



**T.C.
ERCIYES ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
İLETİŞİM BİLİMLERİ ANABİLİM DALI**

**DİJİTAL OKURYAZARLIK VE MAHREMİYET BAĞLAMINDA
KIRSAL BÖLGELERDE İNTERNET TABANLI HİZMETLERİN
KULLANIMI: KAYSERİ ÖRNEĞİ**

**Hazırlayan
Burak ÜNLÜ**

**Danışman
Prof. Dr. Vahit İLHAN**

Doktora Tezi

Ocak 2022, KAYSERİ

**T.C.
ERCIYES ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
İLETİŞİM BİLİMLERİ ANABİLİM DALI**

**DİJİTAL OKURYAZARLIK VE MAHREMİYET
BAĞLAMINDA KIRSAL BÖLGELERDE İNTERNET
TABANLI HİZMETLERİN KULLANIMI: KAYSERİ
ÖRNEĞİ
(Doktora Tezi)**

**Hazırlayan
Burak ÜNLÜ**

**Danışman
Prof. Dr. Vahit İLHAN**

Ocak 2022, KAYSERİ

BİLİMSEL ETİĞE UYGUNLUK

Bu çalışmadaki tüm bilgilerin, akademik ve etik kurallara uygun bir şekilde elde edildiğini beyan ederim. Aynı zamanda bu kural ve davranışların gerektirdiği gibi, bu çalışmanın özünde olmayan tüm materyal ve sonuçları tam olarak aktardığımı ve referans gösterdiğimi belirtirim.

Burak ÜNLÜ

İmza



T.C.

ERCIYES ÜNİVERSİTESİ

Sosyal Bilimler Enstitüsü Müdürlüğü

Anabilim Dalı : İletişim Bilimleri

Program Adı : İletişim Bilimleri Doktora Programı

Tez Başlığı : Dijital Okuryazarlık ve Mahremiyet Bağlamında Kırsal Bölgelerde
İnternet Tabanlı Hizmetlerin Kullanımı: Kayseri Örneği

Yukarıda bilgileri verilen tez çalışmasının a) Giriş, b) Ana bölümler ve c) Sonuç kısımlarından oluşan (Kapak, Ön söz, Özet, İçindekiler ve Kaynakça hariç) toplam 267 sayfalık kısmına ilişkin 8/02/2022 tarihinde **Turnitin** intihal programından aşağıda belirtilen filtreleme uygulanarak alınmış olan özgünlük raporuna göre tezin benzerlik oranı: %7'dir.

Filtrelemeye **alıntılar dahil** edilmiştir. Filtrelemede **yedi (7) kelimedenden daha az** örtüşme içeren metin kısımları hariç tutulmuştur.

Erciyes Üniversitesi Sosyal Bilimler Enstitüsü Tez İntihal Raporu Uygulama Esaslarını inceledim ve bu uygulama esaslarında belirtilen azami benzerlik oranlarına göre tez çalışmasının herhangi bir intihal içermediğini, aksinin tespit edilmesi durumunda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi ve yukarıda vermiş olduğum bilgilerin doğru olduğunu beyan ederim.

Gereğini bilgilerinize arz ederim. 8/02/2022

Danışman: Prof. Dr. Vahit İLHAN

Öğrenci: Burak ÜNLÜ

İmza

İmza

KILAVUZA UYGUNLUK

“Dijital Okuryazarlık ve Mahremiyet Bağlamında Kırsal Bölgelerde İnternet Tabanlı Hizmetlerin Kullanımı: Kayseri Örneği” başlıklı Doktora Tezi, Erciyes Üniversitesi Sosyal Bilimler Enstitüsü, Lisansüstü Tez Yazım Kılavuzuna uygun olarak hazırlanmıştır.

Hazırlayan

Burak ÜNLÜ

İmza

Danışman

Prof. Dr. Vahit İLHAN

İmza

İletişim Bilimleri ABD Başkanı

Doç. Dr. Ebru DAVULCU

İmza

ÖN SÖZ

Bu doktora tezi, 2021 yılının Temmuz ayında, Türkiye'nin güneyinde başta Manavgat olmak üzere onlarca ilçede meydana gelen yangınlar sonucu kaybettiğimiz ormanlarımıza, alevlerin etkisiyle evlerini ve yaşam alanlarını kaybeden kırsal bölgelerde yaşayan vatandaşlarımıza ithaf edilmiştir.

Bu zorlu tez yazım sürecine doğrudan ve dolaylı olarak katkısı olan pek çok dostum, mesai arkadaşlarım ve hocalarım vardı. Bu sebeple öncelikle, beni akademisyenliğe yönlendiren kıymetli hocam Doç. Dr. Levent Eldeniz'e; tezin öneri aşamasında yol gösterici tavsiyeler veren Prof. Dr. Hakan Aydın'a; bu fikri bir doktora tezi olarak ortaya koymamda desteğini hiçbir zaman esirgemeyen danışmanım Prof. Dr. Vahit İlhan'a; yöntem ve istatistiksel analizler konusunda her soruma sıklıkla cevap veren hocam Prof. Dr. Şükrü Balcı'ya ve savunma öncesinde ve sırasında nitelikli önerilerle çalışmanın değerini arttıran Prof. Dr. Adem Yılmaz ve Doç. Dr. Onur Önürmen'e teşekkür ediyorum. Ayrıca, değerli vaktini çalışmanın son okumasına ayırarak gözden kaçan pek çok yazım hatasını ve eksik virgülü fark eden mesai arkadaşım ve değerli hocam Doç. Dr. Meltem Şahin Hassan'a; önerileriyle istatistik dünyasında yolumu kaybetmememi sağlayan Dr. Öğr. Üyesi Mehmet Köprü'ye ve çalışma süreci boyunca desteğini hiçbir zaman esirgemeyen Dr. Öğr. Üyesi Seçil Yılmaz'a ne kadar teşekkür etsem az. Tabii, en büyük minnettarlığım da eğitimimi sürdürmemde, bir meslek edinmemde ve bir birey olarak kendimi gerçekleştirmemde bana her daim destek olan anne ve babama...

Çalışma, kırsal bölgelere yönelmesi gereken araştırmalar için bir ilk adım niteliğinde. Devamının gelmesi dileğiyle.

Burak ÜNLÜ, Kayseri, 2022

DİJİTAL OKURYAZARLIK VE MAHREMİYET BAĞLAMINDA KIRSAL BÖLGELERDE İNTERNET TABANLI HİZMETLERİN KULLANIMI: KAYSERİ ÖRNEĞİ

Burak ÜNLÜ

**Erciyes Üniversitesi, Sosyal Bilimler Enstitüsü
Doktora Tezi, Ocak 2022
Danışman: Prof. Dr. Vahit İLHAN**

ÖZET

İnternet ve internet tabanlı hizmetlerin kullanımı artık sadece altyapı olanaklarının daha fazla olduğu kent merkezlerinde değil, mobil internet dünyasının sunduğu altyapı hizmetleri sayesinde kırsal bölgelerde de hızla yaygınlaşmaktadır. 2021 itibariyle Türkiye’deki hanelerin yüzde 92’si ve bireylerin yüzde 82,6’sı internet kullanmaktadır. On yıl öncesine göre kullanıcı sayısı yaklaşık olarak yüzde 40 artan internetin yeni kullanıcıları, önceki ve tecrübeli kullanıcılara göre daha dezavantajlı konumdadırlar. Bu durum, söz konusu kullanıcıların, mahremiyetlerine yönelik riskleri de artırmaktadır. Çalışmada kırsal bölgelerde yaşayan enformasyon ve iletişim teknolojisi kullanıcılarının dijital okuryazarlık düzeyleri ve çevrim içi mahremiyete ilişkin yönelimleri araştırılmıştır. Çalışmanın ilk bölümünde mahremiyet kavramı ve mahremiyet hakkının tarihsel gelişimi, ikinci bölümünde ise ağ toplumu çerçevesinde dijital vatandaşlık ve dijital okuryazarlık kavramları ele alınmıştır. Çalışmanın üçüncü bölümünde ise, Kayseri’nin 2012 yılındaki mevzuat değişikliği öncesinde köy veya belde statüsünde olan mahallelerinde yaşayan 374 katılımcı ile gerçekleştirilen araştırmaya ilişkin bulgulara yer verilmiştir. Nicel araştırma yöntemlerinden biri olan yüz yüze anket yöntemi ile yapılan saha araştırması sonucunda, katılımcıların dijital okuryazarlık düzeylerinin düşük olduğu ve bu düzeyin yaşa, eğitim seviyesine ve kullanım sıklıklarına göre farklılaştığı sonucuna ulaşılmıştır. Ayrıca, katılımcıların mahremiyet konusunda hassas ve dikkatli oldukları ve mahremiyet yönelimlerinin yüksek olduğu görülmüştür. Analiz sonuçları, dijital okuryazarlık ve dijital vatandaşlık düzeyi ile mahremiyet yönelimi boyutları arasında anlamlı ve pozitif yönlü bir ilişki olduğunu göstermektedir.

Anahtar Kelimeler: Dijital Okuryazarlık, Mahremiyet, Çevrim İçi Mahremiyet, Dijital Vatandaşlık, Ağ Toplumu

**USE OF INTERNET-BASED SERVICES IN RURAL REGIONS IN THE
CONTEXT OF DIGITAL LITERACY AND PRIVACY:
THE CASE OF KAYSERİ**

Burak ÜNLÜ

**Erciyes University, Graduate School of Social Sciences
PhD Thesis, January 2022
Supervisor: Prof. Dr. Vahit İLHAN**

ABSTRACT

The use of internet and internet-based services have not only become widespread in urbans where infrastructures are more abundant, but also in rural areas thanks to the services offered by the mobile internet. As of 2021, 92% of households and 82.6% of individuals in Turkey use the internet. New users of the internet, whose number of users increased by approximately 40 percent compared to ten years ago, are in a more disadvantaged compared to previous and experienced users. This situation also increases the risks to the privacy of the users in question. In this study, digital literacy levels and online privacy orientations of ICT users living in rural areas were investigated. In the first part of the study, the concept of privacy and the historical development of the right to privacy, and in the second part, the concepts of digital citizenship and digital literacy within the framework of network society are discussed. In the third part of the study, the findings related to the research carried out with 374 participants living in the neighborhoods of Kayseri that had village or town status before the legislation change in 2012 are included. As a result of the field research conducted with the face-to-face survey method, which is one of the quantitative research methods, it was concluded that the digital literacy levels of the participants were low and this level differed according to age, education level and frequency of use. In addition, it was observed that the participants were sensitive and careful about privacy and their privacy orientation was high. The results of the analysis show that there is a significant and positive correlation between the level of digital literacy and digital citizenship with the dimensions of privacy orientation.

Keywords: Digital Literacy, Privacy, Online Privacy, Digital Citizenship, Network Society

İÇİNDEKİLER

DİJİTAL OKURYAZARLIK VE MAHREMİYET BAĞLAMINDA KIRSAL BÖLGELERDE İNTERNET TABANLI HİZMETLERİN KULLANIMI: KAYSERİ ÖRNEĞİ

BİLİMSEL ETİĞE UYGUNLUK	i
KILAVUZA UYGUNLUK	iii
KABUL VE ONAY TUTANAĞI.....	iv
ÖN SÖZ	v
ÖZET	vi
ABSTRACT	vii
İÇİNDEKİLER.....	viii
SİMGELER ve KISALTMALAR LİSTESİ.....	xii
TABLolar LİSTESİ.....	xv
ŞEKİLLER LİSTESİ	xviii
GİRİŞ.....	1

BİRİNCİ BÖLÜM MAHREMİYET ve GÖZETİM TOPLUMU

1.1. Mahremiyet.....	8
1.1.1. Mahremiyet Hakkının Temelleri ve Gelişimi.....	13
1.1.2. Mahremiyete Yönelik Tehditler	23
1.1.3. Dijital Dünyada Mahremiyet	27
1.1.3.1. Kuramsal Yaklaşımlar	38
1.1.3.1.1. İletişim Mahremiyeti Yönetimi (CPM) Teorisi.....	39
1.1.3.1.2. Genişletilmiş Mahremiyet Düzenleme (Privacy Regulation) Teorisi	47
1.1.3.2. Dijital Dünyada Mahremiyetin Sınırlanması.....	49
1.1.3.2.1. Güvenli Bir Yaşam Sürme ve Mahremiyet İlişkisi	52
1.1.3.2.2. Kimlik Oluşturma, Sosyalleşme ve Mahremiyet İlişkisi.....	55
1.1.4. Çevrim İçi Mahremiyet Konusunu İnceleyen Çalışmalar	58
1.1.4.1. Literatürdeki Araştırmalar	58
1.1.4.2. Çevrim İçi Mahremiyet ile İlgili Çalışmaların Genel Değerlendirmesi.....	93

1.1.5. Mahremiyet ile İlgili Hukuki Düzenlemeler	96
1.1.5.1. Uluslararası Hukuki Düzenlemeler	97
1.1.5.2. Türkiye’deki Hukuki Düzenlemeler	100
1.2. Gözetim Toplumu	102
1.2.1. Panoptikon	107
1.2.2. Sinoptikon, Postpanoptikon, Ban-Optikon	110

İKİNCİ BÖLÜM AĞ TOPLUMU VE DİJİTAL OKURYAZARLIK

2.1. Ağ Toplumu	118
2.1.1. Kitle Toplumu ile Ağ Toplumu Ayrımı	123
2.1.2. Ağ Toplumuna Entegrasyon	125
2.1.3. Kırsal Yerleşimlerde İnternet Erişimi ve Ağ Toplumuna Entegrasyon	132
2.1.4. Ağ Toplumu Olarak Türkiye	136
2.2. Dijital Vatandaşlık	142
2.3. Dijital Okuryazarlık	147
2.3.1. Dijital Okuryazarlığı Oluşturan Okuryazarlıklar	152
2.3.1.1. Bilgisayar Okuryazarlığı	153
2.3.1.2. Enformasyon ve İletişim Teknolojileri Okuryazarlığı	154
2.3.1.3. Bilgi Okuryazarlığı	155
2.3.1.4. İnternet Okuryazarlığı	156
2.3.1.5. Medya Okuryazarlığı	157
2.3.2. Dijital Okuryazarlık Boyutları	158
2.3.3. Dijital Beceriler, Dijital Yeterlilikler	160
2.3.3.1. Vatandaşlar için Dijital Yetkinlik Çerçevesi (DigComp)	162
2.3.3.2. Dijital Becerilerden Somut Sonuçlara (DiSTO)	164
2.3.3.3. Temel Dijital Beceriler Çerçevesi	167
2.3.3.4. ITU Dijital Beceri Seviyeleri	168
2.4. Literatürdeki Araştırmalar	169

ÜÇÜNCÜ BÖLÜM KAYSERİ KIR NÜFUSUNUN DİJİTAL OKURYAZARLIK DÜZEYİ ve ÇEVİRİM İÇİ MAHREMİYET YÖNELİMLERİ

3.1. Araştırmanın Sorunu	177
3.2. Araştırmanın Amacı	178

3.3. Araştırmanın Önemi	179
3.4. Araştırma Soruları ve Hipotezleri.....	179
3.5. Araştırmanın Kapsam ve Sınırlılıkları.....	184
3.6. Araştırmanın Yöntemi	185
3.7. Araştırmanın Evreni ve Örneklemi.....	186
3.8. Araştırmanın Bilimsel Etiğe Uygunluğu	190
3.9. Kullanılan Ölçekler ve Soru Formu.....	190
3.10. Güvenilirlik ve Geçerlilik.....	192
3.11. Verilerin Analizinde Kullanılan İstatistiki Testler	193
3.11.1. Frekans (Sıklık) Analizi.....	194
3.11.2. Faktör Analizi	194
3.11.3. İki Adımlı Küme (Two-Step Cluster) Analizi	194
3.11.4. Pearson ve Spearman Korelasyon Analizleri	195
3.11.5. Ki-Kare Analizi	195
3.11.6. Ortalama Karşılaştırma Analizleri.....	196
3.11.6.1. Tek Örneklem t-Testi.....	196
3.11.6.2. Bağımsız Örneklem t-Testi.....	196
3.11.6.3. Mann-Whitney U Testi	196
3.11.6.4. Tek Faktörlü Varyans Analizi (One-Way ANOVA).....	197
3.11.6.5. Kruskal -Wallis H Testi	197
3.12. Bulgular	197
3.12.1. Örneklem İlişkin Demografik Bilgiler.....	197
3.12.2. Cihaz, Teknoloji ve Uygulama Kullanımlarına İlişkin Bulgular	200
3.12.3. Anlık Mesajlaşma Programları ile Kurulan İletişimlere İlişkin Bulgular	207
3.12.4. EİT Maruziyeti Süresine ve İnternet Aboneliklerine İlişkin Bulgular	209
3.12.5. Mahremiyet Tercihlerine ve Kişisel Bilgi Paylaşımlarına İlişkin Bulgular	211
3.12.6. Mahremiyet Yönelimlerine İlişkin Bulgular	220
3.12.6.1. Cinsiyete Göre Mahremiyet Yönelimi Boyutları	223
3.12.6.2. Yaş Göre Mahremiyet Yönelimi Boyutları	224
3.12.6.3. Eğitim Durumuna Göre Mahremiyet Yönelimi Boyutları	225
3.12.6.4. EİT Maruziyet Sürelerine Göre Mahremiyet Yönelimi Boyutları	227
3.12.6.5. Gizlilik Ayarları Tercihlerine Göre Mahremiyet Yönelimi Boyutları	228

3.12.6.6. İnternette Paylaşılan Bilgilere Göre Mahremiyet Yönelimi Boyutları	230
3.12.6.7. Sosyal Ağ Sitesi ve Teknoloji Kullanım Sıklıkları ile İnternette Alışveriş Yapma Tercihlerine Göre Mahremiyet Yönelimi Boyutları	232
3.12.7. Dijital Okuryazarlık ve Dijital Vatandaşlık Düzeyine İlişkin Bulgular ...	235
3.12.7.1. Cinsiyete Göre Dijital Okuryazarlık ve Dijital Vatandaşlık Düzeyleri	238
3.12.7.2. Yaş'a Göre Dijital Okuryazarlık ve Dijital Vatandaşlık Düzeyleri	239
3.12.7.3. Eğitim Durumuna Göre Dijital Okuryazarlık ve Dijital Vatandaşlık Düzeyleri	241
3.12.7.4. EİT Maruziyet Sürelerine Göre Dijital Okuryazarlık ve Dijital Vatandaşlık Düzeyleri	241
3.12.7.5. Sosyal Ağ Sitesi ve Teknoloji Kullanım Sıklıkları ile İnternette Alışveriş Yapma Tercihlerine Göre Dijital Okuryazarlık ve Dijital Vatandaşlık Düzeyleri	242
3.12.8. Mahremiyet Yönelimleri ile Dijital Okuryazarlık ve Dijital Vatandaşlık Düzeyi Arasındaki İlişki.....	245
SONUÇ ve ÖNERİLER.....	248
KAYNAKÇA.....	268
EKLER.....	309
EK 1: Araştırmada Kullanılan Anket Soruları	309
EK 2: Etik Kurul Onayı	314

SİMGELER ve KISALTMALAR LİSTESİ

AB	: Avrupa Birliği
ABD	: Amerika Birleşik Devletleri
ADSL	: Asymmetric Digital Subscriber Line
AİHS	: Avrupa İnsan Hakları Sözleşmesi
Akt.	: Aktaran
APCO	: Antecedents / Privacy Concerns / Outcomes
AS	: Araştırma Sorusu
BAE	: Birleşik Arap Emirlikleri
Bkz.	: Bakınız
BT	: Bilişim Teknolojileri
BTK	: Bilgi Teknolojileri ve İletişim Kurumu
CCPA	: California Consumer Privacy Act
CPM	: Communication Privacy Management
DBO	: Dijital Bilgi Okuryazarlığı
DigComp	: The European Digital Competence Framework
DigEuLit	: A European Framework for Digital Literacy Project
DiSTO	: Digital Skills to Tangible Outcomes
DPI	: Deep Packet Inspection
EİT	: Enformasyon ve İletişim Teknolojileri
ETS	: Educational Testing Service
GDPR	: General Data Protection Regulation
GPS	: Global Positioning System
H	: Hipotez

HES	: Hayat Eve Sığar
ICSM	: International Computer Saksharta Mission
ICT	: Information and Communication Technologies
IoT	: Internet of Things
ISTE	: International Society for Technology in Education
ITU	: International Telecommunication Union
İGE	: İnsani Gelişme Endeksi
İHEB	: İnsan Hakları Evrensel Beyannamesi
İMY	: İletişim Mahremiyeti Yönetimi
İSS	: İnternet Servis Sağlayıcı
KVKK	: Kişisel Verilerin Korunması Kanunu
MHRS	: Merkezi Hekim Randevu Sistemi
NRI	: Network Readiness Index
NSA	: National Security Agency
NSFNet	: National Science Foundation Network
ODTÜ	: Orta Doğu Teknik Üniversitesi
OECD	: Organisation for Economic Co-operation and Development
PC	: Personal Computer
PIAAC	: Programme for the International Assessment of Adult Competencies
RTÜK	: Radyo ve Televizyon Üst Kurulu
SDG	: Sustainable Development Goals
SEGE	: Sosyo-Ekonomik Gelişmişlik Sıralaması Araştırması
SIM	: Subscriber Identity Module
TCP/IP	: Transmission Control Protocol / Internet Protocol
TDK	: Türk Dil Kurumu

THE	: Times Higher Education
TİAK	: Televizyon İzleme Araştırmaları Komitesi Anonim Şirketi
TÜİK	: Türkiye İstatistik Kurumu
TÜVEKA	: Türkiye Üniversiteler ve Araştırma Kurumları Ağı
UNDP	: United Nations Development Programme
UNESCO	: The United Nations Educational, Scientific and Cultural Organization
YER-SİS	: Türkiye’de Kentsel ve Kırsal Yerleşim Sistemleri Araştırması
$\bar{X}$	: Ortalama



TABLÖLAR LİSTESİ

Tablo 1.1:	Mahremiyeti Etkileyen Büyük Ölçekli Faktörler	36
Tablo 2.1:	Kitle Toplum ve Ağ Toplumunun Tipolojisi	126
Tablo 2.2:	En Yüksek NRI Skoruna Sahip 20 Ülke.....	129
Tablo 2.3:	En Yüksek İGE Skoruna Sahip 21 Ülke (1990-2019).....	130
Tablo 2.4:	Ülkelerin Nüfusuna Göre İnternet Kullanım Oranları (2010-2020).....	131
Tablo 2.5:	Ülkelerin Cinsiyete Göre Kent-Kır Nüfusu İnternet Kullanım Oranları	134
Tablo 2.6:	Bazı Avrupa Ülkelerinin Kent-Kır Ayrımına Göre Dijital Becerileri (%).....	137
Tablo 2.7:	Türkiye’de Bilgisayar Kullanımı ve İnternet Erişimi Oranları.....	140
Tablo 2.8:	DigComp Yetkinlik Alanları ve Yetkinlikleri	166
Tablo 2.9:	Yeterlilik Düzeylerini Öne Çıkaran Ana Anahtar Kelimeler	167
Tablo 2.10:	İnternet Becerisi Çerçevesi	169
Tablo 3.1:	Örnekleme Dahil Edilen İlçeler ve Toplam Katılımcı Sayıları	194
Tablo 3.2:	Çok Boyutlu Mahremiyet Yönelimleri Ölçeği’nin Cronbach Alpha Skorları.....	198
Tablo 3.3:	Katılımcıların Demografik Özellikleri.....	203
Tablo 3.4:	Uygulama, Cihaz ve Teknoloji Kullanım Sıklıkları	206
Tablo 3.5:	Cinsiyete Göre Uygulama ve Teknoloji Kullanım Farklılığı	207
Tablo 3.6:	Dijital Yerli ve Dijital Göçmen Kategorilerine Göre Uygulama ve Teknoloji Kullanım Farklılığı	209
Tablo 3.7:	Cihaz, Uygulama ve Teknoloji Kullanımının Pandemi Sürecindeki Değişimi.....	211
Tablo 3.8:	Kategorilere Göre Anlık Mesajlaşma Uygulamaları ile Kurulan İletişim	214
Tablo 3.9:	Cinsiyete Göre İlk EİT Kullanımı Tarihleri.....	215
Tablo 3.10:	Katılımcıların İnternet Abonelikleri	215
Tablo 3.11:	Sosyal Medya Uygulamalarındaki Varsayılan Gizlilik Ayarlarını Değiştirme Oranları	217
Tablo 3.12:	Sosyal Medya Uygulamalarındaki Profil ve Gönderilerin Görünürlüğü.....	218

Tablo 3.13:	Cinsiyet ve Yaşa Göre Son Görülme ve Mavi Tik Özelliklerinin Kullanımı	219
Tablo 3.14:	Cinsiyet ve Yaşa Göre Akıllı Telefonlarda Şifre Kullanımı.....	220
Tablo 3.15:	Cinsiyet ve Yaşa Göre Akıllı Telefonlarda Kullanılan Şifrenin Paylaşımı.....	221
Tablo 3.16:	Kimlik Öğelerinin Paylaşılma Oranları	222
Tablo 3.17:	Kimlik Öğelerinin Paylaşılma Oranının Cinsiyete Göre Karşılaştırması	224
Tablo 3.18:	Kimlik Öğelerinin Paylaşılma Oranının Yaşa Göre Karşılaştırması	225
Tablo 3.19:	Çok Boyutlu Mahremiyet Yönelimleri Ölçeği Faktör Analizi	226
Tablo 3.20:	Çok Boyutlu Mahremiyet Yönelimleri Ölçeği Alt Boyutları ve Ortalama Ölçek Puanları	227
Tablo 3.21:	Çok Boyutlu Mahremiyet Yönelimleri Ölçeği Z Skorları ile Alt Boyutların Karşılaştırılması	228
Tablo 3.22:	Mahremiyet Yönelimi Boyutlarının Cinsiyete Göre Karşılaştırması ...	228
Tablo 3.23:	Mahremiyet Yönelimi Boyutlarının Dijital Göçmen - Dijital Yerli Değişkenine Göre Karşılaştırması	229
Tablo 3.24:	Mahremiyet Yönelimi Boyutlarının Yaş Gruplarına Göre Karşılaştırması	230
Tablo 3.25:	Mahremiyet Yönelimi Boyutlarının Eğitim Düzeyine Göre Karşılaştırması	231
Tablo 3.26:	Mahremiyet Yönelimi Boyutları ile EİT Maruziyet Süreleri Arasındaki İlişkiyi Gösteren Korelasyon Analizi	233
Tablo 3.27:	Mahremiyet Yönelimi Boyutlarının Sosyal Medya Profillerindeki Gizlilik Tercihlerine Göre Karşılaştırması.....	234
Tablo 3.28:	Mahremiyet Yönelimi Boyutlarının Anlık Mesajlaşma Uygulamalarındaki Son Görülme Özelliğinin Kullanımına Göre Karşılaştırması	235
Tablo 3.29:	Mahremiyet Yönelimi Boyutlarının Anlık Mesajlaşma Uygulamalarındaki Mavi Tik Özelliğinin Kullanımına Göre Karşılaştırması	235

Tablo 3.30:	Mahremiyet Yönelimi Boyutlarının Eğitim Düzeyinin Paylaşılmasına Göre Karşılaştırması	237
Tablo 3.31:	Mahremiyet Yönelimi Boyutlarının Fotoğrafların Paylaşılmasına Göre Karşılaştırması	237
Tablo 3.32:	Mahremiyet Yönelimi Boyutları ile Sosyal Medya ve EİT Kullanım Sıklıkları Arasındaki İlişkiyi Gösteren Korelasyon Analizi	238
Tablo 3.33:	Dijital Okuryazarlık Ölçeği Betimsel İstatistikleri	241
Tablo 3.34:	Tüm Katılımcıların Dijital Okuryazarlık Düzeyi için Tek Örneklem t Testi.....	242
Tablo 3.35:	Dijital Yerlilerin Dijital Okuryazarlık Düzeyi için Tek Örneklem t Testi.....	242
Tablo 3.36:	Dijital Vatandaşlık Ölçeği Betimsel İstatistikleri	243
Tablo 3.37:	Dijital Okuryazarlık ve Dijital Vatandaşlık Ölçeklerinin Çarpıklık ve Basıklık Değerleri	244
Tablo 3.38:	Cinsiyete Göre Dijital Okuryazarlık ve Dijital Vatandaşlık Düzeyleri	244
Tablo 3.39:	Dijital Yerli ve Dijital Göçmen Ayrımına Göre Dijital Okuryazarlık ve Dijital Vatandaşlık Düzeyleri.....	245
Tablo 3.40:	Yaş Gruplarına Göre Dijital Okuryazarlık ve Dijital Vatandaşlık Düzeyleri.....	246
Tablo 3.41:	Eğitim Düzeyine Göre Dijital Okuryazarlık ve Dijital Vatandaşlık Düzeyleri.....	247
Tablo 3.42:	EİT Maruziyet Süreleri ile Dijital Okuryazarlık ve Dijital Vatandaşlık Düzeyleri Arasındaki Korelasyon.....	248
Tablo 3.43:	Sosyal Medya ve EİT Kullanım Sıklıkları ile Dijital Okuryazarlık ve Dijital Vatandaşlık Düzeyleri Arasındaki Korelasyon	249
Tablo 3.44:	İnternette Alışveriş Yapma Tercihine Göre Dijital Okuryazarlık ve Dijital Vatandaşlık Düzeyleri	251
Tablo 3.45:	Mahremiyet Yönelimi Boyutları ile Dijital Okuryazarlık ve Dijital Vatandaşlık Düzeyleri Arasındaki Korelasyon.....	251
Tablo 3.46:	Mahremiyet Yönelimi Alt Boyutlarına Göre Dijital Okuryazarlık ve Dijital Vatandaşlık Düzeyleri	252

ŞEKİLLER LİSTESİ

Şekil 2.1:	Ağ Toplumunda Üç Parçalı Katılım.....	133
Şekil 2.2:	Kentteki Temelin Üstünde Beceriler ile Kırsaldaki Düşük Beceriler Arasındaki İlişkiyi Gösteren Grafik	139
Şekil 2.3:	Geniş Bant ve Mobil Geniş Bant İnternet Abonelikleri	142
Şekil 2.4:	Yıllara Göre Hanelerdeki EİT Teknolojileri Bulunma Oranları	143
Şekil 2.5:	Türkiye’de Son Üç Ay İçerisinde İnternet Kullanan Bireylerin Dijital Beceri Düzeyleri.....	144
Şekil 2.6:	Türkiye ve AB Ülkelerinde Son Üç Ay İçerisinde İnternet Kullanan Bireylerin Dijital Beceri Düzeyleri (2019).....	145
Şekil 2.7:	Dijital Vatandaşlık Boyutları	149
Şekil 2.8:	Maslow İhtiyaçlar Hiyerarşisi ve Dijital Okuryazarlık	154
Şekil 2.9:	Dijital Okuryazarlık Boyutları	164
Şekil 2.10:	Temel Dijital Beceriler Çerçevesi Diyagramı	171
Şekil 2.11:	Dijital Beceriler	173
Şekil 3.1:	Kayseri İlçelerindeki Mobil Sinyal Yoğunlukları	191
Şekil 3.2:	Kayseri İlçelerinin Sosyo-Ekonomik Gelişmişlik Kademeleri	193
Şekil 3.3:	Araştırmanın Uygulandığı Konumların Oluşturduğu Isı Haritası.....	194
Şekil 3.4:	Anlık Mesajlaşma Uygulamaları ile Kurulan İletişim	213

GİRİŞ

İnternet, sadece kendisinden önce gelen tüm kitle iletişim araçlarını kapsayan yöndeşme yönüyle değil, yaygınlaşma hızı ile de özgün bir araçtır. Kullanıcılarının sadece izleyici/tüketici (*audience*) değil üretici de olabilmesi ve internetin sağladığı etkileşim, bu hizmetin hızla yaygınlaşmasında ve kabul görmesinde pay sahibidir. Yirminci yüzyılın son on yılında bir hizmet olarak halka sunulmaya başlanan internet, öncelikli olarak mevcut telefon kabloları altyapısı ile kullanıcılara ulaştırılmış, daha sonra da özel olarak internet için oluşturulan fiber optik kablo altyapısı ile desteklenmiş, hız ve kapasitesi arttırılmıştır. Geniş bant mobil internetin yaygınlaşması ise yirmi birinci yüzyılın ikinci on yılından itibaren başlamış ve internete erişim için kablo altyapısına yakın olma, kablo ağına eklenme mecburiyeti büyük ölçüde ortadan kalkmıştır. Özellikle mobil geniş bant hizmetinin de etkisiyle, günümüzde toplam dünya nüfusunun yüzde 65'e yakını interneti kullanmaktadır.

Dünya nüfusunun yarısından fazlası tarafından kullanılan ve her geçen gün kullanıcı sayısı artan internet, üzerinde pek çok fırsat, olanak, risk ve tehlikenin bir arada bulunduğu bir ortam, bir alan olarak ifade edilebilir. Sağladığı etkileşim altyapısı ile internet hem kişilerarası iletişimin hem de kitle iletişiminin doğasını değiştirmiştir. İnteraktif bir iletişim aracı olarak internet, sunulan enformasyonun tüketilmesinin yanı sıra kullanıcılarına enformasyon üretme imkânı da tanımaktadır. Üstelik bu üretim imkânı sadece içerik ile de sınırlı değildir. Gerekli temel teknik becerilere sahip ve fikri olan herkes internet üzerinde bir web sitesi oluşturabilir, belirli bir işletim sistemi üzerinde çalışan bir program yazıp onu uygulama marketlerinde satabilir, hatta cep telefonları için bir uygulama kodlayabilir veya çevrim dışı olarak yürüttüğü mesleğinin satış, pazarlama ve lojistiğini internet üzerinden koordine edebilir. Bu özellikleri ile internet fırsat yaratıcı bir ortamdır.

Yeni platformlar, portallar, uygulamalar ve internet siteleri oluřturmanın; temel beceri ve merak önkořulu dıřında bir sermaye gerektirmiyor oluřunun karanlık tarafı ise kötü niyetli kiřilerin de bu sıralananları oluřturabilmesidir. Sık ziyaret edilen bir banka sitesinin birebir bir kopyası kolayca üretilebilir ve dikkatsiz ya da o an dalgın olan kullanıcıların internet bankacılığı hesaplarına ait erişim bilgileri ele geçirilebilir. Araç çubuğunda yazan adres dışında hiçbir farklılık olmadan oluřturulan sahte bir Facebook, Twitter ya da Instagram giriş ekranı, kullanıcıların bu hesaplarına erişim bilgilerinin kötü niyetli kiřiler tarafından ele geçirilmesine neden olabilir. Hatta, ileri düzeyde programlama dili becerisine sahip olan kötü niyetli kiřiler; oluřturdukları tuzaklarla (gelen kutusundaki bir e-posta, sosyal ağı sitelerinden gönderilen bir mesaj vb. ile gelen casus yazılımlar) sadece sosyal medya profillerini değıl bilgisayarda ya da telefonunuzda bulunan ve çevrim içi ortama tařınmayan verileri de hem ele geçirebilir hem de kullanıcının o verilere erişimini engelleyip verilerin kurtarılması için fidye isteyebilir. Kısacası, internet üzerindeki üretme kolaylığı, büyük avantajlar sunarken beraberinde ciddi riskleri de getirmektedir.

Özellikle Web 2.0 olarak nitelendirilen devrimle bařlayan kullanıcı temelli içerik üretimi, herkese söz hakkı tanınması ve ifade özgürlüğü açısından dünya toplumlarının demokratikleřmesi yolunda önemli bir gelişme olarak değıerlendirilebilir. Yaygınlařan akıllı cep telefonu ve yüksek çözünürlükte görüntü kaydedebilen mobil cihazlar ile herkes anı yakalayabilir, paylařabilir ve bunu yüzbinlerce kiřiye ulařtırabilir. Bir mesajın yüzbinlerce kiřiye kolayca ulařtırılabiliyor oluřu konunun ilk bakıřta görünen, heyecan ve umut verici tarafıdır. Meselenin diğıer tarafında ise aşırı enformasyon üretimi ve bu enformasyon yığınları arasında nitelikli verilerin ve doğıru bilgilerin silikleřmesi, kaybolması vardır. Kullanıcı kaynaklı içerik üretimi kimi bilimsel gerçekler hakkında yanlış bilgilerin de yayılmasına, yüzyıllar önce tahmin edilen, geçtiğimiz yüzyıllarda kanıtlanan dünyanın yuvarlaklığının reddine kadar ulařabilen kimi sapmalara neden olabilmektedir. Üstelik herkese söz hakkı tanınması ve ifade özgürlüğü temalarına darbe vuran sadece doğıru olmayan ve niteliksiz bilgilerin yaygınlık kazanması değıildir. Webin (ağın) yedi kanunundan biri olan “dikkatin sınırlılığı kanunu” (van Dijk, 2017) ile ifade edilen duruma göre, internet herkese söz hakkı verir; ancak sınırlı bir kesimin söyledikleri “dikkate” alınır. Çünkü “siber uzayda konuřmak kolay olabilir, ancak duyulmak zordur (Hindman, 2009, s. 142).”

İnternet kullanımında Web 2.0 gibi köklü bir diğer değişim de kullanıcılarının anonim bir şekilde internet kullanımını terk edip gerçek adlarla ve tanımlayıcı kişisel verilerle internette tüketmeye ve üretmeye başlaması olduğu söylenebilir. Bu tercih değişikliğinin tam olarak ne zaman başladığı açık ve noktasal bir şekilde tarihlenemese de sosyal ağ sitelerinin kullanımının yaygınlaşması ile ilişkilendirilebilir. Bu değişimin özellikle, 2004 yılında sadece üniversite öğrencilerinin, 2006 yılında da tüm bireylerin kullanımına sunulan ve halen en fazla kullanıcıya sahip olan Facebook'un (We Are Social, 2021) yaygınlaşması ile hız kazandığı düşünülmektedir.

İnternet kullanıcılarının takma isimler yerine gerçek adları, telefon numaraları ve fotoğrafları ile internette varoluşları, beklenmedik pek çok bağlantı, fırsat, iletişim, şan ve şöhret şansı oluşturur. Münferit, ancak medya aracılığıyla parlatılan örnekler, sıradan insanlara “sen de yapabilirsin” çerçevesinde bir mesajın ulaştırılmasına neden olmaktadır. Bu örnekler, örneklerin parlatılması ve yeni örneklerin ortaya çıkması ile bir çeşit döngü meydana getirir. Bu döngü ise, “ağların dışsallığı kanunu” ile açıklanabilir. Bu kanuna göre; bir ağa ne kadar fazla kişi katılırsa diğerlerinin de katılma olasılığı artar ve üzerlerinde ağa katılma baskısı oluşur. Bu döngü ve ağ baskısı ile bireyler, varlıklarının çevrim içi karşılığına denk düşecek sosyal ağ profilleri oluşturmaya ve bu profilleri belirli bir ritim ve harmoni içerisinde kişisel verileri ile desteklemeye yönelmektedirler.

Ağ kanunlarının varsayımlarını destekler şekilde bireylerin her gün daha fazla kişisel veriyi sosyalleşme, kimlik ve itibar oluşturma, ürün ve hizmetlere erişme gibi gerekçelerle, kimi durumda sadece kendi izin verdiği kişilerle (arkadaş ve takipçi listeleri ile) kimi durumda ise bir sınırlandırma olmaksızın internete erişebilen herkesle paylaşıyor olması, mahremiyet ve kişisel verilerin güvenliği tartışmalarını gündeme getirir. Üstelik bu mahremiyet sorunu sadece yazılan tweet’lerden ya da paylaşılan fotoğraflardan ibaret değildir. Kullanıcılar yaptığı bu işlemler sırasında, üst veri (*metadata*) olarak isimlendirilen ve paylaşılan içeriğin nerede, hangi saatte, hangi cihaz üzerinde, ne kadar sürede oluşturduğu, bu içeriğin boyutunun ne olduğu gibi veriler de üretmektedir ve bu veriler de içeriklerle birlikte kaydedilmektedir. Gerek kullanıcılar tarafından bilinçli olarak yapılan paylaşımların gerekse bu paylaşımların oluşturulmasına ilişkin detayları içeren üst verilere kimler tarafından erişilebileceği ve bu verilerin kimler tarafından işleneceği sosyal ağ sitelerinin ve hizmet sağlayıcılarının tanımladığı gizlilik

tercihleri ile yönetilebilmektedir. Bu tercihlerin doğru bir şekilde ayarlanmaması, kişisel bilgilerin üçüncü şahıslarla paylaşılmasının yasal zeminini oluşturmaktadır.

İnternet ve internet tabanlı hizmetler ile ilgili karamsar ve distopik bir tablo çizmek kolaydır, ancak tamamen doğru değildir. Çünkü bu teknolojiler hakkında temel beceri ve deneyime sahip olunduğunda, risklerin önlenmesi ve çevrim içi katılım, ifade özgürlüğü ve demokratik toplum gibi ideallerin desteklenmesi, güçlendirilmesi mümkün olabilir. Bunun sağlanması için, bireylerin sadece internete ve internet tabanlı hizmetlere erişimi değil, bu teknoloji ve hizmetleri kullanma becerileri de önem kazanmaktadır.

Binyıl başında yapılan araştırmalarda, dijital teknolojilere ülkeler ve ülkeler içerisindeki farklı grupların eşit bir şekilde erişemiyor oluşu sorunsallaştırılmış ve bu sorun, dijital bölünme (*digital divide*) olarak literatüre girmiştir. Yeni yüzyılın yaklaşık beşte biri geride kaldığında, özellikle mobil geniş bant internet hizmetinin de etkisiyle internete erişimdeki bu eşitsizlik büyük ölçüde ortadan kalkmıştır. Ancak, erişim olanaklarını eşitlemek dijital bölünmeyi ortadan kaldırmamış, formunun değişmesine neden olmuştur. İkinci düzey dijital bölünme olarak adlandırılan bu bölünme, bireylerin internet tabanlı hizmet ve teknolojilere erişimine değil erişim sağlayan bireyler arasındaki beceri farklılıklarına dikkat çekmektedir. Bu beceriler, dijital yetkinlikler ya da dijital beceriler olarak nitelendirilebilir ve bu becerilere sahip bireyler dijital okuryazar olarak anılabilirler.

Kırsal bölgeler özelinde düşünüldüğünde, birinci düzey dijital bölünmenin daha yakın bir dönemde kapandığı ya da kapanmaya başladığı söylenebilir. 2018 yılında yapılan bir araştırmaya göre, Çin'in kırsal bölgelerinde yaşayanların internet erişimi son beş yıl içerisinde neredeyse yüzde 40 artmış ve yüzde 62,2'ye ulaşmıştır (akt. C. Chen, 2018). Bu oran diğer ülkelerde daha düşüktür. Yine 2018 verilerine göre Filipinler'de kırsal nüfusun sadece yüzde 31'inin internet erişimi vardır (BusinessWorld, 2018). Türkiye'de ise yapılan araştırmalara göre, 2003 yılında sadece yüzde 1.2 olan kırsal bölgelerdeki internete erişim oranı (Hacettepe Üniversitesi Nüfus Etütleri Enstitüsü, 2004, s. 32), 2013 yılında yaklaşık yüzde 29'a ulaşmıştır. Bu oran aynı tarihte kentsel bölgelerdeki hanelerde yüzde 57.4'tür (TÜİK, 2013). Bu yıldan itibaren TÜİK internet erişimi araştırmalarında kent-kır ayrımı yapmayı bırakmıştır. Özellikle 2016 yılından itibaren geniş bant mobil internet hizmetinin kullanıma sunulması ve bu hizmetin kırsal

bölgeleri de kapsamaya başlamasıyla birlikte, kırsaldaki internet kullanım oranının yükseldiği öngörülmektedir.

Bu tez çalışmasında, ağ toplumuna entegrasyonun sadece erişimle sınırlı olmadığı, toplumların ağ toplumuna geçişinde vatandaşlarının birer dijital vatandaşa dönüşmesi gerektiği ve bu dönüşümün bireylerin edineceği dijital ve eleştirel düşünme becerileriyle kazanacakları dijital okuryazarlık ile mümkün olacağı savunulmaktadır. Bu sebeple araştırmanın çerçevesinde dijital okuryazarlık önemli bir yer tutar. Çalışmada ele alınan diğer konu ise mahremiyettir. İnternet tabanlı hizmetlerden kaynaklanan riskler arasında, belki de en çok tartışılanı kişisel verilerin güvenliğidir. En çok tartışılan boyut olmasının yanında mahremiyet, diğer tüm riskler arasında en kolay karşı karşıya kalınabilecek risklerden biridir. En bilinçli ve dikkatli birey bile, verilerini paylaştığı kurumun sistemlerine yapılan bir saldırı sonucu kişisel verilerinin (örneğin e-posta ve ev adresi, cep telefonu gibi birbiri ile ilişkili verilerinin) üçüncü kişilerin eline geçmesi durumu ile karşı karşıya kalabilir. Bununla birlikte, bilinçli bir şekilde kişisel bilgilerini herkesin erişimine açan bireylerin sayısı da hiç az değildir. Tüm bu sebeplerle, bireylerin mahremiyet yönelimleri de onların ağ toplumundaki varlıklarının ve itibarlarının korunmasında önemli bir yer tutmaktadır.

Bu çerçevede, bu tez çalışmasında, internetin Türkiye'nin kırsal bölgelerinde kullanımının yaygınlaşmaya başlaması ve birinci düzey dijital bölünmenin kısmen kapanıp kullanım becerileri farklılıklarından kaynaklanan ikinci düzey dijital bölünmenin ortaya çıktığı bir dönemde olduğumuz savlanmıştır. Bu savdan hareketle çalışma, kırsal bölgelerde yaşayan enformasyon ve iletişim teknolojileri kullanıcılarının dijital okuryazarlık düzeyleri ve mahremiyet yönelimlerine odaklanmıştır. Birinci bölümde mahremiyet düşüncesinin temelleri ve bir hak olarak mahremiyetin tanımlanmasının literatürdeki yansımaları aktarılmış ve gözetim toplumu kavramı ile özellikle dijital dünyada mahremiyetin karşılaştığı tehditler ele alınmıştır. Çalışmanın ikinci bölümü Ağ Toplumu ve Dijital Okuryazarlık başlığını taşımaktadır ve ağ toplumuna katılımı, dijital vatandaşlık, dijital okuryazarlık ve dijital beceriler çerçevesinde ele almaktadır. Çalışmanın üçüncü bölümü ise araştırmaya ilişkin metodolojik bilgileri ve elde edilen verilerin sunumunu içermektedir.

Araştırmanın evrenini Kayseri'nin dört merkez ilçesi dışındaki ilçelerinde, 2012'deki yasa değişikliği öncesi köy ve belde statüsünde olan mahallelerinde yaşayan enformasyon ve iletişim teknolojisi kullanıcıları oluşturmaktadır. Bu evreni oluşturan nüfus dağınık bir yapıda olduğu için örneklemin belirlenmesinde iki aşamalı bir yol izlenmiştir. Öncelikli olarak nihai örneklem birimlerini içeren ilçe ve mahalleler küme örnekleme yöntemi ile belirlenmiştir. Ancak örneklemin belirlenmesinde, küme örneklemede öngörülen rastlantısal adımlar izlenmemiş; ilçe gelişmişlik düzeyleri (SEGE), ilçelerdeki mobil sinyal yoğunlukları ve mahalle nüfuslarına dayanan bir amaçlı-kasti- örnekleme uygulanmıştır. Önceki bilgi, deneyim ve gözlemlerden faydalanarak araştırmanın amacına uygun olan birimlerin örnekleme dahil edilmesi (Ural & Kılıç, 2013) ile gerçekleştirilen amaçlı örnekleme sonucu altı ilçe ve on sekiz mahalle belirlenmiştir. Araştırmanın nihai örneklemini ise bu mahallelerde ikamet edenler arasından kolayda örneklem yöntemi ile seçilen 374 katılımcıdan oluşmaktadır.

Araştırmanın verileri, 2021 yılının Ağustos ayında amaçlı örnekleme yöntemi ile belirlenen mahallelerde (köylerde) yüz yüze gerçekleştirilen anketlere dayanmaktadır. Anketler, yüklenici firma tarafından istihdam edilen 7 anketçi tarafından katılımcılara okunarak uygulanmıştır. En önemli avantajı katılımcı ile anketçi arasındaki dolaylımsız kişisel iletişim olan yüz yüze anket uygulaması (Stockemer, 2019) tarama araştırması olarak da isimlendirilmektedir. Yapılan tarama araştırması kesitsel ve geçmişe dönük olarak kategorize edilebilir.

Araştırmada, dijital okuryazarlık, dijital vatandaşlık, mahremiyet yönelimleri ve sosyal medya ve EİT (enformasyon ve iletişim teknolojileri) kullanım sıklıkları beşli likert formatındaki sorularla ölçülmüş; internette bilgi paylaşımları için evet-hayır soruları, cinsiyet ve eğitim gibi bilgiler için çoktan seçmeli sorular ve doğum yılı ile diğer tarih bilgileri için nümerik açık uçlu sorular kullanılmıştır. Yüz yüze yapılan anketler kâğıt yerine tablet bilgisayarlar ile uygulanmış ve katılımcıların cevapları doğrudan cihaza kodlanmıştır. Bu yöntem hem kâğıt israfının önüne geçmesi hem de saha araştırması sonrası yürütülmesi gereken veri girişi adımını ortadan kaldırması açısından önemlidir.

Araştırmada, örneklemin EİT ve sosyal medya kullanım sıklıkları, bu kullanımlarının Covid-19 salgını öncesine göre farklılık gösterip göstermediği, internette

hangi bilgileri paylaştıkları ve paylaşmadıkları, sosyal medya ve anlık mesajlaşma uygulamalarındaki gizlilik ayarlarını değiştirip değiştirmedikleri, akıllı telefonlarında bir şifre kullanıp kullanmadıkları ve ne kadar süredir internet, cep telefonu ve akıllı telefon kullandıkları sorularını cevaplayacak bulgular elde edilmiştir. Elde edilen bu bulgular bağımsız değişkenler olarak değerlendirilerek katılımcıların dijital okuryazarlık düzeyleri ve mahremiyet yönelimleri üzerindeki etkileri incelenmiştir.

Bu tez çalışması, kırsal bölgelerde yaşayan bireyler hakkında betimsel istatistikler sağlaması ve bu bölgelerde yaşayan bireylerin dijital okuryazarlık düzeylerini ölçmeye çalışması açısından önemli bulgular içermektedir.



BİRİNCİ BÖLÜM

MAHREMİYET ve GÖZETİM TOPLUMU

Bu bölümde, öncelikle mahremiyet kavramı ve mahremiyet hakkının tarihsel kökenleri ele alınmış ve çeşitli teorisyenlerin mahremiyete yönelik yaklaşımlarına değinilmiştir. Bölümün ilerleyen başlıklarında ise dijitalleşen dünyada mahremiyete yönelen tehditler kategorik olarak değerlendirmiş, güvende hissetme ve kimlik oluşturup sosyalleşme gibi gerekçelerle kişisel mahremiyetin ikinci plana itildiğine değinilmiştir. Literatürdeki çevrim içi mahremiyete yönelik çalışmalara değinildikten sonra mahremiyet konusu ile ilişkili hukuki düzenlemeler ele alınmış ve son olarak mahremiyetin günümüzde bu derece tehdit altında olmasını açıklamak için temel referans noktalarından biri olan “gözetim toplumu” kavramı olabildiğince kısa bir şekilde aktarılmıştır.

1.1. Mahremiyet

“Mahrem” kelimesi gizliliğe, aile hayatına, kadının sahasına, yabancıнын bakışlarına yasaklanan şeye ilişkindir ve aynı zamanda bir erkeğin ailesi anlamına da gelir (Göle, 2016, s. 20). Bu sıfat aynı zamanda, başkalarına söylenmeyen, gizli ve sırdaş anlamlarını da taşımaktadır. Mahrem gibi Arapça kökenli olan mahremiyet ise gizlilik, kişisel gizlilik anlamı taşımaktadır (Türk Dil Kurumu, 2011, s. 1607). Türkiye Bilişim Şurası Hukuk Çalışma Grubu raporunda ise mahremiyet; “bireylerin, devletin ve diğer kişilerin müdahalesinden muaf olarak hareket edebileceği, yaşamsal faaliyetlerini sürdürebileceği bir alanın ve kişilik haklarına bağlı olan tüm unsurların bütününe verilen ad” olarak tanımlanmıştır (akt. İzgi, 2009, s. 69). Erol Mutlu’nun, Altman’a atıfta bulunarak yaptığı mahremiyet tanımı ise şöyledir:

Bir kişi veya grubun başkalarıyla etkileşimini düzenleyen bir kişilerarası sınır koyma süreci. İnsanın başkalarına açıklık derecesini değiştirmek, bu hipotetik

kişisel sınırın başkalarıyla toplumsal etkileşime açıklık derecesini de belirler. Demek ki mahremiyet ister bir bireyin ister bir grubun olsun kendi sınırı üzerinde seçici denetimini içeren dinamik bir süreçtir. Mahremiyet başkalarıyla kurulan temasın ve ilişkinin derecesini denetlemek amacıyla kişinin çevresindeki sınırları açan ve kapatan düzenleyici bir sürece dayanır. Bireylerin arzuladıkları belli mahremiyet düzeyleri vardır, bu düzeyler sınırsal denetim mekanizmalarına dayanır, bu da kolayca sağlanan mahremiyete yol açar (Mutlu, 2004, s. 205).

1948 tarihli Birleşmiş Milletler Evrensel İnsan Hakları Bildirgesi ve 1950’de kabul edilen Avrupa İnsan Hakları Sözleşmesi başta olmak üzere birçok uluslararası sözleşmede ve ulusal anayasada özel yaşam hakkına ilişkin ayrı ve özel hükümler yer almaktadır (Yüksel, 2003, s. 198). Modern toplumlarda evrensel bir insan hakkı olarak nitelendirilen mahremiyet; kişilerin tek başlarına kalabildikleri, istedikleri şekilde düşünüp davranabildikleri, diğer insanlarla hangi yer, zaman ve koşulda ne ölçüde iletişim kuracaklarına bizzat kendilerinin karar verebildikleri bir alanı ve bu alan üzerinde sahip olunan hakkı ifade eder (Yüksel, 2003, s. 182). Mahremiyet, bireyin başkaları tarafından ne ölçüde tanınıp bilinebileceği, başkaları tarafından fiziksel olarak ne ölçüde ulaşılabilir oldukları ve bireyin başkalarının ilgi ve dikkatinin ne ölçüde nesnesi olduğu hususları ile yakından ilişkilidir (Yüksel, 2009, s. 278).

Mahremiyeti, Conklin (1976, s. 263) ihlal edilmemiş yaşam alanı içerisinde hareket özerkliği; Jourard (1966, s. 307), diğerlerine karşı bir muamma olarak kalma ve başkalarının kendisi hakkındaki algısını kontrol edebilme arzusu, kendini gizleme; Altman (1976, s. 8), bireyin benliğine ya da grubuna erişimi üzerindeki seçici kontrolü; Shils (1966), bilginin birey ve grupların sınırları arasındaki hareketi üzerindeki kontrolü; Wolfe ve Laufer bireyin benlik, nesneler, mekanlar ve bilgi ile davranışları üzerinde uyguladığı kontrol yeteneği; Proshansky, Ittleson ve Rivlin, belirli durumlarda bireyin benliği hakkındaki bilgiyi ne şekilde ve kiminle iletişim kurarken kullanacağına kontrol etmesini sağlayan bireysel seçme özgürlüğü ve Chapin de, kendi başına olabilmenin değeri, diğerlerinin varlığının baskısından kurtulma olarak tanımlar (Altman, 1976, ss. 7-8; Burgoon, 1982, s. 207). Wacks (2010, s. 30), daha genel ve kapsayıcı bir tanım ortaya koyar ve en genel düzeyde, mahremiyet fikrinin, yalnız bırakılmayı, kendimiz olmakta özgür olma arzusunu, başkalarının merakı tarafından engellenmemiş ve kısıtlanmamış olmayı kapsadığını söyler. Göle (2016, s. 90) ise özel yaşam ve mahremiyetin Müslüman

toplumlarda farklı bir şekilde algılandığını ve doğrudan kadın cinselliğine, yasak olana gönderme yaptığını söyler ve bu toplumlarda toplumsal düzenin kadının mahremiyetine göre kurulduğunu ifade eder.

Westin (1967, s. 158), mahremiyet teorisini, insanların başkalarının onlara erişebilme imkanlarından geçici olarak azade kalarak kendilerini korumaları esasına dayalı olarak geliştirmiştir ve mahremiyet hakkını “bireylerin, grupların veya kurumların, diğerleriyle iletişime girdiklerinde kendileri hakkındaki bilgiyi ne zaman, nasıl, ne ölçüde vereceklerini belirleme yetkisi” olarak tanımlar (Yüksel, 2009, s. 278). Birey ve sosyal katılım açısından mahremiyet, bireyin fiziksel ya da psikolojik bağlamda gönüllü ve geçici olarak toplumdan çekilmesidir. Bu geri çekilme, tamamen yalnızlık ya da küçük bir yakın çevre içerisine çekilme veya kalabalık gruplar içerisinde anonim kalma ya da kendini muhafaza etme şeklinde olabilir (Westin, 1967, s. 7).

Altman, mahremiyet ile ilgili kavramsal çerçevesini tanımladığı birkaç kilit unsur üzerine inşa eder: Diyalektik bir süreç olarak mahremiyet hem kendini tamamen izole etmeyi hem de başkalarına açmayı kapsar. Kişilerarası sınırların kontrolü süreci olarak mahremiyet ise sosyal etkileşimin ya da “benliğin geçirgenliğinin, şeffaflığının” düzenlenmesi ve kontrolüdür. Altman’a göre mahremiyet, tekdüze olmayan bir girdi-çıkıtı sürecidir ve çeşitli sosyal birimleri ya da farklı kişi ve grup kombinasyonlarını içinde barındırır. Altman’ın, arzu edilen ve elde edilen mahremiyet (*desired and achieved privacy*) ayrımı da sıraladığı unsurlardan biridir. Bu ayrım “özel olarak arzulanan veya anlık ideal mahremiyet seviyeleri (arzu edilen mahremiyet) ve gerçek çıktılar (elde edilen mahremiyet)” şeklinde yapılabilir. Elde edilen mahremiyet, arzu edilenden az olduğunda, kalabalıklaşma (*crowding*) ya da izinsiz giriş, mahremiyet ihlali (*intrusion*) durumu; arzu edilen mahremiyet, elde edilenden fazla olursa sosyal tecrit durumu (*social isolation*) oluşur (Altman, 1976, s. 27). Altman’ın bu ayrımını, sosyal bilimciler ve kültür eleştirmenlerinin günümüzde açığa çıkarılan ve aşınan mahremiyete getirdikleri açıklamalar ile ilişkilendirilebilir. Bu bakış açısına göre, gençler, yalnız kalma ve toplumdan izole olma korkularından dolayı, düşüncelerini ve özel duygularını ağ üzerinde kamu ile paylaşırlar ve bu paylaşımlarla görünürlük ve ün kazanmayı isterler (van Manen, 2010, s. 1026). Bu örnekte görülen şeyin, Altman’ın ifade ettiği elde edilen mahremiyetin, arzu edilene üstün gelmesinden duyulan endişe olduğu söylenebilir.

