

**T.C.
YALOVA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ**

**SOSYAL MEDYA VE E-TİCARET KULLANICILARININ GİZLİLİK VE
GÜVEN ALGILARININ DEĞERLENDİRİLMESİ: TÜRKİYE – ABD
KARŞILAŞTIRMASI**

YÜKSEK LİSANS TEZİ

Erkan ÇETİNTAŞ

**Enstitü Anabilim Dalı: İşletme
Enstitü Bilim Dalı: İşletme**

Tez Danışmanı: Doç. Dr. İkrâm DAŞTAN

KASIM 2018

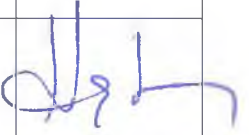
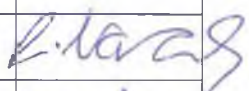
T.C.
YALOVA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ

SOSYAL MEDYA VE E-TİCARET KULLANICILARININ GİZLİLİK VE
GÜVEN ALGILARININ DEĞERLENDİRİLMESİ: TÜRKİYE – ABD
KARŞILAŞTIRMASI

YÜKSEK LİSANS TEZİ
Erkan ÇETİNTAŞ (147201015)

Enstitü Anabilim Dalı: İşletme
Enstitü Bilim Dalı: İşletme

Bu tez 26/11/2023 tarihinde aşağıdaki jüri tarafından oybirliği/oyçokluğu ile kabul edilmiştir.

	Adı SOYADI	Kanaati			İmza
Jüri Başkanı (Danışman)	Doç. Dr. İbrahim DAŞTAN	☒ Kabul	☐ Düzeltme	☐ Ret	
Jüri Üyesi	Doç. Dr. Berrak NARİCİ	☒ Kabul	☐ Düzeltme	☐ Ret	
Jüri Üyesi	Dr. Öğr. Üyesi Kemal DEMİR	☒ Kabul	☐ Düzeltme	☐ Ret	

SOSYAL BİLİMLER ENSTİTÜSÜ
YÜKSEK LİSANS / DOKTORA İNTİHAL YAZILIM RAPORU
BEYAN BELGESİ

Tez Başlığı: Sosyal Medya ve E-Ticaret Kullanıcılarının Gizlilik ve Güven Algılarının Değerlendirilmesi: Türkiye – ABD Karşılaştırması

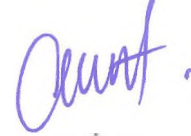
Yukarıda başlığı belirtilen tez çalışmamın toplam 105 sayfalık kısmına ilişkin aşağıda belirtilen filtrelemeler uygulanarak alınmış olan ve 26/11/2018 tarihinde aşağıda ismi yazılı araştırma görevlisi tarafından şahsıma iletilen turnitin intihal tespit programı raporuna göre tezimin benzerlik oranı % 10'dur.

Uygulanan filtrelemeler:

1. Kaynakça hariç,
2. Alıntılar dâhil,
3. 5 kelimeden daha az örtüşme içeren metin kısımları hariç.

Bu bilgiler doğrultusunda tez çalışmamın herhangi bir intihal içermediğini; aksinin tespiti halinde doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi ve yukarıda vermiş olduğum bilgilerin doğru olduğunu beyan ederim.

Gereğini saygılarımla arz ederim.



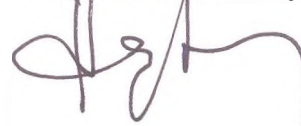
İmza

Adı SOYADI : Erkan ÇETİNTAŞ
Öğrenci Numarası : 147201015
Ana Bilim Dalı : İşletme
Programı : İşletme
Türü : () Proje (x) Yüksek Lisans Tezi () Doktora Tezi

Taramayı Yapan Arş. Gör.
(Adı Soyadı, İmzası, Tarih)
Zafer AY


26.11.2018

Danışman
(Adı Soyadı, İmzası, Tarih)
Doç. Dr. İkrâm DAŞTAN


26.11.2018

ÖNSÖZ

Araştırmanın tüm aşamalarında her türlü desteği esirgemeyen ve yakın ilgi gösteren danışmanım Doç. Dr. İkrâm DAŞTAN'a sonsuz teşekkürlerimi sunarım. Ayrıca araştırmanın uygulama aşamasında yardımcı olan Arş. Gör. Cem GÜRLER ve Arş. Gör. Zafer AY'a da desteklerinden ötürü teşekkür ederim.

Özellikle araştırmanın anket çalışmasına bizzat katılan ve arkadaş çevrelerini de katılmaya teşvik eden başta ağabeyim Gürkan ÇETİNTAŞ olmak üzere tüm arkadaş ve dostlarıma da teşekkürlerimi sunmayı bir borç bilirim.

Son olarak, hayatımın her döneminde yanımda yer alan, her kararında beni destekleyen, sevgisini ve hoş görüşünü eksik etmeyen annem Ayşe ÇETİNTAŞ ve babam Ersan ÇETİNTAŞ ile duaları ile beni destekleyen anneannem Zeynep DEMİR'e şükran ve minnetlerimi sunar, çalışmanın tüm araştırmacılara faydalı olmasını temenni ederim.

Erkan ÇETİNTAŞ

26.11.2018

İÇİNDEKİLER

BEYAN	i
ÖNSÖZ.....	ii
İÇİNDEKİLER	iii
KISALTMALAR LİSTESİ.....	v
TABLolar LİSTESİ.....	vi
ŞEKİLLER LİSTESİ.....	vii
ÖZET.....	viii
SUMMARY	ix
GİRİŞ	1
BÖLÜM 1: ARAŞTIRMANIN ÇERÇEVESİ	5
1.1. Araştırmanın Problemi	5
1.2. Araştırmanın Amacı ve Önemi	5
1.3. Araştırmanın Katkıları.....	6
BÖLÜM 2: KAVRAMSAL ÇERÇEVE VE LİTERATÜR	9
2.1. Gizlilik ve Güvenlik	9
2.1.1. Bilgi Gizliliği ve Güvenliği	9
2.1.2. İnternette Gizlilik ve Güvenlik	10
2.1.3. Bilgi Gizliliği ve Kişisel Verilerin Korunması Kanunları	13
2.2. Sosyal Medya ve E-Ticaret	17
2.2.1. Sosyal Medya ve Gelişimi	18
2.2.2. Sosyal Medya Uygulamaları.....	20
2.2.3. E-Ticaret ve Gelişimi	25
2.2.4. E-Ticaret Uygulamaları.....	28
2.3. Sosyal Medya ve E-Ticarete Gizlilik ve Güvenlik	31
2.3.1. Sosyal Medya’da Gizlilik ve Güvenlik Sorunları	32
2.3.2. E-Ticarete Gizlilik ve Güvenlik Sorunları.....	37
2.4. Sosyal Medya ve E-Ticaret Kullanımında Gizlilik ve Güvenliğe Etki Eden Faktörler	40
2.4.1. Gizlilik ve Güvenlik Farkındalığı	41
2.4.2. Gizlilik ve Güvenlik Endişesi	42
2.4.3. Olumsuz Deneyimler	44
2.4.4. Güven Algısı	45

2.4.5. Risk Algısı	47
2.4.6. Kullanıcı Davranışı	48
BÖLÜM 3: ARAŞTIRMA YÖNTEMİ VE METODOLOJİ	53
3.1. Araştırma Yöntemi	53
3.2. Örneklem ve Verilerin Toplanması	53
3.3. Ölçek Geliştirilmesi	54
3.4. Analiz Yöntemi ve Bulgular	55
3.4.1. Tanımlayıcı İstatistikler	55
3.4.2. Faktör ve Güvenirlik Analizi	63
3.4.3. Yapısal Eşitlik Modeli Analizleri	65
3.4.4. Hipotezlerin Testi	69
3.4.5. Türkiye ve ABD'deki Katılımcıların Sosyal Medya ve Online Alışveriş Kullanımında Gizlilik ve Güvenlik Algılarının Karşılaştırılması	72
SONUÇ VE ÖNERİLER	75
EKLER	81
EK-1: Türkiye'de Kullanılan Anket Formu	81
EK-2: ABD'de Kullanılan Anket Formu	86
KAYNAKÇA.....	93
ÖZGEÇMİŞ	105

KISALTMALAR LİSTESİ

ARPANET: Advanced Research Projects Agency Network (Gelişmiş Araştırma Projeleri Dairesi Ağı)

WEB: World Wide Web (Dünyayı Çevreleyen Ağ)

ABD: Amerika Birleşik Devletleri

FTC: Federal Ticaret Komisyonu (ABD)

FCC: Kişisel Bilgilerin Korunması Kanunu (ABD)

AB: Avrupa Birliği

KVKK: Kişisel Verilerin Korunması Kanunu

EDAM: Ekonomi ve Dış Politikalar Araştırma Merkezi

AIHS: Avrupa İnsan Hakları Sözleşmesi

OECD: Ekonomik Kalkınma ve İşbirliği Örgütü

WTO: Dünya Ticaret Örgütü

ETTK: Elektronik Ticaret Koordinasyon Kurulu

EFT: Elektronik Fon Transferi

EVD: Elektronik Veri Değişimi

TÜİK: Türkiye İstatistik Kurumu

TÜBİSAD: Türkiye Bilişim Sanayicileri Derneği

B2C: İşletmeden Müşteriye E-Ticaret

AWS: Amazon Web Hizmetleri

IoT: Nesnelerin İnterneti

RFID: Radyo Frekansı ile Tanımlama

GPS: Global Konumlama Sistemi

GGF: Gizlilik ve Güvenlik Farkındalığı

GGE: Gizlilik ve Güvenlik Endişesi

KMT: Korunma Motivasyonu Teorisi

TABLÖLAR LİSTESİ

Tablo 1: Veri Kapasite Büyüklüklerinin Örneklerle Kıyaslaması	12
Tablo 2: KVKK'nın Değerlendirilmesi	16
Tablo 3: E-ticaretin 90'lı yıllarda gelişimi	26
Tablo 4: Online Gizlilik ve Güvenlik Konularında Yaşanan Durumlar	31
Tablo 5: Sosyal Medyada Online Gizlilik ve Güvenlik Sorunları	33
Tablo 6: Anket Ölçek Soruları	55
Tablo 7: Katılımcıların Cinsiyet Dağılımı	56
Tablo 8: Katılımcıların Yaş Grupları	56
Tablo 9: Katılımcıların Eğitim Durumu	57
Tablo 10: Katılımcıların Gelir Durumu	57
Tablo 11: Katılımcıların İnternet Kullanım Süreleri	58
Tablo 12: Katılımcıların Akıllı Telefon Kullanım Süreleri	58
Tablo 13: Sosyal Medya Kullanımı	58
Tablo 14: Gün İçerisinde Sosyal Medya Kullanım Sıklığı	59
Tablo 15: Facebook Kullanımı	59
Tablo 16: WhatsApp Kullanımı	60
Tablo 17: Online Alışveriş Kullanımı	60
Tablo 18: Amazon Alışveriş Sitesinin Katılımcılar Tarafından Kullanımı	61
Tablo 19: Aliexpress Alışveriş Sitesinin Katılımcılar Tarafından Kullanımı	61
Tablo 20: Hepsiburada.com Alışveriş Sitesinin Türkiye'deki Katılımcılar Tarafından Kullanımı	61
Tablo 21: Büyük Veri Konusunda Bilgi Düzeyi	62
Tablo 22: Nesnelerin İnterneti Konusunda Bilgi Düzeyi	62
Tablo 23: Kişisel Verilerin Korunması Kanunu (KVKK) Bilgi Düzeyi	62
Tablo 24: KMO ve Bartlett Geçerlilik Değerleri	63
Tablo 25: Döndürülmüş Bileşenler Matrisi	64
Tablo 26: Ölçeğin Geneline ve Kapsadığı Sorulara İlişkin Güvenirlilik Değerleri	65
Tablo 27: Faktör Değişiklikleri Öncesi Modelin Uyum Değerleri	67
Tablo 28: Faktör Değişiklikleri Sonrası Modelin Uyum Değerleri	67
Tablo 29: Standardize Edilmiş Regresyon Katsayıları	68
Tablo 30: Faktörlerin AVE ve CR Güvenirlilik Değerleri	68
Tablo 31: YEM Hipotez Testi Sonuçları	70
Tablo 32: Sosyal Medya ve Online Alışveriş Kullanımında Türkiye ve ABD'deki Kullanıcıların Faktörlere Göre Farklılık Durumları	72

ŞEKİLLER LİSTESİ

Şekil 1: Sosyal medyanın bazı kullanım amaçları	19
Şekil 2: 2008 – 2018 yılları arasındaki Facebook kullanıcı sayısı.....	20
Şekil 3: 2016 – 2021 yılları arası Youtube kullanıcı sayısının artışı	23
Şekil 4: Instagram’ın 2013 – 2018 yılları arasındaki gelişimi	24
Şekil 5: Dünya perakende e-ticaret satışları.....	26
Şekil 6: Türkiye’de e-ticaret pazar büyüklüğü (milyar TL).....	27
Şekil 7: Ülkeler Arası Gizlilik Endişesi	43
Şekil 8: Belli Kurum ya da Kişilerce izlenmekten kaçınan kişi grupları (ABD).....	50
Şekil 9: Araştırma Modeli.....	51
Şekil 10: Ölçek Modeli	66
Şekil 11: Araştırma Modeli Path Diyagramı	69

Yalova Üniversitesi Sosyal Bilimler Enstitüsü Yüksek Lisans Tez Özeti

Tezin Başlığı: SOSYAL MEDYA VE E-TİCARET KULLANICILARININ GİZLİLİK VE GÜVEN ALGILARININ DEĞERLENDİRİLMESİ: TÜRKİYE – ABD KARŞILAŞTIRMASI	
Tezin Yazarı: Erkan ÇETİNTAŞ	Danışman: Doç. Dr. İkrâm DAŞTAN
Kabul Tarihi: 26.11.2018	Sayfa Sayısı: ix (ön kısım) + 105 (tez)
Anabilim Dalı: İşletme	Bilim Dalı: İşletme
ARPANET adlı proje ile “internetin” üniversiteler arasında kullanılmaya başlanmasını world wide web (web) sayfası hizmetinin ve akıllı telefon teknolojilerinin kullanıma girmesi gibi gelişmeler takip etmiştir. Bu gelişmeler ile birlikte internet kullanımını günümüze kadar hızla artarak devam etmiştir. Dünya nüfusunun büyük bir çoğunluğunun gündelik hayatının önemli bir parçası haline gelen internetin en yaygın kullanım alanının başında ise sosyal ağlar ve sosyal medya uygulamaları gelmektedir. Ayrıca günümüzde sosyal ağlar ve online alışveriş sitelerinin alışveriş için sıklıkla kullanılır hale geldiğini görmekteyiz. Tüm bu gelişmeler gündelik hayatımıza birçok kolaylıklar ve yenilikler sağladığı gibi bazı problemleri de beraberinde getirmiştir. Bunların en başında ise sosyal ağlarda ve online alışveriş sitelerinde paylaştığımız kişisel bilgi ve verilerimizin iznimiz olmadan devletler, kurumlar, şirketler ya da 3. Şahıslar tarafından elde edilebilir, işlenebilir ve kullanılabilir olması gelmektedir. Bu durum kişisel bilgi ve verilerimizin yeteri kadar korunamadığı, gizliliği ve güvenliğinin tehdit altında olduğu gerçeğini ortaya koymakta ve internet kullanıcılarının bu tehdit karşısında nasıl davranışlar sergiledikleri sorusunu akla getirmektedir. Bu çerçevede projenin amacı internet kullanıcılarına ait kişisel bilgi ve verilerin gizliliğinin korunmasının son derece önemli hale geldiği bir dönemde sosyal medya ve online alışveriş siteleri kullanıcılarının gizlilik ve güven algılarının Türkiye ve Amerika Birleşik Devletleri (ABD) ölçeğinde karşılaştırılarak değerlendirilmesi, analiz edilmesi ve raporlanmasıdır. Bilgi Gizliliği ve Güvenliği, Sosyal Ağlar, E-ticaret ile Online Gizlilik ve Güvenlik gibi kavramlar ve konular incelendikten sonra araştırma ile hedeflenen Türkiye’de sosyal medya ve online alışveriş siteleri kullanıcıların gizlilik ve güven bağlamında farkındalık ve endişe seviyelerinin, sergiledikleri davranış türleri (kontrol, tedbir vb.) ve farklılıklarının e-ticaret boyutunda araştırılması ve değerlendirilmesidir. Araştırma sonucu elde edilen bulgular ayrıca ABD’deki kullanıcılar ile karşılaştırılarak farklılıklar ve benzerlikler ortaya konacaktır. Tüm araştırma sonuçları değerlendirildikten sonra araştırmanın sınırlılıkları belirlenecek ve ileriki araştırmalar için tavsiye ve öneriler geliştirilecektir.	
Anahtar Kelimeler: Bilgi Gizliliği, Kişisel Verilerin Korunması, Sosyal Medya, Online Alışveriş, Online Gizlilik ve Güvenlik	

Yalova University Insitute of Social Sciences Master Thesis Summary

Thesis Title: THE PRIVACY AND SECURITY PERCEPTIONS OF SOCIAL MEDIA AND E-COMMERCE USERS: TURKEY – USA COMPARISON	
Thesis Author: Erkan ÇETİNTAŞ	Advisor: Assoc. Prof. İkrım DAŞTAN
Date of Acceptance: 26.11.2018	Total Number of Pages: ix (pre text) + 105 (main body)
Department: Business Administration	Field of Study: Business Administration
Being started to use of the “internet” by means of ARPANET Project among some Universities have been followed by developments such as the use of the service of world wide web (web) and smart phone technologies. Along with these developments the use of internet has increasingly come until today. Social networks and social media applications are the leading areas of usage of the internet which is becoming one of the most important parts of the daily life of the world population. Beside we see that social networks and online shopping sites are being used frequently for commercial purposes. All these developments provide many facilities and innovations in our daily life as well as bring some problems along with it. At the outset of these problems are the collection, processing and usage of the personal information - which we shared in the social networks and online shopping sites - by the governments, organizations, companies or the 3rd parties. This situation puts forward the reality of our personal information and data are unable to be protected sufficiently and the privacy and security of those are under threat. And it brings to mind the question of how internet users display behaviours against this threat. In this framework the aim of the research is the assessment, analyse and reporting of the privacy and security perceptions of social media and online shopping site users in terms of Turkey and the United States of America (USA) Comparison in the very important age of the privacy of the personal information and data belong to internet users to be protected. After examination of concepts and subjects like Information Privacy and Security, Social Networks, E-Commerce and Online Privacy and Security the Research aims at studying and evaluating the awareness and concern levels, behaviour types (control, precaution etc.) and differences of social media and online shopping site users in the context of privacy and security. Furthermore the findings obtained as a result of the study will be compared with the users in the USA and differences and similarities will be revealed. After the evaluation of all results of the study limitations of the Research will be determined and recommendations and suggestions will be developed for future researches.	
Keywords: Information privacy, Protection of Personal Data, Social Media, Online Shopping, Online Privacy and Security	

GİRİŞ

Bilginin yayılmasında ve çok daha geniş kitlelere hızlı bir şekilde ulaşmasında etkin rolü oynayan internetin en önemli araçları olarak milyarlarca kişi tarafından kullanılan sosyal medya ve online alışveriş siteleri karşımıza çıkmaktadır. Hızla gelişen teknolojik gelişmeler ile birlikte bilgi ve veri kaynağı olan bu araçlar işletmelerden pazarlamacılara tüketicilerden sosyal medya kullanıcılarına kadar her kesimin bilgi gizliliği ve güvenliği kavramlarını dikkatle ele almasını gerekli kılmaktadır. Zira bilgi gizliliği ve güvenliği tüketici ya da kullanıcıların bilgi sağlamadaki istekliliğini, satın alma davranışlarını dolayısıyla satıcı-müşteri ilişkilerini etkileyen bir unsur olarak ön plana çıkmaktadır. Bu bağlamda kullanıcıların sosyal medya ve e-ticaret platformlarında yer alan ve onların satın alma davranışlarını ile tercihlerinin analiz edilmesini sağlayan kişisel bilgileri ve verileri elektronik ticaret ve işletmeler açısından son derece önemli hale gelmiştir. Diğer taraftan bu durum kullanıcıların kişisel bilgilerinin gizliliği ve güvenliğinin yeteri kadar sağlanıp sağlanmadığı sorusunu da beraberinde getirmiştir. Öyle ki We Are Social ve Hootsuite (2017) tarafından yayınlanan “Digital in 2017 Global Overview” adlı raporda 7,6 milyarlık dünya nüfusunun 3,8 milyarının interneti, 2,8 milyarının ise sosyal medyayı aktif olarak kullandığı belirtilmiştir. Türkiye’de ise internet ve sosyal medya aktif kullanıcı sayısı 48 milyon olarak açıklanırken mobil kullanıcı sayısı 71 milyon, sosyal medyaya mobilden bağlanan kullanıcı sayısı ise 42 milyon olarak açıklanmıştır (We Are Social Digital Yearbook, 2017). Aynı raporda e-ticaret platformları üzerinden çevrimiçi alışveriş yapanların sayısı 1.61 milyar olarak ölçülürken 2016 yılı itibarıyla e-ticaret üzerinden elde edilen gelirler 1.9 trilyon dolar olarak ifade edilmiştir. Bu rakamlar dikkate alındığında ölçülemeyecek büyüklükte bir verinin sadece sosyal medya kullanımı üzerinden toplandığını ve bu verilerin ticaret hacminin ulaştığı nokta itibarıyla işletmeler tarafından sıklıkla kullanılabileceğini rahatlıkla söyleyebiliriz. Bu nedenle gerek sosyal medya kullanımının artarak devam etmesi gerekse e-ticaret pazarındaki hızlı büyüme kullanıcıların kişisel verilerinin korunması, gizliliği ve güvenliği konularının işletmeler açısından incelenmesini gerekli kılmaktadır. Ayrıca kullanıcı ya da tüketicilerin kendilerine ait bilgi ve verilerin gizliliğini sağlamak için sergiledikleri davranışlar yönünden de bu konular değerlendirilmelidir. Bu çerçevede online gizlilik ve güvenlik konularında genel olarak çeşitli araştırmalar yapıldığı ancak sosyal medya ve online alışverişin hızlı gelişimi karşısında daha fazla, daha spesifik ve özellikle ülkeler arası karşılaştırmalı çalışmalar yapılması gerektiği görülmektedir.

Araştırmanın en önemli dayanağını online gizlilik ve güvenlik kavramları oluşturmaktadır. Bu iki kavram birbirleri ile doğrudan bağlantılı olarak kullanılabildiği gibi birbirleri yerine de kullanılabilmektedir. Gizlilik kavramı büyük ölçüde Alan Westin ve Irwin Altman’ın çalışmalarından etkilenmiştir. Hem Westin hem Altman gizliliği sınır yönetiminin dinamik bir süreci olarak ifade etmektedir. Westin gizliliği “bireyin kendisi hakkında hangi bilginin başkaları tarafından bilinmesi gerektiğini belirleme isteği” olarak tanımlarken, Altman gizliliği bireyin

kendisine ya da kendisine ait bir gruba seçici kontrolü üzerinden erişimi olarak tanımlamaktadır (Trepte ve Reinecke, 2011). “Online gizlilik” kavramı ise literatürde Waldo ve arkadaşlarının yaptığı çalışma (Waldo ve diğerleri, 2007) başta olma Mcgraw Hill Enstitüsü, PEW Araştırma Merkezi, merkezi Amerika’da bulunan ve Türkiye’de de şubesi bulunan ISACA derneği tarafından yapılan çalışmalarda da tüketicilerin bilgi gizliliği konusundaki endişeleri incelenmiştir. (Mcgraw Hill Institute 2013; Rainie ve diğerleri, 2013; Madden ve diğerleri, 2014; ISACA 2014). Bunların dışında online bilgi gizliliği ve güvenliği ile doğrudan ilgili olan Büyük Veri, Veri Madenciliği, Bulut Bilişim ve Nesnelerin İnterneti gibi kavramların incelendiği Chen ve arkadaşlarının çalışması literatüre önemli katkıları olan çalışmalar arasındadır (Chen ve diğerleri, 2014). Benzer şekilde büyük verinin gizlilik ve güvenliğe olan etkisinin incelendiği diğer bir çalışma Kshetri tarafından yapılan çalışmadır (Kshetri, 2014). Ayrıca FTI Danışmanlık şirketi tarafından yapılan Amerika ve Avrupa Birliğinin karşılaştırdığı araştırma ile EMC şirketi tarafından küresel boyutta yapılan araştırma elde edilen bulgular açısından oldukça önemlidir (Healey ve diğerleri, 2014; EMC 2014).

Diğer taraftan mevcut araştırmaların büyük bir çoğunluğunun sosyal medya ve online alışveriş sitesi kullanıcılarının gizlilik ve güvenlik algılarına ve bunun sonucunda ortaya koydukları davranış türlerine yönelik olarak yoğunlaştığı görülmektedir. Bu araştırmalardan Tamara Dinev ve Paul Hart tarafından online alışverişlere yönelik kullanıcılarının gizlilik endişeleri ve sosyal farkındalıkları üzerine yapılan çalışma önemli çalışmalar arasında yer almaktadır (Dinev, Hart 2005). Yine Dine ve Hart’ın online gizlilik endişeleri, güven, risk gibi boyutların ve bunların sonucu kullanıcılar tarafından sergilenen davranışların incelendiği araştırması literatüre katkı sağlayan çalışmalar arasındadır (Dinev ve Hart 2006). Facebook ve MySpace uygulamalarının karşılaştırıldığı, kullanıcıların güven ve gizlilik endişelerinin ele alındığı bir araştırma ise Dwyer ve arkadaşları tarafından gerçekleştirilmiştir (Dwyer ve diğerleri, 2007). Güncel çalışmalar arasında ise Hindistan’daki online alışveriş kullanıcılarının gizlilik endişelerine etki eden faktörlerin araştırıldığı Soumava ve Kakoli Bandyopadhyay tarafından gerçekleştirilen çalışmayı gösterebiliriz (Bandyopadhyay, 2017). Güney Batı Nijerya’daki sosyal medya kullanıcılarının bilgi güvenlikleri konusundaki farkındalıklarının incelendiği bir başka araştırma yine farklı bölgeler üzerinde yapılan güncel çalışmalar arasında dikkate alınmalıdır (Okesola ve diğerleri, 2016). Türkiye’de yapılan araştırmalara ise Trakya Bölgesi’ndeki üniversitelerde görev yapan öğretim elemanlarının online alışverişten algıladıkları risk ve fayda üzerine yapılan araştırmayı örnek olarak gösterebiliriz (Altuğ ve Özkan, 2012). Amerikalı ve Çinli tüketici ve kullanıcıların gizlilik endişelerinin karşılaştırıldığı çalışma ise araştırmaya kaynak oluşturan çalışmalar arasında yer almaktadır (Zhang ve diğerleri, 2002).

Yukarıda bahsedilen araştırmalardan hareketle ölçülemeyecek boyutlarda bilgi ve verinin kayıt altına alındığı ve işlendiği günümüz çağında internet kullanıcılarının gizlilik ve güven algılarının Türkiye – ABD karşılaştırması açıdan incelenmesi

araştırmanın konusunu oluşturmaktadır. Araştırma çerçevesinde internet kullanıcıların gizlilik ve güvenlik hususlarında yaşadıkları endişe, risk ve güven sorunlarının sosyal medya ve e-ticaret kullanıma yönelik etkileri ele alınmaktadır. Zira sosyal medya ve online alışveriş sitelerinin ticari amaçlarla kullanımı artarak devam etmekte diğer taraftan tüketici ya da kullanıcıların bilgi gizliliği ve güvenliği konusundaki endişeleri de buna paralel olarak artış göstermektedir. Bu bağlamda araştırma kullanıcı ve tüketicilerin endişe, risk ve güven sorunları karşısında ne tür davranışlar sergilediklerini, bilgi gizliliği ve güvenliği konusunda sahip oldukları farkındalık düzeylerini ortaya koymaya çalışmaktadır. Dolayısıyla gerek işletmeler gerekse tüketiciler yönünden araştırma gelecekte çok daha önemli hale gelebilecek bir konuya araştırmacıların daha fazla dikkatini çekmeyi amaçlamaktadır.

Araştırmanın birinci bölümü giriş bölümü niteliğinde olup bu bölümde araştırmanın problemi, amacı, önemi ve sınırlılıkları açıklanmıştır. İkinci bölümde genel olarak gizlilik ve güvenlik kavramları üzerinden durulurken alt başlıklarda bilgi gizliliği ve güvenliği, internette gizlilik ve kişisel verilerin korunması kanunları kullanıcılar ve işletmeler açısından değerlendirilmiştir. Bu kısımda online gizlilik ve güvenlik konusunda ABD’de yapılan çalışmalar, düzenlemeler ve yasalar incelenerek bunların Türkiye’dekiler ile kıyaslaması yapılmıştır. İkinci bölümde araştırmanın asıl konusu oluşturan gizlilik ve güvenlik konuları sosyal medya ve online alışveriş (e-ticaret) açısından değerlendirilirken sosyal medya ve e-ticaretin gelişimi ve uygulamaları hakkında bilgi verilmiştir. Son olarak ikinci bölümde bilgi gizliliği ve güvenliği açısından sosyal medya ve e-ticaret kullanımında gizlilik ve güvenliğe etki eden faktörler irdelenmiştir. Üçüncü bölümde tüm değerlendirmelerden hareketle sosyal medya ve online alışveriş kullanıcılarının gizlilik ve güvenlik endişeleri, farkındalıkları, deneyimleri bunların güven duygusu, risk algıları, kullanıcı davranışı üzerine etkileri incelenmiş, araştırmanın modeli ve hipotezleri geliştirilmiştir. Daha sonra anket yöntemiyle toplanan bilgi ve veriler doğrultusunda analizler yapılarak araştırmanın hipotezleri test edilmiştir. Araştırmanın sonuç bölümünde ise analiz ve hipotezlerin sonuçları üzerine genel bir değerlendirme yapılarak araştırmanın literatüre olan katkısı ifade edilmiştir.

BÖLÜM 1: ARAŞTIRMANIN ÇERÇEVESİ

1.1.Araştırmanın Problemi

Bilgi ve iletişim teknolojilerinde yaşanan gelişmelerle mobil internet ve akıllı telefonlar hayatımıza hızla girmiştir. Bu gelişmelerin sonucu olarak da sosyal medya uygulamaları ve online alışveriş siteleri toplumların büyük bir kesimi tarafından sıklıkla kullanılır hale gelmiştir. Bu durum çok büyük miktarlarda bilginin toplanıp kayıt altına alınmasını, işlenip farklı amaçlar için kullanılır hale getirilmesi sonucunu doğurmuştur. Bunlar arasında bilim ve teknolojinin geliştirilmesi, yeni ilaçların keşfedilmesi, toplum güvenliğinin artırılması, ulusal güvenliğin korunması, işletmelerin rekabet gücünün artırılması ya da pazarlama hedeflerinin iyileştirilmesi gibi amaçlar sıralanabilir. Ancak online bilgilerin toplanması ve farklı unsurlar tarafından kullanılması kişisel bilgilerin gizliliği ve güvenliği sorununu da beraberinde getirmiştir. Bu konuda özellikle sosyal medya uygulamaları ve online alışveriş siteleri ön plana çıkmaktadır. Devletler, şirketler ya da 3. taraflar kullanıcılar hakkında çok sayıda bilgiyi bu online platformlar üzerinden toplayabilmekte ve farklı amaçlarla kullanabilmektedir. Örneğin 1,5 milyar kullanıcı sayısı ile sosyal medya uygulamalarının en başında yer alan ve online alışveriş için de tercih edilmeye başlanan Facebook, kullanıcılarını sosyoekonomik olarak kategorize etmesine imkan sağlayan yeni bir algoritma geliştirmiştir. Bu algoritma ile Facebook kullanıcılarının dahil oldukları sosyoekonomik sınıfı analiz edebilir hale gelmiştir. Bir başka ifadeyle bundan böyle kullanıcılarının yani müşterilerinin sahip oldukları parayı ve alım güçlerini tahmin edebilecektir. Ayrıca Facebook böylelikle kullanıcılarına alım güçlerine uygun reklamları önerdiğinden emin olabilecektir (Habertürk, 2018). Ayrıca 2018 yılında Facebook'un 87 milyona yakın kullanıcının kişisel verilerini izinsiz bir şekilde Cambridge Analytica şirketiyle paylaştığı bir skandala imza atmıştır (BBC, 2018). Bu durum ise kişisel bilgilerin gizliliği ve güvenliği sorununu en net şekilde ortaya koyan bir durumdur. Bu çerçevede araştırma, “kullanıcılar, kişisel bilgilerini sosyal ağlarda ya da online alışveriş sitelerinde paylaşma konusunda herhangi bir gizlilik ve güvenlik endişesi duyuyorlar mı?” ya da “kullanıcılar, kişisel bilgilerinin ne kadarını paylaşmak istiyorlar?” ya da “kullanıcılar, kişisel bilgilerine hangi kurum ya da kişiler tarafından ulaşılmasında bir sakınca görmüyorlar?” gibi sorulara cevap aramaktadır.

1.2. Araştırmanın Amacı ve Önemi

Sosyal medya ve online alışveriş siteleri bireyler hakkında birçok kişisel bilginin toplanmasına ve kayıt altına alınmasına olanak sağlamaktadır. Bu bilgilerin büyük bir kısmı gönüllü olarak paylaşılmakta ve bu bilgiler hem bireylere hem de kurumlara online gizlilik ve güvenlik açısından bir risk unsuru oluşturmaktadır. Bu durum ise kişisel bilgilerinin gizliliği ya da güvenliği bağlamında insanların zihninde çeşitli endişelere neden olmakta ve online davranışlarına olumsuz etki etmektedir. Online gizlilik ve güvenlik konuları birçok araştırma tarafından incelenmiş olmakla birlikte sosyal ağların hızla gelişmeye devam etmesi, her geçen gün daha da fazla

büyüyen yapıları, daha kapsamlı ve özellikli araştırmalar yapılmasını gerekli kılmaktadır. Çünkü bu tür araştırmalar bireylerin online gizlilik ve güvenliklerinin hükümetler ya da işletmeler tarafından daha etkili bir şekilde korunur hale getirilmesine katkı sağladıkları gibi teknolojik gelişmelerin daha iyi anlaşılıp işletmeler ve tüketiciler için geliştirilmesine de olanak sağlamaktadır. Dolayısıyla araştırma bu amaç doğrultusunda kullanıcı bireylerin karakteristik özellikleri ve algıları başta olmak üzere sosyal medya ve online alışveriş sitelerinin özelliklerini de dikkate alarak bir araştırma modeli oluşturmaktadır. Araştırma böylelikle kullanıcıların online gizlilik ve güvenlik konusundaki farkındalıklarını ortaya koyarken kullanıcı davranışlarını da Türkiye-ABD ölçeğinde açıklamaya çalışmaktadır.

1.3. Araştırmanın Katkıları

Araştırmanın öncelikli hedefi sosyal medya ve online alışveriş kullanıcılarının gizlilik ve güvenlik konularında farkındalık ve bilgi düzeylerini ölçmek, kullanıcıların ve tüketicilerin gizlilik ve güvenlik algıları açısından ne tür davranışlar sergilediklerini ortaya koymaktır. Mevcut çalışmaların büyük bir çoğunluğu davranış türlerini kullanıcıların kişisel özellikleri ve kullanıcı geçmişleri üzerinden açıklamaya çalışmaktadır. Bu çerçevede araştırmamız genel kullanıcı özelliklerinin daha da ilerisine giderek kullanıcıların gizlilik ve güvenlik davranışlarını farkındalık, endişe, risk, güven ve güvenlik boyutlarını kapsayacak şekilde ele alarak literatüre önemli bir katkı sağlamaktadır.

Diğer taraftan online gizlilik ve güvenlik alanında daha önce yapılan proje ve çalışmaların büyük bir çoğunluğu ABD’de yapılmış olup Türkiye üzerine yapılan çalışmalar sınırlı sayıdadır. Bu nedenle gerek coğrafi konumu ve kültürel yapısı gerekse siyasal yapısı itibarıyla hem batılı ülkelere hem de doğulu ülkelere farklılaşması münasebetiyle araştırmanın Türkiye üzerinde uygulanmasının literatüre önemli bir katkı sağlayacağı düşünülmektedir. Ayrıca elde edilecek veri ve bulguların ABD’deki kullanıcılar üzerindeki araştırma verileri ile karşılaştırılacak olması diğer önemli bir katkı olarak değerlendirilebilir. Zira kullanıcıların kişisel verilerinin gizliliği ve güvenliği konusunda ülkeler ve bölgeler farklı yaklaşımlar ve politikalar izlemektedir. Bu bağlamda araştırma çerçevesinde konuya ilişkin ABD’deki düzenleme, uygulama ve kanunların incelenerek Türkiye’deki uygulama ve kanunlar ile karşılaştırılması bir başka katkı olarak ön plana çıkmaktadır.

BÖLÜM 2: KAVRAMSAL ÇERÇEVE VE LİTERATÜR

Bu bölümde gerçekleştirilen inceleme çalışmaya konu olan kavramlar ve çalışmanın temel amacını desteklemek üzere daha önce yapılan akademik araştırmaların genel bir değerlendirmesidir. Bu bölüm “bilgi gizliliği ve güvenliği, kişisel verilerin korunması kanunları, sosyal medya, e-ticaret, online gizlilik ve güvenlik” gibi kavramlar ile gizlilik ve güvenliğe etki eden faktörlerin mevcut literatür çerçevesinde incelenmesi, ilgili hipotezlerin oluşturulması ve araştırma yöntemi ile modelinin oluşturulmasına yönelik kavramsal çerçeveyi kapsamaktadır.

2.1. Gizlilik ve Güvenlik

Gizlilik toplumda farklı şekillerde nitelendirilmekte olan bir kavramdır. Hem yasal açıdan hem de ahlaki açıdan temel bir hak olarak görülmektedir. Aynı zamanda gizlilik “öz itibar, öz değerlendirme, rol yapma ya da kişinin kendisi hakkında iletişimi sınırlandırma ihtiyacı” gibi faktörler ile alakalı davranışsal çıkarımlara sahip bir kavramdır. Gizliliği işlevsel olarak tanımlamak ve kavramın çoklu davranışsal boyutlarını gözlemsel açılardan araştırmak için çeşitli girişimlerde bulunulmuştur (Pastalan, 1970). Bu çerçevede Pastalan (1970) gizliliği, bireylerin amaçları doğrultusunda kendileri hakkındaki hangi bilgilerin hangi koşullarda diğer kişilere iletilip iletilmeyeceğine karar verme hakkı olarak tanımlamaktadır. Diğer taraftan zaman zaman gizlilik kavramı yerine de kullanılabilen ancak daha çok onun tamamlayıcısı niteliğinde olan güvenlik kavramı gizlilik ile birlikte ele alınmaktadır. Araştırmada birbiri ile yakından ilişkili bu iki kavram internet ortamındaki online gizlilik ve güvenlik açısından incelenmektedir. İki kavram farklı disiplinlerden birçok araştırmanın konusu olarak ele alınmış olup, araştırmada bu kavramların sosyal medya ve e-ticaret kullanıcılarının bilgi gizliliği ve güvenliği yönünden değerlendirilmesi yapılmaktadır. Zira Godwin (2001) gizlilik ve güvenlik endişelerinin internetten alışverişin önündeki en önemli engeller olduğunu belirtmektedir. Özellikle güvenlik konusunun internet bankacılığının benimsenmesinde önemli bir engel olduğu belirtilirken, Westin (1998) tarafından gizlilik sorunlarının online hizmetlerin kullanımında karşımıza çıktığı belirtilmektedir (Lallmahamood, 2007). Dolayısıyla araştırmanın genelinde bu iki kavram birlikte değerlendirilmekte, internet kullanıcıların gizlilik ve güvenlik algılarının yanı sıra bu algıların davranışsal etkileri incelenmektedir.

2.1.1. Bilgi Gizliliği ve Güvenliği

Kişisel gizlilik yeni bir tartışma konusu olmamakla birlikte özel hayatın ve gizliliğin ihlali insanlık tarihi boyunca hep süregelen önemini günümüze kadar korumuştur (Ghazinour ve diğerleri, 2014). İlk belgelenmiş gizlilik ihlali 1300’lü yıllarda gizli dinleme olarak kayıtlara geçmiştir ve o zamandan bu yana kişisel gizlilik modern toplumun geliştirdiği matbaa, fotoğrafçılık ve en nihayetinde internet gibi gelişmelerle daha fazla önem kazanmıştır. Online gizliliği bu kadar önemli hale getiren teknolojik gelişmeler çerçevesinde insan davranışlarında ortaya çıkan dikkat

çekici geçiştir. Son yüzyılda özellikle bilgi teknolojileri kişisel sınırların belirlenmesinde en belirleyici rolü oynar hale gelmiştir. Toplum dedikodular üzerinde şekillenen endişelerden özel sırların geniş insan kitlelerine ulaştığı bir toplum haline dönüşmüştür. 1300'lü yıllarda bir kişiye ait bir sırrın ortaya çıkışı ya da toplum üzerindeki etkisi sınırlı durumdayken günümüzde benzer bir sır yüzbinlerce hatta milyonlarca insana saniyeler içerisinde ulaşabilmektedir. Bir taraftan bilgi teknolojilerinin bizlere sağladığı imkânlardan yararlanma isteği dururken diğer taraftan aynı teknolojik imkânların yarattığı gizlilik ihlallerinden kaçınma ya da korunma ihtiyacı ortaya çıkmıştır.

Bilgi gizliliği ve güvenliği kişisel bilgilerin ifşasının merkezine oturmuş durumdadır. Columbia Üniversitesinde eski bir kamu hukuku ve yönetimi profesörü olan ve kişisel veri, gizlilik ve veri korunması üzerine çalışmaları ile tanınan Alan Westin (1968) bilgi gizliliğini bireylerin, grupların ve kurumların kendilerine ait bilgilerin ne zaman, nasıl ve ne derecede diğerlerinin yorumuna açık olduğunu belirleme hakkı olarak tanımlamaktadır. Günümüzde kişisel online bilgiler zengin doğal kaynaklar ve ticareti yapılabilir ya da pazarlanabilir ürünler olarak görülmektedir. Bireylere ait bilgiler kişisel olmaktan çıkarak değiş tokuşu yapılabilir bir meta ya da para birimi haline dönüşmüştür. Bunun sonucu olarak da kişisel bilgiler yönetilmesi zor bir kaynak haline gelmiştir (Culnan ve Armstrong, 1999; Dinev ve Hart, 2006).

