu tür yöntemlerle ilişkili riskin daha düşük algılandığına inanılmaktadır (Salloum vd., 2019: 71). Bazı araştırmalar, güvenin güvenlikten daha önemli olduğu ve güven duymayan tüketicilerin işlemlerini tamamlamak için elektronik ödeme yöntemlerini kullanmayacağı ortaya koymaktadır (Barkhordari vd., 2016: 97). Bu bulgulara dayanarak aşağıdaki hipotezler oluşturulmuştur:

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



ÜÇÜNCÜ BÖLÜM

ELEKTRONİK ÖDEME YÖNTEMLERİNE YÖNELİK TÜKETİCİLERİN GÜVENLİK VE GÜVEN ALGISININ İNCELENMESİNE DAİR ALAN ARAŞTIRMASI

Araştırmanın bu kısmında elektronik ödeme yöntemlerine yönelik tüketicinin güvenlik ve güven algısı bir araştırma modeli kapsamında incelenecektir. Bu doğrultuda araştırmanın amacı ve kapsamı, yöntemi, kısıtları belirtilecek, ardından verilerin analizi ile ilgili bilgilere ve bulgulara yer verilecektir.

3.1. ARAŞTIRMANIN AMACI VE KAPSAMI

Teknolojide yaşanan gelişmelerle beraber internete erişim olanaklarının ve akıllı telefon kullanımının artması, pandemi gibi çevresel etkenler, tüketicinin geleneksel alışveriş yöntemlerinden online alışverişe yönelmesine neden olmuş, buna bağlı olarak da e-ticaretin önemini arttırmıştır. E-ticaretin geleneksel ticarete göre üretim, maliyet, pazar rekabeti, tedarik, uluslararası rekabet ve dağıtım noktalarında daha üstün olması gelişim sürecini hızlandırmıştır (Civelek ve Sözer, 2003: 117). E-ticaretle birlikte gelişen teknolojiye alışverişlerin mobil cihazlar üzerinden yapılmaya başlanması mobil ticaret (m-ticaret) kavramını ortaya çıkarmıştır (Wu vd., 2010: 531-532). Yaşanan bu gelişmeler tüketicilerin geleneksel ödeme yöntemlerinden elektronik ödemeye geçmesine neden olmuştur. Geleneksel ödeme yöntemlerine kıyasla elektronik ödemenin anonimlik, uygulanabilirlik, dönüştürülebilirlik, birlikte çalışılabilirlik, çoklu para birimi olma, izlenebilirlik, kullanılabilirlik bakımından da özelliklerini sıralamak bu anlamda mümkündür (Abrazhevich, 2004: 33-38; Abrazhevich, 2001:85-86). Bu özelliklerinin yanı sıra tüketicilerin online alışverişlerinde kullandıkları ödeme yöntemlerinin güvenilir olup olmadığı kaygı yaratan bir sorun olarak karşımıza çıkmaktadır.

Bu çalışmanın amacı da teknolojiye gelişmelerle birlikte oluşan elektronik ödeme yöntemlerine dair tüketicilerin duyduğu güven ve bu ödeme yöntemlerine karşı sahip olduğu güvenlik algısının ödeme yöntemlerinin kullanımıyla olan ilişkisini tespit etmeyi amaçlamaktadır. Bu amaç doğrultusunda gerçekleştirilen saha araştırması ve

araştırma sonuçlarıyla hem literatüre katkı sağlamak, hem de uygulayıcılara iş stratejilerinin isabetliliğini artırmada bilimsel bilgi sunmak hedeflenmektedir.

3.2. ARAŞTIRMANIN YÖNTEMİ

Bu çalışmada, alan araştırması yapmak üzere, anket tekniğinden yararlanılarak araştırmanın verileri toplanmıştır. Elektronik ödeme yöntemlerine yönelik tüketicilerin güvenlik ve güven algısını inceleyen bu çalışmada, araştırma evreni Manisa Celal Bayar Üniversitesi'nde lisans eğitimini sürdürmekte olan öğrenciler şeklinde belirlenmiştir. Bu bağlamda ana kütle büyüklüğü toplamda 27.826'dır (CBÜ Öğrenci İşleri, 2021. Erişim Tarihi: 06.06.2021). Çalışmada ana kütle temsil etmesi için örneklem oluşturmak istendiğinde 379 ve daha fazla anketin gerekli olduğu sonucuna anakütle büyüklüğü bilinmesi durumunda kullanılan aşağıdaki formül aracılığıyla ulaşılmıştır. N =popülasyon büyüklüğünü, n =örneklem büyüklüğünü. p =olayın görülüş olasılığı, $q(1-p)$ =olayın görülmemesi olasılığını, t =tablo değerini, d =tolerans seviyesini göstermektedir (Calculator.net, Örnek Boyutu Hesaplayıcı, 2021. Erişim Tarihi: 07.06.2021; Tevfikbulut.com, Olasılıklı Örneklem, 2021. Erişim Tarihi: 27.07.2021; Yazıcıoğlu ve Erdoğan, 2004: 50).

$$n = \frac{N(t)^2_x(p*q)}{d^2(N-1)+t^2(p*q)} = \frac{27.826(1,96)^2_x(0,5*0,5)}{(0,05)^2(27.826-1)+(1,96)^2(0,5*0,5)} = 379$$

Çalışmada kolayda ve kartopu örnekleme yönteminden yararlanılmıştır. Anket için oluşturulan form düzenlemesi "Google Forms" aracılığıyla yapılmıştır. Yapılan anket Manisa Celal Bayar Üniversitesi Etik Kurul'dan onay alınarak 17.01.2021 – 10.03.2021 tarihleri arasındaki süreçte toplam 503 katılımcı tarafından doldurulmuştur.

Anket formunun oluşturulmasında elektronik ödeme yöntemlerine yönelik güvenlik ve güven algısı ile ilgili literatür detaylı 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. Kim vd.'nin (2010) gerçekleştirdikleri araştırma kapsamında geliştirdikleri ölçekten yararlanabilmek için iletişime geçilerek izin alınmıştır (Ek-1). Kim vd.'den (2010) yararlanılarak oluşturulan ölçek maddeleri Ek-

2’de gösterilmektedir. Anket formunda araştırmaya katılan katılımcıların demografik özelliklerini ve tercih ettikleri e-ödeme yöntemleriyle online alışveriş sıklıklarını belirlemeye yönelik sorular dışında, bağımlı ve bağımsız değişkenler için toplamda 29 ifade bulunmaktadır.

Araştırmada iki bölümden oluşan bir anket kullanılmıştır (EK-2). Anketin ilk bölümünde sorular Manisa Celal Bayar Üniversitesi’ndeki lisans eğitimini sürdürmekte olan öğrencilere yönlendirildiği için yaş, eğitim seviyesi ve aylık gelir gibi demografik özelliklerini belirleyici sorular kapsam dışında bırakılarak yalnızca cinsiyet durumu araştırmaya alınmıştır. Bununla birlikte anketi değerlendiren katılımcının, internet sitesinden alışveriş yapma sıklığı ve internet alışverişlerinde en çok kullandığı ödeme yöntemleri şeklinde deneyim ve tercih bilgisine erişebilecek sorular birinci bölümde yer almaktadır.

İkinci kısımda ise bağımlı ve bağımsız değişkenlere yönelik beşli likert tipi ölçeğine göre (1: Kesinlikle Katılmıyorum, 5: Kesinlikle Katılıyorum) toplam 29 ifade için katılımcıların değerlendirme yapması istenmiştir. Toplanan veriler analiz edilmeden önce SPSS 25 istatistik programından yararlanılarak uç değer analizi yapılmıştır. 503 katılımcının verileriyle yapılan bu analiz sonuçları incelendiğinde 13 katılımcının anket verisinin çalışma dışı bırakılması uygun görülmüştür. Kalan 490 katılımcının anket verileri üzerinden çalışma analiz edilmiştir. Modelin testinde ise SPSS ve AMOS programlarından yararlanılmaktadır.

3.3. ARAŞTIRMANIN KISITLARI

Araştırma, elektronik ödeme yöntemlerine yönelik tüketicilerin güvenlik ve güven algısının e-ödeme yöntemlerinin kullanımıyla olan ilişkisini incelemeye yöneliktir. Ancak saha araştırması, zaman kısıtından ötürü, yalnızca Manisa Celal Bayar Üniversitesi’nde lisans eğitimini sürdürmekte olan öğrenciler üzerinde gerçekleştirilebilmiştir. Bu bağlamda zaman baskısından dolayı çalışmanın sadece lisans öğrenimi gören öğrencilerin yaş aralığıyla sınırlı kalması bu çalışmanın en temel kısıtı olmuştur. Araştırmanın bir diğer kısıtlılığı ise çalışmaya katılan 503 katılımcının çoğunluğunun kız öğrencilerden (%58 oranında) oluşması nedeniyle cinsiyet açısından eşit dağılım göstermeyen bir örneklem üzerinden veri toplanmış olmasıdır.

Ayrıca anketin 17.01.2021 – 10.03.2021 tarihlerini kapsamı zaman anlamında bu çalışmanın kısıtlılıkları arasında gösterilebilir.

Ankete yanıt veren katılımcıların, sorulara objektif ve samimi yanıtlar verdikleri kabul edilmiştir. Bununla beraber pandemi sebebiyle bireylerin izole bir şekilde yaşamak durumunda kalması, yüz yüze iletişim imkânını engelleyerek çalışmaların daha çok dijital platformlar aracılığıyla yürütölmeye başlanması üniversite öğrencilerine erişimi de zorlaştırmıştır. Bu bağlamda bireylerle yüz yüze görüşölmeden “Google Forms” aracılığıyla anketin mail üzerinden iletilerek verilerinin toplanması ve katılımcıların anket doldurmadaki isteksizliği gecikmeye neden olduđu için bir diğör kısıt olarak karşımıza çıkmıştır.

3.4. VERİ ANALİZİ VE BULGULAR

Araştırmada elde edilen veriler SPSS (Statistical Package for Social Sciences) for Windows 25.0 ve AMOS (Analysis of Moment Structures) 23.0 programı kullanılarak analiz edilmiştir. Ölçeklerin güvenilirliğini test etmek amacıyla “Güvenilirlik Analizi”, “Madde Toplam Puan Korelasyonu”, yapı geçerliliği test etmek için “Açıklayıcı Faktör Analizi (AFA)”, ve Amos programı kullanılarak yapı geçerliliği test etmek için “Doğrulayıcı Faktör Analizi (DFA)” yapılmıştır. Kurulan model doğrultusunda yol analizleri gerçekleştirilmiştir.