Mahremiyet, yukarıda aktarılan tanımlardan anlaşılacağı üzere, farklı bakış açılarından değerlendirilmektedir. Üstelik burada aktarılan tanımlar, geniş literatürde karşımıza çıkan tanımların küçük bir temsilidir. Bu farklı tanımlamalar ve kavramsallaştırmalar mahremiyetin toplumdan topluma, kültürden kültüre, coğrafyadan coğrafyaya, dinden dine farklı şekillerde ele alınması ile ilişkilendirilebilir (Kodak, 2018; Semiz Türkoğlu, 2018). Başka bir ifadeyle, bir toplumda mahremiyet sınırlarının içerisine dahil edilen şeyler, bir diğer toplumda bu şekilde değerlendirilmeyebilir. Bu farklılıklar neticesinde, mahremiyet ve onun sınırlarını belirlemeye çalışan yazarların bir kısmı onu, etkileşimden kaçınma, inzivaya çekilme olarak ele alırken diğerleri ise, bireyin kendisine olan erişimi sınırlandırması, başkalarına kendini açması ya da diğerlerini dışarıda tutması olarak tanımlamaktadır (Altman, 1976; Kalaman, 2017, s. 7). Kültürden kültüre sınırları ve tanım çerçevesi değişen mahremiyet, “panjurları (perdeleri) indirme, kapıyı kilitleme, psikolojik olarak geri çekilme, gözleri kaçırma, gizli yerler kullanma, konuşulan konuya göre ses düzeyini ayarlama, etraftaki kişilerden farklı dil konuşma” gibi basit kültürel yöntemlerle korunmaya çalışılır (Sezen & Erden, 2018, s. 85).

Mahremiyet, çeşitli araştırmacılar tarafından farklı kapsamlar içerisinde ele alınmıştır. Fischer-Hubner’in (1998, s. 422) aktardığına göre mahremiyet üç kapsama sahiptir: bölgesel mahremiyet (*territorial privacy*), bireysel mahremiyet (*privacy of the person*) ve enformasyonel mahremiyet (*informational privacy*). Bölgesel mahremiyet, bireyin yakın fiziksel alanının korunması ile ilgilidir. Bireysel mahremiyet ile bireyin fiziksel aramalar ya da ahlak duygusunu ihlal eden bilgiler gibi gereksiz girişimlere karşı korunması ifade edilmektedir. Enformasyonel mahremiyet ise, bireyin kişisel bilgilerinin ne şekilde toplanacağı, saklanacağı, işleneceği ya da seçici bir şekilde dağıtılacağı üzerinde kontrol sahibi olmasıdır.

Laurie (2002, s. 6) ise, mahremiyeti iki kapsamda ele alır: mekânsal mahremiyet (*spatial privacy*) ve enformasyonel mahremiyet (*informational privacy*). Mekânsal mahremiyet, bireyin fiziki ve psikolojik benliğine erişilmemesi durumuna vurgu yaparken, enformasyonel mahremiyet ise, bireyin kişisel bilgilerinin başkaları tarafından erişilememesi durumunu ifade etmektedir. Bu iki kavrayıştan çıkarılabilecek tanıma göre mahremiyet, diğerlerinden ayrıdır. Fischer-Hubner’in üçlü kapsamı Laurie’deki mekânsal mahremiyetin iki farklı konseptte ayrılmış hali olarak düşünülebilir.

Westin, yukarıdaki kapsamlarından ayrı olarak mahremiyeti farklı bir açıdan ele alır ve dört temel boyut tanımlar: (1) yalnızlık (*solitude*), (2) yakınlık/samimiyet (*intimacy*), (3) anonimlik (*anonymity*) ve (4) ihtiyat (*reserve*). Yalnızlık boyutunda, bireyin etrafındakilerden ayrılarak diğerlerinin gözetiminden kurtulması söz konusudur. Birey bu durumda halen Tanrı veya benzeri güçlerin onu izlediğini ya da otoritenin gizlice onu gözetlediğini düşünebilir olsa da yalnızlık boyutu, bireyin erişebileceği en eksiksiz mahremiyet durumudur. Yakınlık/samimiyet ile bireyin kendisinin belirlediği iki ya da daha fazla kişiden oluşan küçük bir grubun üyeleriyle kurumsal bir inziva içinde kurduğu samimi, yakın ve rahat ilişki ifade edilmektedir. Aile, arkadaş çevresi, iş arkadaşları mahremiyetin bu boyutuna örnek ilişkilerin bulunduğu gruplardır. Anonimlik boyutu, bireyin kamusal alanlarda kamusal performanslar sergilerken gözetlenme ve tanınmadan kaçınmanın bir yolunu bulmasını kapsamaktadır. ‘Mahremiyetin en ince durumu’ olarak ihtiyat boyutu ise, bireyin ‘istenmeyen ihlallere’ karşı kendisini korumak için psikolojik bir bariyer yaratmasıdır (Westin, 1967, ss. 31-32; Kalaman, 2017, s. 8).

Burgoon mahremiyeti fiziksel, psikolojik, sosyal ve enformasyonel olmak üzere dört boyutta ele alır. Fiziksel mahremiyet, bireyin fiziki olarak erişilemez oluşu ya da bunun derecesi ile ilgilidir. Sosyal mahremiyet, bireylerin diğer bireyler ile ya da grupların daha büyük gruplar ile olan temasını kesmeyi seçebilmesidir. Sosyal mahremiyetin içerisindeki dahil etme-dışarda bırakma (*inclusion-exclusion*) konsepti, bir yandan bireyler arasında yakınlığı teşvik ederken diğer yandan da eşzamanlı olarak diğerleri ile arasına mesafe koymaktadır. Bir önceki boyutla ilişkili, hatta onun bir parçası olarak nitelendirilebilen psikolojik mahremiyet, duygusal ve bilişsel girdi-çıktıları kontrol edebilmeyi içermektedir. Burgoon enformasyonel mahremiyetin, psikolojik mahremiyet ile yakınlığını vurgular ve Carroll’ın tanımlaması aktarır: “Kişisel verilerin nasıl, ne zaman ve ne ölçüde başkalarına açılacağını belirleme hakkı.” Bu kişisel bilgiler, kredi kartı harcamaları, eğitim, sağlık, vergi ile ilgili kayıtları ve finansal durum gibi şeyleri içermektedir (Burgoon, 1982, ss. 211-229; Kalaman, 2017, s. 8).

Laufer ve Wolfe (1977), mahremiyete ilişkin herhangi bir durumun üç farklı boyutla tanımlanabileceğini söyler: (1) öz-ego (*self-ego*), (2) çevresel (*environmental*) ve (3) kişilerarası (*interpersonal*). Laufer ve Wolfe’ye göre, herhangi bir özel durumda mahremiyetin anlamı ve mahremiyet deneyimi, bu boyutların ve boyutlara ait öğelerin etkileşimiyle sınırlandırılabilir. Öz-ego boyutu “bireyselleşmeye (özerklik) ve dolayısıyla

kişisel haysiyete odaklanan gelişimsel bir süreci ifade eder.” Araştırmacılar gelişim teorisyenlerinin, benliğin gelişmesinde bireyin sosyal ve fiziksel çevreden ayrılma sürecine yaptıkları vurguyu hatırlatırlar. Çevresel boyut, bireylerin mevcut seçenekleri algılama, edinme ve kullanma becerilerini etkiler. Bu boyut içerisinde yer alan unsurlar anlam ve deneyimin sınırları olarak işlev görürler. Bu unsurlar kültürel anlamlar, sosyal düzenlemeler ile fiziksel ortamlar arasındaki etkileşim ve yaşam döngüsündeki aşamadır. Kişilerarası boyut ise mahremiyetin, hangi biçimde olursa olsun, başkalarının varlığını ve onlarla bir ilişki olasılığını varsayması ile ilişkilidir. Araştırmacılar bu boyutun günlük yaşamdaki mahremiyet olgusunun çekirdeğini oluşturduğunu söylerler ve iki öge tanımlarlar: bilgi yönetimi ve etkileşim yönetimi (Laufer & Wolfe, 1977, ss. 26-33).

Hem bir ihtiyaç hem de bir insan hakkı olan mahremiyet meselesini, gözetim toplumu kavramı ile birlikte ele alacak olan bu bölüme, bu ihtiyacın insanlık tarihinin hangi noktasında belirgin hale geldiğini ortaya koyarak başlanmıştır.

1.1.1. Mahremiyet Hakkının Temelleri ve Gelişimi

“*Mahremiyet: Kısa Bir Tarih*” adlı kitabının başında, David Vincent, on dördüncü yüzyılın mahkeme kayıtlarına geçmiş ilginç birkaç olaya referans verir. Vincent (2017, s. 11), komşularının pencereden ya da yeterince yüksek olmayan bahçe duvarlarından evini izleyebilmesinden şikayetçi olarak dava açan bir kadından bahseder. Kitabın ilk bölümünün adı da mahremiyetin tarihi konusunda bir fikir verir: “Mahremiyetten Önce Mahremiyet 1300-1650.” Bahsi geçen kitabın yazarı bu şekilde ikonik bir örnek ile mahremiyetin tarihini anlatmaya başlamış olsa da bireylerin özel hayatları, mahremiyetleri ile ilgili endişelerinin başlangıcı hakkında önemsiz sayılamayacak bir tartışma söz konusudur.

Avrupa’nın uygarlaşma sürecini kuramsal bir çerçeveye oturtan Norbert Elias, olabildiğince kısa bir şekilde ifade etmek gerekirse, utanma duygusunun ve mahremiyet endişesinin uygarlaşma ile ortaya çıktığını söyler. Uygarlık Süreci adlı iki ciltlik yapıtında (Elias, 2009, 2016), bu tezini desteklemek için özellikle Ortaçağ Avrupası’na ait kaynaklara, resimlere gönderme yapar. Elias’ın savını desteklemek için örnek olarak sunduğu durumlardan biri, soylu bir şövalyenin hizmetçisinin yanında çıplak olmaktan utanmamasıdır. Utanma duygusunun, alt sınıftan kişilere karşı değil, aynı sınıftan ya da üst sınıftan insanlara karşı hissedildiğini söyler. Elias’ın tüm uygarlaşma süreci teorisine

karşı olmasa da özellikle utanma, sıkılma ve mahremiyet ile ilgili düşüncelerine şiddetle karşı çıkan Hans Peter Duerr ise, hem Elias'ın referans verdiği kaynakları yanlış yorumladığını söyler hem de başka kaynaklarla desteklediği antitezini ortaya koyar: Utanma ve sıkılma, çıplaklıktan duyulan utanç ve mahremiyet endişesi, modern ve uygar Avrupa'ya özgü ve orada başlayan bir durum değildir, neredeyse insanlık tarihi kadar eskidir.

Uygarlaşma Sürecinin Miti adıyla beş cilt olarak yayınlanan -sadece iki cildi Türkçeye çevrilen- eserinin özellikle ikinci cildinde Duerr (2004), kadınların erkek hekim karşısında duyduğu utançtan ve jinekolojik muayenenin tabulaştırılmasından başlayarak utanma duygusunun, Elias'ın düşündüğü gibi uygarlığın bir meyvesi olmadığını söyler. Duerr, Ortaçağ'a ait resimlerde "erkek hastaların karşısında oturan erkek hekimlerin" yüzlerinin hastaya dönük olarak resmedildiğini ve kadınların, öteki kadınlar karşısında bile utangaç davrandıklarından hareketle, kadınların erkek hekimlerin karşısında çekingen davranmalarının beklenebileceğini belirtir (Duerr, 2004, s. 82). Utanmanın sadece uygar Batılı toplumlarda görülen bir olgu olmadığını ortaya koymak için Duerr, Türk toplumundan da örneklerle yer verir: "Atatürk döneminden önce, Türk kadınları, bedenlerinin neresinin ağrıdığını anlayabilmesi için hekime gösterdikleri ya da başka bir kadın aracılığıyla gönderdikleri teşhis bebekleri bulunduruyorlardı (Duerr, 2004, s. 85)." Duerr'in Doğu toplumlarından Elias'a karşı sunduğu bir diğer olgu da doğumdur:

Mısırlı bir ebe kadın (daya), kızları doğum yaparken erkek ebe çağırmaktansa, kızlarını ölüme terk etmeyi tercih eden çok sayıda anne tanıdığını söylüyor; Kahire'de yayımlanan bir basın bildirisine göre, altmışlı yılların başında, Siva Vahası'nda lohusa kadınların %35'i, yanlarına bir hekimin gelmesini istemedikleri için ölmüştür. Suudi Arabistan'ın doğusundaki Acıman'dan bir erkek, karısının bir erkek ebeyi reddettiği için doğum sırasında öldüğünü memnuniyetle bildirdi: karısı bir zamanlar bedenini, kocası olmayan bir erkeğe gösterdiği için, kıyamet gününde yaratıcısının karşısında yüzünün kızarmasını istememişti (Duerr, 2004, s. 86).

Elias, uygarlaşma sürecinin çarklarından biri olarak değerlendirdiği iş bölümündeki artışın, sürekli olarak daha fazla insanı, gittikçe daha geniş beşeri alanları birbirine bağımlılık ilişkisine soktuğunu; tekil insanın daha fazla geri durmasını, davranışının ve fevriyetlerinin daha kesin bir düzenlenişini, güdülerinin daha fazla

bağlanmasını istediğini ve bu durumun da daha sürekli bir kendini zorlamayı gerektirdiğini söyler (Elias, 2009, s. 398). Duerr ise, Uygarlaşma Sürecinin Miti adlı eserinin ilk cildinde, küçük ve geleneksel topluluklardaki insanların, kendi gruplarının üyeleriyle bugün alışık olduğumuzdan çok daha yakın bağlar ve ilişkiler kurduklarını göstermeyi amaçladığını belirtir ve şöyle devam eder: “İnsanlar, bugün olduğu gibi, ötekinin toplam kişiliğinin parçalarıyla karşı karşıya kalmıyorlar, aksine tüm kişiliğiyle muhatap oluyorlardı, bu yüzden de bireyin hatalı bir davranışı, günümüzün büyük şehirlerinin yaşamında olduğundan çok daha utanç verici sonuçlar doğurabiliyordu (1999, s. 12).” Duerr’in küçük ve geleneksel topluluklarla ilgili bu görüşü, kırsal yaşamı odağına alan bu tez çalışması için önemli bir hareket noktasıdır.

Bireylerin, kendi başlarına kalabilmeleri ve kendilerine ait bir özel alana sahip olmaları da mahremiyetleri ile ilişkilidir. Elias, geleneksel ve ilkel toplumlarda bu tip alanların eksikliğine değinir. Duerr, Peru’nun kuzeydoğusundaki ormanlarda yaşayan Yagualardaki bir âdeti Elias’a karşı sunar. Bütün ailelerin ne ara duvarları ne de paravanları olan büyük bir evde birlikte yaşadıkları Yagualarda, ilk bakışta bir mahremiyet ortamı olmadığı düşünölebileceğini ve bunun Elias’ın savına kanıt gibi değerdendirilebileceğini söyleyen Duerr, bu ilk izlenimin yanıltıcı olduğunu şu şekilde açıklar:

Yagualar ihtiyaçları olan özel alanı -çıplak yıkanan Japon kadınların ‘hayali giysisi’ gibi- ‘hayali duvar’ denen şeyle oluştururlar. Bir erişkin ya da bir çocuk yalnız kalmak istediğinde, karakteristik bir tavırla evin palmye yapraklarından örölmüş duvarına yaslanır. Bu duruşu aldığında, artık ‘mevcut değildir’ ve acil durumlarda bile kendisine hitap edilmez, hatta bakılmaz (Duerr, 1999, s. 147).

Bakmayarak sağlanan özel alan, alışılmışın oldukça dışında görünse de modern toplumda da benzer bir durum söz konusudur. Büyük şehirlerde birbirini tanımayan yüzlerce insanın aynı otobüsü, treni ya da restoranı paylaşırken etrafındakilere karşı sergiledikleri tutum, modern toplumdaki “hayali duvarlar” olarak değerdendirilebilir. Bu, aynı zamanda Erving Goffman’ın “uygar kayıtsızlık” (*civil inattention*) şeklinde kavramsallaştırdığı durumdur (Goffman, 2017).

Duerr, insan türünün “yarı sosyal” oluşu ve cinsel birliktelikler açısından da “karmakarışık eşli olmayışı”, içinde yaşadığı toplumsal alanı kamusal ve özel olarak ikiye

ayırmasının insanın özünde bulunduğu anlamına geldiğini söyler ve dışlayıcılığın aşkın özündeki varlığını hatırlatarak (“herkesi eşit ölçüde sevseydik “aşk” kavramı anlamını yitirir, Wittgenstein’in deyişiyle “dönmeyen” bir tekerleğe benzerdi”), toplumsal yaşamın belirli alanlarına erişimin denetlenmesinin de insani kimliğe dahil olduğunu öne sürer (Duerr, 2004, ss. 215-216). Başka bir şekilde ifade edilmesi gerekirse, kamusal alan – özel alan ayrımı, Elias ve onu takip edenlerin savladıkları gibi, Batı uygarlığının “nispeten geç bir ürünü” değildir. Tamamıyla şeffaf bir toplumun ya da mahremiyetin olmadığı bir toplumun, anlamlı sosyal ilişkilerden yoksun bir toplum olacağı söylenebilir (Roessler & Mokrosinska, 2013, s. 785).

Privacy and Freedom adlı kitabında Alan Westin de (1967, s. 7), Duerr’in çalışmasından yaklaşık yirmi yıl önce, modern mahremiyet iddiasının insanların hayvan atalarının yaşayışları ile ortak temellere sahip olduğunu ve Amerikan toplumunda şu an kabul edildiği şekliyle mahremiyetin (bireylerin ve grupların özel aktivitelerinin başladığı yerde otoritenin gözetim gücü sınırlandırılır) Antik Yunan toplumuna kadar götürülebileceğini ifade eder. Hatta mahremiyetin insanlık tarihi kadar eski olduğu, ancak modernleşme süreci ile dönüşüme uğradığı söylenebilir. Kodak (2018, s. 93), mahremiyetin sınırlarının ve içeriğinin toplumdan topluma, coğrafyadan coğrafyaya değişe de ihtiyaç duyduğu temel birimin birey olduğunu söyler ve modern öncesi toplumlarda bireyin içinde yaşadığı toplumdan ya da gruptan soyutlanıp öznel bir kimlik oluşturamadığını hatırlatır. Ancak bu, (Duerr’in de üzerinde durduğu gibi) mahremiyetin modernizm süreci ile ortaya çıktığı anlamına gelmez. Kodak’a göre mahremiyet, modernite ile “en yalın ifade ile geleneksel kodlardan sıyrılarak başka bir forma” bürünür.

Vincent, toplumun diğer üyelerini şahsi duygu ve bilgi kayıtları yönetiminden uzaklaştırmayı amaçlamak olarak mahremiyetin ne zaman başladığına ilişkin olarak post-reformasyon dönemindeki kişiye özel ibadet alanı tartışmalarını gündeme getirir. Dönemin püritenlerinin günlüklerinden edinilen izlenime göre, cemaat ya da hane halkı ile birlikte yapılan ibadetlerin aksine “tanrı ile konuşurken mekânsal tecrit ihtiyacında” bir ısrar söz konusudur (Vincent, 2017, s. 31). İbadet edebilmek ya da kendi başına vakit geçirebilmek için ihtiyaç duyulan özel alanla ilgili olarak, İngiliz feminist, romancı, eleştirmen Virginia Woolf’un “Kendine Ait Bir Oda” adlı çalışmasına burada değinmek gerekir. Kadın hakları konusunda çalışan Woolf (2017, s. 59), on dokuzuncu yüzyılın başlarına kadar, ailesi olağanüstü zengin ve/veya soylu olmadıkça bir kadının “sessiz ya

da ses geçirmeyen bir odası olması bir yana, yalnızca kendine ait bir odaya sahip olması bile olanaksızdı” diye yazar. Özel alan ihtiyacının ve özel alana sahip olabilmenin avantajlarını hayal gücünü kullanarak oluşturduğu, Shakespeare’in kız kardeşi metaforu üzerinden anlatır (Woolf, 2017). Kendine ait bir odası olan Shakespeare ile onunla aynı yeteneklere sahip, ancak aynı imkanları kullanamayan kız kardeşinin yaşamlarının ne şekilde seyrettiğini ortaya koyarak mahremiyet ihtiyacı ile yaratıcı süreç arasında bir ilişki kurar.¹ Her ne kadar Woolf, bu bağlantıyı kadın haklarına dikkat çekmek için kurmuş olsa da bu durum birkaç yüzyıl öncesinde erkekler için de geçerlidir.

¹ “Nasıl olursa olsun, Shakespeare’in raftaki yapıtlarına bakarken, piskoposun en azından bu konuda haklı olduğunu düşünmeden edemedim; bir kadının Shakespeare’in çağında Shakespeare’in oyunlarını yazmış olabilmesi her yönüyle ve tümüyle olanaksızdı. Gerçek verilere ulaşmak olağanüstü güç olduğundan, izin verin, düş gücümü harekete geçirip Shakespeare’in Judith adında son derece yetenekli bir kız kardeşi olmuş olsaydı neler olurdu diye şöyle bir tahmin yürütmeye çalışayım. Shakespeare büyük olasılıkla liseye gitmiş, Latince -Ovid, Virgil ve Horace- ve gramer ile mantık üzerine bilgi edinmişti, çünkü annesine yüklü bir miktar miras kalmıştı. Çok ve iyi bilindiği gibi tavşan avlayan, belki de geyik vuran ele avuca sığmaz bir oğlandı ve yapması gerekenden çok daha önce, kendisine normalden çok daha kısa bir sürede çocuk doğuran, komşu çevrelerden bir kadınla evlenmek zorunda kalmıştı. Bu felaket, onun şansını denemek için Londra’ya gitmesiyle sonuçlandı. Tiyatrodan hoşlandığı anlaşıyor; bu işe sahne kapısında at tutmakla başladı. Kısa sürede tiyatrodan iş bulup başarılı bir oyuncu oldu ve dünyanın merkezinde yaşamaya başladı; artık herkesle karşılaşılıyor, herkesi tanıyor, sanatını tahtaların üzerinde uyguluyor, zekasını sokaklarda kullanıyordu; kraliçenin sarayına giriş hakkını bile elde etti. Bu arada, olağanüstü yetenekli kız kardeşinin evde kaldığını varsayalım. O da aynı ölçüde maceracı, aynı ölçüde yaratıcıydı ve dünyayı tanımak için aynı ölçüde yanıp tutuşuyordu. Ama okula gönderilmedi. Horace ve Virgil okumak bir yana gramer ve mantık okumak gibi bir olanağı dahi yoktu. Arada bir eline bir kitap, belki de erkek kardeşininkilerden birini alıp birkaç sayfa okuyordu. Tam o anda annesi ya da babası içeriye girip çorapları yamamasını ya da pişen türlüye bakmasını ve kitap kağıtla oyalanmamasını söylüyordu. Sert ama şefkatle konuşuyorlardı, çünkü bir kadın için yaşam koşullarının ne denli zorlu olduğunu bilen ve kızlarını seven dürüst insanlardı - hatta büyük bir olasılıkla Judith, babasının gözbebeği idi. Belki de bir elma ambarında gizlice birkaç satır karalamış ama yazdıklarını özenle saklamak ya da yakmak durumunda kalmıştı. Ne var ki, daha yirmisine varmadan tanıdık bir yün tüccarıyla arasında söz kesildi. Evlilikten nefret ettiğini haykırdığı için babası tarafından dövüldü. Sonra babası onu azarlamaktan vazgeçti. Bunun yerine kendisini incitmemesi, bu evlilik meselesinde onu utandırmaması için kızına yalvardı. Ona bir dizi boncuk ya da güzel bir etek vereceğini söyledi; gözlerinde yaşlar birikmişti. Judith ona nasıl karşı koyabilirdi? Babasının kalbini nasıl kırabilirdi? Ancak yeteneğinin gücü onu buna zorluyordu. Eşyalarını küçük bir çıkına koyup bir yaz akşamı ipe pencereden aşağı indi ve Londra’nın yolunu tuttu. Henüz on yedisinde değildi. Çalılıklarda ötüşen kuşların sesi kulağa onun sesi kadar hoş gelmezdi. Erkek kardeşininki gibi bir yeteneğe, sözcüklerin uyumu konusunda son derece canlı bir imgeleme sahipti. Yine kardeşi gibi tiyatrodan hoşlanıyordu. Sahne kapısına dikilip oynamak istediğini söyledi. Adamlar gülüp onunla alay ettiler. Şişman, ağzı bozuk bir adam olan tiyatro müdürü kaba bir kahkaha savurdu. Kanişlerin dans etmesi ve kadınların oyunculuk yapmasıyla ilgili bir şeyler böğürdü, hiçbir kadın tiyatro oyuncusu olamaz dedi. Bir şeyler çıtlattı - ne olduğunu tahmin edebilirsiniz. Sanatında eğitim görmesi mümkün değildi. Akşam yemeği için bir tavernaya gidip geceyarısı sokaklarda dolaşabilir miydi? Ne var ki yazarlık dehası kıza rahat vermiyor, erkeklerle kadınların yaşamlarını ve huylarını inceleyerek açlığını doyurmak için yanıp tutuşuyordu. Sonunda -yüzü inanılmaz biçimde Shakespeare’e benziyordu; aynı çelik mavisi gözler, aynı kavisli kaşlara sahipti- en sonunda oyuncu menajer Nick Green, ona acıdı; Judith bu beyefendiden hamile kaldığını öğrendi ve böylece -bir kadın bedeninde kısıtılıp kalmış bir şair ruhunun şiddetini ve ateşini kim ölçekbilir?- bir kış gecesi canına kıydı ve şimdi otobüslerin durduğu bir kavşakta gömülü yatıyor.” (Woolf, 2017, ss. 53-55)

Woolf'un sıra dışı örneğinin ardından, Altman ve Westin'e göre mahremiyetin sahip olduğu işlevlere değinilebilir. Altman'a (1977, s. 68) göre mahremiyetin üç işlevi vardır: sosyal etkileşim yönetimi (*management of social interaction*), başkalarıyla etkileşim için plan ve stratejilerin oluşturulması (*establishment of plans and strategies for interacting with others*) ve öz kimliğin geliştirilmesi ve sürdürülmesi (*development and maintenance of self-identity*). Westin'in (1967, s. 32) mahremiyete atfettiği işlevler ise, (1) bireysel özerklik (*personal authonomy*), (2) duygusal rahatlama (*emotional release*), (3) kendini değerlendirme (*self-evaluation*) ve (4) sınırlı ve korumalı iletişimdır (*limited and protected communication*).

Mahremiyetin bireysel özerklik ya da bireysel otonomi işlevi, demokratik toplumlardaki bireylerin biricikliğine, benzersizliğine olan inanış ile ilgilidir. Bireyin benzersizliğini elde edebilmesi için kendisi ile ilgili kararlarını kendi verebilmesi, başka bir ifade ile özerk olması gerektiği düşünülmektedir. Westin, bireysel özerklik ile mahremiyeti ilişkilendirmek için Erving Goffman'ın 'alanlar ve bölgeler' (*zones and regions*) kavramlarına başvurur. Bireylerin bu alan ve bölgelerde uyguladığı mahremiyet öz benliği mümkün kılar. Bireyin otonomisine yönelik en ciddi tehlike, bireyin öz benliğini oluşturan alanlara "girilmesi" ve en gizli sırlarının açığa çıkmasıdır. Bireyin özerkliğini sağlayan mahremiyet, aynı zamanda bireyselliğin ve bilinçli bireysel tercihlerin geliştirilmesinde de rol sahibidir. Westin, Young'un şu tespitini aktarır: "Mahremiyet olmazsa, bireysellik de olmaz. Sadece belli tipler olur. Düşünceleri ve duyguları ile asla baş başa kalma fırsatı olmayan birinin neler düşünüp neler hissedeceğini kim bilebilir? (Westin, 1967, ss. 33-34)"

Westin'in bireysel özerklik olarak nitelendirdiği işlevi, kişilik bütünlüğü ile ilişkilendirilebilir. Norveç'te oluşturulan Mahremiyet Komisyonu, "mahremiyetin, pek çok durumda, kişilik bütünlüğü için kullanılan bir diğer sözcük olduğunu öne sürer (Løkke, 2018, s. 24)."

Mahremiyetin ikinci işlevi duygusal rahatlama"dır. Toplum içinde yaşamının yarattığı gerginlik, bireyin hem fiziksel hem de psikolojik sağlığı için duygusal bir rahatlama'yı gerekli kılar. Bireyin böyle bir rahatlama'yı yaşayabilmesi için mahremiyete ihtiyacı vardır. Bireyin sürekli olarak bir sosyal rolü "oynadığı" tezinden hareketle, zaman zaman bu rolleri bir kenara bırakıp rahatlama'sı gerektiği düşünülür. Goffman

(2014, s. 77), “tüm dünya tabii ki bir sahne değildir, ama tam olarak neden böyle olmadığına parmak basmak pek de kolay değildir” cümlesiyle bireyin toplum içerisinde sürekli olarak sosyal bir sahnede olduğunu ifade eder. Ancak birey sahnelediği bu rolleri makul süreler boyunca sürdürebilir ve hiç kimse bu rolleri herhangi bir kaçış veya bir rahatlama yaşamadan sürdüremez (Westin, 1967, s. 35). Goffman, bu kaçışın gerçekleşmesi için “arka bölge” ya da “sahne arkası” (off stage) alanının gerekliliğini vurgular. Goffman, sahne arkasını şu şekilde tanımlar:

Arka bölgeyi ya da sahne arkasını belli bir performans tarafından çizilen izlenimle çelişen bir görüntünün yer aldığı bölge olarak tanımlayabiliriz. Bu tür yerlerin kuşkusuz pek çok karakteristik işlevi vardır. Bir performansın kendi ötesinde bir şeyler ifade edebilme becerisi bin bir zahmetle burada geliştirilir; yanılsamalar ve izlenimler adeta tüm repertuvarların ve karakterlerin adeta sıkıştırılmış bir toplamı halinde burada depolanabilir. Farklı türde törensel aletler, örneğin farklı türde içkiler veya giysiler, seyirci kendilerine nasıl davranıldığı ile kendilerine aslında nasıl davranılabileceği arasında bir karşılaştırma yapmasın diye burada gizlenir. [...] Kostümler ve kişisel vitrinin diğer parçaları burada ayarlanabilir ve kusurlar için gözden geçirilebilir. [...] Oyuncu burada rahatlayıp vitrinini ve dizelerini bir kenara bırakabilir, oynadığı karakterden çıkabilir (Goffman, 2014, s. 112).

Mahremiyetin işlevi olarak duygusal rahatlama, bireylerin yaşantılarındaki kayıp ya da şok anlarında ya da kederlendiklerinde de önemli bir role sahiptir. Bu gibi anlarda toplum hem arkadaşların veya yakın çevrenin bir araya gelerek sağladığı toplumsal destek ile hem de bireyin ve yakın çevresinin mahremiyete gösterdiği saygı ile rahatlık sağlar (Westin, 1967, s. 36).

Mahremiyetin üçüncü işlevi olan kendini değerlendirme, bireylerin kişiliklerini farklı durumlara uyarlayabilmek için deneyimlerini anlamlı bir örüntüye yerleştirme ihtiyacı ile açıklanabilir. Entelektüel düzeyde, kişinin maruz kaldığı kesintisiz enformasyon akışı sırasında bir değerlendirmenin yapılamayacağı, mahremiyetin sağladığı bir değerlendirme anına ihtiyaç duyulur. Alan Bates, mahremiyetin bireyin aldığı enformasyonu değerlendirmesini, alternatifleri ve potansiyel sonuçları dikkate almasını ve böylece olabildiğince tutarlı ve uygun bir şekilde davranmasını mümkün kıldığını söylemiştir (akt. Westin, 1967, s. 36).

Westin, sınırlı ve korumalı iletişimi, mahremiyetin dördüncü işlevi olarak nitelendirir. Bu işlev, bireyler arasındaki iletişimin kısmi ve sınırlı olmasına dayandırılır. Bireyin diğerleri ile iletişimde tamamen samimi olması, bildiği ve hissettiği her şeyi başkalarına söylemesi uygarlaşmış sosyal toplumlar için en büyük tehdittir (Westin, 1967, s. 37). Duerr'e (2004, ss. 216-217) göre de samimi iletişimin çok fazla insanla aynı anda sürdürülmesinin, ya da özel alanın çok fazla insanın erişimine açılmasının anlamı, çevrenin basitçe genişlemesi değil, insani kişiliğin temelden değiştirilmesidir: "Bizler ne monad ne de sürü hayvanı olduğumuza göre, özel alanın korunması yönünde bize özgü, derinlerde kök salmış bir ilgimiz vardır." Westin, sınırlı ve korumalı iletişim işlevinin iki yönü olduğunu söyler. İlki, bireye güven ve yakınlığı eşi, ailesi, arkadaşları ve yakın meslektaşları gibi güvенеbileceği kişilerle paylaşma imkânı vermesidir. İkinci yönü ise, en samimiden en resmi ve kamusal durumlara kadar tüm kişisel ilişkilerdeki zihinsel mesafenin gerekli sınırlarını oluşturmayı sağlamasıdır (Westin, 1967, s. 38). Bu işleve paralel olarak Rachels (1975, s. 329), bireylerin kendilerine kimin erişiminin olacağını, kimin kendileri hakkında neleri bileceğini kontrol etme yeteneğinin, diğer insanlarla çeşitli ilişkiler sürdürmelerini sağladığını ve bunun mahremiyeti önemsememizdeki en önemli nedenlerden biri olduğunu söyler.

Temel bir insan hakkı olarak mahremiyet ile ilgili olarak Manning (1997, s. 817), John Rawls'un "*A Theory of Justice*" adlı çalışmasında doğrudan mahremiyetten bahsedilmediğini, ancak konu hakkında bazı çıkarımlar yapılabileceğini söyler. Rawls'a göre, rasyonel bireylerin birbirlerinden çarpıcı biçimde farklı yaşam planları olabilir ve bu tür planlar kimi doğruluk veya haklılık standartlarına uyduğu sürece, herhangi bir sıralamaya ya da derecelendirmeye tabi tutulamazlar. Çünkü adil bir toplum, bireylerin farklı yaşam planlarını gerçekleştirmelerine engel olmak istemez. Bu toplumda, basit bir "iyi teorisi"nin benimsenmiş olması, bireyler için neyin "iyi" olacağına ilişkin bir standardın bulunması ve bireylere de bizzat kendi iyilerini belirlemek için olabildiğince fazla fırsat tanınması gerekmektedir. Rawls, aynı zamanda, "öz saygı ve kişinin kendisinde gördüğü öz değer hissi, belki de en önemli birincil iyidir" der (akt. Manning, 1997, s. 818). Bu noktada, mahremiyete yönelik ihlaller, bir kimsenin kendi iyilerini ya da doğrularını gerçekleştirmesine ya da sürdürmesine müdahale anlamına gelir ve böylelikle, kişinin öz saygısını veya kendisine biçtiği değeri zayıflatır (Yüksel, 2009, s. 283).

“Mahremiyet Hakkına ve Bireysel Özgürlüklere Felsefi Yaklaşımlar” adlı makalesinde Yüksel (2009), liberal ve komüniteryan yaklaşımlarda mahremiyet hakkının ne şekilde değerlendirildiğini, toplumu ve bireyi kavrayış biçimleri üzerinden ele alır. Liberal yaklaşımda, “genel olarak zaman ve mekân bağlamından koparılmış bir “soyut birey” anlayışından hareketle “birey” ve “bireysel özgürlük” kavramları (2009, s. 295)” merkezi konumdadır ve kamunun müdahalelerinden tamamı ile bağımsız bir özel hayat alanı ve mahrem alan kavramsallaştırması vardır. Bu yaklaşım içerisinde özel alan, liberal bir toplum içerisinde yaşayan bireylerin istedikleri şekilde düşünebildikleri ve davranabildikleri alandır. Liberal düşüncede, özgürlük, otonomi ve mahremiyet hakkı gibi değerlere büyük önem verilir. Bu değerler “kişilik değerlerinin dokunulmazlığı” ya da “dokunulamaz kişilik” ilkesinin bir gereği sayılır ve bu bağlamda bireyin, içsel ya da özsel bir değere sahip olduğu savunulur. Komüniteryan yaklaşımda ise, özel alan ve mahrem alan tamamen yok sayılmasa da diğer yaklaşıma kıyasla ikinci plana itilir. Bu yaklaşım, kamu yararı, toplumsal duyarlılık ve sosyal sorumluluk gibi kavramları temeline yerleştirerek bir kuramsal çerçeve sunar. Bu çerçevede, sınırsız ve bağımsız bir özel alan ve mahrem alandan söz edilemez. Çünkü komüniteryan yaklaşımda birey, içinde doğduğu, yetiştirildiği ve yaşadığı toplumdan ayrı düşünülemez ve bireysel özgürlükler toplumsal çıkarların önüne geçemez.

Mahremiyet hakkının sınırlarını belirlemede, liberal ve komüniteryan yaklaşımlar arasındaki bu farklılığın, bir bakıma üstesinden gelmek ve kamu yararı ile mahremiyet hakkı arasında bir denge yakalayabilmek için Amital Etzioni bir başvuru standardı oluşturmaya çalışır. Servis şoförleri, uçak pilotları gibi diğerlerinin hayatlarını bir bakıma ellerinde tutan mesleklerde çalışanlara uygulanan zorunlu testlerden hareketle başladığı makalesinde Etzioni, mahremiyet hakkının sınırlandırılabilmesi için dört kriter ortaya koyar. Bunlardan ilki, özgür bir toplumda mahremiyetin sadece iyi belgelenmiş ve farazi olmayan makro düzeydeki tehlikelerle karşı karşıya kalındığında sınırlandırılmasıdır. İkinci kriter, kamu yararı için gerekli olduğuna karar verildikten sonra, ihtiyaç duyulan bilgilere, kişilerin mahremiyet haklarını ihlal etmeksizin erişilip erişilemeyeceği tartışmasıdır. Etzioni burada, sağlık kuruluşlarındaki tıbbi kayıtların, kimlik ve tanımlayıcı verilerden ayrı olarak incelemeye sunulabileceği örneğini verir. Üçüncüsü, mahremiyet hakkına yönelik sınırlamaların olabildiğince en düşük düzeyde kalması gerektiğidir. Bu kriter için Etzioni’nin örneği, uyuşturucu testleri ve benzeri

uygulamaların, sadece diğerlerinin hayatlarından doğrudan sorumlu olan kişilere (servis şoförleri ve pilotlar gibi) uygulanması gerektiğidir. Son kriter ise, mahremiyet hakkını zorunlu olarak sınırlandıran önlemlerin yan etkilerinin görmezden gelinmesi yerine, bu etkileri önlemeye yönelik tedbirler uygulanmasıdır (Etzioni, 2000, s. 24).

Yüksel, (yukarıda değinilen) çalışmasını, mahremiyet hakkı çerçevesinde yapılan tartışmaların artık birey - devlet, birey - toplum, bireysel çıkar - kamu yararı, bireysellik - kamusalılık gibi ikilemlerin ötesine taşınması gerektiğini ifade eder. Ayrıca, “gerek birey gerekse devlet ve toplum içinde ve karşısında devasa güce kavuşmuş, ulusal ve uluslar ötesi düzeyde etkinlik gösterir hale gelmiş şirketlerin, sivil toplum örgütlerinin, meslek kuruluşlarının, siyasal partilerin, sendikaların ve benzeri örgütlü güçlerin de” bu tartışmalara eklenmesinin önemli olacağını vurgular (Yüksel, 2009, s. 296). Norveç’te 2009 yılında hazırlanan bir raporda da mahremiyet hakkının hem bireysel özgürlük hem de kolektif fayda olarak görülmesi gerektiği öne sürülür (Løkke, 2018, s. 23).

Mahremiyete yönelik tehditleri ele almadan önce, mahremiyet hakkının veya bir hak olarak mahremiyetin temellerini ve hukuki olarak tanımlanması sürecini özetlemek uygun düşecektir. Duerr’ci bir bakış açısı ile bireylerin mahremiyet ihtiyacı -Elias’ın savunduğunun aksine- Batı uygarlığının bir ürünü değildir. Farklı şekillerde de olsa hem İslam toplumlarında hem de kimi ilkel kabilelerde, bireylerin mahremiyetlerine karşı bir hassasiyet bulunduğu söylenebilir. Ancak, modernleşme ile artan bireycilik ve kamusal/özel alan ayrımı, mahremiyeti daha belirgin bir ihtiyaç ve bir insan hakkı haline getirmiştir. Bu noktada Westin de, antropolojik literatüre dayanarak, ilkel topluluklardan modern topluluklara doğru ilerlemenin hem fiziki hem de psikolojik bağlamda mahremiyet ihtimallerini artırdığını söyler ve ekler: “Ancak, modern toplumlar, mahremiyetin bu başarısına karşı çalışacak gelişmeleri de beraberinde getirmiştir: nüfus yoğunluğu ve kalabalık toplumlar, büyük bürokratik örgütsel yaşam, popüler ötekileştirme modları ve güvensizlik (Westin, 1967, s. 21).”

Mahremiyetin hukuksal olarak kavramsallaştırılmasında 1890 yılında kaleme alınan *Mahremiyet Hakkı (The Right to Privacy)* adlı makale, yol gösterici olarak nitelendirilebilir. Değişen toplum koşullarının, özel alanla ilgili anlayışın değişimine katkısını çıkış noktası olarak belirleyen Warren ve Brandeis (1890, s. 193), bu makalelerinde politik, sosyal ve ekonomik gelişmelerin yeni hakların tanımlanması ile

sonuçlandığını söylerler. O dönemdeki yeni icatların ve iş yöntemlerinin bireyi korumak ve -Yargıç Cooley’in deyimi ile- “yalnız kalma hakkını” (*right to be let alone*) korumak için atılması gereken bir sonraki adıma dikkat çektiğini söylerler. Yazarlar, o dönemin yeni teknolojisi olan anlık fotoğrafların ve gazete girişimlerinin özel ve ev hayatının kutsal bölgelerini istila ettiğini de vurgularlar (Warren & Brandeis, 1890, s. 195). Yazarlar, kişisel bilgilerin mahremiyeti ihlal edecek şekilde paylaşılmasını engellemek için temel esaslar geliştirmeyi amaçlamışlardır. Makalenin bu denli önemli addedilmesinde ise, yazarların mahremiyeti ihlal edebilecek bilgilerin aynı zamanda kamu yararına olabileceğini ve bu gerekçe ile paylaşılabilirliğini düşünmeleridir (Løkke, 2018, s. 20). Bu makalede mahremiyete yönelik, kişinin kendisinden kaynaklanmayan, gizlice fotoğrafının çekilmesi ve gazetede yayınlanması gibi tehditler sorunsallaştırılmıştır. Ancak yeni medya teknolojilerinin yaygınlaşması mahremiyete yönelik tehditlerin kaynağını da çeşitlendirmiştir. Yazarların kamu yararı ve özel hayat arasındaki ilişki hakkındaki kavrayışları halen güncel tartışmaları beslemektedir.

1.1.2. Mahremiyete Yönelik Tehditler

Mahremiyete yönelik tehditleri, dijital dünyadan ayırarak, farklı bir başlıkta ele almanın zor olduğu söylenebilir. Çünkü yeni iletişim teknolojileri ve internetin gündelik hayat pratikleri içerisindeki rolü büyüdükçe, bu teknolojilerin mahremiyete yönelik tehditleri de artmaktadır. Başka bir şekilde ifade edilirse, enformasyon ve iletişim teknolojileri bireyin mahremiyetini koruması için çeşitli imkânlar ve araçlar sunsa da bu, mahremiyete yönelik belki de en büyük tehdidi de oluşturmaktadır. Yine de mahremiyete yönelik tehditleri, farklı bir bakışla ele almak doğru olacaktır. Bu doğrultuda, Alan Westin’in (1967), yirmi birinci yüzyılın enformasyon ve iletişim teknolojilerinin yaygınlaşmasından çok önce kaleme aldığı *Privacy and Freedom* adlı kitabına başvurulabilir. Bu çalışmasında, Westin mahremiyete yönelik tehdit kaynaklarını şu şekilde sıralar: (1) kendini açığa vurma (*self-revelation*), (2) merak (*curiosity*) ve (3) gözetim (*surveillance*).

Kendini açığa vurma, bireyin mahremiyet alanı içerisinde değerlendirilebilecek kişisel bilgileri kontrolsüzce başkaları ile paylaşması olarak ifade edilebilir. Simmel, bireyin kendisini etrafındakilere çok fazla açık etmesinin ilişkilerini bozacağını ve özel hayattan söz edilemeyeceğini vurgular. İhtiyatını (*reserve*) kaybeden bireylerin sayısının artması ise, diğerlerinin “ağzı sıkılığı” etkileyebilir ve her şeylerini anlatanlar

diğerlerine de her şeyi sormaya başlayabilirler. 1960'lı yıllarda kaleme aldığı çalışmasında Westin, mahremiyet üzerinde çalışan yazarların “kendi mahremiyetini ihlal etme” trendinin (*self-invasion*) Amerikan toplumunda tehlikeli boyutta yükseldiğinden yakındığını belirtmiştir. Bu yakınmalarının dayanağı ise insanların kamuoyu araştırmalarına ve davranış araştırmalarına verdikleri açık cevaplardır. Amerikan vatandaşlarının, anketi uygulayan kişilerle bilgilerini paylaşma eğilimleri konusunu irdelemek için Westin, alanında lider olan araştırma şirketlerine danışmış ve onlardan son yirmi yılda insanların, aylık gelirleri, cinsel davranışları, politik ve dini inançları ve adli sicil kayıtları gibi kişisel bilgilerini paylaşma istekliliklerine dair trendleri talep etmiştir. Elde edilen veriler ışığında, insanların paylaşmayı en çok reddettikleri konular, gelir ve para ile ilgili olmuştur. Kadınlarda yaş, düşük eğitilmiş bireylerde ise eğitimsel arkaplan yine paylaşmaktan çekinilen konulardır. Westin, kişisel bilgileri paylaşma istekliliğinin son yirmi yılda sürekli bir artış içerisinde olduğunu söylemiştir ve anket şirketlerince toplanan verilerin, insanlar tarafından mahremiyetlerinin ihlali olarak görülmediğini, esas problemin sahte anketler kullanan satıcıların elde ettikleri bilgileri ticari amaçlarla kullanmaları olduğunu eklemiştir (Westin, 1967, ss. 52-53).

Mahremiyete yönelik bir tehdit olarak kendini açığa vurma ile ilgili, Sydney Jourard'ın geliştirdiği “kendini ifşa etme anketi” (*self-disclosure questionnaire*) ile verilerini topladığı ve dört farklı grup üzerinde (beyaz erkekler, beyaz kadınlar, zenci erkekler ve zenci kadınlar) gerçekleştirdiği çalışmasında şu sonuçlara ulaşmıştır: Örneklemi oluşturan kişilerin, kendilerini ifşa ettikleri kişiler farklılık göstermektedir. Bireyler çoğunlukla kendilerini anneye “ifşa” ederlerken; baba, erkek ve kız arkadaşlarına daha az ifşa etmektedirler. Ifşa edilen konular da farklılık göstermektedir. Jourard, benliğin yönlerinin (*aspects of self*) yüksek ifşa ve düşük ifşa kümesi olarak ikiye ayırmıştır. Zevkler ve ilgi alanları, tutumlar ve görüşler ve iş yüksek ifşa kümesi içerisinde iken; para, kişilik ve beden düşük ifşa kümesinde yer almaktadır (Jourard & Lasakow, 1958, s. 95).

Westin'in üzerinde durduğu ikinci tehdit meraktır. Bireyden bireye, kültürden kültüre farklı yoğunluklarda görülen merak, tüm toplumlarda çeşitli önemli işlevlerin (bilgi dolaşımı, dolaylı deneyim ve grup ve aile normlarının teşviki gibi) yerine getirilmesi için gerekli bir unsur olsa da başkalarının özel sırlarını öğrenme çabasını da besler. Çoğu sosyal bilimci, tehlikeli boyutlarda görülen merakı, röntgencilik (*voyeurism*)

kavramına başvurarak ele almıştır. Westin, röntgencilik boyutuna ulaşan merakın, gazete ve dergilerdeki saldırgan reklamlarla teşvik edildiğini ekler. Ayrıca bazı kolluk kuvvetleri gözlemcileri, telefon dinleme, özel dedektiflik, yalan makinesi ve benzeri gözetim ile ilgili aktivitelerin röntgenci tipleri çektiğine inanmaktadır (Westin, 1967, ss. 55-56).

Mahremiyete yönelen son tehdit, gözetimdir. Sosyal kontrolün temel araçlarından biri olarak gözetimin, bir toplumun normlarının uygulanmasında ve vatandaşlarının korunmasında sahip olduğu rolü olsa da bu gözetimin nerede durması gerektiği Antik Yunan toplumlarından beri bir sorundur. Westin (1967), gözetimin insan davranışları üzerindeki etkisinin anlaşılabilmesi için gözetimi üç türe ayırır: (1) gözlemleyerek gözetim (*surveillance by observation*), (2) dışarı çıkarma ile gözetim (*surveillance by extraction*) ve (3) iletişimin yeniden üretilebilirliğinden kaynaklanan gözetim (*surveillance by reproducibility of communication*). Bu üç tür ile ilişkili olarak Westin, fiziksel gözetim (*physical surveillance*), psikolojik gözetim (*psychological surveillance*) ve veri gözetimi (*data surveillance*) ayrımını yapar.

Öznenin haberdar olduğu, dinleyerek ya da izleyerek yapılan gözetimin özne üzerinde sınırlayıcı bir etkisi olduğu söylenebilir. Bu etki, aynı zamanda, gözlemleyerek yapılan gözetimin gerçekleştirilmesinin arkasındaki gerekçedir: kurallara uyulmasını zorlamak. Diğer yandan gözlemleyerek yapılan gözetim, kamusal alanlarda güvenliği sağlamak açısından önemli bir araç olarak da değerlendirilmektedir (Westin, 1967, ss. 58-59).

Dışarı çıkarma ile gözetim, öznenin psikolojik mahremiyet alanına girilerek, mahrem olarak kalmasını istediği bilgileri zorla söyletmek ya da davranışa dökmesini talep etmektir. İşkence ya da benzeri metotlarla gerçekleştirilebilecek bu gözetim, yasalar tarafından yasaklanmıştır. Ancak yalan makinesi ya da kişilik testleri gibi uygulamalar bu tip gözetimin içerisinde değerlendirilebilir. Bu uygulamalar, kişinin kendi başına ‘halledemediği ya da halledebileceği’ sorunları gün yüzüne çıkararak gözlemlenebilir hale getirebilmektedir.

Son olarak, Westin’in iletişimin yeniden üretilebilir oluşundan kaynaklanan gözetim olarak tanımladığı türe değinilebilir. Yeni ses ve görüntü kaydetme cihazları ile öznelerin görüntü ve seslerinin, fark edilmeden kaydedilmesi mümkündür. Bireyler bir mektup yazarken ya da bir belgeyi dosyalarken yazdıklarının başkaları tarafından da

erişilebileceği ihtimalinin bilincindedir ve buna göre davranır. Ancak, yeni kayıt teknolojileri ile bireyin yazı yazarken olduğu kadar kontrolünde olmayan anların da fark edilmeden kaydedilebiliyor oluşu, mahremiyetine yönelik ciddi bir tehdittir (Westin, 1967, s. 62).

Kendini açığa vurma, merak ve gözetim, zaman zaman iç içe geçse mahremiyete yönelen tüm tehditleri kapsayan bir çerçeve sunmaktadır. Sosyal paylaşım ağlarının yaygınlaşması, kendini açığa vurma ve merak tehdidini artırmıştır. Yine enformasyon ve iletişim teknolojilerinin sağladığı olanaklar gözetim ihtimallerini de artırmıştır.

Güvenlik ya da güvende hissetme ihtiyacını mahremiyete yönelik bir tehdit olarak nitelendirmek doğru olmaz. Ancak, mahremiyet ve güvenlik arasındaki ilişkiyi bir çeşit takas olarak değerlendiren *trade-off modeli*, bu yönde bir çıkarım yapmayı mümkün kılabilir. “Bir şeyi elde etmek için başka bir şeyden vazgeçme” olarak çevrilebilecek trade-off modeli, güvenlik ihtiyacını ya da güvende hissetme ihtiyacını karşılamak için mahremiyetten vazgeçilmesidir. 2015 yılında tamamlanan SurPrise kısa adlı Avrupa Birliği projesinin, gözetim tabanlı güvenlik teknolojilerinin algılanan işlevsellikleri ile mahremiyete müdahaleleri (*perceived effectiveness and intrusiveness*) ile ilgili bölümünde, takas modeline (*trade-off model*) değinilmiş ve katılımcıların üç farklı gözetim teknolojisini değerlendirmek için tercih ettikleri “kullanışlı/işlevsel ancak fazlasıyla müdahaleci” (*useful but highly intrusive*) seçeneğinin bu modeli karşıladığı söylenmiştir. Ancak, araştırmada elde edilen sonuçlar, mahremiyet ve güvenlik arasındaki ilişkinin, takas modelinin önerdiğinden daha karmaşık olduğunu göstermektedir. Katılımcıların yüzde 38’i akıllı kapalı devre kamera sistemini (güvenlik kameraları), yüzde 56’sı akıllı telefon konum takibini ve yüzde 66’sı da derin paket incelemesini² kullanışlı ancak fazlasıyla müdahaleci olduğunu düşünmektedir. Gözetim tabanlı güvenlik teknolojileri, ulusal güvenlik için işlevsel olarak algılansa da bu teknolojiler katılımcıları oldukça rahatsız hissettirmektedir. Gözetim tabanlı güvenlik teknolojilerinin, müdahale seviyelerine rağmen sağladıkları kamu güvenliğinin hatırına kabul edilebilirlik oranları da yüzde 50’nin altındadır. Bir diğer önemli bulgu da katılımcıların yüzde 70’inden fazlası yasa ve yönetmeliklerin gözetim teknolojilerinin

² Deep packet inspection (DPI)

kötüye kullanımlarının önüne geçemediğini düşünmeleridir (Strauß, 2015, ss. 27-30). Çalışmanın bu noktasında, güvenlik ihtiyacının da mahremiyete dolaylı bir tehdit oluşturabileceğini not etmek yeterli olacaktır.

Mahremiyet ve kişisel bilgilerin gizliliğine yönelik en güncel tehditlerden birisi de kişisel bilgilerin kazanmaya başladığı ekonomik değerdir. 2008 yılında yapılan bir anket, kullanıcıların, kendilerine ait kişisel olarak tanımlanabilir bilgileri (*personally identifiable information*), ticaret yaptıkları diğer şirketlerle paylaşan, takas eden ya da satan veri simsarları (*data brokers*) ve kredi büroları gibi şirketlerden rahatsız olduklarını göstermiştir (Antón vd., 2010, s. 24). Acquisti, 2010 yılında düzenlenen bir yuvarlak masa toplantısı için hazırladığı raporda, mahremiyeti korumanın refahı azalttığını savlayan ekonomik bakış açısına değinir. Özellikle Şikago okuluna atfedilen bu yaklaşım, mahremiyeti gizlemenin piyasalarda verimsizlik yarattığını söyler ve tüketicilerin kişisel verilerinin iki firma arasında sınırsız olarak paylaşılmasının aslında piyasa bozulmalarını azaltabileceğini ve tüketiciler için de olmak üzere sosyal refahı artırabileceğini iddia eder (Acquisti, 2010, s. 4). Tamamen piyasa odaklı bir yaklaşımda kişisel bilgileri bir ürüne çevrilebilir ve mahremiyetin ortadan kaldırılması ekonomik refahla ilişkilendirilebilir. Her ne kadar bu yaklaşım diğer teorisyenler tarafından eleştirilse de kişisel verilere atfedilen ekonomik değerin, mahremiyet için bir tehdit olduğunu söyleyebiliriz.

1.1.3. Dijital Dünyada Mahremiyet

Elektrik altyapısı ve beraberinde getirdiği tüm teknolojiler, bilgiye erişim olanaklarını hem artırmış hem de erişimi hızlandırmıştır. İnternet kullanımının yaygınlaşması ve dünya toplumlarının birer birer “ağ toplumu” haline gelmeleri, bu toplumların parçası olan bireylerin farkında olarak ya da farkında olmadan daha önce eş görülmemiş bir boyutta veri üretmelerine neden olmuştur. Bireylerin gerek arkalarında bıraktıkları dijital ayak izleri (*digital footprints*), gerek enformasyon ve iletişim teknolojileri ile kurdukları iletişimler, bireylerin mahremiyetinin korunmasının önünde bir sorun olarak durmaktadır. Bu verilerin başkaları tarafından erişilebilirliği, işlenebilirliği ve ayrıştırılabilirliği belki de içinde bulunduğumuz dönemde kişisel mahremiyetin karşısındaki en büyük engeli oluşturmaktadır. Pek çok araştırmacının da belirttiği gibi, teknolojik inovasyonlar bireysel mahremiyetin aşınmasına neden olmaktadır (Cairncross, 2002; Milne & Gordon, 1993, s. 206). Enformasyon teknolojilerinin sahip olduğu kalıcılık, aranabilirlik ve çapraz dizinlenebilirlik gibi

özellikler mahremiyeti aşındırmaktadır (Tufekci, 2008, s. 20). Buchanan vd. de (2007, s. 157) yeni teknolojilerin bilgi toplumunu (*information society*) oluşturduğunu, ancak bu “bilginin” sadece nesnelerle ilişkili olmadığını ve çoğunun insanlar hakkında, onların bilgisi ya da rızası olmadan toplanan bilgiler olduğunu söyler. Garfinkel ve Spafford (2002, s. 203) ise internetin altında yatan teknolojinin kullanıcıların mahremiyetini korumak için değil, “bilgileri transfer etmek” gayesi ile tasarlandığını söyler. Bu durum, mahremiyet konusunu bilgi toplumunun (ya da ağ toplumunun) en çok tartışılan ve endişe edilen yönlerinden biri haline getirir (Waldo vd., 2007, s. 19). Bir önceki başlıkta, mahremiyete yönelik tehditler, “dijital dünya” ile sınırlandırılmadan, daha genel bir çerçeve içinde ele alınmıştı. Bu başlıkta ise hem günümüzdeki enformasyon ve iletişim teknolojilerinin nüfuz ettiği gündelik hayatlarda mahremiyetin durumu aydınlatılmaya çalışılmış hem de dijital teknolojilerden güç bularak mahremiyeti etkileyen faktörler ele alınmıştır. Ayrıca, dijital dünyadaki mahremiyeti incelemek için işe koşulabilecek iki farklı kuramsal yaklaşıma değinilmiştir.