Bilgi gizliliği ve güvenliği ele alındığında bu kavramın bilgi ifşasının dinamikleri ile ilintili olduğu görülmektedir. İfşa olgusu bireylerin kendileri hakkındaki bilgileri diğer kişiler ile paylaşımları sürecini ifade eder ve çoğunlukla ortaya çıkan bilgi miktarı ve paylaşımdaki yakınlık derecesi ile ölçülmektedir (Wheless ve Grotz, 1976). İlki bilginin kapsama genişliğinin ölçümüdür, ikincisi ise etkileşimdeki dürüstlük seviyesinin ölçümü ile alakalıdır. Bireyler bilgi ifşalarının kapsam genişliğini sınırları (limitleri) düzenleme süreci üzerinden yönetmektedir (Petronio, 2012; Xu, 2007). Bu süreç musluk tapasını istedikleri zaman açıp kapattıkları gibi insanların ifşa ettikleri ya da elde ettikleri bilgiler için de istedikleri gizlilik ve güvenlik seviyesini belirleyebildikleri bir süreç olarak tanımlanmaktadır (Shklovski, 2014). İfşa süreci bilgiyi elde etme ve onu paylaşma isteği arasındaki doğal bir gerilimi ifade etmektedir (Altman, 1977; Xu ve diğerleri, 2008).

2.1.2. İnternette Gizlilik ve Güvenlik

İnternet üzerinden iletişim kurabilme imkanı bilgi gizliliği ve güvenliğine yeni bir boyut kazandırmıştır. Bireyler çok düşük bir maliyetle ve çoğu zaman neredeyse hiç düşünmeden tek bir sosyal ağ üzerinden kişisel ve özel bilgilerini anında başkaları ile paylaşabilmektedir. Her bir saniyede binlerce anlık mesaj yayınlanmakta ve milyonlarca e-mail gönderilmektedir (Pappas, 2016). İnternet erişimi ile birlikte bireyler daha önce hiç olmadığı kadar kendileri hakkında paylaşımlarda bulunmaktadır. Çünkü bireyler hayatlarının en mahrem ayrıntılarını yaptıkları online yorumlar, bloglar, resim ve video paylaşımları ile tanıdıkları ve tanımadıkları insanlarla paylaşmaktadır (Granryd, 2016). Bilgi gizliliğinin yönetimine ilişkin eski

yaklaşımları sürdürmek böylelikle çok daha zor hale gelmiştir. Artık günümüz dünyası “gönder” tuşuyla kişisel bilgilerin ifşasını çok daha kolay hale getirmiştir.

Diğer taraftan günümüzde internet tüketicilerin alışveriş yaptıkları, şirketlerin yeni pazar araştırmaları yaptıkları bir araç niteliğindedir. İnternet iş dünyasının gelişiminin özellikle kişiselleştirilmiş ürün ve hizmetler açısından yeni penceresi olmuş ve olmaya devam etmektedir (Brahim ve Martiz 2015; Greengard, 2015). Bu kişiselleştirmenin sonucu ise şüphesiz kişisel bilgi ve verilerin toplanmasıdır. Artık şirketler bireylerin kişilikleri, geçmişleri ve eylemleri hakkında çok büyük miktarda bilgiyi toplayabilme konusunda uzman hale gelmiş durumdadır. Bunun karşılığında ise bireyler kişisel profillerinde endişelenmelerini gerektirecek veri izleri bırakmaktadır (Acquisti ve diğerleri, 2015; Laudon, 1986; Malhotra ve diğerleri, 2004; Smith ve diğerleri, 1996). Kişisel bilgi ve verileri toplama işi rekabetçi büyümenin yakıtı haline gelmiş durumda olup pazarlamacılar müşteri bilgi ve verilerine karşı doyumsuz bir açlık içerisinde ve bu durumun tersine dönebileceğine ilişkin hiçbir emare bulunmamaktadır (Dinev ve Hart, 2003; Keith ve diğerleri, 2017). Gerçekte veri toplama süreci mobile cihazların kullanımı ile birlikte çoğalmaktadır. Milyarlarca internet kullanıcısının büyük bir çoğunluğu internete mobil cihazlar üzerinden bağlanmaktadır. Mobil cihazların kullanımı son beş yılda üçe katlanmış durumdadır ve artarak devam etmektedir (Granryd, 2016). Mobil cihazlar bilgi gizliliği ve güvenliği konusunda kendine özgü özellikler ile birlikte gelmiştir. Bunlardan ilki mobil bilişimin (bilgisayarların) çalışma şekli olup masaüstü bilgisayarların çalışma şeklinden farklıdır. Bireyler mobil cihazları her gün yanlarında taşımakta ve onları kişisel hayatlarının önemli bir parçası olarak görmektedirler (Ling, 2008; Nafus ve Tracey, 2002). Mobil cihazlardaki uygulamalar kişiselleştirilmekte bireylerin kişisel bilgilerine erişimi mümkün hale getirmektedir. Bireylerin sağlıkla ilgili bilgilerinden konum bilgilerine kadar farklı türden bilgi ve verilere uygulamalar üzerinden ulaşılabilir (Boyd, 2008; Keith ve diğerleri, 2017; Xu ve diğerleri, 2012). Dolayısıyla toplanan bilgi ve verilerin artışına paralel olarak bireylerin bilgi gizlilikleri ve güvenlikleri konusunda endişeleri de artmaktadır. Bireyler kendileri hakkında gereğinden fazla bilgi ve verinin toplandığını düşünmekte ve bu bilgilerin şirketler tarafından nasıl toplandığı ve kullanıldığı hususunda kontrolü kaybettiklerini hissetmektedirler (Lin ve diğerleri, 2012; Rainie ve Madden, 2015). Özellikle büyük veri, bulut bilişim ve nesnelerin interneti gibi ortaya çıkan teknolojik gelişmeler hem şirketlere hem de tüketicilere eşsiz avantajlar sağlamakla birlikte bilgi gizliliği ve güvenliği konusundaki endişeleri de her geçen gün daha da artırmaktadır (Westin, 2003).

Bu kavramlar arasında büyük veri özellikle gelişmiş ve gelişmekte olan ülkeler ve işletmeler açısından günümüzde son derece önemli hale gelmiştir. Her ne kadar büyük verinin önemi genel olarak kabul görmüş olsa da insanlar büyük veriyi tanımlamakta farklı görüşlere sahiptir. En genel tanımı ile büyük veri geleneksel bilgi teknolojileri, yazılımları ya da donanımları ile makul zaman diliminde yakalanamayacak, toplanamayacak, yönetilemeyecek, işlenemeyecek ya da analiz edilemeyecek veri setlerini ifade etmek için kullanılmaktadır. 2010 yılında Apache

Hadoop büyük veriyi “normal bilgisayarların kabul edilebilir bir kapsamda elde edemeyeceği, yönetemeyeceği ve işleyemeyeceği türden veri setleri” olarak tanımlamıştır (Chen ve diğerleri, 2014). Bu tanım üzerinden küresel bir danışmanlık firması olan McKinsey&Company ise büyük veriyi “yenilikçiliğin, rekabetin ve verimliliğin bir sonraki adımı” olarak nitelemiştir (Chen ve diğerleri, 2014). Büyük verinin depolama kapasitesine baktığımızda günümüzde sıklıkla kullandığımız 1 gigabayt (GB) yani 1 milyar baytlık verinin 2 saatlik CD kalitesinde sese denk gelirken 1 exabayt (EB) yani 1 quintilyon baytlık verinin 15 milyon adet 16 GB’lık iPod’a tekabül ettiği söylenebilir (Altunışık, 2016). EB ya da ZB hacmindeki verilere Facebook, Amazon, Ebay ve Google örnek olarak gösterilebilir. Bu bağlamda büyük veri büyüklüğünü ve küçük veri ile arasındaki farkı anlamak açısından aşağıda tablo 2’de belirtilen karşılaştırmaya bakmakta yarar vardır.

Tablo 1: Veri Kapasite Büyüklüklerinin Örneklerle Kıyaslaması

Terim	Örnek kıyaslama büyüklüğü	Yaygın kullanım alanı
Bayt (B) Kilobayt (KB)	Bir pirinç tanesi 1 fincan pirinç	Bilgisayarın ilk yılları Bilgisayarın ilk yılları
Megabayt(MB) Gigabayt (GB)	8 çuval dolusu pirinç 3 tır dolusu pirinç	Masaüstü bilgisayar Masaüstü bilgisayar
Terabayt (TB) Petabayt (PB)	2 adet konteyner gemisi pirinç Manhattan adasını kaplayacak kadar pirinç	İnternet İnternet
Exabayt (EB) Zetabayt (ZB)	Amerika’nın Kuzey Batısında yer alan 11 eyaleti örtecek büyüklükte pirinç Pasifik Okyanusunu dolduracak miktarda pirinç	Büyük Veri Büyük Veri
Yotabayt (YB)	Dünya büyüklüğünde bir pirinç tanesi	Gelecek

Kaynak: Bechtold, David (2014), What is big data?

Büyük veri bu özellikleri itibarıyla hem işletmelere hem de tüketicilere çeşitli fayda ve imkanlar sağladığı gibi online olarak bilgi gizliliği ve güvenliği açısından birtakım riskleri ve tehditleri de beraberinde getirmektedir. Bu bağlamda her ne kadar işletmeler kullanıcıların gizliliği ve güvenliğini korumaya yönelik kimliksizleştirme (de-identification) gibi yöntemler kullansa da bu yöntemlerin yetersiz kaldığı ve kullanıcılara hatta devletlere ait verilere izinsiz erişim sonucu gizlilik ve güvenlik tehditlerinin yüksek olduğu görülmektedir. Özellikle kullanıcılar ya da tüketiciler

açısından duruma bakıldığında büyük veri dünyasında gizliliğe ait bilgiler kullanıcıların onayı ya da farkında olmadan bıraktıkları online ayak izleri sonucu oluşmaktadır. Online ayak izleri araştırdığımız web sitesi, izlediğimiz video ya da okuduğumuz yazılar, nerede ve ne zaman online olduğumuz, kullandığımız cihazlar gibi online etkileşimlerimiz sonucu oluşan çok çeşitli verileri kapsamaktadır (Michael ve Miller, 2013). Hemen hemen yapılan her bir online hareket izlenebilmektedir. Tüm etkileşimler kullanılabilir bilgiler haline dönüştürmek üzere veri olarak toplanabilmektedir. Bu çerçevede büyük veri bilgilerimizi kaydetmekte ve bunlar online hareket ve davranışlarımızı yansıtmaktadır. Öyle ki bunlar en başta kişisel ilgi alanlarımız, siyasi görüşümüz, cinsel eğilimlerimiz, dini inancımız, sağlık, finansal ve sosyal bağlantılarımız, arkadaş çevremiz, sosyal durumumuz gibi kişisel gizliliğimizi ilgilendiren konularda çıkarsama yapılmasını sağlamaktadır. Online ayak izlerimizin dışında trafik kontrol kameralarından güvenlik kameralarına, akıllı şehir ve evlerden giyilebilir elektronik cihazlara kadar birçok alanda hayatımıza giren sensörler (alıcılar) ve sensör (algılayıcı) teknolojiler günümüz dünyasının bizleri izleme araçları arasında yer almaktadır. Sensörler ve hızla gelişen sensör teknolojileri devlet planlaması ve hizmetleri, şehir yönetimi, kamu güvenliği, sağlık hizmetleri, ekonomik kalkınma ve insanların gündelik yaşamları başta olmak üzere birçok alanda iyileştirme ve gelişme sağlarken diğer taraftan kişisel gizlilik ve güvenliğimiz için büyük riskleri de beraberinde getirmektedir (Tan ve Pivot, 2015).

Ayrıca çok yaygın şekilde kullanılan internet ve hızla gelişen bulut bilişim online verilere ulaşmayı ve toplamayı çok daha kolay ve etkili hale getirmiştir. Nesnelerin interneti ya da kablosuz sensör teknolojileri ise bilgi teknolojileri dünyasının en önemli gelişmeleri arasındadır. Bu teknolojilere sahip işletmeler ya da hükümetler ise hiç şüphesiz kişisel bilgi ve verilerimize çok kolay ulaşarak bunları kendi amaçları doğrultusunda iznimize olmadan kullanabilmektedir. Bu nedenle günümüzde gizlilik ve güvenlik konuları araştırmacılar tarafından büyük bir önemle ele alınmakta insanların bu konuda karşı karşıya oldukları riskler konusunda farkındalıkları artırılmaya çalışılmaktadır (Tan ve Pivot, 2015).

2.1.3. Bilgi Gizliliği ve Kişisel Verilerin Korunması Kanunları

Tüketiciler satın alma davranışları, online arama alışkanlıkları ve diğer online ve offline faaliyetleri hakkındaki bilgilerin sıklıkla anında ve gizlice toplandığı, analiz edildiği, birleştirildiği, kullanıldığı ve paylaşıldığı bir dünyada yaşamaktadır. Teknolojik gelişmeler ve yeni iş modelleri tüketicilere ait verilerin toplanması, paylaşılması, depolanması ve işlenmesi maliyetlerini düşürmektedir (Ramirez ve diğerleri, 2016). Bu bağlamda hükümetlerin ve online işletmelerin yeni teknolojilerin değişimi ve işletme faaliyetlerine nasıl cevap verecekleri bilgi ve veri gizliğinin geleceğini belirlemektedir.

ABD bilgi ve veri kaynağı olan büyük verinin en büyük üreticisi ve yöneticisi konumundadır. ABD başkanı Bilim ve Teknoloji danışmanlarından oluşan Başkanlık Konseyi tarafından sunulan “Büyük Veri ve Gizlilik” adlı rapor (PCAST), büyük veriden yararlanmak konusunda ABD’nin kararlılığını göstermektedir. Bu

raporda “teknolojiyi daha etkili kullanarak devletin gizliliğe yönelik endişeleri sınırlamak koşuluyla bilgi teknolojilerinin özellikle büyük verinin faydalarından büyük ölçüde yararlanmak suretiyle uluslararası anlamda önderlik edebileceği” belirtilmektedir (PACST, 2014). ABD’nin veri gizliliğinin üstesinden gelme yolu ise daha az sınırlayıcı, sektörel ve daha sıkı cezalarla olmak kaydıyla öz denetim olmak üzere üç şekilde özetlenmektedir (Kugler, 2015). Bir bütün olarak ABD sağlık ve finans ile ilgili bilgilerin toplanmasında daha fazla sınırlayıcı iken online pazarlama konusunda daha az sınırlayıcıdır (Davenport, 2013). ABD’den farklı olarak kişisel verilerin korunmasına ilişkin ilkeler AB’de tüm sektörlerde uygulanırken, ABD’de bu durum sektörler göre değişmektedir (Kugler, 2015). Son olarak ABD’deki genel eğilim öz denetim konusunda şirketlere güvenme şeklindedir ve doğal olarak bu kişisel verilerin korunmasında dogmatik bir yaklaşım olmamaktadır (Economist, 2012).

ABD’deki ilk federal gizlilik kanunlarından birisi tüketicilerin korunması için kurulan Federal Ticaret Komisyonu (FTC) tarafından hazırlanan 1970 tarihli Adil Kredi Raporlama Yasasıdır. 1974 tarihli Kişisel Bilgilerin Korunması Kanunu ise hükümetlerin kişisel bilgi kayıtlarını nasıl toplayabileceği ve kullanabileceğini düzenlemiş ve bireylere kişisel bilgilerine erişim ve bunları doğrulama hakkı vermiştir (Freivogel, 2015). ABD’de veri korunması uygulamaları 1986’da sunulan şeffaflık, onay ve doğrulama özelliklerini kapsayan Adil Bilgi Uygulamaları Kodları ile başlamıştır (Camp ve Connelly, 2008). Daha sonra FTC (2000) adil bilgi uygulamalarını “fark etme, seçme, erişim, güvenlik ve etkili hale getirme” olarak belirlemiştir. FTC (2010, 2012) 2010 ve 2012 yıllarında politika yapıcılar ve şirketler için birtakım önerileri de içerecek şekilde tüketicilerin gizliliğini korunmasına yönelik bir düzenleme yayımlamıştır. En son gerçekleştirilen yasal düzenleme ise 1974 yılında kabul edilen Kişisel Bilgilerin Korunması Kanunun Federal İletişim Komisyonu (FCC) tarafından revize edilmiş ve kabul edilmiş mahremiyet (gizlilik) kurallarıdır. Bu kurallar FCC’nin her bir bireyin Komisyon sisteminde ya da kayıtlarında tutulan, korunan bilgilerinin gizliliğini ve doğruluğunu temin etmeye yönelik bir politikadır (FTC, 2018). 1974 tarihli Kişisel Bilgilerin Korunması Kanununda da belirtildiği üzere bu kuralların temel amacı Federal Hükümetlerin ihtiyaç duyduğu bilgi ile bireylerin gizlilik hakkı arasında makul bir denge ilişkisi sağlamaktır. FCC’nin (2010) Kişisel Bilgilerin Korunması Kanunun 13. Bölümü ise Twitter, Facebook gibi üçüncü taraf sosyal medya sitelerinin açıklık, şeffaflık, kamu katılımı ve işbirliği ilkeleri çerçevesinde federal kurumlara her türlü hükümet erişimi vermesi ile alakalıdır. FCC bu bölümde sosyal medya kullanıcılarının gizliliklerini korumak için ciddi bir önem gösterdiğini belirtmektedir.

FCC tarafından son şekli verilen Kişisel Bilgilerin Korunması Kanunu ABD Başkanı Barack Obama tarafından kabul edilen yeni mahremiyet kuralları sayesinde internet servis sağlayıcılarının kullanıcı bilgilerini içeren verileri üçüncü taraflarla paylaşılmasının önüne geçmekteydi. Ancak geçtiğimiz yıl ABD Temsilciler Meclisi, Başkan Obama döneminde FCC tarafından onaylanan bu kuralları iptal eden yasa tasarısını kabul etmiş ve yasa yeni haliyle Başkan Donald Trump’ın imzası ile

yürürlüğe girmiştir. Yeni Kişisel Bilgilerin Korunması Kanunu online kullanıcıların tarama geçmişleri, konum bilgileri, kullandıkları uygulamalar gibi birçok kişisel veri üzerinde şirketlere izinsiz işlem yapma imkanı verirken diğer taraftan hükümetlere güvenlik gerekçeleriyle kişilere ait her türlü bilgi ve veriye istedikleri gibi ulaşma ve bunları kullanma yetkisini vermektedir (Milord, 2017). Dolayısıyla FCC tarafından belirlenen yeni mahremiyet kurallarına göre online gizlilik ve güvenliğin büyük ölçüde ortadan kalktığı ifade edilmektedir (Collins, 2017; Howell, 2018).

Türkiye’de kişisel verilerin korunmasına ilişkin düzenlemeler yapılması gerektiği ilk olarak 2003 yılında Avrupa Birliği (AB) Katılım Ortaklığı Belgesi’nde yer alan ilgili bir madde ile gündeme gelmiştir. Daha sonra bu madde Türkiye’nin AB’ye Katılım Ulusal Programı çerçevesinde kabul edilmiş ve Türkiye’de bir veri koruması yasa taslağının oluşturulmasının ilk denemeleri 2008 yılında gerçekleştirilmiştir. Ancak kişisel verilerin korunması konusunda kanun yapımının ivme kazanması, Aralık 2014’te Kişisel Verilerin Korunması Kanun (KVKK) tasarısının oluşturulması ve ilgili AB kurumları ve yerel sivil toplum gruplarına yasal yorumları için iletilmesi ile gerçekleşmiştir. Yapılan değişiklikler yeniden düzenlenen ve Meclis’e 18 Ocak 2016 tarihinde sunulan kanun tasarısında yer almıştır (Ünver ve Kim, 2016).

KVKK’nın temel misyonu “Anayasada öngörülen özel hayatın gizliliği ile temel hak ve özgürlüklerin korunması kapsamında, ülkemizde kişisel verilerin korunmasını sağlamak ve buna yönelik farkındalık oluşturarak bilinç düzeyini geliştirmek, aynı zamanda veri temelli ekonomide özel ve kamusal aktörlerin uluslararası rekabet kapasitelerini artırıcı bir ortam oluşturmak” olarak belirlenmiştir (KVKK, 2017). Kanunun amacı ise birinci maddede “kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemek” olarak ifade edilmektedir (KVKK, 2016).

Kanunda KVKK’nın kimler hakkında uygulandığı, kişisel verilerin işlenmesinin ne olduğu, kişisel verilerin nasıl hukuka uygun işlenmesi gerektiği, kişisel verilerin korunmasında veri sahiplerinin haklarının neler olduğu, veri sorumlusu ve veri işleyenin sorumlulukları neler olduğu, hangi hallerde kişisel veri sahiplerinin kişisel verilerin paylaşılması ile ilgili açık rızası aranmadığı konuları düzenlenmektedir (KVKK, 2016).

KVKK’nın çıkış noktası, internet kullanıcılarına ait kayıtların ve bilgilerin bireyleri fişleme için kullanıldığı düşüncesinin önüne geçmek olarak belirtilmektedir. Ayrıca Kanun, mevcut yasal sistemin, kişisel verilerin kamu ve özel sektör tarafından suiistimal edilmesini engellemediğini, bu verileri kimin topladığı ve nasıl işlediğine dair belirsizlik olduğunu öne sürmektedir. Ünver ve Kim (2016) KVKK’nın oluşturulmasının gerekçelerini ve mevcut yasal çerçeveyi “Türkiye’de Veri Gizliliği ve Gözetimi: Kişisel Verilerin Korunması Kanunu Tasarısının Değerlendirmesi” adlı çalışmalarında Ekonomi ve Dış Politikalar Araştırma Merkezi (EDAM) için değerlendirmiştir (bakınız tablo 3). EDAM’ın genel değerlendirmesi ise Kanunun asıl amacının Türkiye’deki Veri Koruma Kanunu’nu AB müktesebatı ile

uyumlaştırmak olduğu bu çerçevede, kanun tasarısının iki temel sorunu bulunduğu şeklindedir. İlk sorun kanun tasarısının Veri Koruma Kurulu'nun bağımsızlığına ilişkin şüpheler olup İkinci sorun kişisel verilere erişim ile ilgili kamuya tanınan geniş istisnalar olarak belirtilmektedir (Ünver ve Kim, 2016).

Tablo 2: KVKK'nın Değerlendirilmesi

Kişisel Verilerin Tanımlanması	Kişisel kimliği, iletişim bilgilerini, sağlık ve mali bilgiler, dini, özel ve siyasi görüşleri belirli hale getirebilecek her tür bilgi.
KVKK Kanununun Gereksinimleri	- Kişisel verilerin kullanımının özel sektör ve kamu sektörü tarafından istismar edilebilmesi. - Bu verilerin yetkisiz bireyler tarafından kullanılması ifşalara, istismara ve Anayasa ile Türkiye'nin taraf olduğu uluslararası sözleşmelerin ihlaline yol açabilmesi. - Ticari faaliyetleri kolaylaştırmak için verilerin sınırsız akışı ile bu verilerin istismar edilmesinin önlenmesi arasında makul bir yasal denge oluşturulması gereksinimi. - Kişisel verilerin kullanımı ve işlenmesi üzerine yasal dayanak ve denetim mekanizması olmamasının bu tür verilerin kullanılması konusunda genel geçer bir şüpheye yol açması. - Türk veri koruma kanunlarını geliştirmiş ülkelerin yasalarıyla uyumlu hale getirme ihtiyacı. - Türkiye güvenlik birimleri ve EUROPOL arasında polis ve güvenlik işbirliği ve istihbaratın elektronik transferi konularında uyumluluğun sağlanması için yeni yasa ihtiyacı. -EUROJUST ile koordinasyonun zedelenmesi ve bunun ortak mücadele operasyonlarını engellemesi. - Sağlık kurumları tarafından toplanan kişisel verilerin artan miktarının gittikçe sorunlu hale gelmesi ve bu kurumların veri saklamak için yasal temelleri veya yeterli güvenlik çerçevelerinin olmaması. - AIHS'nin bu boşluğu kişisel gizliliğin ihlali olarak değerlendirmesi. - Yurtdışında yaşayan Türk vatandaşlarının, askerlik durumu, vatandaşlık ve mali varlıkları konusundaki bilgilerinin paylaşımıyla ilgili sorunların olması ve bunun, Türkiye'deki yasal durumlarını karmaşılaştırması. - Kişisel veri kullanımı kanunundaki yetersizliklerin doğrudan yabancı yatırımların ve Türkiye içindeki yabancı anaparanın yönetimine zarar vermesi. - Bu yasal boşlukların yatırımcıların Türkiye'deki yatırım ve ticari faaliyetlerini geliştirmesini caydırması ve Türk işadamlarının yurtdışına iş ortaklıkları kurmasını kısıtlaması.
Mevcut Yasal Çerçeve	- 5237 Sayılı Türk Ceza Kanunu Madde 135: Kişisel verilerin hukuka aykırı toplanması ve ifşası - Belirlenen Problem: Bu eylemlerin ne zaman yasal ve yasadışı olduğu konusuna yasal açıklık ve karışıklık. - Anayasa Değişikliği (2010 Referandumu) Madde 20: Kişisel verilerin korunması temel bir insan hakkı sayılır. - Avrupa Birliği Katılım Çerçevesi: Katılım Müzakerelerinin

	Dört Faslı kişisel verilerin korunmasıyla alakalıdır. Bu dört fasılda ilerleme kaydedilmesi için yeni, konuya özel bir yasaya ihtiyaç vardır. - Kişisel verilerin korunması Türkiye'nin AB Katılım Ortaklığı Belgesine 2003'te verdiği yanıtta vadedilmiştir. - 64. Hükümet Programı bir Acil Eylem Planı yayınlamış, planda kişisel verilerin korunması reformunun üç ay içerisinde gerçekleştirilmesi vadedilmiştir. - Türkiye OECD'nin 1980 tarihli Mahremiyetin Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkelerine taraftır. - Türkiye Avrupa Konseyi'nin 1981 tarihli Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesine (CETS No. 108) taraftır. - Türkiye Avrupa Parlamentosu ve Konseyi'nin 24 Ekim 1995 tarihli, bireylerin kişisel verilerin işlenmesi ve bu verilerin serbest dolaşımına karşı korunması 95/46/EC Direktifine taraftır.
--	--

Kaynak: Ünver ve Kim, 2016 "Türkiye'de Veri Gizliliği ve Gözetimi: Kişisel Verilerin Korunması Kanunu Tasarısının Değerlendirmesi"

2.2.Sosyal Medya ve E-Ticaret

Günümüz dünyasında bilgi ve haberlerin birkaç kişi tarafından sahip olunup milyonlara dağıtıldığı bir dönemden milyonlar tarafından sahip olunan çok farklı türden ve büyük boyuttaki bilginin birkaç kişiye (niş pazarlara) dağıtıldığı bir döneme geçmiş bulunmaktayız (Qualman, 2010). Şüphesiz bu dönemin en belirleyici unsuru olarak karşımıza çıkan İnternet ve web 2.0 gibi teknolojiler beraberinde bilginin hızla yayılmasını sağlayan ve etki gücü her alanda çok yüksek olan sosyal medyayı getirmiştir. Her gün çok sayıda insan bilginin ve verinin en önemli kaynaklarından biri olan sosyal medya ağının bir parçası olmaktadır. Öyle ki en popüler sosyal medya uygulaması olan Facebook'un 2 milyarı aşan üye sayısı dikkate alındığında dünyadaki her bir devletten daha fazla nüfusa sahip olduğu belirtilmektedir (Tuten ve Solomon, 2017).

İnternet ve web 2.0 teknolojileri sadece sosyal medyanın gelişmesini sağlamamış e-ticareti de hayatımızın önemli bir parçası haline getirmiştir. Özellikle Amazon gibi online alışveriş sitelerinin ortaya çıkışı daha sonra e-ticaretin sosyal medya uygulamalarını da kapsayacak şekilde gelişmesi bilgi teknolojileri çağında ekonomik, sosyal ve siyasal anlamda nasıl bir dönüşüm geçirdiğimizi görmek açısından son derece önemlidir. Sosyal medyanın ulaştığı büyüklük ve sosyal ağlardaki etkileşim sosyal medyayı etkili bir reklam ve pazarlama aracı haline getirmiştir. Bununla birlikte sosyal ticaret kavramı ortaya çıkmıştır. Bu kavramı online alışveriş olarak tanımlayabileceğimiz gibi iki şekilde gerçekleştiğini de görmekteyiz. Bunlardan birisi e-ticaretin en önemli aracı olan ve bazı sosyal medya siteleri (uygulamaları) ile bütünleşik çalışan online alışveriş siteleri (uygulamaları) iken diğeri alış-veriş fonksiyonlarına sahip sosyal medya uygulamalarıdır. Bu

çerçevede aşağıdaki bölümlerde sosyal medya ve e-ticaret kavramları üzerinden çeşitli değerlendirmeler yapılmaktadır.

2.2.1. Sosyal Medya ve Gelişimi

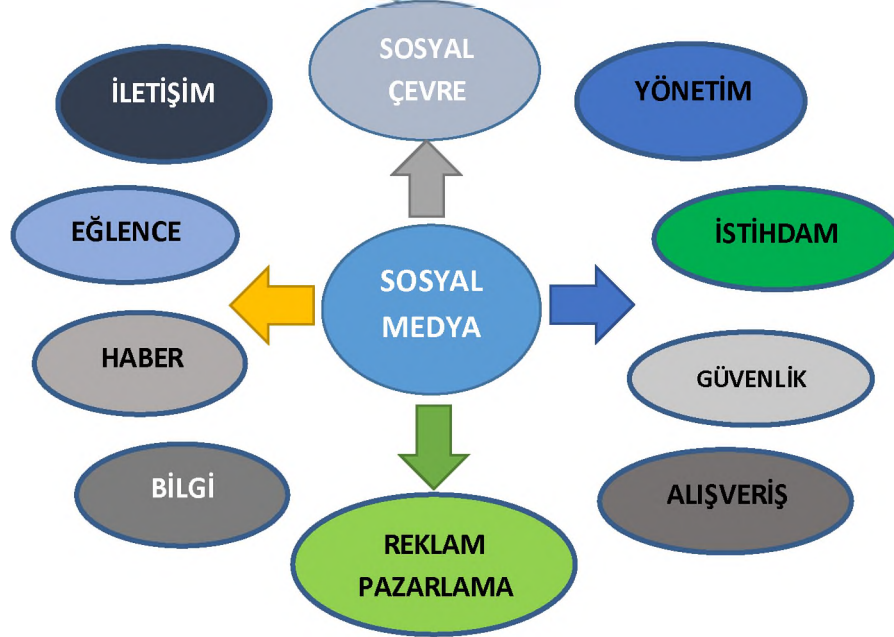
Sosyal medya sürekli olarak gelişen ve değişen, uzmanların üzerinde uzlaştıkları tek bir tanımlı olmayan web tabanlı bir kavram olarak karşımıza çıkmaktadır. Birçok kişi sosyal medyayı en bilinen uygulamalar olan Facebook ve Twitter gibi sosyal ağlar ile özdeşleştirmektedir. Sosyal medyanın en bilindik tanımını Mayfield (2008) insanların iletişim için kullandıkları katılımcılık, açıklık (gizlilikten kaçınma), karşılıklı konuşma, topluluk (ortak yön) ve bağlantılık özelliklerine sahip bir araç olarak yapmaktadır. Ayrıca sosyal medyanın sosyal ağlar (Facebook vb.), bloglar, wikiler (herkesin üzerinde istediği gibi düzenlemeler yapmasına izin veren bilgi sayfaları topluluğu), podcastler (internette hazırlanan veya sonradan internete kopyalanan yayınlar), forumlar, kullanıcıların geliştirdikleri içerikler (youtube videoları gibi) ve mikrobloglar (twitter gibi) olmak üzere karşımıza çıktığını ifade etmektedir (Mayfield, 2008). Mayfield'in tanımından sıklıkla birbirleri yerine kullanılabilen sosyal medya ve sosyal ağlar kavramlarının aslında birbirinden farklı olduğu sosyal ağların sosyal medyanın sadece bir bileşeni olduğu ifade edilebilir. Bu konuda Edosomwan ve arkadaşları da sosyal medya ve sosyal ağ kurmanın (social networking) birbirleri ile bağlantılı olarak kullanılması gereken kavramlar olduğunu belirtmektedir. Zira Edosomwan ve arkadaşları yaptıkları çalışmada sosyal ağ kurmayı iş ya da istihdam gibi amaçlar için kullanılan bilgi alışverişi olarak tanımlarken sosyal medyayı sosyal ağ kurmanın elektronik şekli olarak tanımlamaktadır (Edosomwan, 2011).

Online sözlük alanında faaliyet gösteren Merriam-Webster (2018) Şirketi sosyal medyayı "bilgi, fikir, kişisel mesajlar ve farklı içeriklerin paylaşımı için kullanıcılar tarafından oluşturulan online topluluklar üzerinden kurulan elektronik iletişim şekli (web siteleri aracılığıyla sosyal ağ kurma ya da mikro blogging oluşturma şeklinde" olarak tanımlamaktadır. Bununla beraber son yıllarda sosyal medya hızla gelişerek kişisel etkileşimden daha fazlası haline gelmiştir. Artık toplanan çok büyük hacimdeki bilgi ile sosyal medya; iş ya da ticari kararlar alınması, kamu sağlığı, psikolojik araştırmalar ve birçok farklı amaç için kullanılmaktadır. Sosyal medyaya olan bu ilgi sosyal medyayı her geçen gün daha da popüler hale getirmektedir.

Diğer taraftan Tracy L. Tuten ve Michael R. Solomon "Social Media Marketing" adlı çalışmasında Sosyal Medyayı içerisinde çok sayıda etkileşim kanalının bulunduğu 4 alandan oluşan bir mecra olarak tanımlamaktadır. Bu alanlar çalışmada sosyal topluluk (paylaşım, sosyalleşme, konuşma), sosyal yayıncılık (editöryal, ticari, kullanıcı tarafından oluşturulan), sosyal eğlence (oyun, müzik, sanat) ve sosyal ticaret (müşteri ilişkileri yönetimi, perakende satışlar, insan kaynakları) olarak ifade edilmektedir. Sosyal medyanın kullanım amaçları; sosyal bir çevre oluşturmak, farklı kişilerle etkileşime geçmek, araştırma yapmak, bilgi edinmek-paylaşmak, resim video gibi paylaşımlarda bulunmak, iş aramak hatta ürün satmak ya da satın almak gibi faaliyetler olarak sıralanmıştır. Bunların yanında sosyal medyanın şirketler için

reklam aracı ya da hükümetler ve siyasi partiler için propaganda aracı olarak kullanılmakta olduğu belirtilmiştir (Tuten ve Solomon, 2014). Hatta sosyal medya istihbarat teşkilatları ya da farklı örgütler için çok farklı amaçlar için kullanılan bir platform haline gelmiştir. Öyle ki sosyal medyanın Tunus'tan başlayarak Kuzey Afrika'ya oradan da Orta Doğu'ya yayılan Arap Baharı sürecinde çok etkin bir araç olarak kullanıldığını söyleyebiliriz (Badoura, 2013). Ancak bu tür konular bilgi teknolojileri dünyasında birbirleri ile bağlantılı olsa da farklı disiplinleri ilgilendirmektedir. Dolayısıyla araştırmanın asıl konusunu kişisel verilerin gizliliği ve güvenliği çerçevesinde sosyal medyanın işletmeler için bir pazarlama ve reklam aracı olarak artık sıklıkla kullanılmasını oluşturmaktadır. Zira sosyal medya işletmelerin tüketici düşüncelerini takip edebildikleri, bu düşüncelere yön veren çevresel etmenleri inceleyebildikleri ve tüketicilerin tercihlerini etkilemeye çalıştıkları bir pazarlama aracı olarak karşımıza çıkmaktadır. Bu bağlamda işletmeler kendi çıkarları için kişilerin veri gizliliği ve güvenliğini tehdit ederek farklı sorun ve endişeleri de beraberinde getirmektedir.

Şekil 1: Sosyal medyanın bazı kullanım amaçları



Günümüzde çok sayıda sosyal medya uygulaması bulunmaktadır. Bu uygulamaların sosyal medya olarak kabul edilebilmesi için ise belli kriterler bulunmaktadır. Bunlar: “Sınırları belli olan bir sistemin içerisinde sistemde tanımlı olan herkesin görüntüleyebileceği tam ya da yarı açık bir kişisel profil oluşturabilme yeteneği; bir ilişkinin ya da bir bağın paylaşıldığı diğer kullanıcıların yer aldığı kolay erişebilir bir liste sunma; kişinin çevresinde yer alan kişilerin bağlantılarına ulaşabilme hakkı tanımadır” (Dilmen, 2010). Dolayısıyla bu kriterler çerçevesinde sosyal medya ve uygulamaları hızla gelişerek hayatımızın ayrılmaz parçaları haline gelmiştir. Günümüzdeki bu sosyal medya kriterlerine uygun ilk web tabanlı uygulamalara Classmates.com (1995) ve SixDegrees.com (1997) örnek olarak gösterilmektedir. Classmates.com özellikle geçmişteki sınıf arkadaşlarının bulunmasına yönelik bir tema sunarken, SixDegrees.com kişiler arası ilişkilerde bir bağ aramamaktaydı. Daha

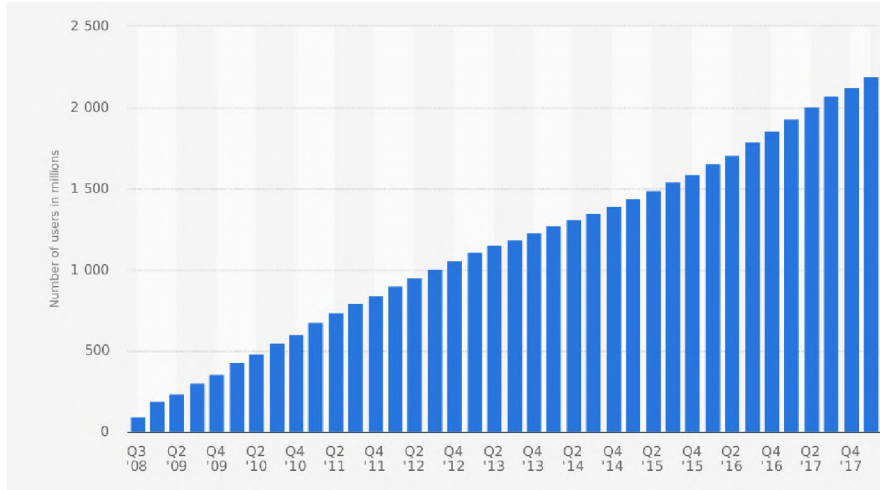
sonra bu web sitelerini 1997 – 2001 yılları arasında LiveJournal, AsianAvenue, BlackPlanet, LunarStorm, MiGente gibi büyük çaplı sosyal medya siteleri takip etmiştir. 2003 yılında ortaya çıkan Myspace ve LinkedIn gibi uygulamalar ise hala güncel olarak sıklıkla kullanılmakta olan popüler uygulamalar arasında yer almaktadır (Dilen, 2010). Ancak hiç şüphesiz sosyal medyanın gelişiminin en büyük örneği bugün milyarlarca kullanıcıya sahip 2004 yılında kurulan Facebook'tur. Facebook'un yanında Whatsapp, Youtube, Instagram, Twitter gibi uygulamalar ise sosyal medyanın gelişen ve yenilenen yüzü olmuştur. Aşağıdaki bölümde sosyal medyanın en popüler bu yenilikçi uygulamaları değerlendirilmektedir.

2.2.2. Sosyal Medya Uygulamaları

Sosyal Medyanın çok farklı amaçlar için kullanılan bir bilgi paylaşımı, etkileşim ve iletişim aracı olduğundan hareketle sosyal medyanın en çok kullanılan ve en popüler uygulamaları olarak Facebook, Twitter, Whatsapp, Youtube ve Instagram ön plana çıkmaktadır.

Facebook: Facebook Şubat 2004'de Harvard Üniversite o zaman öğrenci olan Mark Zuckerberg tarafından kurulan bir sosyal paylaşım sitesidir. İlk defa kullanılmaya başlandığında Facebook sadece Harvard öğrencilerinin kullanımı ile sınır bir web sitesi iken sonradan önce lise öğrencilerinin daha sonra 13 yaşından büyük herkesin kullanımına açılmış bir web sitesi haline gelmiştir. (Edosomwan, 2011). 2018 yılı itibariyle Facebook'un aylık olarak aktif kullanıcı sayısı 2,2 milyar civarındadır (Statista, 2018). Grafik 1'de Facebook'un son 10 yıl içerisindeki kullanıcı sayısının gösterdiği artış görülmektedir. Facebook 2018 yılı itibariyle 90 milyar civarındaki marka değeri ile dünya markaları arasında 5'nci sırada yer almaktadır (Statista, 2018).

Şekil 2: 2008 – 2018 yılları arasındaki Facebook kullanıcı sayısı



Kaynak: Statista, (2018). Number of monthly active Facebook users worldwide as of 1st quarter 2018 (in millions).

Bu sosyal paylaşım sitesinde kullanıcılar kişisel profil oluşturmakta, diğer kullanıcıları arkadaş olarak eklemekte ve birbirlerine mesaj gönderebilmektedir. Bu temel özelliklerinin yanında kullanıcılar resim, video, metin gibi her türlü içeriği

birbirleri ile kişisel profilleri aracılığıyla paylaşabildiği gibi bu paylaşımlar için Facebook'da kurulan grup ya da sayfaları da kullanabilmektedir. Ayrıca başkalarının yaptığı paylaşımları beğenme ve bunlara yorum yapma imkanı da bulunmaktadır.

Facebook'da çok sayıda ortak çıkarları ilgilendiren ya da belli bir amaca yönelik çok sayıda grup ve sayfa bulunmaktadır (Türkiye'de en popüler olanlar olarak onedio.com, TuhafAmaGerçek vb). Bu özelliklerinin yanında Facebook'un günümüzde işletmeler tarafından bir reklam ve pazarlama aracı olarak da sıklıkla kullanıldığını görmekteyiz. McEleny'e göre Facebook'un Nearby (yakınında) ve İ-crossing uygulamaları konum esaslı pazarlama anlayışının temel kaynağını oluşturmaktadır. Benzer şekilde durum güncellemesi, abonelik ya da beğenme gibi Facebook ile özdeşleşen özellikler üzerinden işletmeler kullanıcıların ilgi alanları ve alışkanlıklarına nelere ihtiyaçları olduklarına erişim olanağı sağlamaktadır (Dang, 2013). Türkiye'de Facebook'un hazır giyim firmaları tarafından ne şekilde kullanıldığı ve yapılan pazarlama faaliyetlerinin tüketiciler üzerindeki etkileri incelendiği bir araştırmada firmaların, hedef müşteri kitleleri ve sosyal ağlardan beklentileri doğrultusunda bir Facebook stratejisi oluşturdukları görülmüştür. Bu stratejinin başarılı olması halinde Facebook'un firma bilinirliğini ve tüketici bağlılığını artırdığı ve firmanın satışlarını olumlu yönde etkilediği belirlenmiştir (Kara ve Coşkun, 2012). Örneğin CNBC-e Business Magazine'e göre sosyal medyayı en iyi kullanan 25 şirketten biri olan dünyaca ünlü Türk Firması Mavi Jeans sosyal medyayı özellikle Facebook'u etkin olarak kullanan firmalar arasındadır. American Stylophane Company tarafından hazırlanan sosyal medya raporunda marka hayranlığı dikkate alındığında Mavi Jeans'ın Platinyum kategorisinde dünyadaki tüm markalar arasında 8'inci olduğu, müşteri ile etkileşim konusunda ise 1'nci olduğu belirtilmiştir (Cukul, 2012). Bu konuda online alışveriş sitelerinin dahi yeni gelişen bilgi teknolojileri sayesinde kullanıcıya uygun ürün tavsiyelerinde bulunarak reklam ya da pazarlama aracı olarak Facebook'u kullandıkları görülmektedir.