YEM’in yapılabilmesi için veri setinin çok değişkenli normal dağılımı sağlaması gerekmektedir (Byrne, 2001: 98). Bu bağlamda çok değişkenli uç değerler Mahalanobis uzaklık değerleri ile incelenmiştir. Sıfıra yakın veya negatif değerli gözlemlerin bulunduđu çok değişkenli ve yüksek hacimli veri setlerinde aykırı değerlerin tespiti için gözlemler arası ilişkiye dayalı Mahalanobis ölçütü önerilmektedir (Esen ve Timor, 2019: 268).

Aykırı değerler, hata varyansının değerini arttırdığından istatistiksel testlerin güçleri üzerinde de etkili olmaktadır. Bu nedenle istatistiksel testlerden önce aykırı değerler incelenmiş ve veri setlerinde mevcut olup olmadığına bakılmıştır. 503 veri toplanmıştır ve aykırı-uç değerin çıkarılması sonucunda veri sayısı 490’a düşmüştür. Aykırı-uç değerin varlığı Mahalanobis yöntemiyle tespit edilmiş ve bu değerler veri setinden çıkartılarak çoklu normallik kriteri sağlanmıştır.

Kullanılan verilerin normal dağılıma uygunluğu test edilmiştir. Normal dağılıma uygunluk Q-Q Plot çizimi ile incelenebilir (Chan, 2003:280-285). Ayrıca,

kullanılan verilerin normal dağılım göstermesi çarpıklık ve basıklık değerlerinin ± 3 arasında olmasına bağlıdır (Demirağ ve Durmaz, 2019: 707). Yapılan analizde de tüm değişkenler için bu koşul sağlanmış ve bu sayede verilerin normal dağılım gösterdiği tespit edilmiştir.

Çalışmanın bu bölümünde katılımcıların demografik veri ve özellikleri, veri analizine yönelik açıklayıcı istatistikler ve faktör analizi sonuçları yer almaktadır. Hipotezlerin test edilmesi amacıyla kullanılan yapısal eşitlik modellemesinin (YEM) genel uyum ve uyum iyiliği değerleri ile değişkenler arasındaki ilişkiyi gösteren yol analizinin sonuçları ise bulgular başlığı altında yer almaktadır.

3.4.1. Katılımcılara İlişkin Demografik Veri ve Özellikleri

Katılımcıların demografik özelliklerine Tablo 8’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. Araştırmaya katılan katılımcıların özelliklerine göre dağılımı aşağıdaki tabloda verilmiştir. Katılımcıların cinsiyetlerine göre dağılımları incelendiğinde, katılımcıların %58’inin kadın, %42’sinin ise erkek olduğu görülmektedir.

Tablo 8: Demografik Özellikler

Değişkenler	n	%
Cinsiyet	Kadın	284
	Erkek	206
Toplam	490	100.0

Araştırmaya katılan katılımcıların özelliklerine göre dağılımı Tablo 9’da verilmiştir. Katılımcıların internet alışveriş sıklığına göre dağılımları incelendiğinde, katılımcıların %2.7’sinin hemen hemen her gün, %19.8’inin haftada bir kere, %41.2’sinin ayda bir kere, %26.1’inin 2-3 ayda bir defa, %9.6’sının yılda 1-2 defa ve %0.6’sının ise hiç olduğu görülmektedir.

Katılımcıların alışverişte kullandıkları ödeme türlerine göre dağılımları incelendiğinde, katılımcıların %20.8’inin sanal kart, %87.8’inin kredi kartı ya da

banka kartı, %12.2'sinin nakit, %9.6'sının EFT ve havale, %6.5'inin e-cüzdan, %1'inin sanal para ve %1.8'inin paypal cevabını verdiği görülmektedir.



Tablo 9: Araştırmaya Katılan Katılımcıların Özelliklerine Göre Dağılımı

Değişkenler		n	%	
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	

3.4.2. Verilerin Analizi

Veriler analiz edilmeden önce verilerin normal dağılım değerleri incelenmiştir (Tablo 10). Verilerin çarpıklık ve basıklık değerlerinin ± 3 arasında olması normal dağılıma sahip olduğunu göstermektedir (Demirağ ve Durmaz, 2019: 707).

Tablo 10: Araştırmaya Kullanılan Ölçeklerin Normallik Analizi Sonuçları

	Çarpıklık	Basıklık	Durum
İşlem Prosedürleri	-1.504	1.979	Normal
Teknik Koruma	-0.569	0.575	Normal
Güvenlik Bildirimleri	-0.629	0.614	Normal
Algılanan Güvenlik	-0.098	-0.028	Normal
Duyulan Güven	-0.491	0.257	Normal
Kullanım	-0.785	0.137	Normal

Bu değerler gözden geçirildiğinde, verilerin normal dağılım gösterdiği ortaya çıkmıştır. 490 kişinin katılımı ile ulaşılan verilerin faktör analizine uygunluğu test edilmiştir. Açıklayıcı faktör analizi uygulamasından önce, örneklem büyüklüğünün faktör analizi yapmaya uygun olup olmadığını test etmek amacıyla Kaiser-Meyer-Olkin (KMO) test değerleri ile birlikte korelasyon matrisindeki ilişkilerin analizine

uygunluğunu tespit etmek için Bartlett küresellik testi sonuçlarına da bakılmıştır. Analiz sonucunda KMO değerinin 0.899 olduğu belirlenmiştir. Bu sonuç doğrultusunda, örneklem yeterliliğinin faktör analizi yapmak için “yeterli” olduğu sonucuna ulaşılmıştır. KMO değeri olarak 0.5-1.0 arası değerler kabul edilebilir olarak değerlendirilirken, 0.5’in altındaki değerler faktör analizinin söz konusu veri seti için uygun olmadığının göstergesidir (Altunışık vd., 2010: 266). Ayrıca Bartlett Küresellik testi sonuçları incelendiğinde, elde edilen ki kare değerinin kabul edilebilir olduğu görülmüştür ($\chi^2(406) = 8172.925$; $p < 0,05$) (Kaya, 2013: 180).

Kullanılan ölçeğin faktör desenini ortaya koymak amacıyla faktörleştirme yöntemi olarak temel bileşenler analizi, döndürme olarak da dik döndürme yöntemlerinden varimax seçilmiştir. Ölçeğin faktör desenini ortaya koymak amacıyla yapılan açıklayıcı faktör analizinde, 29 maddelik ölçeğin 6 alt boyutu olduğu belirlenmiştir. Bu faktörler toplam varyansın %65.725’ini açıklamaktadır. Çok faktörlü desenlerde, açıklanan varyansın %50’nin üzeri olması yeterli olarak kabul edilir (Büyüköztürk, 2002: 477; Tavşancıl, 2005: 48). Yapılan açıklayıcı faktör analizi sonucunda maddelerin faktör yüklerinin 0.40’ın üzerinde olduğu ve kabul edilebilir olduğu görülmektedir (Acaroğlu, 2014: 12).

Ölçeğin ve boyutlarının güvenilirlikleri ayrı ayrı değerlendirildiğinde, güvenilirlik katsayıları birinci boyut için 0.893, ikinci boyut için 0.824, üçüncü boyut için 0.901, dördüncü boyut için 0.807, beşinci boyut için 0.800, altıncı boyut 0.806 için ve ölçeğin geneli için 0.919 olarak bulunmuştur. Cronbach Alfa değerlerinin 0.60’tan büyük olması, kullanılan ölçeklerin güvenilir olduğunu göstermektedir (Anderson ve Gerbing, 1988). Bu da çalışmada kullanılan ölçeğin içsel tutarlılıklarının iyi olduğunu göstermektedir. Bu araştırmada ölçeğin açıklayıcı analizine istinaden ele alınan değişkenlerin açıklanan varyans değerleri, güvenilirlik katsayıları, öz değerleri ve toplam madde korelasyon değerleri Tablo 11’de verilmektedir.

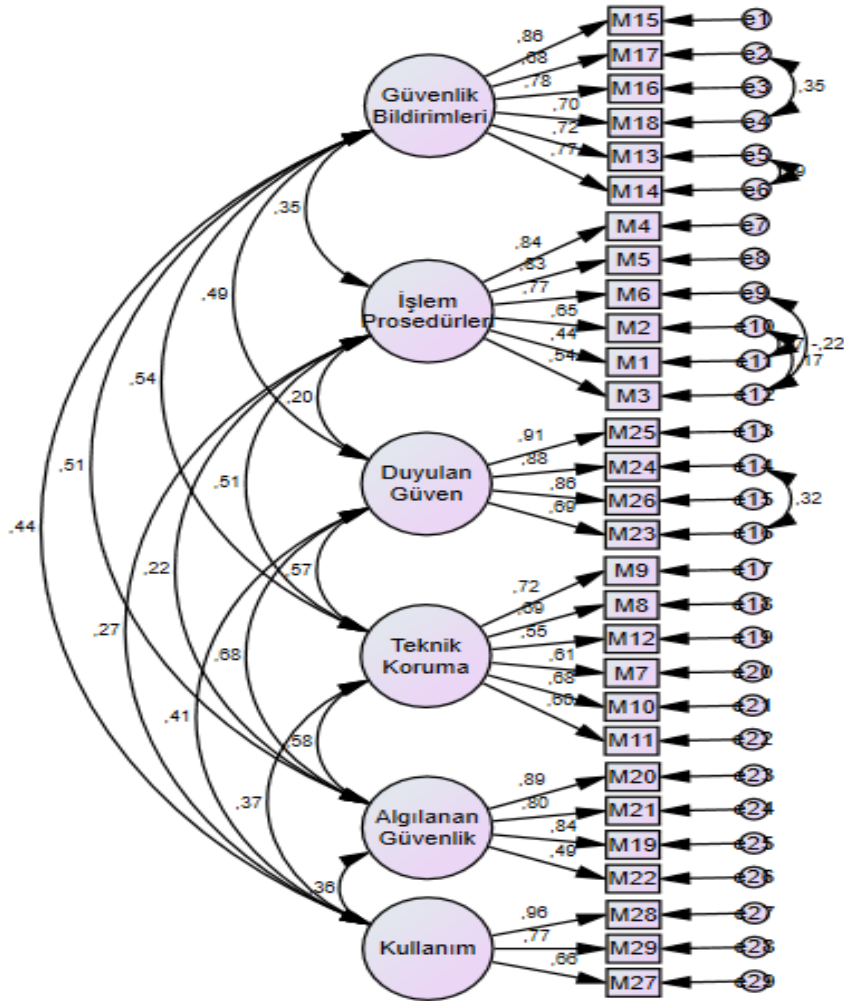
Tablo 11: Araştırmada Kullanılan Ölçeğin Açıklayıcı Faktör Analizi

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							

3.4.3. Ölçüm Modeli, Geçerlilik ve Güvenilirlik

Bu çalışmada kullanılan ölçekler öncelikle güvenilirlik açısından değerlendirilmiştir. Bununla beraber model uyumunun tespit edilebilmesi amacıyla araştırmanın ölçüm modeline doğrulayıcı faktör analizi yapılmıştır (Şekil 7’de gösterilmektedir). Daha sonra, değişkenler arasında ilişkinin gücünü ve yönünün belirlenmesine yönelik olarak yapısal eşitlik modeli uygulanmıştır. Her iki aşamada da Amos 23.0 programı kullanılmıştır.