Dijital çağın mahremiyetin karşısına çıkarabileceklerini, 1960’lı yıllardan, bilgisayar çağının henüz başladığı dönemden öngören Alan Westin’in (Fox, 2013) veri gözetimi (*data surveillance*) kavramına değinmeliyiz. Mahremiyete yönelik tehditlerden biri olan gözetim, iletişimin yeniden üretilebilirlik kazanması, Westin’i veri gözetimi kavramına başvurmaya yönlendirmiştir. Bilgisayar çağının yeni yeni başladığı bir dönemde Westin, bilgi işlem devriminin mahremiyet üstünde oluşturduğu baskıyı anlamak için altı temel trend sıralamıştır:

1. *Bilgisayarların dışında, bilgi toplama ve kayıt tutmak tekniklerindeki genel artış*
2. *Bireylerin hareketlilik kazanmasının ve kitle toplumlarındaki yaşamın standartlaştırılmasının, on milyonlarca yurttaşın kişisel sicil dosyalarını tutan özel veya kamusal soruşturma sistemlerinin geliştirilmesine yol açması*
3. *Genel bilgi toplama ve kişisel sicil dosyası tutma tekniklerinin, sahip oldukları daha fazla kayıt depolama ve daha önce mümkün olmayan hızlarda işleme kapasitesine sahip elektronik dijital bilgisayarların ortaya çıkması ile ciddi oranda hızlanması*

4. *Geliştirilen pek çok yeni kamu programının bireyler hakkında, daha öncesine oranla, daha fazla kişisel veriye gereksinim duyması.*
5. *Bilgisayar alanındaki gelişmelerin bilgisayarları kullananlar arasındaki veri paylaşımını hızlandırması ve bilgisayar dillerinin ve bu dilleri birbirine çeviren makinelerin mükemmelleştirilmesinin, bilgisayarların birbirleri ile doğrudan iletişim kurmasını sağlaması, böylelikle de verilerin bir sistemden diğerine akması.*
6. *Otomatik veri işleminin yavaş yavaş geçmişteki nakit alım-satım işlemlerinin yerini alması ve bireylerin hayatlarındaki önemli alım-satım işlemleri ile ilgili kayıt izleri bırakması (Westin, 1967, ss. 158-162).*

İlk trend olan bilgi toplama ve kayıt tutma tekniklerindeki genel artış ile ilgili olarak, on dokuzuncu yüzyılda, telgraf aracılığı ile gerçekleştirilen bilgi paylaşımı örnek gösterilebilir. Vincent, kararları geciktirmek istemeyen ve işi kaçırma kaygısı taşıyan şirketlerin telgraf gibi hızlı cevap iletebilecek iletişim sistemleri kullandıklarını ve bu iletişimin yüksek maliyetlerinin, bilgi ekonomisine verilen önemi artırdığını söyler ve şöyle devam eder:

Henüz 1885 gibi erken bir tarihte, kırk yedi üyesinin veri tabanlarını birbirine bağlama girişiminde bulunan Ulusal Ticareti Koruma Dernekleri Birliği borçlu adayların kredi itibarını çeşitli kategoriler altında toplayarak, her bir kategoriye bir “telgraf kodu” altında araştırmayı yürüten aboneye göndermeyi denedi. Bu geleceğe dair bir ön izlemeydi ancak, 1970’lerden itibaren tüm ulusal piyasaları kapsayan şirketler ve bilgisayarların gelişine kadar, bu takip formunun baskın aracı, zaman zaman güncellenen ve gerektiğinde sorgulama için özetlenen kağıt dosyadan ibaretti (Vincent, 2017, s. 145).

Şahısların borç bilgileri üzerinden kredi itibarları hakkında bir çıkarımda bulunulabiliyor oluşu, Westin’in belirttiği ikinci trend için de bir örnektir. Bilgiye ulaşma, onu depolama ve paylaşma süreci ne kadar ilkel olursa olsun, bireyler ile ilgili bilgilerin yüz yılı aşkın bir süredir toplandığı ortadadır. Hough (2009, s. 406), bu farklı konumlarda bulunan kağıt dosyaların (kağıtlar üzerinde saklanan kişisel verilerin) aslında koruyucu bir tampon oluşturduğunu ve verilerin önemli bir çaba olmadan ve sadece haklı nedenlerle açığa çıkarılmasını sağladığını söyler. Teknoloji ilerledikçe, kâğıt kayıt sistemlerinin koruyucu verimsizlikleri, yetkin veri işleme ve dijital gözetim teknolojilerine dönüşmüş

ve bir zamanlar mahrem olan bilgilerin saklanma yetkinliđi için ciddi bir risk oluřturmuřtur. Eskiden günler veya aylar süren arka plan soruřturmaları, dakikalar içinde gerçekteřtirilebilmektedir. Bu durum, bilgisayar ve internet teknolojisinin, hem bilgi toplama sürecini kolaylařtırdıđını ve hızlandırdıđını hem de toplanan bu verilerin kolayca iřlenebilmesini ve paylařılabilmesini sađladıđını göstermektedir.

Fischer-Hübner (1998, s. 421), günden güne daha fazla miktardaki alım-satım verisinin eriřilebilir olacađını, bu verilerin dünya genelindeki farklı siteler üzerinde toplanabileceđini ve tüketici profilleri oluřtırmada kullanılabileceđini söylemiř ve demokratik toplumlarda temel bir hak olarak mahremiyetin korunması gerektiđini vurgulamıřtı. Westin'in altıncı trendi ile iliřkili olan bu öngörü, özellikle yirmi birinci yüzyılın bařlarından itibaren kiřiselleřtirilmiř reklamlar, çerezler gibi uygulamaların ortaya çıkması ile bir gerçeklik halini almıřtır.

Bilgi iřlem devriminin, henüz bugünkü etkinliđini kazanmadıđı bir dönemde öngörülen bu trendler, dijital dünya içerisinde özel hayatı ve mahremiyeti korumanın ne kadar zor olacađını göstermektedir. Bu dođrultuda, dijital dünyada mahremiyetin ve özel hayatın artık söz konusu olmadıđını, her řeyin kamusal hale geldiđini ilan eden pek çok arařtırmacı vardır (Marx, 2004). Fischer-Hübner'e (1998, s. 436) göre, tamamen ađa bađlanmış -ađ toplumuna dönuřmüř- bir toplumda mahremiyet ciddi biçimde tehdit altındadır ve sadece mahremiyet ile ilgili yasa ve yönetmeliklerle korunamaz. Yasa ve yönetmeliklerin yanı sıra, enformasyon sistemlerinin tasarım ařamasında mahremiyetin bir kriter olarak ele alınması ve gizlilik řartlarının teknik olarak da uygulanması gerekmektedir. Mahremiyetin korunması konusunu bilgiye eriřim özgürlüğü ile birlikte ele alan Stefanick (2011, ss. 23-24) ise bunların iki zıt kutbu temsil ettiđini, herhangi birinin artmasının diđerinin azalması ile sonuçlanacađını söyler. Stefanick'e göre, bu iki kutupta alınacak pozisyonlarda dođru veya yanlıř yoktur ve demokratik bir toplum iki kutbun arasında bir yerde konumlanmayı hedefler.

Yukarıda, mahremiyetin çeřitli arařtırmacılar tarafından farklı kapsamlara ya da boyutlara ayrıldıđına değinilmiřti. Dijital dünyada mahremiyetin durumunu değerdendirebilmek için bu ayrımlara tekrar gönderme yapmak gereklidir. Burgoon tarafından fiziksel, sosyal, psikolojik ve enformasyonel olarak dört boyutta incelenen mahremiyeti, Laurie'nin kullandıđı gibi, biraz daha genelleřtirerek, fiziksel ve

enformasyonel mahremiyet şeklinde ele almak daha doğru olacaktır. Yeni enformasyon ve iletişim teknolojileri ve beraberinde getirdiği tüm araç ve hizmetler, hem bireylerin coğrafi konumları, görüntüleri, sesleri vb. bilgilere erişilebilirlik ile fiziksel mahremiyet hem de bireylerin farkında olarak ya da olmadan ürettikleri tüm içeriklere, üst verilere (*metadata*) erişimin ihtimal dahilinde olması ile enformasyonel mahremiyet için bir risk oluşturmaktadır.

Fiziksel mahremiyet, bireylerin fiziksel ya da psikolojik benliklerine erişilememesi olarak ele alınabilir (Laurie, 2002, s. 6). Burgoon da benzer bir tanıma atıfta bulunarak fiziksel mahremiyetin hem erişilemezlik durumunu hem de erişimin derecesini kapsadığını söyler. Enformasyonel mahremiyet ise, Alman Anayasa Mahkemesi tarafından, “enformasyonel kendi kaderini tayin hakkı” (*right of informational self-determination*) olarak nitelendirilmiştir (Raguse vd., 2008, s. 11). Daha açık bir şekilde ifade edilirse, enformasyonel mahremiyet, bireyin kişisel bilgilerinin açıklanmasının ve kullanılmasının prensipte kendi takdirinde olması hakkıdır (Fischer-Hübner, 1998, s. 422). Enformasyon mahremiyeti, ya da bilgi gizliliği olarak Türkçeleştirebileceğimiz *information privacy*, Stone vd. (1983, s. 460) tarafından “bireyin kişisel olarak (diğer bireyler, gruplar, kuruluşlar vb. karşısında) kendisi hakkındaki bilgileri kontrol etme yeteneği (kapasitesi)”, Burgoon vd. (1989, s. 134) tarafından ise “kişinin kendisi veya grubu hakkında kimlerin hangi koşullar altında bilgi toplayıp yaydığını kontrol etme yeteneği” olarak tanımlanır. Heravi ve çalışma arkadaşları (2018, s. 443) ise bu konsepti çevrim içi sosyal ağ sitelerine uyarlarlar: “Kullanıcının profil ve duvar sayfası bilgileri, arkadaş listeleri, haber beslemeleri, özel etkileşimler (yani mesajlar ve sohbetler), herkese açık olan ve/veya olmayan fotoğraflar/videolar ve satın alma geçmişi gibi kullanıcı tarafından üretilen içerikleri kapsayan kişisel verilerine; diğer kullanıcıların, çevrim içi sosyal ağ sağlayıcılarının ve üçüncü kişilerin ne ölçüde erişebileceğini belirleme hakkı”.

Raynes-Goldie ise sosyal ve kurumsal mahremiyet (*social and institutional privacy*) ayrımını tesis eder. Bu ayrımı, mahremiyet ikilemi ile ilişkilendiren Raynes-Goldie’ye göre; yaşanacak bir mahremiyet ihlalinin yaratabileceği potansiyel sorunlar, kurumsal (sosyal ağ sitelerinde paylaşılan bilgilerin veri tabanlarında saklanması, bir meta olarak üçüncü taraflara satılması ve güvenlik güçleri tarafından kullanılması) ve sosyal (kişinin itibarının zedelenmesi) olarak ayrılır. Sosyal mahremiyet iki şeyi kapsar:

(1) Kendisi hakkında başkalarına ifşa edilenlerin yönetimi (kimlik veya itibar yönetimi olarak da adlandırılır) ve (2) çeşitli sosyal bağlamlarda ilerleme ve onları yönetme yeteneği (Raynes-Goldie, 2012, s. 81). Raynes-Goldie'nin yaklaşımı kimlik oluşturma ve sosyalleşme için kişisel bilgilerini ifşa etme davranışını açıklar niteliktedir.

Westin (2003), “*Social and Political Dimensions of Privacy*” başlıklı çalışmasında, kendisini 1952 yılından bu yana teknolojik gelişmelerin ve sosyal değişimlerin mahremiyete etkileri üzerine çalışan bir sosyal bilimci olarak tanımlar ve kendi katılımcı-gözlemlerine dayandığı tarihsel ve politik yargılar ışığında, 1945 tarihinden başlayarak bir mahremiyet sahnesi resmeder. Westin'in dört periyoda ayırdığı bu tablo, özellikle enformasyonel mahremiyetin teknolojik gelişmeler karşısındaki durumunu yansıtması açısından değerlidir.

Westin, ilk olarak mahremiyet araştırmalarının referans hattı olarak, İkinci Dünya Savaşı'nın bitimini takip eden ilk 15 yılı işaret eder: 1945-1960 yılları arasında enformasyon teknolojilerindeki gelişim sınırlıdır ve halkın devlete, özel ve kâr amacı gütmeyen sektöre güveni yüksektir. Westin'e göre bu periyot, önemli sivil özgürlükler ve medeni haklar mücadelelerini barındırsa da ne kamusal ne de hukuksal söylemlerde bir enformasyonel mahremiyet hakkı teması yoktur ve mahremiyet üçüncü düzeyde bir sosyal sorundur (Westin, 2003, s. 435).

Westin, 1961-1979 yıllarını çağdaş mahremiyetin gelişiminin ilk evresi olarak nitelendirir. Bu periyot, “yüksek teknoloji çağının açık bir sosyal, politik ve yasal sorunu olarak enformasyon mahremiyetinin yükselişine” sahne olur. Sivil hak mücadelelerine, savaş karşıtı protestolara, cinsel devrime ve Watergate skandalına tanıklık edilen bu çalkantılı dönem, aynı zamanda mahremiyete ilişkin endişelerin gelişimine de sahne olur. Westin, bu gelişimin yeni sosyal sorunlar modeli (*early-social-issues pattern*) olarak nitelendirdiği bir modele paralel bir şekilde gerçekleştiğini söyler: Erken alarmlar, deneysel araştırmalar, alternatif politika formülasyonları ve birinci nesil yasal ve örgütsel eylemler. Mahremiyet endişesinde gözlemlediği bu değişimi değerlendiren Westin, mahremiyetin artık ikinci seviye bir sosyal politika sorununa dönüştüğünü ve bu dönemin önemli mahremiyet ve teknolojinin sosyal etkilerine yönelik araştırmaların ve ilk nesil bilgi çağı mahremiyet yasalarının dönemi olduğunu söyler (Westin, 2003, ss. 435, 439).

Westin, 1980-1989 dönemini, mahremiyetin gelişiminin ikinci evresi olarak nitelendirir. Bu dönem, bilgisayar ve telekomünikasyon performansının arttığı, ancak mahremiyetle ilgili bilgi-toplum ilişkilerinde köklü değişikliklerin olmadığı bir dönemdir. Bu dokuz yıllık periyotta, merkezi veri bankaları dağıtık hesaplama yeteneği kazanır, işyerlerinde video görüntüleme terminalleri kullanılmaya başlanır ve ilk kişisel bilgisayarlar piyasaya sürülür. Kişisel bilgisayar (PC) ile bilgisayar teknolojisi bireylere de güç sağlamaya başlar. Ancak bu mahremiyet durumunu hemen etkilemez, çünkü henüz dağınık durumdaki kişisel bilgisayarlar birbirlerine bağlı değildir. Westin, bu periyodu fırtına öncesi sessizlik dönemi olarak tanımlar (Westin, 2003, ss. 439, 441).

1990-2002 periyodu, mahremiyetin gelişiminin üçüncü evresidir ve bu dönemde mahremiyet birinci seviye bir sosyal ve politik sorun haline gelir. Westin, bu dönem içerisinde gerçekleşen beş büyük teknolojik gelişmeye dikkat çeker. Bu gelişmelerden ilki ve belki de en kapsamlısı 1990'ların ortalarında internetin yükselişidir. İkinci gelişme, kablosuz iletişim cihazlarının (cep telefonları) ortaya çıkması ve yaygınlaşmasıdır. Teknoloji-mahremiyet ilişkisine yeni bir boyut ekleyen üçüncü gelişme ise İnsan Genomu Projesi (*Human Genome Project*) ile genetik kodların kilidinin açılmasıdır. Büyük veri depolama uygulamalarındaki veri madenciliği (*data mining*) yazılımlarının geliştirilmesi ve devletin tuttuğu kamu kayıt sistemlerinin otomasyonu dördüncü gelişmedir. Beşinci ve son büyük teknolojik gelişme ise, federal kolluk kuvvetlerinin ve ulusal güvenlik kurumlarının, güçlü şifreleme programlarına yönelik duydukları endişe ve çevrim içi iletişime erişebilmek için bir uygulama geliştirmeleridir. Bu teknolojik gelişmelerle birlikte, mahremiyet sorunu küresel bir boyut kazanır. Dünya çapında artan iletişim, ticaret, seyahat ve pazarlama faaliyetleri, mahremiyeti küresel bağlamda ele alınması gereken bir sorun haline getirir (Westin, 2003, s. 442).

Mahremiyetin gelişiminin üçüncü evresinde, ABD'de 120'nin üzerinde ulusal çapta mahremiyet ile ilgili anket araştırması yapılır. Bu çalışmalarda elde edilen sonuçları değerlendiren Westin, sosyal ve politik dünyada mahremiyete yönelik tehditlere ilişkin korkuların 1990'lı yıllarda arttığının altını çizer ve kişisel mahremiyete yönelik tehditlere ilişkin endişenin yüzde 64'ten (1978) yüzde 84'e (1995) sıçradığını ekler. 1999 yılına gelindiğinde kişisel verilerin potansiyel kötü kullanımlarına ilişkin kamusal endişe yüzde 94'e yükselir. Yine bu dönemde yapılan araştırmalara göre; tüketicilerin yüzde 80'i şirketlerin tüketicilerin kişisel bilgilerini nasıl topladıkları ve kullandıkları üzerindeki

kontrollerini kaybettiklerini düşünmektedir ve yüzde 59'u çok kişisel olduğunu ya da gerçekten gerekli olmadığını düşündükleri için bir şirkete bilgi vermeyi reddettiklerini belirtmişlerdir (Westin, 2003, ss. 444-445). 11 Eylül saldırıları, vatandaş-devlet arasındaki mahremiyet dengesini değiştirse de tüketici mahremiyeti konusu neredeyse aynı kalır. Saldırıları sonrası devlete duyulan güven artsa da özel sektöre duyulan güvende bir değişiklik olmaz Hatta saldırılar sonrası yapılan bir anket çalışmasına göre; katılımcıların yüzde 26'sı saldırıların öncesine göre daha endişelidir (Westin, 2003, s. 449).

Westin, bu değerlendirmelerini Amerika Birleşik Devletleri perspektifinden ve büyük oranda oradaki gelişmeleri göz önünde bulundurarak gerçekleştirmiştir. Ancak ortaya koyduğu gelişmeler, tamı tamına ve eşzamanlı olmasa da diğer ülkeler için de benzer şekilde gerçekleşmiştir. Özellikle büyük terör saldırıları, kamu güvenliğinin tesisi için mahremiyet hakkından kimi durumlarda vazgeçilmesine ve devletin gözetim sistemlerini kullanırken olabildiğince bireysel mahremiyeti gözettiklerine dair bir güven ortamı oluşturmuştur. Westin (2003, s. 448), kendi kamuoyu araştırmalarına atıfta bulunarak, katılımcıların yüzde 87'sinin güvenlik güçlerinin 11 Eylül sonrası kazandıkları yeni soruşturma yetkilerini ve gözetim yeteneklerini uygun bir şekilde kullanacaklarını düşündüklerini belirtir.

Westin, makalesini 2003 yılında yayınlarken “mahremiyetin gelişiminin üçüncü evresi” olarak adlandırdığı periyodu sonlandırmayı tercih etmiştir. Westin'in bu döneme kadar yaptığı değerlendirmelerde, özellikle tüketicilerin özel şirketlerle kişisel bilgilerini paylaşırlarken duydukları güvensizliğin üzerinde durur. Bu güvensizlik, literatürdeki araştırmalar başlığında değinilecek olan pek çok araştırmada da karşılaşılabileceği gibi devam etmektedir. Ancak, bu güvensizliğe rağmen kişisel bilgiler paylaşılmaktadır. Bu çelişkili davranış, mahremiyet ikilemi (*privacy dilemma*) (Brandtzæg vd., 2010) ya da mahremiyet paradoksu (*privacy paradox*) (Barnes, 2006; Norberg vd., 2007) olarak nitelendirilmektedir. Bu ikiliği yaşayanlar, Westin'in mahremiyet faydacıları kategorisi³ içerisinde değerlendirilebilir. Sosyal ağ sitelerinin yaygınlaşması, kullanıcı sayılarının

³ Westin (2003, s. 445), anket araştırmalarında bireylerin mahremiyete yaklaşımlarını üç farklı kategoride ele alıyordu: (1) Mahremiyet köktencileri (*privacy fundamentalist*), (2) mahremiyet faydacıları (*privacy pragmatist*) ve (3) mahremiyet kaygısızları (*privacy unconcerned*).

artması ve akıllı cihazların (*smart devices*) gelişiminin beraberinde getirdiği sosyal trendlerin (Tablo 1.1) bireylerin mahremiyete olan yaklaşımlarında bir dönüşümü beraberinde getirdiği söylenebilir. Özellikle 2004 yılından itibaren yaşanan gelişmeler, Westin’in çizdiği mahremiyet sahnesinde yeni bir evrenin tanımlanmasının gerekliliğine işaret etmektedir. Bu doğrultuda, hem erişeceği hizmet/ürün için mahremiyetinden ve kişisel bilgilerinin gizliliğinden belirli ölçüde feragat etmeyi göze alan mahremiyet faydacılarından hem de kaygılarına rağmen hizmet ve ürünlere erişmek için kişisel bilgilerini açık edenlerden hareketle, bu evreye mahremiyetin gelişimindeki duraklama evresi diyebiliriz.

Editörlüğünü Waldo, Lin ve Millett’in üstlendiği “*Engaging Privacy and Information Technology in a Digital Age*” adlı kitapta, Westin’in mahremiyet sahnesinde işaret ettiği gelişmeler ile paralellik gösteren bir yaklaşımla, bilgi toplumunda mahremiyeti etkileyen üç büyük ölçekli faktör tanımlanır. Bu faktörler, ya da itici güçler (1) teknolojik değişim (*technological change*), (2) toplumsal trendler (*societal trends*) ve (3) koşullardaki kesintiler (*discontinuities in circumstances*) olarak sıralanır. Tablo 1.1’de, bu faktörler kategorik olarak listelenmiştir.

Tablo 1.1: Mahremiyeti Etkileyen Büyük Ölçekli Faktörler

Teknolojik Değişim	Toplumsal Trendler	Koşullardaki Kesintiler
• Aynı anda her yerde bulunma • Bağlanırlık • Veri toplama • Depolama • Hesaplama gücü • Donanımın metalaşması • Kullanılabilir yazılımlar • Şifreleme • Mahremiyet ile ilgili biyoteknoloji • İnsan duyularının gelişmesi (teknoloji ile) • Veri ve iletişim cihazlarının taşınabilirliği • Bilginin kalıcılığı • Verilerin ve iletişimin makul fiyatlı olması • Sensör teknolojisindeki gelişmeler	• Küreselleşme • Hareketlilik • Sanallık • Kentleşme • Sürekli erişilebilirlik • Münakaşacılık • Demografi/Yaşlanma • Yeni yaşam biçimleri ve iletişim • Sosyal ağ oluşturmadaki artış • Artan toplumsal dayanışma • Elektronik iletişim okuryazarlığındaki artış • Bilginin erişilebilirliği beklentisindeki artış • Bağlantılı parasal sistemler • Bağlantılı üretim sistemleri	• 2001 yılında Dünya Ticaret Merkezi ve Pentagon’a gerçekleştirilen yıkıcı saldırılar • 1972-1973 Watergate Skandalı • 1976 Kilise Komitesi Duruşmaları • 1941 Pearl Harbor saldırısı • 1995 yılında World Wide Web’in icadı • Ulusal ve uluslararası sağlık tehditleri (SARS ve kuş gribi)

Kaynak: (Waldo vd., 2007, s. 28)

Tablo, Westin'in altı temel trendinin ve çizdiği mahremiyet sahnesinin geliştirilmiş ve detaylandırılmış bir versiyonu olarak değerlendirilebilir. Westin'in 1960'lı yıllardaki gözlemleri, gelişmekte olan yeni bilgisayar teknolojisinin mahremiyet üzerindeki mevcut ve potansiyel etkisine yöneliktir. Tablo, bu teknolojilerin ve bu teknolojilere bağlı olarak gelişen internet, akıllı cep telefonu gibi araçların toplumda yaygınlaşması ile kazanılan yeni alışkanlıkların mahremiyete etkisini de kapsamaktadır. Waldo ve arkadaşları da çeşitli kırım anlarının da (11 Eylül Saldırısı vb.) mahremiyeti etkilediğini not düşerler.

Ulusal ve uluslararası sağlık tehditleri de bilgi toplumunda mahremiyeti etkileyen faktörlerden biridir. İnsanlık tarihi boyunca defalarca karşılaşılan salgın hastalıklar, uzak mesafelere seyahat etmek için gereken maliyet ve zamanın azalması ile dünya nüfusunun büyük bir kısmının seyahat imkânına sahip olması nedeniyle farklı bir boyut kazanır: “Kişi bir hastalığa yakalanabilir ve daha hasta olduğunu fark etmeden yabancı bir ülkeye ulaşabilir – özellikle söz konusu hastalığın semptomlarının ortaya çıkması uzun zaman alıyorsa.” Waldo ve arkadaşları (2007, s. 38), hazırladıkları raporda havayolu trafiğinin tamamen engellenmesinin ekonomik maliyetine vurgu yaparak, ulusal hükümetlerin enfekte olmuş kişilerin kendi sınırlarından içeri girmesini önlemek için sahip olduğu tek seçeneğin, diğer ülkelerdeki salgını yakından izlemek olduğunu söylerler. 2020 yılında, tüm dünyayı etkisi altına alan Covid-19 salgını, bu raporda öngörülemeyen önlemleri beraberinde getirmiştir. Bu gelişme, bir bakıma, küresel çaptaki sağlık tehditlerinin mahremiyet hakkını etkileyeceği, bu hakkın tanınmasında kısıtlamalara neden olacağı argümanının somut bir kanıtı olarak değerlendirilebilir.

Norveç Tüketici Konseyi için Brandtzæg ve Lüders (2009) tarafından hazırlanan raporda, kişisel verileri internete taşımanın açıkça artan bir eğilim olduğu belirtilir ve bu eğilimin potansiyel negatif sonuçları şöyle sıralanır:

- Kimlik hırsızlığı riskinin artması
- Kişisel verilere ve bu verilerin ne amaçla kullanılacağına ilişkin kontrolün kaybedilmesi
- Sürekli erişilebilirlik nedeniyle istenmeyen temasların sayısının artması
- Sürekli daha fazla izleyiciye “sergilenme” nedeniyle giderek güçlenen izlenme duygusu

- Özel bölgelerin sonlanması – Hakkında bir şeyler bilinmesi tercih edilmeyen insanlar hakkında çok fazla enformasyon edinilmesi
- Kullanıcı davranışlarının, tercihlerinin ve içeriklerin otomatik olarak haritalanmasına dayanan kişiye özel reklamcılığın ve fiyatlandırmanın artması
- Tüketici haklarının zayıflaması (Brandtzæg & Lüders, 2009, s. 17).

Raporda listelenen olumsuz sonuçların, mahremiyeti sekteye uğrattığı söylenebilir. Hough’a (2009, s. 407) göre çağdaş toplum, başka hiçbir çağda görülmemiş ölçüde, mahremiyetin azalmasından mustarıdır ve bu azalma en açık şekilde mahremiyetin ihtiyat (*reserve*) boyutunda görülebilir. Hough, Westin’in (1967) mahremiyeti dört farklı boyutta inceleyen⁴ yaklaşımındaki “ihtiyat” veya “ihtiyatlı olma” -ya da Kalaman’ın (2017, s. 8) ifadesiyle “kendini muhafaza etme”- şeklinde Türkçeleştirilebilecek “*reserve*” boyutunu, Flaherty’nin benzer yaklaşımındaki “*reserve*” ile eşleştirir. Güvene dayalı bu mahremiyet bileşeninde, belirli bilgilerin ifşa edilip edilmemesi başkalarının takdirine bağlıdır. Hough, Flaherty’nin ihtiyatının üç bileşenden etkilendiğini ifade eder. Bu bileşenler; koleksiyon -ya da toplama (*collection*), yayma (*dissemination*) ve kontroldür (*control*). Hough ilk iki bileşenin genellikle bireyin bilgisi dışında gerçekleştiğini söyler. Hough’a göre, başkalarının bireyler hakkında topladığı bilgiler, zararsız görünseler bile ihtiyat kaybına neden olur. Modern toplumda yaşayan bireylerin, kendileri hakkında toplanan bilgilerin oluşturduğu “koleksiyonu”, modern dünyanın kaçınılmaz bir parçası olarak görmeleri ihtiyatlı olma kabiliyetlerini zayıflatır. Hough, internet teknolojilerinin, ilgi çekiciliği çok az olan herhangi bir kişisel anın yayınlanmasına imkân tanıdığının altını çizerek ve Facebook gibi sosyal ağ sitelerinin “gömülü kalmasını dilediğimiz utanç verici gençlik kaçışlarının ve garip fotoğrafların yeniden dirilişini” sağladığını ekler. Bu sitelerdeki gönderiler, çoğu zaman cep telefonu kameraları ile öznel bilgisi olmadan çekilen ve onların rızası alınmadan paylaşılan fotoğraflardan oluşur. Hough’a göre bu durum, “anlık bir şöhrete, uzun süreli utançlara ve asla geri alınamayacak bir ihtiyat kaybına yol açar (Hough, 2009, s. 409).”

Jones, *Mahremiyet: Farklı Olan Ne? (Privacy: What's Different Now?)* adlı makalesinde, mahremiyetle ilgili iki kritik nokta ortaya koyar ve teknolojiye atfettiği yedi

⁴ Tekrarlamak gerekirse, bu boyutlar (1) yalnızlık (solitude), (2) yakınlık/samimiyet (intimacy), (3) anonimlik (anonymity) ve (4) ihtiyattır (reserve).

özelliğın bunlara etkisini tartıřır. Jones'a göre, bir řeyin mahrem kabul edilip edilemeyeceğı o řeyin doęasında olan bir özellik deęil, özü dıřında yapılan bir tercihtir. Mahremiyetle ilgili bir dięer kritik nokta da hakkınızda bir řeyler bilenlerin kimler olduęunu bilmenin, beraberinde bu kiřilerin bildikleriyle ne yapacaklarına dair bir itimat, güven ve belki de kayıtsızlık getirmesidir. Jones, teknolojik geliřmelerin bu yapıyı deęiřtirdiğini savunur. Artık niyetini dahi bilmediğiniz insanların hakkınızda neler bildiğı ya da bildiklerini rızanız olmadan ne řekilde kullanacağı ciddi kaygı kaynaklarıdır. Jones, teknolojinin bu etkisinin kaynaklarını ortaya koymak için yedi farklı özellik tanımlar. Bunlar, teknolojinin kalıcılık (*permanence*), yoğunluk (*volume*), görünmezlik (*invisibility*), tarafsızlık (*neutrality*), erişilebilirlik (*accessibility*), birleřtirilebilirlik (*assembly*) ve uzaklık (*remoteness*) özelliğidir. Kalıcılık, eskiden geçici olan olayların ve durumların kalıcı hale gelmesidir. Jones, daha önceden de bilginin kalıcı olabildiğini ancak modern teknolojinin, olaylar ve durumlar hakkındaki geçici veri parçalarını dahi kalıcı hale getirdiğini belirtir. Yoğunluk, kalıcı hale gelen verinin boyutu ve çeřitliliğı ile ilişkilidir. Görünmezlik özelliğı, bilgisayar üzerinde yapılan işlemler sırasında üretilen üst verilerin, kolay tercüme edilemedikleri ya da başka bir ifade ile anlaşılır olmadıklarına vurgu yapar. Tarafsızlık, teknolojinin ayırım yapmaksızın her çeřit veriyi saklaması; erişilebilirlik, farklı türdeki verilerin kopyalarının herhangi bir yerde bulunabilmesi ve birleřtirilebilirlik ise farklı kaynaklardaki, konumlardaki verilerin bir araya getirilmesinin çok daha kolay hale gelmesini ifade eder. Son olarak uzaklık ise, bireylerin kendilerine ilişkin verilerin sadece fiziksel olarak deęil mantıksal olarak da uzakta olan kiřilerin dahi erişebileceğı konumda olmasıdır (K. S. Jones, 2003).

1.1.3.1. Kuramsal Yaklaşımlar

Jones'un çalışması, sosyal aę siteleri yaygınlařmadan, hatta en yaygın kullanımda olan Facebook tarih sahnesine çıkmadan önce kaleme alınmıřtır. Jones, daha o dönemde dahi, teknolojinin hali hazırda bireylerin mahremiyet algılarını ya da ona atfettikleri önemi deęiřtirdiğini öne sürmüřtür. Sosyal aę sitelerinin yaygınlařması, bireylerin sadece farkında olmadan deęil, bilerek ve isteyerek kiřisel verilerini paylařtığı bir dönemin bařlangıcı olarak nitelendirilebilir. Çalışmasında, bilgileri deęiř tokuř etmenin veya yaymanın insan doęasının doęal bir parçası olduęunu hatırlatan Hough ise, iletiřim teknolojilerinin geliřmesinden önce bile dedikodunun eęlenceli olduęuna deęinir. Mevcut durumda farklı olan ise bu dedikoduyu milyonlarca insanla aynı anda yapmamızı

veya başka türlü bilgi alışverişinde bulunmamızı sağlayan teknolojilerdir (Hough, 2009, s. 409). Bireylerin kendi mahremiyetlerine farkında olarak ya da olmaksızın zarar veriyor oluşu, Altman'ın arzu edilen ve elde edilen mahremiyet ayrımını ve onun mahremiyete olan yaklaşımını tekrar gündeme getirir. Enformasyon ve iletişim teknolojilerinin şekillendirdiği modern toplumda mahremiyeti çözümlemek için Altman ve Westin'e başvurulabilir. Austin'e göre (2003, s. 164), teknolojik gelişmelerin yarattığı mahremiyet sorunları, geleneksel mahremiyet analizlerinin sınırlarının dışında kalsa da baştan sona yeni bir mahremiyet teorisine yatırım yapılmasına gerek yoktur. Petronio (2002) ile Palen ve Dourish de (2003), baştan sona yeni bir teori geliştirmek yerine, birbirlerinden farklı şekilde, mahremiyet teorilerini Altman'ın yaklaşımı üzerine inşa ederler.

1.1.3.1.1. İletişim Mahremiyeti Yönetimi (CPM) Teorisi

Petronio, “iletişim mahremiyeti yönetimi” (*communication privacy management*) teorisini, Altman'ın; bireyin kendini başkalarına açma ve kapatma arasındaki diyalektik mahremiyet anlayışına dayanarak geliştirir. İMY'nin (CPM), bilgisayar-dolayimli kişilerarası iletişimi anlamlandırmada en değerli mahremiyet teorilerinden biri olduğu söylenebilir (Margulis, 2011, ss. 12-13). Petronio'nun teorisini sunduğu kitabın önsözünde Altman, teknoloji ve küreselleşmenin hayatlarımızın iç içe geçmiş iki özelliği olduğunu ve askeri, politik, ekonomik ve bilimsel yönlerinin yanı sıra küreselleşme ve teknolojinin yarattığı hem kişisel hem de kişilerarası fırsat ve sorunları deneyimlemeye başladığımızı söyler. Altman, kendi diyalektik mahremiyet-ifşa dinamiğinde temellerini bulan İMY teorisini şöyle özetler: Bir dizi “kural” ve sınır koordinasyon ilkeleri tarafından yönetilen bir “sınır düzenleme” süreci olarak görülen diyalektik mahremiyet-ifşa dinamiği (Petronio, 2002, ss. xiii-xiv).

Petronio'nun İMY teorisini (CPM), kural-temelli yönetim sistemini destekleyen beş varsayım ortaya koyar: (1) özel bilgi (*private information*), (2) sınırlar (*boundaries*), (3) kontrol ve sahiplik (*control and ownership*), (4) kural-temelli yönetim sistemi (*rule-based management system*) ve (5) yönetim diyalektiği (*management dialectics*). İlk varsayıma göre, bireyler kendilerini açtıklarında özel bilgileri ifşa ederler. Başka bir ifadeyle ifşanın içeriği özel bilgilerdir. Bu açıdan değerlendirildiğinde, yakınlık (*intimacy*), kendini açma/ifade etme (*self-disclosure*) ile eş anlamlı değil, onun potansiyel bir sonucudur. Özel bilgileri paylaşmak, yakınlık kurmanın bir yolu olabilir, ancak yakın ilişkinin tüm boyutlarının yerine geçemez. Bunun sonucu olarak, ifşa ile yakınlık aynı şeyler değildir

ve her özel bilgi de yakınlık tesis edemez. Petronio'ya göre kişisel bilgileri paylaşmanın yakınlık kurma dışında da sebepler vardır. İnsanlar yüklerini hafifletebilmek, kontrolü ele geçirmek ve kendini ifade etmekten keyif almak için de kişisel bilgilerini paylaşabilirler (Petronio, 2002, ss. 5-6).

İMY teorisi, kamusal ve özel olan arasındaki ayrımı belirlemek için sınır metaforunu kullanır. Bireyler, bu sınırlar içerisinde özel bilgilerini tutarlar (Petronio vd., 1998). Bu teori içerisinde mahremiyet, bireyin kişisel veya toplu olarak özel bilgilere sahip olma hakkı olduğu duygusu olarak tanımlanır ve sınırlar bireyler için sahiplik alanlarını belirler. Kişisel sınırlar (*personal boundaries*), bireyin kendisine ait özel bilgileri tuttuğu alanı işaret eder. Kolektif sınırlar (*collective boundaries*) ise, toplu olarak tutulan mahremiyet sınırlarıdır. Çünkü bu sınırlar içerisindeki özel bilgiler sadece birey ile ilgili değildir. Kolektif sınırlar, içerisinde yönetilen özel bilgilerin türüne göre farklılaşır. Bu sınır içerisindeki bilgiler, bir gruba, çifte, aileye, organizasyona ve hatta bir bütün olarak bir cemiyyete ya da topluma özel olabilir. Bireyler kendi kişisel sınırlarının yanı sıra pek çok farklı kolektif sınırdan da sorumlu olabilir. Petronio'ya göre bu sınırlar geçirgen veya çok sağlam ve diğer mahremiyet sınırlarına bağlı olabilir. Sahipliği açıkça belirlenmiş ya da muğlak olabilir. İnsanlar özel bilgileri etrafındaki sınırları güçlendirmek ya da samimiyet kurmak amacıyla bu sınırları gevşetmek için çalışabilir. Hatta kimi zaman bu sınırlar, sahiplerinin kontrolü dışında gelişen olaylarla da zayıflayabilir. Bu da Petronio'nun çalkantı/türbülans (*turbulent*) olarak ifade ettiği sınır yönetimi sisteminde, dış kaynaklı saldırılar sonucunda oluşan aksaklığı meydana getirir (Petronio, 2002, s. 6).

Berardo, bireylerin mahremiyet sınırlarında yaşam süreci boyunca görülen değişikliklerin (*life span changes*) olduğunu söyler (akt. Petronio, 2002). Çocuklarda mahremiyet sınırları oldukça küçük bir alanı kapsar. Çocuklarda mahremiyet alanının sınırlı olmasında, çocukların öz benlikleri ve diğerleri arasındaki ayrımı yapamamaları ve mahremiyet yönetim sürecinin çocuklar için karmaşık olması etkilidir. Çocuklar, mahremiyet endişesi taşımaları da aileleri tarafından yavaş yavaş eğitilirler ve büyüyüp kendi bağımsız kimliklerini geliştirmeye başladıklarında kişisel olarak değerlendirdikleri bilgilerin etrafına sınırlar oluşturmaya başlarlar. Ergenlik dönemi ile bu sınırların kapsadığı alan büyür ve bireyin yetişkinliğe girmesiyle birlikte sınırlar genişleyerek hem kendilerine hem de diğerlerine ait olabilecek büyük miktarda özel bilgiyi kontrol etmeye

başlarlar. Ancak, yetişkinlikte genişleyen mahremiyet sınırları, bireyler yaşlandıkça daralır (Petronio, 2002, ss. 6-9). Bu daralmada, yaşlıların giderek artan güvenlik ihtiyaçları etkilidir. Bireyler yaşlandıkça, onlara banyo yaptıracak, finansal meselelerini yönetecek ve sağlık sorunları ile ilgilenecek birisine ya da birilerine ihtiyaç duyulabilir. (Petronio & Kovach, 1997). Sonuç olarak, mahremiyet sınırları bir ömür boyunca, bireye ait özel bilgileri barındıracak şekilde değiştirilir.

Kontrol ve sahiplik, İMY teorisindeki üçüncü varsayımdır. İnsanlar özel bilgilerinin kendilerine ait olduğunu düşünür ve onlar üzerinde kontrol sahibi olmayı arzular. Bu isteğin nedeni, özel bilgilerin nasıl yönetildiğine ilişkin risklerin varlığıdır. Başka bir ifadeyle bireyler, başkalarının kendileri hakkında bildiklerini belirleme hakkının kendilerinde olduğunu düşünürler ve kişisel bilgilerinin kendi alanlarında, yani mahremiyet sınırları içerisinde kalmasını isterler (Petronio, 2002, s. 9).

Petronio'nun teorisine göre, bireyler iki tip sınır (kişisel ve kolektif sınır) üzerinde çeşitli seviyelerde (yüksek, orta ve düşük) kontrole sahiptir. Bireyler, kendilerine ait özel bilgiler ve bu bilgilerin açığa çıkması ya da gizli tutulmasını yöneten sınırların kontrolü üzerinde hak iddia ederler. Bununla birlikte, insanlar başkaları ile paylaştıkları ya da başkaları tarafından paylaşılan özel bilgiler üzerinde de ortak mülkiyete sahiptirler. Kolektif olarak sahip olunan bilgiler, sırrı paylaşanlar ve sınırın içinde olduğu düşünülen kişilerle karşılıklı olarak kontrol edilir. Bu bilgiler tüm aileye ya da tüm şirkete ait özel bilgilerden oluşabilir. Petronio'ya göre kontrol, sahipliğin korunmasına yardımcı olur ve kontrole duyulan ihtiyaç özel bilginin sadece bir mülk olmadığını gösterir. Özel bilgiye sahip olma potansiyel kırılganlığı da içinde barındırır. Bilgiyi açıklama/paylaşma veya saklama arasındaki seçim, çoğu zaman dahil olanlar (sınırın içerisindekiler) için bir risk-fayda değerlendirmesine bağlıdır: Bilgileri açıklamak, bireyleri belirli bir ölçüde kırılgan yapabilir. Ancak, kimi durumlarda gizlemek de bu kırılganlığa neden olabilir. Bu kırılganlığa dayanarak Petronio, risk olasılığının mahremiyet yönetimi için kontrol sorunlarının önemini artırdığını söyler: “Ne kadar kırılganlık yaşamak istediğimizi belirleyerek risk-fayda oranımızı kontrol etme ihtiyacını hissediyoruz.” Sonuç olarak, bireyler, özel bilgilerin mülkiyeti ve/veya ortak mülkiyetinden kaynaklanan olası yükümlülükleri nedeniyle kişisel veya kolektif olarak tutulan sınırlar için sınır kontrolü uygular. Bireylerin kişisel veya kolektif kontrolündeki sınırlar kalın olduğunda, erişilebilirlik sınırlandırılır ve özel bilgi üzerinde yüksek seviyede bir kontrol sağlanır.

Yüksek kontrolün zıttı ise açıklıktır. Bu durumda sınırlar oldukça ince ve geçirgendir. İki kontrol seviyesinin arasında ise orta düzeyde kontrolün söz konusu olduğu görece ince sınırlar yer alır (Petronio, 2002, s. 10).

Petronio, iletişim mahremiyetinin, kural-temelli bir şekilde yönetildiğini varsayar. İMY teorisinin dördüncü varsayımını oluşturan kural-temelli yönetim (*rule-based management*) özel bilgilerin nasıl ele alındığına dair bir yapı sunar. Bu sistem üç sürece bağlıdır: (1) mahremiyet kurallarının temelleri (*privacy rule foundation*), (2) sınır koordinasyonu (*boundary coordination*) ve (3) sınır türbülansı (*boundary turbulence*). İlk süreç, kuralların geliştirilmesi ve özelliklerinin belirlenmesidir. İkinci yönetim süreci, kolektif sınırların yönetiminin kurallar aracılığıyla koordine edilişidir. Son süreç ise, koordinasyonun senkronize bir şekilde işleyemeyeceği varsayımına dayanır ve koordinasyonunun yanlış gittiğini ve kuralların eşzamansız hale geldiği zamanları işaret eder (Petronio, 2002, s. 12).

İMY teorisinin son varsayımı, mahremiyet yönetiminin diyalektik bir süreç olduğuna vurgu yapar. Petronio, teorisinin temel tezinin ifşa-mahremiyet (*disclosure-privacy*), saklama-açıklama (*concealing-revealing*), kamusal-özel (*public-private*), açıklık-kapalılık (*openness-closedness*) ve otonomi-bağılılık (*autonomy-connectedness*) arasındaki diyalektiğe dayandığını söyler. İMY, diğer diyalektik yaklaşımlarla benzerlik gösteren yönlerin yanı sıra farklı yaklaşımları da kapsar. En basit ifadesi ile İMY’de dikkate alınan diyalektik gerilim hem saklayarak mahremiyet yaratma hem de açıklayarak kamusal olma arasındaki birbirini baskılayan iki gücü dikkate alır. Petronio’ya göre; bu iki güç arasındaki tansiyon basit bir denklem değildir: Açıklamalar bilgiyi kamusal hale getirir. Kamusalılık derecesi, kaç kişinin bu bilgiye hâkim olduğu (sırrı paylaştığı), bilginin ne kadarının ifşa edildiği ve bilgiyi kimin aldığı gibi bir dizi konuya bağlıdır. Yine de bir kişi özel bilgileri bir kez ifşa ettiğinde, o bilgiler artık daha az özel ve daha fazla kamusaldır (*a little less private and more public*). Petronio, bu noktada kendi teorisini mevcut araştırmalardan ayırır ve çoğu araştırmanın kişinin ifşa ettiği zaman neyi bıraktığını, neyden vazgeçtiğini hesaba katmadan sadece açığa çıkarma boyutu ile ilgilendiğinin altını çizer (Petronio, 2002, s. 12).

Petronio, İMY teorisinin diyalektik olduğunu ortaya koymak için Baxter ve Montgomery’nin ilişkisel diyalektik (*relational dialectics*) teorisine atıfta bulunur.

Baxter ve Montgomery, teorilerinde dört diyalektik konsept sunarlar: (1) çelişkiler (*contradictions*), (2) diyalektik değişim/süreç (*dialectical change/process*), (3) bütünlük (*totality*) ve (4) pratik (*praxis*) (Wikipedia, 2020). Petronio, bu dört konsept üzerinden İMY teorisinde diyalektik bir konumun nasıl belirlendiğini gösterir. En açık ifadesiyle İMY teorisi, mantıksal değil, işlevsel zıtlıkları (*logical and functional opposites*) ve rasyonel değil, biçimsel nedenleri (*efficient and formal cause*) takip eder. İlişkisel diyalektik teorisinde sunulan değişim modelleri, teleolojik (tez-antitez-sentez) ya da son durumu olmayan sarmal bir değişimdir. Petronio, teorisinin iki değişim modelinin bir kombinasyonuna dayandığını ifade eder (Petronio, 2002, ss. 13-18).

İMY teorisine göre özel bilgilerin açıklanma ve/veya saklı tutulma dereceleri kural yönetim süreçleri aracılığıyla düzenlenir. Mahremiyet kuralları, özel bilginin kime, ne zaman, ne kadar çok veya ne kadar az ve nerede açıklanacağını (ifşa edileceğini) ya da nasıl gizli tutulacağını belirler. Petronio, mahremiyet kurallarının işleyiş şeklini yansıtabilmek için üç kural yönetim süreci tanımlar. Bunlar; (a) geliştirilme biçiminden niteliklerini oluşturan unsurlara kadar değişen mahremiyet kurallarının temelleri, (b) sınır koordinasyonu ve (c) çalkantılı durumları içeren sınır türbülansıdır. Mahremiyet kurallarının temelleri sürecinin iki özelliği vardır: gelişim ve nitelikler. İlk özellik, mahremiyet kurallarının hangi yolla geliştirildiğine odaklanır. Petronio'nun teorisine göre; bireyler mahremiyetlerini yönettikleri kuralları kültürel beklentiler, cinsiyet, bağlam ve risk-fayda oranı gibi kriterlerden etkilenerek geliştirirler (Petronio, 2002, ss. 23-24).

DeCew (1997), bireylerin kendi kültürlerinin çeşitli normları içinde sosyalleştiğini ve bu normların mahremiyeti kavrama biçimlerinin temelini oluşturduğunu söyler (akt. Petronio, 2002). Bu nedenle, kültürler mahremiyetin sosyal hayatta ne kadar rol oynadığı değişkenine göre farklılaşabilir. Ancak, hemen hemen her kültürde bir miktar mahremiyete ihtiyaç duyulur (Altman, 1977) ve sonuç olarak her birey kültürel değerleri göz önünde bulundurarak mahremiyetle ilgili beklentiler geliştirir (Petronio, 2002, s. 24).

İMY teorisindeki kuralların geliştirilmesinde etkili olan ikinci kriter cinsiyettir. Her ne kadar mevcut araştırmalarda cinsiyet farklılıkları sorgulanıyor olsa da, erkekler ve kadınların mahremiyet sınırlarını belirlerken kullandıkları yolların farklı olduğunu

gösteren kanıtlar vardır (Petronio & Martin, 1986). Sınır sistemleri içerisinde, erkeklerin ve kadınların, açığa vurmaya, ifşa etmeye ya da gizlemeye karar vermek için farklı kurallara sahip oldukları söylenebilir. Kültürel varyasyonlarda olduğu gibi, farklı cinsiyetler de sosyalleşme ve benzersiz mahremiyet anlayışlarına dayanan farklı kural setleri geliştirirler (Petronio, 2002, s. 24).

Bireylerin motivasyonları (dürtüleri), kural geliştirmede etkili olan diğer kriterdir. Bazı insanlar, kendi duygularını aktarma şansı arayışındayken, bazıları da tepkilerini maskeleyerek hissederek (E. E. Jones & Archer, 1976). Bireyler, mahremiyet kurallarını oluştururken belirli bilgileri açıklayarak kontrol sağlama arayışı veya kendilerini diğerlerinden koruma gibi dürtülerden de etkilenebilirler. Dürtülere (motivasyonlara) ek olarak, içerisinde bulundukları durumun bağlamı da kuralların temellerini etkiler. Bağlam, sosyal çevre ve fiziksel ortam olarak iki ögeye sahiptir. İlk öge, bir durumda belirli bir konuyu gündeme getirmenin uygunluğunu yargılama, değişen koşullar ve bir bağlam içerisinde ifşa etmenin veya gizlemenin zamanlaması gibi bağlamsal faktörleri içerir. Petronio, sosyal çevrenin bağlamsal etkisini yansıtmak için yeni boşanmış kişi örneğini verir. İkinci olarak, fiziksel ortamın açıklama/saklama kararına, bireylerin mahremiyeti tanımlama biçimine bir etkisi söz konusudur (Altman vd., 1981). “Fiziksel ortam hem sözlü olmayan davranışlarımızı hem de özel bilgileri ifşa etme ve gizleme konusundaki seçimlerimizi etkiler.” Bu nedenle, bazı ortamların doğası, ifşa etme veya gizliliği koruma kararını şekillendirebilir (Petronio, 2002, ss. 24-25). Petronio ve arkadaşlarının (1996) gerçekleştirdiği bir diğer araştırma, cinsel istismara maruz kalan çocuk ve ergenlerin, yaşadıklarını açıklamalarında fiziksel ortamın etkisini ortaya koyar. Bu araştırmanın bulguları, çocukların maruz kaldıkları istismarı, “güvenli sığınak” olarak nitelendirilebilecek ev ortamlarında ya da çocuğun güvendiği diğer bir kişiyle televizyon izlemek gibi günlük işlerle uğraştığı durumlarda açıkladığını gösterir.

Risk-fayda oranı kriteri, kural geliştirme sürecini etkileyen son kriterdir. Bireyler, açıklamanın ya da saklı tutmanın yaratacağını hissettikleri güvenlik açıklarını ve bekledikleri avantajları dikkate alırlar. Başka bir ifadeyle, bireyler mahremiyet sınırlarının içerisine erişim izni vermek veya reddetmek için riskleri ve faydaları değerlendirirler. Örneğin bireyler, ifşa etmenin faydalarının risklerinden daha fazla olacağını düşünebilir, açıklamanın ne ölçüde olumlu bir seçenek olduğunu hesaplayabilir ve bu hesaplamaları yansıtan kuralları geliştirip uygulayabilir. Tam tersi bir durumda ise,

istenilen mahremiyet seviyesini ve özel bilgileri korumak için kurallar geliştirilir (Petronio, 2002, s. 26).

Mahremiyet kurallarının temelleri sürecinin ikinci özelliği, kuralların niteliğidir. Petronio, kural niteliklerini iki boyutta inceler: (1) kural edinimi (*rule acquisition*) ve (2) kural özellikleri (*rule properties*). Kural edinimi boyutunda, öğrenilen ve müzakere edilen kurallar ayrımı yapılır. İnsanlar, önceden var olan kuralları sosyalleşme sürecinde öğrenirler. Örneğin aileler, çocuklarına mahremiyetin düzenlenme şekliyle ilgili aile üyelerinin sahip olduğu beklentileri öğretirler. Sosyalleşme yoluyla “öğrenilen” kuralların yanı sıra insanlar, belirli bir kolektif mahremiyet sınırı içerisinde topluca uyulan kurallar oluşturabilmek için yeni kuralları müzakere ederler. Müzakere edilen kurallar, açıkça ifade edilen ve sınır içerisindeki herkesin fikir birliğine vardığı veya daha belirsiz ve bireylerin fikir birliğine varmasını zorlaştıran örtük olarak ifade edilen kurallar olabilir (Petronio, 2002, ss. 26-27).

Petronio, kural niteliklerinin, mahremiyet kurallarının dinamik doğasını yansıtan çeşitli özelliklere sahip olduğunu söyler ve kural özellikleri boyutunda dört özellik tanımlar. İMY teorisine göre mahremiyet kuralları; rutinleşebilir, bir yönelim haline gelebilir, tetikleyici bir olayın ardından değişebilir ve yaptırımlar aracılığıyla kontrol edilebilir. Rutinleşen kurallara örnek olarak Petronio, bir çiftin cinsel hayatları ile ilgili bilgileri çocukları ile paylaşmaktan, tartışmaktan rutin olarak kaçınmasını gösterir. Bazı durumlarda ise bu mahremiyet kuralları, tekrarlanan kullanımlarla yerleşik hale gelir ve mahremiyet değeri ya da yönelimi olarak işlev görebilir (Karpel, 1980). Bazı ailelerde, ailenin tüm bireylerinin finansal meseleleri başkalarıyla konuşmaması, yönelim haline gelen kurallara örnek teşkil edebilir. Üçüncü özellik, mahremiyet kurallarının değişebilmesidir. Petronio’ya göre, bir olay veya durum kuralları yeniden düzenleme ihtiyacını tetiklediğinde kurallar değişebilir. Tetikleyici bir olayın ardından kuralların değişmesini gösteren en açık örnek, boşanan çiftlerdir. Mahremiyet kurallarının dördüncü özelliği ise, yaptırımlarla kontrol edilebilir olmasıdır. Belirli bir mahremiyet sınırı içerisinde yer alan bireyler, sınır erişimi veya korumayı düzenleyen kurallar hakkında bir anlaşmaya vardıklarında, bu onaylanmış kurallara uymayan kişilere cezalar verebilirler (Petronio, 2002, ss. 27-28).

İMY teorisi içerisinde tanımlanan ikinci yönetim süreci, sınır koordinasyonuna odaklanır. Teori içerisinde daha önce de vurgulandığı gibi, özel bilgileri sarmalayan sınırlar hem kişisel hem de kolektif sınırlar olabilir. Kolektif olarak tutulan sınırlar içerisindeki özel bilgiye, o sınır içerisindeki herkes doğrudan ya da dolaylı olarak ortaktır. Böyle durumlarda açıklamak veya gizlemek, sadece bireyi etkileyen bir karar değildir. Özel bilginin gizlenmesi ya da açıklanması, sınır içerisindeki herkesi etkileyeceği için tüm ortaklar bu sınırları koruyan kuralları koordine ederler. Bu koordinasyonun sağlanması için kuralların tüm ortaklar tarafından kabul edilmiş olması gerekir. Böylece tüm ortaklar arasında bir senkronizasyon sağlanır. Petronio, sınırların yönetimi sürecinin üç farklı yola bağlı olduğunu söyler: sınır bağlantısı (*boundary linkage*), sınır mülkiyet hakları (*boundary ownership rights*) ve sınır geçirgenliği (*boundary permeability*). Sınır bağlantısı, sınır ittifakları oluşturan bağlantıları temsil eder. Bireyler çekicilik, cinsiyet, hedef ile kurulan ilişki ve bağlantı kurma istekliliği gibi konulara dayanarak bir mahremiyet sınırına bağlanabilirler. Sınır mülkiyeti, bireylerin sahip oldukları ve başkalarının onları ortak sahip olarak görüp tanıdığı haklar ve ayrıcalıkları kapsar. Sınır geçirgenliği ise, sınır içerisinde tutulan özel bilgilerin ne kadarının sınırların dışına çıkabileceğini ifade eder. Sınır geçirgenlik seviyeleri, açık erişimden (ince sınırlar) kapalı erişime (kalın sınırlar) kadar değişiklik gösterir (Petronio, 2002, ss. 28-31).