Twitter: 2018 yılı itibarıyla aylık kullanıcı sayısı 336 milyonu (Statista, 2018) bulan Twitter mikro blog hizmeti veren bir sosyal medya uygulamasıdır. Mikro blog kullanıcılara kısa cümleler, anlık fotoğraflar veya video linkleri gibi küçük içerik parçalarını paylaşmak için ortam sağlayan bir mekanizmadır. Bu özelliği ile diğer sosyal paylaşım ağlarından ayrılan Twitter 2006 yılında kurulmuş ve 12 yıl içerisinde en etkin interaktif sosyal paylaşım ağlarından birisi olmuştur.

Twitter açık, gerçek zamanlı, basit ücretsiz ve esnek bir uygulamadır. Kullanıcılarına günlük faaliyetlerini paylaşma ya da yayınlama imkanı veren uygulama kullanıcılarına basit ama etkili özellikler sunmaktadır (Taecharungroj, 2017). Twitter'da kısa mesajlara tweet adı verilmektedir. Yakın zamana kadar 140 karakter ile sınırlı olan bu kısa mesaj servisi 2017 yılı itibarıya 280 karaktere çıkartılmıştır (NTV, 2017). Bir kişi Twitter'da başka bir kişiyi ya da bir grubu, bir firmayı, bir markayı haber kaynağında ona ait mesajları alabilmek için gönüllü olarak takip edebilmektedir. Etkileşim Twitter'ın en önemli özelliklerinden biri olarak karşımıza çıkmaktadır. Dolayısıyla bu uygulamada kullanıcılar bir başkasına ait tweeti (mesajı)

retweet (yeniden yayınlamak) yaparak tweetin daha fazla kişiye ulaşmasını sağlamaktadır. Bir başka ifadeyle birbirine bağlı zincirleme bir etkileşim söz konusudur. Ayrıca kullanıcı “@” işaretinin yanına diğer kullanıcının adını yazmak suretiyle bu kişiden bir paylaşımında bahsedebilir ya da ona cevap niteliğinde bir tweet yayımlayabilir. Twitter’da normalde karşılıklı konuşmalar düzensiz bir şekildedir. Ancak anahtar bir kelimenin önüne konulan “#” hashtag işareti ile kullanıcılar ilgilendikleri bir konu hakkında mesajlar ya da konuşmalar arasında arama yapabilmektedir (Taecharungroj, 2017).

Twitter günümüzde kamu kurumları, siyasetçiler ya da ünlülerin geniş kitlelere ulaşmak için kullandığı elverişli bir iletişim mekanizması haline gelmiştir. Bu anlamda özellikle özel sektörde birçok kurum, takipçileriyle iletişime geçerek çeşitli etkinlikler organize etmekte çeşitli kampanyalar düzenlemektedir. Twitter’da en çok tercih edilen kampanya yöntemleri, tweetlerin kullanıcılar tarafından retweet edilerek daha fazla kitleye ulaştırılması üzerinedir. Birçok şirket Twitter’ı bir pazarlama ve reklam aracı olarak kullanmak için yatırımlar yapmaktadır. Örneğin 11 milyon takipçisi bulunan Starbucks firması müşterileri ile twitter üzerinden güçlü bir iletişim ve etkileşim halindedir. Starbucks Twitter sayesinde takipçileri ile sürekli, açık, aktif, interaktif ve merak uyandıran bir ilişki gerçekleştirmiştir.

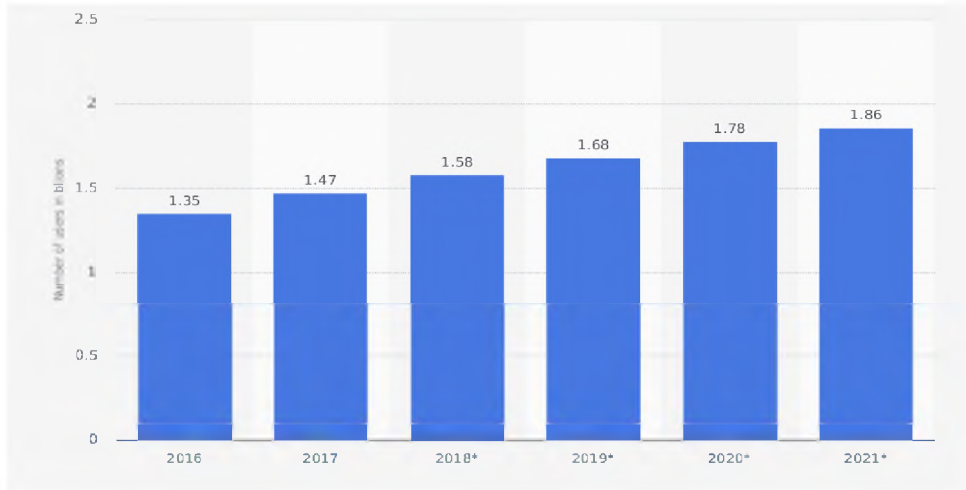
WhatsApp: Akıllı telefonlar için ücretsiz bir mesajlaşma uygulaması olarak geliştirilen WhatsApp zamanla geliştirilen yeni özellikleri ile mesajlaşma aracı olmanın ötesine geçmiş bir uygulamadır. Özellikle gençler arasında yaygın bir şekilde kullanılan bu uygulama zamanla her yaştan insanın çok farklı amaçla sıklıkla kullanır hale geldiği bir sosyal paylaşım ağıdır. Metin mesajı göndermek için kullanılan bu uygulama ile kullanıcılar birbirlerine resim, video, sesli mesaj ve konum bilgisi de gönderebilmektedir. Grup konuşmaları için de sıklıkla kullanılan bu uygulama telefon numaranızı kullanıcı adı olarak kullanmakta olup kullanıcı profiliniz numaranız ile birlikte başka bir telefona da aktarılabilmektedir (Ehibudu, 2017).

2009 yılında eski Yahoo çalışanları Brian Acton ve Jan Koum tarafından kurulan WhatsApp 2014 yılında 600 milyon kişi tarafından kullanılırken (Alsanie, 2015) 2018 yılı itibarıyla 1,5 milyarın üzerinde kullanıcı (Statista, 2018) sayısına ulaşmıştır. Apple IOS (Iphone), Android (Samsung, Sony vb), Windows (Nokia), Symbian (Nokia) işletim sistemi tabanlı yeni nesil akıllı telefonlarda kullanılabilen uygulama son yıllarda telefon görüşmeleri ya da görüntülü konuşma için de sıklıkla tercih edilir hale gelmiştir. Ayrıca WhatsApp sadece akıllı telefonlarda değil “web.whatsapp.com” adresi üzerinden masaüstü ya da dizüstü bilgisayarlarda kullanılabilir. Bunun için internetten ilgili adrese tıklanması karşınıza çıkan QR kodunu akıllı telefonla ile taramanız yeterli olmaktadır. Böylelikle WhatsApp uygulaması bilgisayar ile kullanılabilir (Mefolere, 2016). Bu da WhatsApp üzerinden bilgisayarınıza indirmek istediğiniz içerikler açısından son derece kullanışlı bir özelliktir. WhatsApp kullanıcılar açısından olduğu kadar işletmeler için de son derece faydalı bir uygulama haline gelmiştir. İşletme içi yönetim ve organizasyonlarda kolaylıklar sağladığı gibi işletmelerin müşterileri ile olan

iletiřimleri güçlendirmekte zaman zaman reklam ve pazarlama aracı olarak dahi kullanılmaktadır.

YouTube: Youtube milyonlarca insanın farklı türden videoları keřfedebileceęi, izleyebileceęi, paylařabileceęi ya da kendi videosunu oluřturabileceęi tartiřmasız dünyanın en popüler online sosyal medya uygulamasıdır. 2005 yılında kurulan ve yönetim merkezi San Bruno California’da bulunan uygulama kullanıcılar tarafından oluřturulmuř çok sayıda video içerięi barındırmaktadır. Bu videolar arasında film fragmanları, müzik klipleri, reklam filmleri, eęitici içerikli videolar ya da amatör içerikli kısa videolar olmak üzere sayamadığımız birçok türden video bulunmaktadır. Kullanıcılar bu videoları sadece izlemek ile yetinmemekte Adope Flash Video teknolojisini kullanan uygulama kurulduktan kısa bir süre 2006 yılında Google tarafından satın alınmıřtır. Youtube’un CBS, BBC, Universal Music Group, Sony Music Group, Warner Music Group, NBA, The Sundance Channel gibi birçok firma ile ortaklık iliřkisi bulunmaktadır (Edosomwan, 2016).

řekil 3: 2016 – 2021 yılları arası Youtube kullanıcı sayısının artışı



Kaynak: Statista, (2018). Number of YouTube users worldwide from 2016 to 2021 (in billions).

Youtube ilk kurulduęunda kuruculardan birinin yükledięi video fazla ilgi çekmemiř ama daha sonra Brezilyalı futbolcu Ronaldıno’nun oynadıęı, Nike firmasının reklam filmi ile dünyaca tanınır hale gelmiřtir. Bu reklam videosu o zaman 1 milyon kiři tarafından izlenmiřtir ve sonrasında Youtube’un yükseliři hızla devam etmiřtir (Akbulut, 2016). Bugün kullanıcı sayısı 1,5 milyarı bulan 2015 yılı istatistiklerine göre Youtube’a her dakika 400 saat video içerięi yüklenmektedir (Statista, 2017). Kullanıcı sayısının 2021 yılı itibariyle ise 1,9 milyara ulaşması beklenmektedir (bakınız řekil 3).

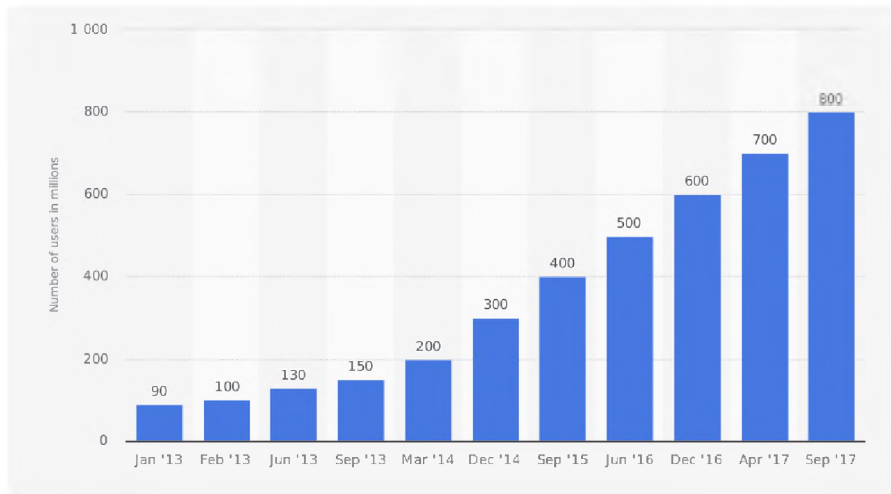
Brüt geliri 20 milyar doların üzerinde olan Youtube Facebook ve Twitter gibi dięer sosyal paylařım aęları ile bağlantılı bir uygulamadır. Ayrıca Youtube yükseliře geçmesinden bu yana kullanıcılarının paylařtıkları videolarının izlenme oranları ile orantılı olarak gelir elde ettikleri bir mekanizma haline gelmiřtir. Buna ilave olarak kullanıcılar ilgilendikleri videoyu izlemek için tıkladıklarında firmalara ait reklamları da izlemek durumunda kalmaktadır. Kullanıcı sayısı dikkate alındığında YouTube’un

işletmeler için iyi bir pazarlama ve reklam aracı olarak ne kadar etkili bir sosyal medya sitesi olduğu görülmektedir.

Instagram: Instagram Ekim 2010 yılında kurulmuş olan ancak çok hızlı bir şekilde dünya genelinde yaygın olarak kullanılmaya başlanmış resim paylaşmak suretiyle durum güncellemesi yapılan bir uygulamadır. Resim ya da video yakalama ve paylaşma uygulaması olarak tanımlayabileceğimiz Instagram kullanıcılarına içinde bulundukları anı yakalayıp resimleyerek anlık olarak takipçileri ile paylaşmanın aracı olarak karşımıza çıkmaktadır. Uygulama akıllı telefonlar için geliştirilmiş olmakla birlikte masa üstü ya da dizüstü bilgisayarlar kullanılarak da uygulamaya ulaşılabilmektedir. Resim ya da videolara çeşitli filtreler uygulama ile mesajlaşma özelliğine de sahip uygulama özellikle gençler arasında sıklıkla kullanılmaktadır.

2016 yılında 600 milyon kişi tarafından kullanılan Instagram'ı 2017 yılı sonu itibariyle aylık 800 milyon kişi kullanmaya başlamıştır. Türkiye'de ise 34 milyon aktif kullanıcısı bulunmaktadır (Statista, 2017). Bu rakamlar dikkate alındığında Instagram'ın kullanıcı sayısı yönünden daha önce kurulmuş olan sosyal medya uygulamalarına göre çok daha hızlı büyüdüğü görülmektedir (bakınız Şekil 4). Ayrıca uygulamanın ulaştığı bu rakamlar Instagramı şirketler ve işletmeler açısından önemli bir reklam ve pazarlama alanı haline getirmektedir. 2016 yılında aktif hale gelen Instagram'ın satın alma özelliği "Shop Now"ın önce Amerikalı pazarlamacılarla buluşmasının ardından kısa bir süre sonra Türkiye'nin içinde yer aldığı birçok ülkede bu özellik kullanılır hale gelmiştir. Böylelikle Instagram günümüzde online alışverişler için kullanılan önemli bir sosyal medya aracı olarak karşımıza çıkmaktadır. Çok büyük marka ve şirketlerden (BMW, Sony vb.) küçük çaplı işletmelere hatta yerel işletmelere kadar birçok firmanın ya da satıcının son zamanlarda Instagram'ı bir satış ve pazarlama aracı olarak kullandığı da görülmektedir. Bu çerçevede Instagram'da özellikle ünlü markalar ürünlerini direkt olarak tanıtmaktansa tüketicilerin ürünleri ile ilgili resim ve videolarını da bir pazarlama yöntemi olarak kullanmaktadır (Nummila, 2015).

Şekil 4: Instagram'ın 2013 – 2018 yılları arasındaki gelişimi



Kaynak: Statista, (2018). Number of monthly active Instagram users from January 2013 to June 2018 (in millions).

2.2.3. E-Ticaret ve Gelişimi

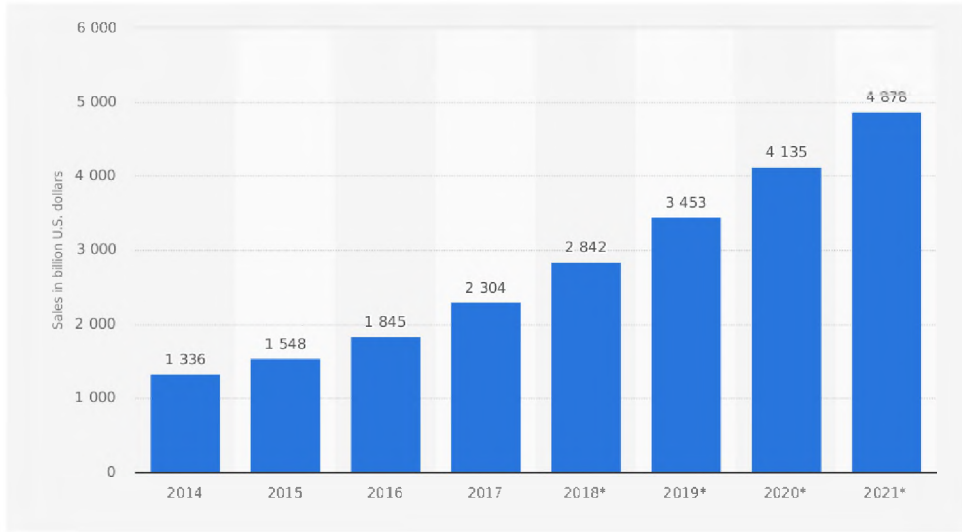
İnternetin gelişimi, kullanıcı sayısındaki büyük artış, internet üzerinden sunulan hizmetlere erişim kolaylığı ve daha birçok yenilikçi girişimler E-ticaret kavramını hayatımızın ayrılmaz bir parçası haline getirmiştir. E-ticaret yoluyla işletmeler, karlılıklarını arttırmak, pazar payını yükseltmek, müşteri hizmetlerini iyileştirmek, dağıtım kanallarını geliştirmek gibi faydalar sağlamaktadır. Ancak bu tanımlamadan e-ticaretin yalnızca online bir katalogdan ürün siparişi verme süreci olarak algılanmaması gerektiği ifade edilmelidir. Tam tersine e-ticaret, işletmenin işlemlerini ve tüm taraflarla (müşteriler, tedarikçiler, devlet, işçiler, yöneticiler vb.) olan iletişimini geliştirmek için bilgi teknolojilerinden yararlanmasını kapsamaktadır (Marangoz 2012).

Ekonomik İşbirliği ve Kalkınma Örgütü'nün (OECD) yaptığı tanıma göre E-ticaret bilgisayar ve internet üzerinden yapılan satış ve satın alma işlemleri olarak tanımlanmaktadır (Frederiksson 2013). Dünya Ticaret Örgütü (WTO) e-ticareti “mal ve hizmetlerin sunum, reklam, sipariş, satış ve pazarlama faaliyetlerinin telekomünikasyon ağları üzerinden yapılmasıdır” şeklinde ifade etmiştir. Türkiye Elektronik Ticaret Koordinasyon Kurulu (ETTK) ise e-ticareti “bireyler ve kurumların açık ağ ortamında (internet) ya da sınırlı sayıda kullanıcı tarafından ulaşılabilen kapalı ağ ortamlarında yazı ses ve görüntü biçimindeki sayısal bilgilerin işlenmesi, iletilmesi ve saklanması temeline dayanan ve bir değer yaratmayı amaçlayan ticari işlemlerin tümü” olarak tanımlamıştır (Gökgül, 2014).

Diğer taraftan e-ticaret daha çok online bir kavramı ifade etmekle birlikte içeriği itibarıyla sadece online işlemleri değil elektronik (dijital) olarak yapılan ticari tüm faaliyetleri kapsamaktadır. Zira e-ticaret yeni bir kavram olmasına karşın, çoğunlukla geleneksel ticaretin ilkelerinden faydalanmaktadır. Dolayısıyla e-ticareti geleneksel ticaretin alternatifi olarak değil de onun bir bileşeni olarak görmek te fayda vardır. Ancak ticaretin geleneksel yapıdan ve usullerden giderek uzaklaştığı, elektronik ortama taşındığı ve yeni ilke ve esaslar getirdiği de unutulmamalıdır. Bu noktada e-ticaretle geleneksel ticaret arasındaki en önemli farkın pazarların genişliği konusunda olduğu ifade edilmektedir (Yılmaz, 2015).

Şekil 5’de görüldüğü üzere 2018 yılı itibarıyla dünya genelinde perakende e-ticaret satışları 3 trilyon dolara dayanmış olup bu rakamın 2021 yılı itibarıya 5 trilyon dolara yaklaşması beklenmektedir. Toplam perakende satışları arasında yüzdesel olarak %23,1 ile en yüksek e-ticaret satışları Çin’de gerçekleşmektedir. Onu sırasıyla İngiltere, Güney Kore, Danimarka ve Amerika takip etmektedir. 2018 yılı verilerine göre online alışveriş yapan müşterilerin sayısı 1.8 milyar civarında olmakla birlikte bu sayının da 3 yıl sonra 2.2 milyar gibi bir rakama ulaşacağı tahmin edilmektedir. (Statista, 2018).

Şekil 5: Dünya perakende e-ticaret satışları



Kaynak: Statista,(2018). E-Commerce Worldwide.

Dünyada ilk e-ticaret uygulamasının başlangıcı olarak 1970 – 1980 yılları arasında gerçekleştirilen elektronik fon transferi (EFT) ve elektronik veri değişimi (EVD) işlemleri kabul edilmektedir. Daha sonra para çekmek için kullandığımız ATM Makinaları ve alışveriş için kullandığımız kredi kartlarının hayatımıza 1980’lerden sonra hızla girişi e-ticaret kavramını geliştiren uygulamalardır. Ancak e-ticareti en fazla geliştiren gelişme 1990’lı yıllarda hayatımızın ayrılmaz bir parçasını haline gelen World Wide Web (www) olmuştur. Peter Drucker, ‘Geleceğin Toplumunda Yönetim’ isimli kitabında e-ticaretin gelişimini “Demiryolu, sanayi devrimi için ne idiye, e-ticaret de bilgi devrimi için odur, tamamen yeni, benzersiz ve beklenmedik bir gelişmedir. 170 yıl önceki demiryolu gibi, e-ticaret de yeni ve farklı bir patlama yaratmakta ekonomiyi, toplumu ve siyaseti değiştirmektedir” şeklinde ifade etmiştir (Gökgül, 2014).

Haziran 1995’de Java’nın piyasaya sürülmesi ve yine aynı yılın Ağustos ayında Netscape tarafından IPO’nun icat edilmesi internetin bir ticaret aracı olarak kullanılmasındaki önemli dönüm noktaları olarak görülmektedir. Böylelikle 1995 yılından beri internet kullanıcıları, interaktif reklamlardan sanal gerçeklik deneyimlerine kadar birçok yenilikçi uygulamanın gelişimine tanıklık etmektedirler (Gökgül, 2014). Tablo 4’de görüldüğü üzere e-ticaretin gelişimi aşama aşama gerçekleşerek günümüz ticaretinin yeni şekli olarak e-ticaret hayatımıza girmiştir.

Tablo 3: E-ticaretin 90’lı yıllarda gelişimi

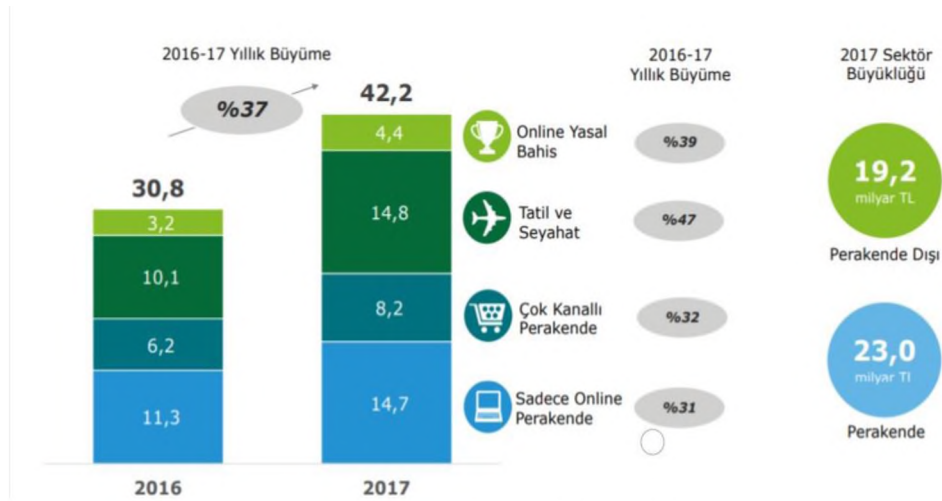
YIL	AÇIKLAMA
1989 - 1991	WWW Hizmeti ve Tarayıcısının oluşturulması ve ticari amaçla kullanılması
1994	Online Bankacılık, Pizza Hut firmasının online dükkanını açması, Netscape's SSL v2 sertifikası ile güvenli online alışverişin başlaması

1995	Online alışveriş sitesi Amazon'un kuruluşu
1996	Online alışveriş sitesi Ebay'ın kuruluşu

Kaynak: Consumers' Perception on Online Shopping, Dr.R.Shanthi, Dr. Desti Kannaiah, 2015.

E-ticaretin günümüzdeki en yaygın kullanım şekli internet üzerinden tüketicilerin mal veya hizmet alımını sağlayan online alışveriş yöntemidir. Sayıları her geçen gün daha da artan online alışveriş siteleri tüketicilerin alışveriş alışkanlıklarını büyük ölçüde etkilemiştir. Online alışveriş, perakendeciler ve müşteriler herhangi bir konumdayken müşterilere ticari ürünleri internetten satın alma imkânı vermektedir. Tüketici tarafından online alışveriş müşterinin zamanını ve parasını perakende mağazalara gitmek zorunda olmadıklarından ötürü kurtarmakta ve belki daha da önemlisi perakendeciler de bu sayede gerçek mağaza konumlarına yatırım yapmak zorunda kalmamaktadır. Böylelikle online alışveriş tedarikçi açısından büyük miktarda maliyeti kurtararak online alışveriş ürünlerini rekabetçi fiyattan sunmayla sonuçlanmaktadır. Özellikle tüketicilerin online alışverişini tercih etme sebepleri "Kolaylık (kullanışlılık), Zamandan Tasarruf, Web Sitesinin Tasarımı ve Güvenlik" olmak üzere 4 ana başlık altında toplanmaktadır. Kolaylık faktörü yukarıda da bahsedildiği üzere müşterilerin istedikleri ürünleri geleneksel alışverişe göre internet üzerinden daha kolay ve daha uygun fiyata bulmalarını ifade ederken fiziksel olarak ürünleri ararken harcanacak zamanı minimuma indirerek zamandan tasarruf faktörünü de ortaya koymaktadır. Üçüncü faktör olan web sitesinin tasarımı ise müşterileri özellikle kalite algısını yaratmak açısından oldukça etkili bir faktördür. Her ne kadar birçok internet kullanıcısı kredi kartı dolandırıcılığı sebebi ile online alışveriş sitelerini kullanmaktan kaçınsa da en son geliştirilen güvenli para transferi ve online alışveriş yöntemleri kullanıcıların online alışverişini etkileyen güvenlik faktörü olarak değerlendirilmektedir (Sultan ve Udin, 2011).

Şekil 6: Türkiye'de e-ticaret pazar büyüklüğü (milyar TL)



Kaynak: TÜBİSAD, (2017). Türkiye'de E-Ticaret, Deloitte, ETİD.

Nielsen araştırma şirketine göre dünya nüfusunun %74'ü internet erişimine sahiptir ve internet erişimi olanların %84'ü internetten alışveriş yapmaktadır. 2014 yılı

Türkiye İstatistik Kurumu (TÜİK) verilerine bakıldığında internet kullanan bireylerin internet üzerinden mal hizmet sipariş verme ve satın alma oranı 2013 yılında %24,1 iken 2014 yılında bu oran %30,8 olarak açıklanmıştır. E-ticaretin ve online alışverişin Türkiye’de hızla gelişerek geldiği noktayı görmek açısından Türkiye Bilişim Sanayicileri Derneği’nin (TÜBİSAD) 2017 yılında hazırladığı rapora bakmakta fayda vardır. 2013 – 2017 yılları arasında e-ticaret %32’lik bir büyüme kaydederken 2016-2017 yılları arasında %37’lik bir büyüme elde etmiştir (bakınız şekil 6).

2.2.4. E-Ticaret Uygulamaları

Önceki bölümde E-ticaretin sadece online bankacılık ve şirketler arasındaki ticari işlem ve faaliyetler ile sınırlı olmadığı Amazon ve Ebay gibi ünlü online alışveriş sitelerinin kurulması ile farklı bir boyut kazandığı üzerinde durulmuştur. Bu bölümde e-ticaretin en önemli araçlarından biri haline gelen online alışverişin en yaygın şekli olarak nitelendirebileceğimiz işletmeden müşteriye (B2C) olan tipinin Türkiye’deki başta olmak üzere dünya çapında en çok kullanılan uygulamaları değerlendirilmektedir.

Hepsiburada.com: 1998 yılında 100 bin lira sermaye ile kurulan Hepsiburada.com 20 yıl içerisinde büyüyerek Türkiye’nin online alışveriş alanındaki en büyük uygulaması olarak karşımıza çıkarken aynı zamanda Türkiye’nin en büyük perakende oyuncuları arasına girmiştir. 2017 yılı itibarıyla net 1 milyar TL’lik cirosu ile Hepsiburada.com Doğu Avrupa, Orta Doğu, Afrika (EEMEA) ve Rusya’yı kapsayan bölgede en büyük e-ticaret şirketi konumuna gelmiştir (Superbrands Türkiye, 2014).

Hepsiburada.com, bilgisayarlardan akıllı telefonlara ve tabletlere, kitaplardan oto aksesuarlarına, spor malzemelerinden mutfak malzemelerine ve bebek bezlerine kadar 27 farklı kategoride 500 binden fazla ürün çeşitliliğine sahip bir uygulamadır. Türkiye’de ilk olarak Hepsiburada.com platformunun sunduğu “tek tıkla alışveriş” hizmeti ile müşteriler, kredi kartı bilgilerini tekrar tekrar girmeden alışveriş yapma imkânına sahiptirler. “Bugün Teslimat” servisi ve “Kolay İade” gibi uygulamalar ise kullanıcıların hayatına hız katan müşteri memnuniyeti odaklı hizmetler olarak Hepsiburada.com’un ön plana çıkan özellikleri arasındadır. Akıllı telefonlarda kullanılmak üzere geliştirilen mobil uygulaması da bulunan Hepsiburada.com üye olmadan alışveriş” özelliğine de sahiptir. Bu sayede siteye üye olmayan kullanıcılar, çok hızlı bir şekilde istedikleri ürünü alıp siteden çıkabilmektedir. Hepsiburada.com’un mobil uygulamalarda satın alma deneyimini zenginleştiren yenilikleri ise devam etmektedir. Barkod tarama, ses ile arama, kişiye özel push gönderimi gibi özellikleri kullanıcılar fiziksel mağazalarda kullanarak fiyat karşılaştırma, ürün hakkında bilgi edinme gibi avantajlardan yararlanmaktadır (Superbrands Türkiye, 2014).

Türkiye’nin Amazonu olarak kabul edilen Hepsiburada.com Black Friday isimli kampanya çerçevesinde 24 Kasım 2017 yılında 2 milyon adet ürün satarak 257 milyon liralık ciro yaptığını açıklamıştır. Bu tarihte toplamda 36 kategoride yüzde

80'e varan indirimler uygulayan Hepsiburada.com, 81 ilden toplamda 523 bin sipariş almayı başararak 11 milyon ziyaretçi tarafından 20 milyon kez ziyaret edilmiştir. Hepsiburada.com'un mobil uygulaması ise gün içinde 604 bin defa indirilmiştir (Webrazzi, 2017).

N11: N11.com e-ticaret sektöründe faaliyet göstermek üzere, Doğu Grubu ile Güney Kore'nin en büyük gruplarından SK Group'un ortaklığında Doğu Planet tarafından 2013 yılında kurulmuş bir online alışveriş sitesidir. N11.com e-ticaret politikasını "Stratejik ortaklıklarla güçlü entegrasyona dayanan eko-sistemimizde, müşterilere Güven ve Kolaylık; mağazalara ise Destek ve Özen üzerine dayalı değer önerileri sunmak" olarak tanımlamaktadır (n11.com, 2018). Dört buçuk yılda 80 bini aşkın kayıtlı mağaza, 10,3 milyon üye, açıldığı günden bu yana satılan 55,7 milyon ürün ve 1,9 milyar toplam ziyaret sayısına ulaşan N11.com, yine kurulduğundan bu yana geçen dört buçuk yılda 2 milyar dolar ticaret hacmine ulaştı. N11.com e-ticaret platformunun devlete sağladığı KDV geliri 261 milyon doları bulmuştur (n11.com, 2017).

Hepsiburada.com gibi e-ticaret pazarının önemli online alışveriş siteleri ile benzer özellikler gösteren ve hizmetler veren N11.com farklı hizmet ve özellikleri ile rakiplerinden ayrılan bir online alışveriş platformudur. Bunların başında 2017 yılında "N11pro" adı ile hizmete sunduğu yeni alışveriş platformu gelmektedir. N11, N11pro ile toptan alım-satım yapabilen, şirketleri tek bir çatı altında toplayan geniş kapsamlı toptan e-ticaret platformu sunmaktadır. Bu platform ürünlere kolay erişim, zengin ödeme seçenekleri, ekonomik çözümler ve nakliye seçenekleri gibi önemli avantajlar sağlamaktadır. Aynı anda hem toptan alım hem de toptan satış yapmaya da imkan sunan N11pro, çoklu kredi kartı, taksit, vadeli ödeme, EFT ve havale gibi birçok farklı ödeme seçeneğine sahip bir platform olarak karşımıza çıkmaktadır (Webrazzi, 2017).

Prudsys RDE (Realtime Decisioning Engine) gibi gelişmiş bilişim sistemleri (Prudsys, 2016) kullanan N11.com uygulaması son yıllarda elde ettiği satış rakamları ile Türkiye'nin en büyük online pazarlarından biri olmayı başarmıştır. Özellikle Çin'de "Yalnızlar Günü" olarak kutlanan ve e-ticaret sitelerinde büyük indirim kampanyaları yapılan 11 Kasım tarihinde büyük bir kampanya gerçekleştiren N11.com, "11.11 Yılın En Uğurlu Kampanyası" adı ile başlatılan ve 24 saat süren kampanyada 140 milyon TL'lik satış gerçekleştirmiştir (Webrazzi, 2017).

Amazon: E-ticaretin online alışveriş ayağının en büyük öncüsü olarak kabul edilen Amazon.com Jeff Bezos tarafından 5 Temmuz 1994 yılında ABD'de kurulmuş dünyanın en büyük alışveriş sitesidir. Online alışveriş alanında ilk başta sadece kitap satışı ile başlayan Amazon süreç içerisinde hızlı bir şekilde bilgisayar oyunlarından elektronik eşyalara oyuncaktan mobilyaya kadar çok farklı türden ürünün satıldığı bir platform haline gelmiştir. Ayrıca Amazon elektronik kitap pazarının lideri konumunda olan Kindle e-kitap okuyucularını üretip satışını yapmaktadır. Bunun dışında bulut bilişim sektöründe de faaliyet gösteren Amazon Web Services (AWS) adı altında işlem, depolama, veri tabanları, analiz, ağ, mobil, geliştirici

araçları, yönetim araçları, nesnelerin interneti (IoT), güvenlik ve kurumsal uygulamalar dahil olmak üzere küresel ölçekte geniş bir hizmet sağlayıcısı konumundadır. Bu hizmetler, kurumların daha hızlı hareket etmesine, bilişim teknolojileri (BT) giderlerini azaltmasına ve ölçeklendirmesine imkan sağlamaktadır (Amazon, 2018).

En büyük rakiplerinden eBay 107 milyon kişi ve Wal-Mart 84 milyon kişi tarafından ziyaret edilirken ABD'nin en popüler alışveriş sitesi olan Amazon.com aylık 183 milyon kişi tarafından ziyaret edilmektedir (Koo & Park 2017). 2017 yılı rakamlarına göre Amazon'un elde ettiği gelir 178 milyar dolar civarındadır (Statista, 2018). 151 milyar dolarlık marka değeri ile dünyada birinci sırada yer alan Amazon'un (Bloomberg, 2018) Amerika Birleşik Devletleri, İngiltere ve İrlanda, Fransa, Kanada, Almanya, İtalya, İspanya, Hollanda, Avustralya, Brezilya, Japonya, Çin, Hindistan ve Meksika için ayrı alışveriş siteleri vardır. Almanya sitesinde Türkçe dil seçeneği sunulmaktadır. Amazon'un Türkiye sitesi bulunmamakla birlikte çeşitli Amazon siteleri uluslararası gönderim kapsamında Türkiye'ye gönderim yapmaktadır (İnternet Gazetesi, 2018).

Amazon tüketici dostu olabilmek için düşük fiyat, geniş ürün seçenekleri, web sitesi kullanım kolaylığı ve tek bir sanal depoda tüm müşterilerinin ihtiyaçlarını karşılayacak elverişliliği sağlayan bir web sitesi tasarlamıştır. Amazon kendisi dışında Amazon'un sunduğu fırsatlardan faydalanan çok çeşitli satıcıların ürünlerini de bünyesinde barındırmaktadır. Bu durum satıcılara kendi imkanları ile ulaşamayacakları sayıda müşteriye ulaşma imkanı vermektedir. Ayrıca bağımsız yayıncılar ve yazarlar kitaplarını Kindle'in yayın hizmetini kullanarak Kindle Store'da yayınlamaları durumunda %70 telif ücreti hakkı elde etmektedir (Lang ve diğerleri, 2012). Bu durumda yazarlar için Amazon.com'u cazip hake getirmektedir.

Jeff Bezos milyar dolarlık şirketini müşterilerine özel hizmetler sunan bir konsept çerçevesinde inşa etmiştir. Bu Amazon forumlarda yapılan inanılmaz sayıdaki olumlu geri bildirimlerle kanıtlanmış bir durumdur. Amazon Prime, Amazon Mom ve Lending Library gibi müşteri sadakati girişimleri dahil olmak üzere birçok faktör müşterilerin olumlu deneyimlemelerine katkıda bulunmaktadır. Bunun yanında Amazon müşterilerini kaçırarak hataları en aza indirgeyecek ve "self servis müşteri" hizmetlerini geliştirecek büyük yatırımlar yapmaktadır (Lang ve diğerleri, Harrison 2012).

Aliexpress: Aliexpress Amazon.com'un en büyük Çinli rakibi olan Jack Ma tarafından kurulan işletmeden işletmeye satış yapan Alibaba alışveriş sitesinin işletmeden müşteriye satış yapan uygulamasıdır. Aliexpress Türkiye'de çok rağbet gören yabancı alışveriş sitelerinden birisidir. Bu nedenle araştırmada Aliexpress'e de değinilmektedir. 2010 yılında kurulmasına rağmen güvenilir tüccarların olması ve ürünlerin tüm dünyada satışa çıkarılıyor olması alışveriş dünyasında bu siteyi kısa sürede cazip hale getirmiştir. Satışı yapılan ürünlerin ucuz olması ve ülkemize ücretsiz kargolanması bakımından da sıklıkla tercih edilen bir alışveriş sitesidir. Böylelikle Aliexpress dünyadaki saygın alışveriş sitelerinden biri olmayı başarmıştır.

3.5 milyon şirketi site içerisinde barındıran 200'e aşkın ülkede satış yapan Aliexpress Müşteri koruması ön planda olan sitelerden biri olarak değerlendirilmektedir (Aliexpressalisveris.com, 2017).

2.3. Sosyal Medya ve E-Ticarete Gizlilik ve Güvenlik

Online bilgi ve verileri oluşturan en önemli araçların başında milyarlarca kişi tarafından kullanılan sosyal medya ve online alışveriş siteleri gelmektedir. Çünkü milyarlarca kişi farklı amaçlarla sosyal ve ekonomik bir etkileşim aracı olarak sosyal medya ve online alışveriş sitelerini kullanmaktadır. Sosyal ağlar ya da online alışveriş siteleri üzerinden etkileşimde bulunabilmek için ise hesap açmak ya da üyelik oluşturmak gerekmektedir. Bu da beraberinde hizmet sağlayıcılar ve diğer kullanıcılar ile kişisel bilgilerimizi önemli derecede paylaşmamızı zorunlu kılmaktadır. Bu noktada kişisel verilerimizin ne derece korunduğu sorusu akıllara gelmektedir. Zira yakın zamanda Facebook skandalı ile birlikte milyonlarca insanın kişisel verilerinin izinsiz olarak paylaşıldığı ve bunların farklı amaçlar için kullanıldığının ortaya çıkması özellikle sosyal medyaya karşı insanlarda gizlilik ve güvenlik endişelerini artırmıştır. Ayrıca sosyal medya ya da online alışveriş kullanıcıları bilgisayar korsanları ya da dolandırıcılar tarafından da kolaylıkla hedef haline gelebilmektedir. PEW Araştırma Merkezinin 2013 yılında yaptığı bir araştırmada kayda değer sayıda internet kullanıcısının kişisel bilgilerinin çalınması konusunda sorunlar yaşadığı belirtilmiştir. Bu bağlamda tablo 5'de belirtildiği üzere kullanıcıların e-mail ya da sosyal medya hesaplarının ele geçirildiği, sosyal güvenlik numarası ya da kredi kartı bilgilerinin çalındığı, online olarak tacize uğradığı, itibarını kaybettiği, dolandırıcılık kurbanı olduğu durumlara dikkat çekilmiştir (Rainie ve diğerleri, 2013).

Tablo 4: Online Gizlilik ve Güvenlik Konularında Yaşanan Durumlar

İnternet kullanıcılarının %21'nin e-mail ya da sosyal medya hesapları başkası tarafından ele geçirilmiştir.	İnternet kullanıcılarının %13'ü kendi aralarında, aile üyeleri ile ya da bir arkadaşı ile yaptıkları bir paylaşım yüzünden sorun yaşamıştır.
İnternet kullanıcılarının %12'si online olarak gizlice takip ya da taciz edilmiştir.	İnternet kullanıcılarının %11'i sosyal sigorta, kredi kartı numarası ya da banka hesabı gibi önemli kişisel bilgileri çalınmıştır.
İnternet kullanıcılarının %6'sı online dolandırıcılık kurbanı olmuş ve paralarını kaybetmiştir.	İnternet kullanıcılarının %6'sının itibarı online gerçekleşen bir durum yüzünden zarar görmüştür.