Şekil 7: Ölçeğin Birinci Düzey Çok Faktörlü Doğrulayıcı Faktör Analizine İlişkin Model



Ölçüm modelinin güvenilirliği, ortalama açıklanan varyans (AVE) ve bileşik güvenilirlik (CR) değerlerine bakılarak sınanmıştır. Ölçüm modelindeki örtük değişkenlerin bileşik güvenilirlik değerinin 0.70 değerinden, ortalama açıklanan varyans değerinin ise 0.40 değerinden yüksek olması gerekmektedir (Dubihlela ve

Dhurup, 2014: 36-37). Tablo 12’de görüldüğü üzere CR değerleri eşik değer olan 0.70 değerinin üzerinde olmakla birlikte, ölçme modelindeki AVE değeri eşik değer olan 0.40 değerinin üstündedir.

Değişkenler arası korelasyonlar incelendiğinde maddelerin faktör yüklerinin 0.40’ın üzerinde olduğu ve tüm korelasyon ilişkilerinin anlamlı olduğu görülmektedir.

Tablo 12: 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

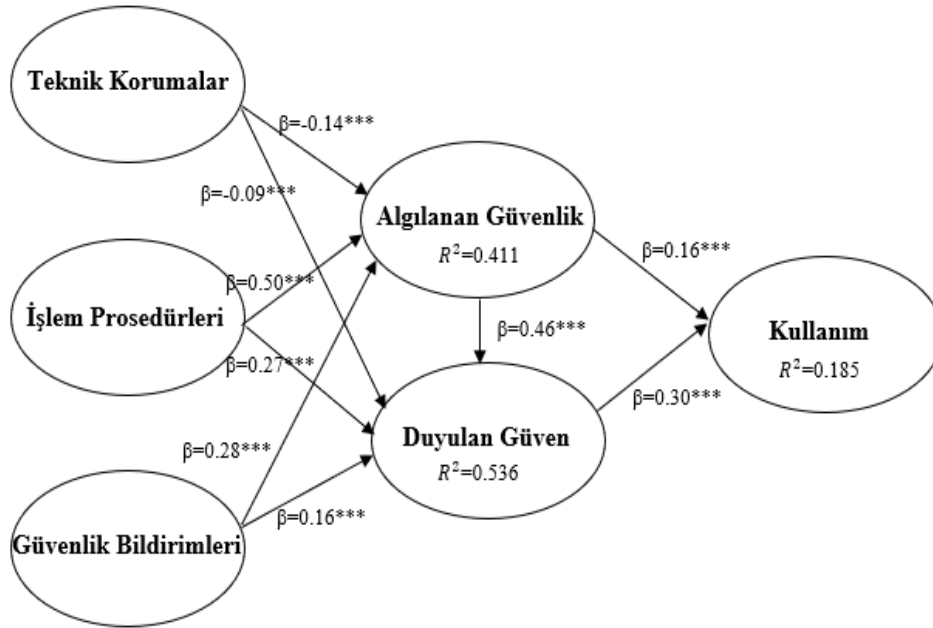
Doğrulamalı faktör analizine göre ölçeğin yapısal denklem model sonucu $p=0.000$ düzeyinde anlamlı olduğu, ölçeği oluşturan 29 madde ve 6 alt boyutun ölçek yapısıyla ilişkili olduğu belirlenmiştir (Tablo 12). Modelde iyileştirme yapılmaktadır. İyileştirme yapılırken uyumu azaltan değişkenler belirlenmiş, artık değerler arasında

kovaryansı yüksek olanlar için yeni kovaryansı oluşturulmuştur. Sonrasında yenilenen uyum indisi hesaplamalarında uyum indisleri için kabul edilen değerlerin sağlandığı Tablo 14’te gösterilmiştir.

3.5. BULGULAR VE TARTIŞMA

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 olanak sağlamaktadır. Değişkenlere ilişkin ölçüm hatalarını görebilmenin yanı sıra doğrudan, dolaylı ve toplam etkilerin görülebiliyor olması da yapısal eşitlik modeli kullanımının avantajları arasında yer almaktadır (Tepe, 2020: 63). Yapısal eşitlik modellemesi yapılırken Amos 23.0 programından faydalanılmıştır. YEM bulguları Şekil 8’de gösterilmektedir.

Şekil 8: Yapısal Eşitlik Modelinin Sonuçları



Yapısal eşitlik modeli ile elde edilen genel uyum değerleri ve tavsiye edilen uyum iyiliği değerleri incelendiğinde; Tablo 13’te görüldüğü üzere modelin kabul edilebilir uyum gösterdiği görülmektedir. Tavsiye edilen uyum iyiliği değerleri Schermelleh-

Engel ve Moosbrugger'ın (2003) alışmasından alınmıştır (Schermelleh-Engel ve Moosbrugger, 2003:52).

Tablo 13: 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 deęişkenlerin aralarındaki ilişkileri deęerlendirmeyi saęlayan yol analizi bulguları Tablo 14'te yer almaktadır. Tabloda yer alan tahminler katsayıları, analize alınan deęişkenlerin aralarındaki ilişkileri göstermektedir. Tabloda gösterilen Beta deęeri (β), bağımsız deęişkenlerle bağımlı deęişkenler arasındaki ilişkilerin incelendięi katsayılardır (Doęan ve Yılmaz, 2017: 391). Modelde yer alan bağımsız deęişkenlerin bağımlı deęişkenler ile ilişki düzeyleri ve bağımlı deęişkenleri açıklama düzeyleri bu katsayı aracılığıyla yorumlanabilmektedir. Yapılan analiz sonucunda, bağımsız deęişkenlerin bağımlı deęişkenler üzerinde istatistiksel olarak anlamlı bir ilişkinin varlığı dikkat çekerken, Beta deęerinin negatif olması negatif yönlü bir ilişkisi olduğunu, pozitif olması pozitif yönlü bir ilişkisi olduğunu göstermektedir. Beta deęerinin sayısal deęeri ise bu etkinin büyüklüęü konusunda fikir vermekte, katsayısının 1'den büyük olması duyarlılık derecesinin yüksek, 1'den küçük olması ise duyarlılık derecesinin düşük olduęu anlamına gelmektedir (Brealey vd., 1997: 265). Örneęin duyulan güvenin kullanım üzerindeki ilişkisinde beta deęeri 0.302 çıkmıştır. Buna göre duyulan güvenin, kullanım durumu üzerinde pozitif yönlü bir ilişkisi vardır. Duyulan güvendeki bir birimlik artış, kullanım durumunda 0.302'lik artışa neden olmaktadır diyebiliriz. Yol analizi sonuçlarına göre araştırmada yer alan hipotezler incelendiğinde de ilişki yönlerinin negatif olması gerekçesiyle H_1 ve H_2 'nin desteklenmedięi görülmektedir.

Tablo 14: 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:

χ^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 H₁ 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 H₂ hipotezi de desteklenmemektedir. Beta katsayısına göre ise ilişkilerin duyarlılık derecelerinin düşük yani ilişkinin zayıf olduğu olduğu görülmektedir ($\beta < 1$). Bu sonuçlar mevcut literatür incelendiğinde Barkhordari vd. (2016), Diep (2020), Hanzae 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 ve ödeme araçlarındaki limitlerinin az olduğu varsayımıyla teknik korumaları çok fazla dikkate almadıkları da bir başka husustur.

İşlem prosedürlerinin tüketicilerin e-ödeme yöntemlerinde algıladığı güvenlik üzerindeki ilişkisi incelendiğinde, analiz sonuçları istatistiksel olarak anlamlı ve pozitif yönde bir etkisi olduğu görülmektedir ($\beta=0.502$, $p<0.05$). Buna göre öne sürülen H_3 hipotezi kabul edilmektedir. Beta katsayısına göre ise ilişkinin duyarlılık derecesinin düşük yani ilişkinin zayıf olduğu olduğu görülmektedir ($\beta<1$). 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 gibi işlem prosedürleri akışının devamlılığı ve bu özelliklerin teknolojik yeniliklere uyumlu olarak geliştirilmesi tüketicilerin algıladığı güvenlik seviyesini arttırarak e- ticaretin gelişimine katkı sağlayacağı beklenebilir.

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 kabul edilmektedir. Beta katsayısına göre ise ilişkinin duyarlılık derecesinin düşük yani ilişkinin zayıf olduğu olduğu görülmektedir ($\beta<1$). Bu sonuçlar literatür incelendiğinde Barkhordari vd. (2016), Diep (2020) ve Hanzaee ve Alinejad (2012)

tarafından yapılan çalışmaların sonuçlarıyla uyumlu iken, Kim vd. (2000) ile Öney vd. (2017) tarafından elde edilen bulgular arasında farklılık gözlemlenmiştir. Yaptığımız analizde elde edilen sonuçlarla birlikte tüketicilerin online alışverişlerinde elektronik ödeme işlemleri aşamasında işlemden önce her katılımcıya kimlik sorgulaması yapmak, tüketicilere ödemenin tamamlanmasına yönelik birkaç ayrı adım sunmak ve ödemenin tamamlanmasının ardından her katılımcıya onay mesajı iletmek gibi işlem prosedürlerinin devamlılığını sağlamak ve işlem prosedürlerini dijital çağa uyumlu bir şekilde hazırlamak tüketicilerin elektronik ödeme yöntemlerine duyduğu güven üzerinde olumlu etki yaratacağı ve bunun sonucunda da e-ticarete yönelme ivme kazandırması beklenebilecektir.