İMY teorisinin tanımladığı üçüncü kural yönetim süreci, çalkantılı durumları içeren sınır türbülansıdır. Kolektif olarak korunan sınırlarda, sınır içerisindekiler arasındaki koordinasyonun doğası gereği, karmaşık ve çeşitli seviyelerde gerçekleşiyor oluşu, sınır türbülanslarını oluşturur. Türbülanslar, koordinasyon süreci boyunca çeşitli şekillerde ortaya çıkabilir. “Örneğin, insanlar mahremiyet kurallarını ihlal edebilir veya kötüye kullanabilir, bu da özel bilgilerin ne zaman, nerede, nasıl ve kiminle açıklanabileceğini senkronize etme yeteneğini engelleyebilir.” Kural geliştirmede farklı kriterlerin kullanılması ve açıklama/gizlemeye dair farklı risk seviyesi algısı da sınır türbülansı yaratabilir. Bunların yanı sıra, sınırların geçirgenlik seviyesi koordine edilmediğinde veya sahiplik beklentilerini ihlal eden sınır bağlantıları oluştuğunda da çalkantılı durumlar oluşabilir. Petronio, sınır türbülansının sınır koordinasyonunun her zaman pürüzsüz işlemediğini ve sınır düzenlemesinin de mükemmel bir sistem olmadığını söyler. Sınır türbülansı gerçekleştiğinde, bireyler sorunu düzeltmeye ve kural sistemine yeni bilgileri entegre ederek tekrar koordinasyonu sağlamaya çalışırlar. Bu,

İMY teorisinin sunduğu sistemi açık bir sistem haline getirir. Başka bir ifadeyle bu teori, sistemin gelişmesi ve işlevsel kalması için kendi kendini düzelten eylemlerin gerçekleşmesine yer bırakır. Bu sayede bireyler, yeni durumlara ve farklı gereksinimlere uyum sağlayarak, mahremiyet sınırları üzerinde belirli bir kontrol düzeyini koruyabilmeleri için kuralları kendi ihtiyaçlarına göre değiştirebilirler (Petronio, 2002, s. 33).

1.1.3.1.2. Genişletilmiş Mahremiyet Düzenleme (*Privacy Regulation*) Teorisi

Palen ve Dourish (2003), Altman'ın (yukarıda değinilen) mahremiyet teorisini, enformasyon teknolojileri kaynaklı tehdit ve imkanları da dahil ederek genişletir. Mahremiyet yönetiminin sadece belirli kurallar belirlemek ve uygulamak ile ilgili olmadığını; daha ziyade, farklı eylem alanları arasındaki sınırların ve bu alanlardaki ifşa derecelerinin sürekli yönetimi olduğunu söyler ve şunları eklerler: “Bağlam değiştikçe sınırlar dinamik olarak hareket eder. Bu sınırlar, çelişen hedefler arasındaki gerilimleri yansıtır; sınırlar denge ve çözüm noktalarında oluşur.” Araştırmacılar, bu sınır yaklaşımında enformasyon teknolojilerinin sınırların denetimini bozma ya da istikrarsızlaştırma yeteneğine vurgu yaparlar ve teknolojinin rolünü daha iyi kavramak için üç farklı sınır tanımlarlar: İfşa sınırı (*disclosure boundary*), kimlik sınırı (*identity boundary*) ve zamansal sınırlar (*temporal boundaries*) (Palen & Dourish, 2003, s. 131). Her bir sınırda bir gerilim söz konusudur: İfşa sınırı, mahremiyet ve aleniyet; kimlik sınırı, benlik ve diğerleri; geçici sınırlar ise, geçmiş ve gelecek arasındaki gerilimin çözüldüğü noktalarda oluşur.

İfşa sınırı, mahremiyet denetiminin sadece bilgi ifşasından kaçınmak olmadığı yaklaşımına dayanır. Sosyal dünyaya katılım, seçici de olsa kişisel bilgilerin ifşasını gerektirir. Aynı şekilde, ağa bağlı dünyanın (ağ toplumunun) bir parçası olmak da kişisel bilgilerin erişime açılması, paylaşılması ile mümkün olur. Kişi, nasıl ürün ve hizmet satın almak için dışarı çıktığında, kamusal alanda “görünür” hale geliyorsa, çevrim içi alışverişi için de kişisel kimlik bilgilerini gerekli işlemsel amaçlar nedeniyle “ifşa” eder. Palen ve Dourish'e göre sorun, katılımın kasıtlı olmadığı ya da kimlik tanımının sınırlarının kişinin kontrolü altında olmadığı durumlarda ortaya çıkar. Örneğin, kişi tarafından yapılan herhangi bir Google araması bile, kişi hakkında geçmiş işlemlere dair izler de dahil olmak üzere, önemli miktarda bilgi açığa çıkarabilir. Başka bir şekilde ifade

edilirse, ifşa sınırı, mahremiyet ile aleniyet arasındaki gerilimdir (Palen & Dourish, 2003, s. 132).⁵

Kimlik sınırı, mahremiyet yönetimindeki ikinci gerilim noktasıdır ve benlik ile diğerleri arasındaki sınırı işaret eder. Palen ve Dourish'e (2003) göre, dolayım ya da arabuluculuk (*mediation*) teknoloji yoluyla sağlanan etkileşimin temel sorunudur. Biriyle doğrudan etkileşim kurmak yerine teknoloji dolayımı ile iletişim kurulduğunda, kişi ile değil, vekil görevini üstlenen bir temsil ile etkileşim kurulmuş olur. Teknolojinin aracılık ettiği ortamlarda, bu vekil temsiller hem verimsizdir hem de bu ortamlarda benlik ve diğerleri arasındaki sınırın göstergeleri belirgin değildir. Teknoloji aracılığı ile kurulacak etkileşimde, alıcının uygunluk ve erişilebilirlik derecesi gibi değişkenler belirleyicidir. Buna rağmen, kurulan etkileşim ile amaçlanan aynı olmadığında, işler karışabilir. Bu karışıklık, (mahremiyeti) düzenleyici güçler dengeyi sağlayamadığında oluşur. Çünkü, etkileşimin niyeti, yeterince iletilemez ya da anlaşılır olmaz.

Kimlik sınırı cephesinde işleri karıştıran bir diğer unsur da teknoloji sayesinde bilginin kalıcı hale gelmesidir. Kalıcı hale gelen enformasyon, benlik ve diğerleri arasındaki sınırın denetimini ve kişinin, bu enformasyon ile ne kadar temsil edebileceği hakkındaki düşüncelerini karmaşıktırır. Kalıcı hale gelen bu enformasyon, her zaman kişinin kontrolünde değildir. Örneğin, internet sitesi ziyareti bile, çerezler aracılığı ile kişi hakkında kalıcı bir bilgi üretir (Palen & Dourish, 2003, s. 132).

Geçici sınırlar, bilginin geçmiş, şimdi ve gelecek zaman arasında kolayca erişilebilir olması ile ilgili olduğu söylenebilir. Palen ve Dourish (2003, s. 133), teknolojinin bilgiyi kolayca erişilebilir hale getirmesi ve geçici bilgileri dahi kalıcı hale getirme yeteneği, açığa çıkmanın (ifşanın) zamansal yapısını etkilediğini söylerler, ama bunun mahremiyet denetimini tamamen ortadan kaldırmadığını da eklerler. Bilginin gelecekteki kullanımları üzerinde tam kontrol sağlanamayacağı için, bunun yerine bilginin doğası veya formatı yönetilebilir.

⁵ Kullanıcının tam kontrolünde olmadan meydana gelen bilgi sızıntıları ile ilgili örnekler çoğaltılabilir. Bu açıdan, dijital dünyada mahremiyetin korunması için farkındalığın artırılmasının oldukça önemli olduğunu söyleyebiliriz.

1.1.3.2. Dijital Dünyada Mahremiyetin Sınırlanması

Petronio'nun İMY teorisi ile Palen ve Dourish'in genişletilmiş mahremiyet denetimi yaklaşımı, enformasyon ve iletişim teknolojileri aracılığıyla sosyalleşme ve kimlik yaratma pratiklerini ele alırken önemli bir başvuru kaynağı olabilir. Ancak, yukarıda aktarılan sınırları ve gerilimleri etkileyen farklı bir değişken vardır: güvenlik ya da güvende hissetme ihtiyacı. Bu ihtiyaç, Petronio'nun anlayışı içerisinde açığa çıkarmanın veya gizlemenin riskleri ve faydaları arasındaki diyalektik ile ele alınabilir.

Güvenlik ihtiyacı bireyleri, özellikle enformasyonel mahremiyetlerinden feragat etmeyi göze almaya itmekte, ya da zorunda bırakmaktadır. Saklayacak bir şeyinin olması, şüpheli veya kanuna aykırı eylemler gerçekleştirilmesi ile ilişkilendirilmektedir. Bu ilişkilendirme ile ilgili en çarpıcı örnek, Google'ın eski yöneticisi Eric Schmidt'in, "hiç kimsenin bilmesini istemediğin bir şeyin varsa, belki de bunu en başından yapmaman gerekiyordur" şeklindeki açıklamasıdır (Esguerra, 2009). Güvenliği, otorite tarafından vatandaşlara sunulan bir hizmet olarak değerlendirirsek, mahremiyetin belirli bir hizmete erişmek için bir kenara bırakıldığını söyleyebiliriz. Bu feragat, sadece güvenlik hizmeti ile sınırlı değildir. Enformasyon ve iletişim teknolojilerinin sağladığı diğer hizmetler de zaman zaman kişisel verilere erişimi, sundukları hizmete ulaşmak için bir önkoşul olarak sunmaktadırlar. Kullanıcı, profilindeki bilgilerinin açığa çıkmasına rıza göstermese bile, buna zorlanabilir (Brunnstein'den akt. Fischer-Hübner, 1998, ss. 426-427). 2010 yılında yapılan bir araştırmada, katılımcıların yüzde 43'ü, bir çevrim içi hizmete erişim sağlamaya veya bir hizmeti kullanmaya çalıştıklarında, kendilerinden gerekenden daha fazla kişisel bilgi istendiğini ifade etmiştir. Yine aynı araştırmada, AB vatandaşlarının yüzde 74'ü, kişisel bilgi ifşasını modern dünyanın yükselen trendi olarak görmekte, sosyal ağ ve paylaşım sitesi kullanıcılarının yüzde 61'i ve çevrim içi alışveriş yapanların da yüzde 79'u, çevrim içi hizmetlere erişimi bilgi ifşasının en önemli gerekçesi olarak ifade etmektedir (TNS Opinion & Social, 2011, s. 1). Bu durumla ilgili sayısız örnek sıralanabilir. Akıllı cep telefonları üzerinde kullanılan pek çok uygulama, kullanıcıların arama kayıtlarına, cihazda kayıtlı fotoğraf/video gibi içeriklere, mikrofona ve kameraya ve konum bilgilerine erişimi talep etmektedir. Bu talebin kabul edilmediği durumlarda, istenilen hizmetten ya hiç yararlanılamamakta ya da hizmete sınırlı bir şekilde ulaşılmaktadır. Örneğin, *Google Keep* adlı kişisel not tutma programı, kullanıcılarına coğrafi konum bazlı hatırlatmalar yapabilmektedir. "Ofise gittiğimde bana toplantımı

hatırlat” şeklinde oluşturulabilecek bir anımsatıcı için, uygulamaya hem anlık konum bilginize erişim iznini hem de ofisinizin konumunun bilgisini vermeniz gerekmektedir. Aynı şekilde, cep telefonu ile çekilen fotoğrafların üst verilerine, coğrafi konum bilgisinin bulunması istendiğinde hem cihazın GPS (*Global Positioning System*) alıcısının aktif durumda olması hem de kamera uygulamasının bu alıcının sağladığı koordinat bilgisine erişebilmesi gerekmektedir.

Dijital dünyada bireylerin mahremiyetlerini ikinci plana itmelerinde etkili olan bir diğer etken de sosyal paylaşım ağları üzerinde bir kimlik oluşturmak ve bu kimlik üzerinden sosyalleşebilmektir. Tüfekçi (2008, s. 21), “teknoloji aracılığıyla sosyallikte, görülmek istediklerimiz tarafından, dilediğimiz şekilde görülmek ve böylece kimlik dışavurumu, iletişim ve izlenim yönetiminin bir parçası” olmanın merkezi motivasyonlar olduğunu söyler. Zhang ve arkadaşları da (2010, s. 13) çevrim içi sosyal ağların, belirli kişilerle ya da ağa katılan tüm kullanıcılarla kolayca bilgi paylaşımını mümkün kılmasının ve sosyal ağların diğer kullanıcıları ile sosyal etkileşim sağlamasının kullanıcıların bu ağlara katılmalarının en temel motivasyonlarından biri olduğunu ifade eder. Bu motivasyonlar, literatürdeki pek çok çalışmada da karşılaşıldığı gibi, mahremiyet endişelerinin bir kenara bırakılmasını beraberinde getirir (bkz. Debatin vd., 2009). Çevrim içi sosyal ağ sitelerinde kişisel bilgileri paylaşmak, iki ucu keskin bir kılıca benzetilebilir (He & Chu, 2008; C. Zhang vd., 2010).

Warren ve Brandies makalelerinde, gazetelerin özel hayat üzerindeki etkilerini tartışmıştır. Løkke, bu tartışmanın günümüzde daha çok önem taşıdığını söyler. Çünkü günümüzde, herkes her şeyi internetten paylaşabilir ve bu paylaşımlar birkaç saat içinde gerçekliği dahi kontrol edilmeden milyonlarca kişiye ulaşabilir. Gazetelerdeki gibi bir redaktörün sorumluluk alanına girmeyen içerikler internette sonsuza dek saklanabilir ve insanların resmi itibarına zarar verecek bilgiler içerebilir (Løkke, 2018, s. 45). Enformasyonun bu derece süratli bir yayılım gösterebildiği çağda, kişisel itibara zarar verebilecek bilgiler hem mahremiyeti ifşasından kaynaklanan bilgi sızıntıları hem de (siber) saldırı tekniklerinden kaynaklanan bilgi sızıntıları ile gerçekleşebilir (X. Chen & Michael, 2012, s. 52).

Pew Research Center’in 2014 yılında yayınladığı “*The Future of Privacy*” başlıklı raporu, 2025 yılında mahremiyetin durumu ile ilgili çeşitli tahminleri içerir.

Mahremiyetin geleceğini keşfetmek için, 2500'ün üzerinde uzman ve internet sitesi kurucusunun yorumlarına danışılır. Birçoğu internetin evriminde teknoloji oluşturucular, araştırmacılar, yöneticiler, politika yapımcılar, pazarlamacılar ve analistler olarak aktif rol oynayan uzmanlardan oluşan katılımcılardan birbiri ile ilişkili üç açık uçlu soru yöneltilir. İlk soru; “*politika yapımcılar ve teknoloji geliştiricileri, 2025 yılına kadar ... güvenli, büyük oranda kabul gören ve güvenilir bir gizlilik hakları altyapısı oluşturacaklar mı?*” şeklindedir. İkinci soruda katılımcılardan, ilk soruya verdikleri cevabı detaylandırmaları ve son soruda ise mahremiyetin geleceğini daha geniş bir sosyal bağlamda ele almaları istenir. Araştırma merkezinin “tetkik” (*canvassing*) olarak nitelendirdiği bu çalışmaya katılanların yüzde 55'i, gelecek on yılda kabul edilmiş bir gizlilik hakları rejiminin ve altyapısının oluşturulacağına inanmadıklarını ifade etmiş, yüzde 45'i ise bu konuya daha olumlu yaklaşmış ve böyle bir rejimin ve altyapının oluşturulacağını söylemiştir. Bu keskin ayrıma rağmen hem evet hem de hayır diyen kullanıcıların paylaştığı fikirler de vardır: “Çevrim içi hayat doğası gereği oldukça kamusaldır.” Anonim bir katılımcı ise mahremiyetin yeni bir tabu olacağını ve gelecek nesillerin bunu takdir etmeyeceğini ya da anlamayacağını söyler (Pew Research Center, 2014, ss. 5-6). Washington Üniversitesi'nde görev yapan Gina Neff'e göre, mahremiyete yönelik müdafaa ve eğitim çabaları arttırılmadığı sürece, insanlar hizmetler için mahremiyetlerini değiş tokuş etmeyi giderek daha fazla kabul edeceklerdir. Eğitimin önemini vurgulayan bu yaklaşımdan farklı olarak, Nick Arnett isimli iş zekası uzmanı ise toplum tarafından kabul edilen mahremiyet ve özgürlük tanımlarının 2025'te fazlasıyla değişeceğini ve günümüzdeki tanımlamaların işlevlerini yitireceğini söyler ve evrilen tanımlamalara yönelik tartışmaların süreceğini de ekler (Pew Research Center, 2014, s. 8).

Dave Eggers, Çember (*The Circle*) adlı romanında, sosyal medyanın ve mahremiyetin geleceği hakkında ürkütücü, ancak olası bir öngörü sunar. Belirsiz bir tarihte geçen romanda, Çember adındaki sosyal medya şirketi, internet üzerinde kullanılan pek çok hizmeti birleştiren ve tek bir kullanıcı hesabıyla tüm bu hizmetlerden faydalanmaya fırsat veren bir girişimdir. Romanda baş kahraman olan Mae'nin, bu şirketin müşteri ilişkileri departmanında çalışmaya başladıktan sonra hayatında gerçekleşen değişimler anlatılır. Örneğin Mae, bu şirkette çalışmaya başladıktan sonra ailesi için bir sağlık sigortası ayarlamaya çalışır ve hasta babasının yüklü tedavi masraflarını bu sigorta ile karşılamaya çalışır. Bunu başarır, ancak karşılığında ailesi ev

içi mahremiyetinden olur. Evin neredeyse tüm odalarına kamera yerleştirilir ve internet üzerinden 24 saat canlı yayınlanır. Ailesine yardım ettiğini düşünen Mae, bir süre sonra kendi hayatındaki mahremiyet alanının da onun tercihleri dışında daraltıldığını fark eder: Bir hafta sonu, ara ara gittiği bir sahilde kanoda kürek çeken Mae, bu aktivitesini sosyal medya üzerinde paylaşmadığı için üstleri tarafından “kınanır.” Romanın sonunda ise Mae, tüm hayatının göğsünde taşıdığı bir kamera ile canlı olarak yayınlanmasını kabul edecektir. Eggers’ın romanında ortaya koyduğu bu ürkütücü gelecekte, çarpıcı olan nokta ise Çember şirketini oluşturan fikri bulan kişinin de yarattığı şeyden korkmaya başlaması ve işin kendisinin kontrolünden çıktığını düşünmesidir (Eggers, 2017).

1.1.3.2.1. Güvenli Bir Yaşam Sürme ve Mahremiyet İlişkisi

Kişi, akıllı telefonsuz, internetsiz ya da banka kartsız yani tamamen analog bir hayat sürmeye kalkıştığında, bu tavır yöneticilerde kuşku uyandıracaktır. İnsanlarda, söz konusu kişinin saklayacak bir şeyi olduğuna dair, pek de nedensiz olmayan bir merak uyandıracaktır çünkü o kişi, elektronik iz bırakmamak adına, bir sürü angarya işe katlanmayı kabul etmeye razıdır (Løkke, 2018, s. 11).

Mahremiyeti korumak için dijital hayattan kaçınmanın doğuracağı muhtemel sonuçlarla ilgili olarak, Julia Angwin’in “*Kuşatma Altındaki Ulus: Sürekli Gözetlenen Bir Dünyada Mahremiyet, Güvenlik ve Özgürlük Arayışı*” (Drugnet Nation: A Quest for Privacy, Security and Freedom in a World of Relentless Surveillance) adlı kitabına değinilebilir. Bu çalışmasında Angwin (2015), analog bir yaşam sürmeye çalışarak elektronik gözetimden kaçabilmenin ne kadar mümkün olacağını araştırmıştır. Bu araştırmanın sonucunda Angwin, gözetlemeden kurtulmaya çalışması nedeniyle resmi mercilerin dikkatini çekmiştir. Bu çıktıdan hareketle, modern insanların dijital ekonomi içerisinde yaşamaya neredeyse mahkum oldukları söylenebilir (Løkke, 2018, s. 12).

“Saklayacak bir şeyiniz yoksa korkacak bir şeyiniz de yoktur.” Bu argüman, güvende hissetmek için mahremiyet hakkınızın ihlal edilebilir olduğunun normalleştirilmesinde çeşitli şekillerde kullanılmaktadır. Yukarıda da aktarıldığı gibi, Google’ın 2009 yılında, yönetim kurulu başkanlığını yapan Eric Schmidt, “Başkalarının bilmesini istemediğiniz bir şeyler yapıyorsanız, belki de bunu hiç yapmamalısınız” şeklinde bir röportaj vermiştir (Tate, 2009). Schmidt daha sonra, “Özel hayatı korumak için mücadele etmeliyiz, yoksa onu kaybetme tehlikesi ile karşı karşıya kalırız” diyerek tutumunu yumuşatmıştır (Colvile, 2013). Schmidt’in bu yaklaşımı, Westin’in bireysel

özerklik, duygusal rahatlama, kendini değerlendirme ve sınırlı ve korumalı iletişim olarak sıraladığı mahremiyet işlevlerini hiçe saymaktadır. Løkke de (2018, s. 22) yukarıdaki argümana karşı, özel hayatın saklayacak bir şeyin olup olmamasıyla ilgili olmadığını söyler ve özel hayatın, “vatandaşların kendi istekleri ve olanakları doğrultusunda hareket edebilme özgürlüğünün korunması” olduğunu, “başka bir deyişle, vatandaşların kendi başlarına iyi bir hayattan ne anladıklarını tanımlamaya ve bunu en iyi biçimde gerçekleştirmeye olanak bulabildikleri bir alan” olarak nitelendirilebileceğini vurgular. Schneier (2006) de, Mahremiyetin Ebedi Değeri (*The Eternal Value of Privacy*) adlı yazısında, benzer bir çizgide, mahremiyetin yanlış olanı saklamak olarak algılanmasının yanlış olduğunu ifade eder ve mahremiyetin en temel insan ihtiyacı olduğunu altını çizer.

Avrupa Birliği ülkelerinde gerçekleştirilen kamuoyu anketleri, mahremiyet ve güvenli bir yaşam arasındaki ilişkiyi açıklayan bazı sonuçlar sunar: 2008 yılında yapılan saha araştırmasına göre, çoğu AB vatandaşının gözünde, uluslararası terörizm ile mücadele, veri koruma haklarının sınırlandırılması için kabul edilebilir bir gerektir. Katılımcıların yüzde 82’si yolcu uçuş bilgilerinin, yüzde 72’si telefon görüşmelerinin, yüzde 75’i internet kullanımlarının ve yüzde 69’u da kredi kartı kullanımlarının terörle mücadele kapsamında izlenebileceğini ifade etmiştir. Aynı zamanda, katılımcıların yüzde 35’i bu izlemelerin sadece şüphelileri kapsamaması gerektiğini eklemiştir. Bu araştırmadaki bir diğer önemli çıktı, son beş yılda internet kullanımlarının ve telefon görüşmelerinin izlenmesini onaylayanların yaklaşık yüzde 12 artmış olmasıdır (The Gallup Organization, 2008, s. 6).

Løkke (2018), eski NSA çalışanı Snowden’in ifşaatlarını, dijital dünyada mahremiyet ve özel hayat açısından bir dönüm noktası olarak nitelendirir. Løkke’ye göre; sürekli dijitalleşen dünyada mahremiyet ile ilgili en büyük sorun, insanların bu konuda çok az endişelenmeleri ve pek çok kişinin gelişmelerden hiç rahatsızlık duymamaları, normal vatandaşın izlenmesini ve devletin yetkilerinin genişletilmesini, neredeyse büyük ölçüde kabul etmeleridir. Ancak yine de Snowden sonrasında, mahremiyetle ilgili endişede bir artış olduğu söylenebilir. 2013 yılında Norveç’te yapılan bir araştırmaya göre, katılımcıların yüzde 26’sı mahremiyetin korunmasıyla çok ilgili, yüzde 61’i de oldukça ilgili olduklarını belirtmiştir. Bu rakamlar, 1997 yılında sırasıyla yüzde 22 ve

yüzde 55'tir. Mahremiyetin korunmasıyla az ilgiliyim diyenlerde de yüzde 10'luk bir azalma söz konusudur (Løkke, 2018, s. 53).

Mahremiyet ve güvenlik arasındaki ilişkiyi konu alan PRISE⁶ kısa adlı Avrupa Birliği projesinde, mahremiyetin demokrasi için bir önkoşul olduğu vurgulanmış ve projenin final konferansında, hiçbir güvenlik teknolojisi ya da otorite tarafından dokunulamayan temel bir mahremiyet alanının tanımlanmasına dikkat çekilmiştir. Takas modelinin (*trade-off model*), mahremiyet ve güvenlik arasındaki ilişkiyi açıklamakta yetersiz kaldığı, ikisi arasındaki değiş-tokuşun sonucunun sıfır olmadığı ve bu ilişkinin, modelin önerdiğinden daha karmaşık olduğu ifade edilmiştir. Aktarılan bir diğer bulgu da emniyet güçlerinin mevcut veri tabanlarına genel erişiminin, mahremiyet açısından kabul edilemez olduğudur. Araştırma sonucunda, mahremiyeti korumanın herkes tarafından paylaşılması gereken bir sorumluluk olduğu vurgusu yapılmış ve mahremiyeti korumanın bir süreç olarak düşünülmesine, ilgili kriterlerin ve yönetmeliklerin düzenli olarak güncellenmesi gerektiğine değinilmiştir. Son olarak, güvenlik sistemlerinin geliştirilmesi aşamasına, mahremiyetin arttırılmasının da dahil edilmesi gerektiğinin altı çizilmiştir (PRISE, 2008). İnternetteki güvenlik problemlerinin temel nedeni olarak, internetin başlangıçtaki tasarımında güvenliğin önemli bir yön olarak ele alınmadığı ve sonradan yapılan düzenlemelerin sadece riski azaltabileceği (Fischer-Hübner, 1998, s. 429) dikkate alındığında, araştırma projesindeki bu vurgunun önemi daha da belirginleşebilir.

PRISE projesinin devamı olarak nitelendirilebilecek olan ve dokuz Avrupa Birliği ülkesinin katılımıyla gerçekleştirilen SurPRISE⁷ adlı projede ise gözetim ve mahremiyet konuları ele alınmıştır. Gözetim, mahremiyet ve güvenlik arasındaki ilişkiye hem akademik perspektiften hem de vatandaşların bakış açısını yansıtacak şekilde yaklaşan projede, yaklaşık bin AB vatandaşının katıldığı bir araştırma yapılmıştır. Bu kapsamlı araştırmadaki, “online olduğumda güvenlik için endişelenirim” (*I worry about security when I am online*) sorusuna katılımcıların yüzde 28'i “kesinlikle katılıyorum”, yüzde 33'ü ise “katılıyorum” cevabını vermiştir. Katılımcıların yüzde 68'i, gözetim temelli

⁶ Privacy enhancing shaping of security research and technology – A participatory approach to develop acceptable and accepted principles for European Security Industries and Policies

⁷ Surveillance, Privacy and Security: A large scale participatory assessment of criteria and factors determining acceptability and acceptance of security technologies in Europe.

güvenlik teknoloji kullanımının kişisel mahremiyeti erozyona uğratacağından endişelenmektedir. 30-39 yaş aralığındaki katılımcıların neredeyse beşte dördü, mahremiyet erozyonu konusunda endişelenmektedir. Eğitim seviyesindeki farklılıklar, katılımcıların mahremiyet erozyonuna ilişkin endişelerinde büyük bir farklılık yaratmamıştır (Strauß, 2015, ss. 23-27).

Daniel J. Solove, *Nothing to Hide* adlı kitabında, mahremiyet ve güvenlik arasındaki “sahte” takası konu alır. Solove, geride bıraktığımız yüzyıl boyunca, bilgi çağına doğru yol alırken, hükümetlerin de güvenliği koruma tekniklerini geliştirdiklerini söyler ve günümüzde emniyet güçlerinin, kayıtları ve verileri bir araya getirmek, sesli ve görüntülü gözetimleri ilişkilendirmek ve hareketi takip etmek için teknolojiyi kullandığını dile getirir. Yazar, bilgi toplama (*information gathering*) kavramını, hükümetin insanların ne yaptıklarını ne düşündüklerini ya da planladıklarını öğrenmek için kullandıkları yöntemleri ifade etmek için kullanır. Hükümetler, bilgi toplamanın yanı sıra, onları depolar, kullanır, analiz eder, birleştirir ve bazen de ifşa edebilir. Tüm bu aktiviteler, mahremiyeti tehdit etmektedir (Solove, 2011, s. 12).

Tarihsel olarak, devletlerin güvenlik tesis etme ihtiyaçları ile bireylerin kişisel mahremiyetleri arasında yinelenen bir çatışma olmuştur ve olmaya devam etmektedir (Strickland & Hunt, 2005, s. 226). Bu çatışmadan hareketle, güvende hissedebilmek, güvenli bir hayat yaşayabilmek ile özel hayatı ve mahremiyeti korumak arasında bir orta yol, bir dengenin bulunmasının oldukça önemli olduğu söylenebilir. Bu denge hem yasal olarak hükümetler tarafından hem de dijital teknolojilerin kullanımları sırasında vatandaşlar tarafından sağlanabilir. Mahremiyeti korumak için gözetimin nerede durması gerektiği ya da güvende hissedebilmek için mahremiyetten ne kadar vazgeçilebileceği sorusu bu çalışmada doğrudan cevabı aranan sorular değildir.

1.1.3.2.2. Kimlik Oluşturma, Sosyalleşme ve Mahremiyet İlişkisi

Sosyal bir varlık olarak insan, etkileşim kurabilmek için tam izolasyondan kaçınır ve kendini “ifşa” eder. Altman’ın, arzu edilen ve elde edilen mahremiyet (*desired and achieved privacy*) kavramlarına dayanarak ilerlersek, kişinin elde ettiği mahremiyet arzu ettiğinden fazla olursa, bir çeşit sosyal izolasyon durumu oluşur. Tam tersi durumda ise istenmeyen bir sosyalleşme, kalabalıklaşma (*crowding*) meydana gelir. Görüldüğü gibi, Altman’da mahremiyet denetimi, dinamik bir süreçtir. Bu süreç, enformasyon ve iletişim

teknolojileri ile dolayımlanmış sosyalleşme için de geçerliliğini korumaktadır. Altman'ın diyalektik mahremiyet anlayışı, Palen ve Dourish tarafından enformasyon ve iletişim teknolojileri çağına uyarlanır. Onların tanımladıkları (yukarıda değinilen) sınırlar, mahremiyet-aleniyet, benlik-diğerleri ve geçmiş-gelecek arasındaki gerilimlerin bir yansımasıdır.

Sosyal ağ sitesi kullanıcısı olan bir kişi, etkileşim kurabilmek için belirli miktarda kişisel bilgisini “ifşa” eder. “Çoğu durumda, bu teknolojik araçlardan yararlanabilmek için benlik hakkında bilgi vermek bir gerekliliktir (Ellison vd., 2011, s. 20).” Bu teknolojilerden ve/veya sosyal ağ sitelerinden faydalanmak için kişisel bilgiler ifşa edilirken, özellikle bilginin kalıcılığı ve/veya istenmeyen kişiler tarafından erişilebilirliğinden kaynaklanan bir gerilim hissedilebilir. Bireyler, bilgilerini paylaşmanın yarattığı mahremiyet riskinin farkında olmayabilir, bu riski önemsemeyebilir ya da sosyalleşebilmek uğruna göz göre göre bu riski alabilir. Bu açmaz, Barnes (2006) ve Norberg vd. (2007) tarafından mahremiyet paradoksu (*privacy paradox*); Brandtzæg ve ekip arkadaşları tarafından ise (2010, s. 1007), mahremiyet ikilemi (*privacy dilemma*) olarak nitelendirilir. Terazide mahremiyet ağır bastığında, sosyalleşme ve içerik paylaşımı tehlikeye girerken mahremiyete oranla sosyalleşmeye daha fazla önem verilince de mahremiyet zarar görmektedir. Her iki durumda da arzulanmayan bir sonuç ortaya çıkar. Livingstone (2008, s. 407), bu ikilemin iki ucunda bulunan fırsatlar ve riskleri dikkate alarak, geç modernitedeki kendini gerçekleştirme anlayışına atıfta bulunur: fırsatlar ve riskler arasındaki denge. Bu yaklaşımı, 13-16 yaşlarındaki gençler üzerinde gerçekleştirdiği derinlemesine görüşmelerden elde ettiği bulgularla ilişkilendirir. Livingstone'a göre; günümüz gençlerinin kendilerini gerçekleştirmeleri, internet tabanlı iletişimin sağladığı fırsatlar (kimlik, yakınlık, sosyallik) ve riskler (mahremiyet, yanlış anlaşılma, istismar) arasında dikkatli bir müzakereyi içerir. Bu ikilem ve sunduğu fırsatlar ve riskler göz önünde bulundurulduğunda, enformasyon ve iletişim teknolojilerinin sunduğu araçlar üzerinde bilgilerini ifşa ederek bir benlik sunumu yaratma ediminin, mahremiyet ihlallerini de beraberinde getirdiği söylenebilir.

Sosyal ağ siteleri, farklı birçok insan tarafından, çeşitli amaçlarla erişilebilir olan bir kimlik yaratımını içerirler. Bu kimliklerin içerdiği kişisel bilgiler, benzer ilgi alanlarına sahip yeni insanlarla tanışmak, romantik bir ilişki ya da cinsel bir birliktelik

yaşamak veya iş bulmak gibi değişken amaçlara bağlı olarak çeşitlilik göstermektedir (Stefanick, 2011, s. 172). Boyd ve Heer'in işaret ettiği gibi (2006), sosyal ağ sitelerindeki profil sayfalarının, birer kimlik sunma aracı haline geldiği söylenebilir. Bunun yanı sıra, kullanıcılar sadece benliklerini sunmak için değil aidiyet hissetmek için de sosyal ağ sitelerine katılırlar. Gangadharbatla (2008), aidiyet ihtiyacı ile sosyal ağ sitelerine katılma arasında pozitif yönde bir korelasyon olduğunu ifade eder.

Sosyal ağ siteleri üzerinde edinilen arkadaş sayısı, mahremiyet açısından başka bir tehdittir. Pek çok kullanıcı, kişisel bilgilerini profillerinde paylaştı da çoğunlukla bu bilgilerin “sadece arkadaşları” tarafından görülmesini tercih ederler. Ancak, arkadaş sayısının fazlalığına yüklenen farklı anlamlar, riski artırmaktadır. Ellison ve arkadaşları (2007), Facebook arkadaş sayısının fazla olmasının, bir tür sosyal sermaye (*social capital*) kaynağı olarak görüldüğünü tespit etmiştir. Başka bir çalışmada ise, Facebook arkadaş sayıları ile sosyal çekicilik arasında bir ilişki olduğu gözlenmiştir. Araştırmada, ortalama 300 arkadaşı olan Facebook profili sahibi, en yüksek sosyal çekicilik oranını elde etmiştir. Tong ve arkadaşları, Facebook arkadaş sayısı gibi bir sosyometrik verinin, çevrim içi sosyal ağda, başkaları hakkında bir sosyal yargıya varmak için kullanılabileceğini ifade etmişlerdir (Tong vd., 2008, ss. 542, 545).

Christofides ve diğerleri (2009, s. 343), yaptıkları çalışmada, genel anlamda ifşa yatkınlığı ve popüler olma ihtiyacının, Facebook'ta bilgi ifşasının önemli belirleyicileri olduğunu ifade etmişlerdir. Henderson ve Gilding de (2004), sosyal ağ siteleri geniş bir kullanıcı kitlesine ulaşmadan önce, yaygın olan sohbet odalarını kullanan 17 kişi ile gerçekleştirdikleri nitel çalışmalarında, çevrim içi iletişimde güven ile kendini ifşa arasında karşılıklı bir ilişki olduğunu belirtmişlerdir. Bu bulguları göz önünde bulundurarak bilgi ifşasının, çevrim içi ilişkinin önemli bir parçası olduğu söylenebilir.

Zhao, Grasmuck ve Martin; Facebook üzerinde kimlik inşasına odaklanan çalışmalarında, 63 Facebook profilinden topladıkları verileri, içerik analizi yöntemiyle incelemişler ve anonim (*anonymous*) ve “nonymous”⁸ çevrim içi ortamlardaki kimlik üretiminin farklılaştığını savlayan hipotezlerini destekleyen bulgular elde etmişlerdir. Anonim olmayan çevrim içi ortamlardaki insanlar, çevrim dışı kimlikleri ile bağlantılı

⁸ Yazarların İngilizcede anonim anlamını taşıyan “anonymous” kelimesinden türettikleri “nonymous”, anonim olmayan anlamında kullanılmaktadır.

olan benliklerini diğerklerine anlatmaktan ziyade, gösterirler. Bu bakış açısında kimlik, fotoğraflar, beğeniler gibi bilgilerin paylaşılması ile inşa edilir ve bir sosyal ürün olarak değerlendirilebilir (Zhao vd., 2008).

Sosyal ağ kullanıcıları; popüler olmak, benliklerini sunmak, aidiyet hissetmek, sosyal sermayelerine kaynak yaratmak ve kimlik inşa etmek için bilgilerini ifşa ederler. Hough'a göre (2009, s. 412), bireylerin mahremiyet konusunda ihtiyatlı olma becerisi ve hatta arzusu zayıftır. Bireyler çoğu zaman, kişisel bilgilerin toplanması ve yayılmasıyla ilgili çok az bilgiye ve bunları kontrol etme konusunda daha az yeteneğe veya muhtemelen iradeye sahiptir. Ancak bu durum, bireylerin mahremiyetlerini tamamen göz ardı ettikleri anlamına gelmemektedir. Üniversite öğrencileri üzerinde gerçekleştirdiği çalışmasında Tüfekçi, öğrencilerin aleniyet ve mahremiyet arasındaki sınırları yönetmeye çalıştıklarını ama bunu tamamen izole olarak yapmadıklarını söyler. Tamamen izole olmak, sosyalleşme şanslarını ortadan kaldıracağı için bunu tercih etmezler. Bunun yerine, mahremiyetlerini optimize etmeye ve sosyal paylaşım sitelerindeki (Myspace ve Facebook) profillerinin bulunabilirliğini ve erişilebilirliği ayarlamaya çalışırlar (Tufekci, 2008, s. 33).

1.1.4. Çevrim İçi Mahremiyet Konusunu İnceleyen Çalışmalar

Bu başlıkta, özellikle enformasyon ve iletişim teknolojilerinin kullanımından kaynaklanan, bu teknolojilerin sebep olduğu veya fırsat verdiği mahremiyet endişelerini, farkındalıklarını, kişisel bilgi ifşalarını mesele edinen araştırmalara, örneklemelerini tanımlayan temel bilgiler ve elde ettikleri bulguların özeti ile yer verilmiş ve daha sonra tüm bu literatüre ilişkin genel bir değerlendirme yapılmıştır. Araştırmalar, yayınlandıkları tarihten ziyade, araştırma verilerinin toplandığı tarihlere göre sıralanmıştır. Bu tercihin arkasında yatan amaç ise, okuyucuda elde edilen bulguların zamansal gelişimine dair bir farkındalık yaratabilmektir.

1.1.4.1. Literatürdeki Araştırmalar

Dinev ve Hart (2003), internet kullanımıyla ilişkili kişisel faydalar ve mahremiyet maliyetleri arasındaki değiş tokuşa odaklandıkları bir çalışma gerçekleştirirler. Çalışmada, takas (*trade-off*) modeli internet kullanımının sağladığı kişisel faydalar ile mahremiyet arasındaki ilişkiyi açıklamak için kullanılır. Çalışma sonucunda, internet kullanımı ile kullanıcıların mahremiyet endişeleri ve kırılganlık algıları arasında negatif; internet sitelerine gönderilen kişisel bilgileri kontrol becerisi algıları ile internet

kullanımları arasında ile pozitif yönde bir ilişki olduğu vurgulanır. Araştırmanın tartışma bölümünde, e-ticaret sitelerinin kullanıcıların sadece ilgi alanlarına yönelik bir yaklaşım sergilemelerinin yetersiz olacağı, kullanıcıların güvenini kazanmaya yönelik bir yaklaşımın gerekli olduğu eklenir (Dinev & Hart, 2003, s. 5). Dinev ve Hart, e-ticaret siteleri kullanımının sağladığı fayda ile mahremiyet arasındaki ilişkiyi takas modeli ile açıklar, ancak (yukarıda değinilen PRISE araştırma projesine göre) bu model, mahremiyet ve güvenlik arasındaki ilişkiyi tanımlamakta yetersizdir (Pavone & Esposti, 2012, s. 568).

“Çevrim içi Mahremiyet Risklerini Azaltma Stratejileri” başlıklı makalelerinde Milne ve Culnan, internet sitelerinin gizlilik bildirimlerinin okunmasına ve bu bildirimlere duyulan güvene odaklansalar da iki binin üzerinde katılımcıyla gerçekleştirilen çevrim içi anket çalışması, mahremiyet koruma deneyimleri ile ilgili ölçümleri de içermektedir. 2001 yılında toplanan veriler, ABD vatandaşı internet kullanıcılarının yüzde 84,8’inin, fazla kişisel ya da gereksiz olduğunu hissettiği için bir internet sitesine bilgi vermeyi reddettiğini; yüzde 82,8’inin, bir internet sitesinden kendi adlarının ya da adreslerinin pazarlama amaçlı listelerden silinmesini ve yüzde 79,4’ünün, isimlerini ya da diğer kişisel bilgilerini başka şirketlerle paylaşmamalarını istediğini; yüzde 63,9’unun, kişisel bilgilerinin nasıl kullanılacağından emin olamadığı için bir internet sitesini kullanmayı ya da bir şey satın almayı reddettiğini; yüzde 31,8’inin, bilgisayarlarını ve internet tarayıcılarını çerezleri (cookies) engelleyecek şekilde ayarladıklarını ve yüzde 34’ünün, bir internet sitesine kayıt olmak için sahte ya da kurgusal kişisel bilgiler verdiklerini göstermektedir (Milne & Culnan, 2004, ss. 21-22). Aynı araştırmada, katılımcıların büyük bir çoğunluğunun (%83,7) internet sitelerinin gizlilik bildirimlerini okudukları görülmektedir. Ayrıca, katılımcıların mahremiyet endişeleri de oldukça yüksektir. Katılımcılar, “tüketiciler kendi kişisel bilgilerinin şirketlerce nasıl toplandığı ve kullandığına ilişkin tüm kontrolü kaybetti” önermesine katıldıklarını (beşli ölçek, M=3,67) ve şirketlerin çok fazla kişisel veri toplamalarından endişe duyduklarını (M=3,96) ifade etmişlerdir (Milne & Culnan, 2004, s. 29).

Gross ve Acquisti, sosyal ağ siteleri ve mahremiyet konusunu inceleyen ilk akademik çalışmalardan biri olan ve Carnegie Mellon Üniversitesi’nde okuyan dört bin öğrencinin Facebook profilleri üzerinde yaptıkları araştırmada, mahremiyete yönelik potansiyel tehditleri ortaya koymuşlardır. Araştırmacıların özellikle vurguladıkları

tehlike, sitelere, öğrenciler tarafından girilen memleket ve doğum tarihi gibi kişisel bilgilerin, öğrencilerin sosyal güvenlik numaralarına erişim olanağı yaratmasıdır (Acquisti & Gross, 2009). Araştırmacılar, öğrencilerin bu risklere karşı kayıtsız kaldıklarını, kişisel bilgilerini cömertçe paylaştıklarını ve çok azının gizlilik ayarlarını değiştirdiğini ifade ederler (Gross & Acquisti, 2005). Govani ve Pashley'in (2005), yine aynı üniversitede okuyan, elli Facebook kullanıcısı üzerinde uyguladıkları anket çalışması sonucunda, katılımcıların yüzde 80'inin mahremiyet ayarlarını bildiği, ancak sadece yüzde 40'ının bu ayarları kullandığı tespit edilmiştir. Yine aynı yıl yapılan bir diğer araştırmada bu oran yüzde 74'e yüzde 62'dir. Aynı araştırmada Facebook'un mahremiyete etki eden sistemsal kusurları olduğu vurgulanır ve Facebook üzerindeki mahremiyetin üç temel faktör tarafından baltalandığı söylenir. Bu faktörler; (1) kullanıcıların çok fazla bilgi ifşa etmeleri, (2) Facebook'un, kullanıcıların mahremiyetini koruyacak yeterli önlemler almaması ve (3) üçüncü tarafların aktif bir şekilde, Facebook üzerinden son kullanıcı bilgilerine erişmeye çalışmalarıdır (H. Jones & Soltren, 2005).

Dinev ve Hart (2005), çevrim içi mahremiyet endişeleri konusunu, sosyal ağ sitelerinin dışında, internet üzerinden alışveriş deneyimine etkisi özelinde ele almıştır. Çalışmalarında geliştirdikleri modelde, mahremiyet endişeleri, internet okuryazarlığı (*internet literacy*) ve sosyal farkındalığı, çevrim içi alışveriş yapma niyetinin öncülleri olarak ele almışlardır. 422 kişi (%49 erkek, %51 kadın) üzerinde gerçekleştirilen anket çalışması sonucunda, mahremiyet endişeleri ile çevrim içi alışveriş yapma niyeti arasında ve internet okuryazarlığı ile mahremiyet endişeleri arasında negatif yönlü bir ilişki tespit etmişlerdir. Araştırmacılar, çalışmalarının internet okuryazarlığı ile mahremiyet endişeleri ve sosyal farkındalık ile internet mahremiyet endişeleri arasındaki ilişkiyi, ampirik olarak doğrulayan ilk çalışma olduğunu belirtmiş ve analiz sonuçları ile desteklenirse de mahremiyet endişeleri ile internet okuryazarlığı arasındaki ilişkinin “sezgisel olarak hissedilen” başka bir yönüne değinmişlerdir: “Teknik olarak daha bilgili bir internet kullanıcısının, internetin ve ağı bağlı bilgi sistemlerinin ciddiyetini, temel güvenlik açıklarını ve güvensizliklerini daha iyi kavrayabileceği ve bu nedenle daha güçlü mahremiyet endişelerine sahip olacağı iddia edilebilir (Dinev & Hart, 2005, s. 19).”

İnternet siteleri, ziyaretçileri tarafından -farkında olarak ya da farkına dahi varmadan- oluşturulan verileri ne şekilde sakladıkları, işledikleri ya da paylaştıkları ile ilgili tutumlarını, gizlilik politikası (*privacy policy*) sayfalarında açıklarlar. Bu metinler,

genellikle çok uzundur ve son kullanıcıların özümsemekte zorlanacakları hukuki bir dile sahip oldukları söylenebilir. Hatta Mcdonald ve Cranor'un (2008) yaptığı hesaplama göre, sıradan bir ABD vatandaşının, ziyaret ettiği tüm internet sitelerinin gizlilik politikalarını okuması, yılda 244 saatine mal olmaktadır. Yukarıda değinilen 2001 tarihli araştırmanın aksine, artık gizlilik politikaları bu özelliklerinden dolayı, çoğu kullanıcı tarafından okunmadan kabul edilmektedir (Schaub vd., 2017). Earp ve çalışma arkadaşları, genellikle okunmadan kabul edilen bu gizlilik politikaları üzerinde bir içerik analizi yapmış ve metinlerde yapılan beyanları, kullanıcıların mahremiyet endişeleri ile karşılaştırmıştır. Yaklaşık elli internet sitesinin gizlilik politikaları, 12 farklı kategoride sınıflandırılmış⁹ ve binin üzerinden internet kullanıcısı ile gerçekleştirilen anket çalışmasında ise, kullanıcıların mahremiyet endişelerinin bu kategorilerden hangilerinde yoğunlaştığı tespit edilmiştir. Yapılan içerik çözümlemesi; gizlilik politikalarında en çok vurgu yapılan kategorilerin; verilerin bütünlüğü ve güvenliği (*integrity/security*), verilerin toplanması ya da koleksiyonu (*collection*) ve kullanıcının verilerinin nasıl kullanılabileceğini seçebilmesi ve onaylayabilmesi (*choice/consent*) ile ilgili olduğunu göstermiştir. Buna karşılık, kullanıcıların en büyük üç endişesi; (1) kişisel verilerinin diğer kuruluşlarla paylaşılması, ödünç verilmesi veya satılmasına dair endişeler (*transfer*), (2) verilerini paylaşmadan önce bu verilerin nasıl kullanılabileceğine dair tam bilgi sahibi olma konusundaki bildirim/farkındalık endişeleri (*notice/awareness*) ve (3) kuruluşların kullanıcı verilerini saklama ve sürdürme yöntemi ile ilgili endişelerdir (*storage*). Araştırma sonuçları, gizlilik politikalarında beyan edilenler ile kullanıcıları en fazla endişelendiren sorunlar arasında, dikkate değer bir tutarsızlık olduğunu göstermektedir (Earp vd., 2005, ss. 233, 235).

Acquisti ve Gross (2006), öğrencilerin mahremiyetleri koruma arzuları ile davranışları arasında bir tutarsızlık olduğunu iddia ederler. Bu tutarsızlık, diğer çalışmalarda da karşılaşılan bir temadır (Boyd & Ellison, 2007). Barnes (2006), Amerikalı yetişkinlerin, hükümet ve özel şirketler tarafından toplanan veriler hakkındaki endişeleri ile gençlerin, özgürce kişisel ve özel bilgilerini online günlüklerde paylaşmaları arasındaki ikiliğe vurgu yapar ve bunu mahremiyet paradoksu (*privacy paradox*) olarak

⁹ Araştırmacılar, bu 12 kategori mahremiyetin korunması (*privacy-protection*) ya da mahremiyetin savunmasızlığı (*privacy-vulnerability*) çerçevesi içinde tanımlarlar (Earp vd., 2005, s. 230).

nitelendirir. Barnes’a göre bu paradoksun nedeni, gençlerin internetin kamusal niteliğinin farkında olmamasıdır. Stutzman’ın (2006) otuz sekiz öğrenci üzerinde uyguladığı pilot çalışmada da öğrencilerin mahremiyet ile ilgili görüşleri ile davranışları arasındaki bir tutarsızlık olduğu görülmektedir.

Mayıs ve Aralık 2006 ve 2007 ilkbaharından oluşan üç farklı dönemde, toplamda 704 öğrenci ile gerçekleştirilen anket çalışmasında, farklı dönemlerde toplanan veriler arasında, istatistiksel olarak belirgin çok az farklılığa rastlanmış ve bu farklılıkların en belirginleştiği nokta ise yükselen mahremiyet farkındalığı ve kaygısı olmuştur. Tüfekçi (2008, s. 25) mahremiyet farkındalığındaki artışı, bu periyotta sosyal ağ sitelerinin sözde tehlikelerinin, medya gündeminde yoğun bir şekilde yer alması ile ilişkilendirir. Mahremiyet farkındalığındaki ve endişesindeki bu artışa rağmen, anketteki çevrim içi mahremiyet endişesi ile ilgili soruya verilen yanıtın ortalaması 2,76’dır (4 = çok endişeliyim, 1 = hiç endişelenmiyorum). Başka bir ifade ile katılımcılar, biraz endişelidirler ama “aşırı endişeli” değildirler. Çalışmada elde edilen verilere göre, sosyal ağ kullanıcı olmayan katılımcıların mahremiyet endişeleri, daha yüksektir. Dikkate değer bir diğer bulgu da, kullanıcıların (Facebook ya da Myspace) profillerinin görünürlük ayarlarını yaparken profillerinin istemedikleri kişiler tarafından erişilebileceği korkularından etkilendikleridir. Buna rağmen, genel anlamda çevrim içi mahremiyet endişesinin bu tercihlerinde bir etkisi yoktur. Katılımcıların, istenmeyen kişiler tarafından görülme endişelerinin, kişisel bilgileri sosyal ağ sitelerinde paylaşma (*disclosure*) tercihlerini -cep telefonu bilgisi dışında- etkilemediği söylenebilir. Bulgular, bu endişe ile Myspace üzerinde takma ad (*nickname*) kullanarak ya da Facebook’ta profilin kimler tarafından görülebilir olduğunu ayarlayarak mücadele edildiğini göstermektedir. Kalıcılık ve aranabilirlikten kaynaklanan endişelerin de profillerin görünürlüğü üzerinde bir etkisi olmadığı söylenebilir (Tufekci, 2008, ss. 26-27, 31).

2007 yılında, 119 üniversite öğrencisi üzerinde gerçekleştirilen bir diğer araştırma, kuramsal temellerini “kullanımlar ve doyumlar” (*uses and gratifications*), üçüncü kişi etkisi (*third-person effect*) ve ritüelleştirilmiş medya kullanımı (*ritualized media use*) teorilerine dayandırır. Debatin ve ekip arkadaşlarının çalışmasında, Facebook’un sosyal hayattaki rolü ve önemi, kullanıcıların günlük ritüellerindeki yeri ve mahremiyete yönelik olumsuz etkileri araştırılmıştır. Katılımcıların önemli bir çoğunluğu, Facebook’un mahremiyet ayarlarına aşina olduğunu ve profillerini

koruduklarını söylese de detaylı kişisel bilgilerini oldukça geniş bir “arkadaş” grubunun erişimine açmaktadırlar. Çalışmada elde edilen veriler ışığında, Facebook kullanımının algılanan faydalarının risklerinden fazla olduğu yönündeki hipotez desteklenmiştir. Başka bir ifade ile katılımcılar, Facebook kullanımı nedeniyle karşılaşılabilecekleri riskleri, kullanımın sağlayacağı faydalara göre daha önemsiz bulmuşlardır. Araştırmada, ritüelleştirilmiş medya kullanımı teorisine dayanılarak geliştirilen, kullanıcıların rutinleşmiş kullanımı nedeni ile Facebook’un kendi hayatlarındaki öneminin farkında olmadıkları hipotezi desteklenmemiştir. Kullanıcıların, kendi mahremiyetlerinden çok başkalarının mahremiyetinin risk altında olduğuna yönelik bir algıları olduğu söylenebilir. Araştırmacılar son olarak, çalışmaya katılanların mahremiyet ayarlarını değiştirmelerinde, kendi başlarına gelen ihlallerin, başka birinin başına gelen ihlallerden daha etkili olduğunu ifade etmişlerdir (Debatin vd., 2009). Çalışmalarının tartışma bölümüne dayanarak kullanıcıların mahremiyet risklerine karşı anlayışlarının yüzeysel olduğu ve profillerini koruyor olsalar da arkadaş sayıları, arkadaş kabul etme pratikleri ve paylaştıkları detaylı kişisel bilgilerin mahremiyetlerini koruma ile ilişkisini tam olarak anlamadıkları söylenebilir. Araştırmacılar; sosyal ağ sitelerinin daha güvenli kullanımının, kullanıcı tutumlarında dramatik bir değişiklik gerektirdiğini eklerler: “Sorumluluk sahibi, bilgilendirilmiş ve yüksek seviye bilgisayar okuryazarlığına (*computer literacy*) sahip – sadece teknik olarak değil, sosyokültürel ve etik anlamda da (Debatin vd., 2009, s. 102).”

Aynı yıl içerisinde Buchanan ve ekip arkadaşları, internet üzerinden uygulanmaya uygun, güvenilir ve sağlam mahremiyet ölçeği geliştirmeyi amaçladıkları bir araştırma gerçekleştirirler. Bu doğrultuda birbirini izleyen üç farklı çalışma yaparlar ve ölçeklerinin performansını, literatürde kullanılan diğer ölçeklerle kıyaslarlar. Çalışmaları sonucunda araştırmacılar, üç kısa ve kendi içinde tutarlı ölçek geliştirirler. Bu ölçeklerden ilk ikisi mahremiyet davranışlarına yöneliktir: Genel dikkat (*general caution*) ve teknik koruma (*technical protection*). Son ölçek ise mahremiyet tutumlarına dair mahremiyet endişesi (*privacy concern*) ölçeğidir. Araştırmacılar, ölçeklerini test etmek için, 69 öğrencinin katıldığı küçük bir çalışma yaparlar. Bu öğrencilerin 38’i, teknoloji temelli programlarda okurken 31’i, sosyal bilimler temelli programlara kayıtlıdır. Anket sonucunda, bu iki öğrenci grubu arasında, mahremiyet endişeleri açısından istatistiksel olarak önemli bir farklılık bulunmaz. Ancak, mahremiyet davranışlarını ölçen genel dikkat ve teknik

koruma ölçekleri, iki öğrenci grubu arasında anlamlı bir farklılık gösterir. Son olarak araştırmacılar, kendi ölçeklerini Westin ve Malhotra vd.'nin (2004) ölçekleri ile karşılaştırdıkları bir çalışma daha yaparlar ve Westin'in ölçeği ile genel dikkat ölçeği arasındaki hariç, tümünde anlamlı bir korelasyon olduğunu gösterirler (Buchanan vd., 2007).

Fogel ve Nehmad'ın 2007 yılında 205 üniversite öğrencisine uyguladıkları anket ile gerçekleştirdikleri araştırmada, bireylerin risk alma yaklaşımları ile sosyal ağ sitesi kullanımları arasındaki ilişki ve bu siteleri duydukları güven ile mahremiyet endişeleri incelenmiştir. Araştırmacılar, sosyal ağ sitelerinde profili olan öğrenciler, olamayanlara kıyasla daha fazla risk alma tutumu sergiledikleri, Facebook'un katılımcılar tarafından güvenilir bulunduğu ve mahremiyet endişesi ile kimlik bilgilerinin ifşası endişesinin kadınlarda erkeklere oranla daha yüksek olduğunu belirtmişlerdir (Fogel & Nehmad, 2009).

Paine ve çalışma arkadaşları, literatürdeki mahremiyet endişesi araştırmalarından farklı olarak, beşli ya da yedili ölçekler yerine açık uçlu sorular ile bir araştırma gerçekleştirirler. Dinamik mülakat programı (*Dynamic Interviewing Programme*) olarak nitelendirilen yazılım, yirmi birinci yüzyılın ilk yıllarında popüler olan anlık mesajlaşma programı ICQ kullanıcısı kişilere rastgele mülakat davetleri gönderir ve kabul edenler on sorudan oluşan mülakatı cevaplarlar. Yaklaşık seksen bin kişiye gönderilen rastgele davetlerin sadece 1507'sine geri dönüş olur ve eksik soru yanıtlayanların elenmesi ile çalışmaya dahil edilen katılımcı sayısı 530 olarak belirlenir. Katılımcıların yüzde 56'sı, çevrim içi mahremiyetleri konusunda endişeli olduklarını ifade etmiştir. Araştırmacılar, bu oranın Likert ölçekleri ile yapılan araştırmalardan düşük olduğunu ifade ederler ve bu durumu, ölçekli araştırmalarda mahremiyet endişesinin kapsamının, mevcut çalışmada tanımlanandan daha geniş tutulması ile açıklamaya çalışırlar. Araştırma sonuçları, mahremiyet endişesinin yaşa göre değişkenlik gösterdiğini ve yaşlı katılımcıların çevrim içi mahremiyet konusunda daha endişeli olduklarını ortaya koyar. Bu çalışmanın değinilmesi gereken son çıktısı ise, internet deneyimi ile çevrim içi mahremiyeti koruma arasındaki ilişkidir. Bu çıktıya göre, internette geçirilen süre ve toplam internet deneyimi ne kadar fazlaysa mahremiyeti korumak için harekete geçme olasılığı da o kadar artar. “Bir kişi ne kadar çok çevrim içi deneyime sahip olursa, olası gizlilik tehditleri hakkında

o kadar çok bilgi sahibi olacak ve kendilerini korumak için nasıl harekete geçeceklerini o kadar çok bileceklerdir (Paine vd., 2007, ss. 533-534).”