İnternet kullanıcılarının %4'ü online gerçekleşen bir durum yüzünden fiziksel şiddete uğramıştır.	İnternet kullanıcılarının %1'i online paylaşımları ya da bir başkasının paylaşımı yüzünden bir iş ya da eğitim fırsatını kaybetmiştir.
---	--

Kaynak: Rainie (2013) Pew Research Center “Anonymity, Privacy, and Security Online”

Birçok internet kullanıcısı kendilerine ait resim ve videoları, e-mail adresleri, doğum tarihleri, telefon numaraları, ev adresleri ve ait oldukları sosyal gruplar gibi anahtar niteliğindeki kişisel bilgilerinin online olarak ulaşılabilir olduğunu bilmektedir. Sayıları artmakta olan internet kullanıcıları ayrıca kendileri hakkındaki online kişisel bilgilerin miktarı konusunda endişe duyduklarını ifade etmektedir. 2009 yılı ile kıyaslandığında endişe duyanların sayısı %33 oranında artmış durumdadır. Bu endişeler sonucunda kullanıcılar kişisel bilgileri üzerinde kontrol sağlamak istemektedir. Birçok durumda sadece kendilerinin ya da yetkili kişilerin kişisel bilgi ve verilere ulaşabilmesinin çok önemli olduğunu vurgulayan kullanıcılar e-maillerinin içeriği, e-mail gönderdikleri kişiler, indirdikleri dosyaların içeriği, online oldukları yerler ve ne zaman online oldukları gibi bilgilerin çok iyi korunması gerektiğini düşünmektedir (Rainie ve diğerleri, 2013). Bu durum da sosyal ve ekonomik açılardan veri gizliliği ve güvenliği konularının önemle ele alınmasını gerektirmektedir.

2.3.1. Sosyal Medya’da Gizlilik ve Güvenlik Sorunları

Kizza (2014) sosyal medya üzerinden gizliliğe yönelik sorunların kullanıcı bilgilerinin ele geçirilmesi, kullanıcı bilgilerinin amaç dışı kullanılması, bilgiye izinsiz ulaşılması (güvenliği ihlal etme) ve izinsiz kullanılması olmak üzere farklı şekillerde ortaya çıktığını ifade etmektedir. Bilgiye izinsiz ulaşılması sosyal ağlara üye olan kişilere ait bilgilerin zorla elde edilmesini kapsamaktadır. Kullanıcı bilgisinin amacı dışında kullanılması ya da güvenilen sosyal ağlardaki bilgilerin kullanılması ise kullanıcının isteği dışında onaylamadığı durumları belirtmektedir. Bu durumlara üçüncü kişilere kullanıcıların kişisel bilgisinin satılması örnek olarak gösterilmektedir. Bununla birlikte kullanıcıların faaliyetleri ve bulundukları yerleri içeren aşırı bilgi paylaşımları gizliliğe yönelik sorunları fazlasıyla artırmaktadır. Özellikle kullanıcılarının konum bilgisini paylaşan ya da onların online olduğunu gösteren son dönem sosyal medya uygulamaları konum bilgisi ve diğer verilerin sızmasına sebebiyet verebilmektedir. Bu uygulamalar bir kullanıcının diğer bir kullanıcı ile bağlantı kurduğunu dahi göstermektedir (Kizza, 2014).

Bir başka araştırmada ise sosyal ağlara yönelik sorunlar; gizlilik tehditleri, klasik ağ ve bilgi güvenliği tehditleri, kullanıcı kimlik bilgisi ile ilgili tehditler ve sosyal tehditler olarak sınıflandırılmıştır (Hogben, 2007; Huber ve diğerleri, 2010). Gizliliğe yönelik tehditler dijital dosyaların kümelenmesi (toplanması), ağ yapısı ve faaliyetlerinden ikincil verilerin toplanması, yüz tanıma, içerik temelli görsellerin ele geçirilmesi, sahibi olmayan kullanıcı tarafından etiketlenen görsel üst veriden bağlantı analizi yapılması ve kullanıcı hesabının tümüyle kaldırılmasındaki güçlük

olarak sıralamak mümkündür. Aynı zamanda gizliliğe yönelik sorunlar gizli dinleme, verileri değiştirme, başka bir ağa atak yapan kullanıcının kendisini atak yaptığı sistemin yetkili bir üyesi olarak göstermesi (masquerading), kimlik ifşası, yanlış güvenlik politikası, kötü amaçlı-casus yazılımlar ve uygunsuz imtiyaz elde etme şeklinde de detaylandırılmaktadır (Tomlinson ve diğerleri, 2010).

Sosyal ağlardaki spam içerikli paylaşımlar, virüsler, çapraz site komut çalıştırma gibi güvenlik sorunlarının büyük bir çoğunluğu üçüncü taraf uygulamalarının zayıflığından kaynaklanmaktadır. Sosyal medya uygulamalarının bilgi toplayıcılarının çoklu sosyal medya uygulamalarına tek bir yetki üzerinden erişim izni vermesinden dolayı online güvenlik sorunları daha da büyümektedir. Bu çerçevede Koobface gibi geliştirilen virüslerin sosyal medya uygulamalarını hedef aldığı görülmüştür (Tanner ve diğerleri, 2010; Thomas ve Nicol, 2010). Kullanıcıların kimlik bilgileri ile ilgili sorunlar arasında kimlik hırsızlığı, sosyal ağlara gizlice sızılması, çalınan kimlik bilgileri ile kişi profilinin itibarsızlaştırılması ve haysiyetinin karalanması gösterilmektedir. Ayrıca sosyal ağlara yönelik sorunlara online taciz, fiziksel şiddet ve kurumsal casusluk gibi faaliyetleri de eklemek mümkündür (De Paula, 2010). Sosyal medyaya yönelik olası gizlilik ve güvenlik sorunları tablo 6’da gösterildiği üzere listelenmiştir.

Tablo 5: Sosyal Medyada Online Gizlilik ve Güvenlik Sorunları

Sorun Türü	Sorunlar
Gizlilik sorunları	Dijital dosyaların kümelenmesi (toplanması)
	İkincil verilerin toplanması
	Yüz tanıma,
	İçerik temelli görsellerin ele geçirilmesi
	Görsel üst veriden bağlantı analizleri yapılması
	Kullanıcı hesabının tümüyle kaldırılması güçlüğü
Ağ ve bilgi güvenliği sorunları	İstenmeyen e-postalar
	Çapraz site komut çalıştırma
	İnternet virüsleri
	İnternet solucanları
	Tek oturum açma
Kimlik sorunları	Kimlik hırsızlığı - e-dolandırıcılık

	Sosyal ağlara gizlice sızma
	Kişi profilinin itibarsızlaştırılması
	Kişi haysiyetinin karalanması
Sosyal sorunlar	Online taciz
	Fiziksel şiddet
İşletme sorunları	Verimlilik (performans) kaybı
	Kurumsal casusluk
	Çalışanların rakiplere kaptırılması
	Siber saldırılar

Kaynak: Hogben, (2007); Huber, ve diğerleri, (2010); Tomlinson, ve diğerleri, (2010).

İşletmeler açısından da sosyal medya uygulamalarının çalışanlar tarafından kullanımının olumsuz etkileri olabileceği ifade edilmektedir. İşletmelerin bu konudaki endişeleri ise verimlilik kaybı, özel bilgilerin sızdırılması, nitelikli çalışanların rakip şirketlere kaptırılması ve siber saldırılar olarak sıralanabilir. Bu bağlamda işletmelerin kurum imajları can sıkıcı ifşaatlar üzerinden yapılan olumsuz reklamlar ya da aktivistler tarafından gerçekleştirilen saldırılar sonucu zarar görebilmektedir. Özellikle bilgisayar korsanları sosyal ağlardan derledikleri işletme ve ilişki bilgilerini işletmelere yönelik e-dolandırıcılık ya da kimlik hırsızlığı saldırıları için kullanabilmektedir (Langheinrich ve Karjoth, 2010).

Diğer taraftan kendilerinden beklenilen aksine sosyal medya kullanıcılarının tam olarak kendilerine ait hesapları ve bunlarla alakalı güvenlik ve gizlilik politikalarını yönetebilecek düzeyde olmadıklarını yapılan araştırmalar sonucu görmekteyiz (Ahn ve diğerleri, 2011). Kullanıcıların gizlilik ayarlarını tam olarak anlayamadığı durumlar olduğu gibi internette paylaşılan beklenmedik sonuçları olan bilgiler karşısında da kullanıcıların şaşırabildiği durumlar ortaya çıkmaktadır. Bazen kullanıcılar varsayılan ayarlar üzerinden kolaylıkla kişisel verilerine geniş şekilde erişilebileceğini umursamazken bazen de gizlilik ayarları kullanıcılara fazlasıyla karmaşık gelebilmektedir (Strater ve Lipford, 2008). Sosyal medya kullanıcı profillerine yönelik yapılan bir araştırma kullanıcıların büyük bir çoğunluğunun sosyal ağlar tarafından kendilerine sunulan varsayılan gizlilik ayarlarını olduğu gibi kabul ettiğini, böylelikle profillerinin herkesçe sorgulanabilir ve herkese görünür olduğuna dikkat çekmiştir (Gross ve Acquisti, 2005). Bu tür kullanıcılar gizlilik konusunda belli bir farkındalığa sahip olsalar da gündelik kullanımlarında çoğu zaman kullanıcı gizliliklerini ihmal etmektedir. Eğer arkadaşları kişiye özel kullanıcı profili oluşturmuşlarsa ve kendileri de kişisel verilerinin gizliliği ve erişimi konusunda daha fazla farkındalığa sahipse aktif sosyal medya kullanıcılarının da

kişiyi özel kullanıcı profili edinme eğiliminde olduğu görülmüştür (Lewis ve diğerleri, 2008). Sosyal medya kullanıcıları çok büyük boyutlarda kendilerini tanımlayan kişisel bilgiyi sosyal ağlarda paylaşmakta ve bu bilgileri arkadaşları dışında yabancılarla da paylaşmaktan çekinmemektedir (Stutzman, 2006). Öyle ki sosyal medya kullanıcıları sosyal ağlardaki paylaşımları çok kolay ulaşılabilir olduğu halde özel hayatlarının ifşa olduğu durumlar karşısında şaşkınlık yaşayabilmekte ve kişisel verileri üzerindeki kontrolü kaybettiklerini düşünebilmektedir (Hoadley ve diğerleri, 2010).

Online gizliliğe yönelik bir başka sorun olarak karşımıza normal arkadaşlarımız ile olan ilişkilerimizde sıkça gerek duyduğumuz güven duygusu çıkmaktadır. Zira sosyal medya kullanıcıları ile sosyal ağlar arasında güven temelli bir ilişki olduğunu ifade etmek yanlış olmayacaktır. Bu ilişkide kullanıcılar sosyal medya uygulamalarının onların kişisel verilerini koruyacakları beklentisinden hareketle bir güven davranışı sergilemektedirler. Ancak son yaşanan Facebook skandalında olduğu gibi sosyal medya hizmeti sağlayıcısının üçüncü bir tarafa verdiği erişim izinleri sayesinde kullanıcıların kişisel verileri izinleri dışında ele geçirilebilmekte ve farklı amaçla kullanabilmektedir. Bu da beraberinde güven sorununu getirmektedir.

Bu alandaki çalışmalar henüz oldukça yeni olmakla birlikte bu zamana kadar sosyal medyada gizlilik ve güvenlik konularında yine de birçok çalışma yapıldığı görülmektedir. Özellikle son yıllara ait çalışmaların başında Sabine Trepte ve Leonard Reinecke tarafından derlenen Privacy Online adlı kitap gelmektedir. 30 üzerinde araştırmacının katkı sağladığı çalışma sosyal ağlarda online gizlilik konusuna çok farklı bakış açılarından yaklaşmakta olup gizlilik yönetimi uygulamalarından mobil gizliliğe ve kişisel bilgilerin sosyal medyada paylaşılmasına kadar çok sayıda konu farklı isimler tarafından ele alınmıştır (Trepte ve Reinecke, 2011). Özellikle sosyal medya kullanıcılarının kişisel bilgilerini ifşa etmelerinin öncülleri üzerinde bir başka çalışmada ise bilginin ifşası, kişisel bilgiler üzerinde kontrol, kullanıcıların farkındalıkları ve sosyal bağlamda güvenlik konuları arasındaki ilişki incelenmektedir (Benson ve diğerleri, 2015).

Literatürde yapılan çalışmaların büyük bir çoğunluğunda online gizlilik ve güvenlik konuları birlikte ele alınmakta zaman zaman gizlilik ve güvenlik kavramları birbirleri yerine kullanılmaktadır. Bu iki kavram arasındaki farkın belirsizliğinden hareketle “Can Privacy and Security Be Friends?” adlı çalışmada araştırmacılar sosyal ağlarda sergilenen gizlilik ve güvenlik davranışlarını kültürel özellikler açısından ele almış ve davranışlara etki eden faktörleri sınıflandırmıştır (Dincelli ve Goel, 2017). İlgili alanda son yıllarda yapılmış kapsamlı ve çok boyutlu çalışmalara Jaime Ortiz, Wen-Hai Chih ve Faa-Shyan Tsai (2018) tarafından gerçekleştirilen ve bilgi güvenliği farkındalığı, bilgi gizliliği endişesi, müşteri ötekileştirilmesi (soğuma-uzak durma), gizlilik riski inancı, gizli dinleme, kendini gizleme arasındaki ilişkiyi inceleyen araştırma örnek olarak karşımıza çıkmaktadır. Bu çalışmada internet kullanımında güvenlik farkındalığı yüksek olan sosyal medya kullanıcılarının kişisel bilgilerinin gizliliği konusunda daha fazla endişeye sahip oldukları belirtilmektedir. Birçok sosyal medya kullanıcısı kişisel özel bilgileri ve gizliliklerinin ihlali sonucu ortaya

çıkacak kayıpları konusunda endişe duymaktadır. Bu nedenle gizliliklerinin korunması bu kullanıcılar için büyük bir önem arz etmektedir. Elde edilen bulgular sosyal medya kullanıcılarının güvenlik konusundaki farkındalık seviyelerinin gizlilik riski anlayışı üzerinde önemli derecede olumlu bir etkiye sahip olduğunu ortaya koymaktadır. Kullanıcılar eğer yüksek seviyede güvenlik farkındalığına sahipse tehdit değerlendirmesi üzerinden kendilerini korumakta ve gizliliğe yönelik güçlü bir risk anlayışı oluşturmaktadır (Ortiz ve diğerleri, 2018).

Bir başka araştırmada ise online gizlilik alanındaki çalışmaların ABD başta olmak üzere gelişmiş ülkelerde yapılmış olmasından hareketle ise online gizlilik endişesi farklı bir coğrafya olan Batı Balkanlar çerçevesinde değerlendirilmiştir. Bu çalışmada online gizlilik, izleme ve kişisel verilerin korunması konularında gelişmiş ülkelerden farklı olarak dört Balkan ülkesi incelenmiş ve elde bulgular açısından farklılıklar olduğu tespit edilmiştir. Bununla beraber araştırmada yüksek eğitim seviyesine sahip kullanıcıların izleme/izlenme ve verilerin korunması konularında farkındalık seviyelerinin artmakta olduğu belirtilmiştir. Diğer çalışmalarda da işsiz ya da nitelsiz çalışanların bilgi iletişim teknolojileri ile ve yeni gelişen teknolojiler ile çok fazla alakadar olmaması izlenme ya da verilerin korunması hususunda daha az endişe sergilemelerinin sebepleri olarak gösterilmektedir. (Budak ve diğerleri, 2014).

Online gizlilik ve güvenlik alanında yapılan çalışmalar sadece akademik araştırmalarla sınırlı olmayıp birçok akademik araştırmaya katkı sağlayan önemli kuruluşlarca gerçekleştirilen anket ve raporlama çalışmaları mevcuttur. Bunlardan birisi bir önceki bölümde değindiğimiz PEW Araştırma Merkezi tarafından Amerikalı internet kullanıcılarına yönelik yapılan çalışmadır. Bu çalışmada online yetişkin kullanıcılarının % 21'nin sosyal medya ya da e-mail hesaplarının ele geçirildiği %11'nin ise sosyal güvenlik numarası, banka hesabı ya da kredi kartı bilgilerinin çalındığı tespit edilmiştir. Ayrıca araştırma sonuçlarına göre yaşları 18 – 29 arasında değişen gençlerin büyük bir çoğunluğunun sosyal medya hesapları ele geçirilirken bu gençler online taciz ya da zorlamalara, itibar zedelenmesi ya da fiziksel tehditlerle karşı karşıya kalmaktadır (Rainie ve diğerleri, 2013).

Yine PEW Araştırma Merkezi tarafından Gizli NSA belgelerini medyaya ifşa eden Edward Snowden sonrası dönemde insanların gizlilik ve güvenlik algılarını ölçmek için yapılan bir başka araştırmada insanların kablolu telefon ile sosyal medya kullanımı karşılaştırılmıştır. Araştırma raporunda insanların kişisel bilgilerini paylaşmak konusunda %31'inin kablolu telefon kullanırken kendini güvende hissetmediği ifade edilirken sosyal medya kullananların %81'inin kendini güvende hissetmediği belirtilmiştir. Diğer taraftan ücretsiz bir online hizmeti almak için kişisel bilgilerini paylaşma konusunda sosyal medya kullanıcılarının %60 gibi bir rakamla daha istekli ve rahat davrandığını, sosyal medya kullanıcısı olmayanların %52'sinin ise bu konuda tedirgin davrandığı ortaya konmuştur (Madden, 2014).

2.3.2. E-Ticarete Gizlilik ve Güvenlik Sorunları

Hızla gelişen internet ve bilişim teknolojileri online olarak alışveriş yapmayı mümkün kıldığı gibi geleneksel alışveriş anlayışını da büyük ölçüde değiştirmeye başlamıştır. Liu, Burns ve Hou online alışverişin tüketiciler tarafından herhangi bir satış elemanı baskısının olmadığı rahat ve eğlenceli bir tecrübe aracı olarak görüldüğünü ifade etmektedir (Liu ve diğerleri, 2013). Diğer taraftan e-ticaretin en önemli aracı olan bu online alışveriş siteleri kullanıcıların kişisel tercihleri, alışveriş alışkanlıkları, yaptıkları aramalar ve beğenileri gibi kullanıcılara ait çok büyük boyutta kişisel bilgi ve veriyi özellikle büyük veri uygulamaları aracılığıyla toplayabilmektedir. Artık gelişen teknoloji sayesinde sadece veriyi toplamak değil aynı zamanda bu veriyi işlemek de oldukça kolay hale gelmiştir (Gupta ve Dubey, 2016). Tabiki bu durum da sosyo-ekonomik anlamda gizlilik, güvenlik, güven, yasalar ve benzeri hususlarda birçok risk ve sorunu beraberinde getirmektedir. Bu bağlamda e-ticaretin özellikle en önemli sorunları olarak gizlilik ve güvenlik konuları karşımıza çıkmaktadır. Zira Culnan ve diğerlerinin yapmış olduğu çalışmada gizlilik endişelerinin insanların online olmaktan kaçınmaları ve online ortamlarda yanlış bilgi vermelerinin en önemli sebebinin kullanıcıların gizlilik endişeleri olduğu belirtilmiştir. Aslında nispeten bazı kullanıcılar kişisel bilgilerin nasıl ortaya çıktığı, kullanıldığı ya da işletmelere satıldığı hususunda kişisel bilgileri üzerinde kontrol sahibi olduklarına inandıkları ifade edilmektedir. Günümüz işletmelerinin uygulamaları, tüketicilerin korkuları ve medya baskısı birleşerek gizliliği e-ticaret için güçlü bir problem haline getirmiştir. Bazıları gizliliği temel bir hak olarak görürken bazıları satılabilir bir eşya olarak görmektedir (Gupta & Dubey, 2016).

Gizlilik ve güvenlik konularında yapılan çalışmalar tüketicilerin internette alışveriş yapmak konusunda endişelerinin olduğunu ve kullanıcıların online alışverişe yönelik algıladıkları risk sebebiyle ürün almak konusunda da tereddütlü davrandıklarını ortaya koymaktadır. Bazı bireyler algıladıkları risk sebebiyle online alışverişini tercih etmedikleri gibi bazı bireyler de sağladığı faydalar yönünden online alışverişini benimsemiş durumdadırlar (Forsythe ve diğerleri, 2006; Wani ve Malik, 2013). Bu çerçevede Liu ve arkadaşlarının yapmış olduğu çalışma literatüre katkı sağlayan çalışmalar arasındadır. Bu çalışmada tüketicilerin online alışveriş yapmama kararlarının sebepleri şöyle sıralanmaktadır: “a) ürüne dokunamamak ya da hissedememek, b) güven eksikliği, c) kredi kartı güvenliği, d) bilgi gizliliği ve e) ürünü geri iade etme güçlüğü (Liu ve diğerleri, 2013). Dolayısıyla tüketicilerin online alışverişinin devamını sağlamak amacıyla online satıcılar tüketicilerin algıladıkları riski azaltacak önlemler almalıdır. Özellikle online alışveriş alanında faaliyet gösteren işletmeler bu anlamda tüketicilerin online olarak ürün almalarını etkileyecek onların endişelerini azaltacak girişimlerde bulunmayı hedef haline getirmeleri gerekmektedir. McCole ve diğerlerinin (2010) yaptığı bir çalışma ise müşteri korkuları nedeniyle henüz internetin e-ticaretin gerçek potansiyelini ortaya koyamadığını ifade etmektedir. Federal Ticaret Komisyonu (1998) müşterilerin risk algılarını müşterilerin güvenlerini artırmak hususunda online ticaretin gelecekteki gelişiminin önündeki

başlıca engel olarak tanımlamaktadır. Gizlilik ve güvenlik ihlalleri müşteri güvensizliği ve yasal zorunluluk sözleşmeleri sebebiyle online perakende mağazacılığını engellemektedir (FTC, 2000; Petty, 2000). Diğer taraftan e-ticaret gelişen bilgi teknolojileri ile birlikte her geçen gün daha da büyümekte ancak gelişen bilgi teknolojileri gizlilik ve güvenlik endişelerini ortadan kaldırmamaktadır. Bu nedenle online alışverişin ilerlemesi için özellikle online pazarlamacıların bilgi güvenliğini en etkin şekilde sağlaması gerekmektedir (Maleki ve Pasha, 2012).

Boritz ve No (2011) çalışmalarında gizliliği bireylerin kişisel bilgilerini ve bu bilgileri şirketlerin nasıl kullandıklarını kontrol etme hakkı olarak tanımlamaktadır. Müşteriler bu noktada kişisel bilgilerinin şirketler tarafından nasıl kullanıldığı konusunda endişe duymakta ve bu durum da onların e-ticarete olan güven seviyesini düşürmektedir (Boritz ve No, 2011). E-ticaret işlemleri satın almalar için işletmelerin müşterilerinin kişisel bilgilerini almalarını gerektirmektedir. Bu kişisel bilgiler ise şirketlerin iç ve dış hedeflerini gerçekleştirmelerini sağlamaktadır. Sonuç olarak şirketler müşteri bilgilerinin korunmasına yönelik gizlilik ve güvenlik uygulamalarını gerçekleştirmek konusunda bir baskı ile karşı karşıya kalmaktadır. Bu bağlamda Miyazaki ve Fernandez'e ait çalışma (2001) internet kullanıcılarının tecrübeleri, risk algıları ve online alışveriş oranları arasındaki ilişkiyi inceleyen çalışmalar arasındadır. İlgili çalışma online alışverişin müşteriler tarafından benimsenmesinde risk algılarının önemli bir rol oynadığını ortaya koymaktadır (Miyazaki ve Fernandez, 2001).

Kayıt ve ürün siparişi verme gibi e-ticaret işlemlerinde müşteriler bazı bilgilerini satıcılara sağlamaktadır fakat satıcılar bu bilgiler olmadan da veri ve bilgi elde imkanına farklı yollarla ulaşabilmektedir. İnternet protokolleri ya da IP adresleri şirketlere müşterileri web sitelerine erişim sağladıklarında onların hangi siteleri ya da ürünleri araştırdığı bilgilerini sağlamaktadır (Harper, 2010). Özellikle radyo frekansı ile tanımlama (RFID) ve global konumlama (GPS) sistemleri şirketlere fiziksel konum bilgilerini ve ürünlerin ve kişilerin hareketlerini takip etme (izleme) olanağı vermektedir (Trocchia ve Ainscough, 2012). Diğer bilgi teknolojileri uygulamaları ile birlikte RFID ve GPS gibi izleme yöntemleri tüketicilerin kişisel ilgi alanlarını belirlemede yardımcı olmaktadır. Bununla birlikte bu tür bilgi teknolojilerini kullanan online pazarlamacılar izlenme önlemleri ve verilerine nasıl ulaşıldığı ya da verilerinin nasıl kullanıldığı konusunda her zaman tüketicileri bilgilendirmemektedir. Tüketicilerin izinleri olmadan onlara ait bilgilere ulaşılmasında amaç dışı kullanım (kötüye kullanma) durumu ortaya çıkmakta, şirketler ellerindeki bilgiyi başka şirketlere satabilmekte ya da özel bilgiler farklı mecralara sızdırılmaktadır. Bu durumda kişiler şiddete maruz kaldıklarını hissedebilmekte ve kişisel verilerinin ileride kendilerine karşı kullanılabileceği ya da gelecekte e-ticaret fırsatlarından uzak kalabilecekleri konusunda endişeye kapılmaktadır.

E-ticarete gizlilik ve güvenlik sorunlarına ilişkin bir başka konu tüketicilerin online alışveriş sitelerinin gizlilik ve güvenlik uygulamaları hakkındaki farkındalık seviyeleridir. Şirketlerin sunduğu gizlilik ve güvenlik önlemlerini içeren ağ güvenlik protokolleri ya da uygulamalarını kullanmayan tüketiciler e-ticaret işlemleri

esnasında gizlilik ve güvenliklerine yönelik sorunlar yaşayabilmektedir. Bu noktada önemli olan işletmelerin ilgili protokol ya da uygulamalar konusunda tüketiciyi doğru şekilde bilgilendirmesi ve yönlendirmesidir. Yeterli ağ güvenliği sağlamayan ya da bu konuda tüketicileri doğru şekilde yönlendirmeyen online alışveriş sitelerine yönelik olarak tüketicilerin endişe seviyeleri artmakta bundan da online alışveriş sektörünün büyümesi olumsuz etkilenmektedir. Bu durum online pazarlamacıları daha fazla müşteri çekmek ya da mevcut müşterilerini korumak açısından gerekli ağ güvenliğini sağlamak ve yönlendirmeleri yapmak konusunda sorumlu kılmaktadır (Pi ve diğerleri, 2012). Mandic (2009) güvenliği bir şirketin tüketici bilgisini koruyabilme ve online dolandırıcılığı önleyebilme kabiliyeti olarak tanımlamaktadır. Güvenlik tüketici bilgisinin korunması yönetsel ve verilere sınırlı erişimi içeren yönetsel ve teknik önlemleri içermektedir. Yönetsel önlemler verinin kanun dışı amaçlar için kullanımını önlemek amacıyla uygulanan veri erişimi sınırlamalarını kapsamaktadır. Teknik önlemler ise tüketicilerin bilgilerini yetkisi olmayan taraflara karşı korumak amacıyla uygulanan veri şifreleme, kullanıcı parolası zorunluluğu ve verinin güvenli ağlarda, sunucularda ya da bilgisayarlarda saklanması ve depolanması gibi uygulamalardır (Shalhoub, 2006).

Gupta ve Dubey'in çalışmasında (2016) e-ticaret güvenliği, e-ticaret hesaplarının yetkisiz erişimlerden, izinsiz kullanımlardan, tahrip edilmesinden ya da değiştirilmesinden korunması olarak ifade edilmektedir. Tüketiciler finansal bilgilerinin kaybolmasından, e-ticaret siteleri ise kötü reklam ve sitelerinin çökertilmesi sonucu yaşanacak finansal kayıplardan dolayı endişe duymaktadır. Online güvenlikle ilgili olarak çok sayıda kritik sosyal ve kurumsal sorunlar bulunmaktadır. Bunlardan ilki risk yönetimi için yeterli kurumsal süreçlerin geliştirilmesi, görevler ayrımı, güvenlik teminatı ve erişim kontrolüdür. İkincisi teknolojiye ziyade daha çok kullanıcı ve çalışanlar gibi zayıf halkaların oluşturduğu güvenlik sorunlarıdır. Üçüncüsü ise yazılım mühendisliği yönetimi ya da güvenlik teknolojilerinin nasıl uygulandığıdır (Gupta ve Dubey, 2016).

Gupta ve Dubey (2016) çalışmasında e-ticarete yönelik sorunları ya da tehditleri "yetkisiz erişim, hizmet engelleme, hırsızlık ve dolandırıcılık" olmak üzere üç ana başlık altında toplamaktadır. Yetkisiz erişim bilgisayar korsanlarının özellikle büyük veri kanalları üzerinden zayıf ağların güvenlik duvarlarını kırabilmelerini, alışveriş siteleri ve burada depolanan bilgilere izinsiz olarak ulaşabilmelerini ifade etmektedir. Yetkisiz erişimde bilgisayar korsanlarının sıklıkla kullandığı kaynaklar internet çerezleri ya da e-mail yollu virüslerdir. Hizmet engelleme de toplu olarak gönderilen ve internet iletişim kurallarına aykırı olduğu kabul edilen e-posta (spam) ve internet solucanı ya da truva atları gibi virüsler yoluyla gerçekleşmektedir. E-ticarete hırsızlık ve dolandırıcılık faaliyetleri ise çalınan verilerin farklı amaçlarla kullanılması ya da değişikliğe uğratılması sonucu gerçekleşmektedir. Bu durum sıklıkla online alışveriş sitelerinde yaşanmakta kullanıcıların özellikle kredi kartı bilgilerinin çalındığı durumlar ortaya çıkmaktadır (Gupta ve Dubey, 2016). En nihayetinde gizliliğe ve güvenliğe yönelik bu sorunlar e-ticaret kullanıcılarına olumsuz deneyimler olarak yansımakta, kullanıcıların güven duyguları zedelenmekte

ya da algıladıkları risk seviyesi artmaktadır ve bundan sonraki e-ticaret işlemlerinde tedirgin davranışlar sergilemelerine sebep olmaktadır. Dolayısıyla e-ticarete gelişimin sağlanmasının kullanıcı gizliliği ve güvenliğine yönelik sorunların asgari seviyeye indirilmesi ile mümkün olduğu görülmektedir. Bunun için e-ticarete ilerlemek isteyen şirketlerin sorunları iyi analiz etmesi, gizlilik ve güvenlik için gerekli amaçları ve araçları doğru belirlemesi gerekmektedir (bakınız tablo 6).

Diğer taraftan gizlilik ve güvenlik sorunlarının temelini oluşturan başlıca faktörlerden birisi olarak güven duygusu karşımıza çıkmaktadır (Shalhoub, 2006). Angriawan ve Thakur (2008) çalışmalarında e-güven ile gizlilik ve güvenlik arasında karşılıklı bir ilişki bulunduğunu ortaya koymuştur. Online tüketiciler online alışveriş işlemlerini yönetmek hususunda belli bir kabiliyete sahip olduklarında işletmeler de müşterilerine karşı e-güveni sağlamaktadır. Gizlilik ve güvenliğe yönelik potansiyel tehditler müşterilerde güven eksikliğine neden olmakta ve onların e-ticaretin sunduğu fırsatlardan yararlanma noktasında kabiliyetlerini ortadan kaldırmaktadır. Satıcılar ve alıcılar, alıcılar ve ürünler arasında fiziksel bir durumun bulunmayışı ve e-ticaretin kendine özgü zorlukları satıcılar açısından müşterileri ile ilişki kurmayı güçleştirmektedir. Mandic (2009) online bilgi teknolojilerinin güvenli hale getirilmesi ve müşterilerin gizliliğine öne verilmesinin gerekli güveni kurmada yardımcı olduğunu, bunun tüketicilerin e-ticarete daha fazla yaklaşmasını ve şirketlerle ilişki kurmasını sağladığını belirtmektedir.

2.4. Sosyal Medya ve E-Ticaret Kullanımında Gizlilik ve Güvenliğe Etki Eden Faktörler

Kişisel bilgilerin, faaliyetlerin, coğrafi konum bilgilerinin günümüz bilgi teknolojileri ile geniş çapta toplanabilir olması insanların gizlilik ve güvenliklerini tehdit eder hale geldiği gibi kendi özgür iradeleri ile sosyal medya ve e-ticaret uygulamalarını kullanmaları özgürlüklerini sınırlamaktadır. Bu uygulamalar üzerinden kişisel veri ve bilgilerin toplanmasının yanı sıra insanlar gizlice izlenebilmekte bu da insan hak ve özgürlüklerine büyük bir tehdit oluşturmaktadır. Hükümet yetkilileri ve işletmeler sosyal medya ve e-ticaret işlemleri üzerinden kişilere ya da sosyal gruplara ait çok sayıda ve farklı türden bilgiyi toplayabilmektedir. Toplanan bu bilgi ve veriler ise analiz edilip işlendikten sonra kullanıcıların davranışlarını tahmin etmek ya da etkilemek üzere ticari ya da siyasi amaçlarla kullanılmaktadır. Buradan hareketle araştırmanın nihai amacı bilgi ve verinin en önemli kaynakları olan sosyal medya ve e-ticaret uygulamalarının kullanımı sonucu ortaya çıkan online gizlilik ve güvenlikle ilgili faktörlerin ve sorunların kullanıcı davranışlarına olan etkisini ortaya koymaktır. Bu çerçevede araştırmada öncelikle sosyal medya ve e-ticaret kullanıcılarının gizlilik ve güvenlik endişeleri, farkındalık seviyeleri ve yaşadıkları olumsuz deneyimler ölçülmüştür. Daha sonra bu faktörlerin kullanıcılarının güven duygusu ve risk algıları, bunların da korunma ve gizleme şeklinde ortaya çıkan davranış türleri üzerine etkisi değerlendirilmiştir.

2.4.1. Gizlilik ve Güvenlik Farkındalığı

Sosyal medya ve online alışveriş siteleri kullanıcılarının gerek gizlilik ve güvenlik endişelerini gerek güven ve risk algılarını gerekse doğrudan ve dolaylı olarak online olarak satın alma davranışlarının etkileyen ana faktörlerden birisi gizlilik ve güvenlik farkındalığıdır (GGF). GGF, online olarak kişisel bilgilerin toplandığı ve toplanan bilgilerin kullanımını sınırlamak için bir takım yöntemlerin olduğuna yönelik bilgi düzeyini ifade etmektedir (Phelps ve diğerleri, 2000). Diğer bir tanıma göre GGF, bireyin gizlilik ve güvenlik uygulamaları ve politikaları ile paylaşılan bilgilerinin nasıl kullanıldığı hakkında ne derece bilgilendirildiği ve bireyin özel alanını muhafaza etmek için sahip olduğu yetenekleri ne ölçüde kullanabildiğini yansıtmaktadır (Dunfee ve diğerleri, 1999; Phelps ve diğerleri, 2000). Eğer kullanıcılar bilgilerinin toplandığı gerçeğinin farkında değil iseler, hiç şüphesiz kullanıcı davranışlarını değiştirmek ya da gizlilik ve güvenlik ayarlarına uyum sağlamak hususlarında herhangi bir endişe duymayacaktır. Federal Ticaret Komisyonu (FTK) online tüketicilerin hangi amaçla verilerinin kullanıldığı ve ne derece bu verilerinin üçüncü taraflarla paylaşıldığı konusunda ilgisiz ya da bilgisiz olabileceği durumlara dikkat çekmektedir. Diğer taraftan online kullanıcıların bir kısmı bu durumun farkında olarak endişe duyabilir yanıltıcı bilgi vermek, güvenliğini artırıcı araçlar kullanmak ya da çerezlerini sıklıkla temizlemek gibi işlemlere ya da yöntemlere başvurabilmektedir. (FTC, 2010).

Dinev ve Hart (2006) sosyal farkındalığı gizlilik endişelerinin tahmin edici unsuru olarak geliştirmiştir. Onlara göre yüksek sosyal (gizlilik-güvenlik) farkındalığa sahip bireyler tesadüfi, kötü niyetli ya da kasti olarak kişisel bilgilerin sızdırılması sonucu oluşacak olası gizlilik kayıpları ile gizlilik-güvenlik politikalarının geliştirilmesi gibi sorunları genel olarak yakından takip etmektedir. Medya haberleri ve kamuoyunda geniş yer bulan olaylar bireylerin olası gizlilik ve güvenlik ihlalleri ve ilgili risklere daha aşina olmalarını sağlamaktadır. Bu tür kullanıcılar daha güçlü bir farkındalığa sahip olmakta ve sosyal hayattaki gizliliğin önemini daha iyi kavrayabilmektedir. Zira 2013 yılının Haziran ayında ortaya çıkan Edward Snowden'in Amerikan Güvenlik Dairesi (NSA) ile ilgili itirafları, izleme-gözetleme teknolojilerinin devletler tarafından nasıl kullanıldığının ve bunun sonucunda ortaya çıkan ihlallerin gizlilik ve güvenlik konusunda çok farklı bir seviyeye taşındığının en büyük göstergelerinden biri olarak kabul edilmektedir. Öte yandan Facebook, Twitter, Amazon ve E-bay gibi birçok büyük şirketin internet ortamında gerçekleştirdikleri online reklamcılık faaliyetleri de gizlilik ve güvenlik ihlallerinin diğer ayağını oluşturmaktadır. Bu konuda da yakın zamanda yaşanan Facebook krizi yaşanan en önemli gizlilik ve güvenlik ihlalleri arasında gösterilmektedir.

Diğer taraftan sosyal medya ve online alışveriş kullanıcılarının IoT ve büyük veri başta olmak üzere online gizlilik ve güvenlik ile alakalı veri madenciliği, web 3.0, bulut bilişim, yapay zeka gibi teknolojiler konusundaki bilgi düzeyleri de farkındalık seviyeleri hususunda oldukça önemlidir. Ayrıca bu konuda devletlerin ya da hükümetlerin kişisel verilerin korunmasına ilişkin uyguladıkları düzenlemeler ve yasalar konusunda kullanıcıların sahip olduğu bilgi düzeyleri, gizlilik ve güvenlik

farkındalığı çerçevesinde dikkate alınması gereken önemli bir etkidir. Rainie ve arkadaşlarının ABD’de yapmış olduğu çalışmada katılımcılara online faaliyetlerine yönelik mevcut gizlilik yasalarının yeteri bir koruma sağlayıp sağlamadığı sorulmuştur. Katılımcıların %66’sı yasaların yeterli olmadığını ifade ederken %24’ü yasaların yeterli bir koruma sunduğunu belirtmiştir (Rainie ve diğerleri, 2013). Madden (2014) ise yaptığı çalışmada hükümetin izleme-görüntüleme (takip) programları hakkında daha fazla farkındalığı olan Amerikalıların sabit telefon hatları, mobil telefonlar, tekst mesajları, mailler, anlık mesajlaşma hizmetleri ve görüşmeleri, sosyal medya ve alışveriş siteleri gibi etkileşim ve iletişim kanallarını pek de güvenli görmedikleri sonucuna varmıştır. Yaklaşık 10 yıl önce Zuerik (2010) tarafından Çin’de yer alan 7 büyük büyükşehir ve il merkezine yönelik gerçekleştirilen araştırmada ise katılımcıların büyük bir çoğunluğunun IoT, büyük veri, veri madenciliği ve RFID gibi teknolojiler konusunda ya “çok az bilgi sahibi oldukları” ya da “hiç bilgi sahibi olmadıkları” sonucuna ulaşılmıştır.

Türkiye’de online GGF konusunda sınırlı sayıda araştırma olduğu görülmektedir. Yapılan araştırmalarda online kullanıcıların güvenlik tehditlerinin ve önlemlerinin farkında olmalarına rağmen güvenlik konusunda yeteri derecede tedbirler almadığı, mevcut güvenlik kontrollerini (dosya şifreleme, cihaz parolası kilidi, uzaktan dosya silme, cihaz bulucu) devre dışı bıraktıkları veya bu kontrollerden habersiz oldukları, internetten alış-verişte güvenlikle ilgili farkındalıkları olduğu diğer taraftan gerekli bilgi ve beceriler açısından zayıf oldukları şeklinde sonuçlar elde edilmiştir (Talan ve diğerleri, 2015; Akgün ve Topal, 2015). Bu çerçevede Türkiye’de ilgi alanda yapılan çalışmaların sınırlığından ve GGF’nin sosyal medya ve online alışveriş kullanıcılarının davranışlarına olan etkisinden dolayı araştırmamızda online kullanıcıların GGF düzeyleri ele alınarak aşağıdaki hipotezler geliştirilmiştir.

H1a: Sosyal medya ve online alışveriş siteleri kullanıcılarının GGF’sinin GA’ları üzerinde olumlu bir etkisi bulunmaktadır.

H1b: Sosyal medya ve online alışveriş siteleri kullanıcılarının GGF’sinin RA’ları üzerinde olumlu bir etkisi bulunmaktadır.

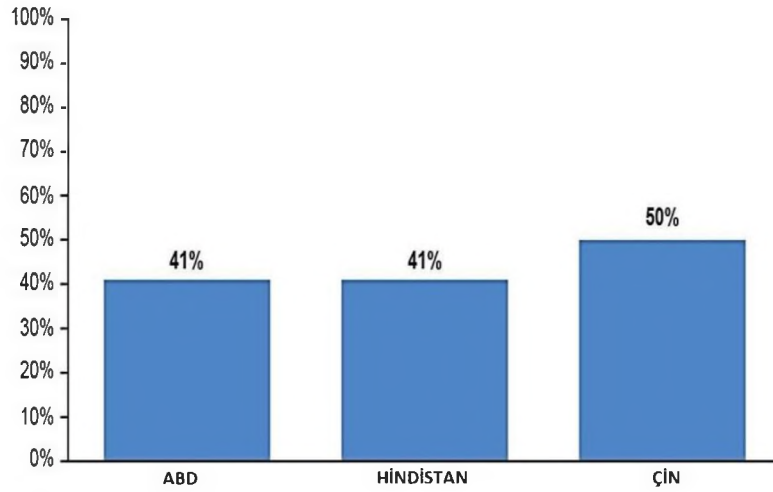
2.4.2. Gizlilik ve Güvenlik Endişesi

Gizlilik ve güvenlik endişeleri (GGE) sosyal medya ya da online alışveriş siteleri kullanıcıların bilgilerinin şirketler ya da diğer kuruluşlar tarafından elde edilmesi, saklanması ve farklı amaçlarla kullanılması sonucu ortaya çıkan endişe türlerini ifade etmektedir. Hong ve Thong (2013) GGE’yi bireylerin web sitelerinin kullanımı esnasında firmaların kişisel bilgilerini ne şekilde topladığı ve kullandığı hususundaki kontrol kabiliyeti olarak tanımlamaktadır. Hong ve Thong (2013) GGE hakkındaki mevcut kavramlaştırmalar ile önerilen karşılaştırmalar arasındaki benzerlikleri incelemek amacıyla bir karşılaştırma yapmıştır. Yapmış oldukları çalışmanın sonucunda etkileşim ve bilgi yönetiminin GGE’yi etkilediğini ve online kullanıcıların kişisel bilgilerinin toplanması ve bunların web siteleri tarafından kullanılması hususlarında endişe duydukları belirtilmiştir. Ayrıca ilgili çalışmada kişisel bilgilerinin korunması amacıyla yürütülen faaliyetler konusunda da

kullanıcıların endişelendikleri ifade edilmiştir. Medyada çıkan kimlik hırsızlığı ve kredi kartı dolandırıcılığındaki artışları gösteren raporlar ise kullanıcıların endişelerini haklı çıkarmaktadır (Hong ve Thong, 2013).