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. Beta katsayısına göre ise ilişkinin duyarlılık derecesinin düşük yani ilişkinin zayıf olduğu olduğu görülmektedir ($\beta<1$). Bu sonuçlar mevcut literatür incelendiğinde Barkhordari vd. (2016), Diep (2020), Kim vd. (2000) ile Miyazaki ve Fernandez (2000) tarafından yapılan çalışmaların sonuçlarıyla uyumlu iken, Hanzae 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 ve sitede güvenlikle ilgili açıklamaların çok fazla teknik kelime içermekten kullanılması gibi güvenlik bildirimleri tüketicilerin elektronik ödeme yöntemlerinde algıladığı güvenliği etkileyerek kullanımlarını arttıracak ve dolayısıyla e- ticaretin de artacağı öngörülmektedir.

Güvenlik bildirimleri ile tüketicilerin e-ödeme yöntemlerine duyduğu güven ilişkisi incelendiğinde, istatistiksel olarak anlamlı, pozitif yönde ve beta katsayısının büyüklüğüne göre zayıf bir ilişki olduğu görülmektedir ($\beta=0.162$, $p<0.05$). Buna göre öne sürülen H_6 hipotezi kabul edilmektedir. Bu sonuçlar mevcut literatür ile uyum göstermekteyken (Barkhordari vd., 2016; Diep, 2020; Kim vd., 2000; Miyazaki ve Fernandez, 2000), Hanzae ve Alinejad (2012) ile Öney vd. (2017) tarafından elde edilen bulgu arasında farklılık gözlemlenmiştir. Çalışmanın bulgularına göre tüketicilerin elektronik ödeme aşamasında güvenlik bildirimlerine kolay erişmesi, elektronik ödeme yöntemlerinin web sitesinde bulunan bildirimler aracılığıyla güvenlik sorunlarının çözülmesi, sitede güvenlikle ilgili açıklamaların dikkati çekecek

şekilde hazırlanarak tüketiciye sunulması gibi unsurların güven sağlaması bakımından elektronik ödeme yöntemleri kullanımında 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, pozitif ve diğer hipotezlerdeki ilişkinin gücüne kıyasla görece yüksek bir ilişkinin varlığına işaret etmektedir ($\beta=0.463$, $p<0.05$). Buna göre H_7 hipotezi kabul edilmektedir. Bu sonuçlar mevcut literatür ile uyum göstermektedir (Barkhordari vd., 2016; Diep, 2020; Hanzae ve Alinejad, 2012; Kim vd., 2000, Maqableh vd., 2015, Öney vd., 2017; Sthephanides, 2005). Çalışmanın bulguları doğrultusunda tüketicilerin elektronik ödeme yöntemlerinde algıladığı güvenlik ne kadar artarsa buna bağlı olarak tüketicinin ödeme yöntemlerine duyduğu güvenin de olumlu yönde etkilendiği ve daha fazla güven duyduğu sonucuna varmak mümkündür. 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 beklenmektedir.

Algılanan güvenliğin tüketicilerin e-ödeme yöntemleri kullanımı üzerindeki ilişkisi incelendiğinde, algılanan güvenliğin tüketicilerin e-ödeme yöntemleri kullanımı üzerinde istatistiksel olarak anlamlı ve pozitif yönde bir etkisi olduğu görülmektedir ($\beta=0.163$, $p<0.05$). Buna göre H_8 hipotezi kabul edilmektedir. Beta katsayısına göre ise ilişkinin duyarlılık derecesinin düşük yani ilişkinin zayıf olduğu görülmektedir ($\beta<1$). Bu sonuçlar mevcut literatür incelendiğinde Barkhordari vd. (2016), Diep (2020), Hanzae ve Alinejad (2012), Kim vd. (2000), Maqableh vd. (2015), Öney vd. (2017) ve Sthephanides (2005) tarafından yapılan çalışmaların sonuçlarıyla uyumlu olduğu gözlemlenmiştir. Çalışmanın bulgularına göre, 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 yöntemlerini kullanarak e-ticaretin gelişimini desteklemesi beklenebilecektir.

Duyulan güvenin tüketicilerin e-ödeme yöntemleri kullanımı ile ilişkisi 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. Beta katsayısına göre

ise ilişkinin duyarlılık derecesinin düşük yani ilişkinin zayıf olduğu görülmektedir ($\beta < 1$). Bu sonuçlar mevcut literatür ile uyum göstermektedir (Barkhordari vd., 2016; Diep, 2020; Hanzae 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.

SONUÇ VE ÖNERİLER

Teknolojik gelişmeler, akıllı telefon sahipliğinin artması, tüketicilerin geleneksel alışverişten online/mobil alışverişe yönelmelerine neden olmuştur. Bununla beraber tüketiciler geleneksel ödeme yöntemlerinden ziyade, online ödeme yöntemlerini yani e-ödeme yöntemlerini tercih etmeye başlamışlardır. Yaşanan bu gelişmeler tüketicilerin online alışverişlerinde kullandıkları elektronik ödeme yöntemlerinin güvenilir olup olmadığı sorusunu gündeme getirmiştir. Bu amaçla çalışma, tüketicilerin elektronik ve mobil ticarete kendilerine sunulan elektronik ödeme yöntemlerine yönelik güvenlik ve güven algısını ve bunların bu araçları kullanımı arasındaki ilişkiyi araştırmaya yönelik yapılmıştır.

Çalışmanın birinci bölümünde internetin ortaya çıkmasıyla birlikte oluşan e-ticaret ve mobil ticaret kavramları incelenmiştir. E-ticarette kullanılan ödeme yöntemleri detaylandırılmış, elektronik ödemenin sınırlamaları, elektronik ödeme yöntemlerinin avantajları ile dezavantajları üzerinde durarak elektronik ödeme yöntemlerindeki yeni trendlerden bahsedilmiştir. Bunun sonucunda pandeminin de etkisiyle e-ticarete olan ilginin dolayısıyla ödeme yöntemlerine olan ilginin de arttığı gözlemlenmiştir. İkinci bölümde teknolojinin gelişmesiyle birlikte e-ödeme yöntemlerinin güvenlik sistemleri ve e-ödemeye karşı duyulan güven konuları literatür taramasına ve bibliyometrik analiz yapılarak detaylı bir şekilde incelenmiştir. Literatürde elektronik ödemelerin arttığını ve bu artışın zaman kaybını ortadan kaldırmakla birlikte internet erişimine zorunlu hale getirdiğini, aynı zamanda bireylerin 24 saat alışveriş yapabilmesinin ekonomik yaşamı kolaylaştıran imkanları da beraberinde getirdiğini ve yeni kuşağın teknolojilere daha hızlı adapte olup daha

aktif kullandığı görülmüştür. Bunun yanında pandeminin de etkisiyle birlikte elektronik ödeme yöntemlerine yönelimdeki artışla, elektronik ödeme yöntemlerindeki güvenlik ve güven konularının akademinin de gündeminde yer aldığı ve yayınların özellikle 2020 yılında yoğunlaştığı gözlemlenmiştir. Bu doğrultuda bir model önerisinde bulunulup, konuyla ilgili hipotezler geliştirilmiştir. Üçüncü ve son bölümde ise çalışmanın amacına, kapsamına, yöntemine ve kısıtlarına yer vererek veri analizi oluşturularak elde edilen bulgulara yer verilmiştir.

Bu tez çalışması ile daha önce literatür çalışmalarında bahsedilen elektronik ödeme yöntemlerine yönelik duyulan güven ve algılanan güvenlik kavramları anket yoluyla lisans öğrencilerinden alınan veriler ile daha kapsamlı incelenmiştir. Yapılan çalışmada algılanan güvenlik ve duyulan güvenin belirleyici faktörlerini ve bu iki değişkenin elektronik ödeme yöntemleri kullanımı üzerindeki ilişkisini betimleyen bir araştırma modeli önerilmiş ve test edilmiştir. Ayrıca araştırma hipotezleri incelendiğinde sadece teknik koruma değişkeninin algılanan güvenlik ve güven ile ilişkisine dair geliştirilen hipotezler desteklenmemiş, diğer tüm hipotezler tüketicinin e-ödeme yöntemlerine yönelik güvenlik ve güven algısı ile bunların kullanımı arasında pozitif bir ilişkinin var olduğu bulgularıyla, çalışmanın örnekleme doğrultusunda desteklenmiştir. Bulgularımızda hem işlem prosedürlerinin hem de güvenlik bildirimlerinin tüketicilerin algılanan güvenliğini ve duyulan güveni arttırmak için önemli faktörler olduğunu göstermektedir. Tüketicilerin algılanan güvenliği, tüketicilerin duyulan güveni ve elektronik ödeme yöntemleri kullanımı ile pozitif ilişkilidir. Son olarak tüketicilerin algılanan güveni ve elektronik ödeme yöntemleri kullanımı üzerinde olumlu bir etkiye sahiptir.

Modelin testinin ardından elde edilen bulgular şu şekilde belirtilebilmektedir.

Yapılan ankette değerlendirilmeye alınan verilere göre elde edilen sonuçlar 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 büyük yöntem olmuştur. Dolayısıyla lisans öğrencilerine uyguladığımız anket sonuçlarına göre bu yaş aralığındaki bireylerin genel olarak internet ortamından kopmadan online olarak da alışverişlerini yapmayı tercih ettikleri sonucuna ulaşılmıştır.

Çalışmadaki analiz verileri göz önüne alındığında yapılan araştırma, algılanan güvenlik ve duyulan güvenin elektronik 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 güvenliğini tetiklemenin yollarını aramalıdır. 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 yoğunlaşmalıdır. Aynı zamanda kullanıcıların kişisel bilgilerinin (isim, adres, telefon numarası, kredi kartı numarası vb.) güvende tutulmasını ve transferlerin hızlı ve güvenilir olmasını sağlamalıdır. Ayrıca sonuçlar, kullanıcıların kendilerini güvende hissetmeleri ve elektronik ödeme yöntemlerine güvenmeleri için kullanıcı dostu, kullanımı kolay ve sorunsuz sistemlere ihtiyaç duyduklarını da göstermiştir.

Elde edilen verilerle tüketicinin elektronik ödeme yöntemlerine duyduğu güven ve algılanan güvenlik konusunda hem akademisyenler için teorik birikime hem de elektronik ödeme yöntemlerinin güvenlik yönleriyle ilgilenen uygulamacılara yaratılacak bilgi ile katkı sağlaması bakımından önem taşımaktadır.