Hoy ve Milne (2010, s. 32), 2008 yılında gerçekleştirdikleri web tabanlı anket çalışmasının katılımcılarına, Facebook’ta kurdukları bir grup üzerinden ulaşmışlardır. 18-24 yaş aralığındaki 589 Facebook kullanıcısının katıldığı araştırmaya bakılarak, kadınların mahremiyet endişelerinin erkeklere oranla daha yüksek olduğu söylenebilir. Aynı zamanda kadınlar, sosyal ağ sitelerine gönderilen kişisel bilgilerin, farklı amaçlarla kullanılabileceğinin bilincinde olmanın önemli olduğuna inanırlar. Bu sonuçla paralel olarak, araştırmaya katılan kadınların kendilerini koruyacak proaktif davranışlar gösterme ihtimalleri, erkeklere göre daha fazladır (Hoy & Milne, 2010, ss. 41-42).

2008 yılında Antón, Earp ve Young, altı yıl önce gerçekleştirdikleri anket çalışmasını tekrarlamışlardır. İlk çalışmada bilgi transferi, bildirim/farkındalık ve bilgi depolama, ABD vatandaşlarının en önemli üç mahremiyet endişesi kaynağını oluşturmaktadır. Bu araştırmada ise aradan geçen altı yıla ve değişen çevrim içi trendlere, yürürlüğe giren yasalara rağmen, ilk üç mahremiyet endişesi aynı kalmıştır. Örnekleme, yaklaşık iki bin (1525’i ABD’de, 421’i başka bir ülkede yaşayan) internet kullanıcısından olmaktadır. Araştırmacılar, sonuçları bir önceki çalışmaları ile karşılaştırdıklarında, katılımcıların internette daha fazla vakit geçirmeye başladıklarını ve altı yıl öncesine göre daha fazla kullanıcının çevrim içi alışveriş yaptığını gözlemlemişlerdir. Kullanıcıların enformasyon mahremiyeti endişelerinin niteliği değişmese de bu endişelerinin seviyesi artmıştır: Artık kullanıcılar, satın alma modellerinin ifşa edilmesinden ve kişisel olarak tanımlanabilir bilgilerinin (*personally identifiable information*) üçüncü kişilere satılmasından daha fazla endişe duymaktadırlar. Bunun yanı sıra, kullanıcıların kişisel olarak tanımlanabilir bilgilerinin korunması için kullanılan güvenlik önlemleri hakkında bilgilendirilme talepleri artmıştır. Uluslararası katılımcılar ile ABD’de ikamet edenler karşılaştırıldığında ise, mahremiyet endişesi yaratan ilk üç kaynağın aynı olduğu, ancak iki grup arasında farklı seviyelerde olduğu görülmüştür. Bilgi transferi konusunda, ABD vatandaşlarının endişeleri daha büyükken bilgilerin depolanması konusundaki endişeler özellikle 22-28 yaş aralığındaki uluslararası katılımcılarda daha fazladır (Antón vd., 2010, ss. 23-25).

Aynı yıl Türkiye’de farklı üniversitelerden 280 öğrenci ile gerçekleştirilen çalışma, Facebook kullanımının öğrenciler için oldukça yeni bir pratik olduğunu gösterir. Araştırmaya katılan öğrencilerin çoğu, son altı ay içerisinde Facebook kullanmaya başlamışlardır. Araştırma, öğrencilerin Facebook’ta hangi bilgileri, kimlerin erişimine açtığını da ortaya koyar. Buna göre, katılımcıların yaklaşık yüzde 21’i, profillerini herkesin erişimine açık tutarken, yüzde 65,4’ünün profiline ise sadece Facebook arkadaşları erişebilmektedir. Araştırmaya katılan öğrencilerin neredeyse tamamı (%98,9) ad ve soyadlarını paylaşmaktadır. Bununla birlikte en çok paylaşılan bilgiler fotoğraflar ve doğum tarihidir. Cep telefonu, ev adresi ve sabit telefon numarası bilgileri, en az paylaşılan kişisel bilgilerdir. Araştırmacılara göre bu, kullanıcıların mahremiyet endişeleri olduğunu göstermektedir (Güven & Kovanlıkaya, 2008).

Christofides, Muise ve Desmarais’in, büyük bir çoğunluğu kadın öğrencilerden oluşan 343 üniversite öğrencisi üzerinde gerçekleştirdiği çalışmasında, öğrencilerin kişisel bilgilerini Facebook üzerinde paylaşma pratikleri ile ilgili literatürdeki araştırmaları destekleyen veriler toplanmıştır. Uygulanan çevrim içi anket ile kullanıcıların kişisel bilgileri Facebook üzerinde açıklamalarının (yedili ölçeğe M=4,26), genel olarak kişisel bilgilerini açıklamalarından (M=4,08) daha muhtemel olduğu ve ortalama 297 Facebook arkadaşları bulunduğu sonuçları elde edilmiştir. Aynı araştırma, çalışmaya katılan öğrencilerin yüzde 97’sinin bir ağa katıldıklarını¹⁰, yüzde 96’sının doğum günü bilgisini, yüzde 85’inin eposta adreslerini ve memleket bilgilerini ve yüzde 81’inin romantik ilişki durumlarını paylaştıklarını göstermiştir. Cep telefonu ve ev adresi bilgisinin Facebook üzerinde paylaşılma oranı ise sırasıyla yüzde 24 ve yüzde 4’tür (Christofides vd., 2009, ss. 342-343).

Yukarıda aktarılan çalışmalarda görüldüğü gibi, sosyal ağ siteleri üzerinde, özellikle mahremiyet ile ilgili yapılan araştırmalar, çoğunlukla gençlere ve üniversite öğrencilerine odaklanmıştır. Bu yönelimin sebebi, en yaygın sosyal ağ sitelerinden biri olan Facebook’un, 2004-2006 yılları arasında sadece öğrencilerin kullanabildiği bir platform (Boyd & Ellison, 2007, s. 212) olmasıdır. Brandtzæg, Lüders ve Skjetne, 2010 yılında gerçekleştirdikleri çalışmada, literatürdeki bu boşluğu doldurmak için,

¹⁰ Facebook, özellikle sadece üniversite öğrencilerinin üyeliğini kabul ettiği dönemde, bir ağ sistemi ile çalışırdı. Örnek: Marmara University Network.

örneklemelerini hem genç hem de yaşlı Facebook kullanıcılarından oluşturmuşlardır. Sekizer kişilik gruplardan oluşan genç ve yaşlı Facebook kullanıcılarının yaşları 16-33 ve 40-62 arasındadır. Çalışmanın sonuç bölümünde araştırmacılar, mahremiyetlerini kontrol etme becerisi ve sosyal pratikler açısından kuşaklar arasında bir farklılık olduğunu belirtmişlerdir. Genç kullanıcılar, daha odaklı ve daha sık aralıklarla Facebook kullanırken, yaşlıların Facebook kullanımı ise daha uzun seanslar halinde gerçekleşmektedir. Yaşlı kullanıcılar genellikle eski arkadaşları ve aile üyeleri ile sohbet etmek gibi daha az organize ve daha amaçsız bir kullanım sergilerlerken genç kullanıcılar arkadaşları ve okul arkadaşları ile etkileşimin koordine edilmesi gibi daha amaca yönelik bir kullanım sergilerler. Araştırmacıların işaret ettiği bir diğer önemli bulgu, genç kullanıcıların Facebook’u artık daha az ve daha dikkatli kullandıklarını belirtmiş olmalarıdır. Bunun sebepleri ise, Facebook’un artık daha az ilgi çekici olması ve çok fazla arkadaşın kullanım ve paylaşım sürecini karmaşılaştırmasıdır. Genç kullanıcılar arasında kişisel farkındalığın ve uyumculuğun (*conformity*) artmasının nedeni, ebeveynler ve aile üyelerinin de -gençlerin bir zamanlar sadece kendileri için ve özgürce davranabildikleri bir sosyal alan olarak gördükleri- bu kişisel ağın bir parçası haline gelmesidir. Araştırmadaki yaşlı kullanıcıların Facebook’u kullanmaya başlama motivasyonu, çocuklarının Facebook aktivitelerini takip edebilmektir. Araştırmacılar, genç kullanıcıların daha yetenekli sosyal ağ kullanıcıları olduklarını, yaşlılara göre mahremiyet farkındalıklarının ve mahremiyet ayarlarını değiştirme ihtimallerinin daha yüksek olduğunu belirtmişlerdir (Brandtzæg vd., 2010, ss. 1026-1027).

Henson ve arkadaşları (2011), sosyal ağda mahremiyet ve güvenlik ile çevrim içi mağduriyet¹¹ arasındaki bağlantıya odaklanan çalışmalardan farklı olarak, kişisel ve sosyal ağ sitesinin sağladığı güvenlik ile çevrim içi kişilerarası mağduriyet arasındaki ilişkiyi incelerler. 2009 yılında 914 üniversite öğrencisine (%61’i kadın, yaş ortalaması 20) çevrim içi anket sonucunda, katılımcıların yaklaşık yüzde 42’sinin bir çeşit çevrim içi kişilerarası mağduriyete maruz kaldığı görülmüştür. Araştırmacılar, birkaç faktörün bu mağduriyeti istatistiksel olarak anlamlı bir şekilde tahmin ettiğini belirtmişlerdir. Bu faktörlerden ilki cinsiyettir: Kadın kullanıcıların bu mağduriyeti yaşama ihtimalleri,

¹¹ Araştırmacılar, çalışmalarını kaleme aldıkları dönemde “online victimization” ve “online interpersonal victimization” kavramlarını kullanmışlardır. Günümüzde bu kavramların literatürdeki karşılığının siber zorbalık (*cyberbullying*) olduğunu belirtmek yerinde olacaktır.

erkeklerle göre neredeyse iki kat daha fazladır. Farklı sosyal ağ sitelerine üyelik sayısı, bu sitelerdeki günlük güncelleme sayılarındaki artış da çevrim içi mağduriyeti arttıran bir değişkendir. Sosyal ağdaki profillerin tanımadıkları kişilerin erişimine açık tutulması, mağduriyet yaşama ihtimalini yaklaşık 2,6 kat arttırdığı söylenebilir (Henson vd., 2011, s. 263). Son olarak, araştırmaya katılan öğrencilerin, sosyal ağ sitelerindeki profillerinde, hangi kişisel bilgilerini ne oranda paylaştıklarına değinilebilir. Araştırmadaki öğrencilerin yaklaşık yüzde 75'i sosyal ağ sitelerinde gerçek isimlerini kullanırlarken neredeyse yüzde 90'ı doğum günü tarihlerini paylaşmaktadırlar. Katılımcıların sadece yüzde 10'undan daha azı ev ya da okul adreslerini paylaşmışlardır. Fiziksel alanlarla ilgili bilgiler, çoğunlukla paylaşılmazken, e-posta adresleri (%70) ve anlık mesajlaşma adresleri (%40) gibi elektronik iletişim kanalları ile ilgili bilgileri paylaşırlar. Katılımcıların yüzde 25'i ise cep telefonu bilgisini dahi paylaşmıştır (Henson vd., 2011, s. 260).

Nosko, Wood ve Molema, Facebook üzerinde hangi potansiyel içeriklerin erişilebilir olduğunu ve hangi bilginin kimler tarafından ifşa edildiğini kapsamlı bir şekilde tetkik etmeyi hedefledikleri çalışmalarında, Facebook'taki 8 Kanada ağından, rastlantısal örneklemele seçtikleri 400 profili incelemişlerdir. Örneklem ile ilgili olarak şu bilgiler paylaşılmıştır: Cinsiyet bilgilerine erişilebilen 328 kişinin 116'sı kadın ve 155'i erkektir. 301 kişinin yaşları, profillerinde ifşa ettikleri bilgilerden öğrenilebilmiştir. Kadınların yaşları 19 ila 47 (ortalama 22,9), erkeklerinki ise 17 ila 61 (ortalama 23,9) arasında değişmektedir (Nosko vd., 2010, s. 407). İçerisinde üç farklı çalışmayı barındıran bu araştırmanın ilk çıktıları bir tanımlayıcı özet sunmaktadır. Nosko ve arkadaşları, öncelikle bir Facebook profilinde paylaşılan verileri incelemek için 97 maddelik bir kontrol listesi oluşturmuşlar ve daha sonra örneklemdaki 400 profili bu listeye göre kodlamışlardır. Örneklem içerisindeki Facebook profillerinde en fazla ifşa edilen veriler, profillerin yüzde 63'ünden fazlasında erişilebilir olan doğum tarihi, cinsiyet, profil fotoğrafı ve fotoğraf albümü gibi kişisel tanımlayıcı bilgiler ile üyesi olunan gruplar, arkadaş listeleri gibi sosyal bağlantılardır. Araştırmacıların belirlediği 97 maddenin 26'sı, örneklemi oluşturan profillerin yarısında ifşa edilmiş durumdadır. İlginç bir şekilde, profillerde ifşa edilen bilgiler ne güvenli ne de güvenli değildir. Profillerde hem en yaygın hem de en az yaygın paylaşılan bilgiler, son derece kişisel bilgilerdir (Nosko vd., 2010, s. 408). Araştırmacılar, kimlerin bu açıklayıcı bilgileri daha çok

paylaşma eğiliminde olduklarını ve hangi tür bilgilerin birlikte üretildiğini anlamak için iki çalışma daha gerçekleştirmişlerdir.

Nosko ve arkadaşları, ikinci çalışmaları için üç farklı ifşa kategorisi geliştirmişlerdir. Bunlar, (1) kişisel kimlik bilgileri (*personal identity information*), (2) hassas kişisel bilgiler (*sensitive personal information*) ve (3) potansiyel damgalayıcı bilgilerdir (*potentially stigmatizing information*). Kişisel kimlik bilgileri (ya da varsayılan/standart bilgiler), ev adresi, şehir, posta kodu, cinsiyet, doğum günü, doğum yılı, profil fotoğrafı ve e-posta adresidir. Hassas kişisel bilgiler kategorisi ise, e-posta adresi, işveren, işteki pozisyon, durum bildirimleri, mini feed, profil duvarı, profil fotoğrafı, fotoğraf albümleri, seçilmiş fotoğraflar, etiketlenmiş fotoğraflar, mesajlar, dürtmeler, armağanlar ve görülebilir arkadaşlar oluşmaktadır. Potansiyel damgalayıcı bilgiler, toplumda damgalanmaya neden olabilecek hassas kişisel bilgileri içermektedir. Bunlar dini görüşler, politik görüşler, doğum yılı, cinsel yönelim, fotoğraflar, görülebilir arkadaşlar, ilgi alanları, aktiviteler, favori müzikler, filmler, diziler, kitaplar, alıntılar ve hakkımda alanına girilen bilgilerden oluşmaktadır (Nosko vd., 2010, s. 410).¹² Örneklemdeki profiller, bu kategorilere dahil olan bilgilerin ne kadarını paylaştığına göre kodlanmıştır. İlk kategori 8, ikinci ve üçüncü kategori ise 14 farklı bilgiyi içermektedir. Başka bir şekilde ifade edilirse; bir profilin ilk ifşa kategorisinden alabileceği en yüksek skor 8, diğer kategorilerden ise 14'tür. Cinsiyet, ilişki durumu ve yaş bilgilerinin paylaşılması değişkenine göre yapılan istatistiksel testlerde, bu bilgileri profillerinde paylaşanların paylaşmayanlara göre her üç ifşa kategorisinde de daha fazla bilgiyi ifşa ettikleri görülmüştür. İlişki durumuna göre (yalnız, ilişkisi var ya da belirtilmemiş), yalnız olanların diğerlerine göre daha fazla bilgi ifşa ettiği söylenebilir. Yapılan istatistiksel karşılaştırmalar, ilişki durumunu belirtenlerin, belirtmeyenlere göre daha fazla varsayılan/standart (yalnız M=3,34, ilişkisi var M=3,11, belirtilmemiş M=2,54) ve hassas kişisel bilgiyi (yalnız M=10,12, ilişkisi var M=10,08, belirtilmemiş M=8,94) ifşa ettiğini göstermektedir. Her üç ifşa kategorisinde de yaş arttıkça paylaşılan bilgi miktarında azalma olmaktadır (Nosko vd., 2010, ss. 411-412).

¹² Araştırmacılar, bu ifşa kategorilerini belirlemek için çeşitli tematik analizlerin yanında bir de pilot anket çalışması gerçekleştirmişlerdir. Mevcut çalışmanın anlam bütünlüğünü bozmamak için sadece üretilen kategoriler aktarılmıştır.

Nosko ve arkadaşlarının son çalışması, ikinci çalışmada oluşturulan kategorilere dahil edilmeyen verileri de işe koşmak -ve bir bakıma ikinci çalışmayı doğrulamak- için tasarlanmıştır. Bu tasarımda ise on farklı kategori tanımlanmıştır.¹³ Daha sonra potansiyel farklılıkları tespit edebilmek ağ türü (üniversite ağı ya da topluluk ağı), cinsiyet (belirtilmiş ya da belirtilmemiş ve kadın ya da erkek), ilişki durumu ve yaş (belirtilmiş ya da belirtilmemiş) bilgilerinin her biri için ayrı 11’er t-testi gerçekleştirilmiştir. Bu testlere göre, bir topluluk ağına dahil olanların üniversite ağına bağlı olanlara ve erkeklerin de kadınlara oranla politik ve dini görüşlerini daha fazla paylaştıkları görülmüştür. İlişki durumu bilgisini paylaşanlar, paylaşmayanlara oranla kişisel bilgiler, fotoğraf ve güncelleme bilgileri, fotoğraf albümü ve profil fotoğrafı bilgileri, yaş ve görüş bilgilerini daha çok paylaşmaktadır. Yaş ile ilgili yapılan analizler, ikinci çalışmada olduğu gibi, ters orantı göstermektedir: yaş arttıkça ifşa edilen bilginin miktarı azalmaktadır (Nosko vd., 2010, s. 414). Araştırmacıların bu kapsamlı -ve üç farklı çalışmayı kapsayan- araştırmalarının çıktıları genel olarak değerlendirildiğinde, yaş ve ilişki durumunun, kimin daha fazla bilgi ifşa edip etmeyeceğini tanımlamada, cinsiyet gibi geleneksel bir değişkene kıyasla daha başarılı olduğu söylenebilir.

Lemieux, kurmaca kişisel bilgilerle oluşturduğu Facebook profili üzerinden deneysel bir çalışma gerçekleştirmiş ve katılımcıların belirsiz ve tanımadıklarını birini Facebook arkadaşı olarak kabul edip etmediklerini incelemiştir. Çalışmanın bulguları, örneklemin yüzde 72’sinin tanımadığı bir “kurgusal” kişiyi arkadaş olarak kabul edebildiğini göstermektedir. Kurgusal olmasının yanında, profilindeki eksik ve yetersiz bilgilere rağmen arkadaşlığın kabul edilmesi, eşit olmayan bir bilgi alışverişi oluşturmaktadır. Bu alışveriş, karşılıklılık normlarına (*norms of reciprocity*) uymamaktadır (Lemieux, 2012, s. 291). Sınırlı bir çalışma olsa da sosyal ağ siteleri üzerinde arkadaş olabilmenin bu kadar basit olması, en yaygın tercih edilen mahremiyet ayarlarından olan “sadece arkadaşlarım görebilsin” seçeneğini anlamsızlaştırmaktadır.

¹³ Bu kategoriler, kişisel bilgiler (*personal information*), ilişki durumu (*relationship information*), yaş (*age information*), iletişim bilgileri (*contact information*), eğitim bilgileri (*education information*), iş bilgileri (*work information*), görüş bilgileri (*view information*), genel fotoğraf bilgileri (*general picture information*), mesaj ve dürtme kabulü (*message and poke acceptance*) ve duvar ve güncelleme bilgileri (*wall and update information*) şeklindedir.

2012 yılında, Türkiye’de gerçekleştirilen bir çevrim içi anket çalışmasında, kartopu örneklem yöntemi kullanılmış ve yüzde 47’si kadın, yüzde 53’ü erkek olan 514 kişiye ulaşılmıştır. Yaklaşık yüzde 60’ı bekar, yüzde 20’sinin öğrenci, yüzde 68,1’inin tam zamanlı bir işte çalıştığı örneklemin yaş ortalaması ise 30’dur. Bu çalışma, farklı yaş grubu ve eğitim düzeyine dahil olan bir katılımcı kitlesine ulaştığı için, ortaya koyduğu betimleyici istatistikler faydalı olabilir. Araştırmada katılımcılara, Facebook üzerindeki mahremiyet kaygıları ile ilgili çeşitli sorular sorulmuş ve geçerli cevapların oranları yüzde olarak paylaşılmıştır. Buna göre, katılımcıların yüzde 45,5’i kimlik bilgilerinin çalınmasından, yüzde 42,6’sı Facebook’taki bilgilerinin üçüncü şahıs ve/veya kurumlarla paylaşılma olasılığından, yaklaşık yüzde 40’ tanımadıkları kişilerin kendileri hakkında bilgi edinebilmesinden, yüzde 31’i Facebook’ta arkadaşıyla paylaştığı iletinin başkaları tarafından okunabilmesinden, yaklaşık yüzde 30’u başkaları tarafından gözetleniyor olmaktan ve yaklaşık yüzde 20’si de Facebook’ta paylaştığı iletilerden, gelecekte utanç veya sıkıntı duymaktan kaygı duymaktadırlar (M. O. Zengin & Zengin, 2015, ss. 8, 9, 18).

Yukarıda aktarılan çalışmaların çoğunda olduğu gibi, literatürdeki araştırmaların genellikle üniversite öğrencileri ve gençler üzerinde yapıldığı görülmektedir. Brandtzæg vd. gibi (2010) Christofides ve ekip arkadaşları da, ergen ve yetişkinlerin çevrim içi ifşa ve mahremiyeti koruyucu davranışlar çerçevesindeki farklılıklarını ve bu farklılaşmanın nedenlerini araştırdıkları çalışmaları ile literatürdeki genel trendden ayrılırlar. Çalışma kapsamında, yaşları 9 ila 18 arasında değişen (M=14,4) 288 ergen (112 erkek, 171 kadın) ve yaşları 19 ila 71 arasında olan (M=31,6) 285 yetişkine (118 erkek, 165 kadın) ulaşılmış ve veriler çevrim içi anket yöntemiyle toplanmıştır. Elde edilen veriler, ergenlerin (55,9 dakika) yetişkinlere (38,2 dakika) göre Facebook’ta daha fazla zaman geçirdiklerini ve ortalama arkadaş sayılarının birbirine yakın olduğunu göstermektedir. Ancak araştırmadaki ergenler, olabildiğince fazla arkadaş edinmeye yetişkinlere göre daha fazla önem vermektedir ve bu sebeple arkadaş toplama davranışı sergileme (*friend collecting behavior*) ihtimalleri daha yüksektir. Her ne kadar, araştırma sonuçları, ergenlerin yetişkinlere oranla daha fazla bilgi ifşa ettiklerini ve gizlilik ayarlarını daha az kullandıklarını gösterse de, bu davranışların belirleyicileri açısından iki grup benzerlik göstermektedir. Her iki grupta da Facebook’ta geçirilen zamanın artması, tahmin edilen bilgi ifşası olasılığını artırmaktadır (Christofides vd., 2012, ss. 51-52).

Yeni medya atmosferinde ve dijital dünyada, mahremiyeti sosyal ağ sitelerinde, özellikle öğrenciler ve gençler tarafından ifşa edilen kişisel bilgiler üzerinden kavramaya çalışmak önemlidir, ancak yeterli değildir. Bu açığı kapatmak için Hallinan ve arkadaşları, Avrupa Birliği'nde yapılan pek çok kamuoyu anketi üzerinde bir meta analiz gerçekleştirirler. Veri koruma ve mahremiyete odaklanan kamuoyu yoklamalarından elde edilen sonuçları yorumlayan araştırmacılar, Avrupa Birliği vatandaşlarının mahremiyet ve veri koruma fikrine halen yüksek bir değer verdiğini ve mahremiyeti koruma stratejilerinin temel ilkelerine yönelik farkındalığın yüksek olduğunu, ancak bunun yüzeysel bir seviyede kaldığını belirtmişlerdir. Araştırmacılar, bu yüzeysel farkındalığın ve sınırlı bilginin, vatandaşları mevcut veri ortamında yeterli sayıda davranış kalıplarına sahip olmadan hareket etmeye zorladığını ifade etmişlerdir. Çalışmada son olarak, vatandaşların veriler üzerindeki kontrolü kaybettikleri yönündeki hisleri ve karmaşık, akışkan ve şeffaflıktan yoksun veri ortamının açıklığa kavuşması, katılaşması ve anlaşılır hale gelmesi yönündeki arzularına değinilmiştir (Hallinan vd., 2012, s. 271).

Stutzman ve ekip arkadaşları (2013), 5076 Facebook kullanıcısının, 2005-2012 yılları arasındaki verilerini içeren veri seti üzerinde yaptıkları analizlerle, sosyal ağlarda mahremiyetin dönüşümüne dair bir tablo ortaya koyarlar. Yaptıkları analizlerin ardından, üç farklı eğilime dikkat çekerler. Bunlardan ilki, zaman içerisinde kullanıcıların herkese açık (*public*) olarak paylaştıkları kişisel verileri, aşamalı olarak azaltmaları ve daha fazla gizlilik aramaya başlamalarıdır. Araştırmacılar, bu ilk eğilimin, araştırma periyodunun sonlarına doğru, Facebook tarafından yapılan kimi kullanıcı arayüzü ve gizlilik ayarları güncellemeleri ile baskılandığını ve bazı durumlarda bu eğilimi tersine çevirdiğini ifade ederler. Araştırmacıların vurguladıkları son eğilim ise, kullanıcıların bağlantıda olduğu profillerle (yani Facebook arkadaşlarıyla) paylaştıkları kişisel bilgilerin miktarının ve kapsamının zaman içerisinde artmasıdır. Bu üçüncü eğilim, sosyal ağlardaki sessiz dinleyiciler (*silent listeners*) olarak nitelendirilen Facebook'u kendisi, üçüncü taraf uygulamaları ve dolaylı olarak da reklam verenlerin hizmetine sunulan kişisel bilgi miktarının da artmasına neden olur. Araştırmacılara göre, elde ettikleri bulgular, sosyal ağ sitesi kullanıcılarının çevrim içi gizliliği yönetmeye çalışırken karşılaştıkları zorlukları ve sosyal medya hizmetleri sağlayıcılarının, arayüzler ve varsayılan ayarlar aracılığıyla bireylerin ifşasını ve mahremiyet davranışlarını etkileme gücünü göstermektedir (Stutzman vd., 2013, s. 31).

2010-2013 yılları arasında, 6 farklı ülkeden (Almanya, Belçika, Finlandiya, Polonya, Avusturya ve İsrail), 14-23 yaş aralığındaki 1428 ergen üzerinde gerçekleştirilen araştırmada, mahremiyet ve veri güvenliğine ilişkin bazı bulgular ortaya koyulmuştur. Sonuçlar, ergenlerin gizliliğe yüksek değer atfettiğini ve bir çevrim içi şirketin, ergenlerin kişisel çıkarlarına meydan okuması durumunda aktif olarak karşı çıkmaya hazır olduklarını gösterir. Buna rağmen, gençler diğer faydalar için mahremiyetten vazgeçme eğilimindedirler. Ergenlerin mahremiyet algısı ve veri koruması, kültürel çeşitlilikten, yaştan ve cinsiyetten etkilenir (Soffer & Cohen, 2014, s. 155). Aynı dönemde, Mısır'da gerçekleştirilen bir diğer araştırma da benzer çıktılar ortaya koyar. Kahire'de yaşayan 359 internet kullanıcısı üzerinde yapılan araştırmada, kadınların Facebook ve Google'ın gizlilik politikalarına ilişkin farkındalıkları, erkeklere oranla daha az olduğu, ancak mahremiyet endişelerinin erkeklerden daha fazla olduğu sonucuna ulaşılır. Aynı araştırmanın çıktıları, internet kullanım tecrübelerinin, çevrim içi mahremiyet endişeleri üzerinde anlamlı bir etkisi olmadığını gösterir (Alfred, 2014, s. 84). Burada, kullanıcıların internet kullanım tecrübelerinin tek bir soru ile ölçüldüğü ve katılımcıların kendi deneyim seviyelerini üç seçenek arasında seçim yaparak belirlediklerini eklemek gerekir. Kahire'de gerçekleştirilen araştırmada, değinilmesi gereken son çıktı, eğitim seviyesi ile çevrim içi gizlilik politikaları farkındalığı arasındaki ilişkidir. Bulgular, eğitim seviyesi ile çevrim içi gizlilik politikaları farkındalığı arasında anlamlı bir ilişki olduğunu, ancak bu politikaların detaylı okunması ile bir ilişkisi olmadığını gösterir (Alfred, 2014, s. 76).

Young ve Quan-Haase, üniversite öğrencilerinin, kendilerini mahremiyete yönelik potansiyel tehlikelere karşı korumak için geliştirdikleri stratejilere odaklandıkları çalışmalarında, Raynes-Goldie'nin (2010, 2012, s. 81) sosyal ve kurumsal mahremiyet (*social and institutional privacy*) ayrımını işe koşarlar ve bu ayrımın öğrencilerin geliştirdikleri stratejileri anlamakta önemli olduğunu ifade ederler. Araştırmanın verileri, 77 iletişim çalışmaları öğrencisinin katıldığı anket ve 21 öğrencinin katıldığı mülakatlarda toplanmıştır. Ankete katılanların ortalama yaşı 19,68'dir ve yüzde 71'i kadındır. Mülakatlara katılanların ise yüzde 76'sı kadındır. Araştırmacılar derinlemesine görüşmeler sırasında, katılımcıdan Facebook hesaplarına giriş yapmalarını istemiş ve katılımcıların profillerinde paylaştıkları bilgiler ve kullandıkları gizlilik ayarları

üzerinden ilerlemişlerdir. Profil analizi (*profile analysis*)¹⁴ olarak nitelendirdikleri bu yöntem, öğrencilerin genellikle hangi bilgileri ifşa ettiklerini ve hangi gizlilik ayarlarını kullandıklarını ya unutmuş olduklarını ya da bunların farkında olmadıklarını göstermiştir. Anket sonuçlarına göre; katılımcıların yüzde 71'i Facebook'un varsayılan gizlilik ayarlarını,¹⁵ “sadece arkadaşlar” ya da “bazı ağlar ve tüm arkadaşlar” şeklinde değiştirdiği, ancak yüzde 14'ünün varsayılan ayarları koruduğu ve hatta yüzde 8'inin de bu ayarları daha da esneterek profillerini tüm Facebook ağına açtıkları görülmüştür. Sosyal ve kurumsal mahremiyet ayrımı dikkate alındığında, öğrencilerin sosyal mahremiyetleri hakkında daha çok endişelendikleri ve buna yönelik stratejiler geliştirdikleri söylenebilir. Bu çalışmada değinilmesi gereken son çıktı ise öğrencilerin mahremiyetlerini korumak için profillerine kurgusal bilgiler girme stratejisini tercih etmemeleridir (Young & Quan-Haase, 2013, s. 492).

Litt, Pew Research Center'ın “*İtibar Yönetimi ve Sosyal Medya*” (*Reputation Management and Social Media*) veri seti üzerinde, yaş ve cinsiyet ile sosyal ağ sitelerinde mahremiyet araçları kullanımı arasındaki ilişkiye bir cevap aramış ve daha fazla sosyal ağ sitesi tecrübesi olan ve/veya çalkantılı bir çevrim içi deneyim (*online turbulent experience*) yaşayan bireylerin, olmayanlara kıyasla daha fazla mahremiyet aracı kullanacağını savlayan hipotezleri test etmiştir. Veri setinde bulunan 2253 yanıtın uygun olmayan kayıtlar çıkarılmış ve 490 kişilik bir örnekleme ulaşılmıştır. Litt'in kullandığı veri setinde, özellikle mahremiyet endişesi sadece tek bir evet-hayır sorusu ile ölçülmüş olsa da araştırmaya katılanlara kendileri hakkında yayınlanan çevrim içi bilgiler nedeniyle kötü veya utanç verici durumlar yaşayıp yaşamadıklarının ve daha sonra paylaşmaktan pişmanlık duydukları içeriği çevrimi içi olarak yayınlamış olup olmadıklarının sorulması açısından dikkat çekicidir. Bunun yanı sıra araştırmada, teknolojik mahremiyet araçları kullanımları ile ilgili beş soru yer almaktadır.

¹⁴ Araştırmacılar, bu yöntemi kullanmanın, sadece kendi kendine bildirim (*self-report*) verilerine güvenmenin yarattığı iki sorundan kaçınmaya yaradığını söyler. İlki, bu metodun bir veri doğrulama aracı olarak hizmet etmesidir. Katılımcılar, Facebook'un ayarlarını çok sık değiştirdiği göz önüne alındığında, mevcut ayarlarını unutmuş olabilirler veya en son uyguladıkları ayarları doğru şekilde hatırlamakta zorluk çekebilirler. Katılımcıların profillerinde hangi kişisel bilgileri açıkladıklarını unutmuş olmaları da mümkündür. İkincisi ise, bu yöntemin, sosyal arzu edilebilirlik bağlamında (*social desirability*) katılımcıların, araştırmacıların duymak isteyeceklerini düşündüğü şeyleri söylemesinden kaynaklanabilecek sorunları önlemesidir (Young & Quan-Haase, 2013, s. 496).

¹⁵ Facebook 2007 yılında bu ayarları “tüm ağlar ve tüm arkadaşlar” (*all networks and all friends*) olarak değiştirmiştir.

Katılımcılara sosyal ağ sitelerinde hiç (1) gizlilik ayarlarını değiştirip değiştirmedikleri, (2) ağlarından/arkadaş listelerinden birilerini silip silmedikleri, (3) fotoğraflardan etiket kaldırıp kaldırmadıkları, (4) belirli güncellemeleri belirli kişilere sınırlayıp sınırlamadıkları ve (5) başkalarının yorumlarını profillerinden silip silmedikleri sorulmuştur. 490 kişilik örneklemin yaklaşık yüzde 32'si mahremiyet endişesi taşırken sadece yüzde 14,69'u çalkantılı bir çevrim içi deneyim yaşadıklarını ifade etmiştir. Ortalama teknolojik mahremiyet aracı kullanma sayısı ise 2,46'dır. Katılımcıların yüzde 65'i profillerinin gizlilik ayarlarını değiştirmiş, yüzde 58'i arkadaş listelerinden birini silmiş, yaklaşık yüzde 33'ü belirli güncellemeleri belirli kişilere sınırlamış, yaklaşık yüzde 34'ü profillerinden başka birisinin yorumunu silmiş ve yüzde 30'u da etiketlendikleri bir fotoğraftan etiketlerini silmiştir. Litt, iletişim mahremiyeti yönetimi teorisine (*communication privacy management theory*) dayanan hipotezlerini desteklemek için üç farklı lineer regresyon analizi gerçekleştirmiştir. Analizler sonucunda, kadınların teknolojik mahremiyet araçları kullanımının, erkeklere göre daha çeşitli olduğu, çalkantılı bir çevrim içi deneyim yaşayanların daha fazla teknolojik mahremiyet aracı kullandığı ve kısmen de olsa daha fazla sosyal ağ tecrübesi olanların daha çok teknolojik mahremiyet aracı kullandığı görülmüştür (Litt, 2013, ss. 1652-1654). Debatın ve arkadaşlarının, yukarıda değinilen araştırmasında olduğu gibi bu çalışma da tecrübe edilen olumsuz bir çevrim içi olayın, mahremiyet ayarlarını değiştirme motivasyonunu artırdığını göstermektedir.

Petronio (2002) tarafından geliştirilen iletişim mahremiyeti yönetimi teorisine (CPM) dayanan diğer bir çalışma da, Facebook platformu üzerinde kullanılan bireysel ve grup mahremiyet yönetimi stratejilerini inceler. 900 geçerli cevabın toplandığı çevrim içi anket çalışması sonucunda, yaş ve bireysel mahremiyet yönetimi arasında pozitif yönlü bir ilişki tespit edilmiştir. Araştırmanın çıktılarına bakıldığında, Petronio'nun teorisine paralel bir şekilde, kadınların erkeklere oranla daha fazla bireysel mahremiyet yönetimi stratejisi kullandığı görülmektedir. Grup mahremiyet yönetimi stratejilerinin kullanımında ise tam tersi bir durum söz konusudur (De Wolf vd., 2014, s. 451).

Taneja, Vitano ve Gengo, planlı davranış teorisi (*theory of planned behavior*) ve rasyonel seçim teorisi (*rational choice theory*) üzerinde geliştirdikleri çalışmalarında, rasyonellik temelli inançların, bireylerin Facebook'taki mahremiyet kontrollerini kullanma tutum ve niyetlerine etkisini incelemişlerdir. Örneklem 249 üniversite

öğrencisinden oluşmaktadır. Elde edilen bulgular; örneklemin temel Facebook kullanım amaçları insanlarla iletişim halinde olmayı, diğerleri ile fotoğraf paylaşmayı, etkinlik ve haberleri duyurmayı ve aile üyelerini ve arkadaşları hayattaki değişiklikler hakkında bilgilendirmeyi içerdiğini göstermektedir. Çalışma sonucunda, Facebook'taki mahremiyet kontrollerini kullanma niyeti ile tutumu arasında ve niyeti ile sosyal normlar arasında istatistiksel olarak anlamlı ilişki bulunmuştur. Mahremiyet kontrollerini kullanmanın faydaları ve kullanmamanın maliyeti ile tutumlar arasında da anlamlı bir ilişki tespit edilmiştir. Sonuç olarak, Taneja ve arkadaşları (2014, s. 172), çalışmalarının, mahremiyet kontrollerini kullanma maliyetinin tutuma olan etkisinin, bu kontrolleri kullanmama maliyeti kadar güçlü olduğunu gösterdiğini ifade etmişlerdir.

Alkeinay ve Norwawi (2014), sosyal ağlar için kullanıcı odaklı bir mahremiyet modeli geliştirilmesi gerektiğini ifade ettikleri çalışmalarında, 161 katılımcı üzerinde bir araştırma gerçekleştirmişlerdir. yüzde 57'si erkek ve yüzde 83'u 18-29 yaşları arasında olan katılımcıların, yüzde 49'u on yıldan uzun bir süredir internet kullanmaktadır. Bu çalışmadan not etmemiz gereken, katılımcıların yüzde 61'inin kendileri hakkında doğru bilgileri ve fotoğraflarını, hiçbir kısıtlama olmadan paylaştıklarını ancak konu coğrafi konumların paylaşılmasına geldiğinde daha dikkatli davranıldığınıdır. Katılımcıların yüzde 17'si konumlarını paylaştıklarını ve mahremiyetlerinin korunmasını önemsemediklerini bildirirken, yüzde 30'u sadece cep telefonu kullanırlarken konum bildirimini yaptıklarını ve yüzde 53'ü de mahremiyete ihtiyaç duydukları için konumlarını paylaşmadıklarını ifade etmişlerdir (Alkeinay & Norwawi, 2014, s. 194).

Nosko, Wood ve Molema'nın, yukarıda bahsedilen çalışmalarındaki araştırma tasarımına benzer bir şekilde, Külcü ve Henkoğlu da (2014, s. 763), literatürdeki araştırmalarda sıkça tercih edilen anket yönteminden farklı olarak, kullanıcıların mevcut mahremiyet, güvenlik ve farkındalıklarını ölçmenin en güvenilir yolu olduğunu ifade ettikleri, kullanıcı profillerinden veri toplama yöntemiyle bir araştırma gerçekleştirmişlerdir. Bu çalışmada, bilgi ve belge yönetimi uzmanı 400 Facebook kullanıcısının profillerinden, Mart-Nisan 2013 tarihinde toplanan veriler analiz edilmiş ve kullanıcıların mahremiyet oranları (*privacy rates*) hesaplanmıştır. Bu hesaplama, kullanıcıların hangi kişisel bilgileri profilinde paylaşıp paylaşmadığı verisi üzerinden gerçekleştirilmiştir. Elde edilen veriler, kullanıcıların yüzde 95'inden fazlasının adres, telefon numarası, doğum tarihi, ilham kaynağı kişiler, spor, politik görüş ve dini görüş

gibi önemli ve hassas kişisel bilgileri sakladıklarını göstermektedir. Çalışmadaki katılımcılar açısından fotoğraflar, yaşanan şehir ve iş/okul bilgisinin en az mahrem kabul edilen bilgilerdir. Literatürdeki çalışmalarda da görüldüğü gibi, bu çalışmadaki kadınlar da mahremiyet konusunda daha hassastırlar ve erkeklere göre profillerine mahremiyet ayarları ile daha fazla kısıtlama getirmişlerdir. Araştırmacılar, Facebook'taki arkadaş sayısı ve paylaşılan fotoğraf sayısı ile mahremiyet ve farkındalık seviyesi arasında bir ilişki olduğunu bulgulamışlardır (Külcü & Henkoğlu, 2014, s. 767). Kullanıcıların, mahremiyet ayarlarını kullanarak sakladıkları kişisel bilgilerine göre hesaplanan mahremiyet oranları; yüksek, orta ve düşük seviye mahremiyet olarak gruplandırılmış ve katılımcıların yüzde 44,5'inin yüksek, yüzde 34,8'inin orta ve yüzde 20,8'inin de düşük mahremiyet seviyesinde oldukları görülmüştür. Cinsiyete göre bakıldığında ise, kadınların yarısının yüksek mahremiyet seviyesinde olduğu, buna karşılık erkeklerin sadece yüzde 38,3'ünün mahremiyetlerine bu seviyede dikkat ettiği görülmektedir (Külcü & Henkoğlu, 2014, s. 765).

Saeri ve arkadaşları, Avustralya'daki bir üniversitede psikoloji okuyan 111 birinci sınıf öğrencisi ile iki aşamalı bir çalışma gerçekleştirmiştir. İlk aşamada, bir bilgisayar laboratuvarına, en fazla onar kişilik gruplar halinde alınan öğrencilere bir anket uygulanmıştır ve mahremiyet niyetler ölçülmeye çalışılmıştır. Çalışmanın ikinci aşaması ise, iki hafta sonra, izin veren öğrencilerin (107) Facebook profillerinin incelenmesiyle gerçekleştirilen mahremiyet davranışı araştırmasıdır. Çalışmada, yaşlı katılımcıların mahremiyetlerini koruma niyetlerinin daha fazla olduğu ve cinsiyetin herhangi bir anlamlı farklılık yaratmadığı, ancak niyetlerin davranışa dönüşümünde ise bir farklılaşma olduğu görülmüştür. Buna göre kadınlar, erkeklere göre daha fazla mahremiyeti koruma davranışı sergilerken yaş değişkeninin davranışlarda bir etkisi olmadığı söylenebilir. Araştırmacılar, niyetlerin mahremiyet bağlamında davranışlara genellenemeyeceğini ve bunun mahremiyet korumaya yönelik literatür için önemli bir uyarı olduğunu ifade etmişler (Saeri vd., 2014, ss. 359, 361, 366) ve elde ettikleri bulguların, diğer güvenlik uzmanlarının, bireylerin genellikle güvenlik ayarlarını güncelleyip değiştiremediklerine dair uyarılarıyla da tutarlı olduğunu belirtmişlerdir (Furnell, 2005).

Sezin Baysal Berkup, farklı dönemlerde dünyaya gelen ve farklı koşulların etkisi altında büyüyen X ve Y kuşaklarının, sosyal medya kullanımında mahremiyetlerini paylaşma eğilimlerini inceleyen nitel bir araştırma gerçekleştirmiştir. Her iki kuşaktan

yirmişer kişi ile (10 kadın – 10 erkek) Kasım 2014 – Ocak 2015 tarihleri arasında gerçekleştirdiği derinlemesine görüşmeleri, dört mahremiyet boyutu üzerinden ele alır: (1) Beden, (2) kadın–erkek ilişkileri ve cinsellik, (3) ev ve aile yaşantısı ve (4) dini ve siyasi görüş mahremiyetleri. Araştırma sonucunda, X kuşağına mensup bireylerin beden mahremiyetlerini, ev ve aile yaşantısına dair daha az paylaşım yaparak ev-mekân mahremiyetlerini, kadın-erkek ilişkileri ile ilgili bilgileri ve duyguları daha az paylaşarak ikili ilişki mahremiyetlerini ve siyasi görüş mahremiyetlerini Y kuşağına mensup bireylere göre daha fazla koruma eğiliminde oldukları sonucuna ulaşılmıştır. İki kuşak arasında, sadece dini görüşün sosyal ağlarda paylaşılması konusunda bir farklılık söz konusu değilken diğer boyutlarda X kuşağına mensup bireylerin daha korumacı bir mahremiyet anlayışı geliştirdikleri gözlemlenmektedir (Berkup, 2015, ss. 295-297).

Nemec Zlatolas ve arkadaşları, mahremiyet konularının sosyal ağ siteleri üzerinde kendini ifşayı nasıl belirlediğini anlamak için, mahremiyet bilinci, mahremiyet sosyal normları, mahremiyet politikası, mahremiyet kontrolü, mahremiyet değeri, mahremiyet kaygıları ve kendini ifşa etmeyi içeren bir araştırma modeli oluşturmuşlardır. Yaşları 18-65 (M=26,76) arasında değişen 661 katılımcıya (%43,1 erkek, %56,9 kadın) çevrim içi anket yöntemiyle ulaşılmıştır. Katılımcıların, ortalama Facebook arkadaş sayısı ise 302,98'dir. Araştırma; mahremiyet farkındalığı, mahremiyet sosyal normları, mahremiyet politikası, mahremiyet değerleri ve mahremiyet kaygılarının, Facebook'ta kişisel ifşayı etkilemede önemli olduğunu ve mahremiyet sosyal normlarının, mahremiyet politikasının ve mahremiyet kontrolünün mahremiyet değeri üzerinde bir etkiye sahip olduğunu göstermiştir. Araştırmacılar elde ettikleri sonuçların literatürdeki diğer sonuçları desteklediğini ifade etmişlerdir (Nemec Zlatolas vd., 2015, ss. 165-166). Farklı çalışmalarda ayrı ayrı incelenen mahremiyete ilişkin farkındalık, endişe, kontrol, değer vb. konuların tek bir çalışma altında ve kendini ifşayı da kapsayacak şekilde bir modele dönüştürülmüş olması bu çalışmayı özgün kılmaktadır.

Potoglou ve arkadaşları (2017), 2012-2015 yılları arasında gerçekleştirilen PACT¹⁶ kısa adlı AB projesinin verilerini kullanarak gerçekleştirdikleri analizlerle, bireysel mahremiyet tercihlerinin kültürel/ulusal çerçevede yaş, cinsiyet ve eğitim

¹⁶ Public perception of Security and privacy: Assessing knowledge, Collecting evidence, Translating research into action.

durumuna göre deęişkenlik gösterdiğini ortaya koyarlar. Araştırma, katılımcıları ortalama olarak, internet kullanım geçmişlerini saklamayan, herhangi bir veriyi en fazla bir aya kadar saklayan ve üçüncü şahıslarla paylaşmayan bir internet servis sağlayıcıyı (İSS) tercih ederler. Bununla birlikte katılımcılar, (polis tarafından gerçekleştirilen) sürekli devlet gözetimindeki potansiyel faydayı kabul ederler. Ancak bunun yalnızca uygun bir hesap verebilir yasal zemin altında olması gerektiğini söylerler.

Taddicken, sosyal ağ kullanıcılarının ne kadar kişisel bilgiyi ifşa ettiklerini ve bunun mahremiyet endişelerinden, sosyal alaka (*social relevance*) düzeyinden, yaş ve kullanılan uygulama sayısından nasıl etkilendiğini incelemek için, 2739 Alman sosyal ağ kullanıcısı üzerinde çevrim içi bir araştırma gerçekleştirir. Bulgular, mahremiyet endişesinin kendini ifşaya etkisinin çok düşük olduğunu ancak sosyal alaka ve kullanılan uygulama sayısının belirgin olduğunu gösterir. Araştırmacılar, literatürdeki çoğu araştırmadan farklı olarak, yaşın kendini ifşa etme düzeyi ve mahremiyet endişesi üzerinde neredeyse hiçbir etkisi olmadığı sonucuna ulaşırlar. Bulgular, örneklemin sadece üniversite öğrencilerinden oluşmadığı ve 13 ile 83 gibi geniş bir aralıkta dikkate alındığında, dikkate değerdir. Son olarak, cinsiyet ile ilgili yapılan analizlerde ise cinsiyetin çevrim içi mahremiyet endişeleri ile kendini ifşaya yönelik genel isteklilikte etkili olduğu sonucuna ulaşılır. Ancak bu cinsiyet farklılığı, sadece hassas kişisel bilgilerin (*sensitive personal information*) herkesin erişimine açıldığı durumlarda geçerlidir (Taddicken, 2014, ss. 265-268).

Momen ve Piekarska (2017), yaygınlaşan akıllı cep telefonu kullanımının doğurduğu kişisel veri mahremiyeti konusuna odaklanırlar. Akıllı cihazlara kurulan ve çeşitli izinler (*permissions*) verilen uygulamalar ile ilgili küçük bir anket çalışması (toplamda 252 katılımcıya sadece iki soru sorulur) yapan araştırmacılar, kullanıcı farkındalığını geliştirmek için “Aware” ismini verdikleri bir uygulama da geliştirirler. Katılımcılara sorulan “uygulamaları yüklerken "gerekli izinlere" ne sıklıkla dikkat ediyorsunuz? (Her zaman, bazen, asla)” ve “kabul et düğmesine ne kadar hızlı basıyorsunuz? (Anında, bir dakika içinde, bir dakikadan fazla)” sorularına verilen cevaplara göre, katılımcıların yüzde 90’ından fazlasının bu önemli kararı bir dakika içinde ya da anında verdiğini gösterir. Araştırmacılar, kişisel verilere yönelik saldırıları önlemede farkındalık eksikliğinin büyük bir engel olduğuna işaret ederler ve mahremiyetin büyük ölçüde bireysel algıya bağlı olduğunu, kullanıcıları eğitmenin ve

güçlendirmenin anahtarının onlara akıllı telefonlarında olup bitenlere dair şeffaflık sağlamak olduğunu savunurlar (Momen & Piekarska, 2017, s. 23).

Sefer Kalaman'ın Kasım 2015 – Ocak 2016 tarihleri arasında Türkiye'deki 15 yaş ve üzeri beş bin Facebook kullanıcısından yüz yüze anket yöntemi ile topladığı verilere dayanarak hazırladığı çalışmada, katılımcıların Facebook'ta mahrem bilgilerini ne oranda ifşa ettikleri, Facebook aracılığıyla gözetlendiklerinin ve mahremiyetlerinin ihlal edildiğinin farkında olup olmadıkları ve katılımcıların demografik özellikleri ile mahremiyetin ifşası, gözetimin farkındalığı ve mahremiyetin ihlalinin farkındalığı arasında bir ilişkinin olup olmadığı incelenmiştir (Kalaman, 2017, s. 10). Araştırmanın sonuçları, kullanıcıların mahremiyetlerini paylaşma konusunda oldukça paylaşımcı eğilimler gösterdiklerini ve büyük oranda kendi mahremiyetlerini ifşa ettiklerini göstermektedir. Katılımcıların yüzde 93'ü Facebook profillerinde gerçek adlarını kullanmakta, yüzde 71,6'sı doğum tarihlerini, yüzde 77,4'ü yaşadığı yeri, yüzde 66,5'i eğitim durumunu, yüzde 29'u ilişki durumunu, yüzde 39,4'ü mesleğini, yüzde 61,7'si memleketini ve yüzde 23,2'si de aile veya akrabalarını profil sayfasında paylaşmaktadır. Kişisel bilgilerin paylaşıldığı Facebook profillerinin gizlilik ayarları ise katılımcıların yüzde 55,6'sı tarafından yapılmıştır (Kalaman, 2016, s. 135). Araştırmada ayrıca, katılımcıların büyük bir kısmının Facebook aracılığı ile gerçekleşen gözetimin farkında olmadığı sonucuna ulaşılmıştır. Bunun yanı sıra araştırmada, erkeklerin kadınlara göre mahremiyetlerini daha fazla ifşa ettiği ancak buna rağmen gözetlendiklerine dair farkındalığın yine erkeklerde daha fazla olduğu ortaya çıkmıştır. Araştırma sonucunda, kişilerin mahremiyet eğilimleri ile yaş, cinsiyet, eğitim ve çalışma durumu ve yaşanan bölge değişkenlerine göre farklılık gösterdiği söylenebilir (Kalaman, 2017, ss. 24-25).

Yeni medya ve mahremiyet literatürüne katkı sağlayan bir diğer doktora tez çalışmasında, Konya il merkezinde yaşayan sosyal ağ kullanıcılarına yönelik bir saha araştırması yapılmıştır. Yeni medya kullanıcılarının “mahremiyet tutum ve davranışlarında bir dönüşüm meydana gelip gelmediğini, meydana gelmişse mahremiyet dönüşümüne etki eden unsurların neler olduğunu ve mahremiyetin yeni sınırlarını” ortaya koymayı amaçlayan çalışmada, 736 kişilik (%47,7 kadın, %52,3 erkek) bir örneklem grubu oluşturulmuştur. 2015 yılında gerçekleştirilen araştırmaya katılanların yüzde 72,3'ü sosyal ağlara akıllı telefonlar aracılığıyla ulaştıklarını belirtmişlerdir. Araştırmadaki “sosyal ağlarda paylaştığınız içerikleri gerçek hayattaki çeşitli

ortamlarda da paylaşıyor mısınız?” sorusuna, katılımcıların yüzde 66,3’ü bir kısmını paylaşırım, yüzde 25,8’i evet, hepsini paylaşırım ve yüzde 7,9’u hiçbirini paylaşmam cevabını vermiştir. Katılımcıların neredeyse yüzde 40’ı sosyal ağ sitelerinin topladıkları kişisel verileri kamu kuruluşları veya özel şirketlerle paylaşabileceğini bildiklerini ve bu gerekçe ile çok az şahsi bilgi paylaştıklarını ve yüzde 32,6’sı ise konu hakkında fikirleri olmadığını söylemiştir. Katılımcılara göre, bedenın bazı bölgeleri, cinsel hayat ve aile içi sorunlar en mahrem olan konulardır. Buna karşılık dini görüşler, siyasi görüşler ve kıyafet mahrem olarak görülmemektedir (Budak, 2016, ss. 146, 155-157, 159). Araştırmacı, çalışmadan elde ettiği veriler ışığında, yeni medya kullanımının kuşakların mahremiyet tutum ve davranışlarını görelı olarak etkilediğı, bu etkiye bağılı olarak mahremiyet sınırlarının merkeze doğru çekildiğı ve belli konularla sınırlandırılmaya başladığı sonucuna ulaşmıştır. Bu değişimin yanı sıra, katılımcıların mahremiyet tutumu ile davranışları arasında farklılaşmalar da gözlemlenmiştir: Aile ile ilgili özel anları mahrem alan içerisinde değerlendiren katılımcıların “çocuklarının gelişim süreçlerini, nişan, düğün doğum günü vb. özel günlerini” yüksek oranda paylaştıkları görülmüştür (Budak, 2016, ss. 236-237). Özel ilişkileri mahrem olarak değerlendiren katılımcıların yüzde 37,2’si de eşi ya da sevgilisiyle olan özel anlarının fotoğraflarını sosyal ağlarda paylaştıkları ifade etmişlerdir. Budak (2018, s. 168), bu durumu sosyolojik açıdan, özel ilişkilerin mahrem alan içindeki konumunda belli bir dönüşümün başladığının işareti olarak değerlendirilir. Budak son olarak, mahremiyet tutumları ile davranışları arasındaki uyumsuzlukların, bilişsel uyum çerçevesinde mahremiyetin aleyhine bir dönüşüme uğrayacağını ifade eder.

Zhang ve Fu (2020), stres ve cinsiyetin mahremiyet endişeleri ile sosyal ağlarda kendini ifşa etme arasındaki ilişkiyi nasıl etkileyebileceğini incelemek için bir çalışma gerçekleştirir. Araştırmada kullanılan veriler, 2016 yılında Hong Kong’daki bir üniversitede okuyan 18-25 yaşlarındaki 560 öğrenciye (%60,7 kadın, %39,3 kadın) uygulanan sınıf içi anketlerden elde edilir. Araştırmacılar, Wheelless ve Grotz’un (1976) kendini ifşa için tanımladıkları beş boyutu kullanırlar. Bunlar miktar (*amount*), samimiyet (*intimacy*), dürüstlük (*honesty*), niyet (*intent*) ve değerdir (*valence*). Zhang ve Fu, bu boyutların ilk dördünü çalışmalarına dahil ederler. Yapılan analizler sonucunda, mahremiyet endişesi ile sosyal medyadaki ifşanın “miktar”, “samimiyet” ve “dürüstlük” boyutları arasında negatif yönlü bir ilişki olduğu ancak stres düzeyinin bu ilişkiyi

hafiflettiğini ortaya koyar. Başka bir ifadeyle bir kişi ne kadar çok stres yaşarsa, mahremiyet endişeleri ile ifşa miktarı ve samimiyeti arasındaki ilişkinin yönü değişir. Bu çıktılar, mahremiyet paradoksu (*privacy paradox*) olarak bilinen fenomeni çürütür. Bulgular aynı zamanda, stresin hafifletici etkisinin cinsiyete göre farklılaştığını da gösterir (R. Zhang & Fu, 2020, ss. 245-247).