Günümüz dünyasında bilgi gizliliği ve güvenliği konusundaki endişeler sosyal medya ya da online alışveriş siteleri üzerinden yapılan e-ticaretin gelişimini ve başarısını önemli ölçüde etkilemektedir. Uygulanan güçlü gizlilik ve güvenlik mekanizmalarının ise sosyal medya ya da online alışveriş siteleri üzerinden satış yapan kişi ya da işletmelere olan güveni ise artırdığı birçok çalışma ile ortaya konmuştur (Meinert ve diğerleri, 2006).

Şekil 7: Ülkeler Arası Gizlilik Endişesi



Kaynak: Pingitore, G., Meyers, J., Clancy, M., & Cavallaro, K. (2013). Consumer concerns about data privacy rising: What can business do. JD Power report.

Boritz ve No (2011) kullanıcıların ülke ve kültürlerinin GGE üzerinde etkisi olduğunu ileri sürmektedir. Bu çerçevede literatürde çoğunluğu ABD başta olmak üzere farklı ülke ve kültürlerle yönelik olarak birçok araştırma yapılmıştır. ABD sosyal medya ve online alışverişin sıklıkla kullanımında ön plana çıkmakta olup nüfusu dünyanın en kalabalık ülkeleri olan Hindistan ve Çin gibi ülkelere de sosyal medya ve online alışveriş sitelerinin kullanımı hızla artmaktadır. Bu ülkelerin kültürel yönden ABD'den çok farklı olmaları itibarıyla farklı ülkelere yönelik GGE çalışmalarının da buna paralel olarak arttığı görülmektedir. Bununla beraber McGraw Hill Financial Enstitüsünün çalışması (Pingitore ve diğerleri, 2013) online penetrasyon, gizlilik ve güvenlik yasaları ve veri girişi kontrolüne yönelik yaklaşımlardaki ülkeler arası farklılıklara rağmen dünya genelinde GGE'nin tüm yaş gruplarından kullanıcılar için benzer özellikler gösterdiği sonucunu elde etmiştir. Örneğin online gizlilik konusunda Hindistan'daki kullanıcıların endişe seviyelerinin ABD'deki kullanıcıların endişe seviyeleri (%41) ile aynı olduğu görülmüştür. Ancak her iki ülkedeki endişe seviyeleri Çinli kullanıcılarındaki ile karşılaştırıldığında (%50) belli bir dereceye kadar daha düşük olduğu gözlenmiştir (bakınız şekil 7).

Genel olarak bakıldığında kişisel bilgilerin korunması ile ilgili olarak ülkeler arası kişisel verilerin yönetimi konusundaki endişeler çoklu yapıya sahip ülkelere faaliyet

gösteren işletmeler için dikkat edilmesi gereken bir husus olarak karşımıza çıkmaktadır. Hindistan'daki online kullanıcıların (tüketicilerin) %74'ü, Çin'dekilerin ise %72'si kişisel bilgilerin nasıl toplandığı ve şirketler tarafından nasıl kullanıldığı hususunda kontrolü kaybettiğini ifade ederken ABD'de bu oran %80 olarak kaydedilmiştir (Pingitore ve diğerleri, 2013).

Rainie ve arkadaşları ise yaptığı çalışmada ABD'de de online kullanıcıların %68'nin maillerinin içeriğine, %55'nin indirdikleri dosya ya da içeriğe, %54'nün konum bilgilerine, %51'nin online yazışma ve görüşmelerinin içeriğine, %46'sının araştırdığı web sitesine ve %44'nün yaptıkları internet aramalarına sadece kendilerinin ya da yetkili kişilerin ulaşabilmesi gerektiğine inandıklarını belirtmektedir.

Ülkeler arası çalışmaların verilerinden hareketle sosyal medya ve online alışveriş kullanıcıların bilgi gizliliği ve güvenliği kapsamında GGE'lerinin incelendiği çalışmamızda Türkiye ölçeğinde elde edilen veriler ABD'deki veriler ile karşılaştırılarak literatüre katkı sağlanması hedeflenmiştir. Bu çerçevede GGE'nin sosyal medya ve online alışveriş kullanıcılarının risk algıları ve güveni üzerine etkisi ile doğrudan kullanıcı davranışlarına nasıl etki ettiği sorgulanmış, aşağıdaki hipotezler geliştirilmiştir.

H2a: Sosyal medya ve online alışveriş siteleri kullanıcılarının GGE'nin GA'ları üzerinde olumlu bir etkisi bulunmaktadır.

H2b: Sosyal medya ve online alışveriş siteleri kullanıcılarının GGE'nin RA'ları üzerinde olumlu bir etkisi bulunmaktadır.

H2c: Sosyal medya ve online alışveriş siteleri kullanıcılarının GGE'nin kullanıcı koruma davranışı üzerinde olumlu bir etkisi bulunmaktadır.

H2d: Sosyal medya ve online alışveriş siteleri kullanıcılarının GGE'nin kullanıcı gizleme davranışı üzerinde olumlu bir etkisi bulunmaktadır.

2.4.3. Olumsuz Deneyimler

Daha önceki bölümlerde de belirtildiği üzere çok sayıda kişisel bilgi ve veri, büyük veri bankalarında depolanmakta ve bunlar işletmeler tarafından farklı amaçlar için kullanıcıların izni olmadan kullanılabilir. Bu durum daha çok kullanıcıların bilgi gizliliğini ilgilendirmekle beraber asıl sorun yetkisi olmayan üçüncü şahısların bu bilgilere izinsiz erişimleri sonucu yaşanmaktadır. Zira sosyal medya ve online alışveriş sitelerini kullanabilmek için bireyler bazı kimlik bilgilerini, e-mail adreslerini paylaşmak durumunda olduğu gibi ürün satın almak için kimlik numarası, kredi kartı numarası ve banka hesap bilgileri gibi çok önemli bilgilerini de vermeleri gerekmektedir. Bu tür bilgiler bilgisayar korsanları gibi erişim yetkisi olmayan üçüncü taraflarca çalınabilmekte ve kullanıcılar kimlik hırsızlığı kapsamında online dolandırıcılık, tehdit ve şantaj gibi olumsuz durumlarla karşı karşıya kalabilmektedir.

Sosyal medya ve online alışveriş siteleri kullanıcılarının gizlilik ve güven endişelerinin yanında güven ve risk algılarına etki eden önemli faktörlerden birisi

online işlemleri esnasında tecrübe ettikleri yukarıda bahsedilen olumsuz deneyimlerdir. Birçok araştırmada kullanıcı deneyimleri online gizlilik ve güvenlik sorunları ile ilişkili olarak gizliliğin ve güvenliğin korunması, algılanan risk ve güven boyutu başlıkları altında ve daha çok kimlik hırsızlığı şeklinde ele alınmıştır (Choi ve Lee, 2003; Ha, 2004; Milne ve diğerleri, 2004). Kimlik hırsızlığı FTK tarafından son yıllarda ABD’de hızla artış gösteren ve kullanıcıların online işlemlerini olumsuz şekilde etkileyen, bir kişinin kişisel ve finansal bilgilerini çalmak suretiyle işlenen online dolandırıcılık ve hırsızlık faaliyeti olarak tanımlanmaktadır (FTC, 2004). Bu araştırmada ise kullanıcıların online işlemleri sonucu karşılaştıkları dolandırıcılık ve hırsızlık gibi durumlar olumsuz deneyimler başlığı altında ayrı bir boyut olarak değerlendirilmektedir.

Diğer taraftan olumsuz bir deneyim ile karşı karşıya kalmak için herhangi bir sosyal medya ya da online alışveriş platformunda hesabınızın olması yeterli olabilmektedir. Yine yetkisi olmayan kişilerce kullanıcılara ait hesaplar çalınabilmekte ve kişilerin itibarına zarar verecek paylaşımlar başkalarınınca yapılabilir. Buna ilave olarak özellikle kullanıcılar kimsenin müdahalesi olmadan da sosyal paylaşım ağlarındaki bazı paylaşımları yüzünden tacize, tehdide uğrayabilmekte, bir iş ya da eğitim fırsatını kaybedebilmekte, yakınları ile çeşitli sorunlar yaşayabilmekte hatta fiziksel şiddete maruz kalabilmektedir. Rainie ve arkadaşlarının (2013) ABD’de yaptığı çalışmada anket katılımcılarından %21’inin mail ya da sosyal medya hesaplarının izinleri dışında ele geçirildiği, %12’sinin online olarak takip ve taciz edildiği, %11’nin sosyal güvenlik numarası, kredi kartı numarası ya da banka hesap bilgileri gibi bilgilerinin çalındığı, %6’sının online olarak gelişen olaylar karşısında itibarının zarar gördüğü, %6’sının online dolandırıcılık kurbanı olduğu ve parasını kaybettiği ve %4’nün ise online olarak gelişen olaylar karşısında fiziksel şiddete uğradığı belirtilmiştir.

Bu çerçevede özellikle ABD’de yapılan araştırmalardan hareketle Araştırmada gizlilik ve güvenlik kanunları ile alakalı en güncel ve en önemli sorunlardan biri olarak karşımıza çıkan kimlik hırsızlığı, itibar zedelenmesi gibi durumlar olumsuz deneyimler başlığı altında değerlendirilerek aşağıda belirtilen hipotezler geliştirilmiştir.

H3a: Sosyal medya ve online alışveriş siteleri kullanıcılarının OD’nin GA üzerinde olumlu bir etkisi bulunmaktadır.

H3b: Sosyal medya ve online alışveriş siteleri kullanıcılarının OD’nin RA üzerinde olumlu bir etkisi bulunmaktadır.

2.4.4. Güven Algısı

Herhangi bir ilişki türünün ya da sosyal etkileşimin vazgeçilmez unsuru olan güven kavramı en basit tanımı ile bir tarafın diğerinin zayıflıklarından avantaj sağlama yoluna gitmeyip ahlaki ve tutarlı şekilde bir davranış sergilemesi bunun sonucunda diğerinin risk alma eğiliminde olmasını ifade etmektedir (Mayer ve diğerleri, 1995). Güven soyut bir kavram olmakla birlikte araştırmaların büyük bir çoğunluğu kişiler

arası güven üzerine yoğunlaşmaktadır. Güven sosyal medya ve e-ticaret faaliyetlerinin gelişimi ile beraber online kullanımlarda önemli bir rol oynamaktadır. Sosyal medyanın gelişimi internetin yayılmasına dayandığından internete olan güven ile alakalı literatürle sosyal medyaya olan güven konusundaki tartışmalar arasında bağlantı kurmak çok doğal bir durumdur. E-ticaret çerçevesinde güven kavramı ele alındığında ise ilgili taraflar online alıcılar ve satıcılar olduğundan güveni online satıcılar ve işletmelere yönelik olarak yorumlamak mümkündür. E-ticaret araştırmaları güven kavramı ile bilgi paylaşımı arasında güçlü bir bağlantı olduğunu ortaya koymaktadır. Araştırmalarda güvenin algılanan maliyetin hesaplanmasında kullanıldığı ifade edilmektedir. Yüksek güven düşük maliyet algısını yaratırken tam tersi durumda yüksek maliyet algısı oluşmaktadır. Kişiler arası karşılıklı alışveriş durumlarını inceleyen çalışmalar güvenin kendini ifade etmenin ön koşulu olduğunu çünkü güvenin özel bilgilerin paylaşılması ile ilgili durumlarda algılanan riskleri azalttığını belirtmektedir (Dwyer ve diğerleri, 2007). Görüldüğü üzere güven ve risk arasında yakın bir ilişki bulunmaktadır. Güven bireyin kontrol sahibi olmadığı olumsuz sonuçlar algıladığı riskli durumlarda gerekli bir unsur olarak karşımıza çıkmaktadır. Eğer risk yoksa ve tüm değişkenlerin kontrolü bireyin elindeyse güvene ihtiyaç yok demektir (Scholsser ve diğerleri, 2006).

Güven-Risk ilişkisi özellikle internette sosyal medya ve online alışveriş sitelerinde kişiler arası etkileşimlerde gizlilik ve güvenlik konularında kayıplar yaşanmasından dolayı oldukça önemli hale gelmiştir. Bu nedenle etkileşimde bulunan tarafın güveni önemle ele alınmalıdır. Çalışmalar özellikle e-ticaret işlemlerinde güvenin algılanan riski azalttığını ortaya koymaktadır (Van Slyke ve diğerleri, 2006, Malhotra ve diğerleri, 2004, Kimery ve McCord 2002). Güven bireylerin online olarak işletmeler ya da satıcılar ile etkileşime geçmesini ve işletme ya da satıcıların iyi niyetli ve etik olarak davrandıklarına inanmalarını sağlamaktadır. Birçok araştırma güveni işletmeden müşteriye olan (B2C) e-ticaretin geliştirilmesinin ve online işlemlerin başarı elde etmesinin anahtar değişkeni olarak tanımlamaktadır (Martin ve Camarero, 2009). Tüketicilerin online alışverişlerinde endişe etmelerinin önemli sebeplerinden birisi online satıcılara güvenememesi olarak açıklanmaktadır (Connolly ve Bannister, 2008). Online ticari işlemlerde güven alıcıların satıcılara duyduğu güven ile ölçülmektedir. Yu, Ha, Choi ve Rho (2005); Hsu, Chuang ve Hsu (2014) tüketicilerin e-ticarete olan güvenini e-ticareti kullanmaya yönelik tutumları çerçevesinde incelemektedir. Yaptıkları çalışmalarda tüketici güveninin tüketicilerin e-ticareti kullanmaya yönelik tutumlarını olumlu anlamda etkilediğini ifade etmektedirler.

Online gizlilik ve güvenlik konusunda tüketicilerin ya da kullanıcıların sosyal medya ve e-ticaret sitelerine olan güvenlerin onların satın alma niyetlerini olduğu kadar kullanıcı davranışlarını da etkilediğini söylemek mümkündür. Bununla beraber özellikle güven ve risk kavramları arasındaki güçlü ilişki dikkate alındığında yönetim ve online gizlilik çalışmalarında bu kavramların ele alınması büyük önem taşımaktadır. Birbiri ile etkileşim halinde bulunan bu iki faktör ele alındığında riskin kullanıcıları güven arayışına iterken, güvenin de aynı zamanda kullanıcıların risk

algılarını etkilediği görülmektedir. Bu noktadan hareketle araştırmamızda risk-güven arasındaki ilişki incelenirken aynı zamanda bu iki faktörün kullanıcı davranışlarına olan etkisi incelenmektedir. Bu çerçevede aşağıdaki hipotezler geliştirilmiştir.

H4a: Sosyal medya ve online alışveriş siteleri kullanıcıların güven algılarının risk algıları üzerinde olumlu bir etkisi bulunmaktadır.

H4b: Sosyal medya ve online alışveriş siteleri kullanıcılarının güven algılarının koruma davranışları üzerinde olumlu bir etkisi bulunmaktadır.

H4c: Sosyal medya ve online alışveriş siteleri kullanıcılarının güven algılarının gizleme davranışları üzerinde olumlu bir etkisi bulunmaktadır.

2.4.5. Risk Algısı

Risk algısı kavramı kişinin kararları ile alakalı potansiyel olarak oluşabilecek olumsuz sonuçları hakkındaki öznel düşüncelerini ifade etmektedir. Diğer bir ifadeyle “algı” kelimesi tüketici ile ilişkili bir ürün ya da alternatifin nesnel çıktılarının dağılımına karşılık olarak kullanılan bir kavram olarak görülmektedir (Samadi ve Nejadi, 2009). Bir başka tanıma göre ise risk algısı kişisel bilgilerin ifşa edilmesi (paylaşılması) olasılığı olarak ifade edilmekte ve araştırma sonuçlarına göre bireyler gizlilik ve güvenlik riskini diğer risk türlerine göre daha önemli bulmaktadır (Cases, 2002).

Risk algısı üzerine yapılan araştırmalar kavramın hem öncülleri hem de sonuçları üzerine gerçekleştirilmiştir. Risk algısının öncülleri üzerine yapılan araştırmalarda aşinalık (alışkanlık) (Van Slyke ve diğerleri, 2006), daha az hassasiyet içeren bilgiler (Malhotra ve diğerleri, 2004), itibar (Chen ve Dubinsky, 2003), web sitesi tavsiyesi (Garbarino ve Strahilevitz, 2004), bireyin gizlilik endişesi (Van Slyke ve diğerleri, 2006; Malhotra ve diğerleri, 2004), marka imajı (Tan, 1999) ve geçmiş internet deneyimleri (Liebermann ve Stashevsky, 2002; Kuhlmeier ve Knight, 2005) risk algısını azaltıcı öncüller olarak karşımıza çıkmaktadır. Ayrıca kültür (Choi ve Geistfeld 2004), yaş (Ueltschy, 2004), cinsiyet (Garbarino ve Strahilevitz, 2004) ve medeni durum (Liebermann ve Stashevsky, 2002) gibi demografik değişkenlerin de risk algısı üzerinde etkisi olduğu yapılan araştırmalar ile ortaya konmuştur.

Risk algısının belirsizlik ve sonuçları olmak üzere iki boyutu bulunmaktadır. Belirsizlik bir ürünün özellikleri ve işlevleri konusunda tüketicilerin aşina olmadığı ya da alışkanlık sahibi olmadığı endişe durumları ile alakalıdır. Sonuçlar ise daha çok satın alma ya da kullanma sonrası tüketicilerin zaman, para ve zihniyet kaybı sonucu yaşadığı sıkıntıları ifade etmektedir. Yani sosyal medya ya da online alışveriş sonucu oluşabilecek her türlü kayıplar ya da taciz ve şiddete uğrama gibi durumlar risk algısının sonuçları ile alakalı sorunlardır ve risk algısının yüksek oluşuna doğrudan etki yapmaktadır. Hassan ve arkadaşları (2006) algılanan riskin çok yönlü bir kavram olduğunu ve sekiz boyutta kavramlaştırılmasını gerektiğini söylemektedir. Bu boyutlar; maddi kayıplar, performans kaybı, zaman kaybı, sosyal, fiziksel, psikolojik riskler ile kaynak ve gizlilik riski olarak sıralanmaktadır. Hassan ve arkadaşlarından farklı olarak algılanan riskin kavramlaştırılması üzerine daha fazla vurgu yapan ve bu

çerçevede yeni ölçekler geliştiren Faqih (2013) ise deneysel olarak algılanan risk ile davranışsal niyet arasındaki ilişkiyi test etmiştir. Ürdün’de ölçeğinde yapılan bu çalışmada algılanan riskin online alışveriş üzerinden ürün satın almaya yönelik davranışsal niyeti olumsuz olarak etkilediği sonucuna varılmıştır. Teo ve Liu (2007), Katos (2012), ve Hsu ve arkadaşları (2014) da risk algısının tutum üzerine etkisini incelemiş ve risk algısının tutum üzerinde önemli bir negatif etkisi olduğunu ortaya koymuştur. Diğer taraftan bir önceki bölümde belirtildiği üzere birbiri ile etkileşim halinde olan risk ve güven algısı arasındaki ilişkiye de dikkate etmekte fayda vardır. Zira araştırmada bu iki faktör arasındaki ilişki de incelenmektedir.

Araştırmada risk algısının sosyal medya ve online alışveriş sitelerinin kullanımı çerçevesinde gizlilik ve güvenlik riski boyutu ele alınmaktadır. Kişinin bilgisi dışında kişisel bilgileri üzerindeki kontrol kaybı ve izinsiz bu bilgilerin kullanılması gizlilik riskini oluşturmaktadır (Aldás-Manzano ve diğerleri, 2009). Sosyal medya ve online alışveriş kullanıcıları özel bilgilerini firmalarla ya da satıcılarla paylaşırken firmaların kişisel bilgilerini kötü amaçlarla kullanması ya da bu bilgileri başkaları ile paylaşması ihtimaline karşı tedirginlik duymaktadır. Bu durum kısaca algılanan gizlilik riski olarak açıklanmaktadır. Bununla beraber Roca, Garcia, ve de la Vega (2009) diğer boyut olan güvenlik riskini veri ya da ağlara yönelik ekonomik sıkıntılar çıkarabilecek tahribat, bilgilerin ifşası, veriler üzerinde değişiklik yapma, hizmeti engelleme, boşa harcama, dolandırıcılık ve kötüye kullanma gibi şekillerde ortaya çıkan tehditler ya da tehlikeler olarak ifade etmektedir. Bu bağlamda mevcut literatür üzerinden araştırmada gizlilik ve güvenlik riski ve güven ile ilişkili olarak aşağıdaki hipotezler geliştirilerek sosyal medya ve online alışveriş kullanıcıların gizlilik ve güvenlik algıları ile koruma ve gizleme olmak üzere ortaya çıkan davranış şekilleri incelenmeye çalışılmaktadır.

H5a: Sosyal medya ve online alışveriş siteleri kullanıcılarının risk algılarının koruma davranışları üzerinde olumlu bir etkisi bulunmaktadır.

H5b: Sosyal medya ve online alışveriş siteleri kullanıcılarının risk algılarının gizleme davranışları üzerinde olumlu bir etkisi bulunmaktadır.

2.4.6. Kullanıcı Davranışı

Sosyal medya ve e-ticaret (online alışveriş) kullanımına yönelik yapılan son araştırmalar bilgi paylaşımının çok büyük boyutlarda olduğuna dikkate çekmektedir (Lenhart and Madden, 2007). Özellikle sosyal medya uygulamalarının kullanımına yönelik olarak insanların gizlilik değerlerini ya da güvenliklerinin çok da fazla önemsemedikleri sosyalleşmenin onlar için daha önemli olduğu görülmektedir. Benzer durum online alışveriş uygulamaları için de geçerlidir. Kullanıcılar gizlilikleri ve güvenliklerinden ziyade sağlayacakları fayda ile daha fazla ilgilenmektedir. Diğer taraftan kullanıcılar her ne kadar gizliliklerini önemsemeseler de son yaşanan gelişmeler karşısında gizlilik ve güvenlik konularında farkındalık ve endişe seviyeleri giderek artış göstermektedir. Büyük veri ve benzeri teknolojik girişimler ile çok büyük boyutlardaki kişisel verilerin toplandığı ve farklı amaçlarla

kullanıldığı gerçeğinin daha fazla insan tarafından kabul görmesi ile birlikte kullanıcıların gizlilik ve güvenlik algıları ve davranışları da değişim göstermektedir.

Bazı araştırmalar gizlilik ve güvenliğı çelişkili kavramlar olarak nitelemekte ve konu gizlilik ve güvenliğe geldiğinde insanların tutum ve hareketleri ile ilgili olarak ikiyüzlü göründüklerini belirtmektedir (Norberg ve diğerleri, 2007; Berenth ve diğerleri, 2005; Acquisti ve Grossklags, 2004). Gizlilik ve güvenlikleri hakkında ne söyledikleri üzerine oluşan kullanıcı davranışlarında bir tutarsızlık bulunmaktadır. Daha da önemlisi kullanıcılar gizlilik ve güvenlik endişelerinin sergiledikleri fiili davranışlardan daha yüksek olduğunu ifade etmektedir. Bu durumu açıklamak adına Berendt ve arkadaşları (2005) deneysel bir çalışma gerçekleştirmiş ve gizlilik tercihleri üzerine olan beklentilerinden çok daha fazla bilgiyi online depolama alanlarına sağladıklarını tespit etmiştir. Benzer şekilde Norberg ve arkadaşları (2007) offline (çevrimdışı) bilgi ifşası deneyinde toplanan bilgi miktarının bireylerin beyan etmeyi düşündükleri (sisteme bildirecekleri) bilgiden çok daha büyük boyutta olduğu sonucunu elde etmiştir.

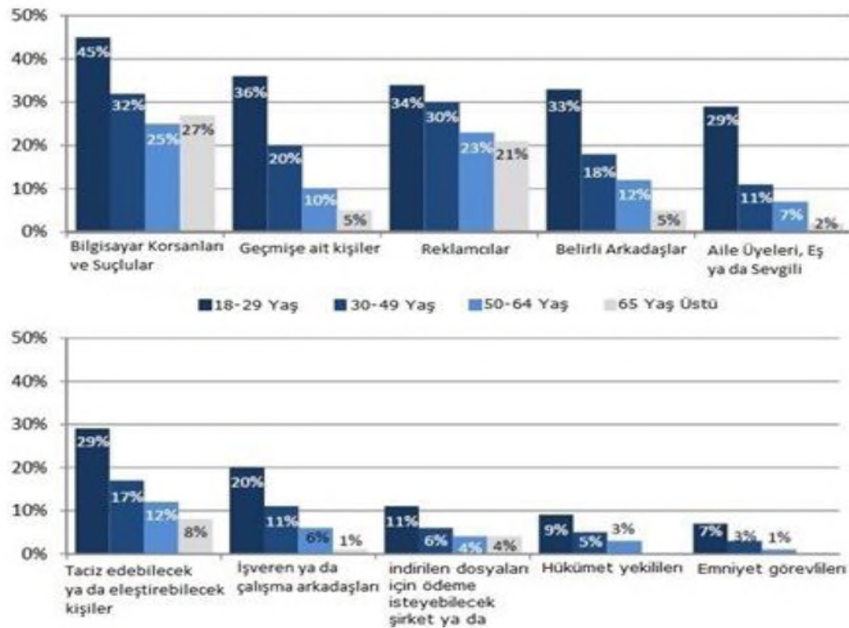
Mevcut literatürden ve sosyal medya ve online alışveriş kullanıcılarının gizlilik ve güvenlik algılarından hareketle araştırmada sorgulanan kullanıcı davranışları Korunma Motivasyonu Teorisi (Protection Motivation Theory) kapsamında ele alınmaktadır. Korunma Motivasyonu Teorisi (KMT) bireylerin riskleri ve faydaları tartarak kendilerini koruyacakları ve oluşabilecek zararların önüne geçebilecekleri davranış süreçlerini açıklamaktadır. Bu sürecin çıktısı ise bireylerin aldıkları savunma (başa çıkma) önlemleridir. Bir nevi savunma mekanizması olarak nitelenebilecek bu süreç adaptif (uyumlu) ve maladaptif (uyumsuz) yaklaşımlar şeklinde ortaya çıkmaktadır (Rippetoe ve Rogers, 1987). Uyumlu başa çıkma davranışları tavsiye edilen korunma mekanizmalarını kullanarak bilfiil tehdidin üstesinden gelme ya da tehdidi hafifletme yöntemleri (gizlilik ayarlarını kullanma vb.) olarak belirtilmektedir. Örneğin Youn (2005) KMT'yi risk ve ödül arasındaki ilişkinin geçerliliğini, bilgi sağlama eğilimini (istekliliğı), gizliliğı korumak için uygulanan başa çıkma davranışlarını (eksik ya da yanlış bilgi verme vb.) deneysel olarak sınamak için kullanmıştır. Bu bağlamda sosyal medya ya da online alışveriş sitelerine kişisel bilgileri sağlama hususunda risk algısı yüksekse, online kullanıcıların gizlilik ve güvenlik koruma davranışları içine gireceğı beklenmektedir. Uyumsuz başa çıkma davranışları da bireyin algılan riskin üstesinden gelebilmesi için birtakım yollar sunmaktadır. Bu yollar gizlilik ya da güvenlik tehdidi karşısında ortaya çıkan algı ya da hislerle bilişsel olarak başa çıkmayı öngörmektedir. Bu yollar tehdidin varlığını reddetme (kaçınma) ve tehdidin olabileceğini kabul etmeme (çaresizlik) gibi yöntemler olarak ifade edilmektedir (Rippetoe ve Rogers, 1987). Kısacası uyumsuz yaklaşımlarda birey yüksek bir risk algıladığında bu riskin üstesinden bilişsel yollarla gelmeye çalışacaktır. İlgili araştırmamızda ise KMT'nin adaptif (uyumlu) davranışları içeren boyutu ele alınmaktadır.

Özellikle online kullanıcıların farkındalık ve endişe seviyelerinin koruyucu teknolojileri kullanma ya da koruyucu davranışlar sergileme yönündeki niyetleri olumlu anlamda etkileyebileceğı çeşitli araştırmalar ile ortaya konmuştur. (Dinev,ve

diğerleri, 2009; Dinev ve Hu, 2007). Araştırmada bu faktörlerin yanı sıra güven ve risk algılarının da kullanıcı davranışlarında nasıl bir etki yarattığı sorgulanırken Türkiye ve ABD’deki kullanıcıların karşılaştırılması yapılmaktadır. Araştırmanın temel belirleyicisi olmamakla birlikte Türkiye ve ABD’de ki kullanıcıların karşılaştırılmasıyla online gizlilik ve güvenlik ve bu konudaki yasal düzenlemeler çerçevesinde kültürel farklılıkların kullanıcı davranışlarında farklı bir etkiye sebep olup olmadığı da araştırmada değerlendirilmektedir. Ayrıca yaş, cinsiyet, gelir durumu gibi demografik özelliklerin kullanıcı davranışları üzerindeki etkisi ve farklılıkları da araştırma kapsamında incelenmektedir.

Araştırmanın ABD’deki sosyal medya ve online alışveriş kullanıcılarının gizlilik ve güvenlik algılarına yönelik de yapılmasını sağlayan temel çalışmalardan birisi önceki bölümlerde de sonuçlarına sıklıkla değindiğimiz Rainie ve arkadaşlarına (2013) ait “Anonymity, Privacy, and Security Online” isimli araştırmanın verileridir. Bu araştırmada özellikle online gizlilik ve güvenlik endişeleri karşısında kullanıcıların sergiledikleri korunma ve gizleme davranışları üzerinde durulmaktadır. Araştırmada ankete katılanların %86’sının sosyal medya ya da online alışveriş gibi kanalları kullanırken isimsiz ya da gizli olmayı tercih ettikleri ve online davranışlarını maskeleye ya da izlenmekten kaçınmaya yönelik önlemlerden en az birisini aldıkları belirtilmektedir (Rainie ve diğerleri, 2013). Bu önlemler online hareketlerini ya da bilgilerini gizleyerek ortaya çıkan korunma davranışları şeklinde değerlendirilmektedir. İlgili araştırmamızda ise gizlilik ve güvenlik algıları çerçevesinde sosyal medya ve online alışveriş kullanıcılarının davranışları korunma ve gizleme şeklinde iki kategoride değerlendirilmektedir.

Şekil 8: Belli Kurum ya da Kişilerce izlenmekten kaçınan kişi grupları (ABD)



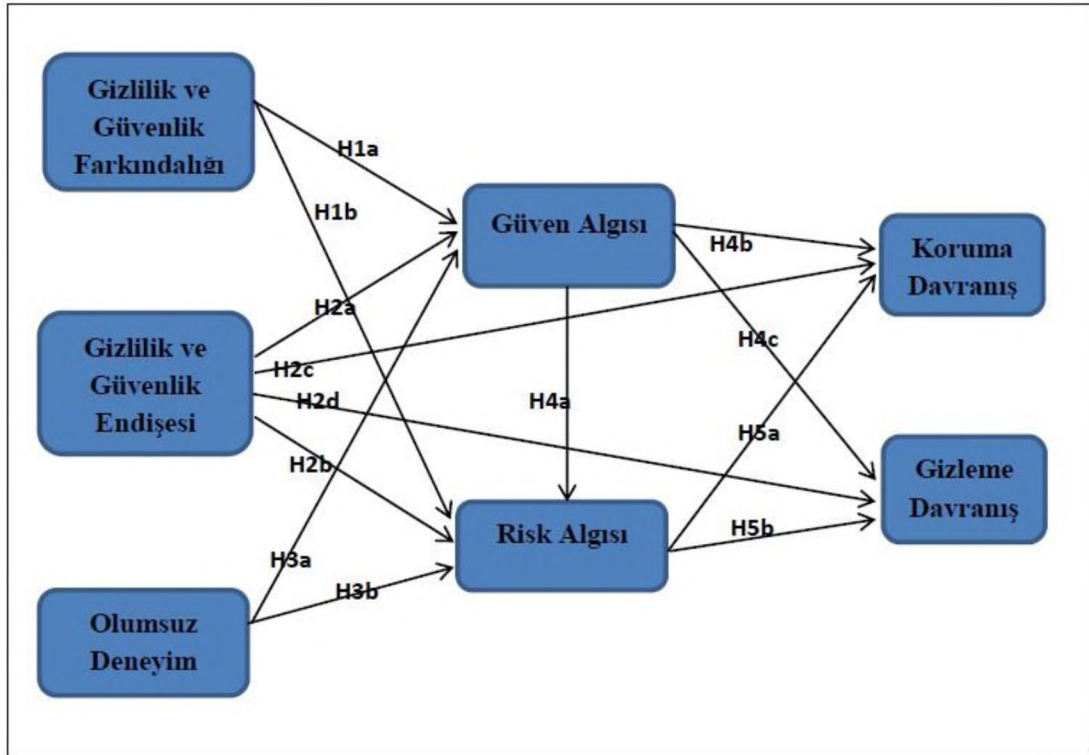
Kaynak: Rainie (2013) Pew Research Center “Anonymity, Privacy, and Security Online”

Rainie ve arkadaşlarının yaptığı araştırmaya katılanların büyük bir çoğunluğu tamamen online olarak gizli olunamayacağını belirtirken çok küçük bir kısmı tamamen online olarak gizlenebileceklerini yani görünmez olabileceklerini

savunmaktadır. Araştırmada %33 ile en yüksek oranda online kullanıcıların faaliyetlerini bilgisayar korsanları ya da suçlulardan gizlemeye çalıştıkları, bunu %28 ile reklamcıların takip ettiği belirtilmektedir. Hükümet yetkililerinden faaliyetlerini gizleme %5 olarak açıklanırken bu oran emniyet görevlileri için %4 olarak ifade edilmektedir (Rainie ve diğerleri, 2013).

Sonuç olarak bilgi gizliliği ve güvenliği açısından sosyal medya ve online alışveriş kullanıcılarının gizlilik ve güvenlik algılarının değerlendirildiği bu çalışmada beş temel faktörün kullanıcı davranışlarına olan etkisi değerlendirilmektedir. Önceki beş bölümde belirtilen soru ve hipotezler çerçevesinde kullanıcıların gizlilik ve güvenlik farkındalıkları ile endişelerinin, olumsuz deneyimlerinin, risk ve güven algıları arasındaki ilişkiler ve bunların kullanıcı davranışlarına olan etkisi aşağıda belirtilen araştırma modeli çerçevesinde incelenmektedir.

Şekil 9: Araştırma Modeli



BÖLÜM 3: ARAŞTIRMA YÖNTEMİ VE METODOLOJİ

Araştırma sosyal medya ve online alışveriş kullanıcılarının gizlilik ve güvenlik davranışlarını açıklayan karşılaştırmalı ve kapsamlı bir çalışma olarak gerçekleştirilmiştir. Araştırmada bilgi gizliliği ve güvenliği çerçevesinde sosyal medya ve online alışveriş kullanıcılarının koruma ve gizleme şeklinde ortaya çıkan davranışları Koruma Motivasyonu Teorisi (KMT) açısından ele alınmaktadır. Araştırmanın en önemli katkılarından birisi online kullanıcıların (tüketicilerin) karakteristik özellikleri ile gizlilik ve güvenlik algılarının Türkiye ve ABD olmak üzere iki farklı ülkede kullanıcı davranışlarına nasıl etki ettiğine yönelik değerlendirmeler içermesidir. Farklı model ve kavramsal çerçeveler doğrultusunda Araştırma post-pozitivist bir yaklaşımla online gizlilik ve güvenlik davranışlarına daha fazla ışık tutmayı amaçlamaktadır.

3.1. Araştırma Yöntemi

Çalışma pozitivist bir yaklaşımla belli sorulara cevap arayan ve hipotezleri sorgulayan nicel araştırma yöntemlerine dayalı açıklayıcı (explanatory) bir araştırma niteliğindedir. Nicel araştırmaların büyük bir çoğunluğu nitel araştırmalar ile karşılaştırıldığında daha kesin sonuçlar ortaya koyması bakımından daha etkilidir. Bu açıdan nitel araştırmalar ile değerlendirilemeyecek konular için ölçülebilir ve sayılabilir veriler sunması nicel araştırmaları daha tercih edilebilir kılmaktadır. Nicel araştırmaların temel amacı farklı değişkenler arasındaki özel ilişkileri sayılabilir veriler üzerinden açıklamaya çalışmaktır. Bu araştırmada konu ile ilgili literatür değerlendirildikten ve teorik bir çerçeve oluşturulduktan sonra çeşitli hipotezler geliştirilmiştir. Hipotezlerin test edilmesi ve araştırma sorularına cevap bulabilmek için Türkçe ve İngilizce dillerinde online anket formu düzenlenmiş ve anket Türk ve Amerikalı sosyal medya ve online alışveriş kullanıcılarına uygulanmıştır. Böylelikle nicel araştırmada çerçevesinde anket sorularının güvenilirliği ve geçerliliği test edilmiştir.

3.2. Örnekleme ve Verilerin Toplanması

Araştırmada sosyal medya ve online alışveriş kullanıcılarının demografik bilgileri, gizlilik ve güvenlik algıları ve bu kavramlarla ilişkili diğer faktörler ile kullanıcı davranışları arasındaki ilişki incelenmiştir. Online bir anket oluşturmak günümüzdeki en kolay uygulanabilir yöntemlerden biri haline gelmiştir. SurveyMonkey, SurveyMonkey, Doodle, LimeSurvey ve Google Dokümanlar gibi online araçlar farklı araştırma ve konular için çok çeşitli seçenekler sunmaktadır. Araştırmada Google Dokümanlar uygulaması üzerinden “Sosyal Medya ve E-Ticaret Kullanıcılarının Gizlilik ve Güven Algılarının Değerlendirilmesi” adıyla Türkçe ve İngilizce olmak üzere iki dilde bir anket formu hazırlanmıştır.

Anket çalışmasında kartopu örnekleme yaklaşımı kullanılmıştır. Katılımcılar e-mail ve facebook, linkedin gibi sosyal medya uygulamaları üzerinden araştırmaya davet edilmiş ve arkadaşlarını da anket çalışmasına katılmak üzere davet etmeleri için

teşvik edilmiştir. Araştırmada grup çeşitliliğini sağlamak açısından aynı zamanda farklı gruplar anket çalışmasına katılmak için davet edilirken bu farklı grupların başka farklı gruplara ulaşması hedeflenmiştir. Bu sayede farklı yaş gruplarından farklı eğitim ve gelir durumuna sahip kullanıcıların ankete katılması sağlanmıştır. Bunun dışında sınırlı sayıda da olsa Türkçe anketlerin bir kısmı online katılım yerine elden teslim etmek isteyen katılımcılara ulaştırılmıştır. Daha sonra bu anket verilerinin Google Dokümanlarda hazırlanan ankete girişleri yapılmıştır. Aynı anketin Amerikalı katılımcılara ulaştırılması için ayrıca Amazon's Mechanical Turk (MTurk) veri toplama web sitesi kullanılmıştır.

Anket çalışmasına Türkiye'den 142, ABD'den 120 kişi olmak üzere toplam 262 kişi katılmış olup iki ülkedeki katılımcıların toplanan verilerinin araştırma çerçevesinde karşılaştırılması yapılmıştır.

3.3. Ölçek Geliştirilmesi

Anket çalışmasında kullanılan sorular daha önce farklı çalışmalarda kullanılmış, geçerlilikleri test edilmiş ölçeklerden uyarlanarak araştırma anketine uygun hale getirilmiştir. Anket soruları tanımlayıcı (betimleyici) bilgileri ölçen sorular ile birlikte sosyal medya ve online alışveriş kullanımı ile alakalı gizlilik-güvenlik farkındalığı, endişeleri, güven, risk, tecrübe ve bazı online davranış türleri ile alakalı sorulardan oluşmaktadır. Anket soruları hazırlanırken ölçek çevirilerinde en fazla kullanılan geleneksel yaklaşım takip edilmiştir. ABD'li katılımcılara ölçek sorularının orijinal İngilizcesi uygulanırken Türk katılımcılar için öncelikle ölçek soruları İngilizceden Türkçeye çevrilmiştir. Daha sonra çevrilen ölçek tekrar İngilizceye geri çevrilmiş ve iki çeviri arasındaki eşitliğin her iki dili de konuşan örneklemeler üzerinde denenmesi ve sınanması gerçekleştirilmiştir.

Ölçeği oluşturan sorular çerçevesinde araştırmada online gizlilik ve güvenlik algıları sonucu oluşan, kullanıcı (tüketici) davranışlarına etki eden faktörler (değişkenler) “Gizlilik ve Güvenlik Farkındalığı (GGF)”, “Gizlilik ve Güvenlik Endişesi (GGE)”, “Olumsuz Deneyimler OD”, “Güven Algısı (GA)” ve “Risk Algısı (RA)” olarak belirlenmiş ve araştırmanın amacına uygun şekilde anket çalışmasına uyarlanmıştır. Araştırmada 7 ölçek toplamda 48 soru bulunmakta olup anketin hazırlanmasında tablo 6'da belirtilen kaynaklardan yararlanılmıştır. Araştırmada kullanılan ifadelerden 22'si çoktan seçmeli olup tanımlayıcı sorulardan yaşla ilgili olanı kısa yanıt şeklinde düzenlenmiştir. Tanımlayıcı İstatistik Bilgiler “Cinsiyet, Yaş, Eğitim, Gelir Durumu, İnternet ve Akıllı Telefon Kullanma Süresi, Sosyal Medya ve Online Alışveriş Kullanma Durumu ve Sıklığı, En Çok Kullanılan Sosyal Medya ve Online Alışveriş Uygulamaları ve Büyük Veri gibi Bilgi Teknolojileri Hakkındaki Bilgi Seviyesi” olmak üzere 12 kısımdan oluşmaktadır.