Bu çalışma, teknolojik ilerlemelere paralel olarak elektronik ödeme yöntemlerinde güvenlik ve güven alanına önemli teorik ve pratik katkılar da sağlamaktadır. 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 faktörleri, 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. Ayrıca elektronik ödeme yöntemlerinde güvenlik ve güven hakkında daha ayrıntılı bilgi veren diğer faktörlere odaklanmak için daha fazla araştırma yapılması da önerilebilir. Gelecekteki diğer çalışmalarda dijitalleşmenin hız kazandığı ortamda elektronik ödeme yöntemlerine olan güven ve güvenlik algısına yönelik tutumları çeşitli güvenlik araçlarıyla bu kapsamda değişen ve gelişen yapısı göz önüne alındığında bu çalışmanın zaman içerisinde tekrarlanmasının bulguların güvenilirliğini arttırarak literatürün gelişmesine

katkıda bulunacağı da öngörülmektedir. Gelecekte farklı yaş grupları/kuşaklar üzerinde çalışmanın gerçekleştirilmesi, farklı demografik özelliklere sahip tüketicilerin e-alışveriş sırasındaki yolculuklarını tasarlamada anlamlı çıktılar üretebilecektir.



KAYNAKÇA

Abrazhevich, D. (2001). Classification and Characteristics of Electronic Payment Systems. Lecture Notes in Computer Science. 81-90.

Abrazhevich, D. (2004). Electronic Payment Systems: A User-Centered Perspective and İnteraction Design. Eindhoven: Technical University of Eindhoven Phd Thesis.

Acaroğlu, R. (2014), Florence Nightingale Hemşirelik Dergisi, Revize Edilen Hemşirelerin Mesleki Değerleri Ölçeği Türkçe Formunun Güvenirlik ve Geçerliği. 22(1): 8-16.

Ahn, T., Ryu , S. ve Han, I. (2007). The Impact of Web Quality and Playfulness On User. Information ve Management. 44(3): 263-275.

Aigbe, P. ve Akpojar, J. (2014). Analysis of Security Issues in Electronic Payment. International Journal of Computer Application. 108(10): 10-14.

Akpunar, E. N. (2017). Türkiye'de Elektronik Dış Ticaretin Gelişimi ve İstihdam İlişkisi. Harran Education Journal. 2(2): 18-32.

Al-Dala'in, T., Summons, P. ve Luo, S. (2009). The Relationship between a Mobile Device and a Shopper's Trust for E-payment Systems . The 1st International Conference on Information Science and Engineering, 3132-3135.

Aliyev, A. (2019). Dünya'da ve Azerbaycan'da Ödeme Sistemleri. İstanbul: Marmara Üniversitesi Bankacılık ve Sigortacılık Enstitüsü Yüksek Lisans Tezi.

AL-Maaitah, M. ve Shatat, A. (2011). Empirical Study in the Security of Electronic Payment Systems. International Journal of Computer Science Issues. 8(4): 393-401.

AL-Maaitah, T. A., Osman, A., Suberi, M., AL-Maaitah, D. ve AL-Dhmour, F. (2015). Review Study On The Security Of Electronic Payment Systems. International Journal of Economics, Commerce and Management. 3(9): 821-829.

Alptekin, V. (2016). Makro Ekonomi. Konya: Eğitim Kitabevi.

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: Areview and recommended two-step Approach. Psychological Bulletin, 103(3): 411-423.

Angel, J. ve McCabe, D. (2014). The Ethics of Payments: Paper, Plastic, or Bitcoin? Journal of Business Ethics. 132(3): 603-611.

Ardiansah, M. N., Chariri, A., Rahardja, S. ve Udin. (2020). The Effect of Electronic Payments Security on E-Commerce Consumer Perception: An Extended Model of Technology Acceptance. Management Science Letters. 10(7): 1473-1480.

Asokan, N., Janson, P., Steiner, M. ve Waidner, M. (2000). Electronic Payment Systems. Research Report. IBM Research Division. 1-16.

Avunduk, H. ve Aşan, H. (2018). Blok Zinciri(Blockchain) Uygulamaları: Genel Bir Değerlendirme. Dokuz Eylül Üniversitesi İktisadi ve İdari Bilimler Dergisi. 33(1): 369-384.

Ayhan, A. (2018). Elektronik Ticaret ve Türkiye'de Online Ödeme Sistemleri Üzerine Bir Sanal Pos Uygulaması. Konya: Karatay Üniversitesi Fen Bilimleri Enstitüsü Yüksek Lisans Tezi.

Aytekin, A. ve Yücel, Y. B. (2017). Yeni Ödeme Teknolojilerinin İş Hayatına Etkileri. Avrasya Sosyal ve Ekonomi Araştırmaları Dergisi (ASEAD).4(12): 93-115.

Bankacılık Düzenleme ve Denetleme Kurulu. (2021). Türkçe Mevzuat Düzenleme Taslakları, https://www.bddk.org.tr/websitesi/turkce/mevzuat/duzenleme_taslaklari/13479karttebligi, (30.03.2021).

Bankalararası Kart Merkezi. (2020). BKM Ekspres, <https://bkm.com.tr/urunler-ve-hizmetler/bkm-ekspres/>, (14.03.2021).

Bankalararası Kart Merkezi. (2018). Türkiye Kartlı Ödemeler Raporu, https://bkm.com.tr/wp-content/uploads/2015/06/BKM-FAAL%C4%B0YET-RAPORU-2018_bask%C4%B1_.pdf, (03.04.2020).

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): 89-116.

Belanger, F., Janine, S. ve Wanda, J. (2002). Trustworthiness in Electronic Commerce: The Role of Privacy, Security and Site Attirubutes. Journal Of Strategic Information Systems. 11(3-4): 245-270.

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): 611-627.

Bezhovski, Z. (2016). The Future of the Mobile Payment as Electronic Payment System. European Journal of Business and Management. 8(8): 127-132.

Bilir, H. ve Çay, Ş. (2016). Elektronik Para ve Finansal Piyasalar Arasındaki İlişki. Niğde Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi. 9(2): 21-30.

Brindle, M. ve Cox, R. (2004). Law of Bank Payments. Londra: Sweet & Maxwell.

Brealey R.A., Myers S.C. ve Marcus A.J. (1997). İşletme Finansının Temelleri. İstanbul: Literatür Yayıncılık.

Büyüköztürk, Ş. (2002). Faktör Analizi: Temel Kavramlar ve Ölçek Geliştirmede Kullanımı. Kuram ve Uygulamada Eğitim Yönetimi Dergisi. (32): 470- 483.

Byrne, B. M. (2001). Structural Equation Modeling With Mplus. New York: Rotledge Taylor & Francis Group.

Calculator.net. (2021). Örnek Boyutu Hesaplayıcı, <https://www.calculator.net/sample-size-calculator.html?type=1&cl=95&ci=5&pp=50&ps=27826&x=55&y=5>, (07.06.2021).

Canpolat, Ö. (2001). E-Ticaret ve Türkiye'deki Gelişmeler. Ankara: T.C. Sanayi ve Ticaret Bakanlığı Hukuk Müşavirliği.

Castro, D., Atkinson, R. ve Ezell, S. (2010). Embracing the Self-Service Economy. The Information Technology & Innovation Foundation. 1-54.

Celal Bayar Üniversitesi Öğrenci İşleri Daire Başkanlığı. (2021). 2020-2021 Öğrenci Sayıları, İstatistik, http://ogrenciisleri.cbu.edu.tr/db_images/file/OgrenciSayilari/2020-2021%20kampus_baz%C4%B1nda_ogrenci_say%C4%B1lar%C4%B1.pdf, (06.06.2021).

Chan, D.W. (2003). Hardiness and its Role in The Stres- Burnout Relationship Among Prospective Chinese Teachers in Hong Kong. Teaching and Teacher Education. 19(4): 381-395.

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): 358-368.

Chung, K.-C. ve Holdsworth, D. (2012). Culture and Behavioural İntent to Adopt Mobile Commerce Among the Y Generation: Comparative Analyses Between Kazakhstan, Morocco and Singapore. Young Consumers. 13(3): 224-241.

Civelek, M., & Sözer, E. G. (2003). İnternet Ticareti Yeni Ekososyal Sistem ve Ticaret Noktaları. İstanbul: Beta Basım Yayım.

Çağlar, Ü. (2007). Elektronik Para: Enformasyon Teknolojisindeki Gelişmeler ve Yeni Ödeme Sistemleri. Sosyal Bilimler Dergisi. 9(17): 177-186.

Dal, N. E. ve Şahin , Ö. (2018). Elektronik Ticarete Güven Oluşturan Faktörlerin Satınalma Niyeti İle İlişkisi: Trendyol Alışveriş Sitesi Müşterileri ile Bir Araştırma. Avrasya Sosyal ve Ekonomi Araştırmaları Dergisi(ASEAD). 5(12): 240-259.

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): 695-726.

Depren, Ö., Kartal, M. T. ve Kılıç Depren, S. (2018). Borsalarda Oynaklık Üzerine Yayınlanmış Akademik Çalışmaların Bibliyometrik Analizi. Bankacılık ve Sermaye Piyasası Araştırmaları Dergisi. 2(6): 1-15.

Diep, L. T. (2020). Retention Using Electronic Payment Systems: An Empirical. Journal of Physics: Conference Series.(1793): 1-9.

Dinler, Z. (2015). İktisada Giriş. Ankara: Ekin Kitabevi.

Diostech. (2021). Kioks Sistemleri, <http://dios.com.tr/sayfa/7/kiosk-sistemleri#.YKazJagzZPY>, (19.05.2021).

Doğan, V. ve Yılmaz, C. (2017). Yönetim Bilimleri ve Pazarlama Alanında Bağımsız Değişkenlerin Karşılaştırılması ve Bastırıcı Etki Tespiti. Uluslararası Yönetim İktisat ve İşletme Dergisi. 13(2): 385-406.

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): 33-41.

Dündar, S. ve Duramaz, S. (2014). Elektronik Ödeme Sistemlerinin Karşılaştırılması: Türkiye ve İtalya Örneği. Uşak Üniversitesi Sosyal Bilimler Dergisi. 7(1): 24-37.

E- Ticaret Bilgi Platformu. (2021). 2020 Yılı E- Ticaret Verileri- İstatistikler, <https://www.eticaret.gov.tr/istatistikler>, (08.05.2021).