Mahremiyet yönetimi davranışları konusunda, gençler (ergenler) ve genç yetişkinler üzerinde yapılan araştırmaların yanında, yetişkin yaş grupları arasındaki farklılıklara odaklanan çalışmaların sınırlı olduğunu söyleyen Kezer ve çalışma arkadaşları, toplamda 518 Facebook kullanıcısı yetişkin üzerinde bir çalışma gerçekleştirir. Araştırmacılar 18-40, 41-65 ve 65+ olmak üzere üç farklı yaş grubuna ayrılan katılımcıların Facebook kullanımları, mahremiyet tutumları, çevrim içi mahremiyet yazarlıkları ve Facebook'taki mahremiyetlerini koruyucu ve kişisel bilgilerini açıklayıcı davranışlarını incelerler. Çalışmadan elde edilen bulgular, yaş gruplarının çevrim içi mahremiyet okuryazarlığı, mahremiyet endişesi ve davranışları ve Facebook'taki kendini ifşa etme ve mahremiyetlerini koruyucu davranışları açısından farklılaştıklarını gösterir. Araştırmaya göre daha genç yetişkinlerin sosyal ağ sitelerini daha sık kullandıkları, Facebook'u sosyal etkileşim amacıyla kullandıkları ve daha geniş bir arkadaş ağına sahip oldukları söylenebilir. Araştırmada elde edilen bir diğer sonuç ise genç yetişkinlerin daha fazla kendilerini ifşa ettikleri ve buna bağlı olarak daha fazla mahremiyeti koruyucu davranış sergiledikleridir. Araştırmacılar bu sonucun, yaşlı yetişkinlerin, mahremiyeti koruyucu davranışlara gençler kadar ihtiyaç duymadıklarından kaynaklanıyor olabileceğini söylerler (Kezer vd., 2016).

Kezer ve çalışma arkadaşlarının çalışmasında, Baruh ve Cemalcılar (2014) tarafından geliştirilen çok boyutlu mahremiyet yönelimi ölçeği de kullanılır. Mahremiyet tutumlarının tüm boyutları ile Facebook'ta mahremiyeti koruyucu önlemlerin benimsenmesi arasında pozitif yönlü bir ilişki vardır. Yaş grupları arasında, bir hak olarak mahremiyet ve kendi mahremiyetine ilişkin kaygı boyutlarında, istatistiksel olarak anlamlı bir fark yoktur. Yaşlı katılımcıların, başkalarının mahremiyetine değer verme ve diğer ihtimalli mahremiyet boyutlarındaki farkındalıkları genç yetişkinlere kıyasla daha fazladır (Kezer vd., 2016).

Heravi, Mubarak ve Raymond Choo, kullanımlar-doyumlar yaklaşımı ve Smith, Dinev, ve Xu (2011) tarafından geliştirilen öncüler - mahremiyet endişeleri - sonuçlar (APCO)¹⁷ modeline dayanarak gerçekleştirdikleri çalışmada, literatürün aksine, bir mahremiyet paradoksu ile karşılaşmadıklarını, katılımcıların mahremiyet endişelerinin mahremiyet davranışları ile birbirine paralel seyrettiğini ifade etmişlerdir. 918 ve 521 geçerli katılımın sağlandığı iki farklı araştırma gerçekleştiren Haravi vd., ilk çalışmanın çıktıları ışığında çevrim içi sosyal ağ kullanımının en yaygın güdülerini; (1) ilişki sürdürme (*relationship maintenance*), (2) eğlence (*entertainment*), (3) ilişki kurma (*relationship building*) ve (4) bilgi arama (*information seeking*) şeklinde sıralamışlardır. Bu güdüler ile enformasyon mahremiyeti endişeleri arasındaki ilişkinin pratik önemi oldukça azdır. Araştırmacılar, çevrim içi sosyal ağ sitelerinden sağlanan doyumun, kullanıcıların enformasyon mahremiyeti konusunda daha katı veya daha gevşek bir tutum benimsemesine yol açmadığını, ancak bu doyumların, kendini ifşa üzerinde belirgin bir etkisi olduğunu söylerler. Son olarak, enformasyon mahremiyeti endişelerinin mahremiyeti koruma önlemlerine, literatürdeki çalışmalardan farklı olarak, pozitif bir etkisi olduğu gözlemlenmiştir (Heravi vd., 2018, ss. 452-453).

Semiz Türkoğlu (2018), sosyal medyada mahremiyetin değişimi, dönüşümü ve mahremiyet farkındalığını ölçebilecek bir ölçek geliştirmeye çalışır. Yapılan iki pilot çalışmanın ardından, yüzde 74,9'u 18-24 yaş aralığında ve büyük çoğunluğu kadın olan (%71,5) 386 üniversite öğrencisi ile bir çalışma gerçekleştirir. Yapılan çalışma, uygulanabilir bir ölçek ortaya koyamasa da üniversite öğrencilerinin mahremiyet kavramından ne anladıklarını ortaya koyar. Anket sonuçlarına göre, öğrenciler için mahremiyet¹⁸ gizlilik (M=1,55), özel alan (M=1,57) ve kişilik haklarına saygılı olunmasıdır (M=1,72). Araştırmacı, aynı seçenekleri sosyal medyada mahremiyet başlığı altında tekrar sormuştur ve buna göre sosyal medyada mahremiyet öğrenciler için özel alan (M=1,50), izinsiz fotoğraf kullanmamak (M=1,53) ve izinsiz video kullanmamaktır (M=1,57).

¹⁷ Antecedents / Privacy Concerns / Outcomes

¹⁸ Çalışmada beşli ölçek kullanılmış ve 1 kesinlikle katılıyorum 5 ise kesinlikle katılmıyorum seçeneğini ifade etmektedir.

Yabancı, Akça ve Ulutaş, çevrim içi mahremiyet kaygısı ile duygusal zekâ arasındaki ilişkiyi inceleyen çalışmalarında, Buchanan vd. (2007) tarafından geliştirilen ve Alakurt (2017) tarafından Türkçeye çevrilen, çevrim içi mahremiyet ölçeğini kullanırlar. Örnekleme 147'si (%33) kadın, 295'i (%67) erkek olmak üzere toplam 442 üniversite öğrencisinden oluşan araştırmada, duygusal zekâ ile çevrim içi mahremiyet kaygısı arasında anlamlı bir ilişki olmadığı, ancak çevrim içi mahremiyet kaygısının yaş ile doğru orantılı olduğu sonucuna ulaşılr. Özellikle 18-25 yaşındaki öğrenciler ile 36-40 yaşındaki öğrenciler arasında çevrim içi mahremiyet kaygısı açısından anlamlı bir farklılık vardır. Araştırmaya katılan öğrencilerin en çok takip ettiği sosyal medya platformlarına ilişkin istatistikler de toplanmıştır. En çok takip edilen sosyal medya platformu sorusuna öğrencilerin yüzde 60'ı Instagram, yüzde 15'i Twitter, yüzde 14'ü Facebook ve yüzde 4'ü YouTube cevabını vermiştir (Yabancı vd., 2018, ss. 201, 207).

Kodak, üç farklı kuşak üzerinde mahremiyetin dönüşümüne odaklanan, yapılandırılmış görüşme yönteminin benimsendiği bir araştırma gerçekleştirir. Mahremiyetin kuşaklar arasında nasıl değiştiğine yönelik bir perspektif sunan çalışma sonucunda Kodak, farklı kuşaklardaki bireylerin mahremiyet anlayışları arasında hem benzerlikler hem de farklılıklar olduğunu ve bunun da düşünömsel modernite ile açıklanabileceğini ifade eder. Araştırmadaki, *“İnsanların gündelik yaşamlarını sürekli sosyal medya üzerinden birbirleriyle paylaşmalarını nasıl değerlendiriyorsunuz?”* sorusuna verilen yanıtlar, katılımcıların çevrim içi ortamda mahremiyete yönelik algılarına dair fikir vermesi açısından değerlidir. Araştırmadaki birinci kuşak kadın grubuna dahil katılımcılar, özellikle doğum fotoğraflarının, yenilen yemeklerin fotoğraflarının ve gidilen mekanların paylaşılmasına değinerek “herkesin bir mahreminin olması gerektiğini” söylemişlerdir. Aynı kuşaktaki erkekler için bu paylaşımlar, kişilerin komplekslerinden ileri gelmektedir: Onlara göre, yaşamlarında yeterince sosyal deneyime sahip olamayanlar bu paylaşımları yapmaktadır. İkinci kuşak kadınlar ise, bu paylaşımların gerçekliğini sorgularlar ve “herkesin hayatını çok iyiymiş gibi” gösterdiğini ifade ederler. Bu gruptaki katılımcılar, kutlama ve ziyaretlerin paylaşılabileceğini, ancak özel anların paylaşılması gerektiğini belirtmişlerdir. İkinci kuşak erkek katılımcılardan biri, “başarı, mezuniyet, yurtiçi veya yurtdışı gezilerine ait fotoğrafların, anıların paylaşılmasında bir sakınca görmediğini ama özel olanın paylaşılması gerektiğini belirtmiştir.” Bir diğeri ise, hazzın ‘deneyimden mi, yoksa

deneyimi paylaşmaktan mı' elde edildiğini sorgulamış ve deneyimi paylaşımının nedenini şöyle yorumlamıştır: “O paylaşım, o yaşadığı ona yetmediği için yapılıyor.” Üçüncü kuşak kız torun grubu ise, “sosyal mecraların gerçek olmadığını, insanların oradaki paylaşımlarla oldukları gibi değil, olmak istedikleri gibi bir imaj çizdiklerini ifade etmişlerdir.” Bu grup için sosyal medyayı kullanmakta bir sakınca yoktur, ancak gündelik hayattaki her an da paylaşılmalıdır. Erkek torunlara göre ise bu paylaşımlar, insanların egolarını beslemektedir ve sosyal medya paylaşımları sosyalleşmenin yerini almıştır. Onlara göre, bu mecralar insanları yalnızlaştırmış ve yaşam stili teşhirinden ötürü diğer insanları aşağılamayı örtük biçimde olsa da meşrulaştırmaktadır (Kodak, 2018, ss. 109-110).

Akikol, kadın dijital göçmenlerle yaptığı yarı yapılandırılmış görüşmeler ve 367 kişiye uyguladığı anket çalışması sonucunda, kadın dijital göçmenlerin, yüz yüze iletişimde bulunduğu kişilerden çok daha fazla sayıda kişiyle, Facebook üzerinden kişisel bilgilerini paylaştıkları, özel yaşantılarını kamusal alana taşıdıkları sonucuna ulaşır. Katılımcılar, “cinsel çağrışımlı bilgiler, kişisel fotoğraflar, ilişki durumu, yorumlar ve yazışmalar, yemek paylaşımları gibi” konuların özel alana girdiğini ifade ederler ancak, yaptıkları paylaşımların çoğu bu özel alan olarak nitelendirdikleri alana girer. Sonuçları değerlendiren Akikol, kadın dijital göçmenlerin özel alan olarak belirledikleri alanı daralttıklarını, kamusal alan ile özel alan ayırımında sınırların değiştiğini ve muğlaklaştığını ifade eder (Akikol, 2018).

2018 yılında Livberber Göçmen tarafından hazırlanan doktora tezi, kişilerin kendileri hakkındaki bilgi paylaşımlarına, tanıdık ve yabancıları içeren diğer kişiler hakkındaki bilgileri öğrenmelerine ve mahremiyete yönelik diğer tüm tutumlarına odaklanır. Bu çerçevede, araştırmaya katılanların röntgencilik ve teşhir düzeylerini ölçen ölçekler kullanılır. İzmir ve Konya’da gerçekleştirilen saha araştırmalarında, toplam 815 (%56,4’ü kadın, %43,6’sı erkek) kişiye ulaşan araştırmacı, hem dijital yerli-dijital göçmen ayırımını işe koşarak bulguları değerlendirir. Katılımcıların yüzde 53,7’sini dijital göçmenler, yüzde 46,3’ünü de dijital yerliler oluşturmaktadır. Araştırmacı, mahremiyet yönelimleri ile sosyal medya kullanım amaçlarını da ölçmüştür. Bulgular ışığında, en güçlü üç sosyal ağ kullanımı nedeninin “arkadaşlarla iletişimde bulunmak”, “mesaj göndermek ya da mesaj almak” ve “eğlenmek ve rahatlamak” olduğu söylenebilir. Katılımcıların en sık kullandığı sosyal ağ aracı ise WhatsApp’tır. Katılımcıların

neredeyse tamamı (%95) sosyal ağlarda gerçek adlarını kullanırlarken, yaklaşık yüzde 86'sı yaşadıkları yer ve memleket bilgilerini, yaklaşık yüzde 78'i eğitim bilgilerini ve sadece yüzde 17,3'ü siyasi görüşlerini paylaşmaktadır (Livberber Göçmen, 2018, s. 136). Araştırmacının, cinsiyetler ve şehirler arasındaki farklılığı ortaya koymak için yaptığı ki-kare testlerine bakıldığında, “erkeklerin kadınlara, İzmir’deki katılımcıların da Konya’daki katılımcılara göre” kişisel bilgilerini daha yüksek oranda paylaştığı söylenebilir. Livberber Göçmen, bu sonucun iki şehir arasındaki toplumsal yapı farklılığıyla açıklanabileceğini söyler.

Aynı araştırma, katılımcıların röntgencilik ve kendini teşhir düzeylerini de ölçer. Bu verilere göre, Konya’da yaşayan katılımcıların İzmir’dekilere göre ve kadınların da erkeklere göre tüm röntgencilik düzeylerinde daha yüksek orana sahip olduğu görülmektedir (Livberber Göçmen, 2018, ss. 148-149). Betimleyici istatistikler ışığında, anlamlı bir farklılık görülme de erkeklerin kadınlara göre ve İzmir’de yaşayanların Konya’da yaşayanlara göre kendini daha fazla teşhir ettiği söylenebilir (Livberber Göçmen, 2018, ss. 155-156).

Livberber Göçmen, Baruh ve Cemalcılar (2014) tarafından geliştirilen “mahremiyet yönelimi ölçeği” ile toplanan verileri kullanarak örneklemini üç alt boyuta ayırır: (1) mahremiyet savunucuları, (2) mahremiyet bireycileri ve (3) mahremiyet umursamazları. Katılımcıların yüzde 55’i mahremiyet bireycileri, yüzde 42,7’si mahremiyet savunucuları ve sadece yüzde 2,3’ü mahremiyet umursamazları alt boyutlarında yer alır. Mahremiyet yönelim boyutlarında, yaşanan şehir ve cinsiyete göre anlamlı bir farklılık olup olmadığına ilişkin yapılan testler, iki şehir arasında “bir hak olarak mahremiyet” ve “kendi mahremiyetine ilişkin kaygı” boyutlarında istatistiksel olarak anlamlı bir farklılık olduğunu gösterirken “başkalarının mahremiyetine ilişkin kaygı” ve “diğer ihtimalli mahremiyet” boyutlarında farklılık anlamlı değildir. Cinsiyetler arasında ise tüm boyutlarda anlamlı bir farklılık söz konusudur. Bu sonuçlara göre, araştırmaya katılan kadınların erkeklere göre mahremiyeti daha fazla bir hak olarak gördükleri, kendilerinin ya da başkalarının mahremiyetine ilişkin kaygılarının daha yüksek olduğu ve “kişinin mahremiyetinin korunmasında diğerlerinin de gösterdiği çabanın önemine vurgu yapan diğer ihtimalli mahremiyet noktasında” da daha yüksek oranlara sahip olduğu söylenebilir. Son olarak, bu araştırmada değinilmesi gereken yaş ve eğitim durumuna göre yapılan karşılaştırmalardır. Dijital göçmen ve dijital yerli

ayrımının kullanıldığı çalışmada, mahremiyet yönelim boyutlarının tümünde iki kategori arasında istatistiksel olarak anlamlı bir farklılık saptanmıştır. Eğitim durumuna göre ise, “diğer ihtimalli mahremiyet” boyutunda anlamlı bir farklılık olduğu, ancak “bir hak olarak mahremiyet”, “kendi mahremiyetine ilişkin kaygı” ve “başkalarının mahremiyetine ilişkin kaygı” boyutlarında anlamlı bir farklılık olmadığı söylenebilir (Livberber Göçmen, 2018, ss. 160-163).

Liu ve Wang, sosyal medya kullanıcılarının sosyal ağlarda farklı sosyal çevrelerle etkileşimde bulunurken mahremiyet sınırlarını nasıl oluşturdıklarını, kendi kendini ifşa kararları nasıl verdiklerini ve ayrıca kültürün mahremiyet sınırlarının oluşum sürecindeki etkisini incelemek için bir araştırma gerçekleştirir. Araştırmanın teorik temellerini Petronio’nun (2002) İMY teorisi ve Hofstede’nin (2002) kültür boyutları oluşturur. ABD’den 381, Çin’den ise 450 geçerli yanıtın toplandığı çevrim içi anket çalışmasından elde edilen veriler sonucunda, sosyal ödüller (*social reward*) ile kendini ifşa etme niyeti arasında (*intention to self-disclose*) pozitif yönlü bir ilişki olduğu; mahremiyet riski (*privacy risk*) ve mahremiyete değer verme eğiliminin (*disposition to value privacy*) ise kendi kendini ifşa etme niyetiyle negatif yönde ilişkili olduğunu gösterir. İki ülke arasında yapılan karşılaştırmalarda ise Çinliler için grup normlarının mahremiyet kontrolü üzerinde daha güçlü bir etkiye sahip olduğu; gizlilik ayarlarının algılanan etkinliğinin (*perceived effectiveness of privacy settings*) sosyal ödüller ve mahremiyet kontrolü üzerindeki etkisinin ise Amerikalılarda Çinlilere göre daha güçlü olduğu görülür (Liu & Wang, 2018).

Kütükoğlu (2019), üç farklı kuşak (X, Y ve Z) üzerinde gerçekleştirdiği araştırmasında, sosyal medyadaki mahremiyet algısını ortaya koymaya çalışır. Hem yüz yüze hem de çevrim içi anket yönteminin tercih edildiği çalışmada, 1625 geçerli katılımcıdan (%52,8 kadın, %48,2 erkek) toplanan veriler analiz edilmiştir. Analiz sonuçlarına bakılarak, sosyal medyada yapılan paylaşımlara ilişkin kaygı düzeyinin kuşaklara, cinsiyete ve eğitim düzeyine göre istatistiksel olarak anlamlı farklılık gösterdiği söylenebilir (Kütükoğlu, 2019, ss. 188, 192). Araştırmacının, katılımcıların mahremiyet kaygısını ölçmek için tek bir ölçek kullanmak yerine, literatürdeki araştırmalarda kullanılan sorulara dayanarak alternatif bir soru formu oluşturduğunu hatırlatmak yerinde olacaktır.

Aydın'ın (2018) tüketici mahremiyeti üzerine hazırladığı doktora tezi, katılımcıların hangi kişisel bilgileri mahrem olarak gördüklerine dair bir tablo sunar. Araştırmaya katılan 484 kişiye göre en mahrem bilgiler parmak izi, kimlik numarası, kredi kartı numarası ve anne kızlık soyadıdır. Yaş, cinsiyet ve eğitim düzeyi gibi bilgiler ise en az mahrem olarak algılanan bilgilerdir. Bulgular, yaşlıların gençlere göre daha fazla mahremiyet endişesi taşıdığını göstermektedir. Literatürdeki pek çok araştırmayı destekleyen bu sonuç, “gençlerin teknolojiye ve internete olan yatkınlıkları ve bu araçları kullanma sıklıkları” ile ilişkilendirilebilir (Aydın, 2018, s. 138).

2018-2019 yılları arasında, Endonezya'da gerçekleştirilen ve 164 katılımcıya ulaşılan küçük çaplı bir araştırma, Endonezyalı Y kuşağının kendileriyle ilgili kişisel verilerden çok, aileleriyle ilgili verilerin korunması gerektiğini gösterir. Araştırmacılar, Y kuşağının interneti kullanırken genel olarak, endişeli ve temkinli oldukları ve internet geçmişlerinin kaydedilmesinden endişelendikleri eklerler. Araştırmada üzerinde durulması gereken belki de en çarpıcı sonuç ise, katılımcıların internette kendi verileri korumak için hükümetin yaptırımlarından çok kendi yeteneklerine güveniyor olmalarıdır (Noor, 2020, s. 85). Bu çıktı, dijital okuryazarlığın önemi ile ilişkilendirilebilir: Hükümetler, mevcut yasal düzenlemeler ve uluslararası anlaşmalar çerçevesinde, vatandaşlarının internet üzerindeki haklarını koruyucu önlemler almalı ve çeşitli yaptırımlar uygulamalıdır. Ancak hiçbir yasal düzenleme ve yaptırım, teknolojinin ve mahremiyete yönelik oluşan tehditlerin hızına yetişemez. Bu sebeple, bireylerin kendi mahremiyetlerini ve kişisel verilerini korumak için kendi yeteneklerine güvenmeleri oldukça önemlidir. Bu yetenekler ise dijital okuryazar olarak elde edilebilir.

Furini ve arkadaşları (2020), yukarıda aktarılan çalışmalardan farklı olarak kullanıcıların akıllı cep telefonu uygulamalarının kullanımına ilişkin mahremiyet algılarına odaklanır. İki farklı hipotezin test edildiği çalışma için, iki farklı araştırma tasarlanır. 200 gönüllünün katıldığı ilk araştırma, “kullanıcılar akıllı telefonda depolanan verilerin önemini hafife alıyor ve bu kıt bilgi, gizlilik konusundaki algılarını etkiliyor” şeklinde ifade ettikleri hipotezi test eder. Bu araştırmada, katılımcılara aynı anket soruları, mahremiyet riskleri hakkında bilgilendirilmeden önce ve sonra sorulur ve cevaplar arasındaki farklılık istatistiksel olarak karşılaştırılır. Katılımcılara, “akıllı telefon kullanırken mahremiyetinize verdiğiniz önemi derecelendirin” sorusu ile bu sorunun rehber, multimedya içerikler, Wi-Fi bağlantıları, mikrofon, kamera, çalışan uygulamalar

ve titreşim için özelleştirilmiş halleri sorulmuş ve katılımcılardan bu sorular için yüksek, orta, biraz, hiç ve fikrim yok cevaplarından birini tercih etmesi istenmiştir. Daha sonra kullanıcılar, çeşitli veri paylaşımlarından kaynaklanabilecek sorunlar hakkında bilgilendirilmiş ve sorulara tekrar cevap vermeleri istenmiştir. Araştırmacılar yaptıkları karşılaştırmalar sonucunda, ilk hipotezlerini destekleyen sonuçlara ulaşmıştır: Mahremiyete verdikleri önemi yüksek olarak gören katılımcıların oranı, bilgilendirme sonrası yüzde 30'dan yüzde 82'ye çıkmıştır.

Furini ve arkadaşları, ikinci hipotezlerini, “kullanıcılar, kişisel bilgilerine ne zaman, nasıl ve ne ölçüde erişildiği ile ilgilenmezler: hangi verilerin alınacağını ve bunların uygulamanın çalışması için gerçekten gerekli olup olmadığını araştırmadan uygulamaları yüklerler” şeklinde ifade ederler. Bu hipotezi test etmek için kartopu örneklem yöntemi ile 30 gönüllüye ulaşırlar. Gönüllülerden, cep telefonlarında şu an kurulu olan uygulamaların listesini paylaşmaları istenmiş ve toplamda 843 yüklü uygulamanın bilgisine ulaşılmıştır. Araştırmacılar, bu uygulamaların kullanıcılardan talep ettikleri erişim izinlerinin, uygulamanın çalışabilmek için gerek duyduğundan daha fazla olup olmadığını analiz etmiş ve gönüllülerin telefonlarındaki yüklü olan uygulamalar ile ilgili olarak şu bulgulara ulaşmışlardır:

- Kişiler: yüzde 24'ü erişiyor ve yüzde 39'u kullanıcının gizliliğini ihlal ediyor;
- Konum: yüzde 36'sı erişiyor ve yüzde 28'i kullanıcının gizliliğini ihlal ediyor;
- Telefon Kimliği (IMEI): yüzde 8'i erişiyor ve yüzde 68'i kullanıcının gizliliğini ihlal ediyor;
- SMS: yüzde 7'si erişiyor ve yüzde 37'si kullanıcının gizliliğini ihlal ediyor;
- Multimedya depolama: yüzde 56'sı erişiyor ve yüzde 29'u kullanıcının gizliliğini ihlal ediyor;
- Mikrofon: yüzde 12'si erişiyor ve yüzde 38'i kullanıcının gizliliğini ihlal ediyor;
- Wi-Fi bağlantıları listesi: yüzde 33'ü erişiyor ve yüzde 52'si kullanıcının gizliliğini ihlal ediyor;
- Titreşim: yüzde 37'si erişiyor ve yüzde 22'si kullanıcının gizliliğini ihlal ediyor;
- Çalışan uygulamalar listesi: yüzde 7'si erişiyor ve yüzde 58'i kullanıcının gizliliğini ihlal ediyor;
- Fotoğraf Kamerası: yüzde 26'sı erişiyor ve yüzde 46'sı kullanıcının gizliliğini ihlal ediyor;
- Video Kamera: yüzde 14'ü erişiyor ve yüzde 64'ü kullanıcının gizliliğini ihlal ediyor (Furini vd., 2020, s. 1060).

Araştırmacılar, bu bulgulara dayanarak, kullanıcıların cep telefonlarına yükledikleri uygulamaların hangi verilere eriştiklerini ve özellikle bu verilere erişimin

uygulamanın çalışabilmesi için gerekli olup olmadığını önemsemedikleri sonucuna ulaşırlar.

Gökalier ve Saatçioğlu (2020), amaçlı örneklem yöntemi ile seçilen 8 kadın ve 10 erkek üzerinde, 2019 yılında gerçekleştirdikleri derinlemesine görüşmeler ile katılımcıların, sosyal ağlardaki gizlilik kurallarına bakış açıları ve veri paylaşımına yönelik görüşleri ile katılımcıların hangi tür gizlilik yaklaşımına sahip oldukları sorularına yanıt ararlar. Örneklemin sosyal ağları kullanma amacı, çoğunlukla iletişim ve haber almaktır. Derinlemesine görüşmeler sonucunda, katılımcıların yaklaşık yüzde 28'i özel yaşamlarını sosyal medyada paylaşmamayı tercih ettiği, yüzde 11,2'sinin sosyal medyayı yaşamlarının bir yansıması olarak kullandığı ve yüzde 22,2'sinin de sık olmasa da zaman yaşamlarındaki gelişmeleri paylaştıkları görülür. Gizlilik ayarları açısından incelendiğinde, katılımcıların yüzde 33,3'ünün profillerinin sadece tanıdıklarına açık tuttukları, yüzde 11,2'sinin paylaşım yaparken kişi listeleri üzerinden sınırlamalar yaptıkları ve yüzde 11,2'sinin de profillerinde hiçbir kişisel bilgiye yer vermedikleri bulgularına ulaşılr (Gökalier & Saatçioğlu, 2020, ss. 149, 152). Araştırmacılar, Westin'in üç mahremiyet yaklaşımı türünü göz önünde bulundurarak katılımcılara gizlilik ile ilgili tutumlarının hangi türde yer aldığını sorarlar. Daha önce bahsedildiği gibi Westin (2003, s. 445), (1) mahremiyet köktencileri/tutucuları (*privacy fundamentalist*), (2) mahremiyet faydacıları (*privacy pragmatist*) ve (3) mahremiyet kaygısızları/umursamazları (*privacy unconcerned*) şeklinde üç mahremiyet yaklaşımı kategorisi tanımlar. Katılımcıların yüzde 55,5'i kendisini faydacı, yüzde 11,2'si de tutucu olarak nitelendirir. Dört katılımcı da düşüncelerinin tutucu kategorisinde yer aldığını ancak davranış olarak faydacı ve umursamaz olarak nitelendirilebileceklerini söylerler. Bunu da gizlilik sorunlarına rağmen sosyal medyayı kullanmaya devam etmelerine bağlarlar (Gökalier & Saatçioğlu, 2020, s. 155).

Khan ve arkadaşları (2020), 5G mobil iletişim ağ teknolojilerini güvenlik ve mahremiyet açısından ele aldıkları çalışmalarında, bu teknolojilerin yarattığı risklerle birlikte potansiyel çözümleri de ortaya koymaya çalışır. Çalışmada, 5G ağının sunduğu akıllı servislerin kullanıcılar açısından yarattığı mahremiyet meselelerine odaklanılır. Araştırmacılar, kullanıcı perspektifinden üç farklı mahremiyet kategorisi tanımlarlar: (1) veri mahremiyeti (*data privacy*), (2) konum mahremiyeti (*location privacy*) ve (3) kimlik mahremiyeti (*identity privacy*). Veri mahremiyeti, 5G ağlarının yüksek çözünürlüklü akış

(*high resolution streaming*) ve akıllı ölçüm (*smart metering*) gibi akıllı ve veri-yoğun (*data-intensive*) hizmetleri sağlamak için topladığı ve işlediği kişisel verilere ilişkindir. Konum mahremiyeti, 5G ağları üzerindeki çoğu cihazın, her yerde bulunan konum tabanlı servislere (*location based services*) bağlı durumda olması nedeniyle oluşan mahremiyet sorununu gündeme getirir. Kimlik mahremiyeti ise, kişinin kimliğine ilişkin, onu tanımlayan bilgilerin, çeşitli siber saldırılara karşı korunmasıdır (Khan vd., 2020, s. 32). Araştırmacılar; 5G ağları üzerinde kullanıcılar, cihazlar, uygulamalar ve makineler tarafından üretilen verilerin sınırlar ötesi de dahil olmak üzere birçok farklı amaç için toplanabileceğini, depolanabileceğini, analiz edilebileceğini, işlenebileceğini ve birleştirilebileceğini vurgularlar ve bu ağlarda mahremiyetin en önemli sorunlardan biri olacağını söylerler. Araştırmacıların bu soruna yönelik önerileri ise teknolojilerin tasarımı aşamasında mahremiyetin göz önünde tutulmasıdır (Khan vd., 2020, s. 40). Aynı araştırma ekibi tarafından sunulan bir bildiride ise uçtan uca veri gizliliği, sorumluluk belirsizliği/veri sahipliği, paylaşılan ortam, görünürlük, sınır ötesi veri akışı, hacklenme, üçüncü şahıslar için veri sağlama ve nesnelerin interneti (*IoT*), 5G kaynaklı mahremiyet tehditleri olarak belirtilir (Liyanage vd., 2018, s. 199).

Teknolojilerin tasarımı aşamasında mahremiyetin de göz önünde bulundurulması, son yirmi beş yıl içerisinde çeşitli araştırmacılar tarafından farklı makalelerde önerilmektedir (bkz. Fischer-Hübner, 1998; Liyanage vd., 2018). Ancak, internet teknolojilerinin bugünkü durumu, bu önerinin önemini artırmış ve yasa yapıcılar da konu ile ilgili yaptıkları yasal düzenlemelerde bu kriteri göz önünde bulundurmaya başlamıştır. Tasarım gereği mahremiyet (*privacy by design*) ve tasarım gereği güvenlik (*security by design*) bu yaklaşımları açıklamak için kullanılan kavramlardır. Haber ve Tamò-Larrieux çalışmalarında, bu yaklaşımların AB ve İsrail'deki düzenlemelerdeki etkisini araştırır. Araştırmacılar, Avrupa Birliği'nin Genel Veri Koruma Yönetmeliği'ni (*GDPR: General Data Protection Regulation*) İsrail'deki düzenlemelere nazaran daha katı olduğunu ve tasarım gereği mahremiyetin GDPR içerisine kodlandığını söylerler. AB'deki düzenlemelerde, tasarım gereği güvenlik kavramının kullanılmadığını ekleyen araştırmacılar, İsrail'deki Veri Güvenliği Yönetmeliği'nde (*Data Security Regulations*) bu tasarım gereği güvenlik anlayışının izlerinin sürülebileceğini ifade ederler. Araştırmacılar, AB'deki yaklaşımı daha ilkesel, İsrail'dekinin ise daha organizasyonel ve geliştirici dostu olduğunu eklerler ve hangi yaklaşımın daha doğru olacağını anlamak için

farklı arařtırmaların yrtlmesi gerektiđini nerirler (Haber & Tam-Larrieux, 2020, ss. 8-9).

2020 yılı, kresel apta bir salgını da beraberinde getirmiř ve koronavirsn yeni bir formunun (SARS-CoV-2) sebep olduđu ve Covid-19 olarak adlandırılan hastalık; mahremiyet, gvenlik ve toplum sađlıđı ile ilgili yeni tartıřmalar bařlatmıřtır. 2007 yılında hazırlanan bir raporda, ulusal sınırların dıřından kaynaklanan salgınları nlemek iin halk sađlıđı aısından mevcut seenekler sınırlı olduđu belirtilmiř ve havayolu trafiđinin hacmine vurgu yapılarak ciddi ekonomik sonular olmadan bu trafiđin azaltılamayacađına deđinilmiřtir. nerilen tek seenek ise diđer lkelerdeki salgınları yakından izlemek ve hastalık tařıyıcısı olanların kendi ulusal sınırlarını gemesini nlemeye alıřmaktır (Waldo vd., 2007, s. 38). Mevcut salgın srecinde neredeyse tm lkeler, bu ciddi ekonomik sonuları ikinci planda tutarak havayolu trafiklerini tamamen durdurmuř ve hastalıđın yayılmasını engellemek iin mobil teknolojilerin mmkn kıldıđı takip ve gzetim olanakları kullanmaya bařlamıřlardır. Avrupa Birliđi'ndeki (AB) ulusal hkmetler, virsn yayılması ve riskleri hakkında bilgi toplamak iin yaygın gzetim ve temas takibine (*contact tracing*)¹⁹ ynelmiřlerdir (van Kolfshootten & de Ruijter, 2020). Apple ve Google da yerel halk sađlıđı yetkililerinin, potansiyel maruziyetleri Bluetooth teknolojisi yardımıyla tespit etmesini ve maruz kalan bireyleri uyarmasını sađlayan maruziyet bildirim sistemlerini (*Exposure Notifications System*) hizmete sunmuřlardır (Gerke vd., 2020, s. 1176). Bu uygulamaların Trkiye'deki karřılıđını, Sađlık Bakanlıđı tarafından geliřtirilen ‘‘Hayat Eve Sıđar’’ (*Life Fits into Home*) uygulaması oluřturmaktadır. Uygulama hem Bluetooth teknolojisi ile kullanıcısına hem de GPS teknolojisi ile bakanlıđa vatandařların virs bulařma riskinin yksek olduđu ortamlarda bulunup bulunmadıđı ya da virsl birisi ile temas edip etmediđine dair bilgi sađlar. Yine bu uygulama ierisinde geliřtirilen ve uygulamanın bař harfleri ile isimlendirilen HES kodunun, řehirlerarası seyahat ve kamu kurum ve kuruluřlarında iřlem yapabilmek iin zorunlu olarak alınması gerekmektedir. Kamu kurum ve kuruluřlarında alıřan personel de bu kodu alıp alıřtıkları birimdeki yetkilendirilmiř personele bildirmekle ykmldrlar. Bu kodun, enformasyonel

¹⁹ Temas takibi, ya da temaslı takibi (*contact tracing*), sađlıđına ciddi bir tehdit oluřturabilecek bir patojene maruz kalmıř, hastalıđı tařıyan ya da tařıma potansiyeli olan bireylerin ve onların temas kurduđu diđerlerinin takip edilmesidir (van Kolfshootten & de Ruijter, 2020, s. 2).

mahremiyet ve hasta mahremiyeti açısından ciddi sorunlar yaratabileceği iddia edilebilir, ancak bu ihlalin arkasında geçerli bir sebep olarak toplum sağlığını korumak vardır. Yine de bu uygulamaların, hükümetlere büyük bir gözetim yetkisi verdiği; kişilerin sağlık cinsiyet, yaş, dil, din, ırk, etkin köken, göçmenlik statüsü veya engellilik gibi kişiler için hassas olabilecek verilerin işlenmesini mümkün kıldığı için toplumda önyargı ve ayrımcılık yaratma riski oluşturabileceği ifade edilmektedir (Çayır, 2020).

Avrupa Birliği üyesi ülkelerin çoğunda, mahremiyet hakkını koruyan tüm yasal düzenlemelerine rağmen, kamu sağlığını korumak, mahremiyet hakkını korumaktan daha ağır basmıştır. van Kolschooten ve de Ruijter (2020, s. 2), mevcut salgının, mahremiyetin mutlak bir hak olmadığını ve sağlık güvenliği tehditlerinin bulunduğu koşullarda sınırlandırılabilirliğini örneklediğini söyler. Araştırmacılar, bu sınırlandırmaların yasal arka planını değerlendirdikleri çalışmalarında, mahremiyet uzmanlarının en büyük çekincesinin, salgın sürecinde yaratılan gelişmiş teknolojik olanakların, salgın bittikten sonra da kullanılmaya devam edileceği yönünde olduğunu ve bu argümanı 11 Eylül saldırıları sonrasında yaşanan sürece dayandırdıklarını belirtirler. van Kolschooten ve de Ruijter (2020, s. 11), temas takibi için veri toplayan ve diğer AB ülkeleri ile paylaşan üye ülkelerin, mahremiyet hakkının sınırlandırılmasının, kamu sağlığını koruma amacı ile orantılı tutması gerektiğini, ancak böyle yeni bulaşıcı hastalıklar söz konusuysa ulusal sağlık otoritelerinin bu oranı korumasının kolay olmadığını vurgularlar ve üye ülkelerin kamu sağlığı gözetimi ve temaslı takibi konularındaki sorumluluklarının daha açık bir şekilde tanımlanmasını önerirler.

1.1.4.2. Çevrim İçi Mahremiyet ile İlgili Çalışmaların Genel Değerlendirmesi

İnternetin, son kullanıcıların içerik üretimine imkân vermesiyle, literatürde sıkça kullanılan şekilde ifade edilirse, Web 2.0 çağının başlaması ile gelişen sosyal medya ve sosyal ağ siteleri, platformları, uygulamaları ortaya çıkmış ve bireylerin bu mecralar dolayımı ile etkileşim kurması mümkün hale gelmiştir. İnternet üzerindeki enformasyon, artık sadece “tüketilmemekte” aynı zamanda onu tüketen kullanıcılar tarafından “üretilmektedir.” Son kullanıcılar tarafından gerçekleştirilen bu enformasyon üretiminin azımsanamayacak bir kısmını kişisel bilgiler oluşturmaktadır. Ağ toplumunun bir parçası haline gelen birey için bir ritüele dönüşen sosyal ağ sitesi kullanımı pratiğinin yarattığı ya da yaratabileceği potansiyel mahremiyet riskleri ve bireylerin bu riskler karşısındaki tutum ve endişeleri, bu mecraların ilk ortaya çıktığı dönemden bu yana iletişim

alıřmaları alanında nemli bir arařtırma alanı olmuřtur. Bu alana yapılan ve yukarıda bir kısmı paylařılan arařtırmalar, kullanıcıların mahremiyet anlayıřlarında, kiřisel bilgilerini paylařma pratiklerinde ve bilgisayar dolayımı ile iletiřim kurma pratiklerinde yařanan deęiřimi ortaya koymaktadır.

Arařtırma sorununu evrim ii mahremiyetin oluřturduęu alıřmalar incelendięinde, zellikle yirmi birinci yzyılın bařında yapılan arařtırmaların, aę toplumuna katılanların byk oęunluęunun mahremiyet endiřeleri tařıdıklarını gsterdięi sylenebilir (akt. Buchanan vd., 2007). Bu noktada, 2001 yılında gerekleřtirilen bir arařtırmaya dayanan ıktıların, internet kullanıcılarının yzde 80’den fazlasının “fazla kiřisel ya da gereksiz olduęunu hissettięi iin bir internet sitesine bilgi vermeyi reddettięi” ve “bir internet sitesinden kendi adlarının ya da adreslerinin pazarlama amalı listelerden silinmesini istedięi” (Milne & Culnan, 2004) hatırlanabilir. O dnemde kullanıcılar iin ok yeni bir mecra olan internete ynelik geliřen bu endiřelerin, doęal bir alıřma srecinin parası olduęu sylenebilir.

Facebook’un nclk ettięi sosyal aę sitelerinin yaygınlařması, ncelikle niversite ęrencileri, daha sonra da tm internet kullanıcıları iin alternatif bir sosyalleřme pratięi oluřturmuřtur. Sosyal aęlar aracılıęı ile sosyalleřebilmek, bu aę sitelerinde bireyi temsil edecek benlik sunumlarının (profillerin) oluřturulmasını gerektirir. Kullanıcılar, kiřisel verilerini paylařarak sosyal aę sitelerindeki kimliklerini aktif bir řekilde inřa ederler (Boyd, 2008). Literatrdeki arařtırmalar deęerlendirildięinde, sosyalleřebilmek iin kiřisel bilgi ifřasının nkořul olduęu sosyal aę sitelerinin yaygınlařmasının, kullanıcıların mahremiyet endiřelerini azaltmadıęı, ancak azımsanamayacak miktarda kiřisel bilginin de bu endiřelere raęmen paylařıldıęı sylenebilir. Kullanıcıların, mevcut mahremiyet endiřelerine raęmen, sosyal aę sitelerinde etkileřim kurabilmek iin kiřisel bilgilerini paylařıyor oluřları, mahremiyet paradoksu ya da mahremiyet ikilemi kavramları ile aıklanır (Barnes, 2006; Norberg vd., 2007; Brandtzæg vd., 2010).

Mahremiyet ikilemi ve/veya mahremiyet paradoksu karřısında kullanıcıların elde edecekleri hizmet ya da sonu ile (rneęin sosyalleřme, kimlik oluřturma, poplerleřme, tanınma vb.) kendi mahremiyetlerini “takas ettikleri” sylenebilir. Takas (*trade-off*) modeline dayanan bu deęerlendirmenin, mahremiyet ve gvenlik arasındaki iliřkiyi

açıklamakta yetersiz kaldığını ifade eden araştırmalar olsa da (Strauß, 2015, ss. 27-30), tüm endişelerine rağmen sosyal ağ sitelerinde kişisel bilgilerini ifşa eden bireylerin davranışlarını açıklamak için başvurulabilecek bir modeldir. Literatürdeki araştırmaların çoğu, mahremiyet ile ilgili görüşler ile davranışlar arasındaki bir tutarsızlık olduğunu göstermektedir.

Baruh, Secinti ve Cemalcılar'ın (2017), çevrim içi mahremiyet endişeleri ve mahremiyet yönetimi alanındaki literatür üzerinde gerçekleştirdikleri meta-analiz, hem literatürdeki araştırmaları değerlendirmek hem de mahremiyet görüş ve davranışları arasındaki tutarsızlığı (mahremiyet paradoksu) sorgulamak için önemli bir başvuru kaynağıdır. Araştırma için EBSCOHOST, ScienceDirect ve SCOPUS veri tabanlarında “mahremiyet endişesi, mahremiyet bilgisi ve koruyucu davranış” (*privacy concern, privacy knowledge, and protective behavior*) anahtar kelimeleri ile yapılan aramalar sonucunda elde edilen İngilizce dilindeki, 166 araştırma makalesi ve konferans bildirisi analiz edilmiştir. Tüm araştırmalardaki toplam katılımcı sayısı 75 binin üzerindedir ve bu geniş örneklem 34 farklı ülkenin vatandaşlarından oluşmaktadır. Yapılan meta-analiz sonucu elde edilen bulgular, “mahremiyet paradoksu” kavramının önerdiğinin aksine mahremiyet endişelerinin bireylerin çevrim içi hizmetleri ne ölçüde kullandığını ve mahremiyet yönetimine ne ölçüde dahil olduğunu öngörebildiğini gösterir. Paradoks sadece sosyal ağ kullanımları ile mahremiyet endişeleri arasında geçerliliğini korur. Araştırmacılar, sosyal ağ sitesi kullanımı ile mahremiyet endişesi arasındaki bu tutarsızlığın olası nedeninin Petronio'nun İMY (CPM) teorisi ile açıklanabileceğini söylerler. İMY teorisine göre bireyler mahremiyet sınırlarını yönettikleri kuralları kendi motivasyonlarından ve risk-fayda analizlerinden etkilenir. Meta-analizde, kültürel ve yasal sistem farklılıkları, cinsiyet ve veri toplama şekli potansiyel ılımlı etki faktörleri olarak değerlendirilir. Hofstede'nin kültür boyutlarından olan hoşgörü/kısıtlama (*indulgence/restraint*) yönelimi ile mahremiyeti koruma yasalarının belirgin ılımlı etkisi yoktur. Cinsiyet ile ilgili olarak ise, örnekleminin çoğunluğu kadınlardan oluşan çalışmalarda, mahremiyet endişelerinin çevrim içi hizmetleri kullanma niyetleri ile sosyal ağ sitelerini kullanma davranışlarında güçlü bir negatif etkisi olduğu söylenebilir. Araştırmacılar, analiz sonuçlarına dayanarak kadınların mahremiyet okuryazarlığı açısından dezavantajlı olsalar bile, mahremiyetlerini korumak için harekete geçme ihtimallerinin erkeklere göre daha yüksek olduğunu söylerler (Baruh vd., 2017, s. 49).

Toparlamak gerekirse, çevrim içi mahremiyet konusunu inceleyen araştırmaların oluşturduğu literatürde, birbirini destekleyen ve tekrar eden bazı sonuçlardan bahsedilebilir. Bunlardan ilki gençlerin yaşlılara göre daha fazla kişisel bilgiyi sosyal ağlarda paylaştığı ve yaşlıların gençlere göre daha fazla mahremiyet endişesi taşıdıklarıdır. Benzer şekilde mahremiyet endişesi ve kişisel bilgi paylaşımı açısından kadınların erkeklere oranla daha temkinli davrandıkları gözlemlenmektedir.

1.1.5. Mahremiyet ile İlgili Hukuki Düzenlemeler

Bir insan hakkı olarak mahremiyet hem ulusal hem de küresel ölçekteki hukuk metinlerinde tanımlanmış ve kapsamı ortaya koyulmuştur. Mahremiyetin hukuki boyutunu tartışan ilk akademik yayın olduğu düşünülen ,1890 tarihli *The Right to Privacy* adlı makalede mahremiyet, “yalnız bırakılma hakkı” olarak tanımlanır ve dönemin gazetelerinin ve gazetecilerinin bireylerin gündelik hayatlarına ilişkin ifşalarını sorunsallaştırır. Aradan geçen yaklaşık yüz otuz yılın ardından, bireylerin mahremiyetinin karşısındaki tehlike, o dönemin gazeteleri ve gazetecilerinden daha büyüktür. Gelişen ve yaygınlaşan enformasyon ve iletişim teknolojileri, bu ifşaların herkes tarafından kolayca yapılmasını sağlamıştır. Yeni teknolojiler, yukarıda tartışıldığı gibi, bireylerin çeşitli sebeplerle mahremiyet haklarından feragat etmesini ve risk-fayda hesaplamaları yaparak kendi kişisel bilgilerini açık etmesini de beraberinde getirmiştir. Her ne kadar bireyle kendi rızaları ile mahremiyetlerinden vazgeçiyor olsalar da hem bu vazgeçişin henüz farkında olmadıkları sonuçları hem de mahremiyetlerinin üçüncü taraflar tarafından işgal edilmesi ihtimali nedeniyle mahremiyetin hukuki zeminde korunması, demokratik ve modern bir toplum için oldukça önemlidir.

Mahremiyetin ve kişisel veri güvenliğinin hukuki zemine oturtulması ve hukuken korunması konusunda, Avrupa Birliği’nin gerek insan hakları sözleşmeleri gerekse çıkardığı direktifler ve yasalarla diğer ülkelere öncülük ettiği söylenebilir. Avrupa Birliği, hem insan hakları sözleşmesi hem 1995 tarihli Veri Koruma Direktifi (*Directive 95/46/EC*) hem de yakın dönemde yürürlüğe soktuğu Genel Veri Koruma Yönetmeliği (*GDPR*) ile birlik vatandaşlarının kişisel verilerini korumayı hedefler. Ancak, AB’nin bu korumacı tutumu her ülkede görülmemektedir. Örneğin, Amerika Birleşik Devletleri’nde veri güvenliği ya da mahremiyet konularını kapsayan tek bir yasa yoktur. Bunun yerine, özellikle veri koruma kavramıyla ilgilenen bir dizi kanun ve icra emri vardır. Stratford ve Stratford’a (1999, s. 17) göre bu yasaların en önemlileri 1974’te yürürlüğe giren

Mahremiyet Yasası (*Privacy Act*) ve Bilgisayar Eşleştirme ve Mahremiyet Yasası'dır (*Computer Matching and Privacy Act*). Aşağıda hem uluslararası ölçekteki hem de Türkiye'deki mahremiyet hakkını tanımlayan sözleşmelere ve yasal düzenlemelere değinilmiştir.

1.1.5.1. Uluslararası Hukuki Düzenlemeler

Hukuk alanında mahremiyet önemli ancak yanıltıcı bir konsepttir (Stratford & Stratford, 1999, s. 17). Uluslararası hukukta mahremiyet hakkına ilk olarak İnsan Hakları Evrensel Bildirisi'nde yer verilmiştir. Bildirinin 12. maddesine göre; “Hiç kimsenin özel yaşamına, ailesine, konutuna ve haberleşmesine keyfi olarak karışamaz, onur ve ününe saldırılamaz” ve “Herkesin bu tür karışma ve saldırılara karşı yasal korunma hakkı vardır (Aybay, 2006).” Doğrudan hukuki yaptırım taşımayan bildiriye paralel olarak, 1950 yılında kabul edilen Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesi özel ve aile hayatına saygı hakkını tanımlar:

- 1. Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir.*
- 2. Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir (Council of the European Union, 2010).*

Maddenin ikinci bendi, mahremiyet hakkının ne zaman ve hangi durumlarda kısıtlanabileceğini göstermektedir. Özellikle 11 Eylül saldırıları sonrasında, kamu güvenliği ve Covid-19 salgınında ise kamu sağlığı için alınan önlemler ve yapılan düzenlemeler, sözleşmede belirlenen istisnaların uygulama alanlarına bir örnektir.

1966 yılında kabul edilen Siyasi ve Medeni Haklar Uluslararası Sözleşmesi'nin 17. maddesi de İHEB'e benzer hükümler ile mahremiyet hakkını güvenceye almaktadır (United Nations Human Rights, 1966). 2012 yılında kabul edilen Avrupa Birliği Temel Haklar Bildirgesi'nin 7. Maddesi, daha önceki metinlerde olduğu gibi özel ve aile yaşamına saygıyı tanımlarken 8. madde “Kişisel bilgilerin korunması” başlığını taşır:

1. Herkes, kendisine ilişkin kişisel bilgilerinin korunmasını isteme hakkına sahiptir.
2. Bu tür bilgiler, belirtilen amaçlar için ve ilgili kişinin muvafakatine veya yasada öngörülen başka meşru temele dayalı olarak adil şekilde kullanılmalıdır. Herkes, kendisi hakkında toplanmış olan bilgilere erişme ve bunlarda düzeltme yaptırma hakkına sahiptir.
3. Bu kurallara uyulması, bağımsız bir makam tarafından denetlenecektir (Charter of Fundamental Rights of the European Union, 2012; Avrupa Birliği Türkiye Delegasyonu, 2012).

Avrupa Birliği üye ülkeleri, kişisel verilerin işlenmesine karşı bireyleri korumak için 1981 yılında bir sözleşme imzalamışlardır: Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi (*Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*). Sözleşmenin ardından, 24 Ekim 1995'te kişisel verilerin işlenmesine ilişkin bireylerin korunması ve bu tür verilerin serbest dolaşımı hakkında bir direktif çıkarılmıştır (Directive 95/46/EC of the European Parliament and of the Council, 1995). Direktif, kişisel verilerin korunması için önemli bir araç olarak nitelendirilebilir (European Union, 2010, s. 6). 1995 direktifi, bireylerden toplanan kişisel verilerin işlenmesi ve bireylerin erişim, bildirim ve düzeltme hakları için standartlar tanımlamıştır. Stratford ve Stratford (1999, s. 19), direktifin 25. maddesine dikkat çeker. Çünkü bu madde, kişisel verilerin üçüncü ülkelere aktarılmasını düzenlemektedir. AB içerisindeki devletler veri aktarımını sadece verilerin aktarılacağı ülkenin (üçüncü ülke) yeterli düzeyde veri koruması sağladığını teyit ettikten sonra gerçekleştirebilirler ve bunu belirlemek için de o ülkenin hukukunu dikkate almalıdırlar. Bu madde ile direktif, sadece AB ülkeleri için değil, AB ile ticaret içerisinde olan diğer tüm ülkeler için bağlayıcı bir nitelik kazanır. Direktifin, ülkeler arasındaki ticaret için ciddi etkileri vardır ve Avrupa Birliği içinde ve diğer ülkelerde, mahremiyet yasalarının geliştirilmesinde itici güç olmuştur (Stefanick, 2011, s. 39).

Uluslararası bağlayıcılığı olan AIHS'nin yanı sıra, mahremiyet hakkını düzenleyen bir diğer sözleşme de 22 Kasım 1969 tarihinde imzaya açılan, Amerikan İnsan Hakları Sözleşmesi'dir. Bu sözleşmenin 11. Maddesi, "Mahremiyet Hakkı" (*Right to Privacy*) başlığını taşır ve diğer uluslararası sözleşmelerle benzer ifadeler içermektedir (American Convention on Human Rights, 1969). Amerika kıtasındaki devletler

tarafından imzalanan bu sözleşme, her ne kadar Avrupa'daki ile benzerlik gösterse de yasal düzenlemeler Avrupa'daki kadar kapsayıcı değildir. Avrupa'da mahremiyetin korunması, hem kamu hem de özel sektörü kapsayan çok amaçlı mevzuat tarafından ele alınırken ABD'deki düzenlemeler, genellikle federal güçlerin bireylerin kişisel verilerine olan erişimi düzenlemekte ve özel sektörü büyük oranda özdenetime yönlendirmektedir (Stratford & Stratford, 1999, s. 19).

Ekonomik Kalkınma ve İş Birliği Örgütü (OECD) tarafından 1980 yılında Mahremiyetin Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Kılavuz kabul edilmiştir. Kılavuzda 8 prensip yer almaktadır (OECD, 2003a, s. 5):

- Veri toplamanın sınırlandırılması (*collection limitation*)
- Veri kalitesi (*data quality*)
- Amacın belirginleştirilmesi (*purpose specification*)
- Sınırlandırmaların yapılması (*use limitation*)
- Güvenlik önlemleri (*security safeguards*)
- Açıklık (*openness*)
- Bireysel katılım (*individual participation*)
- Hesap verebilirlik (*accountability*)

OECD'nin kılavuzu, 2003 yılında gözden geçirilip güncellenmiştir. Güncellenen kılavuz, risk yönetimi ve geliştirilmiş birlikte çalışabilirlik yoluyla mahremiyetin küresel boyutunun ele alınması ihtiyacı temalarını içermektedir. Kılavuzda ayrıca, ulusal mahremiyet stratejilerine ve gizlilik yönetimi programlarına vurgu yapılır. Kılavuzda tanımlanan bir diğer önemli konsept de veri güvenliği ihlali bildirimidir (*data security breach notification*) (OECD, 2003b).

Avrupa Birliği'nin, veri güvenliği konusunda yürürlüğe soktuğu en güncel düzenleme GDPR'dir (*General Data Protection Regulation*). Bu düzenleme, çeşitliliği ve miktarı artan veri trafiği ve bu verilerin işlenmesinde kullanılan teknolojilere ayak uydurma çabasının sonucudur. Bu düzenlemeden önce, yukarıda değinilen 95/46/AT sayılı “Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Direktif”, kişisel verilerin korunması bağlamında, sadece Avrupa ile sınırlı kalmayan bir çerçeve sunmaktaydı. Türkiye'deki mevcut yasal düzenleme olan KVKK da bu direktif çerçevesinde oluşturulmuştur (BT Bilgi Teknolojileri, 2018).

Geniş bir bölgesel kapsama sahip olan GDPR, belirli koşullar altında, AB dışındaki şirketler için dahi bağlayıcı olabilmektedir. Bu düzenlemenin ayrıca, ABD'nin

Kaliforniya eyaletinde 2020 yılında yürürlüğe giren Kaliforniya Tüketici Mahremiyeti Yasası'na (CCPA) da ilham verdiği söylenebilir (Gerke vd., 2020, s. 1180).

1.1.5.2. Türkiye'deki Hukuki Düzenlemeler

Dünyada, kişisel verilerin korunması konusunda, 1970'li yıllardan itibaren ciddi önlemler alınmaya başlanmıştır. Ancak Türkiye'de, bu konudaki tedbir ve çalışmalar (2016 yılına kadar) oldukça sınırlı düzeyde kalmış, gelişen teknoloji ve uygulamalara ayak uyduramamıştır (Yüksel Civelek, 2011, s. 181). 28 Ocak 1981 tarihinde imzaya açılan, "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi" o tarihte Türkiye tarafından imzalanmış olsa da TBMM'de sözleşmedeki ilkeler çerçevesinde bir kanun kabul edilip yasalaşmadığı için yürürlüğe girememiştir (İlkiz, 2013). Türkiye Cumhuriyeti Anayasası'nın 90. maddesine göre, usulüne göre yürürlüğe konulmuş Milletlerarası antlaşmalar, kanun hükmünde kabul edilmektedir (Türkiye Cumhuriyeti Anayasası, 1982). Bu bakımdan yukarıda değinilen İHEB ve AİHS, Türkiye hukuk sistemi içerisine eklenmiştir. Hatta 2004 yılında anayasaya eklenen, "Usulüne göre yürürlüğe konulmuş temel hak ve özgürlüklere ilişkin milletlerarası antlaşmalarla kanunların aynı konuda farklı hükümler içermesi nedeniyle çıkabilecek uyuşmazlıklarda milletlerarası antlaşma hükümleri esas alınır" ibaresi ile bu antlaşmaların, ülkenin hukuk sistemindeki önemi vurgulanmaktadır.

Türkiye Cumhuriyeti Anayasası'nın 21, 22 ve 23. maddeleri sırasıyla; özel hayatın gizliliği, konut dokunulmazlığı ve haberleşme hürriyeti haklarını garanti altına almaktadır. 20. maddede, herkesin, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahip olduğunu ve özel hayatın ve aile hayatının gizliliğine dokunulamayacağı belirtilmiştir. Bu maddeye 2010 yılında yapılan ekleme ile bireylerin kendileriyle ilgili kişisel verilerin korunmasını isteme hakkı da anayasal olarak garanti altına alınmıştır:

Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir (Türkiye Cumhuriyeti Anayasası, 1982).

Türkiye’de, kişisel verilerin korunmasına ilişkin esas ve usulleri belirleyen kanun, hazırlıkları daha önceye dayansa da 2016 yılına kadar kabul edilememiştir. KVKK öncesi, mahremiyet hakkına yönelik oluşan ihlallere uygulanacak yaptırımlar, Türk Ceza Kanunu’nun dokuzuncu bölümü olan, “Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar” içerisinde yer almaktadır. TCK’nin 132-140. maddeleri, haberleşme gizliliğinin ihlali, kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması, özel hayatın gizliliğinin ihlali, kişisel verilerin kaydedilmesi, verilerin hukuka aykırı olarak verilmesi ya da ele geçirilmesi ve verileri yok etmeme suçlarına uygulanacak cezaları belirler (Türk Ceza Kanunu, 2004).