Tablo 6: Anket Ölçek Soruları

Değişken	Soru Sayısı	Alıntı Yapılan Kaynaklar
Gizlilik ve Güvenlik Farkındalığı	8	Kumaraguru ve Cranor, 2005; Zureik ve diğerleri, 2010; Dinev ve Hu, 2007
Gizlilik ve Güvenlik Endişesi	9	Taylor, 2003; Rainie, ve diğerleri, 2013; Madden, 2014
Olumsuz Deneyim	8	Rainie, ve diğerleri, 2013
Güven Algısı	5	Dwyer, ve diğerleri, 2007
Risk Algısı	6	Chen, ve diğerleri, 2009; Fogel & Nehmad, 2009; Malhotra ve diğerleri, 2004; C. L. Anderson & Agarwal, 2010; Johnston& Warkentin, 2010; Liang&Xue,2010
Korunma davranışı	7	Stern, 2011; Rainie, ve diğerleri, 2013
Gizleme davranışı	8	Rainie, ve diğerleri, 2013

Kullanıcı Davranışları ile buna etki eden 5 faktörün ölçümünde 5’li Likert Ölçeği kullanılmıştır. GGF faktörü “1” (Kesinlikle Katılmıyorum)’den “5” (Kesinlikle Katılıyorum)’e kadar, GGE faktörü endişe seviyesine göre “1” (Hiç)’den “5” (Çok)’e kadar, OD ve Kullanıcı Davranışlarını içeren faktörler “1” (Hiçbir zaman)’den “5” (Her zaman)’e kadar, Güven ve Algılanan Risk faktörleri ise yine “1” (Kesinlikle Katılmıyorum)’den “5” (Kesinlikle Katılıyorum)’e kadar derecelendirilmiştir.

3.4. Analiz Yöntemi ve Bulgular

Araştırma çerçevesinde toplam 262 katılımcıya ait anket verileri ve bulgularına yönelik tanımlayıcı istatistik, faktör, güvenilirlik, yapısal eşitlik modeli ve t-testi analizleri gerçekleştirilmiştir. Analizler için Sosyal Bilimler İstatistik Programı (SPSS) 21 ve AMOS (Analysis of Moment Structures) paket programları kullanılmıştır. Ayrıca Microsoft Excel Programından da verileri ve bulguları derlemek ve düzenlemek için faydalanılmıştır.

3.4.1. Tanımlayıcı İstatistikler

Araştırmada elde edilen tanımlayıcı bulgular anket katılımcılarının demografik özellikleri ve bazı kavramlara ilişkin bilgi düzeyleri frekans dağılımları ve crosstab (çapraz tablo) yöntemi kullanılarak analiz edilmiştir. Özellikle araştırmanın Türkiye ve ABD olmak üzere iki farklı ülke katılımcılarının karşılaştırılmasına yönelik olarak yapılması ve örneklem sayısının küçük ol münasebetiyle crosstab yöntemi analizlerde tercih edilmiştir.

Çapraz tablo analizi örneğin, etnik köken ve bölge arasında bir ilişkinin olup-olmaması gibi iki kategorik (isimsel veya dereceli) değişken arasındaki ilişkiyi incelememizi sağlayan bir yöntemdir (Özbay, 2009). Çapraz tablolar izlenen amaca göre Bir değişkenin bir başka değişken üzerindeki etkisini göstermek, Bir grubun kompozisyonunu (dağılımını) belirlemek ve Çaprazlanan değişkenler sonucu ortaya

çıkan olası alt grupların bütün içindeki kompozisyonunu belirlemek olmak üzere üç türlü yapılmaktadır (Özbay, 2009).

Tablo 7: Katılımcıların Cinsiyet Dağılımı

		Erkek	Kadın	Toplam
Türkiye	Katılımcı Sayısı	85	57	142
	Yüzdelik Oranlar	59,9%	40,1%	100,0%
ABD	Katılımcı Sayısı	80	40	120
	Yüzdelik Oranlar	66,7%	33,3%	100,0%
Toplam	Katılımcı Sayısı	165	97	262
	Yüzdelik Oranlar	63,0%	37,0%	100,0%

Cinsiyet bilgilerine yönelik yapılan analiz sonuçları Türkiye ve ABD olmak üzere Tablo 7’de gösterilmektedir. Türkiye’deki 142 katılımcının %59,9’unu erkekler, %40,1’ini kadınlar oluşturmaktadır. Amerika’daki 120 katılımcının ise % 66,7’sini erkekler oluştururken kadın katılımcıların oranı %33,3’dür. Yaş gruplarına göre ankete katılanların yüzdelik oranları ise Tablo 8’de belirtilmiştir. Türkiye’deki katılımcıların büyük bir çoğunluğunu 30 – 39 yaş aralığındaki grup (%39,4) oluştururken ABD’deki katılımcıların büyük bir çoğunluğunu 29 yaş altı grup (%54,2) oluşturmaktadır.

Tablo 8: Katılımcıların Yaş Grupları

		+29	30-39	40-49	50-59	60-69	70+	Toplam
Türkiye	Katılımcı Sayısı	15	50	33	23	4	2	127
	Yüzdelik Oran	11,8%	39,4%	26,0%	18,1%	3,1%	1,6%	100,0%
ABD	Katılımcı Sayısı	65	38	7	6	3	1	120
	Yüzdelik Oran	54,2%	31,7%	5,8%	5,0%	2,5%	0,8%	100,0%
Toplam	Katılımcı Sayısı	80	88	40	29	7	3	247
	Yüzdelik Oran	32,4%	35,6%	16,2%	11,7%	2,8%	1,2%	100,0%

Katılımcıların eğitim, gelir durumu gibi bilgilerinin de araştırma bulguları üzerinde etkili olduğu görülmektedir. Türkiye’deki katılımcıların %47,9’u üniversite mezunu iken bu oran ABD’li katılımcılarda %59,2 olarak ortaya çıkmıştır. Türkiye’deki katılımcılardan lise mezunu olanların oranı %29,6, ABD’li katılımcılarda bu oran %10,8’dir. ABD’deki katılımcıların %25,8’i yüksek lisans, Türkiye’dekilerin %14,8’i yüksek lisans mezunudur. Dolayısıyla araştırmada ABD’li katılımcıların

eğitim profilinin daha yüksek olduğu tespit edilmiştir. Araştırma çerçevesinde ankete katılım sağlayanların gelir durumları incelendiğinde ise Türk katılımcılar arasında %43,7 ile gelir seviyesi 3000 – 5000 TL arasında olanların oranının daha yüksek olduğu, buna karşılık Amerikalı katılımcılarda gelir durumu açısından en yüksek katılım oranının %40 ile 1000 – 2000 Dolar arasında gelire sahip olan gruba ait olduğu görülmektedir (bakınız Tablo 9-10).

Tablo 9: Katılımcıların Eğitim Durumu

		İlkokul	Ortaokul	Lise	Üniversite	Y. Lisans	Doktora	Toplam
Türkiye	Katılımcı Sayısı	1	6	42	68	21	4	142
	Yüzdelik Oran	0,7%	4,2%	29,6%	47,9%	14,8%	2,8%	100,0%
ABD	Katılımcı Sayısı	1	1	13	71	31	3	120
	Yüzdelik Oran	0,8%	0,8%	10,8%	59,2%	25,8%	2,5%	100,0%
Toplam	Katılımcı Sayısı	2	7	55	139	52	7	262
	Yüzdelik Oran	0,8%	2,7%	21,0%	53,1%	19,8%	2,7%	100,0%

Tablo 10: Katılımcıların Gelir Durumu

		Hiç Gelir Olmayan	1000-2000	2000-3000	3000-5000	5000 +	Toplam
Türkiye (TL)	Katılımcı Sayısı	1	12	35	62	32	142
	Yüzdelik Oran	0,7%	8,5%	24,6%	43,7%	22,5%	100,0%
ABD (Dolar)	Katılımcı Sayısı	0	48	30	23	19	120
	Yüzdelik Oran	0,0%	40,0%	25,0%	19,2%	15,8%	100,0%
Toplam	Katılımcı Sayısı	1	60	65	85	51	262
	Yüzdelik Oran	0,4%	22,9%	24,8%	32,4%	19,5%	100,0%

Sosyal medya ve online alışverişi mümkün kılan en önemli araç hiç şüphesiz internet kullanımıdır. Diğer önemli araç ise toplumda hemen hemen herkesi kullandığı akıllı telefonlardır. Bu bağlamda ankete katılan Türkiye'deki 142 katılımcının %76,8'i interneti 10 yıldan daha fazla bir süredir kullandığını ifade ederken hiç kullanmadığını belirten kişi bulunmamaktadır (bakınız Tablo 11). Diğer taraftan

ABD’deki 120 katılımcının %57,5’luk kısmı interneti 10 yıldan fazla süre kullandığını belirtmiştir. Bu oran Türkiye anket verileri ile kıyaslandığında internet kullanım süresi açısından belirgin şekilde az olduğu görülmektedir.

Tablo 11: Katılımcıların İnternet Kullanım Süreleri

		1 Yıldan Az	1 – 3 Yıl	4 -6 Yıl	7 – 9 Yıl	10 Yıl +	Toplam
Türkiye	Katılımcı Sayısı	1	3	4	25	109	142
	Yüzdelik Oran	0,7%	2,1%	2,8%	17,6%	76,8%	100,0%
ABD	Katılımcı Sayısı	6	19	9	17	69	120
	Yüzdelik Oran	5 %	15,8%	7,5%	14,2%	57,5%	100,0%
Toplam	Katılımcı Sayısı	7	22	13	42	178	262
	Yüzdelik Oran	2,85%	8,95%	5,15%	15,9%	67,15%	100,0%

Birçok bilgi ve verinin depolandığı akıllı telefonların kullanımında Türkiye’de “7-9” ve “10 yıl ve üzeri” cevabını verenlerin toplam yüzdesi %65,5 iken bu oran ABD’de %44,2 ile daha düşük çıkmıştır. ABD sosyal ve teknolojiden açıdan daha gelişmiş bir ülke ve katılımcılarının eğitim profilinin daha yüksek olmasına rağmen akıllı telefon kullanımındaki yılların düşüklüğü dikkat çekicidir (bakınız Tablo 12).

Tablo 12: Katılımcıların Akıllı Telefon Kullanım Süreleri

		1 Yıldan Az	1 – 3 Yıl	4 -6 Yıl	7 – 9 Yıl	10 Yıl +	Toplam
Türkiye	Katılımcı Sayısı	7	8	34	64	29	142
	Yüzdelik Oran	4,9%	5,6%	23,9%	45,1%	20,4%	100,0%
ABD	Katılımcı Sayısı	3	27	37	35	18	120
	Yüzdelik Oran	2,5%	22,5%	30,8%	29,2%	15,0%	100,0%
Toplam	Katılımcı Sayısı	10	35	71	99	47	262
	Yüzdelik Oran	3,75%	14,05%	27,35%	37,15%	17,7%	100,0%

İki ülke kullanıcıları arasında ortaya çıkan bir başka dikkat çekici bulgu ise sosyal medya ve online alışveriş kullanımına yönelik karşımıza çıkmaktadır. Türkiye’deki anket katılımcılarının tamamı %100’ü sosyal medya uygulamalarını kullandığını belirtirken ABD’de bu oran benzer şekilde elde edilmiştir (bakınız Tablo 13).

Tablo 13: Sosyal Medya Kullanımı

		Evet	Hayır	Toplam
Türkiye	Katılımcı Sayısı	142	0	142
	Yüzdelik Oran	100,0%	0,0%	100,0%
ABD	Katılımcı Sayısı	120	0	120
	Yüzdelik Oran	100,0%	0,0%	100,0%
Toplam	Katılımcı Sayısı	262	0	262
	Yüzdelik Oran	100,0%	0,0%	100,0%

Ayrıca anket çalışmasında sosyal medya kullananların gün içerisinde uygulamaları kullanım sıklıkları da değerlendirilmiştir. Elde edilen sonuçlara göre Türkiye’deki katılımcıların %57,7’si sosyal medya uygulamalarını sıklıkla, %12’si çok sık, %23,2’si az ve %7’si çok az kullandığını ifade etmiştir. Araştırmada sosyal medya kullanan ABD’li katılımcıların kullanım sıklıkları ise “çok az”, “az” “sık sık” ve “çok sık” olmak üzere sırasıyla %4,2, %25, %38,3 ve %32,5 şeklinde bulunmuştur (bakınız Tablo 14).

Tablo 14: Gün İçerisinde Sosyal Medya Kullanım Sıklığı

		Çok Az	Az	Sık Sık	Çok Sık	Toplam
Türkiye	Katılımcı Sayısı	10	33	82	17	142
	Yüzdelik Oran	7,0%	23,2%	57,7%	12,0%	100,0%
ABD	Katılımcı Sayısı	5	30	46	39	120
	Yüzdelik Oran	4,2%	25,0%	38,3%	32,5%	100,0%
Toplam	Katılımcı Sayısı	15	63	128	56	262
	Yüzdelik Oran	5,7%	24,0%	48,9%	21,4%	100,0%

Araştırma çerçevesinde sosyal medya uygulamaları arasında yapılan analiz sonuçlarına göre her iki ülkede de en çok kullanılan uygulamanın Facebook olduğu görülmektedir. Diğer taraftan ülkemizde son yıllarda en çok kullanılan uygulama olarak WhatsApp ön plana çıkmaktadır. Bu bağlamda ABD merkezli her iki uygulamanın katılımcılar tarafından kullanım durumları da araştırma çerçevesinde değerlendirilmiş ve Facebook kullanımına ilişkin elde edilen sonuçlara göre Türkiye’deki katılımcılardan %71,8’nin, ABD’li katılımcılardan %79,2’nin Facebook kullandığı görülmüştür (bakınız Tablo 15).

Tablo 15: Facebook Kullanımı

		Hayır	Evet	Toplam
Türkiye	Katılımcı Sayısı	40	102	142
	Yüzdelik Oran	28,2%	71,8%	100,0%
ABD	Katılımcı Sayısı	25	95	120
	Yüzdelik Oran	20,8%	79,2%	100,0%
Toplam	Katılımcı Sayısı	65	197	262
	Yüzdelik Oran	24,8%	75,2%	100,0%

Diğer taraftan Tablo 16’da belirtildiği üzere ABD merkezli diğer bir uygulama olan ve ülkemizde çok sık kullanılan WhatsApp uygulamasını kullanan Türk katılımcıların oranı araştırmada %90,1 olarak elde edilirken bu oran Amerikalı katılımcılar için %48,3 şeklinde gerçekleşmiştir. Araştırma sonuçlarına göre Amerikalı katılımcıların yarısından fazlasının bu uygulamayı kullanmayı tercih etmedikleri görülmüştür.

Tablo 16: WhatsApp Kullanımı

		Hayır	Evet	Toplam
Türkiye	Katılımcı Sayısı	14	128	142
	Yüzdelik Oran	9,9%	90,1%	100,0%
ABD	Katılımcı Sayısı	62	58	120
	Yüzdelik Oran	61,7%	48,3%	100,0%
Toplam	Katılımcı Sayısı	76	186	262
	Yüzdelik Oran	29,0%	71,0%	100,0%

Online alışveriş kullanımı konusunda araştırmada yapılan analiz sonuçlarına göre ABD'deki katılımcıların % 98,3 gibi çok yüksek oranla online alışveriş tercih ettikleri görülürken hedeflenen kitle online alışveriş kullanıcıları olmasına rağmen bu oran Türkiye'deki katılımcılarda % 57,7 ile neredeyse yarı yarıya düşmüş durumdadır (bakınız Tablo 17). Bu durum Türkiye'deki katılımcıların online alışveriş konusunda alışkanlıkları ya da güvenlik sebepleri nedeniyle daha temkinli davrandığı şeklinde yorumlanabilir.

Tablo 17: Online Alışveriş Kullanımı

		Evet	Hayır	Toplam
Türkiye	Katılımcı Sayısı	101	41	142
	Yüzdelik Oran	71,1%	28,9%	100,0%
ABD	Katılımcı Sayısı	118	2	120
	Yüzdelik Oran	98,3%	1,7%	100,0%
Toplam	Katılımcı Sayısı	219	43	262
	Yüzdelik Oran	83,6%	16,4%	100,0%

Online alışverişte tercih edilen uygulama ya da web siteleri ülkeden ülkeye değişiklik göstermektedir. Ancak günümüzde online alışverişin öncüsü kabul edilen dünyaca ünlü Amazon alışveriş sitesi uluslararası anlamda tercih edilen alışveriş sitelerindendir. Son yıllarda ülkemizde ayrıca Çin merkezli online alışveriş sitelerinin de sıklıkla tercih edildiği görülmektedir. Bu bağlamda bu iki alışveriş sitesinin kullanımına yönelik Türkiye'deki ve ABD'deki katılımcılar arasında karşılaştırılması yapılmıştır. Yapılan analizler sonucu Amazon alışveriş sitesinin Türk katılımcılar arasındaki kullanım oranı %12 olarak elde edilirken bu oran ABD'li katılımcılar arasında %98,4 (bakınız Tablo 18) olarak gerçekleşmiştir. Dolayısıyla ABD'li katılımcıların hemen hemen hepsinin Amazon'u alışveriş için tercih ettikleri rahatlıkla söylenebilir.

Tablo 18: Amazon Alışveriş Sitesinin Katılımcılar Tarafından Kullanımı

		Hayır	Evet	Toplam
Türkiye	Katılımcı Sayısı	88	12	100
	Yüzdelik Oran	88,0%	12,0%	100,0%
ABD	Katılımcı Sayısı	2	118	120
	Yüzdelik Oran	1,6%	98,4%	100,0%
Toplam	Katılımcı Sayısı	90	130	220
	Yüzdelik Oran	44,8%	55,2%	100,0%

Amazon alışveriş sitesinin en büyük rakibi olarak görülen Alibaba web sitesinin perakende satış sitesi Aliexpress'in elde edilen sonuçlar doğrultusunda ABD'li katılımcılar arasında %5,8'lik bir değerle çok az tercih edildiği, Türkiye'deki katılımcılar arasında ise tercih oranının %30 (bakınız Tablo 19) olarak ortaya çıktığı görülmüştür. Ayrıca Türkiye'nin Amazonu olarak kabul edilen Hepsiburada.com alışveriş sitesi Tablo 20'de görüldüğü üzere Türkiye'deki katılımcılar arasında diğer alışveriş siteleri ile karşılaştırıldığında %61 ile en yüksek orana sahip alışveriş sitesi olarak karşımıza çıkmaktadır.

Tablo 19: Aliexpress Alışveriş Sitesinin Katılımcılar Tarafından Kullanımı

		Hayır	Evet	Toplam
Türkiye	Katılımcı Sayısı	70	30	100
	Yüzdelik Oran	70,0%	30,0%	100,0%
ABD	Katılımcı Sayısı	113	7	120
	Yüzdelik Oran	94,2%	5,8%	100,0%
Toplam	Katılımcı Sayısı	183	37	220
	Yüzdelik Oran	29,0%	71,0%	100,0%

Tablo 20: Hepsiburada.com Alışveriş Sitesinin Türkiye'deki Katılımcılar Tarafından Kullanımı

		Hayır	Evet	Toplam
Türkiye	Katılımcı Sayısı	39	61	100
	Yüzdelik Oran	39,0%	61,0%	100,0%

Araştırmada kişisel verilerin toplanması, depolanması, kullanılması ile ilgili büyük veri kavramı, bu kavramla ilişkili veri madenciliği, nesnelerin interneti, yapay zeka gibi kavramlar ile kişisel verilerin korunmasına ilişkin kullanıcıların bilgi düzeyleri de ayrıca değerlendirilmiştir. Dört kategoride yapılan değerlendirme sonucu Türkiye'deki katılımcılardan büyük veri konusunda % 36,5'inin "hiç bilgi sahibi" olmadığı, %40,9'unun "az bilgi sahibi" olduğu, ABD'deki katılımcıların ise % 42,5'inin "yeterince bilgi sahibi" ve 19,2'sinin "çok bilgi sahibi" olduğu görülmektedir (bakınız Tablo 21). Bu da ABD'deki katılımcıların büyük veri konusundaki bilgi düzeylerinin daha fazla olduğunu ortaya koymaktadır. Ayrıca bu bulgudan ABD'deki katılımcıların online gizlilik ve güvenlik konusundaki farkındalıklarının daha yüksek olduğu çıkarımını yapmak mümkündür.

Tablo 21: Büyük Veri Konusunda Bilgi Düzeyi

		Hiç	Az	Yeterince	Çok	Toplam
Türkiye	Katılımcı Sayısı	50	56	26	5	137
	Yüzdelik Oran	36,5%	40,9%	19,0%	3,6%	100,0%
ABD	Katılımcı Sayısı	21	25	51	23	120
	Yüzdelik Oran	17,5%	20,8%	42,5%	19,2%	100,0%
Toplam	Katılımcı Sayısı	71	81	77	28	257
	Yüzdelik Oran	27,6%	31,5%	30,0%	10,9%	100,0%

Diğer taraftan büyük veri ile ilgili diğer kavramlar konusunda da ABD’li katılımcıların bilgi düzeylerinin Türkiye’deki katılımcıların bilgi düzeylerinden belirgin şekilde yüksek olduğu sonucu elde edilmiştir. Örneğin Nesnelerin interneti konusunda yeterince bilgi sahibi olan Türk katılımcıların oranı % 10,3 iken bu oran Amerikalı katılımcılarda % 42,5 şeklindedir (bakınız tablo 22).

Tablo 22: Nesnelerin İnterneti Konusunda Bilgi Düzeyi

		Hiç	Az	Yeterince	Çok	Toplam
Türkiye	Katılımcı Sayısı	84	36	14	2	136
	Yüzdelik Oran	61,8%	26,5%	10,3%	1,5%	100,0%
ABD	Katılımcı Sayısı	16	23	51	30	120
	Yüzdelik Oran	13,3%	19,2%	42,5%	25,0%	100,0%
Toplam	Katılımcı Sayısı	100	59	65	32	256
	Yüzdelik Oran	39,1%	23,0%	25,4%	12,5%	100,0%

Diğer önemli bir konu ise her iki ülkeye özgü kişisel verilerin korunması kanunları ile alakalı bilgi düzeyleridir. Türkiye’de kısaca ilgili kanun KVKK şeklinde ABD’de ise FCC Gizlilik Kuralları şeklinde bilinmektedir. KVKK konusunda Türkiye’deki bilgi bir başka anlamda farkındalık düzeyi %31,2 iken ABD’li katılımcılara yönelik yapılan araştırmada bu oran %32,5 ile neredeyse aynı düzeydedir (bakınız Tablo 23).

Tablo 23: Kişisel Verilerin Korunması Kanunu (KVKK) Bilgi Düzeyi

		Hiç	Az	Yeterince	Çok	Toplam
Türkiye	Katılımcı Sayısı	29	62	44	6	141
	Yüzdelik Oran	20,6%	44,0%	31,2%	4,3%	100,0%
ABD	Katılımcı Sayısı	26	39	39	16	120
	Yüzdelik Oran	21,7%	32,5%	32,5%	13,3%	100,0%
Toplam	Katılımcı Sayısı	55	101	83	22	261
	Yüzdelik Oran	21,1%	38,7%	31,8%	8,4%	100,0%

3.4.2. Faktör ve Güvenirlik Analizi

KMO-Barlett Testi bir ölçeği oluşturan ifadelerin faktör analizine uygun olup olmadığını tespit etmek için kullanılan yöntemlerden birisidir (Kaya, 2013). Araştırmada faktör analizinden önce ilk olarak ölçeğimizin geçerliği Kaiser – Meyer – Olkin (KMO) testi Varimax döndürme yöntemi kullanılarak test edilmiştir. KMO testi için 0.50 değerinin alt sınır olması gerektiği ve $KMO \leq 0.50$ için veri kümesinin faktörleştirilemeyeceği belirtilmektedir (Kaya, 2013). Bu doğrultuda yapılan analizler sonucu KMO değeri 0.88 olarak bulunmuş olup bu da örneklem boyutumuzun geçerli ve örneklem büyüklüğünün faktör analizi için yeterli olduğunu ortaya koymuştur. Ayrıca Bartlett testi sonucunun (Chi-Square = 9850,457, $p=0.000<.05$) da anlamlı olduğu Tablo 24’de görülmektedir.

Tablo 24: KMO ve Bartlett Geçerlilik Değerleri

KMO değeri	0,885
Bartlett Test Değeri (Ki-Kare)	9850,457
df	1275
Sig.	0,000

“Faktör analizi, aynı yapıyı ya da niteliği ölçen değişkenleri bir araya getirerek ölçmeyi az sayıda faktör ile açıklamayı amaçlayan bir istatistiksel teknik” olarak tanımlanmaktadır (Yıldırım, 2015). Faktör analizi çerçevesinde ölçeğe etki eden faktörlere son halini vermek amacıyla faktörleştirme yöntemi olarak temel bileşenler analizi; döndürme yöntemi olarak da dik döndürme yöntemlerinden maksimum değişkenlik (varimax) kullanılmıştır. Diğer bir ifadeyle ifadelerin hangi faktörde güçlü korelasyonun olduğunu belirlemek için döndürülmüş bileşenler matrisi (rotated component matrix) oluşturularak ölçek ifadelerinin binişiklik ve faktör yük değerlerinin kabul düzeyini karşılayıp karşılamadığı incelenmiştir.

Yapılan analiz sonucunda OD1, OD2, OD3, OD4, OD5, OD6, OD7 ve OD8 ifadelerinin (maddelerin) birinci faktör; GGE11, GGE12, GGE13, GGE14, GGE15, GGE16, GGE17 ve GGE18 ve GGE19 maddelerinin ikinci faktör; GD5, GD6, GD8, GD9, GD10 ve GD11 maddelerinin üçüncü faktör; KD5, KD8, KD9 ve KD10 maddelerinin dördüncü faktör; RA1, RA2, RA3, RA4, RA5 ve RA6 maddelerinin beşinci faktör; GGF11, GGF12, GGF13, GGF14, GGF15, GGF16, GGF17 ve GGF18 maddelerinin altıncı faktör; GA1, GA2, GA3, GA4 ve GA5 maddelerinin ise yedinci faktör altında toplandığı görülmüştür. GD7, KD6 ve KD7 maddeleri ise birinci faktörün altında toplanmıştır. Faktör yük değerlerinin de; birinci faktör için 0,73 ile 0,86, ikinci faktör için 0,68 ile 0,81, üçüncü faktör için 0,59 ile 0,81, dördüncü faktör için 0,52 ile 0,82, beşinci faktör için 0,70 ile 0,81, altıncı faktör için 0,48 ile 0,80, yedinci faktör için 0,76 ile 0,81 arasında değiştiği görülmektedir (bakınız Tablo 25).

Tablo 25: Döndürülmüş Bileşenler Matrisi

	Bileşenler						
	1	2	3	4	5	6	7
OD7	0,869						
OD5	0,852						
OD8	0,849						
OD3	0,840						
OD4	0,811						
OD1	0,809						
OD2	0,777						
OD6	0,734						
GGE19		0,813					
GGE15		0,789					
GGE14		0,782					
GGE18		0,737					
GGE16		0,723					
GGE13		0,721					
GGE11		0,698					
GGE12		0,696					
GGE17		0,685					
GD8			0,816				
GD9			0,795				
GD6			0,770				
GD10			0,719				
GD11			0,710				
GD12			0,646				
GD5			0,613				
GD7	,472		0,592				
KD4				0,820			
KD8				0,783			
KD10				0,702			
KD5				0,676			
KD9				0,673			
KD6	,453			0,588			
KD7	,436			0,524			
RA6					0,810		
RA5					0,794		
RA1					0,781		
RA3					0,770		
RA2					0,752		
RA4					0,707		
GGF13						0,805	
GGF14						0,772	
GGF12						0,767	
GGF11						0,717	

GGF15						0,591	
GGF18						0,552	
GGF16						0,534	
GGF17						0,483	
GA1							0,810
GA2							0,801
GA4							0,795
GA5							0,783
GA3							0,763

Döndürülmüş bileşenler matrisi analizden sonra üç ifade ölçekten çıkarılarak 48 madde ile son hali verilen ölçeğin alt boyutlarına ve tamamına ilişkin güvenilirlik analizi yapılmıştır (Kaya, 2013). Ölçeğimizi oluşturan “Gizlilik ve Güvenlik Endişesi (GGE), Gizlilik ve Güvenlik Farkındalığı (GGF), Olumsuz Deneyim (OD), Risk Algısı (RA), Güven Algısı (GA), Koruma Davranışı (KD) ve Gizleme Davranışı (GD)” ifadelerine ilişkin Tablo 26’da belirtilen Cronbach-Alpha değerlerine ulaşılmıştır.

Tablo 26: Ölçeğin Geneline ve Kapsadığı Sorulara İlişkin Güvenirlik Değerleri

Değişkenler	İfade Sayısı	Cronbach-alpha Kat Sayıları
Gizlilik ve Güvenlik Endişesi (GGE)	9	0,92
Gizlilik ve Güvenlik Farkındalığı (GGF)	8	0,89
Olumsuz Deneyim (OD)	8	0,96
Risk Algısı (RA)	6	0,90
Güven Algısı (GA)	5	0,90
Koruma Davranışı (KD)	5	0,89
Gizleme Davranışı (GD)	7	0,90
Ölçeğin Geneli	48	0,95

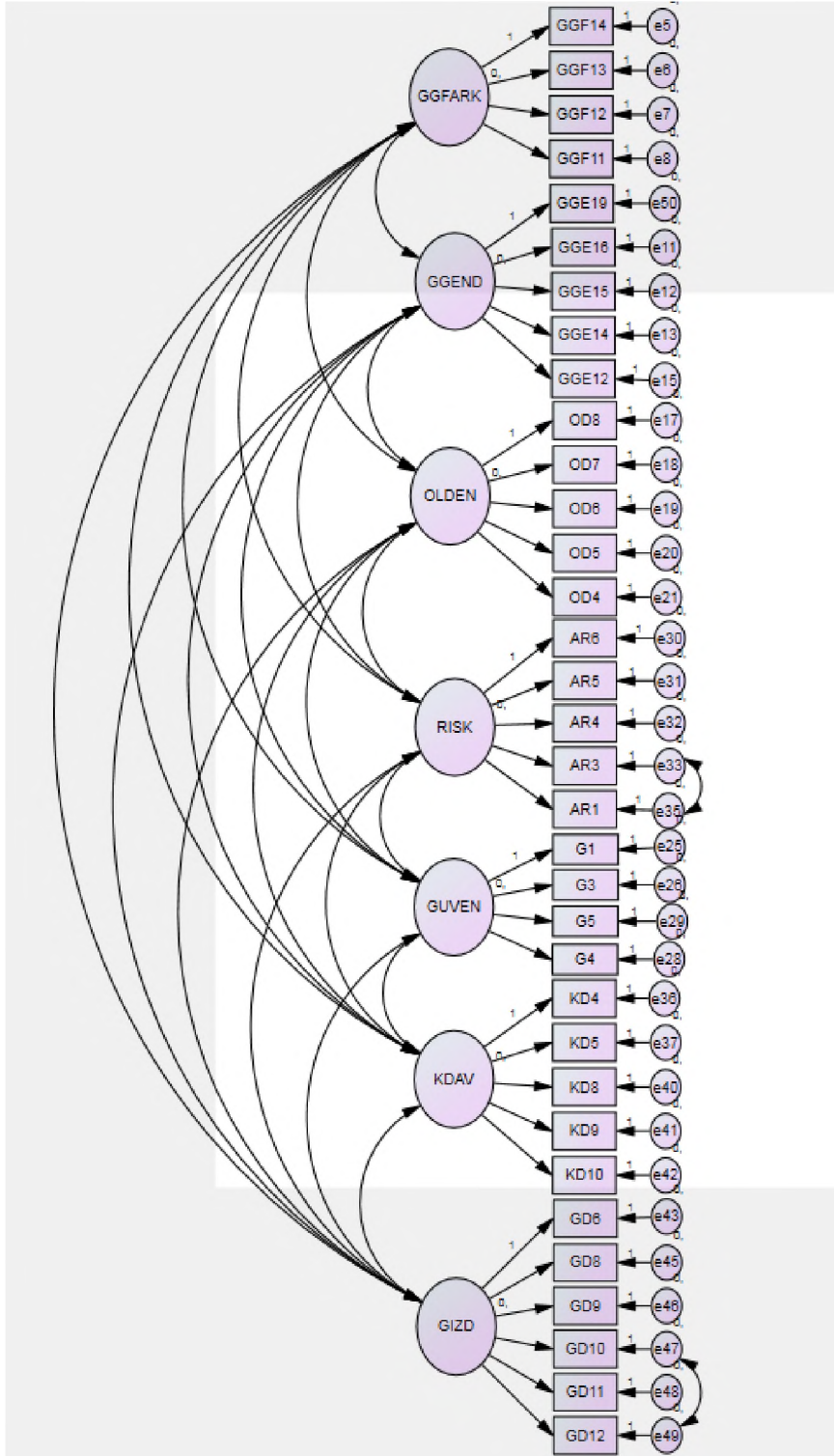
Tablo 26’daki sonuçlara bakıldığında, her bir faktöre ilişkin hesaplanan Cronbach Alpha değerlerinin sırasıyla 0,92, 0,89, 0,96, 0,90, 0,89, 0,90 şeklinde olduğu görülmüştür. Ayrıca ölçeğin genelinde 0,95 Cronbach Alpha değeri elde edilmiştir. Bu değerler 0,70’den büyük olduğu için, ölçeğimizin sosyal bilimler açısından oldukça güvenilir ve kabul edilebilir bir düzeyde olduğu ifade edilebilir.

3.4.3. Yapısal Eşitlik Modeli Analizleri

Yapısal Eşitlik Modeli (YEM) gözlenen değişkenler (observed variable) ve örtük değişkenler (latent variable) arasındaki nedensel ilişkilerin ve korelasyon ilişkilerinin

bir arada bulunduğu modellerin test edilmesi için kullanılan istatistiksel bir teknik olup bağımlılık ilişkilerini tahmin etmek için, varyans, kovaryans analizleri, faktör analizi ve çoklu regresyon gibi analizlerin birleşmesiyle meydana gelen çok değişkenli bir yöntemdir. YEM özellikle psikoloji, pazarlama vb. bilimlerde değişkenler arasındaki ilişkilerin değerlendirilmesinde ve modellerin testinde kullanılmaktadır (Dursun ve Kocagöz, 2010).

Şekil 10: Ölçek Modeli



Araştırma ölçeği daha güvenilir ve geçerli sonuçlar alınabilmesi için YEM yöntemi ile ayrıca analiz edilmiştir. Bu bağlamda Şekil 10'da gösterilen ölçek modeli ile sosyal medya ve online alışveriş kullanıcılarının gizlilik-güvenlik algılarının katılımcıların kullanıcı davranışlarına etkisinin ölçülmesi için araştırmada AMOS Programı aracılığıyla YEM kullanılmıştır. Şekilde belirtilen kısaltmalar sırasıyla GGFARK, gizlilik ve güvenlik farkındalığını; GGEND, gizlilik ve güvenlik endişesini; OLDEN, olumsuz deneyimi; RISK, risk algısını; GUVEN, güven algısını; KDAV, koruma davranışını ve GIZD, gizleme davranışını ifade etmektedir.

Ancak YEM analizinin ilk aşamasında araştırma modelinin uyum ve yapısal geçerliliği faktör analizi ile test edildikten sonra yine model ile uyumsuz bazı ifadeler tespit edilmiştir. Dolayısıyla tutarlılık ve uygunluk bakımından kontrol edilen bu ifadelerden uyumsuz olanlar ölçekten çıkartılarak analiz işlemi tekrar edilmiştir. İlk yapılan analiz sonuçlarına göre elde edilen uyum değerleri Tablo 27'de gösterilmiştir.

Tablo 27: Faktör Değişiklikleri Öncesi Modelin Uyum Değerleri

Uyum indeksi	Değer	Kabul Edilebilir Uyum
Ki-Kare/sd	1,553	1-5
GFI	,908	$0,90 \leq GFI \leq 0,95$
NFI	,808	$0,90 \leq NFI \leq 0,97$
CFI	,917	$0,90 \leq CFI \leq 0,97$
RMSEA	,063	$0,05 \leq RMSEA \leq 0,08$

Uygun olmayan ifadeler elenerek yapılan faktör analizi sonrası ise elde edilen değerlere göre ölçek modeli uyumlu ve ölçek ifadeleri kabul edilebilir hale gelmiştir (bakınız Tablo 28).

Tablo 28: Faktör Değişiklikleri Sonrası Modelin Uyum Değerleri

Uyum indeksi	Değer	Kabul Edilebilir Uyum
Ki-Kare/sd	1,596	1-5
GFI	,916	$0,90 \leq GFI \leq 0,95$
NFI	,817	$0,90 \leq NFI \leq 0,97$
CFI	,925	$0,90 \leq CFI \leq 0,97$
RMSEA	,065	$0,05 \leq RMSEA \leq 0,08$

Modelde yapılan gerekli değişiklikler sağlandıktan sonra ölçek modelinin geçerliliği için yapılan faktör analizi sonucu ortaya çıkan standardize edilmiş regresyon katsayıları ise Tablo 29'da belirtilmiştir. Bu sonuçlara göre standardize edilmiş değerler 0,5'in üzerinde olup en son ortaya çıkan ölçek maddelerinin ilgili faktörlerle güçlü bir ilişki içerisinde olduğu görülmüştür.

Tablo 29: Standardize Edilmiş Regresyon Katsayıları

				Değer					Değer
1	GGF14_1	<---	GGFARK	.925	18	G5_1	<---	GUVEN	.771
2	GGF13_1	<---	GGFARK	.882	19	AR6_1	<---	RISK	.965
3	GGF12_1	<---	GGFARK	.968	20	AR5_1	<---	RISK	.961
4	GGF11_1	<---	GGFARK	.840	21	AR4_1	<---	RISK	.767
5	GGE19_1	<---	GGEND	.792	22	AR3_1	<---	RISK	.770
6	GGE16_1	<---	GGEND	.665	23	AR1_1	<---	RISK	.782
7	GGE15_1	<---	GGEND	.902	24	KD4_1	<---	KDAV	.933
8	GGE14_1	<---	GGEND	.762	25	KD5_1	<---	KDAV	.852
9	GGE12_1	<---	GGEND	.739	26	KD8_1	<---	KDAV	.753
10	OD8_1	<---	OLDEN	.930	27	KD9_1	<---	KDAV	.619
11	OD7_1	<---	OLDEN	.949	28	KD10_1	<---	KDAV	.721
12	OD6_1	<---	OLDEN	.518	29	GD6_1	<---	GIZD	.846
13	OD5_1	<---	OLDEN	.946	30	GD8_1	<---	GIZD	.841
14	OD4_1	<---	OLDEN	.667	31	GD9_1	<---	GIZD	.818
15	G1_1	<---	GUVEN	.730	32	GD10_1	<---	GIZD	.792
16	G3_1	<---	GUVEN	.785	33	GD11_1	<---	GIZD	.760
17	G4_1	<---	GUVEN	.907	34	GD12_1	<---	GIZD	.533

Önceki bölümde anketlerde kullanılan ölçeklerin güvenirlikleri için yapılan analizler sonucu elde edilen değerler 0,70'den büyük olduğu için, ölçeğimizin sosyal bilimler açısından oldukça güvenilir ve kabul edilebilir bir düzeyde olduğu ifade edilmişti. Ancak YEM yöntemi yapılan değişikler sonrası ölçek faktörlerinin güvenirlik analizleri bu sefer varyans katsayıları (AVE) ve bileşik güvenirlik (CR) değerleri üzerinden yapılmıştır. Elde edilen sonuçlara göre her bir faktörün açıkladığı varyansın 0,50'den büyük olduğu görülürken, CR değerlerinin de tüm değişkenler için kritik seviye olan 0,60'ın üzerinde olduğu tespit edilmiştir (bakınız Tablo 30).

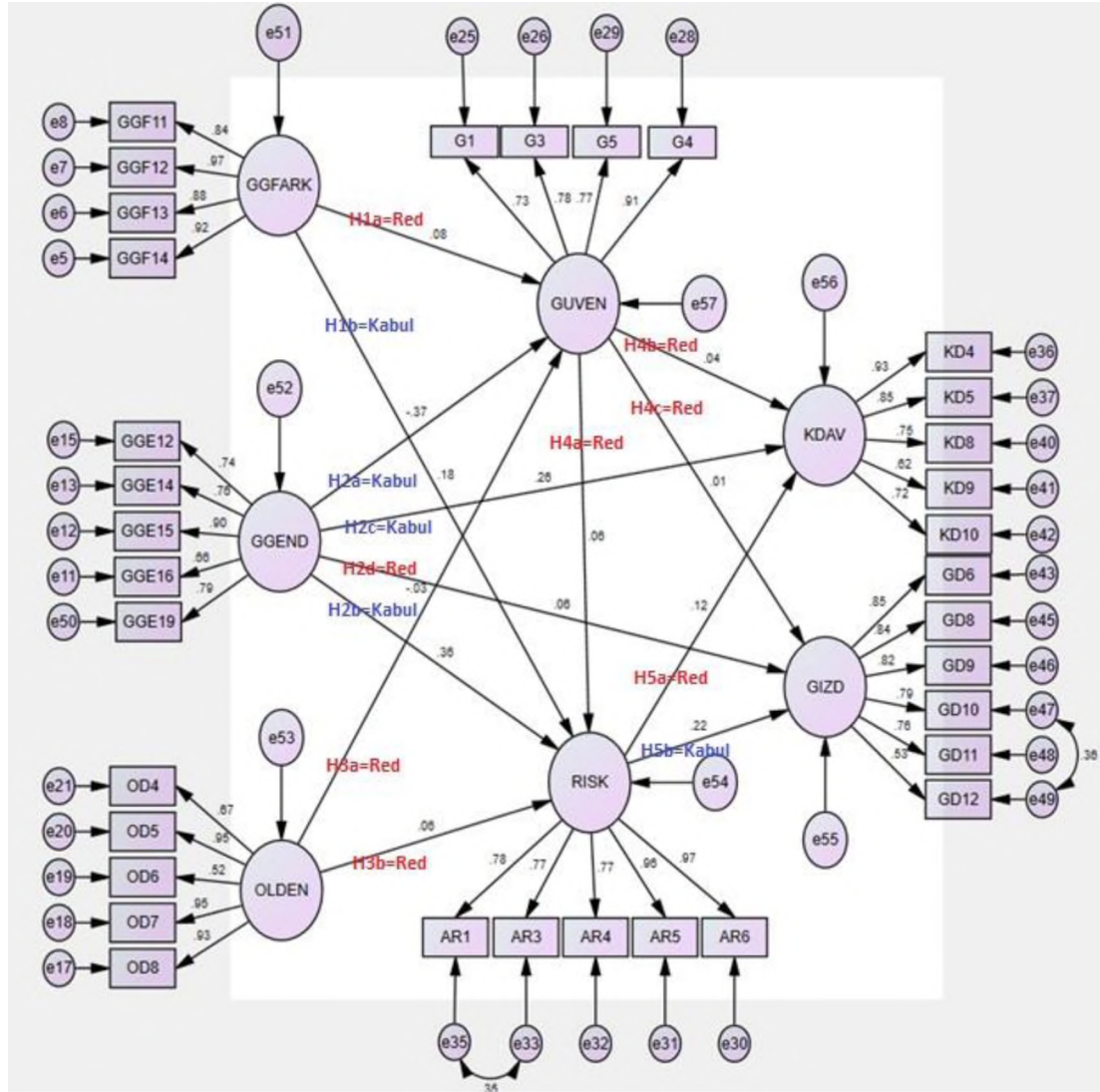
Tablo 30: Faktörlerin AVE ve CR Güvenirlik Değerleri

	CR	AVE	MSV	MaxR (H)	GIZD	GGFRK	GGEND	OLDEN	GUVEN	RISK	KDAV
GIZD	0.897	0.597	0.105	0.913	0.773						
GGFARK	0.890	0.600	0.059	0.973	0.204	0.774					
GGEND	0.882	0.602	0.163	0.979	0.137	0.198	0.776				
OLDEN	0.908	0.675	0.048	0.986	0.050	-0.155	0.218	0.822			
GUVEN	0.858	0.604	0.163	0.987	0.035	0.029	-0.404	-0.125	0.777		
RISK	0.932	0.734	0.143	0.991	0.240	0.236	0.378	0.099	-0.060	0.857	
KDAV	0.876	0.550	0.105	0.992	0.324	0.242	0.296	0.215	-0.069	0.215	0.742

3.4.4. Hipotezlerin Testi

Hipotez testleri için araştırma modeline son hali verilmiştir. Şekil 11’de belirtildiği üzere modelde toplam 7 ölçeğe ait 48 ifadeden 34 ifade (madde) güvenilirlik ve uyum yönlünden gerekli yeterliliğe ulaşmış, böylelikle geliştirilen hipotezler YEM yöntemleri ile test edilmiştir.