Ekici, K. M. (2013). E-Ticaret. Ankara: Savaş Kitap ve Yayınevi.

Ekşioğlu, E. (2017). Elektronik Para Kullanımının Ekonomik Etkileri(Türkiye Üzerinde Bir Uygulama). Sivas: Cumhuriyet Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmış Doktora Tezi.

Erbaşlar, G. ve Dokur, Ş. (2016). Elektronik Ticaret. Ankara: Nobel Akademik Yayıncılık.

Erden, R. S. (2014). Elektronik Ticaret ve Dış Ticarete Etkisi. İstanbul: Marmara Üniversitesi Sosyal Bilimler Enstitüsü Yüksek Lisans Tezi.

Erdoğan, C. (2004). Avrupa Birliği'nde Elektronik Ödeme Sistemlerindeki Gelişmeler. Bankacılar Dergisi. (48): 80-92.

Eren, D. B. (2020). Alışverişlerde Temassız Kredi Kartı Kullanım Niyetini Etkileyen Unsurların Belirlenmesi: Nesnelerin İnterneti Kavramının Bankacılık Yansıması. Bankacılar Dergisi. (115): 107-128.

Ersoy, E. (2017). Tüketicilerin Değişen Alışveriş Alışkanlıkları. İletişim Çalışmaları Dergisi. 3: 87-129.

Ersoy, Z. (1999). Elektronik Ticaret ve Ticaret Noktaları. Ankara: İGEME.

Esen, M. F. ve Timor, M. (2019). Çok Değişkenli Aykırı Değer Tespiti İçin Klasik Ve Dayanımlı Mahalanobis Uzaklık Ölçütleri: Finansal Veri İle Bir Uygulama. Uluslararası İktisadi ve İdari İncelemeler (UİİİD) Dergisi. (25): 267-282.

Esparza, O., Mun˜oz, J. L., Soriano, M., ve Forne, J. (2006). Secure Brokerage Mechanisms For Mobile Electronic Commerce. Computer Communications. 29(12): 2308-2321.

Fan, C.-I. ve Huang, V.-M. (2010). Provably Secure Integrated On/Off-Line Electronic Cash for Flexible and Efficient Payment. IEEE Transactions on Systems. 40(5): 567-579.

Fatonah, S. ve Wibowo, F. W. (2018). A Review of E-Payment System in E-Commerce. Journal of Physics. 1140: 1-7.

Gökgül, M. (2014). Türkiye' de Elektronik Ticaret ve İşletmelere, Tüketicilere Sağladığı Avantajlar, Dezavantajlar. İstanbul: Kültür Üniversitesi Sosyal Bilimler Enstitüsü Yüksek Lisans Tezi.

Guan, S. ve Hua, F. (2003). A Multi-Agent Architecture for Electronic Payment. International Journal of Information Technology & Decision Making. 2(3): 497-522.

Gupta, M. P. ve Dubey, D. (2016). E-Commerce- Study of Privacy, Trust and Security from Consumer's Perspective. International Journal of Computer Science and Mobile Computing. 5(6): 224-232.

Gururajan, R. (2006). A Discussion on Security Risks in Mobile Commerce. e-Business Review. 7(2): 1-14.

Günel, M. (2010). Para Banka ve Finansal Sistem. İstanbul: Nobel Akademik Yayıncılık.

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 . 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): 1575-1581.

Hasiloğlu, S. B. (2003). Elektronik Ticaret ve Stratejileri. Denizli: Türkmen Kitabevi.

Hassan, M. A., Shukur, Z., Hasan, M. K., ve Al-Khaleefa, A. S. (2020). A Review on Electronic Payments Security. *Symmetry*.12(8):1-24.

Hoofnagle, C. J., Urban, J. ve Li, S. (2012). Mobile Payments: Consumer Benefits and New Privacy Concerns. *SSRN Electronic Journal*. 1-19.

Hwang, R. J., Shiau, S. H. ve Jan, D. F. (2007). A New Mobile Payment Scheme for Roaming Services. *Electronic Commerce Research and Applications*. 6(2): 184-191.

Isaac, J. T. ve Zeadally, S. (2014). Secure Mobile Payment Systems. *IEEE Computer Society*. 16(3): 36-43.

İşler, B. ve Gülaç, H. (2017). Mobil Ödemeler, Güvenlik Sorunları ve Çözüm Önerileri. *BDDK Bankacılık ve Finansal Piyasalar Dergisi*. 11(2): 53-86.

İyzico. (2020). Temassız Ödeme Hakkında Merak Edilenler, <https://www.iyzico.com/blog/temassiz-odeme-hakkinda-merak-edilenler/>, (30.03.2021).

Kabir, M. A., Saidin, S. ve Ahmi, A. (2015). Adoption of e-Payment Systems: A Review of Literature. *International Conference on E-Commerce*. 113-120.

Kalyoncuoğlu, S. (2018). Tüketicilerin Online Alışverişlerindeki Sanal Kart Kullanımlarının Teknoloji Kabul Modeli İle İncelenmesi. *Afyon Kocatepe Üniversitesi Sosyal Bilimler Dergisi*. 20(2): 193-213.

Katsaros, P. (2009). A Roadmap to Electronic Payment Transaction Guarantees and A Colored Petri Net Model Checking Approach. *Information and Software Technology*. 51(2): 235-257.

Kaya, F. (2009). Türkiye'de Kredi Kartı Uygulaması. İstanbul: Türkiye Bankalar Birliği.

Kaya, M. F. (2013). Sürdürülebilir Kalkınmaya Yönelik Tutum Ölçeği Geliştirme Çalışması. *Marmara Coğrafya Dergisi*. (28): 175-193.

Kayalıderen, D. ve Çetiner, M. (2018). Monitoring National Payment Schemes: Some Global Practices and Turkish Payment Scheme – Troy. *Journal of Business in The Digital Age*. 2(1): 67-75.

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): 84-95.

Kniberg, H. (2002). What Makes a Micropayment Solution Succeed. Sweden: Kungliga Tekniska, Institution for Applied Information Technology Höskolan Masters Thesis.

Koenigstorfer, J. ve Groeppel-Klein, A. (2012). Consumer Acceptance of the Mobile Internet. *Mark Lett*. (23): 917-928.

Konuk, F. A. ve Yıldırım, E. (2012). Sanal Kart Bilinirliği Üzerine Bir Araştırma: Sakarya İlinde Bir Uygulama. 11. Ulusal İşletmecilik Kongresi. 85-87.

Krishna, K. ve Shanmugam, V. (2018). Usage of E-Payment and Customer Satisfaction. Indian Journal of Public Health Research & Development. 9(3): 130-133.

Lee, M.K.O. ve Turban, E. (2001). A Trust Model for Consumer Internet Shopping. International Journal of Electronic Commerce. 6(1): 75-91.

Licina, A., Radtke, H. ve Johansson, C. (2018). Usability in M-Commerce. Boras: University of Boras Bachelor's Thesis in Informatics.

Liebana-Cabanillas, F., Munoz-Leiva, F. ve Sanchez-Fernandez, J. (2015). Payment Systems in New Electronic Environments: Consumer Behavior in Payment Systems via SMS. International Journal of Information Technology and Decision Making. 14(2): 421-449.

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): 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. 1-11.

Mallat, N. (2007). Exploring Consumer Adoption of Mobile Payments – A Qualitative Study. Journal of Strategic Information Systems.16(4): 413-432.

Maqableh, M., Masa'deh, R., Shannak, R. ve Nahar, K. (2015). Perceived Trust and Payment Methods: An Empirical Study of MarkaVIP Company. Int. J. Communications, Network and System Sciences. 8(11): 409-427.

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): 1-18.

Mathur, D. (2017). A Survey of Awareness about Security in E-payment System. International Journal Of Engineering and Information Technology. 5(3): 1846-1850.

McKnight, D. ve Chervany, N. (2001). What Trust Means in E-Commerce Customer Relationships: An Interdisciplinary Conceptual Typology. International Journal of Electronic Commerce. 6(2): 35-39.

Meng, B. ve Xiong, Q. (2004). Research on Electronic Payment Model . The 8th International Conference on Computer Supported Cooperative Work in Design Proceedings. 597-602.

Miyazaki, A. D. ve Fernandez, A. (2000). Internet Privacy and Security: An Examination of Online Retailer Disclosures. Journal of Public Policy & Marketing. 19(1): 54-61.

Muhuri, P. K., Shukla, A. ve Abraham, A. (2019). Industry 4.0: A Bibliometric Analysis and Detailed Overview. *Engineering Applications of Artificial Intelligence*. 78: 218-235.

Mukherjee, A. ve Nath, P. (2003). A Model of Trust in Online Relationship Banking. *International Journal of Bank Marketing*. 21(1): 5-15.

Mlkt, U. (2017). Elektronik Ticarete Mobil Uygulamaların Denetimi ve Vergisel Boyutu. İstanbul: İstanbul Ticaret niversitesi Sosyal Bilimler Enstits Yksek Lisans Tezi.

Nakamoto, S. (2008). Bitcoin: Peer to Peer Electronic Cash System. 1-9.

Nguyen, T. D. Ve Huynh, P. A. (2018). The Roles of Perceived Risk and Trust on E-Payment Adoption. *Studies in Computational Intelligence*. 760: 926-940.

Niranjanamurthy , M., Kavyashree , N., Jagannath, S. ve Chahar, D. (2013). Analysis of E-Commerce and M-Commerce: Advantages, Limitations and Security issues. *International Journal of Advanced Research in Computer and Communication Engineering*. 2(6): 2360-2370.

Niranjanamurthy, M. (2014). E-commerce: Recommended Online Payment Method - PayPal. *International Journal of Computer Science and Mobile Computing*. 3(7): 669-679.

Obaidat, M. ve Boudriga, N. (2007). Introduction to E-Security. *Security of e-Systems and Computer Networks*. 3-24.

Ogbanufe, O. ve Kim, D. J. (2018). Comparing Fingerprint-based Biometrics Authentication versus Traditional Authentication Methods for e-Payment. *Decision Support Systems*. 106: 1-14.

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: 33-46.