Türkiye’de enformasyonel mahremiyet ve kişisel verilerin güvenliği alanını düzenleyen, 6698 sayılı Kişisel Verilerin Korunması Kanunu, 2016 yılında kabul edilerek yasalaşmıştır. KVKK yasalaşmadan önce, bu alan Türk Ceza Kanunu’nun dokuzuncu bölümündeki maddeler ile düzenlenmekteydi ve “kişisel veri” tanımını içermediği için uygulamada hukuki bir boşluk yaratıyordu (Yüksel Civelek, 2011, s. 185). KVKK’nin, uygulamadaki bu boşluğu kapattığı söylenebilir.

KVKK’nin 4. maddesi kişisel verilerin işlenmesinde (a) hukuka ve dürüstlük kurallarına uygun olma, (b) doğru ve gerektiğinde güncel olma, (c) belirli, açık ve meşru amaçlar için işlenme, (ç) işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ve (d) ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkelerine uyulmasını zorunlu kılar (Yücedağ, 2019). Yasada aynı zamanda, kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği açık bir şekilde belirtilmiştir. Yasanın 5. maddesinin ikinci fıkrası, kişisel verilerin bireyin rızası olmaksızın işlenebileceği durumları listeler. Burada, bireylerin mahremiyet yönelimleri ile ilişkilendirilebilecek bir şart belirtilmiştir. Buna göre, bireyin kendisi tarafından alenileştirilmiş bilgiler, açık rıza olmaksızın işlenebilmektedir (Kişisel Verilerin Korunması Kanunu, 2016). Bu durum, yasal düzenlemeye rağmen bireylerin kendi mahremiyetlerini ve kişisel verilerini korumaları konusunda taşıdıkları sorumluluğun bir göstergesi olarak değerlendirilebilir.

KVKK ile özel nitelikli kişisel veri tanımı da hukuk sistemimize kazandırılmıştır. 6. madde bu tanımı içerir: “Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği,

sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir.” KVKK, 18. maddede tanımlanan kabahatler için idari para cezası yaptırımını uygularken, diğer suçlar için TCK’nin 135, 138 ve 140. maddelerine gönderme yapmıştır.

Teknoloji, yirminci yüzyıl boyunca gözlemlendiği gibi, sürekli olarak regülasyon süreçlerinden daha hızlı ilerlemektedir. Türkiye’deki özel televizyon yayıncılığının başlangıcı ve geciken yasal düzenlemeler bu durumun en açık örneklerinden biridir. Enformasyon ve iletişim teknolojilerindeki gelişmeler, oldukça büyük miktarda verinin toplanmasını, işlenmesini ve paylaşılmasını olanaklı hale getirmiştir. Böyle bir sistem içerisinde bireylerin mahremiyetlerini korumak ve sürekli bir çabayı gerekli kılmaktadır. KVKK da bu çabanın Türkiye’deki en güncel sonucudur. Ancak sadece yasal düzenlemeler, kişisel verilerin korunması için yeterli olmamakta, bireysel bilinçlenme ve farkındalık kazanma da kişisel verilerin ve enformasyonel mahremiyetin korunması için önem taşımaktadır.

1.2. Gözetim Toplumu

Yirmi birinci yüzyılda bir norm haline gelen gözetim, çeşitli formlar içerisinde gerçekleşmektedir: Kameralar, parkta yürüyüş yapanları ya da içki satışı yapılan bir markette alışveriş yapan insanları kaydeder; GPS (*Global Positioning System*) alıcıları anne-babalara, çocuklarının arabalarını nereye götürdüğünü gösterir; kimi yazılımlar, insanların sosyal ağ siteleri için ürettikleri bilgileri toplar ve işverenlerin incelemesine sunar; şirketler müşterileri ile yaptıkları telefon görüşmelerini “kalite güvencesi için” kaydeder ve ürünlere yerleştirilmiş etiketler hem şirketlerin hem de tüketicilerin sevkiyat halindeki ürünün hareketlerinin izlenmesini sağlar (Stefanick, 2011, s. 125). Mevcut teknolojik gelişmelerin sunduğu bu imkanlar, gözetimin günümüzde alabileceği şekiller ile ilgili genel bir fikir verebilir. Bu başlıkta, gözetim ve gözetim toplumu kavramları olabildiğince kısa bir şekilde ele alınmış ve gözetim olgusu incelenirken sıklıkla atıfta bulunulan “panoptikon” kavramının, yirmi birinci yüzyıl dijital teknolojilerinin sağladığı gözetim olanaklarını açıklamakta ne kadar yeterli olduğu ya da yetersiz kaldığı değerlendirilmiştir.

Türkçede “birine veya bir şeye gizlice bakmak, dikizlemek ve birinin yaptıklarını belli etmeden izlemek” anlamlarını barındıran gözetlemek, (Türk Dil Kurumu, 2011, s.

985) Lyon’a (2013, s. 14) göre, insan toplumunun temelinde yer alan bir pratiktir. İşlevsel olarak gözetim, “belli bir toplumun hem içinde hem de dışında çevrede olup biten olaylarla ilgili bilginin toplanmasını ve dağıtımını dile getiren iletişimsel bir işlev” olarak nitelendirilebilir (Mutlu, 2004, s. 117). İletişimsel bir işlev olmasının ötesinde gözetimi; “etiketleme, yönetme, koruma, yönlendirme gibi amaçlarla kişisel enformasyona dönük odaklı, sistemli ve düzenli ilgi (Lyon, 2013, s. 31)” şeklinde tanımlamak mümkündür.

Marx, Oxford sözlüğünde gözetimin, “özellikle şüpheli bir kişinin yakın gözlemi” şeklinde tanımlandığını, ancak artık gözetimin sadece şüpheli kişilere yönelik olmadığını ve bu tanımın mevcut gözetimi kapsamakta yetersiz kaldığını söyler. Marx’a göre (2004, s. 20); yeni gözetim, “kişisel verilerin çıkarılması veya oluşturulması için teknik araçların kullanılması” şeklinde tanımlanabilir.

Lyon, Giddens’a atıfta bulunarak gündelik gözetimin modern toplumlara özgü bir “hastalık” olduğunu ve gözetimin moderniteyi oluşturan temel toplumsal süreçlerden biri olduğunu söyler (Giddens’tan akt. Lyon, 2013). Gözetimi, disiplin toplumunun oluşturulmasındaki önemi üzerinden ele alan Foucault da Giddens’ın argümanına paralel olarak özgürlükleri keşfeden Aydınlanma Çağı’nın, disiplinleri de keşfettiğini vurgular (Foucault, 1992, s. 279). Modernitenin belirsizliği fethetme vaadi ile düzensizliğin dışlanması, verimliliğin artırılması düşüncelerinin (Bauman, 2014), bu ideallere ulaşmak için gereken araçları da beraberinde getirdiği söylenebilir. Bu bakış açısıyla, dijital ya da elektronik gözetimin, modernite ideallerinin beraberinde getirdiği araçlar olduğu düşünülebilir.

Nebeker ve Tatum (1993, s. 509), elektronik izlemeyi (*electronic monitoring*), bireysel veya grup eylemlerini veya performanslarını toplamak, depolamak, analiz etmek ve raporlamak için; ses, video ve bilgisayar sistemleri gibi elektronik aletlerin veya cihazların kullanımı olarak tanımlar. Araştırmacıların bu tanımlaması, modernite hedefleri ile ilişkilendirilebilir. Ancak burada izleme ve gözetim (*monitoring and surveillance*) gibi sıklıkla birbiri yerine kullanılabilen iki kavram arasındaki ince ayrımı belirginleştirmek gereklidir. İzleme terimi, gözetime kıyasla daha genel bir anlama sahiptir ve işyeri ile ilgili tüm otomatik enformasyon toplama işlemlerini, amaçlarına bakılmaksızın kapsar. Buradaki amaçlar, çalışanların ikramiyesini belirlemek veya envanteri takip etmek olabilir. Gözetim ise daha dar bir anlama sahiptir ve bir otorite ile

davranışlarını kontrol etmek istediği kişiler arasındaki ilişkiyi ifade eder. İki kavram arasındaki ilişki ve ayrımı ortaya koymak için, izlemenin gözetimde kullanılan bilgileri ürettiği ve tüm gözetimlerin izlemeyi içerdiği söylenebilir. Ancak tüm izlemeler gözetim için kullanılmaz (Botan, 1996, ss. 294-295).

Bauman'a göre gözetim teknolojileri, günümüzde iki karşıt stratejik amaca hizmet etmekte, iki farklı cephede gelişmektedir: hapsetmek ya da dışarıda bırakmak (Bauman & Lyon, 2013, s. 69). Bu yaklaşıma göre gözetim, hem içeride bulunanların denetlenmesini ve kontrol edilmesini sağlar, hem de içeride olanları dışarıdaki "ötekilerden" korur. Lyon da *Gözetim Çalışmaları* adlı kitabında, beş farklı gözetim alanı olduğunu altını çizer ve bu alanları şu şekilde sıralar: (1) askeri gözetim, (2) idari gözetim, (3) işçi gözetimi, (4) polis gözetimi ve (5) pazarlama gözetimi. Bu gözetim alanları içerisinde özellikle, kişisel verilerin yaygın sistemli ve rutin bir şekilde işleniyor olması, gözetim toplumundan söz etmeyi mümkün kılar (Lyon, 2013).

Gözetim, eski bir sosyal süreçtir ve kurumsal rutinlerin ve insan sosyalliğinin bir bileşeni olduğu söylenebilir. Geç modernitenin, baskın örgütlenme pratiği olarak ortaya çıkışı ise son 40 yıl içerisinde gerçekleşmiştir (Ball vd., 2012). Bu örgütlenme biçiminin oluşturduğu toplum yapısını açıklamak için, gözetim toplumu kavramı kullanılabilir. Kavram, ilk olarak 1985 yılında sosyolog Gary T. Marx tarafından ortaya atılmıştır. Marx'a göre (1985), dönemin (1980'li yıllar kastediliyor) gözetim teknolojileri; fiziksel, sosyal ve kişisel alanlarda derinlere inebilir, fısıltıları duyabilir ve duvarları, pencereleri, bulutları ve karanlığı delebilir. Bu teknolojiler aynı zamanda, daha geniş alanları da kapsar. Marx'ın ifadesiyle; önceden birbirine bağlanmayan gözetim iplikleri artık devasa bilgi duvar halılarına dokunmaktadır. Gözetim teknolojilerindeki tüm bu gelişmeler neticesinde gözetim, artık sadece birkaç şüpheliye yönelik değildir ve Marx'a göre bu teknolojiler herkesin gözetimin hedefine dönüştüğü bir toplum yaratır. Toplumdaki tüm insanların gözetimin birer nesnesi haline gelmesi, gözetim toplumunu mümkün kılar. Marx'a göre, daha öncesinde sadece bilimkurgu yazarlarının distopik hayallerinde var olan kontrol ve gözetim teknolojilerinin (ısı, ışık, hareket, ses ve koku sensörleri, gece görüş gözlüğü, elektronik etiketleme, biyometrik erişim cihazları, ilaç testi, DNA analizi vb.) kullanılabilir hale gelmesi, bizi bir gözetim toplumu yapmaktadır (Marx, 2004).

Enformasyon ve iletişim teknolojileri, gözetimin yakın dönem tarihi ile çok yakından bağlantılıdır (Bruno, 2012). Lyon da bu teknolojiler ile gözetim toplumu arasındaki ilişkiye değinir ve yönetilme ve kontrol işlevleri için, enformasyon ve iletişim teknolojilerine bağımlı olan bütün toplumların, gözetim toplumu olduğunu söyler. Bu gözetlemenin etkileri, daha önce tarihte hiç görülmemiş bir biçimde, günlük hayatta fazlasıyla hissedilmektedir (Lyon, 2006, s. 11).

Yirminci yüzyılın sonunda ve yeni yüzyılın başında bu teknolojilerde yaşanan ilerlemeler, gözetim yöntemlerinin sayısını, kapasitesini ve yoğunluğunu artmıştır. İnternet gözetimi ya da Fuchs'un ifade ettiği gibi, Web 2.0 gözetimi de bu yeni yöntemlerden biridir. Fuchs (2011), Google veya Facebook gibi çağdaş web platformlarının, büyük miktarda kişisel veri ve kullanıcı davranışı bilgilerini depoladığı, işlediğini, analiz ettiğini ve sattığını hatırlatarak Web 2.0 gözetimi çalışmalarının önemine vurgu yapar. Fuchs, bu gözetimin, neden problematik ve zararlı olduğuna ilişkin olarak kullanım koşullarının ve gizlilik politikalarının karmaşıklığı, kullanıcıların internet becerilerindeki farklılıklar ve dijital eşitsizlik, internetin ticarileşmesi, pazar yoğunlaşması ve ihtiyaçların manipülasyonu, seçme özgürlüğünü sınırlayan reklam uygulamaları ve çevrim içi gözetimin görünmezliği gibi konulara dikkat çeker. Haggerty ve ekip arkadaşlarının gözetim asamblesi (*surveillant assemblage*) olarak ifade ettikleri gözetim uygulamaları, 'ortadan kaybolmanın ortadan kaybolmasına' neden olur. Başka bir ifadeyle, bireylerin anonimliklerini korumaları ya da sosyal kurumların gözetiminden kaçmaları giderek daha zorlaşır (D. Haggerty, Richard V. Ericson, 2000). O'Harrow'un (2005, s. 10) ifadesiyle gözetim yöntemleri çok daha güçlü, çeşitli ve sofistike hale gelmiştir ve sadece teröristler ya da suçlular için değil tüm toplum için "saklanacak hiçbir yer yoktur."

McGrath (2012) çalışmasında, 2010'lu yıllarla birlikte, "mümkün olan en fazla sayıda insanın ruh halimizi, nerede olduğumuzu, fikirlerimizi, planlarımızı ve hatta ahiretle olan ilişkimizi bilmesini sağlamanın çoğumuz için sosyal bir gereklilik haline geldiği bir dünyaya" girdiğimizi söyler. McGrath'a göre, bilgi almak yerine ağ oluşturma ve etkileşime dayanan Web 2.0'ın geliştirilmesiyle, bireylerin çevrim içi olarak paylaştığı bilgi miktarı artmış ve devlet kayıtları ya da kredi bilgileri gibi basit veriler yerini, sürekli güncellenen anlatılara, görüntülere ve duygusal içeriğe bırakmıştır. Bireylerin bu paylaşımları yapmaya zorlanmadıkları ya da mecbur bırakılmadıkları söylenebilir. Bu da

Lyon’ın ifade ettiđi, gözetimin sadece gözetleyenlerin imtiyazlı olduđu bir güç ilişkisi olmadığını, aynı zamanda “gözetlenenin” de rol oynadıđı bir “katılım” olduđu savını destekler niteliktedir (Lyon, 2013, s. 33). Bauman ise bu katılımı, “gözetlenenlerin sessiz ya da gürültülü, bilinçli ya da bilinçsiz, maksatlı ya da olağan ama hiç şüphesiz muazzam ölçekteki işbirliđi” şeklinde ifade eder (Bauman & Lyon, 2013, s. 129). Bu çalışmanın, mahremiyet ile kimlik oluşturma ve sosyalleşme arasındaki ilişkiyi inceleyen kısmı da “katılım” tezine vurgu yapar.

“Bilgi altyapıları ve veri tabanlı ekonomilerin kurulduđu her yerde gözetleme uygulamaları hızla artan bir oranda büyümektedir (Lyon, 2006, s. 18).” Tekrar edilecek olursa, Lyon’a göre, bilgi toplumu (ya da enformasyon toplumu) olarak adlandırılan bütün toplumların doğasından gelen bir özelliđi de benzer şekilde gözetim toplumu olmalarıdır. Günümüz toplumunu nitelendirmek için kullanılan ve iç içe geçen bu kavramlara ek olarak Andrejevic ve Burdon, sensör toplumu (*sensor society*) kavramını öne sürerler. Araştırmacılar, Schermer’in 2008 yılındaki bir sunumuna atfettikleri sensör toplumu nosyonunun, dijital çağda gözetim ve güçten mahremiyet ve sosyal sınıflandırmaya kadar deđişen konulardaki tartışmaları yeniden yönlendirmeye yardımcı olabileceđini vurgularlar. Sensör toplumu çerçevesi, nispeten istisnai ve ayırık izleme karakterinin kural olduđu dönemden, izleme altyapısının pasif, dağıtılmış, her zaman açık veri toplamaya izin verdiđi döneme geçişe odaklanır (Andrejevic & Burdon, 2015).

11 Eylül saldırıları, gözetimin ve günümüz toplumlarının gözetim toplumuna dönüşmesinin miladı olarak deđerlendirilebilir. Ancak bu deđerlendirme, gözetim konusunda çalışan araştırmacılar tarafından eleştirilir. 2001 yılında gerçekleştirilen terör saldırıları, gözetimi başlatmaktan ziyade, onu görünür hale getirmiştir. Başka bir ifade ile toplumsal gözetim, 1980’li yıllardan itibaren uygulamada olan bir pratikken, bu saldırılar sonucunda hem görünümü hem de yoğunluđu artırdıđı savunulabilir. Lyon da (2013) bu saldırıların, “devletlerinin ve emniyet güçlerinin gözetim kapasiteleri hakkında belli belirsiz de olsa bir farkındalık” geliştirdiđini vurgular. Lyon ayrıca, bu saldırılar sonrasında yükselen ulusal güvenlik vurgusuyla birlikte, ulus devletlerde odađın refahtan güvenliğe kaydıđını ekler.

Günümüzde gözetimin, sadece kişisel alana saldırmanın ve bireylerin mahremiyetini bozmanın deđil, toplulukları sınıflandırma ve ayırmanın da bir yolu

olduğu söylenebilir (Lyon, 2006, s. 306). Oscar Gandy, gözetimin; toplumu sıralama, sınıflandırma ve ayırmadaki etkisini ifade etmek için “*panoptic sort*” kavramını kullanır. Panoptik sıralama olarak Türkçeleştirilebilen kavram, vatandaşlar, çalışanlar ve tüketiciler olarak bireylerin, günlük yaşamları boyunca kendileri veya grupları hakkında ürettikleri bilgilerin toplanmasını, işlenmesini, paylaşılmasını ve bu bilgilerin, modern kapitalist ekonomi içindeki mal ve hizmetlere erişimin koordine ve kontrol edilmesi için kullanılmasını sağlayan karmaşık teknolojiye atıfta bulunur. Gandy’nin ifadesiyle panoptik sıralama, bireyleri rutin ölçümlere göre kategorilere ve sınıflara ayıran bir fark makinesidir ve sosyal, ekonomik ve politik sistemlerin rasyonelleştirilmesine yönelik genelleştirilebilecek bir endişe tarafından yönlendirilir (Gandy, 1993). Lyon, gözetim konusunun, insanlarda ilk akla getirdiği şeyin mahremiyet kaybı olduğunu, ancak bunun en önemli sorun olmadığını söyler. Ona göre, anonimlik, gizlilik ve mahremiyet konuları göz ardı edilemez, ancak “konunun tarafsızlık ve adalet, temel özgürlükler ve insan hakları ile bağlantısı da unutulmamalıdır. Çünkü bugünün gözetiminin temelde elde ettiği şey, öyle ya da böyle toplumsal sınıflandırmadır (Bauman & Lyon, 2013, s. 21).” Lyon, bireylerin, gözetimin toplumsal sınıflandırma gücü nedeniyle, tehlikede olduklarını ve tek tipleştirme, ayrımcılık, ötekileştirme ve dışlama karşısında savunmasız kaldıklarını iddia eder (Lyon, 2013). Kanuni yaptırımların da her zamankinden daha karmaşık hale gelen gözetim tekniklerine ayak uyduramadığı (Clarke, 1988; Akdeniz vd., 2001) dikkate alındığında, bireylerin gözetim karşısındaki savunmasızlıklarının daha belirgin hale geldiği söylenebilir.

Takip eden başlıklarda, gözetimi ve onun topluma etkilerini anlamlandırmak için sıklıkla kullanılan panoptikon kavramına ve onun yetersiz kaldığı noktalarda devreye giren diğer kavramlar kısaca açıklanmıştır.

1.2.1. Panoptikon

Bir gözetim modeli olarak panoptikon, Yunanca pan ve optikon kelimelerinden türetilmiştir ve “her şeyi gören yer” anlamını taşır (Bauman & Lyon, 2013). Panoptikon, Jeremy Bentham’ın on sekizinci yüzyılda tasarımını yaptığı, en basit ifade ile tüm kısımları merkezden gözlemlenebilen bir hapisane projesidir (Jeanneney, 2006).

Detaylı bir şekilde ifade etmek gerekirse panoptikon, her iki ucu açık bireysel hücrelerden oluşan, dairesel bir bina ile çevrili olan merkezi bir kule ile iç mekanın tüm

bölümlerinin tek bir noktadan görülebildiği bir hapishane, çalışma evi, okul veya tıbbi tesistir (Botan, 1996). Bu bağlamda mimari yapı olarak panoptikon, “tek bir görünmez gözünün, aynı anda pek çok insanı gözetlemesini olanaklı kıldığı otomatik bir gözetim biçimidir (Lyon, 2013, s. 57).”

Panoptikon projesi, her ne kadar bir hapishane olarak kurgulansa da temeli Jeremy Bentham’ın kardeşi Samuel’in, fabrika işçilerinin denetlenmesi için oluşturduğu plana dayanır (Lyon, 2013). Simon Werret, panoptikon tasarımının, Samuel Bentham’a ait olduğunu ve bu tasarımın Rusya’nın on sekizinci yüzyıl kültürünün etkilerini taşıdığını söyler. Werret’a göre Jeremy Bentham’ın başarısı, Samuel Bentham’ın ‘Krichev Panoptikonu’nda yansıtılan “özel olarak uygulanabilirlik durumlarını” “evrensel olarak uygulanabilir” kılmasıdır (Bentham vd., 2016, s. 109).

Panoptikon, Jeremy Bentham tarafından Birleşik Krallık’ta inşa edilmesi için hapishane olarak tasarlanırsa ve Bentham yaklaşık yirmi yılını bu projeye adanarak da gerekli bütçe, izin ve desteği sağlayamadığı için hiçbir zaman inşa edilememiştir (Bentham, 1969; Lyon, 1994). Bentham’ın bu çabası, bir panoptikon hapishanesi inşa edilmesine yetmese de yarattığı metafor, işyerinde gözetimin etkilerini incelemek için kullanışlı bir araç haline gelir (D’Urso, 2006). Hatta Michel Foucault’un, *Hapishanenin Doğuşu* adlı kitabında ifade ettiği gibi panoptikon, bir çeşit iktidar laboratuvarı gibi işler. Foucault’a göre bu, “ütopya” ceza evi olarak maddi bir biçime bürünmüş ve yeterince ilgi görmemiş olsa da gerçek bir tabi olma durumunu, hayali bir ilişkiden mekanik olarak ortaya çıkarması ve “mahkûmu iyi davranmaya, deliyi sakın olmaya, işçiyi çalışmaya, okul çocuğunu özenli olmaya, hastayı tedaviye uymaya zorlamak için” güç uygulamaya gerek bırakmaması ile iktidara sağladıkları açısından önemlidir (Foucault, 1992, s. 254).

Özgürlüklerle birlikte disiplini de keşfeden modernite, gözlem mekanizmaları sayesinde, insanların tutumları üzerinde daha etkin olabilir ve daha fazla nüfus olanağına kavuşur (Foucault, 1992). Panoptikon, Foucault’un önerdiği “disiplin toplumu”nun hem bir işareti hem de metaforudur (Zuboff, 1988). Bu metafor, George Orwell’in *Bin Dokuz Yüz Seksen Dört* adlı distopik romanında, her şeyi gören Büyük Birader olarak ortaya çıkar (Orwell, 2009). Lyon da panoptikonun, elektronik gözetimi anlamak için güçlü ve ikna edici bir metafor olduğunu söyler. Ona göre, görünmez gözlemcilerin, dijital ayak

izlerini takip edebildiği hapishane benzeri toplum, gerçekten de panoptik görünür (Lyon, 1994, s. 71).

Panoptikon, hem Foucault'un ifade ettiği gibi toplumun disipline edilmesinde hem de modern işyerlerinde verimliliğin artırılmasında gözetim aygıtlarının potansiyelini ifade etmek için kullanılan bir kavramdır. Tasarımı gereği panoptikon, birinin (ya da bir kurumun) diğerlerini gözetleme olanağı bulduğu bir yapıdır. Gelişen enformasyon ve iletişim teknolojileri, panoptikon metaforunun önerdiği gözetim akışını değiştirmiştir. Bu sebeple araştırmacılar panoptikonu, gelişen teknolojilerin sağladığı yeni gözetim pratiklerine uyarlamak için çeşitli çabalar harcamışlardır. Örneğin Botan (1996), elektronik panoptikon metaforunu kullanarak işyerlerindeki elektronik gözetim için panoptik etki (*panoptic effect*) modelini sunar. Enformasyon ve iletişim teknolojilerinin, kurumsal iletişim için kullanılmaya başlamasıyla bir gözetim teknolojisi haline geldiğini belirten Botan, panoptik etkinin, bireysel çalışanların iletişim teknolojisi üzerinde sahip oldukları kontrol veya bu teknolojiler aracılığıyla kontrol edilme dereceleri ile ilgili olduğunu ekler. Diana Gordon da (1987) tüm toplumun elektronik panoptikon içerisine kapatıldığını belirtir.

Campbell ve Carlson (2002), *Panopticon.com* adlı çalışmalarında, çevrim içi kurumsal gözetimin sosyal etkilerini anlamak için internet reklam sunucularını ve enformasyon aracıları olarak ifade edilebilecek (*infomediaries*) internet sitelerini²⁰ analiz ederler. Araştırmacılara göre, Foucault'un panoptikon metaforu, çevrim içi gözetimi ve siber uzaydaki güç ilişkilerini kavramsal olarak açıklamak için yeterlidir. Zuboff da enformasyon panoptikonu (*information panopticons*) kavramını geliştirir. Ona göre, bireylerin davranışlarını kaydeden ve görüntüleyen sistemler, evrensel şeffaflığı Bentham'ın "en tuhaf fantezilerini bile aşan" bir boyutta sağlayabilir ve bu sistemler, zaman ve mekânın sınırlamasından kurtulmuş, binaların fiziksel konumlarına veya endüstriyel yönetim tarafından tutulan kayıtlara bağlı olmayan enformasyon panoptikonları haline gelebilir. Enformasyon sistemleri hem gözlenen hem de gözetleyenin karşılıklı varlığını dahi gerektirmeden, tasarım sürecinde belirlenen amaçlarla yakalanmak isteneni (enformasyon) otomatik ve sürekli olarak kaydedebilir

²⁰ Infomediaries: Bir malın veya hizmetin üreticileri ve potansiyel müşterileri hakkında özel bilgi sağlayan internet siteleri (tureng.com)

(Zuboff, 1988). Zuboff (1988, s. 337), enformasyon panoptikonunun hiyerarşik olarak organize edilmiş olması ile orijinalinden ayrıldığını ve organizasyonun her seviyesinde, gözlemcinin teknik kontrolün aracı kadar hedefi olmasının muhtemel olduğunu söyler. Başka bir ifade ile enformasyon panoptikonu, bireyin hem gözlemci hem de gözlenen olmasını sağlayabilir (D'Urso, 2006).

Bireylerin, gözetlenen nesne olmanın da ötesine geçerek gözetleyebiliyor olması ve gözetlemenin, panoptikonun önerdiği gibi tek bir noktadan değil farklı pek çok kurum, kurum ya da şirket tarafından yapılabilen olması, araştırmacıları panoptikon metaforunu geride bırakmaya yönlendirir. Bir sonraki başlıkta panoptikon sonrası başvuru kavramlarına değinilmiştir.

1.2.2. Sinoptikon, Postpanoptikon, Ban-Optikon

Panoptikon, tasarımı gereği azın çoğu izlediği, birinin diğerleri hakkında pek çok şeyi bilebildiği bir sistemdir. Yirminci yüzyılın sonunda ve mevcut yüzyılın ilk yirmi yılında gelişen ve yaygınlaşan kitle iletişim araçları ile enformasyon ve iletişim teknolojileri bu denklemi değiştirmiştir. Bu değişimle ilgili olarak, panoptikon metaforu yerine farklı öneriler sunulmuştur. Bu önerilerden biri olan sinoptikon metaforu, Thomas Mathiesen tarafından Yunancadaki birlikte ve aynı anda anlamına gelen “syn” eki ile türetilir.

Mathiesen, Avrupa ülkelerinin sahip oldukları istihbarat altyapıları ve gözetim olanaklarına atfen, “azın çoğu izlediği” bir toplumda yaşadığımızı, ancak aynı zamanda gelişen kitle iletişim araçları sayesinde “çoğun” da -VIP’ler, muhabirler, film yıldızları gibi yeni bir sınıfı kapsayan- “azı” izlediğini öne sürer. Mathiesen’e göre içinde yaşadığımız toplum, sadece panoptisizm değil aynı zamanda sinoptisizm tarafından da karakterize edilir ve izleyici toplumu (*viewer society*) olarak nitelendirilebilir. Çalışmasında, kitle iletişim araçlarının gelişim tarihini kısaca ele alan Mathiesen, medyanın sinoptik karakterinin temel olarak televizyon tarafından geliştirildiğini; televizyon ile yüz milyonlarca insanın sahnedeki azınlığı izleyebildiğini söyler. Mathiesen, aynı zamanda Foucault’yu toplumun çoğunluğun azınlığı izlediği durumdan, azınlığın çoğunluğu izlediği duruma doğru geliştiğini iddia etmesi nedeniyle eleştirir ve onun kitle iletişimindeki sinoptik gelişim dalgalarını hesaba katmadığını belirtir (Mathiesen, 1997).

Lyon’a göre, Mathiesen’in dikkat çektiği en önemli nokta, günümüz toplumlarında panoptik etkilerin sinoptik etkilerden ayrı bir biçimde düşünülmemesidir. Bunun temel sebebi ise panoptik etkilerin sinoptik etkileri şekillendirmeye yardımcı olmasıdır (Bauman & Lyon, 2013, s. 74). Bu, Mathiesen’in çalışmasında öne sürdüğü üç savdan biridir. Araştırmacı tarafından öne sürülen diğer savlar ise hem panoptikon hem de sinoptikonun gelişiminin, 1800-2000 yılları arasındaki periyotta gerçekleştiği ve her ikisinin de kökeninin sanılanın aksine 1700’lü yıllara değil “antik” dönemlere dayandığıdır. Ek olarak Mathiesen, genel olarak kitle iletişim araçları ve özellikle de televizyon ile sinoptisizmin bilinçlerimizi kontrol ve disipline ettiğini belirtir ve Horkheimer ve Adorno’nun kültür endüstrisi analizlerine gönderme yapar.

Mathiesen’in argümanlarını özetlemek gerekirse, içinde yaşadığımız izleyici toplumu sadece “az insanın çok insanı izlediği bir gözetim toplumu değil, aynı zamanda çok insanın az insanı izlediği” bir kitle iletişim toplumdur. Ona göre modern kültürümüzde görünürde olan panoptik etkiler olsa da sinoptik etkiler diğerine ilişkin deneyimlerimizi şekillendirir ve bu etkiler sinoptik etkiler ile bağlantılı olarak değerlendirilmelidir. Kısacası, Mathiesen’e göre bu ikisi (panoptikon ve sinoptikon) birlikte çalışır (Lyon, 2013).

Panoptikon metaforunun yetersiz kaldığı noktada önerilen sinoptikon da özellikle enformasyon ve iletişim teknolojilerinin yaygınlaştığı toplumlardaki gözetim pratiklerini kapsama açısından eksik kaldığı söylenebilir. Bu noktada, kullanılan yöntemlere atıfta bulunarak gözetimi dönemlere ayıran Lyon’a danışmak yerinde olacaktır. Lyon, üç gözetim dönemi tanımlar: (1) modern öncesi dönem, (2) modern dönem ve (3) postmodern dönem. Modern öncesi gözetim yöntemleri, şimdiki zamana odaklı, doğrudan, yüz yüze ve yereldir. Modern yöntemler, daha karmaşık, dolayımli ve sadece şimdiki zaman değil aynı zamanda geçmiş yönelimlidir. Modern yöntemler ile yapılan gözetim hem yerel ve hem de ulusaldır ve dosyaya dayalı koordinasyondan yararlanılarak gerçekleştirilir. Bu gözetim yöntemi, kapsayıcılığı, aynılığı ve bir örnekliği özendirme eğilimdedir. Postmodern yöntemler ile yapılan gözetim ise, gelecek yönelimli, dijital aracılı, davranışsal ve biyometrik özelliklere dayalıdır. Ayrımcı olma eğiliminde olan postmodern gözetim yöntemleri, mikro (beden) ve makro (dünya) odaklıdır. Bu yöntemde elektronik arayüzler, özne ile gözetim sistemi arasında konumlanarak gözetimin şekil değiştirmesini sağlar (Lyon, 2013).

Postmodern gözetim yöntemleri, bir önceki başlıkta dikkat çekildiği gibi sadece bireylerin mahremiyetini değil, aynı zamanda toplumsal sınıflandırmaya sağladığı azımsanamayacak destek ile toplumsal eşitliği de tehdit eder. Yirmi birinci yüzyılın ikinci on yılının hâkim gözetim yöntemini, postmodern yöntemlerin oluşturduğu söylenebilir. Bu dikkate alındığında ise ne azın çoğu izlediği panoptikon ne de onunla birlikte çalışan çoğun azı izlediği sinoptikon metaforlarının tek başlarına yeterli olmadığı söylenebilir.

Aaron Doyle'a göre, Mathiensen'in sinoptikonu televizyon odaklıdır ve internetin gelişimine neredeyse hiç değinmemektedir. Doyle (2011, s. 290), teorik bir araç olarak sinoptikonun, direniş pratiklerine hemen hemen hiç yer vermediğini söyler ve metaforun en temel sınırlılığının buradan kaynaklandığını belirtir. Doyle, Mathiesen'in, internetin de televizyonda olduğu gibi büyük şirketler tarafından kontrol edilen ve tek yönlü bir iletişim aracı olacağı tahmininde yanıldığını ve iki yönlü bir kitle iletişim aracı olarak internetin, gözetime yönelik direniş ihtimallerini artırdığını ifade eder.

Marx, -pek kapsamlı olmadığını itiraf ederek- yeni topluma adını veren ve onun bazı temel yönlerini belirleyen gözetim denemelerinin, Bentham'ın panoptikonundan başlayan temsili bir listesini sunar. Listede yer alan yirmi dokuz farklı araştırmacı ve yeni topluma ya da onun özelliklerine ilişkin nitelendirmelerinden bazıları şunlardır: Foucault'un disiplin toplumu, Laudon'un dosya toplumu (*dossier society*), Clarke'ın veri gözetimi (*dataveillance*), Poster'ın süperpanoptikonu, Deleuze'un denetim toplumu (*society of control*), Boyne'un post-panoptikonu, Bigo'nun ban-opticonu ve Vaidhyathan'ın kriptopikonu (*cryptopicon*) (Marx, 2016, ss. 43-44).

Bruno, *Post-Panopticism* adlı çalışmasında, temel panoptik paradigmaya karşı dört sosyo-teorik argüman sıralar. İlki, panoptikon paradigmasının kendi içerisinde yer alan, bir gün bireylerin fiziksel aygıtlara ve dış kontrollere ihtiyaç duymadan kendilerini gözetleyebileceği bir aşamaya gelineceği ihtimalinin, bugün gerçekleşmiş olabileceğidir. İkinci argüman, artık neler olup bittiğini gözlemleme pratiğinin yerini, öngörü ve önlemeyi içeren ön-izleme (*previsualization*) pratiğinin almasıdır. Üçüncü argüman, sinoptikon metaforu ile ilgilidir. Kutupların yer değiştirmesi, panoptikon metaforunu tamamen yapıbozuma uğratabilir. Son argüman ise panoptikonun çeşitli türlerde şekil bozuklukları üreterek kendi kendini yenilgiye uğratarak post-panoptikon uzlaşmalarının oluşumunu kaçınılmaz kılmasıdır (Boyne, 2000, s. 299). Murakami Wood (2013) ise

bilgisayar ve iletişimin, militarizm ve finans kapitalin büyümesiyle sağlanan tipik bir post-panoptik gözetim çağına sahip olduğumuzu söyler.

Clarke ise, gözetim çalışmalarına veri gözetimi kavramını kazandırır. Clarke'a göre (1988, s. 499) veri gözetimi (*dataveillance*), “bir veya daha fazla kişinin eylemlerinin veya iletişimlerinin araştırılması veya izlenmesinde, kişisel veri sistemlerinin sistematik olarak kullanılmasıdır.” Veri gözetimi; doğası gereği, müdahaleci ve tehdit edicidir. *Information Technology and Dataveillance* adlı çalışmasında, kişisel ve kitlesel gözetim ayrımı yapan Clarke, veri gözetiminin birey ve topluma yönelttiği tehditleri sıralar. Kişisel veri gözetiminin bireye yönelttiği tehditler; yanlış tanımlama, düşük veri kalitesi, verilerin bağlam dışı kullanılması, bireyin bilgi ve rızası olmayan veri akışı, fişleme ve kefarettir. Kitlesel veri gözetimi ise hem bireysel hem de toplumsal tehditler oluşturur (Clarke, 1988, s. 505). Clarke, çalışmasını hem kişisel hem de kitlesel veri gözetiminin öz olarak kötü olmadıklarını; yarattığı tehditlerin azaltılarak faydalarının ön plana çıkarılması gerektiğini önererek sonlandırır.

Didier Bigo, artan küresel terörizm tehlikesinin yarattığı güvensizlik ortamında yapılan gözetimi kapsayacak bir metaforik araç olarak ban-optikonu (*ban-opticon*) önerir. Bigo için, Foucault'nun çalışmasında kullandığı haliyle, panoptikon toplumun genel olarak nasıl işlediğini anlamının bir yolu olarak hizmet etse de 11 Eylül saldırıları sonrası oluşan güvensizlik ortamında, bireylerin sınır ötesi hareketlerine odaklanan gözetim biçimleri olarak bilişim ve biyometrinin güçlenmesinin oluşturduğu diyagram panoptikon değildir. Bigo, bunun yerine Jean Luc Nancy ve Giorgio Agamben'den ödünç aldığı “ban” ve Foucault'tan aldığı “opticon” ile ban-optikon metaforunu üretir. Ban-optikon, heterojen ve çapraz uygulamalar ağının, uluslararası düzeyde bir güvensizlik biçimi olarak nasıl işlediğini anlamamızı sağlar. Bigo'ya göre mevcut gündem, herkesin gözetimi değil, hareketliliğin zorunluluğuna hapsolmuş olan az sayıdaki insan grubunun gözetimidir ve bu yapıyı kavramakta ban-optikon, faydalı bir başvuru kaynağıdır. Ban-optikon, söylemleri (tehdit, göç, içerideki düşman, göçmenler, radikal Müslümanlara karşı iyi Müslümanlar, dışlanmaya karşı entegrasyon vb.), kurumları (kamu kurumları, hükümetler, uluslararası kuruluşlar, sivil toplum kuruluşları vb.) ve mimari yapıları (havalimanlarındaki gözaltı merkezleri, bekleme alanları ve Schengen trafik şeritleri, bazı şehirlerdeki entegre video kamera ağları, güvenlik ve video izleme kapasiteleriyle donatılmış elektronik ağlar gibi) analiz etmek için kullanılabilir (Bigo, 2008, s. 32).

Basitçe söylemek gerekirse ban-optikon, profil çıkarma teknolojilerinin kimlerin belli başlı gözetim teknolojileri ile izleneceğini belirlemede kullanılmasıdır (Bauman & Lyon, 2013).

Mark Poster ise, yirminci yüzyılın sonlarında gözetimin teknik koşullarının önemli ölçüde ilerlediğini, ancak Foucault'un bunu dikkate almayı ihmal ettiğini söyler. Poster'a göre (1990), "günümüzün "iletişim devreleri" ve bunların ürettiği veri tabanları; duvarları, pencereleri, kuleleri veya korumaları olmayan bir gözetleme sistemi" olarak süperpanoptikonu (*superpanopticon*) oluşturur. "Gözetim teknolojilerindeki niceliksel ilerlemeler, gücün mikrofiziğinde niteliksel bir değişiklikle sonuçlanır." Ancak, teknolojiye değişimler sürecin sadece bir parçasıdır. Bu gelişmelerle birlikte toplum da gözetim ve sürece katılım konusunda disiplin altına alınmıştır. Poster, bu argümanını desteklemek için, sosyal güvenlik kartları, ehliyetler, kredi kartları ve kütüphane kartları gibi kartların kullanımını örnek gösterir. Bireyler, bu kartlara başvurmak, her zaman hazır bulundurmak ve sürekli kullanmakla yükümlüdür. Bu kartlar sayesinde, yapılan her işlemin kaydedilebilir, kodlanabilir ve veri tabanlarına eklenebilir. Poster, süperpanoptikonda bireylerin çoğunun, aynı anda hem bilgi kaynağı hem de bilginin kaydedicisi olduğunu söyler. Poster'a göre; söylem ve pratik olarak panoptikon, endüstriyel süreçlerin gelişmesi için insan kitlelerini kontrol etmenin bir aracıydı ve benzer şekilde, veri tabanlarının söylemi olan süperpanoptikon da enformasyonun postmodern, post-endüstriyel biçiminde, kitleleri kontrol etmenin bir aracıdır (Poster, 1990).

Vaidhyathan'a göre, günümüzde Avrupa'da, Kuzey Amerika'da ve dünyanın geri kalanında iş başında olan güçler, panoptikonun tam tersidir: birey tek, merkezi bir otoritenin bakışına tabi değildir, potansiyel olarak herkes tarafından, her zaman gözetlenebilir. Bu gözetim yapısını tanımlamak için Vaidhyathan, kriptopikon (*cryptopicon*) metaforunu kullanır. Kriptopikonda bireyler hangi yöntemlerle, yollarla izlendiğini, tanımlandığını ya da profillerinin nasıl çıkarıldığını bilmeden, sadece gözetlendiklerini bilerek ve davranışlarını düzenlemeden yaşarlar. Bireylerin bu umursamazlığı, mevcut gözetimin istediği bir durumdur (Vaidhyathan, 2011). Kısacası, kriptopikon, toplumdaki bireylerin gözetlendiklerinin farkında olmaları, ancak bu gözetimin nasıl işlediğine dair farkındalıklarının ve bilgilerinin olmadığını ifade eder.

Marx'ın yapmış olduđu listeye ek olarak, gözetim çalışmaları içerisinde yer almasa da bireyler tarafından gerçekleştirilen gözetimi ifade etmek için dikizleme kültürü kavramına değinilebilir. Niedzwiecki (2019), Dikizleme Günlüğü adlı kitabında, içinde bulunduğumuz çağı “Dikizleme Çağı” olarak isimlendirir ve bu çağda, herkesin hem her şeyi bilmek istediğine hem de herkesin her şeyi bilmesini istediğine dikkat çeker. Araştırmacı, bu çağın kültürünü oluşturan “Dikizleme Kültürü”nün, bu derece yaygınlaşmasını iki temel sebebe dayandırır: (1) bir ruhun başka bir ruha ulaşma ve hayatın anlamını paylaşma çabası ve (2) popüler kültürün bize enjekte ettiğı ilgi çekme ve farkına varılma arzusu. Niedzwiecki'nin yaklaşımı, bir bakıma, bireylerin gözetime gönüllü katılım gösterdiklerini ve bu katılımın gözetim toplumunu daha da yaygınlaştırdığını ve ona güç kazandırdığını işaret etmektedir.

Dikizleme kültürüne ek olarak, belki de çoğu noktada onunla iç içe geçen, gözetim kültürü kavramı da hem dijital dünyada mahremiyeti hem de gözetim toplumunu anlamlandırmada faydalı bir referans olabilir. David Lyon, *The Culture of Surveillance* adlı çalışmasında, insanların izleme araçlarıyla gün geçtikçe daha fazla meşgul olmalarının, gözetim kültürünü ortaya çıkardığını söyler. Başka bir ifade ile bireylerin sosyal medya aracılığıyla, başkalarının hayatlarını kontrol edebiliyor oluşu ve aynı zamanda paylaştıkları metinleri, tweetleri, gönderileri ve görselleri kamuya açık hale getirerek bunu mümkün kılması gözetim kültürünü mümkün kılar. Lyon'a göre; bugünün gözetiminde katılım çok daha belirgin bir özelliktir ve kullanıcılar, bu etkileşimin kapsamını anlamasalar bile, telefonlarının, giyilebilir cihazlarının, diğer akıllı aygıtlarının ve dijital platformların etkinlikleriyle etkileşime girdiğini bilmektedirler (Lyon, 2018).

Gözetim kültürünün yaygınlığını ve gözetimin günlük hayatın içerisinde de yapıldığını işaret eden örneklerden biri de ebeveynlerin, çocuklarını kontrol etmek için gözetim cihazları kullanmalarıdır. Bununla birlikte, az önce değinildiğı gibi, sosyal medyada birbirini takip eden arkadaşların birbirlerini gözetlemeleri de gözetim kültürünün mevcut yaygınlığına vurgu yapar. Lyon'ın gözetim kültürüne ilişkin belirttiğı bir diğer örnek ise bireylerin sağlık ve zindeliklerini korumak ve takip etmek amacıyla, akıllı sensörler kullanarak “kendilerini izlemesinin”, giderek daha fazla yaygınlaşmasıdır (Lyon, 2018).

Mevcut çağa ve toplumu anlamlandırmak için panoptikon, sinoptikon, süper panoptikon, post-panoptikon veya kriptopikon metaforlarının; disiplin, denetim, gözetim veya ağ toplumu kavramlaştırmalarının ya da topluma hâkim olan kültürü tanımlamak için dikizleme ya da gözetim kültürü tanımlamalarının kullanılabilir olduğunu ve tamamında az ya da çok bireysel mahremiyetin ve Lyon'ın sürekli altını çizdiği gibi, toplumsal eşitliğin tehdit edildiğini söyleyebiliriz. Bu noktada, bireylerin hem kendi kişisel verilerinin, mahremiyetlerinin farkına varmaları ve kendilerini korumaları hem de toplumsal eşitliği tehdit eden gözetim pratikleri hakkında bilgi sahibi olmaları önemlidir. Bir sonraki bölümde, bireylerin, doğrudan bu farkındalıklar bütününe kapsamasa veya bunlarla sınırlanmasa da modern toplumda bilgi ve haber alma, iletişim kurma, sosyalleşme, kamu ve özel sektör hizmetlerine erişme gibi ihtiyaçlarını karşılamada yaşayacağı sorunları, tamamen ortadan kaldırmasa bile azaltmada etkili olabilecek, dijital okuryazarlık konusu ele alınmaktadır.

İKİNCİ BÖLÜM

AĞ TOPLUMU VE DİJİTAL OKURYAZARLIK

Dijital teknolojiler; bir yandan yönetim, denetim, pazarlama, üretim ve eğitim gibi alanlarda yenilikçi çıktılar sağlarken diğer yandan sakıncalı ve zararlı olabilecek içerikler, ortamların istismar amaçlı kullanımı, oluşabilecek etik sorunlar, güvenlik riskleri, sağlıksız kullanım ve mahremiyet ihlalleri gibi olumsuz yönleri de barındırmaktadır (Sağıroğlu vd., 2020a).

Günümüz toplumu, karamsar ve temkinli bir açıdan bakıldığında disiplin toplumu, denetim toplumu, dosya toplumu (*dossier society*) ve gözetim toplumu olarak nitelendirilebilir. Enformasyon ve iletişim teknolojileri kaynaklı risk ve tehditlere odaklanan bu kavrayışların karşısına, bu teknolojilerin sunduğu imkân ve fırsatlara odaklanan bir yaklaşım ile çıkılabilir. Daha iyimser bir bakış açısı ile günümüz toplumu, bilgi toplumu, ağ toplumu, internet toplumu ve siber toplum olarak değerlendirilebilir. Toplumu iyimser bir bakış açısı ile ele almak, imkân ve fırsatları ön plana çıkarır. Ancak risk ve tehditleri görmezden gelmek, özellikle bireysel mahremiyet, toplumsal eşitlik ve ifade özgürlüğü gibi hakların erimesine göz yummak anlamına gelebilir. Bu ikilemden kurtulmak için topluma hangi perspektiften bakılırsa bakılsın, risk ve tehlikeler hakkında farkındalığın ve imkân ve fırsatlar hakkındaki farkındalık ile desteklenmesi, geliştirilmesi ve çoğaltılması gereklidir.

Bu bölüm, bir bakıma, enformasyon ve iletişim teknolojilerinin yaygınlaşması ile erişilebilir olan fırsatlara ve bu fırsatların toplumun tamamı için erişilebilir ve kullanılabilir olmasında dijital okuryazarlık kavramını merkeze alan bir yaklaşım taşımaktadır. Bu yaklaşım çerçevesinde, önce ağ toplumu (*network society*) ve dijital vatandaşlık kavramları ele alınmış, daha sonra okuryazarlık ile medya okuryazarlığı kavramlarına atıfta bulunularak dijital okuryazarlık kavramı değerlendirilmiştir.

2.1. Ağ Toplumu

Ağ toplumu kavramı, yirminci yüzyılın sonunda, özellikle enformasyon ve iletişim teknolojilerindeki hızlı gelişimin toplum yapılanmalarına olan etkisini nitelemek için ortaya çıkmıştır. Kavram, iki farklı araştırmacıya atfedilse de (van Dijk ve Castells) ilk olarak, 1991 yılında van Dijk tarafından, Felemenkçe yayınlanan *De Netwerkmaatschappij (The Network Society)* adlı kitapta kullanılmıştır. Yazar, ağ toplumunu, her düzeyde (bireysel, grupsal/örgütsel ve toplumsal) ana örgütlenme biçimini mümkün kılan ve sosyal ve medya ağları altyapısına sahip bir sosyal oluşum olarak tanımlar ve bu ağların giderek artan bir şekilde, bu toplumların tüm birimlerini veya parçalarını (bireyler, gruplar ve kuruluşlar) birbirine bağladığını ifade eder (van Dijk, 2006).

Ağ toplumu kavramını ilk olarak Enformasyon Çağı: Ekonomi, Toplum ve Kültür adlı üç ciltlik kitap serisinin ilk cildi olan Ağ Toplumunun Yükselişi kitabında kullanan Castells'e göre (2005) ağ toplumu; en basit ifadeyle, ağların düğümlerinde biriken enformasyonlar temelinde bilgi üreten, işleyen ve dağıtan mikro elektronik ve dijital bilgisayar ağlarına ve enformasyon ve iletişim teknolojileri tarafından işletilen ağlara dayalı bir sosyal yapıdır. Başka bir ifade ile ağ toplumu; sosyal organizasyon, sosyal değişim ve enformasyon ve iletişim teknolojileri etrafında oluşturulan teknolojik paradigma arasındaki etkileşimden kaynaklanan sosyal yapıya vurgu yapar (Castells, 2004b). Yazar bu kavramı kullanma gerekçesini ise, sosyal organizasyonun ve sosyal pratiğin tüm kilit boyutlarının ağlardan oluştuğu gözlemine dayandırır: Ağlar, insanlık tarihindeki eski bir örgütlenme biçimi olsa da Bilgi Çağı'nın beraberinde getirdiği dijital ağ teknolojileri, sosyal ve örgütsel ağları, ağ oluşturma biçimlerinin geleneksel sınırlamalarını aşarak ağların sonsuz genişlemelerine ve yeniden yapılandırmalarına izin verecek şekilde güçlendirir (Castells, 2010c).

van Dijk, enformasyon toplumu ile ağ toplumu kavramları arasındaki ayrımın netleştirilmesi gerektiğini savunur. İlk kavramın, daha çok içerik üzerinde durduğunu belirten araştırmacı, ağ toplumunun ise modern toplumun biçim ve örgütlenmesine odaklandığını söyler. Başka bir ifade ile “enformasyon toplumu kavramında, toplumlardaki faaliyet ve süreçlerin değişim özüne vurgu” yapılmakta iken “ağ toplumu kavramında ise dikkat ve ilgi bu toplumların değişen örgütlenme biçimleri ve (alt)yapılarına kaymaktadır (van Dijk, 2017, s. 41).” Castells de içinde bulunduğumuz

toplumun ne enformasyon ne de bilgelik toplumu olarak nitelendirilebileceğini söyler ve bilgi ve enformasyonun, her zaman üretkenlik ve gücün temel kaynakları olduğunu; günümüzdeki sürecin de diğer tarihsel dönemlerdekinden farklı olmadığını ifade eder. Araştırmacıya göre, günümüzde farklı olan ve toplumsal süreçlerin temel belirleyicisi olarak nitelendirilebileceğimiz değişken ise yeni bir teknolojik paradigma temelinde, yeni bir sosyal yapının, elektronik iletişim teknolojilerinden oluşan bir yapının -güçlü, sosyal ağların- ortaya çıkmasıdır. Başka bir ifade ile farklı olan enformasyon ve bilginin kullanımının artışı değil, teknoloji ve ağ bağlantılı sosyal yapı ile ağ oluşturma mantığındaki belirli ilişkiler dizisidir. Buradan hareketle Castells, günümüz toplumunu tanımlamak için, ağ toplumu kavramının kullanılması gerektiğini savunur (Castells, 2004a, s. 41).

1990'lı yıllarda internetin popülerleşmesinin, yeni bir tür iletişimsel ilişkilerin oluşumu üzerinde büyük bir etkiye sahip olduğu ve böylece ağ toplumunu ortaya çıkardığı söylenebilir (Śliwińska, 2017). Castells de (2010b) dünyamız ve yaşamlarımızın, küreselleşme ve kimliğin çatışan eğilimleri tarafından şekillendiğini; bilgi teknolojisi devriminin ve kapitalizmin yeniden yapılandırılmasının, yeni bir toplum biçimi olarak ağ toplumunu teşvik ettiğini ifade eder. Sosyal yapısı, mikro elektronik temelli bilgi ve iletişim teknolojilerinden güç alan ağlardan oluşan bir toplum biçimi olarak ağ toplumunun, aşağıda listelenen faktörler tarafından karakterize edildiği söylenebilir (Castells, 2004a):

- Stratejik olarak belirleyici ekonomik faaliyetlerin küreselleşmesi
- Organizasyonun ağ oluşturma biçimi
- İşin esnekliği, istikrarsızlığı ve emeğin bireyselleştirilmesi
- Yaygın, birbirine bağlı ve çeşitlendirilmiş bir medya sistemi tarafından inşa edilen gerçek bir sanallık kültürü
- Hayatın, mekânın ve zamanın maddi temellerinin, bir akışlar ve zamansız zamanın oluşturulması yoluyla, egemen faaliyetlerin ve kontrol eden seçkinlerin ifadeleri olarak dönüştürülmesi (Castells, 2010b, s. 2).

Castells, yirminci yüzyılın son çeyreğindeki kimi birbirinden bağımsız gelişmenin, ağırlıklı olarak ağlara dayalı yeni bir toplumsal yapı olan ağ toplumunun habercisi olarak değerlendirir. Bu gelişmeler, (1) ekonominin yönetim esnekliğine, sermayenin, üretim ve ticaretin küreselleşmesine yönelik ihtiyaçları; (2) bireysel özgürlük ve açık iletişim değerlerinin üstün hale geldiği toplumda yükselen talepler ve (3) mikro elektronik devriminin mümkün kıldığı bilgi işlem ve telekomünikasyondaki

olağanüstü gelişmelerdir (Castells, 2002, 2004a). van Dijk (2006) ise ağ toplumuna zemin hazırlayan süreçlerin teknik temellerini beş başlık altında incelenebileceğini söyler: (1) Mikro-elektronik (*micro-electronics*), (2) dijitalleşme (*digitalization*), (3) depola ve ilet prensibi (*store and forward principle*), (4) katmanlı örgütlenme (*layered organization*) ve (5) yeni bağlantılar (*new connections*). Mikro-elektronikteki birbirini takip eden birkaç devrimsel gelişme ve sadece birkaç milimetre karelik bir yüzey üzerinde yüz binlerce bağlantıdan oluşan bir çip olan entegre yarı iletkenin icat edilmesiyle mikroişlemciler üretilebilmiştir ve bu işlemcilerin işlem güçleri, ortalama on sekiz ayda bir ikiye katlanmaktadır. Dijitalleşme de mikro-elektronikteki gelişmelere bağlı olarak gelişen, tüm içerik türlerini kapsayan ve değiş tokuş edilebilen tüm sinyaller için kullanılabilen tek tip bir dilin gelişmesidir. Bu dil, yeni medyanın doğruluk, seçicilik ve uyaran zenginliği gibi iletişim kapasitelerini destekler. Depola ve ilet prensibi de içeriğin elektronik hafızalarda ve veri tabanlarında depolanması ile ilgilidir. Aynı zamanda bu prensip ile ağ üzerindeki her bir eylem kaydedilmesi ve saklanması söz konusu olduğu için mahremiyet korumasına yönelik potansiyel bir tehdit oluşturur (van Dijk, 2006).

Ağ Toplumu kitabının daha güncel bir basımında van Dijk (2017), bu beş temele ek olarak değinilmesi gereken güncel trendleri ele alır. Bu trendler; yakınsama/yöndeşme, minyatürleşme, gömülü teknoloji, mobil ve kablosuz teknolojisi, geniş bant teknolojisi ve bulut bilişimdir. Yöndeşme telefon, bilgisayar ve radyo-televizyon gibi teknolojilerin, kademeli olarak bütünleşmesini işaret eder. Minyatürleşme ve gömülü teknolojiler, EİT'lerin daha küçük ve daha güçlü hale gelmelerini vurgularken mobil ve kablosuz teknolojideki gelişmeler, ağın altyapı ulaştırmakta sıkıntı yaşanan bölgelere dahi ulaşmasını sağlar.