Şekil 11: Araştırma Modeli Path Diyagramı



Yapılan YEM analizleri sonucu, araştırma çerçevesinde geliştirilen toplam 13 hipotezden 5’i kabul edilirken 8’i reddedilmiştir (bakınız Şekil 11). YEM’e göre test edilen hipotezlere ilişkin sonuçlar ise Tablo 31’de belirtilmiştir.

Tablo 31: YEM Hipotez Testi Sonuçları

Hipotezler				Katsayı	S.E.	C.R.	P	Sonuç
H1a	GGFARK	--->	GUVEN	.055	.062	.879	.380	Red
H1b	GGFARK	--->	RISK	.162	.072	2.251	.024	Kabul
H2a	GGEND	--->	GUVEN	-.297	.077	-3.839	***	Kabul
H2b	GGEND	--->	RISK	.349	.093	3.765	***	Kabul
H2c	GGEND	--->	KDAV	.394	.156	2.527	.012	Kabul
H2d	GGEND	--->	GIZD	.075	.124	.605	.545	Red
H3a	OLDEN	--->	GUVEN	-.032	.099	-.328	.743	Red
H3b	OLDEN	--->	RISK	.090	.114	.794	.427	Red
H4a	GUVEN	--->	RISK	.077	.112	.692	.489	Red
H4b	GUVEN	--->	KDAV	.077	.179	.433	.665	Red
H4c	GUVEN	--->	GIZD	.012	.144	.083	.934	Red
H5a	RISK	--->	KDAV	.179	.139	1.287	.198	Red
H5b	RISK	--->	GIZD	.260	.113	2.302	.021	Kabul

Elde edilen sonuçlara göre göre:

H_{1a} hipotezi % 5 anlamlılık düzeyinde reddedilmiştir. Diğer bir ifadeyle sosyal medya ve online alışveriş kullanıcılarının gizlilik ve güvenlik farkındalıklarının güven algıları üzerinde olumlu bir etkisi bulunmamaktadır. İki faktör arasındaki ilişkinin istatistiksel açıdan anlamsız olduğu “p” (0,380) değeri ile görülmektedir.

H_{1b} hipotezi % 5 anlamlılık düzeyinde kabul edilmiştir. Diğer bir ifadeyle sosyal medya ve online alışveriş kullanıcılarının gizlilik ve güvenlik farkındalıklarının güven algıları üzerinde olumlu bir etkisi bulunmaktadır. İki faktör arasındaki ilişkinin istatistiksel açıdan anlamlı olduğu “p” (0,024) değeri ile görülmektedir. Ayrıca elde edilen sonuçlar doğrultusunda kullanıcıların gizlilik ve güvenlik farkındalıklarında meydana gelecek bir puanlık artışın güven algılarında 0,16 puanlık bir artışa veya tersi durumda bir puanlık azalışın 0,16 puanlık bir azalışa neden olacağı ifade edilebilir.

H_{2a} hipotezi % 5 anlamlılık düzeyinde kabul edilmiştir. Diğer bir ifadeyle sosyal medya ve online alışveriş kullanıcılarının gizlilik ve güvenlik endişelerinin güven algıları üzerinde olumlu ancak negatif yönlü bir etkisi bulunmaktadır. İki faktör arasındaki ilişkinin istatistiksel açıdan anlamlı olduğu “p” (0,000) değeri ile görülmektedir. Ayrıca elde edilen sonuçlar doğrultusunda kullanıcıların gizlilik ve güvenlik endişelerinde meydana gelecek bir puanlık artışın güven algılarında 0,30 puanlık bir azalışa veya tersi durumda bir puanlık azalışın 0,30 puanlık bir artışa neden olacağı ifade edilebilir.

H_{2b} hipotezi % 5 anlamlılık düzeyinde kabul edilmiştir. Diğer bir ifadeyle sosyal medya ve online alışveriş kullanıcılarının gizlilik ve güvenlik endişelerinin e risk algıları üzerinde olumlu bir etkisi bulunmaktadır. İki faktör arasındaki ilişkinin istatistiksel açıdan anlamlı olduğu “p” (0,000) değeri ile görülmektedir. Ayrıca elde edilen sonuçlar doğrultusunda kullanıcıların gizlilik ve güvenlik endişelerinde

meydana gelecek bir puanlık artışın risk algılarında 0,35 puanlık bir artışa veya tersi durumda bir puanlık azalışın 0,35 puanlık bir azalışa neden olacağı ifade edilebilir.

H_{2c} hipotezi % 5 anlamlılık düzeyinde kabul edilmiştir. Diğer bir ifadeyle sosyal medya ve online alışveriş kullanıcılarının gizlilik ve güvenlik endişelerinin koruma davranışları üzerinde olumlu bir etkisi bulunmaktadır. İki faktör arasındaki ilişkinin istatistiksel açıdan anlamlı olduğu “p” (0,012) değeri ile görülmektedir. Ayrıca elde edilen sonuçlar doğrultusunda kullanıcıların gizlilik ve güvenlik endişelerinde meydana gelecek bir puanlık artışın koruma davranışlarında 0,39 puanlık bir artışa veya tersi durumda bir puanlık azalışın 0,39 puanlık bir azalışa neden olacağı ifade edilebilir.

H_{2d} hipotezi % 5 anlamlılık düzeyinde reddedilmiştir. Diğer bir ifadeyle sosyal medya ve online alışveriş kullanıcılarının gizlilik ve güvenlik endişelerinin gizleme davranışları üzerinde olumlu bir etkisi bulunmamaktadır. İki faktör arasındaki ilişkinin istatistiksel açıdan anlamsız olduğu “p” (0,545) değeri ile görülmektedir.

H_{3a} hipotezi % 5 anlamlılık düzeyinde reddedilmiştir. Diğer bir ifadeyle sosyal medya ve online alışveriş kullanıcılarının olumsuz deneyimlerinin güven algıları üzerinde olumlu bir etkisi bulunmamaktadır. İki faktör arasındaki ilişkinin istatistiksel açıdan anlamsız olduğu “p” (0,743) değeri ile görülmektedir.

H_{3b} hipotezi % 5 anlamlılık düzeyinde reddedilmiştir. Diğer bir ifadeyle sosyal medya ve online alışveriş kullanıcılarının olumsuz deneyimlerinin risk algıları üzerinde olumlu bir etkisi bulunmamaktadır. İki faktör arasındaki ilişkinin istatistiksel açıdan anlamsız olduğu “p” (0,427) değeri ile görülmektedir.

H_{4a} hipotezi % 5 anlamlılık düzeyinde reddedilmiştir. Diğer bir ifadeyle sosyal medya ve online alışveriş kullanıcılarının güven algılarının risk algıları üzerinde olumlu bir etkisi bulunmamaktadır. İki faktör arasındaki ilişkinin istatistiksel açıdan anlamsız olduğu “p” (0,489) değeri ile görülmektedir.

H_{4b} hipotezi % 5 anlamlılık düzeyinde reddedilmiştir. Diğer bir ifadeyle sosyal medya ve online alışveriş kullanıcılarının güven algılarının koruma davranışları üzerinde olumlu bir etkisi bulunmamaktadır. İki faktör arasındaki ilişkinin istatistiksel açıdan anlamsız olduğu “p” (0,665) değeri ile görülmektedir.

H_{4c} hipotezi % 5 anlamlılık düzeyinde reddedilmiştir. Diğer bir ifadeyle sosyal medya ve online alışveriş kullanıcılarının güven algılarının gizleme davranışları üzerinde olumlu bir etkisi bulunmamaktadır. İki faktör arasındaki ilişkinin istatistiksel açıdan anlamsız olduğu “p” (0,934) değeri ile görülmektedir.

H_{5a} hipotezi % 5 anlamlılık düzeyinde reddedilmiştir. Diğer bir ifadeyle sosyal medya ve online alışveriş kullanıcılarının risk algılarının koruma davranışları üzerinde olumlu bir etkisi bulunmamaktadır. İki faktör arasındaki ilişkinin istatistiksel açıdan anlamsız olduğu “p” (0,198) değeri ile görülmektedir.

H_{5b} hipotezi % 5 anlamlılık düzeyinde kabul edilmiştir. Diğer bir ifadeyle sosyal medya ve online alışveriş kullanıcılarının risk algılarının gizleme davranışları

üzerinde olumlu bir etkisi bulunmaktadır. İki faktör arasındaki ilişkinin istatistiksel açıdan anlamlı olduğu “p” (0,021) değeri ile görülmektedir. Ayrıca elde edilen sonuçlar doğrultusunda kullanıcıların gizlilik ve güvenlik farkındalıklarında meydana gelecek bir puanlık artışın güven algılarında 0,26 puanlık bir artışa veya tersi durumda bir puanlık azalışın 0,26 puanlık bir azalışa neden olacağı ifade edilebilir.

3.4.5. Türkiye ve ABD’deki Katılımcıların Sosyal Medya ve Online Alışveriş Kullanımında Gizlilik ve Güvenlik Algılarının Karşılaştırılması

Araştırmaya katılan Türkiye ve ABD’deki sosyal medya ve online alışveriş kullanıcılarının gizlilik ve güvenlik algıları açısından sergiledikleri koruma ve gizleme davranışları ile bunları etki eden faktörlerin iki ülke açısından karşılaştırılması yapılarak aralarında fark olup olmadığı incelenmiştir. Bunun için araştırmada bağımsız örneklem t-testi analizi uygulanmıştır. Bağımsız örneklem t-testi, iki bağımsız (ilişkisiz) örneklem ortalamaları arasındaki farkın anlamlı olup olmadığını test etmek için kullanılır. Bağımsız örneklem için t- testinin varsayımları şunlardır (Balliel ve Sarıkaya, 2015): “1) Bağımlı değişkene ait ölçümler ya da puanlar, aralık ya da oran ölçeğindedir ve karşılaştırılan iki grup ortalaması aynı değişkene aittir. 2) Bağımlı değişkene ait ölçümlerin dağılımı her iki grupta da normaldir. 3) Ortalama puanları karşılaştırılan örneklem ilişkisizdir.” Yapılan t-testi analizi sonuçlarına göre tablo 32’de belirtilen değerlere ulaşılmıştır.

Tablo 32: Sosyal Medya ve Online Alışveriş Kullanımında Türkiye ve ABD’deki Kullanıcıların Faktörlere Göre Farklılık Durumları

Faktörler	Ülkeler	N	Ortalama	Standart Sapma	t	p
Gizlilik-Güvenlik Farkındalığı	Türkiye	134	3,27	0,87	-4,782	0,000
	ABD	120	3,73	0,63		
Gizlilik-Güvenlik Endişesi	Türkiye	136	3,38	1,00	-2,020	0,044
	ABD	120	3,62	0,91		
Olumsuz Deneyim	Türkiye	134	1,43	0,70	-8,394	0,000
	ABD	120	2,50	1,33		
Güven Algısı	Türkiye	134	3,03	1,02	-1,271	0,205
	ABD	120	3,19	1,06		
Risk Algısı	Türkiye	135	3,85	0,91	1,679	0,094
	ABD	120	3,68	0,65		
Koruma Davranışı	Türkiye	135	2,44	1,03	-9,971	0,000
	ABD	120	3,56	0,71		
Gizleme Davranışı	Türkiye	135	2,67	0,86	-5,268	0,000
	ABD	120	3,20	0,88		

T- testi analizi sonuçlarına göre (bakınız Tablo 32) Türkiye’deki ve ABD’deki katılımcıların sosyal medya ve online alışveriş kullanımının gizlilik ve güvenlik farkındalığı, gizlilik ve güvenlik endişesi, olumsuz deneyim, güvenlik algısı, risk algısı, koruma ve gizleme davranışları faktörlerine göre farklılık gösterip göstermediği incelenmiştir. Yapılan incelemede güven ve risk algısı faktörleri (güven algısı t değeri= - 1,271 ve risk algısı t değeri= 1,679) hariç diğer tüm faktörlerde %5

anlamlılık düzeyinde bir farklılık görülmüştür. Güven ve risk algısı faktörlerinin t değeri 1,96'dan düşük olması ile zaten bu faktörlerde testin anlamlı olmadığı ifade edilebilir. Zira elde edilen p değerleri de sırasıyla güven algısı için 0,205, risk algısı içinse 0,094 olarak bulunmuştur.

Bunların dışında faktörlerin ortalama değerlerine bakıldığında ABD'deki sosyal medya ve online alışveriş kullanıcılarının gizlilik ve güvenlik farkındalığının Türkiye'deki kullanıcılardan 3,73 ortalama ile daha fazla olduğu görülmüştür. Aynı şekilde ABD'deki kullanıcıların gizlilik ve güvenlik endişesi de 3,62 ortalama ile Türkiye'deki kullanıcılardan yüksektir. Olumsuz deneyim faktörü açısından iki ülke kullanıcıları değerlendirildiğinde ikisi arasında belirgin bir fark olduğu sonucuna ulaşılmıştır (ABD=2,50; Türkiye=1,43). Bu sonuçlardan ABD'deki kullanıcıların sosyal medya ve online alışveriş kullanımında kimlik hırsızlığı ve online dolandırıcılık gibi olumsuzluklarla daha fazla karşılaştığı ifade edilebilir.

Ayrıca kullanıcıların gizlilik ve güvenlik algılarının sosyal medya ve online alışveriş kullanımındaki davranışlarına nasıl etki ettiği açısından iki ülke karşılaştırıldığında ABD'deki kullanıcıların Türkiye'dekilere kıyasla daha fazla koruma ve gizleme davranışı sergiledikleri görülmüştür (koruma davranışı için ABD=3,56; Türkiye=2,44; gizleme davranışı için ABD=3,20; Türkiye=2,67).

Sonuç olarak Türkiye ve ABD'deki sosyal medya ve online alışveriş kullanıcıları arasında güven ve risk algıları açısından anlamlı bir fark bulunmadığı ancak gizlilik ve güvenlik farkındalığı, gizlilik ve güvenlik endişesi, olumsuz deneyim, koruma ve gizleme davranışları açısından değerlerin ABD'deki kullanıcılar için daha yüksek olduğu sonucuna varılmıştır. Bir başka ifadeyle gizlilik ve güvenlik açısından ABD'deki kullanıcıların farkındalık ve endişe düzeyleri daha yüksek olduğu gibi tecrübe ettikleri olumsuz deneyimler de Türkiye'deki kullanıcılara göre daha fazladır. Bu durumun da ABD'deki kullanıcıların Türkiye'deki kullanıcılara nazaran daha fazla koruma ve gizleme davranışı sergiledikleri şeklinde yorumlanabilir.

SONUÇ VE ÖNERİLER

Özellikle günümüzde akıllı telefon ve mobile internet kullanımı ile internet kullanımının ve online bilgi paylaşımının çok hızlı bir şekilde geliştiğini görmekteyiz. Kişisel bilgi ve verilerimiz bilgi teknolojileri aracılığıyla toplanmakta, depolanmakta, işlenmekte ve farklı amaçlar için özellikle de şirketler ve hükümetlerce izinsiz kullanılmaktadır. Bilgi ve veri bankalarına en fazla kaynak sağlayan online araçlar ise sosyal medya ve e-ticaret (daha çok online alışveriş) uygulamaları olarak karşımıza çıkmaktadır. Araştırma sonuçlarından da görüldüğü üzere hemen hemen herkes sosyal medya ya da online alışveriş uygulamalarından en az birisini kullanmakta ve dolayısıyla kişisel verilerini paylaşmaktadır. Şirketler için sosyal medya uygulamaları çok önemli bir pazarlama ve reklam aracı olarak kullanılmakta ve bu uygulamalar paylaşılan bilgi ve veriler açısından şirketler için büyük bir önem kazanmaktadır. Bu doğrultuda şirketler ya da dolandırıcı ve bilgisayar korsanları gibi taraflar da bu bilgi ve verilerden yararlanmak uğruna kişilerin gizlilik ve güvenliklerini ihlal etmektedir. Bunun sonucunda kişiler istenmeyen olumsuz durumlarla karşılaştıkları gibi bu durum kişilerin gizlilik ve güvenliklerine yönelik endişeleri de artırmaktadır. Diğer taraftan kişisel verilerin korunmasına yönelik hukuksal düzenlemeler araştırmada da görüldüğü üzere ABD gibi gelişmiş demokrasilerde dahi yeterli olmamakta, bu düzenlemeler hükümetler ve şirketlerin çıkarlarına yönelik düzenlenmektedir.

Mevcut çalışmada şirketlerce, hükümetlerce ya da dolandırıcılar gibi üçüncü taraflarca yapılan gizlilik ve güvenlik ihlalleri karşısında internet kullanıcılarına yönelik ortaya çıkan olumsuz deneyimler, kullanıcıların güvenlik ve risk algıları, gizlilik ve güvenlik ile alakalı farkındalık ve endişe seviyeleri ve bunların davranışlarına etkisi Türkiye ve ABD olmak üzere karşılaştırmalı olarak incelenmiştir. Yapılan incelemeler sonucu sosyal medya ve online alışveriş kullanıcılarına yönelik tespit edilen önemli farklılıklardan birisi online alışveriş kullanımında görülmüştür. ABD'deki katılımcıların % 98,3 gibi çok yüksek oranla online alışveriş tercih ettikleri görülürken bu oranın Türkiye'deki katılımcılarda % 57,7 ile neredeyse yarı yarıya olduğu görülmüştür. Bu durum online alışverişin Türkiye'de güvenlik ya da mevcut alışkanlıkların devamı gibi sebeplerle henüz tam olarak kabullenilmediği şeklinde yorumlanabilir. Zira TÜSİAD (2017) tarafından hazırlanan e-ticaret raporunda belirtildiği üzere Türkiye'nin Çin, Hindistan, Güney Afrika gibi ülkelerden internet ve akıllı telefon kullanımında daha önde olduğu görülse de, Türkiye'de e-ticaretin toplam perakendeden aldığı pay göreceli olarak düşük kalmaktadır. 2016 yılı itibarıyla Çin'in % 17,1, İngiltere'nin %14,9, ABD'nin %10,5 seviyelerine ulaştığı perakende e-ticaret sektöründe, Türkiye için bu rakam %3,5 seviyelerindedir (Kantar ve diğerleri, 2017). Bu durum araştırmada elde edilen bu sonucu doğrular niteliktedir. Bununla beraber ABD merkezli Amazon alışveriş sitesinin Türk kullanıcıların %12'si, Çin merkezli Aliexpress alışveriş sitesinin ise Türk kullanıcıların %30'u tarafından alışveriş için tercih edilmesi Türk toplumundaki alışveriş tercihlerinin sadece ulusal alışveriş siteleri ile sınırlı kalmadığını yabancı alışveriş sitelerine de yönelim olduğunu göstermesi açısından önemli bir bulgu olarak karşımıza çıkmaktadır. Türkiye ve ABD'deki kullanıcı profillerini daha iyi anlamak açısından sosyal medya

uygulamalarının da kullanımı mevcut çalışmada karşılaştırılmıştır. Bu bağlamda uygulamalar arasında iki ülke kullanıcıları birlikte değerlendirildiğinde diğer uygulamalar (whatsapp, youtube, instagram vb.) arasında %75,2 ortalama ile en çok kullanılan uygulamanın Facebook olduğu görülmüştür. Facebook’u takip eden uygulama ise %71 ortalama ile WhatsApp olmuştur. Ancak bu durum WhatsApp uygulamasının Türkiye’de çok yaygın kullanımı sonucu ortaya çıkmıştır. Zira ABD’de kullanım oranı %48,3 iken Türkiye’de bu oran %90,1 olarak tespit edilmiştir.

Şüphesiz araştırmanın en önemli bulgularından birisi sosyal medya ve online alışveriş kullanıcılarının büyük veri ve ilintili veri madenciliği, bulut bilişim, nesnelerin interneti gibi teknolojiler ve kavramlar hususunda da bilgi seviyelerine yönelik elde edilen sonuçlardır. Araştırmada elde edilen sonuçlara göre Türkiye’deki katılımcılardan büyük veri konusunda % 36,5’inin “hiç bilgi sahibi” olmadığı, %40,9’unun “az bilgi sahibi” olduğu, ABD’deki katılımcıların ise tersine % 42,5’inin “yeterince bilgi sahibi” ve 19,2’sinin “çok bilgi sahibi” olduğu görülmüştür. Bir başka ifadeyle sonuçlar ABD’deki katılımcıların büyük veri konusundaki bilgi düzeylerinin daha fazla olduğunu ortaya koymaktadır. Benzer sonuçlar veri madenciliği (ABD= %70; Türkiye=%27) ve nesnelerin interneti (ABD=%67,5; Türkiye=%11,8) kavramları için de geçerlidir. Diğer taraftan önemli bir konu ise her iki ülkeye özgü kişisel verilerin korunması kanunları ile alakalı bilgi düzeyleridir. Türkiye’de kısaca ilgili kanun KVKK şeklinde ABD’de ise FCC Gizlilik Kuralları şeklinde bilinmektedir. KVKK konusunda Türkiye’deki bilgi düzeyi %31,2 iken ABD’li katılımcılara yönelik yapılan araştırmada bu oran %32,5 ile neredeyse aynı düzeydedir.

Araştırma çerçevesinde geliştirilen hipotezlerin test sonuçları incelendiğinde toplam 13 hipotezden 5’i kabul edilirken 8’i reddedilmiştir. Elde edilen sonuçlara göre birinci grup hipotezler değerlendirildiğinde sosyal medya ve online alışveriş kullanıcılarının gizlilik ve güvenlik farkındalıklarının risk algıları üzerinde olumlu bir etkisi olduğu, güven algıları üzerinde ise olumlu bir etkisi olmadığı görülmüştür. Bu bağlamda Tsai ve Yeh (2010) tarafından tüketicilerin online alışverişlerindeki gizlilik algıları doğrultusunda yapılan araştırmada da benzer sonuçlar elde edildiği görülmektedir. Elde edilen sonuçlar doğrultusunda gizlilik ve güvenlik endişelerinin risk algıları üzerinde olumlu etkisi olduğu dolayısıyla bunun da satın alma niyetlerini etkilediği sonucuna varılmıştır.

İkinci grup hipotezler için sosyal medya ve online alışveriş kullanıcılarının gizlilik ve güvenlik endişelerinin güven ve risk algıları üzerinde olumlu bir etkisi bulunduğu görülmüştür. Zira e-ticaret konusunda güven, risk, gizlilik ve güvenlik boyutlarının incelendiği başka bir araştırmada gizlilik ve güvenlik endişesinin tüketicilerin online satın alma davranışları üzerinde güçlü bir etkisi olduğu sonucu elde edilmiştir (Roca ve diğerleri, 2009). Aynı grup hipotez içerisinde ise sosyal medya ve online alışveriş kullanıcılarının gizlilik ve güvenlik endişelerinin koruma davranışları üzerinde olumlu bir etkisi olduğu tespit edilirken gizleme davranışları üzerinde olumlu bir etki yaratmadığı görülmüştür. Bu çerçevede yapılan farklı ülkelere (Güney Kore, Hindistan) ait araştırmalarda kullanıcıların gizlilik ve güvenlik endişelerinin hem koruma ve hem de gizleme davranışları üzerinde olumlu bir etkisi olduğu sonucuna varılmıştır (Youn, 2009; Adhikari ve Panda, 2018). Online kullanıcıların farkındalık ve endişe seviyelerinin

koruyucu teknolojileri kullanma ya da koruyucu davranışlar sergileme yönündeki niyetleri olumlu anlamda etkileyebileceği başka araştırmalar ile de ortaya konmuştur. (Dinev ve diğerleri, 2009; Dinev ve Hu, 2007). Yine online gizlilik ve güvenlik endişeleri karşısında kullanıcıların sergiledikleri korunma ve gizleme davranışları üzerine yapılan başka önemli bir araştırmada düzenlenen ankete katılanların %86'sının sosyal medya ya da online alışveriş gibi kanalları kullanırken isimsiz ya da gizli olmayı tercih ettikleri ve online davranışlarını maskeleye ya da izlenmekten kaçınmaya yönelik önlemlerden en az birisini aldıkları belirtilmektedir (Rainie ve diğerleri, 2013).

Üçüncü grup hipotezler değerlendirildiğinde sosyal medya ve online alışveriş kullanıcılarının olumsuz deneyimlerinin güven ve risk algılarına olumlu etki etmediği sonucuna ulaşılmıştır. Bu konuda yapılan diğer araştırma sonuçlarına bakıldığında araştırmamızın aksine olumsuz deneyimlerin online tüketicilerin güven ve risk algıları üzerinde etkili olduğu sonucu elde edilmiştir (Adhikari ve Panda, 2018; Schaik ve diğerleri, 2018).

Dördüncü grup hipotezlerde sosyal medya ve online alışveriş kullanıcılarının güven algılarının ilgili faktörler üzerindeki etkisi incelenmiştir. İnceleme sonuçlarına göre sosyal medya ve online alışveriş kullanıcılarının güven algılarının risk algıları, koruma ve gizleme davranışları üzerinde olumlu bir etkisi olmadığı görülmüştür. Ancak diğer başka araştırmalarda araştırma sonuçlarından farklı sonuçlar elde edildiği görülmektedir. Bu konuda yapılan bir araştırmada özellikle e-ticaret işlemlerinde artan güvenin algılanan riski azalttığı sonucu elde edilmiştir (Van Slyke ve diğerleri, 2006, Malhotra ve diğerleri, 2004; Kimery ve McCord 2002). Ayrıca diğer bazı araştırmalara bakıldığında online kullanıcı ya da tüketicilerin güven ve risk algıları doğrultusunda koruma ve gizleme davranışları sergiledikleri, dolayısıyla güven ve risk algılarının koruma ve gizleme davranışları üzerinde etkili olduğu sonucu elde edilmiştir (Metzger, 2007). Son grup hipotezler incelendiğinde ise sosyal medya ve online alışveriş kullanıcılarının risk algılarının gizleme davranışlarına etki ettiği ancak koruma davranışlarına herhangi bir etkisi bulunmadığı sonucu elde edilmiştir. Buradan kullanıcıların sosyal medya ve online alışveriş kullanımında herhangi bir güvensizlik ya da risk algılamaları durumunda “çerezleri ve tarama geçmişini temizleme, güvenlik ayarlarını en sıkı şekilde uygulama” gibi koruma davranışları sergilemediği ancak kullanıcıların ve tüketicilerin “bilgisayar korsanları ve reklamcılar gibi taraflardan bilgilerini gizlemeye” yönelik davranışlar sergiledikleri şeklinde bir sonuca varılmıştır.

Araştırma sonuçları değerlendirildiğinde özellikle sosyal medya ve online alışveriş kullanıcılarının gizlilik ve güven endişelerinin gizleme davranışları, güven algılarının koruma ve gizleme davranışları, risk algılarının koruma davranışları üzerinde olumlu bir etkisi olmaması, ayrıca kimlik hırsızlığı, taciz ve itibar kaybı gibi olumsuz deneyimlerin sosyal medya ve online alışveriş kullanıcılarının risk ve güven algıları üzerinde etkili olmaması üzerinde durulması ve tekrardan araştırılması gereken bir husus olarak karşımıza çıkmaktadır. Diğer taraftan özellikle sosyal medya ve online alışveriş kullanıcılarının gizlilik ve güvenlik endişesi ile farkındalıklarının Türk ve Amerikalı kullanıcılar arasında coğrafi ve kültürel farklılıklar rağmen Amerikalı kullanıcılarda daha yüksek olsa da yine de birbirine yakın seviyelerde olması ise elde edilen önemli sonuçlar

arasındadır. Zira günümüzde büyüyen ekonomisi ile ABD'nin en büyük rakibi konumunda olan Çin'de yapılan bir araştırmada Çinli tüketicilerin Amerikalı tüketicilere nazaran gizlilik ve güvenlik endişeleri ile farkındalıklarının çok daha düşük olduğu buna karşılık online alışveriş ya da sosyal medya sitelerine yönelik güven algılarının yüksek olması beklenirken daha düşük olduğu sonucuna varılmıştır (Zhang ve diğerleri, 2002).

Araştırmada Türkiye'deki ve ABD'deki katılımcıların sosyal medya ve online alışveriş kullanımının gizlilik ve güvenlik farkındalığı, gizlilik ve güvenlik endişesi, olumsuz deneyim, güvenlik algısı, risk algısı, koruma ve gizleme davranışları faktörlerine göre farklılık gösterip göstermediği incelenmiştir. Yapılan incelemede güven ve risk algısı faktörleri (güven algısı t değeri= - 1,271 ve risk algısı t değeri= 1,679) hariç diğer tüm faktörlerde %5 anlamlılık düzeyinde bir farklılık görülmüştür. Ayrıca ABD'deki sosyal medya ve online alışveriş kullanıcılarının gizlilik ve güvenlik farkındalığının (3,73), gizlilik ve güvenlik endişesinin (3,62) ortalama ile Türkiye'deki kullanıcılardan daha fazla olduğu görülmüştür. Olumsuz deneyim faktörü açısından iki ülke kullanıcıları değerlendirildiğinde ikisi arasında belirgin bir fark olduğu sonucuna ulaşılmıştır (ABD=2,50; Türkiye=1,43). Bu sonuçlardan ABD'deki kullanıcıların sosyal medya ve online alışveriş kullanımında kimlik hırsızlığı ve online dolandırıcılık gibi olumsuzluklarla daha fazla karşılaştığı sonucuna varılmıştır. Bunlara ilave olarak kullanıcıların gizlilik ve güvenlik algılarının sosyal medya ve online alışveriş kullanımındaki davranışlarına nasıl etki ettiği açısından iki ülke karşılaştırıldığında ABD'deki kullanıcıların Türkiye'dekilere kıyasla daha fazla koruma ve gizleme davranışı sergiledikleri görülmüştür (koruma davranışı için ABD=3,56; Türkiye=2,44; gizleme davranışı için ABD=3,20; Türkiye=2,67). Sonuç olarak gizlilik ve güvenlik açısından ABD'deki kullanıcıların farkındalık ve endişe düzeyleri çok yüksek olmamakla birlikte Türk kullanıcılardan daha yüksektir, ayrıca ABD'deki kullanıcıların tecrübe ettikleri olumsuz deneyimler de Türkiye'deki kullanıcılara göre daha fazladır. Bu durum ise ABD'deki kullanıcıların Türkiye'deki kullanıcılara nazaran neden daha fazla koruma ve gizleme davranışı sergilediklerini açıklamaktadır.

Son olarak araştırma çerçevesinde öneri mahiyetinde özellikle Türk kullanıcıların gizlilik ve güvenlik konusundaki farkındalık seviyelerinin daha düşük olduğundan hareketle sosyal medya ve online alışveriş kullanıcılarının kişisel verilerinin korunmasına yönelik daha fazla önlem alması gerektiği belirtilmelidir. Kullanıcılar her paylaşımda ya da işlemde dahi belirli listelere izinler vermek için gizlilik ve güvenlik ayarlarını kontrol etmeli ve bu konudaki gelişmeleri takip etmelidir. Ayrıca KVKK hakkında daha fazla bilgi sahibi olmalı gerekirse gizlilik ve güvenlik ihlalleri karşısında sessiz ve etkisiz kalmayıp gerekli hukuki yollara başvurulmalıdır. Diğer taraftan şirketler ya da hükümet yetkilileri kişisel verilerin korunması konusunda daha fazla hassasiyet göstermeli, gerekli tedbirleri almalı ve daha güçlü yasal düzenlemeleri hayata geçirmelidirler. Zira günümüzde klasik alışveriş ve ticaret anlayışından uzaklaşmakta zaman ve mekanın öneminin ortadan kalktığı sanal alışveriş ve ticaretin yerleştiği bir döneme geçilmektedir. Özellikle bu durum e-ticaret ve online alışverişin merkezi ABD'de belirgin bir şekilde görülmekte ve yaşanmaktadır. Alışveriş ve ticaret anlayışı sadece Amazon, Aliexpress, Hepsiburada gibi alışveriş siteleri ile sınırlı kalmamakta Facebook, Instagram gibi sosyal

medya uygulamaları da alışveriş ve ticaret için kullanılmaktadır. Dolayısıyla sosyal medya uygulamaları ile birlikte e-ticaret ve online alışveriş sitelerinin kullanıcılara sağladığı gizlilik ve güvenlik hizmetleri, kullanıcıların kişisel verilerinin korunması çok daha önemli hale gelmektedir. Bu durum online kullanıcı ve tüketiciler açısından önemli olduğu kadar yeni ticaret ve alışveriş anlayışının yerleşmesi ve şirketlerin verimliliğini ve rekabet gücünü artırması yönünde de oldukça önemlidir. Bu bağlamda şirket ve işletmelerin kullanıcıların gizliliği ve güvenliği ile kişisel verilerini korumak adına gerekli önlemleri alması ve daha fazla hassasiyet göstermesi gerektiğinin bir kez daha altı çizilmelidir.

EKLER

EK-1: Türkiye’de Kullanılan Anket Formu

SOSYAL MEDYA – E-TİCARET KULLANICILARININ GİZLİLİK VE GÜVEN ALGILARININ DEĞERLENDİRİLMESİ: TÜRKİYE – ABD KARŞILAŞTIRMASI

Değerli katılımcılar bu anket formu “Sosyal Medya – E-Ticaret Kullanıcılarının Gizlilik ve Güven Algılarının Değerlendirilmesi: Türkiye – ABD Karşılaştırması” adlı araştırma çerçevesinde geliştirilmiştir.

Lütfen her soruya cevap vermeye çalışınız. Anket formunda isim belirtmeye gerek yoktur. Araştırma sırasında sizden alınan bilgiler araştırmada saklı kalacak ve toplanan veriler yalnızca bilimsel amaçla kullanılacaktır. Zaman ayırarak araştırmamıza katkı sağladığınız için teşekkür ederiz.

Erkan ÇETİNTAŞ

(Yalova Üniversitesi, İşletme Anabilim Dalı, İşletme Bilim Dalı, Yüksek Lisans)

Cinsiyetiniz	☐ Erkek	☐ Kadın	Yaşınız			
Eğitim Durumunuz	☐ İlkokul	☐ Ortaokul	☐ Lise	☐ Üniversite	☐ Yüksek lisans	☐ Doktora
Gelir Durumu (TL)	☐ 1500 - 2000	☐ 2000 - 3000	☐ 3000 - 5000	☐ 5000 - 8000		
Kaç yıldır internet kullanıyorsunuz?	☐ Hiç	☐ 1 yıldan az	☐ 1-3 yıl	☐ 4-6 yıl	☐ 7-9 yıl	☐ 10 yıl +
Kaç yıldır akıllı telefon kullanıyorsunuz?	☐ Hiç	☐ 1 yıldan az	☐ 1-3 yıl	☐ 4-6 yıl	☐ 7-9 yıl	☐ 10 yıl +

Sosyal medya uygulamalarını kullanır mısınız?	☐ Evet	☐ Hayır					
Evetse gün içerisinde sosyal medya kullanma sıklığınız nedir?	☐ Çok az	☐ Az	☐ Sık sık	☐ Çok sık			
En çok kullandığınız sosyal medya uygulaması hangisidir?	☐ Facebook	☐ Facebook Messenger	☐ Whatsapp	☐ Twitter	☐ Youtube	☐ LinkedIn	☐ Pinterest

	☐	Snapchat			
	☐	Diğer (belirtiniz)			
Alışveriş için internet sitelerini tercih eder misiniz?	☐	Evet	☐	Hayır	
Evetse en çok alışveriş yaptığınız internet sitesi hangisidir?	☐	Hepsiburada			
	☐	N11			
	☐	Gittigidiyor			
	☐	Letgo			
	☐	eBay			
	☐	Amazon			
	☐	Aliexpress			
	☐	Diğer (belirtiniz)			
Genel olarak aşağıdaki kavramlar hakkında ne kadar bilgi sahibi olduğunuzu belirtiniz.		Hiç bilgi sahibi değilim	Az bilgi sahibiyim	Yeterince bilgi sahibiyim	Çok bilgi sahibiyim
Büyük veri	☐	☐	☐	☐	
Veri madenciliği	☐	☐	☐	☐	
Bulut Bilişim	☐	☐	☐	☐	
Nesnelerin interneti	☐	☐	☐	☐	
Web 3.0	☐	☐	☐	☐	
Yapay Zeka	☐	☐	☐	☐	
Kişisel Verilerin Korunması Kanunu (KVKK)	☐	☐	☐	☐	
Aşağıdaki ifadelere ne oranda katıldığınızı belirtiniz.	Kesinlikle katılmıyorum	Katılmıyorum	Kararsızım	Katlıyorum	Tamamen katlıyorum
Birçok işletmenin müşterilerinin alışveriş alışkanlıkları, kişisel özellikleri ve kredi geçmişi hakkındaki bilgilere ilişkin kişi profili oluşturduklarını biliyorum.	☐	☐	☐	☐	☐
İşletmelerin ilgimi çekecek ürün ve hizmetlerle ilgili olarak müşteri ve sosyal medya profilime ait bilgileri kullanabileceğini biliyorum.	☐	☐	☐	☐	☐
Sosyal medya ve online alışveriş hesaplarımda özel kampanya ve teklifler için vereceğim ev adresi, meslek, e-mail adresi ve telefon numarası gibi bilgilerin büyük veri bankasında toplandığını biliyorum.	☐	☐	☐	☐	☐
Sosyal medya hesaplarımda paylaştığım bazı kişisel bilgilere işletmeler tarafından bilgim olmadan ulaşılabilirliğini biliyorum.	☐	☐	☐	☐	☐

Aşağıdaki ifadelere ne oranda katıldığınızı belirtiniz.	Kesinlikle katılmıyorum	Katılmıyorum	Kararsızım	Katılıyorum	Tamamen katılıyorum
Online gizlilik ve gizlilik ihlali konularındaki haber ve gelişmeleri takip ederim	☐	☐	☐	☐	☐
Online gizlilik konuları ile şirket ve hükümetlerin sağladığı gizlilik çözümlerini yakından takip ederim	☐	☐	☐	☐	☐
Sosyal medya ve online alışveriş sitelerine yönelik gizlilik sorunları hakkındaki yazıları okurum	☐	☐	☐	☐	☐
Arkadaşlarım ve çevremdekilerle sosyal medya ve online alışveriş sitelerine yönelik güvenlik sorunlarını tartışırım	☐	☐	☐	☐	☐
Aşağıda belirtilen online faaliyetler ile ilgili olarak hizmeti sağlayan şirketlerin toplayabilecekleri bilgiler beni endişelendirir ("1"den "5"e kadar değerlendiriniz).	1 (Hiç)	2	3	4	5 (Çok)
Araştırdığım web sitesi	☐	☐	☐	☐	☐
İnternet kullanırken bulunduğum konum	☐	☐	☐	☐	☐
İndirdiğim içerik ve dosyalar	☐	☐	☐	☐	☐
İnternette dolanan resimlerim	☐	☐	☐	☐	☐
Yaptığım internet taramaları	☐	☐	☐	☐	☐
Maillerimin içeriği	☐	☐	☐	☐	☐
Online konuşmalarımın-yazışmalarımın içeriği	☐	☐	☐	☐	☐
Alışveriş alışkanlıklarım	☐	☐	☐	☐	☐
Video izleme alışkanlıklarım	☐	☐	☐	☐	☐

Sosyal medya ve online alışveriş faaliyetlerim sonucu aşağıda belirtilen durumları ile karşılaştım	1 (Hiçbir zaman)	2	3	4	5 (Her zaman)
Kimlik kartı numaram, kredi kartı ya da banka hesap bilgilerim çalındı	☐	☐	☐	☐	☐
Izın olmadan e-mail, sosyal medyaya ya da online alışveriş hesabım çalındı	☐	☐	☐	☐	☐
Online dolandırıcılık kurbanı oldum ya da param çalındı	☐	☐	☐	☐	☐
Online olarak takip edildim ya da taciz edildim	☐	☐	☐	☐	☐
Online olarak şahsım ya da bir başkası tarafından yapılan bir paylaşım yüzünden bir iş ya da eğitim fırsatını kaybettim	☐	☐	☐	☐	☐
Online olarak yaptığım bir paylaşım yüzünden eşim, sevgilim, aile üyelerim ya da bir arkadaşım ile sorun yaşadım	☐	☐	☐	☐	☐
Online gerçekleşen bir durum yüzünden itibarımı kaybettim	☐	☐	☐	☐	☐
Online olarak gerçekleşen bir durum yüzünden fiziksel şiddete maruz kaldım	☐	☐	☐	☐	☐

Aşağıda ki ifadelere ne oranda katıldığınızı belirtiniz	Kesinlikle katılmıyorum	Katılmıyorum	Kararsızım	Katılıyorum	Tamamen katılıyorum
Sosyal Medya ya da online alışveriş sitelerinde verilen bilgilerin güvenilir olduğunu düşünüyorum	☐	☐	☐	☐	☐
Sosyal medya ve online alışveriş sitelerindeki kişilerin/satıcıların güvenilir olduğunu düşünüyorum	☐	☐	☐	☐	☐
Kullandığım sosyal medya ya da online alışveriş sitelerinin güvenilir olduğunu düşünüyorum	☐	☐	☐	☐	☐
Kişisel bilgilerimin gizliliğinin kullandığım sosyal medya ya da online alışveriş siteleri tarafından korunduğunu düşünüyorum	☐	☐	☐	☐	☐
Kullandığım sosyal medya ya da online alışveriş sitelerinin kişisel bilgilerimi farklı bir amaç için kullanmayacağını düşünüyorum	☐	☐	☐	☐	☐

Aşağıda ki ifadelere ne oranda katıldığınızı belirtiniz.	Kesinlikle katılmıyorum	Katılmıyorum	Kararsızım	Katılıyorum	Tamamen katılıyorum
Sosyal medya ve online alışveriş sitelerinde kişisel ya da ticari bilgilerin paylaşılması risklidir	☐	☐	☐	☐	☐
Sosyal medya ve online alışveriş sitelerinde paylaşılan bilgiler kötü amaçlarla kullanılabilir	☐	☐	☐	☐	☐
Yetkisi olmayan kişiler sosyal medya ve online alışveriş hesaplarım üzerinden kişisel ya da ticari bilgileri ulaşabilirler	☐	☐	☐	☐	☐
Sosyal medya ve online alışveriş sitelerini kullanırsam bilgisayarım ya da telefonuma virüs bulaşabilir	☐	☐	☐	☐	☐
Sosyal medya ve online alışveriş sitelerinde paylaştığım bilgi ya da resimler bilgisayar korsanları tarafından çevremdeki insanlar ya da benden bilgi çalmak amacıyla kullanılabilir	☐	☐	☐	☐	☐
Sosyal medya ve online alışveriş sitelerinde paylaştığım bilgiler bilgisayar korsanları tarafından çevremdeki insanlara online saldırıda bulunmak için kullanılabilir	☐	☐	☐	☐	☐

Kişisel bilgilerimi korumak amacıyla aşağıda belirtilen adımları uygulamam ("1"den "5"e kadar değerlendiriniz).	1 (Hiçbir zaman)	2	3	4	5 (Her zaman)
Çerezleri ve tarama geçmişini temizlerim	☐	☐	☐	☐	☐
Tarayıcıyı ya da çerezleri devre dışı bırakırım	☐	☐	☐	☐	☐
Kasti olarak yanlış ya da yanıltıcı bilgi veririm	☐	☐	☐	☐	☐
İnternette isimsiz olarak gezinmemi sağlayan VPN gibi hizmetleri	☐	☐	☐	☐	☐

kullanırım					
Sosyal medya güvenlik ayarlarını en sıkı şekilde uyguladım	☐	☐	☐	☐	☐
Geçici kullanıcı adı ve e-mail adresi kullanırım	☐	☐	☐	☐	☐
Elektronik cihazlarımda konum-GPS bilgisini devre dışı bırakırım	☐	☐	☐	☐	☐

Aşağıda belirtilen kişi ya da taraflardan online faaliyetlerimi gizlemeyi denerim ("1"den "5"e kadar değerlendiriniz).	1 (Hiçbir zaman)	2	3	4	5 (Her zaman)
İşveren - iş arkadaşları	☐	☐	☐	☐	☐
Eleştiren, taciz eden ya da hedef haline getiren kişiler	☐	☐	☐	☐	☐
Bilgisayar korsanları	☐	☐	☐	☐	☐
Ziyaret edilen web sitesini yöneten şirket ya da kişiler	☐	☐	☐	☐	☐
İndirilen şarkı, film ya da oyun dosyaları için ödeme isteyebilecek şirket ya da kişiler	☐	☐	☐	☐	☐
Geçmişe ait kişiler	☐	☐	☐	☐	☐
Reklamcılar	☐	☐	☐	☐	☐
Hükümetler	☐	☐	☐	☐	☐

THE PRIVACY AND SECURITY PERCEPTIONS OF SOCIAL MEDIA AND E-COMMERCE USERS: TURKEY – USA COMPARISON

Dear participants this survey has been developed in the context of the research entitled “The Privacy and Security Perceptions of Social Media and E-Commerce Users: Turkey – USA Comparison”

Please try to give answer to each question. There is no need to state your name in the survey. The information you provide will remain confidential in the research and data collected in the framework of research will be used for scientific purposes only. Thanks in advance for your contribution to our research.