Organ, İ. ve avdar, F. (2012). Elektronik Ticaretin Vergilendirilmesinde Uluslararası Alanda Yaşanan Sorunlar. *IUYD*. 3(1): 64-84.

ney, E., kszoęlu Gven, G. ve Rizv, W. (2017). The Determinants of Electronic Payment Systems Usage From Consumers' Perspective. *Economic Research-Ekonomska Istraživanja*. 30(1): 394-415.

zbaş, M. Y. (2019). Elektronik Para ve Sanal Para: Bitcoin Geleceęin Para Birimi Olabilir Mi? *İşletme Ekonomi ve Ynetim Araştırmaları Dergisi*. 2(1): 85-104.

zer, A. C., Poyraz, E. ve Kızıgın, Y. (2019). Nakitsiz Toplum Yaratmada Elektronik deme Araçlarının Benimsenmesi. *Business & Management Studies: An International Journal*. 7(2): 735-755.

Özgener, Ş. (2004). Kobi'lerin E-Ticarette Karşılaştıkları Sorunların Çözümüne Yönelik Alternatif Stratejiler. 6(22): 167-181.

Özkan, S., Bindusara, G. ve Hackney, R. (2010). Facilitating The Adoption of E-Payment Pysystems: Theoretical Constructs and Empirical Analysis. Journal of Enterprise Information Management. 23(3): 305-325.

Öztürk, N., ve Koç, A. (2006). Elektronik Para, Diğer Para Türleriyle Karşılaştırılması ve Olası Etkileri. SÜ İİBF Sosyal Ve Ekonomik Araştırmalar Dergisi. 6(11): 207-243.

Panurach, P. (1996). Money in Electronic Commerce: Digital Cash, Electronic Fund Transfer, and Ecash. Communications ACM. 39(6): 45-50.

Párhonyi, R., Nieuwenhuis, L. ve Pras, A. (2006). The Fall and Rise of Micropayment Systems. Enschede : University of Twente.

Pirinççi, A. E. (2018). Yeni Dünya Düzeninde Sanal Para Bitcoin'in Değerlendirilmesi. International Journal of Economics Politics Humanities and Social Sciences. 1(1): 45-52.

Polasik, M., Wisniewski, T. ve Lightfoot , G. (2012). Modelling Customers Intentions to Use Contactless Cards. Int. J. Banking, Accounting and Finance. 4(3): 1-45.

R.C.Mayer, Davis, J. ve Schoorman, F. (1995). An Integrative Model of Organizational Trust. 20(3): 709-734.

Rehman, M. H., Salah, K., Damiani, E. ve Svetinovic, D. (2019). Trust in Blockchain Cryptocurrency Ecosystem. IEEE Transactions On Engineering Management. 1-17

Reisoğlu, S. (2004). Banka Kredi Kartları ve Uygulama Sorunları. Bankacılar Dergisi. 49: 100-123.

Rob, M. A. ve Opara, E. (2003). Online Credit Card Processing Models: Critical Issues to Consider by Small Merchants. Human Systems Management. 22: 133-142.

S.M.Furnell ve Karweni, T. (1999). Security İmplications of Electronic Commerce: A Survey of Consumers and Businesses. Published in Internet Research. 9(5): 372-382.

Sanayei, A. ve Noroozi, A. (2009). Security of Internet Banking Services and its Linkage with Users' Trust. International Conference on Information Management and Engineering. 3-7.

Salloum, A. S., Al-Emran, M., Khalaf, R., Habes, M. ve Shaalan, K. (2019). An Innovative Study of E-Payment Systems Adoption in Higher Education: Theoretical Constructs and Empirical Analysis. International Journal of Interactive Mobile Technologies (iJIM). 13(6): 68-83.

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): 23-74.

Serhateri, A. (2015). Elektronik Ticarete Güvenliğin Tüketicilerin İnternet Üzerinden Alışveriş Yapma Tutumlarına Etkisi: Kocaeli Örneği. *Karedeniz Dergisi*. 27: 227-249.

Shafie, I. S., Yusof, Y., Mahmood, A., Ishar, N., Jamal, H. ve Kasim, N. (2018). Factors Influencing the Adoption of E-Payment: An Empirical Study in Malaysia. *Advances in Business Research International Journal*. 4(2): 53-62.

Sharma, N. ve Patterson, P. (2000). Switching Cost, Alternative Attractiveness and Experience as Moderators of Relationship Commitment in Professional, Cunsomer Services. 11(5): 470-490.

Singh, A., Singh, K., Shahazad ve Chandra, M. (2012). A Review: Secure Payment System for Electronic Transaction. *International Journal of Advanced Research in Computer Science and Software Engineering*. 2(3): 237-243

Sırma, İ. (2002). Elektronik Ticaret Stratejileri. İstanbul Üniversitesi. *Aksan Bülteni*. 94-106.

Smith, S. W. (2005). *Trusted Computing Platforms: Design And Applications*. Boston: Springer Science + Business Media, Inc.

Sönmez, A. (2014). Sanal Para Bitcoin. *The Turkish Online Journal of Design, Art and Communication – TOJDAC*. 4(3): 1-14.

Suwunniponth, W. (2016). Customers' Intention to Use Electronic Payment System for Purchasing. *International Scholarly and Scientific Research & Innovation*. 10(12): 3925-3930.

Şeker, M. (2011). Elektronik Ödeme Sistemleri. İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi. 10(20): 55-73.

Tan, Y.-H. ve Thoen, W. (2000). Toward a Generic Model of Trust for Electronic Commerce. *International Journal of Electronic Commerce*. 5(2): 61-74.

Tan, Y. H. ve Thoen, W. (2000a). An Outline Of A Trust Model for Electronic Commerce. *Applied Artificial Intelligence: An International Journal*. 14(8): 849-862.

Tariq, K. R., Bakhtyar, R., Forsyth, D. ve Johni, R. (2017). Security Aspects in Online Purchasing Applications. *KJAR*. 2(3): 1-3.

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

- T.C. Sağlık Bakanlığı COVID- 19 Bilgilendirme Platformu. (2020). COVID- 19 nedir? <https://covid19.saglik.gov.tr/TR-66300/covid-19-nedir-.html>, (09.05.2021).
- Teoh, W. M.-Y., Chong, S., Lin, B. ve Chua, J. (2013). Factors Affecting Consumers' Perception of Electronic Payment: An Empirical Analysis. *Internet Research*. 23(4): 465-485.
- Tepe, G. (2020). Fonksiyonel ve Sembolik Faydanın Mobil Hizmetlerin Kullanım Niyeti Üzerindeki Etkisi: Mobil Hizmet Kalitesi Açısından Bir İnceleme. Ankara: Ankara Üniversitesi Sosyal Bilimler Enstitüsü Yüksek Lisans Tezi.
- Tevfikbulut.com. (2021). Olasılıklı Örneklem. Tabakalı Örneklem Üzerine Bir Simülasyon Çalışması, <https://tevfikbulut.com/tag/olasilikli-orneklem/>, (27.07.2021).
- Ting, H., Yacob, Y., Liew, L. ve Lau, W. (2016). Intention to Use Mobile Payment System: A Case of Developing Market by Ethnicity. *Procedia - Social and Behavioral Sciences*. 224: 368-375.
- Tsiakis, T. ve Sthephanides, G. (2005). The Concept of Security and Trust in Electronic Payments. *Computers&Security*. 24(1): 10-15.
- Tsiakis, T., Stephanides, G. ve Pekos, G. (2005). Trust and Security in Electronic Payments: What We Have and Need to Know? *Proceedings Of World Academy Of Science, Engineering And Technology*. 5:147-150.
- Türkiye İstatistik Kurumu (TÜİK). (2019). Hanehalkı Bilişim Teknolojileri Kullanım Araştırması, [https://data.tuik.gov.tr/Bulten/Index?p=Hanehalki-Bilisim-Teknolojileri-\(BT\)-Kullanim-Arastirmasi-2018-30574](https://data.tuik.gov.tr/Bulten/Index?p=Hanehalki-Bilisim-Teknolojileri-(BT)-Kullanim-Arastirmasi-2018-30574), (21.03.2020).
- Turban, E., ve Brahm, J. (2000). Smart Card-Based Electronic Card Payment Systems in the Transportation Industry. *Journal of Organizational Computing and Electronic Commerce*. 10(4): 281-293.
- Türk Dil Kurumu (TDK). (2020). Türk Dil Kurumu Sözlükleri, <https://sozluk.gov.tr/>, (04.05.2020).
- Türkiye Cumhuriyet Merkez Bankası(TCMB). (2014). Ödeme Sistemleri Türkiye'de Ödeme Sistemleri, <https://www.tcmb.gov.tr/wps/wcm/connect/a28ff0bd-1e9a-42be-8f7d-3249a1b3cf1c/OdemeSistemleri.pdf?MOD=AJPERES>, (30.03.2020).
- UNCTAD (2021). Covid-19 and E-Commerce: A Global Review. New York: United Nations Publications, https://unctad.org/system/files/official-document/dtlstict2020d13_en_0.pdf, (08.05.2021).
- 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 (08.05.2021).

Ülgen, K. (2010). Elektronik Para: Türkiye ve Dünya Uygulaması. Malatya: İnönü Üniversitesi Sosyal Bilimler Enstitüsü Yüksek Lisans Tezi.

Wang, Y. M. (2008). Determinants Affecting Consumer Adoption of Contactless Credit Card: An Empirical Study. *Cyberpsychology & Behavior*. 11(6): 687-689.

Wibowo, F., A, Y. ve S, F. (2018). A Review of E-Payment System in E-Commerce. *Journal of Physics: Conference Series*. 1140: 1-8.

Wu, X., Chen, Q. ve Zhou, W. (2010). A Review of Mobile Commerce Consumers' Behaviour Research: Consumer Acceptance, Loyalty and Continuance. *Int. J. Mobile Communications*. 8(5): 528-560.

Yahid, B., Shahbahrami, D. ve Nobakht, D. (2013). Providing Security for E-Wallet using E-Cheque. *International Journal of Information Science and Management*. 86-96.

Yapı Kredi Bankası. (2021). Güvenli Alışveriş, 3D-Secure, <https://www.worldcard.com.tr/world-dunyasi/guvenli-alisveris/3d-secure>, (23.04.2021).

Yazıcıoğlu, Y. ve Erdoğan, S. (2004). SPSS Uygulamalı Bilimsel Araştırma Yöntemleri. Ankara: Detay Yayıncılık.

Yükçü, S. ve Atağan, G. (2014). Anadolu'da İlk Paranın Ayar ve Alışımı. *Muhasebe ve Finans Tarihi Araştırmaları Dergisi*. (7): 28-48.

Yüksel, A. ve Bozkurt, E. (2015). Elektronik Para, Sanal Para, Bitcoin ve Linden Doları'na Hukuki Bir Bakış. *İstanbul Üniversitesi Hukuk Fakültesi Dergisi*. 73(2): 173-220.

Zengin, B. ve Güngördü, A. (2013). Elektronik Ödeme Sistemlerinin Olası Etkileri Üzerine Bir İnceleme. *Gazi Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*. 15(3): 129-150.

EK1:

ANKET FORMU

Değerli Katılımcı;

Bu anket, Manisa Celal Bayar Üniversitesi Sosyal Bilimler Enstitüsü Ekonomi ve Finans Anabilim dalında öğrenci olan Helin Aslan'ın "Elektronik Ödeme Yöntemlerine Yönelik Tüketicinin Güvenlik ve Güven Algısının İncelenmesi" adlı tez çalışması için yapılmakta olup tüketicilerin elektronik ödeme yöntemlerine göre güvenlik ve güven algısının araştırılmasına katkı sağlayacaktır.

Araştırma bilimsel bir nitelik taşıdığından derlenen bilgiler gizli tutulacaktır. Sorulara objektif ve samimi cevaplar vereceğinize inanıyorum. Değerli katkılarınız için şimdiden teşekkür ederiz.

Tez Danışmanı

Unvanı Adı Soyadı: Dr.Öğr. Üyesi Asiye Ayben ÇELİK

Görev yeri/Kurum adresi MCBÜ İşletme Fakültesi

Araştırmacı

Adı Soyadı: Helin Aslan

Lütfen soruları tam olarak okuduktan sonra kendinize en uygun olan cevabı işaretleyiniz.

1.BÖLÜM

Bu bölümde, soruları parantez içindeki boşluklara çarpı (X) işareti koyarak cevaplandırınız.

CİNSİYET
☐ KADIN ☐ ERKEK
İNTERNET SİTESİNDEN ALIŞVERİŞ YAPMA SIKLIĞI
☐ HEMEN HEMEN HER GÜN
☐ HAFTADA BİR KERE
☐ AYDA BİR KERE
☐ 2 3 AYDA BİR DEFA
☐ YILDA BİR İKİ DEFA
☐ HİÇ

İNTERNET ALIŞVERİŞLERİNDE EN ÇOK KULLANILAN ÖDEME YÖNTEMİ
☐ KREDİ KARTI VE BANKA KARTI
☐ EFT VE HAVALE
☐ SANAL KART
☐ NAKİT
☐ E-CÜZDAN
☐ SANAL PARA
☐ PAYPAL

2.BÖLÜM

Bu bölümde, elektronik ödeme yöntemlerine yönelik tüketicinin güvenlik ve güven algısının incelenmesi amacıyla çeşitli maddeler verilmiştir. Lütfen bu soruları 1) Kesinlikle katılmıyorum 2) Katılmıyorum 3) Kararsızım 4) Katılıyorum 5) Kesinlikle katılıyorum seçeneklerinden birine çarpı (X) işareti koyarak cevaplandırınız.

	SORULAR	KESİNLİKLE KATILMIYORUM	KATILMIYORUM	KARARSIZIM	KATILIYORUM	KESİNLİKLE KATILIYORUM
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.					

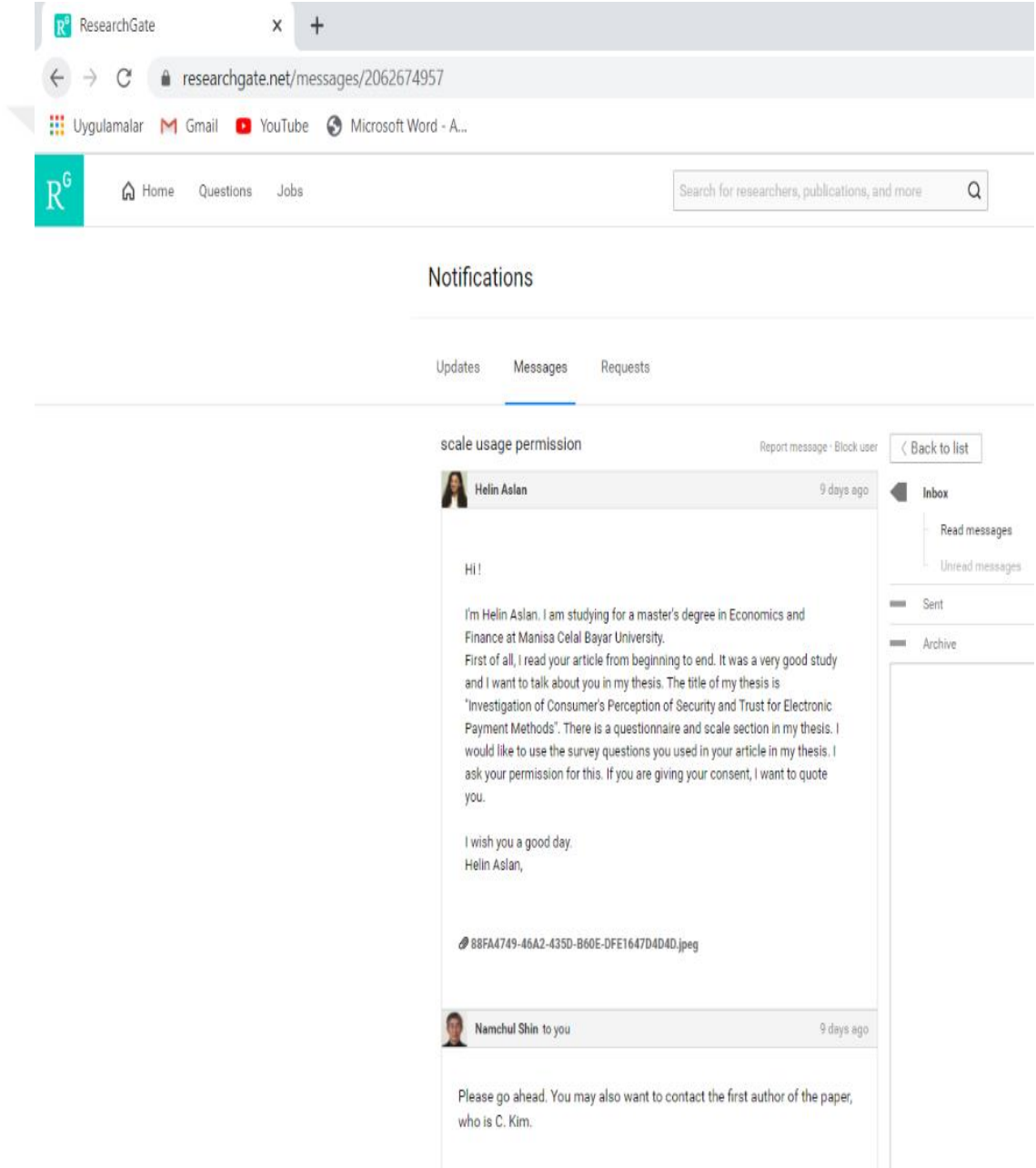
	6. Ödemenin gerçekleştirildiğinden emin olmak için size sms, e-posta gibi yöntemlerle onay mesajı gönderilir.					
TEKNİK KORUMA	7. Kişisel bilgileriniz (hesap bilgisi, iletişim bilgisi gibi) elektronik ödeme sistemi kullanılmasından dolayı daha önce hiç çalınmadı.					
	8. Kişisel bilgileriniz başka 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.					

EK2:

ÖLÇEK KULLANIM İZNİ

Ölçeklerin kullanımıyla ilgili ölçek sahipleriyle Researchgate web sitesi üzerinden iletişime geçilerek izin alınmıştır. Yapılan yazışmalara dair görseller aşağıda sunulmaktadır.



x
+

archgate.net/messages/2062674957

il
YouTube
Microsoft Word - A...



Helin Aslan
8 days ago

thank you so much. However, I could not reach the first author at c.kim@ynu.ac.kr e-mail address. Do you know the e-mail address I can take you to cc? I can send an explanatory mail again.



Namchul Shin to you
2 days ago

I understand you couldn't reach him. His email address seems not working. I lost his contact as well. So just go ahead and use the survey instrument for your thesis.



Helin Aslan
2 days ago

I want your permission to use your scales in my thesis. If you are giving your consent, I want to quote you.

I wish you a good day.
Helin Aslan



Namchul Shin to you
2 days ago

Yes. I give you my permission.



Helin Aslan
2 days ago

Thank you for everything. I wish you a good day..



Namchul Shin to you
2 days ago

Wish you good luck for your thesis.

117

EK3:

T.C.
MANİSA CELAL BAYAR ÜNİVERSİTESİ REKTÖRLÜĞÜ
SOSYAL VE BEŞERİ BİLİMLER BİLİMSEL ARAŞTIRMA VE YAYIN ETİK
KURULU KARARLARI

Toplantı Tarih	: 19.11.2020
Toplantı Sayısı	: 2020/ 11
Toplantıda Alınan	
Karar Sayısı	: 10

Sosyal ve Beşeri Bilimler Bilimsel Araştırma ve Yayın Etik Kurulu 19.11.2020 tarih ve saat 11:00'da Rektörlük Yönetim Kurulu Toplantı odasında toplanmış, aşağıdaki kararlar alınmıştır.

KARAR:

- 4- MCBÜ İşletme Fakültesi Öğretim Üyesi Dr. Öğr. Üyesi Asiye Ayben ÇELİK'in 16.10.2020 tarih ve E.34836 sayıda kayıtlı MCBÜ Sosyal Bilimler Enstitüsü Ekonomi ve Finans Anabilim Dalı Yüksek Lisans öğrencisi Helin ASLAN'ın "Elektronik Ödeme Yöntemlerine Yönelik Tüketicinin Güvenlik ve Güven Algısının İncelenmesi" adlı tez araştırmasının etik yönden uygunluğuna toplantıya katılan üyelerin oy birliği ile karar verildi.

(e-imzalıdır)

Prof.Dr.Ramazan GÖKBUNAR
Başkan

(e-imzalıdır)

Prof.Dr.Fatma ŞAŞMAZ ÖREN
Üye

(e-imzalıdır)

Prof.Dr.Nurettin GÜLMEZ
Üye

Prof.Dr.Osman Murat KOÇTÜRK
Üye
(Katılmadı)

(e-imzalıdır)

Prof.Dr.Doğan UYSAL
Üye- Başk. Yard

(e-imzalıdır)

Prof.Dr.Mustafa MIYNAT
Üye

(e-imzalıdır)

Prof.Dr. Kenan ERDOĞAN
Üye