Erkan ÇETİNTAŞ

(Yalova University, Department of Business Administration, Master Thesis)

Gender	☐ Male ☐ Female Age					
Education Status	☐ Primary ☐ Secondary ☐ High School ☐ University ☐ Master ☐ Doctorate					
Monthly Income (Dolar)	☐ 1000 - 1500 ☐ 1500 - 2000 ☐ 2000 - 3000 ☐ 3000 – 5000 ☐ 5000+					
How long have you been using internet?	☐ Never ☐ Less than a year ☐ 1-3 years ☐ 4-6 years ☐ 7-9 years ☐ 10 years +					
How long have you been using smart phone?	☐ Never ☐ Less than a year ☐ 1-3 years ☐ 4-6 years ☐ 7-9 years ☐ 10 years +					
Do you use social media applications?		☐ Yes ☐ No				
If yes, How often do you use the social media on a daily basis?		☐ Seldom	☐ Sometimes	☐ Often	☐ Always	
Which are the most used social media application/s of yours?			☐ Facebook			
			☐ Messenger			
			☐ Whatsapp			
			☐ Twitter			
			☐ Youtube			
			☐ LinkedIn			
			☐ Pinterest			
			☐ Snapchat			
			☐ Other (please specify)			

Do you prefer websites for shopping?	☐	Evet	☐	Hayır
If yes, Which are the most used online shopping web sites of yours?	☐	Amazon		
	☐	eBay		
	☐	Walmart		
	☐	Newegg		
	☐	Bestbuy		
	☐	Taobao		
	☐	Aliexpress		
	☐	Other (please specify)		
In general, how knowledgeable are you about each of the following technologies?	Not at all knowledgeable	Not very knowledgeable	Somewhat knowledgeable	Very knowledgeable
Big Data	☐	☐	☐	☐
Data Mining	☐	☐	☐	☐
Cloud Computing	☐	☐	☐	☐
Internet of Things	☐	☐	☐	☐
Web 3.0	☐	☐	☐	☐
Artificial Intelligence	☐	☐	☐	☐
FCC Privacy Rule	☐	☐	☐	☐

To what extent do you agree or disagree with the following statements?	Strongly disagree	Disagree	Fairly	agree	Strongly agree
I know that many businesses create profiles about their customers that include information about purchasing habits, personal characteristics and credit history	☐	☐	☐	☐	☐
I know that businesses may use information from your customer profile to inform you of products or services that they think would be of interest to you	☐	☐	☐	☐	☐
I know that in my social media and online shopping accounts when I sign up for a special offers my information such as home address, occupation, email address and phone number will be collected in big data bank	☐	☐	☐	☐	☐
I know that some of the information I share on social networking sites likely might be accessed by businesses without my knowledge	☐	☐	☐	☐	☐

To what extent do you agree or disagree with the following statements?	Strongly disagree	Disagree	Fairly	agree	Strongly agree
I follow the news and developments about the privacy issues and privacy violation	☐	☐	☐	☐	☐
I keep myself updated about privacy issues and the solutions that companies and the government employ to ensure our privacy	☐	☐	☐	☐	☐
I read about the problems of privacy invasion on social media and online shopping websites	☐	☐	☐	☐	☐
I discuss with friends and people around me security issues of social media and online shopping websites	☐	☐	☐	☐	☐
For each of the following online activities, how much are you concerned about that they may be collected by the company running the service? (Please evaluate from 1 to 5)	1 (Not at all)	2	3	4	5 (Extremely)
The websites you browse	☐	☐	☐	☐	☐
Your location when you use the Internet	☐	☐	☐	☐	☐
The content and files that you download	☐	☐	☐	☐	☐
The photos of you circulating on the Internet	☐	☐	☐	☐	☐
The searches you perform	☐	☐	☐	☐	☐
The content of your emails	☐	☐	☐	☐	☐
The content of your online chats or hangouts with others	☐	☐	☐	☐	☐
Your shopping habits	☐	☐	☐	☐	☐
Your viewing habits	☐	☐	☐	☐	☐

Have you ever had any of these experiences as a result of your social media and online shopping activities? (Please evaluate from 1 to 5)	1 (Never)	2	3	4	5 (Always)
Had important personal information stolen such as your Social Security Number, your credit card, or bank account information	☐	☐	☐	☐	☐
Had an online shopping or social networking account of yours compromised or taken over without your permission by someone else	☐	☐	☐	☐	☐
Been the victim of an online scam and lost money	☐	☐	☐	☐	☐
Been stalked or harassed online	☐	☐	☐	☐	☐
Lost a job opportunity or educational opportunity because of something you posted online or someone posted about you online	☐	☐	☐	☐	☐
Experienced trouble in a relationship between you and a family member or a friend because of something you posted online	☐	☐	☐	☐	☐
Had your reputation damaged because of something that happened online	☐	☐	☐	☐	☐
Something happened online that led you into physical danger	☐	☐	☐	☐	☐

To what extent do you agree or disagree with the following statements?	Strongly disagree	Disagree	Fairly	agree	Strongly agree
I think information on social media and online shopping websites are trustworthy.	☐	☐	☐	☐	☐
I think people/sellers on social media and online shopping websites are trustworthy	☐	☐	☐	☐	☐
I think the social media and online shopping websites I use are trustworthy.	☐	☐	☐	☐	☐
I feel that the privacy of my personal information is protected by social media and online shopping websites that I use	☐	☐	☐	☐	☐
I trust that social media and online shopping websites I use will not use my personal information for any other purpose	☐	☐	☐	☐	☐

To what extent do you agree or disagree with the following statements?	Strongly disagree	Disagree	Fairly	agree	Strongly agree
It is risky to post personal or business information on social media and online shopping websites.	☐	☐	☐	☐	☐
Personal or business information posted on social media and online shopping websites may be misused.	☐	☐	☐	☐	☐
Unauthorized people may access my personal or business information through my social media and online shopping websites	☐	☐	☐	☐	☐
My computer may be infected with malware (virus or spyware) if I use social media and online shopping websites	☐	☐	☐	☐	☐
The information or picture I post on social media and online shopping websites may be used by hackers to steal information from me or people around me	☐	☐	☐	☐	☐
The information I post on social media and online shopping websites may be used by hackers to attack people around me	☐	☐	☐	☐	☐

Have you ever done any of the following for the purpose of protecting your personal information? (Please evaluate from 1 to 5)	1 (Never)	2	3	4	5 (Always)
Cleared cookies and browser history	☐	☐	☐	☐	☐
Set your browser to disable or turn off cookies	☐	☐	☐	☐	☐
Purposefully gave incorrect or misleading information about yourself	☐	☐	☐	☐	☐
Used services such as the VPN that allow you to browse the Web anonymously	☐	☐	☐	☐	☐
Tightened social media security settings	☐	☐	☐	☐	☐

Used a temporary username or email address	☐	☐	☐	☐	☐
Disabled GPS functions on your electronic devices	☐	☐	☐	☐	☐

Have you ever tried to keep any of the following people from being able to see your online activities? (Please evaluate from 1 to 5)	1 (Never)	2	3	4	5 (Always)
Employers, supervisors, colleagues	☐	☐	☐	☐	☐
People who might criticize, harass, or target you	☐	☐	☐	☐	☐
Hackers or criminals	☐	☐	☐	☐	☐
The companies or people that operate the websites you visited	☐	☐	☐	☐	☐
Companies or people that might want payment for the files you download such as songs, movies, or games	☐	☐	☐	☐	☐
People from your past	☐	☐	☐	☐	☐
Advertisers	☐	☐	☐	☐	☐
The government	☐	☐	☐	☐	☐

KAYNAKÇA

- Acquisti, A., & Grossklags, J. (2004). Privacy attitudes and privacy behavior. In *Economics of information security* (pp. 165-178). Springer, Boston, MA.
- Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, 347(6221), 509-514.
- Adhikari, K., & Panda, R. K. (2018). Users' Information Privacy Concerns and Privacy Protection Behaviors in Social Networks. *Journal of Global Marketing*, 31(2), 96-110.
- Ahn, J. (2011). Digital divides and social network sites: Which students participate in social media?. *Journal of Educational Computing Research*, 45(2), 147-163.
- Akgün, Ö. E., Topal, M., Eğitim Fakültesi Son Sınıf Öğrencilerinin Bilişim Güvenliği Farkındalıkları: Sakarya Üniversitesi Eğitim Fakültesi Örneği, *Sakarya University Journal of Education*, [S.1.], v. 5, n. 2, p. 98-121, Aug. 2015. ISSN 2146-7455.
- Aldás-Manzano, J., Lassala-Navarré, C., Ruiz-Mafé, C., & Sanz-Blas, S. (2009). The role of consumer innovativeness and perceived risk in online banking usage. *International Journal of Bank Marketing*, 27(1), 53-75.
- Alsanie, S. I. (2015). Social Media (Facebook, Twitter, WhatsApp) Used, and it's Relationship with the University Students Contact with their Families in Saudi Arabia. *Universal Journal of Psychology*, 3(3), 69-72.
- Altman, I. (1977). Privacy regulation: Culturally universal or culturally specific?. *Journal of social issues*, 33(3), 66-84.
- Altunışık, R., (2015), Büyük Veri Fırsatlar Kaynağı mı Yoksa Yeni Sorunlar Yumağı mı?, *YILDIZ Social Science Review*, Volume: 1, Issue: 1, (MAY 2015), pp:45-76.
- Amazon, (2018), https://aws.amazon.com/tr/products/?nc1=h_ls
- Angriawan, A., & Thakur, R. (2008). A parsimonious model of the antecedents and consequence of online trust: An uncertainty perspective. *Journal of Internet Commerce*, 7(1), 74-94.
- Arzu, A. R. I., & ONDER, H. FARKLI VERİ YAPILARINDA KULLANILABİLECEK REGRESYON YÖNTEMLERİ. *Anadolu Tarım Bilimleri Dergisi*, 28(3), 168-174.
- Aslanyürek, M., (2016), İnternet ve Sosyal Medya Kullanıcılarının İnternet Güvenliği ve Çevrimiçi Gizlilik ile İlgili Kanaatleri ve Farkındalıkları, *Maltepe Üniversitesi İletişim Fakültesi Dergisi*, 3(1) bahar/spring: 80-106.
- Badoura, S., The role of social media in the Arab Spring, <https://www.sdu.dk/-/media/files/om.../c.../badoura.pdf>
- Ballhel, B., & Sarıkaya, M. (2015). Seventh grade students' perceptions on webquest-aided learning apporoach in terms of science Webquest destekli işbirlikli öğrenme yaklaşımının yedinci sınıf öğrencilerinde fene yönelik algıları. *Journal of Human Sciences*, 12(1), 1056-1069.

- Bandyopadhyay, S., (2011), Online Privacy Concerns Of Indian Consumers, *International Business & Economics Research Journal*, Volume 10, Number 2.
- BBC, (2018), <https://www.bbc.com/turkce/haberler-dunya-43649116>
- Boritz, J. E., & No, W. G. (2011). E-commerce and privacy: Exploring what we know and opportunities for future discovery. *Journal of Information Systems*, 25(2), 11-45.
- Boyd, D. (2008). Facebook's privacy trainwreck: Exposure, invasion, and social convergence. *Convergence*, 14(1), 13-20.
- Budak, J., Rajh., E., Anic, I.D., (2014), Privacy Concern in Western Balkan Countries: Developing a Typology of Citizens, *The Institute of Economics*, Zagreb.
- Bechtold, David (2014), What is big data? <http://www.oldcolony.us/wp-content/uploads/2014/11/whatisbigdata-DKB-v2.pdf>
- Benson, V., Saridakis, G., & Tennakoon, H. (2015). Information disclosure of social media users: does control over personal information, user awareness and security notices matter?. *Information Technology & People*, 28(3), 426-441.
- Berendt, B., Günther, O., & Spiekermann, S. (2005). Privacy in e-commerce: stated preferences vs. actual behavior. *Communications of the ACM*, 48(4), 101-106.
- Brahim, J. & Martiz, P. (2015). *Big & Fast Data: The Rise Of Insight-Driven Business*. (Industry Report). Capgemini.
- Camp, J., & Connelly, K. (2008). Beyond consent: Privacy in ubiquitous computing (ubicomp). In A., Acquisti, S. Gritzalis, C. Lambrinoudakis, & S. D. C. di Vimercati (Eds.), *Digital privacy: Theory, technologies, and practices* (pp. 327-343). New York, NY: Auerbach Publications.
- Carlos Roca, J., José García, J., & José de la Vega, J. (2009). The importance of perceived trust, security and privacy in online trading systems. *Information Management & Computer Security*, 17(2), 96-113.
- Cases, A. S. (2002). Perceived risk and risk-reduction strategies in Internet shopping. *The International Review of Retail, Distribution and Consumer Research*, 12(4), 375-394.
- Chen, M., Mao, S., Zhang, Y., Leung, V.C.M., (2014), *Big Data: Related Technologies, Challenges and Future Prospects*, Springer.
- Chen, M., Mao, S., & Liu, Y. (2014). Big data: A survey. *Mobile networks and applications*, 19(2), 171-209.
- Chen, Z., & Dubinsky, A. J. (2003). A conceptual model of perceived customer value in e-commerce: A preliminary investigation. *Psychology & Marketing*, 20(4), 323-347.
- Choi, J., & Lee, K. H. (2003). Risk perception and e-shopping: a cross-cultural study. *Journal of Fashion Marketing and Management: An International Journal*, 7(1), 49-64.

- Choi, J., & Geistfeld, L. V. (2004). A cross-cultural investigation of consumer e-shopping adoption. *Journal of Economic Psychology*, 25(6), 821-838.
- Collins, Keith, (2017). Why Net Neutrality Was Repealed and How It Affects You, <https://www.nytimes.com/2017/12/14/technology/net-neutrality-rules.html?action=click&module=RelatedCoverage&pgtype=Article®ion=Footer>
- Connolly, R., & Bannister, F. (2008). Factors influencing Irish consumers' trust in internet shopping. *Management Research News*, 31(5), 339-358.
- Cukul, D., (2012), Social Media as a Tool For Fashion Marketing: Success of Mavi Jeans.
- Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization science*, 10(1), 104-115.
- Dang, A. E., (2013), Location-Based Marketing On Facebook: Connecting With Consumers Through A More Targeted Strategy, https://www.icrossing.com/sites/default/files/insight_pdf_files/Location-Based-Marketing-on-Facebook-iCrossing.pdf
- De Paula, A. M. G. (2010). Security aspects and future trends of social networks. *International Journal of Forensic Computer Science (IJoFCS)*, 1, 60–79.
- Dincelli, E. ve Goel, S., (2017), Can Privacy and Security Be Friends? A Cultural Framework to Differentiate Security and Privacy Behaviors on Online Social Networks, *Proceedings of the 50th Hawaii International Conference on System Sciences*.
- Dinev, T., & Hart, P. (2003, August). PRIVACY CONCERNS AND INTERNET USE--A MODEL OF TRADE-OFF FACTORS. In *Academy of Management Proceedings* (Vol. 2003, No. 1, pp. D1-D6). Briarcliff Manor, NY 10510: Academy of Management.
- Dinev, T. and Hart, P., (2004), Internet privacy concerns and their antecedents – measurement validity and a regression model, *BEHAVIOUR & INFORMATION TECHNOLOGY*, NOVEMBER–DECEMBER 2004, VOL. 23, NO. 6, 413–422.
- Dinev, T. and Hart, P., (2006) An Extended Privacy Calculus Model for E-Commerce Transactions. *Information Systems Research* 17(1):61-80.
- Dinev, T., & Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *Journal of the Association for Information Systems*, 8(7), 23.
- Dunfee, T. W., Smith, N. C., & Ross, W. T. Jr. (1999). Social contracts and marketing ethics. *Journal of Marketing*. 63.
- Dursun, Y., & Kocagöz, E. (2010). Yapısal Eşitlik Modellemesi Ve Regresyon: Karşılaştırmalı Bir Analiz Erciyes Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, (35), 1-17.
- Dusseault, P.L., (2013), Privacy And Social Media In The Age Of Big Data, Report of the Standing Committee on Access to Information, Privacy and Ethics.

- Dwyer, C., Hiltz, S.R., Passerini, K., (2007), Trust and Privacy Concern Within Social Networking Sites: A Comparison of Facebook and MySpace, AMCIS 2007 Proceedings. 339.
- Edosomwan, S., Prakasan, S.K., Kouame, D., Watson, J., Seymour, T., (2011), The Journal of Applied Management and Entrepreneurship, Vol. 16, No.3.
- Ehibudu, I. E., and Sira, T.V., (2017), Influence of Whatsapp and Facebook Social Media Usage on Academic Performance of Secondary School Students in Port Harcourt Local Government Area, Rivers State, Nigeria. IOSR Journal Of Humanities And Social Science (IOSR-JHSS) Volume 22, Issue 12, Ver. 5, p-ISSN: 2279-0845.
- EMC Privacy Index, (2014), Global & In-Depth Country Results. <https://www.emc.com/collateral/brochure/privacy-index-global-in-depth-results.pdf>
- Faqih, K. M. (2013). Exploring the influence of perceived risk and internet self-efficacy on consumer online shopping intentions: Perspective of technology acceptance model. International Management Review, 9(1), 67-77.
- FTC, (2010), <https://www.ftc.gov/news-events/press-releases/2010/12/ftc-staff-issues-privacy-report-offers-framework-consumers>
- FTC, (2012), <https://www.ftc.gov/news-events/press-releases/2012/03/ftc-issues-final-commission-report-protecting-consumer-privacy>
- FCC, (2010), <https://www.fcc.gov/general/privacy-act-information#block-menu-block-4>
- Forsythe, S., Liu, C., Shannon, D., & Gardner, L. C. (2006). Development of a scale to measure the perceived benefits and risks of online shopping. Journal of interactive marketing, 20(2), 55-75.
- Freivogel, W. H. (2015). The right to be let alone. In W. A. Babcock & W. H. Freivogel (Eds.), Guide to key issues in mass media ethics and law (pp. 303-318). Thousand Oak, CA: SAGE Publications.
- Garbarino, E., & Strahilevitz, M. (2004). Gender differences in the perceived risk of buying online and the effects of receiving a site recommendation. Journal of Business Research, 57(7), 768-775.
- Gantz, J. and Reinsel D., (2012), THE DIGITAL UNIVERSE IN 2020: Big Data, Bigger Digital Shadows, and Biggest Growth in the Far East, IDC iView.
- Ghazinour, K., Razavi, A. H., & Barker, K. (2014). A model for privacy compromisation value. Procedia Computer Science, 37, 143-152.
- Gökgül, M. (2014). Türkiye'de Elektronik Ticaret ve İşletmelere, Tüketicilere Sağladığı Avantajlar, Dezavantajlar (The Electronic Commerce and Business, The advantages to consumers, Disadvantages in Turkey,) Yüksek Lisans Tezi. İstanbul: TC İstanbul Kültür Üniversitesi SBE, 26.
- Gupta, P. And Dubey, A., (2016), E-Commerce- Study of Privacy, Trust and Security from Consumer's Perspective, IJCSMC, Vol. 5, Issue. 6.
- Granryd, M. (2016). You're Probably Reading This On Your Mobile, World Economic Forum. <https://www.weforum.org/agenda/2016/01/what-role-will-mobile-play-in-future-of-internet>

- Greengard, S. (2015). The Internet Of Things. MIT Press.
- Gross, R., & Acquisti, A. (2005). Information revelation and privacy in online social networks. In Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society: WPES 2005 (pp. 71–80). New York, NY: ACM.
- Ha, H. Y. (2004). Factors influencing consumer perceptions of brand trust online. Journal of Product & Brand Management, 13(5), 329-342.
- Habertürk, (2018) <http://www.haberturk.com/facebook-kullanilarini-sosyoekonomik-gruplara-ayiracak-algoritmasini-patentledi-1856241-ekonomi>
- Harper, G. W. (2010). U.S. Patent No. 7,676,436. Washington, DC: U.S. Patent and Trademark Office.
- Hassan, A. M., Kunz, M. B., Pearson, A. W., & Mohamed, F. A. (2006). Conceptualization and measurement of perceived risk in online shopping. Marketing Management Journal, 16(1).
- Healey, D., Candon, G., Koeppl A., Bhavnani, R., (2014), Data Privacy in the EU and the US, FTI Consulting.
- Hoadley, C. M., Xu, H., Lee, J. J., & Rosson, M. B. (2010). Privacy as information access and illusory control: The case of the Facebook News Feed privacy outcry. Electronic commerce research and applications, 9(1), 50-60.
- Hogben, G. (2007). Security issues and recommendations for online social networks. (ENISA Position Paper No. 1). Heraklion, Crete, Greece: European Network and Information Security Agency.
- Hong, W., Thong, J. Y. L., & Tam, K. Y. (2005). The Effects of Information Format and Shopping Task on Consumers' Online Shopping Behavior: A Cognitive Fit Perspective, Journal of Management Information Systems 21 (3) 149-184.
- Howell, S. (2018). Broadband Privacy. Santa Clara L. Rev., 58, 59.
- Huber, M., Mulazzani, M., Schrittwieser, S., & Weippl, E. (2010), Cheap and automated socio-technical attacks based on social networking sites. In Proceedings of the 3rd ACM Workshop on Artificial Intelligence and Security: AISec, (pp. 61 64). New York, NY: ACM.
- Hsu, M H., Chuang, L W. & Hsu, C S. (2014). Understanding Online shopping intention: the roles of four types of trust and their antecedents. Internet Research. 24(3):332-352.
- İnternet Gazetesi (2018), <https://www.internetingazetesi.com/amazonun-kurucusu-jeff-bezosun-projeleri/>
- KANTARCI, Ö., ÖZALP, M., SEZGİNSOY, C., ÖZAŞKINLI, O., & CAVLAK, C. (2017). Dijitalleşen dünyada ekonominin itici gücü: E-ticaret. TUSIAD Yayınları, İstanbul.
- Kara, Y., & Coşkun, A. (2012). Sosyal ağların pazarlama aracı olarak kullanımı: Türkiye'deki hazır giyim firmaları örneği. Afyon Kocatepe Üniversitesi İİBF Dergisi, C: XIV, S: II, 73-90.
- Kaya, M. F. (2013). Sürdürülebilir kalkınmaya yönelik tutum ölçeği geliştirme çalışması.

- Keith, M. J., Babb, J., Furner, C., Abdullat, A., & Lowry, P. B. (2016). Limited information and quick decisions: consumer privacy calculus for mobile applications.
- Kessinger K. and Berger, A., (2014), ISACA IT Risk/Reward Barometer - US Consumer Results.
- Kimery, K. M., & McCord, M. (2002, January). Third-party assurances: the road to trust in online retailing. In System Sciences, 2002. HICSS. Proceedings of the 35th Annual Hawaii International Conference on (pp. 10-pp). IEEE.
- Kizza, J. M., (2014), Computer network security and cyber ethics (4th ed.), Jeferson, North Carolina : McFarland & Company, Inc., Publishers.
- Kugler, L. (2015). Online privacy: Regional differences. Communications of the ACM, 58(2), 18-20.
- Kuhlmeier, D., & Knight, G. (2005). Antecedents to internet-based purchasing: a multinational study. International Marketing Review, 22(4), 460-473.
- Kumaraguru, P. and Cranor, L.F., (2005), Privacy Indexes: A Survey of Westin's Studies, Institute for Software Research International, Carnegie Mellon University, Pittsburgh.
- Kshetri, N., (2014), Big data's impact on privacy, security and consumer welfare, Telecommunications Policy 38, 1134–1145.
- KVKK, (2017), <https://www.kvkk.gov.tr/Icerik/2074/Misyon---Vizyon>
- Lallmahamood, M. (2007). An Examination of Individual's Perceived Security and Privacy of the Internet in Malaysia and the Influence of this on their Intention to Use E-commerce: Using an Extension of the Technology Acceptance Model. Journal of Internet Banking and Commerce, 12(3), 1.
- Lane, J., Stodden, V., Bender, S., and Nissenbaum, H., (2014), Privacy, Big Data, and the Public Good: Frameworks for Engagement, Cambridge University Press.
- Lang, S., Tinder, L., Zimmerman, J., & Harrison, J. S. (2012). Amazon. com: Offering Everything from A to Z.
- Langheinrich, M., & Karjoth, G. (2010). Social networking and the risk to companies and institutions. Information Security Technical Report, 15(2), 51–56.
- Laudon, K. C. (1986). Data quality and due process in large interorganizational record systems. Communications of the ACM, 29(1), 4-11.
- Lenhart, A., & Madden, M. (2007). Social networking websites and teens: An overview.
- Lewis, K., Kaufman, J., & Christakis, N. (2008). The taste for privacy: An analysis of college student privacy settings in an online social network. Journal of Computer-Mediated Communication, 14(1), 79-100.
- Liebermann, Y., & Stashevsky, S. (2002). Perceived risks as barriers to Internet and e-commerce usage. Qualitative Market Research: An International Journal, 5(4), 291-300.
- Lin, J., Amini, S., Hong, J. I., Sadeh, N., Lindqvist, J., & Zhang, J. (2012, September). Expectation and purpose: understanding users' mental models of

- mobile app privacy through crowdsourcing. In Proceedings of the 2012 ACM Conference on Ubiquitous Computing (pp. 501-510). ACM.
- Ling, R. S. (2008). *New tech, new ties*. Cambridge, MA: MIT press.
- Liu, X., Burns, A. C., & Hou, Y. (2013). Comparing online and in-store shopping behavior towards luxury goods. *International Journal of Retail & Distribution Management*, 41(11/12), 885-900.
- Madden, M., (2014), Public Perceptions of Privacy and Security in the Post-Snowden Era, Pew Research Center. <http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/>
- Madden, M., Gilman, M., Levy, K. and Marwick, A., (2017), Privacy, Poverty, and Big Data: A Matrix of Vulnerabilities for Poor Americans, 95 Wash. U. L. Rev. 053.
- Maleki, M., & Akbarzadeh Pasha, M. (2012). Ethical Challenges: Customer's Rights. *SCMS Journal of Indian Management*, 9(4).
- Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information systems research*, 15(4), 336-355.
- Mandić, M. (2009). Privacy And Security In E-Commerce. *Trziste/Market*, 21(2).
- Manyika, J., Chui, M., Brown, B., Bughin, J., Dobbs R., Roxburg, C., Byers, A.H., (2011), *Big Data: The Next Frontier For Innovation, Competition and Productivity*, McKinsey Global Institute.
- Mayfield, A. (2008). What is Social Media?.iCrossing eBook. http://www.ijbssnet.com/journals/Vol_3_No_22_Special_Issue_November_2012/16.pdf
- McCole, P., Ramsey, E., & Williams, J. (2010). Trust considerations on attitudes towards online purchasing: The moderating effect of privacy and security concerns. *Journal of Business Research*, 63(9-10), 1018-1024.
- Meinert, D. B., Peterson, D. K., Criswell, J. R., & Crossland, M. D. (2006). Privacy policystatements and consumer willingness to provide personal information. *Journal of Electronic Commerce in Organizations (JECO)*, 4(1), 1-17.
- Mefolere, K. (2016). WhatsApp and Information Sharing: Prospect and Challenges. *International Journal of Social Science and Humanities Research*, 4(1), 615-625.
- Merriam Webster, (2018), <https://www.merriamwebster.com/dictionary/social%20media>
- Metzger, M. J. (2007). Communication privacy management in electronic commerce. *Journal of Computer-Mediated Communication*, 12(2), 335-361.
- Michael, K., & Miller, K. W. (2013). Big data: New opportunities and new challenges [guest editors' introduction]. *Computer*, 46(6), 22-24.
- Milne, G. R., & Culnan, M. J. (2004). Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *Journal of interactive marketing*, 18(3), 15-29.

- Milord, Joseph, (2017). What Is Net Neutrality? Trump's FCC Is Expected To Repeal Internet Regulations. <https://www.elitedaily.com/p/what-is-net-neutrality-trumps-fcc-is-expected-to-repeal-internet-regulations-6338760>
- Miyazaki, A. D., & Fernandez, A. (2001). Consumer perceptions of privacy and security risks for online shopping. *Journal of Consumer affairs*, 35(1), 27-44.
- Nafus, D., & Tracey, K. (2002). 13 Mobile phone consumption and concepts of personhood. *Perpetual contact*, 206.
- Norberg, P. A., Home, D. R., & Home, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, 41(1), 100-126.
- Nummala, M. (2015). Successful social media marketing on Instagram. *Case@minoshoes*.
- NTV, (2017), <https://www.ntv.com.tr/galeri/teknoloji/twitterda-yeni-donem-basladi-karakter-savisi-artti.tJL9EozDfEOJNv-G3s8Krw>
- Okesola, O., Onashoga, A. & Ogunbanwo, A., (2016), 'An investigation into users' information security awareness on social networks in south western Nigeria', *South African Journal of Information Management* 18(1), a721.
- Ortiz, J., Chih, W.H., Tsai, F.T., (2018) *Computers in Human Behavior* 80 143 – 157.
- Ölçeği, F. B. Ö. K. (2015). Geçerlilik ve Güvenirlilik Çalışması, *Fen Bilimleri*, 3(1).
- ÖZBAY, Ö., (2009), Çapraz tablo analizi nasıl yapılır?: pratik bir açıklama. *HÜTAD*, (9).
- Pappas, N. (2016). Marketing strategies, perceived risks, and consumer trust in online buying behaviour. *Journal of Retailing and Consumer Services*, 29, 92-103.
- Pastalan, L. A. (1970). Privacy as a behavioral concept. *Social Science*, 93-97.
- Petronio, S. (2012). *Boundaries of privacy: Dialectics of disclosure*. Suny Press.
- Phelps, J., Nowak, G., and Ferrel, E., (2000), Privacy Concerns and Consumer Willingness to Provide Personal Information, *Journal of Public Policy & Marketing*, Vol. 19, No. 1, Privacy and Ethical Issues in Database/Interactive Marketing and Public Policy, pp. 27-41.
- Pi, S. M., Liao, H. L., & Chen, H. M. (2012). Factors that affect consumers' trust and continuous adoption of online financial services. *International Journal of Business and Management*, 7(9), 108.
- Pingitore, G., Meyers, J., Clancy, M., & Cavallaro, K. (2013). Consumer concerns about data privacy rising: What can business do. *JD Power report*.
- Raine, L., & Madden, M. (2015). *American Views On Government Surveillance Programs*. Pew Research Center: Internet, Science & Tech, 16.
- Rainie, L., Kiesler, S., Kang, R. and Madden, M., (2013), *Anonymity, Privacy, and Security Online*, Pew Research Center's Internet & American Life Project, Washington. <http://pewinternet.org/Reports/2013/Anonymity-online.aspx>

- Ramirez, E., Brill, J., Ohlhausen, M.K., McSweeney, T., (2016), Big Data: A Tool for Inclusion or Exclusion?, FTC Report.
- Rippetoe, P. A. and Rogers, R.W., (1987), Effects of Components of Protection-Motivation Theory on Adaptive and Maladaptive Coping With a Health Threat, *Journal of Personality and Social Psychology*, Vol. 52, No. 3, 596-604
- Samadi, M., & Yaghoob-Nejadi, A. (2009). A survey of the effect of consumers' perceived risk on purchase intention in e-shopping. *Business Intelligence Journal*, 2(2), 261-275.
- San Martín, S., & Camarero, C. (2009). How perceived risk affects online buying. *Online Information Review*, 33(4), 629-654.
- Schlosser, A. E., White, T. B., & Lloyd, S. M. (2006). Converting web site visitors into buyers: how web site investment increases consumer trusting beliefs and online purchase intentions. *Journal of Marketing*, 70(2), 133-148.
- Shalhoub, Z. (2006). Trust, privacy, and security in electronic business: the case of the GCC countries. *Information Management & Computer Security*, 14(3), 270-283.
- Shklovski, I., Mainwaring, S. D., Skúladóttir, H. H., & Borgthorsson, H. (2014, April). Leakiness and creepiness in app space: Perceptions of privacy and mobile app use. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 2347-2356). ACM.
- Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: measuring individuals' concerns about organizational practices. *MIS quarterly*, 167-196.
- Sultan, M. U., & Uddin, M. (2011). Consumers' Attitude towards Online Shopping: Factors influencing Gotland consumers to shop online.
- Statista, (2018), <https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/>
- Statista, (2018), <https://www.statista.com/statistics/805656/number-youtube-viewers-worldwide/>
- Statista, (2018), <https://www.statista.com/statistics/253577/number-of-monthly-active-instagram-users/>
- Statista, (2018), <https://www.statista.com/statistics/260819/number-of-monthly-active-whatsapp-users/>
- Statista, (2018), <https://www.statista.com/study/10653/e-commerce-worldwide-statista-dossier/>
- Statista, (2018), <https://www.statista.com/statistics/264875/brand-value-of-the-25-most-valuable-brands/>
- Stern, T., (2011), User Behavior on Online Social Networks and the Internet: A Protection Motivation Perspective, A dissertation submitted to the Graduate Faculty in Business in partial fulfillment of the requirements for the degree of Doctor of Philosophy, The City University of New York.
- Strater, K., & Lipford, H. R. (2008, September). Strategies and struggles with privacy in an online social networking community. In *Proceedings of the 22nd British HCI Group Annual Conference on People and Computers:*

- Culture, Creativity, Interaction-Volume 1 (pp. 111-119). British Computer Society.
- Stutzman, F. (2006). An evaluation of identity-sharing behavior in social network communities. *Journal of the International Digital Media and Arts Association*, 3(1), 10-18.
- Taecharungroj, V. (2017). Starbucks' marketing communications strategy on Twitter. *Journal of Marketing Communications*, 23(6), 552-571.
- Tan, Q., Pivot, F., (2015), Big Data Privacy: Changing Perception of Privacy, IEEE International Conference on Smart City, Canada.
- Tanner, B. K., Warner, G., Stern, H., & Olechowski, S. (2010). Koobface: The evolution of the social botnet. In *Proceedings of the 2010 eCrime Researchers Summit* (pp.1-10). Piscataway, NJ: IEEE.
- Thomas, K., & Nicol, D. M. (2010). The Koobface botnet and the rise of social malware. In *Proceedings of the 5th International Conference on Malicious and Unwanted Software: MALWARE 2010* (pp. 63-70). Piscataway, NJ: IEEE.
- Tomlinson, A., Yau, P.-W., & MacDonald, J. A. (2010). Privacy threats in a mobile enterprise social network. *Information Security Technical Report*, 15(2), 57-66.
- Trepte, S. and Reinecke, L., (2011), *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web*, Springer.
- Trocchia, P. J., & Ainscough, T. L. (2012). Consumer attitudes toward RFID tracking in the retail environment. *The Review of Business Information Systems (Online)*, 16(2), 67.
- Tsai, Y. C., & Yeh, J. C. (2010). Perceived risk of information security and privacy in online shopping: A study of environmentally sustainable products. *African Journal of Business Management*, 4(18), 4057-4066.
- Tuten, T. L., & Solomon, M. R. (2014). *Social media marketing*. Harlow, Essex: Pearson.
- TÜBİSAD, (2017). Deloitte, ETİD, http://www.tubisad.org.tr/tr/images/pdf/tubisad_2018_e-ticaret_sunum_tr.pdf
- Ueltschy, L. C., Krampf, R. F., & Yannopoulos, P. (2004). A cross-national study of perceived consumer risk towards online (Internet) purchasing. *Multinational Business Review*, 12(2), 59-82.
- Ünver, H.A., Kim, G., (2016), Türkiye'de Veri Gizliliği ve Gözetimi: Kişisel Verilerin Korunması Kanunu Tasarısının Değerlendirmesi, EDAM Siber Politika Kağıtları Serisi 2.
- Qualman, Erik, (2010), *Socialnomics: How Social Media Transforms The Way We Live and Do Business*, John Wiley & Sons, Inc., New Jersey.
- Waldo, J., Herbert S. Lin, and Lynette I. Millett, (2007), *Engaging Privacy and Information Technology in a Digital Age*, National Academies Press, Washington.

- Wani, S. N., & Malik, S. (2013). A Comparative Study of Online Shopping Behaviour: Effects of Perceived Risks and Benefits. *International Journal of Marketing & Business Communication*, 2(4).
- Westin, A. F. (2003). Social and political dimensions of privacy. *Journal of social issues*, 59(2), 431-453.
- We Are Social Digital Yearbook, (2017), We Are Social and Hootsuite. <https://wearesocial.com/special-reports/digital-in-2017-global-overview>
- Webrazzi, (2017) <https://webrazzi.com/2017/11/27/1-gunde-604-bin-defa-indirilen-hepsiburada-252-milyon-tllik-satis-gerceklestirdi/>
- Wheless, L. R., & Grotz, J. (1976). Conceptualization and measurement of reported self-disclosure. *Human communication research*, 2(4), 338-346.
- Xu, H. (2007). The effects of self-construal and perceived control on privacy concerns. *ICIS 2007 proceedings*, 125.
- Xu, H., Dinev, T., Smith, H.J., Hart, P., (2008), Examining the Formation of Individual's Privacy Concerns: Toward an Integrative View, *ICIS 2008 Proceedings*. Paper 6.
- Xu, H., Teo, H. H., Tan, B. C., & Agarwal, R. (2012). Research note—effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: a study of location-based services. *Information Systems Research*, 23(4), 1342-1363.
- Van Schaik, P., Jansen, J., Onibokun, J., Camp, J., & Kusev, P. (2018). Security and privacy in online social networking: Risk perceptions and precautionary behaviour. *Computers in Human Behavior*, 78, 283-297.
- Van Slyke, C., Shim, J. T., Johnson, R., & Jiang, J. J. (2006). Concern for information privacy and online consumer purchasing. *Journal of the Association for Information Systems*, 7(6), 16.
- Youn, S. (2009). Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. *Journal of Consumer affairs*, 43(3), 389-418.
- Yu, J., Ha, I., Choi, M. & Rho, J. (2005). Extending the TAM for a t-commerce. *Information & Management*. 42: 965-976.
- Yue “Jeff” Zhang, Jim Q. Chen & Kuang-Wei Wen, (2008) Characteristics of Internet Users and Their Privacy Concerns, *Journal of Internet Commerce*, 1:2, 1-16.
- Zhang, Y. J., Chen, J. Q., & Wen, K. W. (2002). Characteristics of Internet users and their privacy concerns: A comparative study between China and the United States. *Journal of internet Commerce*, 1(2), 1-16.

ÖZGEÇMİŞ

Erkan Çetintaş; 23.02.1982 İstanbul doğumludur. 2001 yılında Uludağ Üniversitesi Uluslararası ilişkiler Bölümünden mezun oldu. Mezuniyetinin ardından askerlik görevini 2007 yılında Adana İncirlik Hava Üssünde kısa dönem er olarak tamamladı. 2008 yılında Yalova Belediyesi Yerel Gündem 21 Sekreterliğinde Proje Sorumlusu olarak işe başlayan Erkan Çetintaş halen Yalova Belediyesi Dış İlişkiler biriminde Proje Sorumlusu olarak görev yapmaktadır.