Castells'e göre (2010a, s. 387); "ağ toplumu, diğer herhangi bir sosyal yapı gibi, çelişkilerden, sosyal çatışmalardan ve alternatif sosyal örgütlenme biçimlerinden gelen meydan okumalardan yoksun değildir." Ancak bu zorluklar, ağ toplumunun özelliklerinden kaynaklandıkları için endüstriyel çağın getirdiği zorluklardan keskin bir şekilde farklıdır. Ağ toplumu, çelişki ve mücadelelerden muaf olmasa da giderek artan bir biçimde toplumun bileşenlerini organize ederek ve birbirine bağlayarak mevcut sosyal yapıyı güçlendirebilir. Bu, van Dijk'in (2017) öne sürdüğü temel önermelerinden biri olan "internet gibi ağlar, devirmek yerine toplumun mevcut yapılarını güçlendirir" ifadesi ile desteklenebilir. Castells (2004a) için de, yeni teknolojilerden yararlanan ağlar,

kazandıkları esneklik, ölçeklenebilirlik ve sürdürülebilirlik özellikleri ile en verimli organizasyon biçimidir.

van Dijk, ağ toplumu teorisini özetlemek için, ağın (webin) kanunları olarak nitelendirdiği yedi kanun tanımlar. Kavramın ilk olarak Huberman tarafından kullanıldığını belirten araştırmacıya göre, bu kanunlar doğa kanunları gibi değildir ve sadece ağlardaki insan davranışları üzerinde tanımlayıcı ve olanak sağlayıcı koşulları içermektedir (van Dijk, 2017):

- Ağ eklemlleme kanunu
- Ağların dışsallığı kanunu
- Ağ genişlemesi kanunu
- Küçük dünyalar kanunu
- Dikkatin sınırlılığı kanunu
- Ağlardaki güç kanunu
- Eğilimleri güçlendirme kanunu

Ağın ilk kanunu olan eklemlleme kanunu, ağ toplumunda ilişkilerin, birimler veya aralarında bağlantı kurulan düğümlerden daha önemli hale geldiğini ve toplumun alt sistemlerindeki tüm ilişkilerin yüzeye çıktığını belirtir. Ağların dışsallığı kanununa göre ağlar, ağ dışında şeyler/insanlar üzerinde de etki sahibidir. Bir ağa ne kadar fazla insan katılırsa diğerlerinin de katılma olasılığı artar ve üzerlerinde ağa katılma baskısı oluşturur. Bu etki, “ağ etkisi” olarak isimlendirilir. van Dijk bu baskının iki tane taşma noktası olduğunu belirtir: İlki, ağ kullanıcılarının yeterli çoğunluğa eriştiği, yani nüfusun yüzde 20 ila yüzde 25’inin ağa katıldığı noktadır. Bu şart sağlandığında, nüfusun geri kalanının da ağa bağlanması mantıklı hale gelir. İkinci taşma noktası ise toplumun üçte ikisinin (yaklaşık %67’sinin) katılımıyla sağlanır ve bu noktadan sonra ağa bağlanmayanlar, dışlanmamak için ağa katılmaya “neredeyse zorlanırlar (van Dijk, 2017).” Castells (2004a) de herkesin ağ toplumunun bir parçası olmadığını, buna rağmen herkesin, bu sosyal yapıdan etkilendiğini ifade eder. Araştırmacıya göre, dünyanın her yerinde insan yaşamını şekillendiren ve kontrol eden finansal piyasalar, üretim, yönetim, mal ve hizmetlerin dağıtımı, bilim, teknoloji, iletişim medyası, kültür, sanat, spor ve uluslararası sivil toplum örgütlenmeleri gibi faaliyetler ya da faaliyet alanları, küresel ağlarda organize edildiği için ağlar herkesi etkilemektedir. Bu bakış açısı, ağların dışsallığı kanunu ile örtüşmektedir.

Ağın genişlemesi kanunu, ağın/webin büyümesinin içsel boyutunu ortaya çıkarır. Bu kanun ile ağların her birim veya düğüm noktasının doğrudan birbirine bağlanması için bir anda çok büyük hale gelmesi gerektiği öngörülür. Başka bir ifade ile “web gibi ağlar büyüdükçe genellikle aşırı büyük hale gelirler” ve ağdaki birimler birbirlerine görünmez olurlar. Bu sorun, aracı sistemlerle çözülür. Bu araçlar; arama motorları, sosyal ağ siteleri, portallar, fiyat karşılaştırma siteleri ve randevu siteleri olarak ifade edilebilir (van Dijk, 2017, s. 63).

Ağın dördüncü kanunu olan küçük dünyalar kanunu, büyük ağlardaki birimlerin birbirlerine komşu olmasalar dahi küçük bir dünya yaratacak şekilde, birkaç adım ile erişebilir olmalarına vurgu yapar. Altı derecelik ayrılık (*six degrees of separation*) olarak kavramsallaştırılan bu fenomene göre, dünya üzerindeki insanlar birbirlerinden altı veya daha az sosyal bağlantı ile bağlantılıdır. Bu fenomene göre, herhangi iki kişiyi en fazla altı adımda birbirine bağlamak için bir “arkadaşın arkadaşı” ifadeleri zinciri oluşturulabilir (Wikipedia, 2021). Milgram (1967), altı derecelik ayrılık metaforunu, Küçük Dünya Sorunu (*Small World Problem*) başlıklı makalesinde ele alır. Milgram ve diğer araştırmacıların yürüttüğü araştırmalar, tamamen çevrim dışı sosyal ağlar üzerinde gerçekleştirilir. van Dijk, çevrim içi sosyal ağlarla birlikte, ayrılık derecelerinin beşe hatta dörde düştüğünü bulgulayan araştırmalara değinir ve küçük dünyalar kanununun web ve diğer iletişim ağlarının kullanımıyla dünyanın nasıl birbirine daha bağlı ve interaktif hale geldiğini açıkladığını belirtir. Ancak bu bağlılık ve interaktivite etkisi, sadece üç dereceye kadar ulaşabilmektedir (van Dijk, 2017). Christakis ve Fowler’ın (2007), otuz iki yıllık bir periyotta (1971-2003), yaklaşık on iki bin kişinin sosyal ağlarında (çevrim dışı), obezitenin yayılmasında etkili olan faktörleri inceleyen çalışması, üç derecelik etkiye ilişkin nicel bulgular ortaya koyar. Bu etki kuralına göre, sosyal etki, sadece tanıdığımız insanlarla sınırlı değildir ve örneğin bir bireyin arkadaşının arkadaşının arkadaşının kilo alması ya da sigarayı bırakması, o bireyin de kilo alma ya da sigarayı bırakma olasılığını artırır (Christakis & Fowler, 2011).

Dikkatin sınırlılığı kanunu, prensip olarak ağ üzerindeki bireylerin, diğer herkesle iletişim kurabilme ve bağlanabilme ihtimali nedeniyle, alıcı olarak bireylerin okuma/dinleme/izleme görme sürelerinin azalmasına dayanır. Ağ üzerindeki bireyler daha fazla mesaja maruz kalacakları için kimi mesajlara zaman ayıramayacaklardır. Başka bir ifade ile ağ içerisinde ne kadar çok sayıda kullanıcı içerik üretirse, bu içeriklerin

okuyucularının sayısı da ortalama olarak o kadar azalır. Bu durum, ağlarda dikkatin sınırlılığı kanunu olarak ifade edilir (van Dijk, 2017). Hindman'ın (2009, s. 142) “siber uzayda konuşmak kolay olabilir, ancak duyulmak zordur” ifadesi de dikkatin sınırlılığı kanununu ile ilişkilendirilebilir.

Ağlardaki güç kanunu, büyük ağlarda halihazırda daha fazla bağlantıya sahip olan birimlerin, daha fazla bağlantı kurması ve buna karşılık ağdaki çoğu birimin, sadece birkaç bağlantıya sahip olması ile ilgilidir. Başka bir ifade ile güç kanunu, ağlarda bir orta noktanın olmamasını açıklamakta kullanılabilir. Bu kanun, ağlardaki bağlantı sayısı dağılımını açıklayan “istatistiksel bir düzenlilik” Ağlardaki düğüm noktaları ve bağlantı sayıları normal dağılmaz. Bu durum, internet üzerinde “zenginlerin daha çok zenginleşmesi ve fakirlerin daha çok fakirleşmesi etkisi” olarak nitelendirilebilir (van Dijk, 2017). Ağdaki güç kanununu açıklamak için goooglearşi (*googlearchy*) kavramını kullanan Hindman'a göre (2009), görünürlüğü yüksek sitelerin sayısı azdır ve bu az sayıdaki görünürlüğü yüksek site, diğer ilgili sitelerin toplamından daha fazla bağlantıya sahiptir.

Ağın son kanunu olan eğilimleri güçlendirme kanunu ise ağların, mevcut sosyal ve yapısal eğilimleri güçlendiren ilişkisel yapılar olduğunu savlar. EİT'ler vb. teknolojilerin kullanılması eğilimleri güçlendirir. van Dijk'in çalışmasındaki temel önermelerden biri, bu kanun ile ilişkilidir: “İnternet gibi ağlar devirmek yerine toplumdaki mevcut yapıları güçlendirir (van Dijk, 2017, s. 67).”

van Dijk, medya ağlarının modern toplumun sinir sistemi haline geldiğini ve sosyal organizasyonun araç ve yapılarını şekillendirdiğini ifade eder (akt. van Deursen & van Dijk, 2015). Kitle toplumlarında ise toplumsal organizasyon, halen yüz yüze sosyal ağlara dayalıdır. Bir sonraki başlıkta, kitle toplumu ile ağ toplumu arasındaki farklılığa değinilmiştir.

2.1.1. Kitle Toplumu ile Ağ Toplumu Ayrımı

Kitle toplumu, “modern toplumu homojenize edilmiş ama aynı zamanda atomize bireylerden oluştuğu için parçalanmış olarak nitelendirmek” amacıyla kullanılan bir kavramdır (Munro, 2017). Kavram, artan bir iç homojenliğe sahip, elit ve bürokratik bir kombinasyonun, “kitleler” olarak adlandırılan nüfusun çoğunluğunu kontrol ettiği, belirli bir baskın kültür türünün (kitle iletişim araçları ile bağlantılı kitle kültürü) ve liberal

olmayan bir siyaset biçiminin hâkim olduğu toplumlar için kullanılır. Bu toplumlar aynı zamanda, “kitlesele üretim” ve “kitlesele tüketim” yoluyla endüstriyel ekonominin gelişmesinde yeni bir aşamayı yansıttıkları söylenebilir (Giner, 2001). Bu toplumların, her seviyedeki örgütlenme biçimlerinin gruplar, örgütler ve toplulukların (kitlelerin) oluşturduğu bir altyapı tarafından şekillenen sosyal oluşumlar olduğu ifade edilir (van Dijk, 2017). Buna karşılık, yukarıda aktarılan tanımında olduğu gibi, ağ toplumlarında sadece kitleler arası değil her düzeyde örgütlenmeyi mümkün kılan sosyal ve medya ağlarından oluşan bir altyapı mevcuttur. Aşağıdaki tablo, bu iki toplum türünü farklı bileşenler üzerinden karşılaştırmaktadır.

Tablo 2.1: Kitle Toplumu ve Ağ Toplumu Tipolojisi

Özellikler	Kitle Toplumu	Ağ Toplumu
Temel öğeler	Kollektiviteler (gruplar, örgütler, topluluklar)	(Ağlarla birbirine bağlanan) bireyler
Bileşenlerin doğası	Homojen	Heterojen
Ölçek	Genişletilmiş	Genişletilmiş ve eksiltilmiş
Kapsam	Yerel	Küreyerel (<i>global</i>)
Bağlanırlık ve bağlanmışlık	Öğeler içinde yüksek	Öğeler arasında yüksek
Yoğunluk	Yüksek	Daha az
Merkezileşme	Yüksek (az sayıda merkez)	Düşük (çok merkezli)
Kapsayıcılık	Yüksek	Düşük
Topluluk türü	Fiziksel ve bölünmez	Sanal ve dağınık
Örgüt türü	Bürokrasi Dikey entegre	İnfokrasi Yatay farklılaşmış
Hanehalkı türü	Geniş aileyle büyük	Çeşitli aile ilişkileriyle küçük
Temel iletişim türü	Yüz yüze	Artan biçimde dolayımlanmış
Medya türü	Broadcast kitle medyası	Narrowcast interaktif medya
Medya sayısı	Düşük	Yüksek

Kaynak: (van Dijk, 2006, s. 33, 2017, ss. 69-70)

Tablo 2.1’e dayanarak, kitle toplumlarında ağ toplumlarına kıyasla, iletişim medyalarının niceliksel olarak daha az ve interaktivitesi daha düşük, yoğunluğun ve merkezileşmenin ise daha yüksek olduğu söylenebilir. Kitle toplumlarında, hane halkları (bir arada yaşayan aile fertlerinin etkisiyle) daha büyükken ağ toplumlarında küçüktür. Kitle toplumlarının kapsamı yerelken ağ toplumlarında kapsam hem küresel hem de yerel

boyuttur ve “küreyerel” (*glocal*) olarak nitelendirilebilir. Son olarak, kitle toplumlarındaki bağlantı ve iletişimler daha çok ögeler içerisinde, yani mevcut grup, örgüt ya da topluluk içerisinde yoğunlaşırken ağ toplumlarındaki bağlantı ve iletişimler ögeler arasında daha fazladır.

2.1.2. Ağ Toplumuna Entegrasyon

Dijital ağlar, kendilerini yeniden yapılandırma kapasitelerinde sınır tanımadıkları için küreseldir. Bu noktadan hareket ederek altyapısı dijital ağlara dayanan bir sosyal yapı da tanımı gereği küresel olacağı için, ağ toplumu küresel bir toplum olarak kabul edilebilir. Bu küresellik, dünya genelindeki tüm insanların bu ağlara dahil olduğu anlamına gelmesi de herkesin, bu egemen toplumsal yapının küresel ağlarında meydana gelen süreçlerden etkilendiği söylenebilir. Bunun nedeni ise, gezegenin her köşesinde insan yaşamını şekillendiren ve kontrol eden temel faaliyetlerin, bu küresel ağlarda organize ediliyor olmasıdır (Castells, 2004a). Ancak, ülke toplumlarının ağ toplumlarına geçişi, sadece teknolojik bir geçiş ve internet kullanımının yaygınlaşması ile ilgili değildir. Bu geçiş aynı zamanda sosyo-politik bir değişimi de yansıtır. Cardoso’ya göre (2005) bu geçiş, önce diktatörlüklerden demokratik kurumsal siyasete ve ardından demokrasinin rutinleşmesine doğru gerçekleşir.

van Dijk’e göre, günümüz modern toplumları ağ toplumuna dönüşme sürecindedirler ve gelişmekte olan toplumlar ise halen birer kitle toplumudur. Batı toplumlarında bireyler, ağ toplumunun temel birimi haline gelmiş ve ağlarla birbirine bağlanmış durumdadır. Doğu toplumlarında ise, temel birim halen ağlarla birbirine bağlanan aile, topluluk veya çalışma ekibi gibi gruplardır. Ancak, yine de van Dijk’e göre pek çok gelişmiş toplum halen tam teşekküllü bir ağ toplumu olarak nitelendirilecek noktada değildir.

Ağ toplumuna entegrasyonu tamamlayan toplumları belirlemek için çeşitli istatistiklere ve uluslararası organizasyonlar tarafından hazırlanan dizin ve karşılaştırmalara başvurulabilir. Örneğin, dünya genelindeki 41 şehri kapsayan Networked Society City Index’te, şehirler EİT olgunluğuna ve sürdürülebilir kentsel gelişimdeki performanslarına göre sıralanır. En günceli 2016 yılına ait olan çalışmada, ağa bağlı toplum şehirleri listesinin ilk üç sırasında; İsveç’in başkenti Stockholm, İngiltere’nin başkenti Londra ve Singapur yer alır. Bu dizini hazırlamakta kullanılan

sosyal, ekonomik ve çevresel göstergeler ile EİT olgunluğuna ilişkin veriler, teknolojiye hızlı değişikliklerin insanlar tarafından benimsenmesinin şehirleri daha da ağa bağlı topluma doğru yönlendirdiğini ortaya koyar. Aynı verilere bakılarak, dünyanın dört bir yanındaki şehirlerin EİT altyapılarında açık bir gelişme olduğu söylenebilir. Altyapıdaki bu gelişmelerle birlikte bu teknolojilerin daha ekonomik ve ucuz hale gelmesi, EİT kullananların sayısını ve bu teknolojilerin kullanım şeklini de değiştirir. “İnternet artık mobil cihazlarda tüketilen ve günlük yaşamın giderek daha fazla alanında kullanılan gerçekten kişisel bir deneyimdir (Networked Society Lab, 2016, s. 13).”

Ağ oluşturma kapsamının genişlemesi ve ağın yayılmasının, mobil ve kablosuz iletişim teknolojilerindeki gelişmeler ile hızlandığı söylenebilir. Neredeyse tüm dünya nüfusu, artık bir mobil hücreli ağ sinyalinin menzili içerisinde yaşamaktadır (ITU, 2018b). Bu teknolojilerdeki gelişmeler, gelişmiş ülkelerdeki kırsal kesimlerin ve gelişmekte olan ülkelerdeki tüm bölgelerin, artık daha kolay ve ucuz telefon sistemleri, uydu yayını ve internet erişimine ulaşmalarını sağlar. Bu erişim şekli, kablolar ve sabit erişim noktalarıyla sınırlı olmadığı için internet kullanımını, ev ve iş yerlerinden ulaşım ve boş zamanlara doğru kaydırır. van Dijk’in ifadesi ile bu teknolojiler, “ağ toplumunu dünyadaki en uzak yerlere ve en derin deliklere doğru yayacaktır (van Dijk, 2017, ss. 88-89).”

Ağ toplumuna entegrasyona ilişkin bilgiler sunan bir diğer dizin olan Network Readiness Index’te (NRI) ülkeler; teknoloji, insan, yönetim ve etki kategorileri altında birleştirilen verilere dayanarak sıralanırlar. NRI 2020 modelinde yer alan bu kategoriler, çeşitli alt kategorilere ayrılırlar. Teknoloji kategorisinde; erişim, içerik ve gelecek teknolojilerine ilişkin veriler bulunur. İnsan kategorisi ise bireyler, işletmeler ve hükümetler alt kategorilerine sahiptir ve birey, işletme ve hükümetlerin ağ ekonomisine katılımda EİT kullanımlarına ve becerilerine ilişkin verileri içerir. Yönetim kategorisi; güven, düzenleme ve dahil etme, kapsama alt kategorilerinde karşılaştırma yapmaya imkân tanıyıcı göstergeleri barındırır. Dördüncü kategori olan etki kategorisi ise ağ ekonomisine katılımın; ekonomik, sosyal ve Sürdürülebilir Kalkınma Amaçları (SDG) bağlamında etkisini kapsayan üç alt kategoriye sahiptir. Özetle, NRI içindeki on iki alt kategori için toplamda altmış farklı gösterge kullanılmış ve ülkeler bu göstergelere göre sıralanmıştır (Dutta & Lanvin, 2020, s. 26). Aşağıdaki tablo, bu dizinin ilk yirmi sırasında yer alan ülkeleri ve bu ülkelerin dört farklı kategorideki skorlarını göstermektedir.

Tablo 2.2: En Yüksek NRI Skoruna Sahip 20 Ülke

Ülke	Bölge	NRI Sırası	NRI Skoru	Teknoloji	İnsan	Yönetim	Etki
İsveç	Avrupa	1	82,75	83,82	78,07	88,88	80,23
Danimarka	Avrupa	2	82,19	79,71	80,81	89,80	78,45
Singapur	Asya&Pasifik	3	81,39	76,16	77,86	83,35	88,17
Hollanda	Avrupa	4	81,37	83,81	73,45	89,47	78,75
İsviçre	Avrupa	5	80,41	85,67	70,02	85,04	80,93
Finlandiya	Avrupa	6	80,16	78,24	78,19	88,61	75,59
Norveç	Avrupa	7	79,39	75,23	73,88	91,30	77,14
ABD	Amerika	8	78,91	82,88	74,59	86,23	71,96
Almanya	Avrupa	9	77,48	79,18	70,54	83,52	76,69
İngiltere	Avrupa	10	76,27	78,34	69,69	82,65	74,40
Lüksemburg	Avrupa	11	75,27	79,28	68,35	82,06	71,39
Avustralya	Asya&Pasifik	12	75,09	70,38	71,91	86,77	71,30
Kanada	Amerika	13	74,92	73,59	68,71	85,85	71,53
Güney Kore	Asya&Pasifik	14	74,60	65,02	79,60	81,44	72,33
Japonya	Asya&Pasifik	15	73,54	65,55	76,79	77,53	74,29
Yeni Zelanda	Asya&Pasifik	16	73,27	68,44	69,56	86,57	68,49
Fransa	Avrupa	17	73,18	69,52	67,77	82,56	72,85
Avusturya	Avrupa	18	72,92	70,47	69,44	80,04	71,74
İrlanda	Avrupa	19	72,13	72,10	59,17	80,71	76,54
Belçika	Avrupa	20	70,67	69,26	63,80	79,57	70,05

Kaynak: (Dutta & Lanvin, 2020, ss. 31-32; Portulans Institute, 2020)

Tablo, NRI 2020 skoru en yüksek olan yirmi ülkeyi listelemektedir. Bu listede yer alan tüm ülkeler (hatta ilk otuz üç ülke), yüksek gelir grubunda yer almaktadırlar. Listede yer alan ülkelerin yarısından fazlası (13) Avrupa ülkesidir. Ağa ve ağ ekonomisine en hazır ülke olarak listenin başında yer alan İsveç, tek bir alt kategoride dahi listenin başında yer almamasına rağmen, on iki alt kategorinin altısında ilk beşte yer almaktadır. Teknoloji kategorisinde en başarılı ülke İsviçre, insan kategorisinde Danimarka, yönetim kategorisinde Norveç ve etki kategorisinde ise Singapur'dur (Dutta & Lanvin, 2020).

Birleşmiş Milletler Kalkınma Programı (UNDP, 2020) tarafından hazırlanan İnsani Gelişme Raporu da (*Human Development Report*), doğrudan ülkelerin ağ toplumuna entegrasyona ilişkin bir profil sunmasa da diğer dizinler ile karşılaştırma

yapmaya imkân verecek bir tablo sunar. 2020 yılında hazırlanan en güncel raporda, İnsani Gelişme Endeksi (İGE) için doğumda beklenen yaşam süresi, beklenen öğrenim süresi, ortalama öğrenim süresi ve kişi başına düşen milli gelir verileri kullanılır ve ülkeler bu göstergeleri kullanarak yapılan hesaplamalar sonucu elde edilen İGE skorlarına göre sıralanırlar. Aşağıdaki tablo, bu endekste ilk yirmi bir ülkeyi göstermektedir.

Tablo 2.3: En Yüksek İGE Skoruna Sahip 21 Ülke (1990-2019)

Ülke	İGE Sırası	1990	2000	2010	2014	2015	2017	2018	2019
Norveç	1	0,849	0,915	0,940	0,944	0,947	0,954	0,956	0,957
İrlanda	2	0,773	0,867	0,901	0,928	0,935	0,947	0,951	0,955
İsviçre	2	0,840	0,898	0,941	0,942	0,947	0,949	0,955	0,955
Hong Kong	4	0,784	0,830	0,904	0,926	0,930	0,941	0,946	0,949
İzlanda	4	0,807	0,867	0,898	0,931	0,934	0,943	0,946	0,949
Almanya	6	0,808	0,876	0,927	0,937	0,938	0,943	0,946	0,947
İsveç	7	0,821	0,903	0,911	0,935	0,938	0,942	0,943	0,945
Avustralya	8	0,871	0,903	0,930	0,933	0,938	0,941	0,943	0,944
Hollanda	8	0,836	0,882	0,917	0,932	0,934	0,939	0,942	0,944
Danimarka	10	0,806	0,870	0,917	0,935	0,933	0,936	0,939	0,940
Finlandiya	11	0,790	0,864	0,916	0,928	0,930	0,935	0,937	0,938
Singapur	11	0,721	0,821	0,909	0,926	0,931	0,933	0,936	0,938
İngiltere	13	0,781	0,874	0,912	0,925	0,923	0,926	0,928	0,932
Belçika	14	0,813	0,880	0,910	0,918	0,922	0,929	0,930	0,931
Yeni Zelanda	14	0,826	0,876	0,906	0,916	0,921	0,926	0,928	0,931
Kanada	16	0,850	0,867	0,901	0,918	0,921	0,926	0,928	0,929
ABD	17	0,865	0,886	0,916	0,920	0,921	0,924	0,925	0,926
Avusturya	18	0,803	0,847	0,904	0,913	0,915	0,919	0,921	0,922
İsrail	19	0,801	0,861	0,895	0,909	0,910	0,913	0,916	0,919
Japonya	19	0,818	0,858	0,887	0,906	0,908	0,915	0,917	0,919
Lihtenştayn	19	-	0,862	0,904	0,911	0,911	0,916	0,919	0,919

Kaynak: (UNDP, 2020, s. 347)

Tablodaki verilerin hesaplanmasında, mobil telefon aboneliği, internet kullanımı ve kadınların internet kullanımı gibi değişkenler dışında, daha çok sosyo-ekonomik gelişmişlik, eğitim ve ekonomi gibi parametreler ön plandadır. Buna rağmen, İGE'deki ilk 20 ülkenin 17'si yukarıda değinilen NRI'deki ülkeler ile (sıraları farklı olsa da)

aynıdır. Bu açıdan bakıldığında, insani gelişime yönelik verilerin ağa toplumuna entegrasyona ilişkin bir tablo sunacağı ifade edilebilir.

Ağ toplumuna entegrasyon ile ilgili olarak dikkate alınabilecek bir diğer gösterge de ülkelerdeki vatandaşların internet kullanım oranlarıdır. Uluslararası Telekomünikasyon Birliği'nin (ITU) derlediği verilere göre, 2019 itibarıyla dünya nüfusunun yaklaşık yüzde 57'si internet kullanmaktadır (The World Bank, 2021). Hatta Mart 2021 verilerine göre bu oran, yüzde 65 civarındadır (Internet World Stats, 2021). Aşağıdaki tabloda, 2010-2020 yılları arasında nüfusa göre internet kullanım oranı en yüksek olan yirmi ülke yer almaktadır.

Tablo 2.4: Ülkelerin Nüfusuna Göre İnternet Kullanım Oranları (2010-2020)

Ülke	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
BAE	68,0	78,0	85,0	88,0	90,4	90,5	90,6	94,8	98,5	99,1	100,0
Katar	69,0	69,0	69,3	85,3	91,5	92,9	95,1	97,4	99,7	99,7	99,7
Bahreyn	55,0	77,0	88,0	90,0	90,5	93,5	98,0	95,9	98,6	99,7	99,5
Lüksemburg	90,6	90,0	91,9	93,8	94,7	96,4	98,1	97,4	97,1	97,1	98,8
Kuveyt	61,4	65,8	70,5	75,5	78,7	78,0	78,4	98,0	99,6	99,5	98,6
Suudi Arabistan	41,0	47,5	54,0	60,5	64,7	69,6	74,9	94,2	93,3	95,7	97,9
Norveç	93,4	93,5	94,6	95,1	96,3	96,8	97,3	96,4	96,5	98,0	97,0
Danimarka	88,7	89,8	92,3	94,6	96,0	96,3	97,0	97,1	97,3	98,0	96,5
Güney Kore	83,7	83,8	84,1	84,8	87,6	89,9	92,8	95,1	96,0	96,2	96,5
Umman	35,8	48,0	60,0	66,5	70,2	73,5	76,8	80,2	85,5	90,3	95,2
İngiltere	85,0	85,4	87,5	89,8	91,6	92,0	94,8	90,4	90,7	92,5	94,8
İsveç	90,0	92,8	93,2	94,8	92,5	90,6	89,7	93,0	89,2	94,5	94,5
İspanya	65,8	67,1	69,8	71,6	76,2	78,7	80,6	84,6	86,1	90,7	93,2
Hong Kong	72,0	72,2	72,9	74,2	79,9	84,9	87,5	89,4	90,5	91,7	92,4
Finlandiya	86,9	88,7	89,9	91,5	86,5	86,4	87,7	87,5	88,9	89,6	92,2
İrlanda	69,9	74,9	76,9	78,2	83,5	83,5	83,5	84,1	87,0	87,0	92,0
Belçika	75,0	81,6	80,7	82,2	85,0	85,1	86,5	87,7	88,6	90,3	91,5
Hollanda	90,7	91,4	92,9	94,0	91,7	91,7	90,4	93,2	91,9	93,3	91,3
Güney Kıbrıs	53,0	56,9	60,7	65,5	69,3	71,7	75,9	80,7	84,4	86,1	90,8
Slovakya	75,7	74,4	76,7	77,9	80,0	77,6	80,5	81,6	80,4	82,9	89,9

Kaynak: (The World Bank, 2021)

Tablodaki ülkeler, 2020 yılı internet kullanım oranlarına göre sıralanmıştır. Bu tabloda yer alan ülkelerin 12'si NRI'nin ilk yirmisinde yer alan ülkeler ile ve 13'ü de

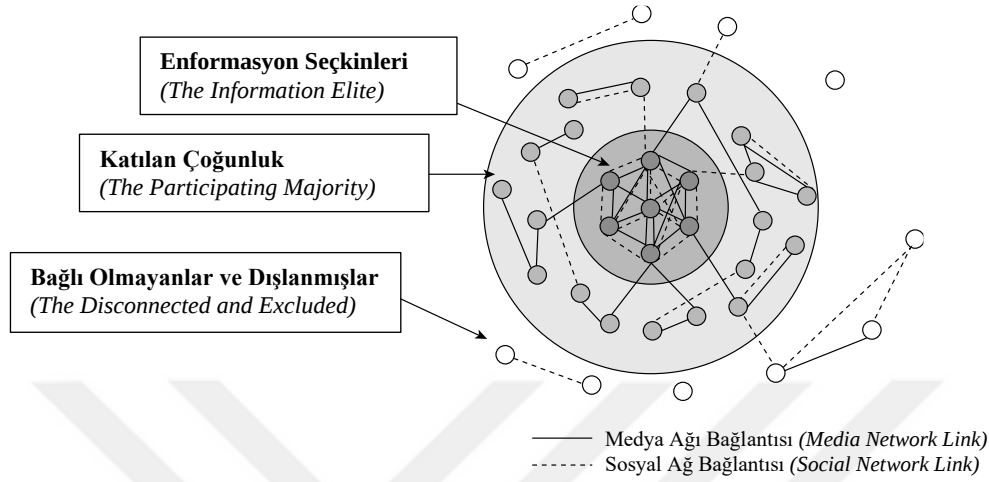
İGE'dekiler ile aynıdır. Listenin ilk üç sırasında yer alan Birleşik Arap Emirlikleri, Katar ve Bahreyn'de yaşayanların neredeyse tamamı internet kullanmaktadır. Bu üç ülke dışında listede yer alan Suudi Arabistan ve Umman, on yıllık periyot içerisinde internet erişim oranlarını neredeyse üç katına çıkarmışlardır. Ancak bu ülkelerin hiçbiri NRI'nin ilk yirmi ülkesi arasında yer almamaktadır. Bu durum, internet erişiminin tek başına yeterli bir gösterge olmadığının bir işaretçisi olarak okunabilir. İnternet ve ilişkili uygulamaların benimsenmesi kullanılması ve bunların giderek çeşitlenmesi, dijital içermeyi (*digital inclusion*) bir sorun olmaktan çıkarır ve kullanım derecesine ve farklı kullanım biçimlerine odaklanan bir sorun haline getirir. Dijital içermenin karmaşıklığı, giderek daha fazla kabul görmektedir (Salemink vd., 2017). Bu durumu açıklamak için ikinci ve üçüncü düzey dijital bölünme kavramına değinmek gereklidir.

Dijital bölünme (*digital divide*), ağ toplumuna entegrasyon kapsamında değinilmesi gereken bir kavramdır. Bu terim, hem enformasyon ve iletişim teknolojilerine (EİT) erişim fırsatları hem de bu teknolojilerin kullanımları açısından farklı sosyo-ekonomik düzeylerdeki bireyler, haneler, işletmeler ve coğrafi alanlar arasındaki farklılığı, uçurumu ifade eder (OECD, 2001). Daha basit bir şekilde nitelendirmek gerekirse dijital bölünme, genel anlamı ile internete erişimdeki eşitsizliğin altını çizer (Castells, 2002). Mobil ve kablosuz iletişim teknolojilerinin yaygınlaşması ve erişilebilir olması ile dijital bölünmenin erişim boyutunun, yüzyılın başına kıyasla küçüldüğü söylenebilir. İnternete erişim kaynaklı bu bölünme, daha sonra birinci düzey dijital bölünme (*first-level digital divide*) şeklinde ifade edilmeye başlanır ve takiben iki düzey daha tanımlanır: ikinci düzey olarak beceri ve kullanım seviyeleri kaynaklı bölünme ve üçüncü düzey olarak internet kullanımının somut sonuçları kaynaklı bölünme (Scheerder vd., 2017). van Dijk, dijital bölünmenin bu farklı düzeylerine vurgu yaparak, ağa entegre olmuş ve ağ toplumuna dönüşen toplumların sahip olduğu yapısal eşitsizliğe değinir.

Kullanım beceriler ve somut çıktılar açısından dijital bölünme ağ toplumlarını, katmanlı bir hale getirir. van Dijk (2017), bu katman yapısının enformasyona “sahip olanlar ve “sahip olmayanlar” kadar basit ve iki katmanlı olmadığını söyler ve ağ toplumunun üç katmandan oluştuğunu savunur. Bu katmanları (1) enformasyon seçkinleri, (2) katılanlar ve (3) dışlanmışlar şeklinde sıralar. Aşağıdaki şekilde, nüfusunun

yaklaşık yüzde 15'ini enformasyon seçkinlerinin oluşturduğu bir (gelişmiş) toplum tasvir edilmektedir.

Şekil 2.1: Ağ Toplumunda Üç Parçalı Katılım



Kaynak: (van Dijk, 2006, s. 186, 2017, s. 286)

Ağ toplumunu oluşturan katmanların en ayrıcalıklısı olan bu kesime dahil olan bireyler, yüksek eğitim ve gelir düzeylerine, en iyi işlere ve toplumsal konumlara sahiptir ve bu kesimin neredeyse tamamı EİT'lere erişim sağlamaktadır. van Dijk, bu seçkinlerin aslında toplumdaki tüm önemli kararları verdiğini, uzaktan stratejik olarak önemli çok sayıda bağa sahip yoğun sosyal ağlarda yaşadıklarını ifade eder (van Dijk, 2006). İkinci ve en kalabalık katman olan katılan çoğunluk, orta ve işçi sınıfından oluşur. Bilgisayar ve internete erişim imkânı olan bu katmandakilerin kullanım becerileri ve kullanım çeşitlilikleri, enformasyon seçkinlerine göre daha azdır. Katılan çoğunluk, interneti kariyer, iş ya da eğitim amaçlarından çok eğlence amacıyla kullanmakta ve daha küçük bir sosyal ağ ile uzak mesafeler ile daha az zayıf bağa sahiptir. Gelişmiş ve teknolojiye erişimi yüksek toplumların dahi yüzde 20'ye yakını oluşturulan dışlanmışlar katmanındaki bireylerin, bilgisayar ve internete erişimi yoktur ve istemli ya da istem dışı olarak toplumun bazı alanlarına katılımdan dışlanmışlardır. Bu katman daha çok en düşük sosyal sınıfları, bazı etnik azınlıkları ve yeni göçmenleri kapsar. Ayrıca bu kesimde, kimi yüksek sosyal statü sahibi, sosyal açıdan kendisini izole etmiş ve bilgisayar ve internet kullanmayan büyük bir yaşlı nüfus da bulunur (van Dijk, 2017).

2.1.3. Kırsal Yerleşimlerde İnternet Erişimi ve Ağ Toplumuna Entegrasyon

Dünya genelindeki kırsal topluluklar, dijital teknolojilerdeki gelişmelere ayak uydurma mücadelesi içindedir. Artan bölgesel eşitsizlikleri önlemek için tüm bölgelerin ve toplulukların internete erişimi olması gerektiği fikrinden hareketle batı toplumları, kırsal telefon ağlarını internet bağlantısına elverişli hale getirmek için, yirminci yüzyılın sonunda hem devlet hem de özel sektör destekli pek çok altyapı yatırımı yapılmıştır (Salemin vd., 2017). Hizmet kalitesinin iyi olduğu büyük ölçüde kentsel alanlar ile hizmetlerin ve altyapının yetersiz olduğu kırsal alanlar arasındaki farkların kırsal dijital bölünmeyi ortaya çıkardığı söylenebilir (Townsend vd., 2013). Kentsel ve kırsal bölgelerdeki bu eşitsizlik, kırsal ceza (*rural penalty*) şeklinde nitelendirilebilir. Kırsal cezanın çeşitli boyutları olmasına rağmen başlıca kaynağı; nüfus yoğunluğunun düşük olmasının neden olduğu düşük pazar yoğunluğudur. Pazar hacminin küçüklüğü enformasyon, işgücü ve diğer kaynaklara uzak kalmayı beraberinde getirir (Malecki, 2003). Her ne kadar, özellikle mobil internet teknolojisinin yaygınlaşması, kırsal bölgelerin internet erişim olanaklarını artırmış olsa da halen erişim kaynaklı bir dijital bölünmeden söz edilebilir (Meachem & Herald-Tribune, 2020; Vogels, 2021).

Uluslararası Telekomünikasyon Birliği'nin (ITU) Dünya Telekomünikasyon/EİT Göstergeleri veri tabanında, kırsal kesimde internet kullanım oranlarına ilişkin on dokuz farklı ülkeye ait istatistik bulunmaktadır. Aşağıdaki tablo, bu ülkelerin kent ve kır nüfuslarının cinsiyete göre internet kullanım oranlarını göstermektedir.

Tablo 2.5: Ülkelerin Cinsiyete Göre Kent-Kır Nüfusu İnternet Kullanım Oranları

Ülke	Tarih	Toplam	Cinsiyet			Kent			Kır	
			E	K	T	E	K	T	E	K
Danimarka	2020	96,5	97,4	95,7	97,6	98,2	97,1	96,0	97,0	95,0
İsrail	2019	86,8	87,5	86,1	86,1	86,9	85,4	95,1	95,5	94,8
İsviçre	2019	93,1	95,1	91,3	93,7	95,9	91,7	91,5	93,1	90,0
Japonya	2019	92,7	94,6	91,0	95,5	96,7	94,3	91,2	93,5	89,0
Estonya	2020	89,1	88,5	89,6	88,7	88,8	88,6	89,8	87,7	92,0
Letonya	2020	88,9	88,2	89,6	90,0	-	-	86,5	-	-
Avustralya	2017	86,5	87,0	86,1	87,0	87,7	86,2	82,8	81,4	85,5
Fransa	2019	83,3	84,6	82,2	83,7	85,1	82,5	82,0	83,1	81,0
Brezilya	2019	73,9	74,4	73,5	74,4	74,3	74,5	69,7	75,0	65,3
Filistin	2019	70,6	72,3	68,9	70,8	72,0	69,5	69,7	73,8	65,5

Ülke	Tarih	Toplam	Cinsiyet			Kent			Kır	
			E	K	T	E	K	T	E	K
Azerbaycan	2019	81,1	84,2	78,0	92,8	98,4	87,4	67,7	68,3	67,1
Dominik Cumhuriyeti	2018	74,8	74,6	75,0	78,1	78,5	77,7	60,5	58,9	62,3
Ermenistan	2019	66,5	65,8	67,2	70,8	70,3	71,1	59,9	59,2	60,7
Yeşil Burun Adaları	2019	61,9	62,9	61,0	69,0	68,9	69,0	47,5	50,5	44,5
El Salvador	2019	50,5	52,4	48,9	59,7	62,4	57,4	35,0	36,1	34,1
Cezayir	2018	49,0	55,1	42,9	56,2	61,7	50,8	34,1	41,9	25,9
Fildişi Sahili	2019	36,3	39,8	32,9	53,6	58,2	49,5	16,1	19,5	12,7
Küba	2019	68,0	60,7	75,1	84,1	76,7	91,1	13,8	12,4	15,5
Mozambik	2017	7,8	9,6	6,1	17,8	21,3	14,6	2,6	3,4	1,8

Kaynak: (ITU, 2020b)

Tabloda yer alan verilerin güncelliği ülkeden ülkeye değişiklik göstermektedir. İnternet erişimi istatistiklerinde, kent-kır ayrımı gözetilen ülke sayısı sınırlıdır. Listede yer alan ülkeler, toplam kırsal internet erişimi oranlarına göre sıralanmıştır. Verilere göre, Danimarka, kırsal nüfusunun internete erişim oranı kent nüfusuna oranla sadece yüzde 1,6 azdır ve kır nüfusunun yaklaşık yüzde 97'si internete erişebilmektedir. Tabloda yer alan on dokuz ülkenin on biri, ağların dışsalılığı kanununa dayanan ağ etkisinin ikinci taşıma noktası olan, toplumun üçte ikisinin ağına katılması (van Dijk, 2017) şartını kırsal nüfus açısından da sağladığı görülmektedir. Aynı zamanda, bu on dokuz ülkenin büyük bir kısmında, kırsal bölgede internet kullanan kadın ve erkekler arasında, erkekler lehine aşağı yukarı yüzde 2'lik bir fark mevcuttur. Kırsal bölgedeki kadınların erkeklerden daha fazla internete erişim sağladığı ülkeler ise Estonya, Avustralya, Dominik Cumhuriyeti, Ermenistan ve Küba'dır. Brezilya, Filistin ve Cezayir kırsal bölgelerinde yaşayan erkeklerin internet kullanım oranları, kadınlara göre en az yüzde 8 daha fazladır.

ITU tarafından sunulan veriler ışığında mobil hücresel ağı dünya nüfusunun neredeyse tamamını kapsadığı söylenebilir. Bu kapsamın yaklaşık yüzde 80'ini de 4G ağlar oluşturmaktadır. Buna rağmen, mobil geniş bant internet ağı açısından kentsel ve kırsal bölgeler arasında halen bir eşitsizlik söz konusudur. Dünyadaki hemen hemen tüm kentsel alanlar bir mobil geniş bant ağı tarafından kapsanırken, birçok kırsal alanda bu hizmete erişim mümkün değildir. Dünya genelindeki kentlerin yüzde 95'i 4G şebekelerin

kapsama alanında iken kırsal bölgelerde bu oran yüzde 71'dir. Kırsal bölgelerin yüzde 13'ü 3G ve yüzde 8'i de 2G şebekelerce kapsamaktadır (ITU, 2020c, s. 5).

Dünya genelinde, kentsel-kırsal bölgede yaşayan bireylerin internete erişim oranları incelendiğinde, bir kırsal cezadan söz edilebilir. Kentte internet erişimi oranı yüzde 72 iken kırdada sadece yüzde 37'dir. İnternet erişiminin yanı sıra bilgisayar erişimi de kent-kır farklılığının belirgin olduğu bir diğer değişkendir. Kentte yaşayan bireylerin bilgisayara erişimi (%63), kırdakilerin (%25) iki katından daha fazladır. Bu oranlar arasındaki fark, gelişmiş ölkelerde kapanırken, gelişmekte olan ölkelerde artmaktadır (ITU, 2020c, s. 6).

Ağ toplumuna entegrasyon başlığında değinildiği gibi, internet ya da materyal erişimi tek başına dijital içirme (*digital inclusion*) ve ağ toplumuna katılım için yeterli göstergeler değildir. Ayrıca kırsal bölgedeki erişim oranlarının, toplum geneli internet erişim oranları kadar yüksek olmadığı da dikkate alındığında, kırsal bölgelerin ağ toplumuna entegrasyonunun özellikle gelişmekte olan ölkelerde henüz tamamlanmadığı söylenebilir. Bu denkleme dijital beceriler değişkeninin eklenmesi, dijital topluma katılımdaki bir diğer engeli de gündeme getirir. Düşük EİT becerileri, dijital topluma anlamlı katılımın önünde bir engeldir (ITU, 2020c). Üstelik bu engel sadece kırsal bölgelerin sorunu değil, tüm toplumu ilgilendiren bir sorundur.

Dijital okuryazarlık ve dijital beceriler konusu, bu bölümün ilerleyen başlıklarında detaylı olarak ele alınmıştır. Ancak dijital bölünmenin ikinci seviyesi olarak değerlendirilen, beceri temelli bölünme açısından kent ve kır nüfusunun beceri seviyelerini, bu başlık altında karşılaştırmak daha uygundur. Avrupa İstatistik Ofisi (Eurostat) tüm AB üyesi ve üye adayı ölkelerden toplanan verileri araştırmacıların kullanımına sunar. Bu veri seti ile bireylerin dijital becerilerini yaş, eğitim seviyesi ve ikamet edilen bölge (kent-kır) gibi parametrelere göre filtreleyerek incelemek mümkündür. Dijital becerilerin düşük (*low*), temel (*basic*) ve temelin üstünde (*above basic*) olarak üç düzeyde listelendiği veriler ölkelere göre kent ve kır nüfusu arasındaki dijital beceri düzeyi farklılıklarını ortaya koyar. Aşağıdaki tabloda, Avrupa ölkelerinde kentlerde ve kırsal bölgelerde yaşayan ve son üç ay içerisinde internet kullanan bireylerin dijital beceri seviyelerine ilişkin oranlar yer alır.

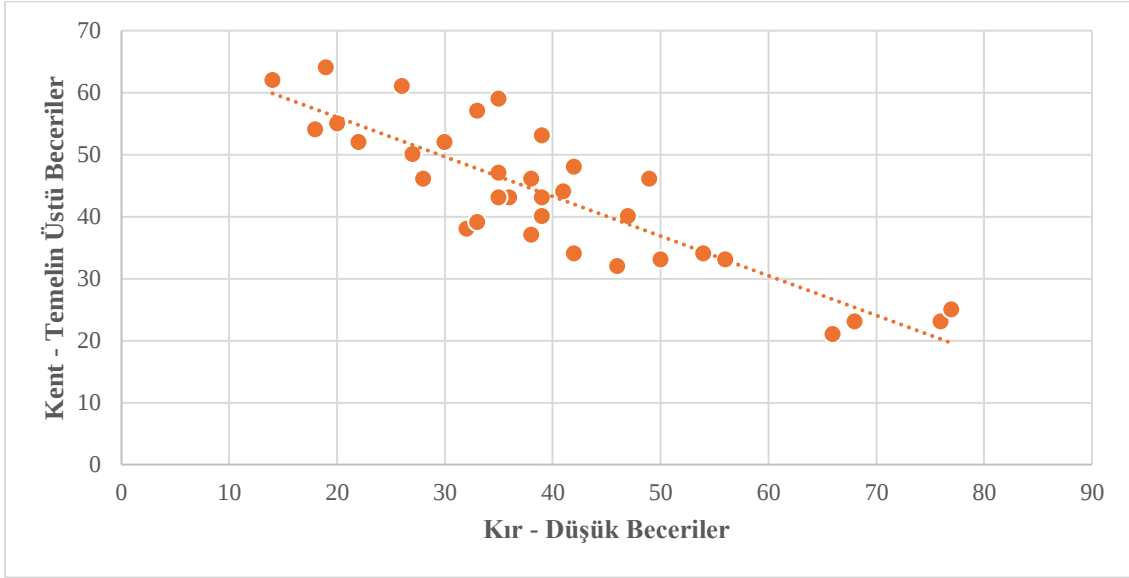
Tablo 2.6: Bazı Avrupa Ülkelerinin Kent-Kır Ayrımına Göre Dijital Becerileri (%)

Ülkeler	Kent				Kır			
	Yok	Düşük Düzey	Temel Düzey	Temelin Üstü	Yok	Düşük Düzey	Temel Düzey	Temelin Üstü
Kosova	4	57	15	25	8	77	7	8
Kuzey Makedonya	0	47	30	23	0	76	12	13
Bulgaristan	0	46	31	23	1	68	20	11
Romanya	-	52	27	21	-	66	26	8
Letonya	1	43	23	33	2	56	22	21
Güney Kıbrıs	1	43	23	34	1	54	23	22
Polonya	1	36	30	33	1	50	26	23
İrlanda	1	31	22	46	2	49	19	30
Macaristan	0	30	30	40	1	47	29	23
İtalya	3	38	28	32	4	46	25	26

Kaynak: (Eurostat, 2021)

Tabloda, ülkelerin farklı bölgelerinde (kent veya kır) yaşayan ve son üç ay içerisinde internete erişim sağlamış olan bireylerin sahip olduğu dijital beceri seviyeleri, yüzdesel olarak gösterilmektedir. Bahsi geçen kitle, toplamda dört farklı beceri düzeyine göre sınıflandırılmıştır: (1) Yok (*no digital skills*); (2) düşük düzey (*low digital skills*), (3) temel düzey (*basic digital skills*) ve (4) temelin üstünde dijital beceriler (*above basic digital skills*). Tabloda yer alan on ülke, kırsal bölgelerinde yaşayan düşük dijital becerilere sahip bireylerinin oranına göre sıralanmıştır. Tablodaki veriler incelendiğinde, ülkelerin kentlerde yaşayan bireyleri, kırlarda yaşayanlara göre daha fazla temel ve temelin üstünde dijital beceriye sahipken kırsal bölgelerde ise düşük düzey dijital beceriye sahip bireylerin oranı daha fazladır. Aşağıdaki grafik, kent ve kırdaki yaşayan internet kullanıcılarının beceri düzeyi farklılıkları arasındaki ilişkiyi göstermektedir.

Şekil 2.2: Kentteki Temelin Üstünde Beceriler ile Kırsaldaki Düşük Beceriler Arasındaki İlişkiyi Gösteren Grafik



Grafikte Kullanılan Veriler: (Eurostat, 2021)

Eurostat veri tabanından elde edilen verilerin, Microsoft Excel for Mac v16'da sunulan araçlar ile analiz edilmesi sonucu elde edilen yukarıdaki grafikte, son üç ayda internet kullanmış olan kentteki temelin üstünde beceriye sahip ve kırdaki düşük beceriye sahip bireylerin oranları arasında yüksek derecede ilişki olduğu görülmektedir. Aynı veriler, kırsal bölgede temelin üzerinde beceriye sahip bireylerdeki artışın, kentte de aynı trendi oluşturduğunu işaret eder. Buradan hareketle, toplumların ağ toplumuna entegrasyonunda, özellikle kırsal bölgelerdeki dijital beceri düzeyini yükseltmenin önemli bir katkı sağlayacağı söylenebilir. Çünkü van Dijk'in (2017) ifade ettiği gibi dijital bölünme, artık erişim boyutunda değil, beceri boyutunda bir sorundur.

2.1.4. Ağ Toplumu Olarak Türkiye

Sağıroğlu ve ekip arkadaşları (2020b, s. 12), gerek araştırmalar gerekse istatistiksel veriler dikkate alındığında, özellikle bilgisayar kullanımı ve hanelerin internet erişimi konusunda yüzde 90'ın üzerindeki oranların, Türkiye'nin dijital çağa entegrasyonu konusunda önemli bir bilgi sunduğunu belirtir. Özellikle mobil internet hizmetinin yaygınlaşması, kapsama alanlarının ve hızının artması Türkiye'de internet erişimini yüzde 82,6 seviyesine getirmiştir (TÜİK, 2021c). Bu oran, ağların dışsallığı kanunu ile ilişkili olarak çalışan ağ etkisinin ikinci taşma noktasının (yaklaşık yüzde 67) (van Dijk, 2017) üzerindedir ve bu etkinin oluşturacağı baskının toplumun geri kalanını

da internete erişime “zorlayacağı” söylenebilir. Aşağıda, Türkiye’nin ağ toplumuna entegrasyonuna ilişkin hem ülke içinden (TÜİK, BTK) hem de uluslararası organizasyonlar tarafından sağlanan istatistiki verilere ve endekslere yer verilmiştir.

Türkiye’de internete erişim sağlayan altyapının temelleri, 1986 yılına dayanır. Her ne kadar internet olarak tanımlanamayacak olsa da Ege Üniversitesi’nin girişimleri ile kurulan TÜVEKA (Türkiye Üniversiteler ve Araştırma Kurumları Ağı) ile Türkiye’deki bazı üniversiteleri birbirleri ve Avrupa’daki bazı araştırma ağları ile ilişkilendirerek ülkedeki internet erişimi altyapısına öncülük etmiştir. Gerçek anlamda ilk internet bağlantısı ise 12 Nisan 1993’te ODTÜ Bilgi İşlem Daire Başkanlığı’ndaki yönlendiriciler kullanılarak, ABD’deki NSFNet’e (*National Science Foundation Network*) TCP/IP protokolü üzerinden gerçekleştirilmiştir (akt. Saka, 2019). O dönemde bu bağlantı, İstanbul Teknik, Boğaziçi, Bilkent, Gazi, Hacettepe gibi üniversite ve çeşitli kamu kuruluşlarına hizmet ediyordu. 1996 yılında Türk Telekom’un TURNET Projesi ile ticari kuruluşların internetten faydalanabilmeleri sağlandı ve ilk internet servis sağlayıcıları ortaya çıktı. Bu servis sağlayıcılar, belirledikleri tarifeler ile vatandaşlara çevirmeli bağlantı ve daha sonrasında ise ADSL ile internet hizmeti sunmaya başladılar (Denizer, 2019). 1999 yılında Türkiye nüfusunun sadece yüzde 2,3’ü internete erişim sağlarken iki yıl içerisinde bu oran yüzde 3,8’e ulaşır (Güngör & Evren, 2002). TÜİK’in internet erişimine ilişkin ilk istatistikleri ise 2004 yılına aittir. Aşağıdaki tabloda, 2004-2021 yılları arasında Türkiye nüfusunun internete erişim sağlama oranları yer alır.

Tablo 2.7: Türkiye’de Bilgisayar Kullanımı ve İnternet Erişimi Oranları

Yıllar	Bilgisayar Kullanımı			İnternet Erişimi		
	TOPLAM	Erkek	Kadın	TOPLAM	Erkek	Kadın
2004	23,6	31,1	16,2	18,8	25,7	12,1
2005	22,9	30,0	15,9	17,6	24,0	11,1
2007	33,4	42,7	23,7	30,1	39,2	20,7
2008	38,0	47,8	28,5	35,9	45,4	26,6
2009	40,1	50,5	30,0	38,1	48,6	28,0
2010	43,2	53,4	33,2	41,6	51,8	31,7
2011	46,4	56,1	36,9	45,0	54,9	35,3
2012	48,7	59,0	38,5	47,4	58,1	37,0
2013	49,9	60,2	39,8	48,9	59,3	38,7

Yıllar	Bilgisayar Kullanımı			İnternet Erişimi		
	TOPLAM	Erkek	Kadın	TOPLAM	Erkek	Kadın
2014	53,5	62,7	44,3	53,8	63,5	44,1
2015	54,8	64,0	45,6	55,9	65,8	46,1
2016	54,9	64,1	45,9	61,2	70,5	51,9
2017	56,6	65,7	47,7	66,8	75,1	58,7
2018	59,6	68,6	50,6	72,9	80,4	65,5
2019	-	-	-	75,3	81,8	68,9
2020	-	-	-	79,0	84,7	73,3
2021	-	-	-	82,6	87,7	77,5

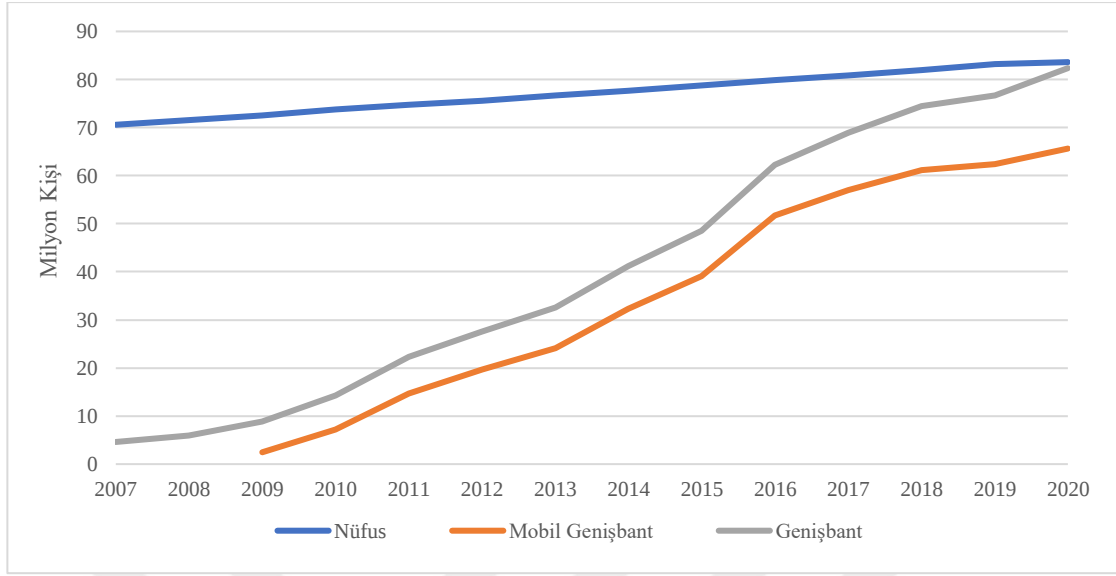
Kaynak: (TÜİK, 2021c)

TÜİK verileri, Türkiye’de internet erişiminin on yedi yıl içerisinde neredeyse dört buçuk kat arttığını gösterir. İnternet erişiminin bir hizmet olarak vatandaşların kullanımına açıldığı 1996 yılından 2004 yılına gelinceye kadar geçen süreçte, Türkiye nüfusunun beşte birinden azının internete erişimi varken sekiz yıl sonra (2012) bu oran yüzde 47’ye ve 2021 itibariyle de yüzde 82,6’ya ulaşmıştır. Hanelerin internet erişimi ise 2004 yılında sadece yüzde 7 iken şimdi yüzde 92’dir. İnternet erişiminde cinsiyetler arasındaki farklar azalsa da halen mevcuttur.

Türkiye’de cep telefonu kullanımı da internet erişimi gibi hızla artan bir diğer bilgi toplumu parametresidir. Ülkedeki cep telefonu aboneliği olan vatandaşların sayısı, 1994 yılında yaklaşık 81 bindir. 2011 yılında 65 milyonu bulan abone sayıları (TÜİK, 2012, s. 434), 2015 yılında 73,5 milyonu ve 2020 yılında da 82 milyonu aşmıştır (BTK, 2021).

Cep telefonu kullanımının yaygınlığı, beraberinde mobil internet hizmeti kullanımını da getirir. Mobil ve kablosuz teknolojilerdeki gelişmelerin, “ağ toplumunu dünyadaki en uzak yerlere ve en derin deliklere doğru” (van Dijk, 2017, ss. 88-89) yayacağı söylenebilir. Türkiye’deki veriler de mobil internet hizmetinin vatandaşların kullanımına sunulması ile nüfusun genelindeki internet erişimini arttığını gösterir. Bilgi Teknolojileri ve İletişim Kurumu’nun (BTK) yayınladığı yıllık istatistik bültenlerine göre, ilk mobil internet abonelikleri 2009 yılında gerçekleşmiştir. O yıl sadece yaklaşık 2,5 milyon kişi mobil internet kullanmaktadır (BTK, 2014). 2020 yılında Türkiye’deki mobil geniş bant internet abonesi sayısı 65,5 milyonu aşmıştır (BTK, 2021).

Şekil 2.3: Geniş Bant ve Mobil Geniş Bant İnternet Abonelikleri

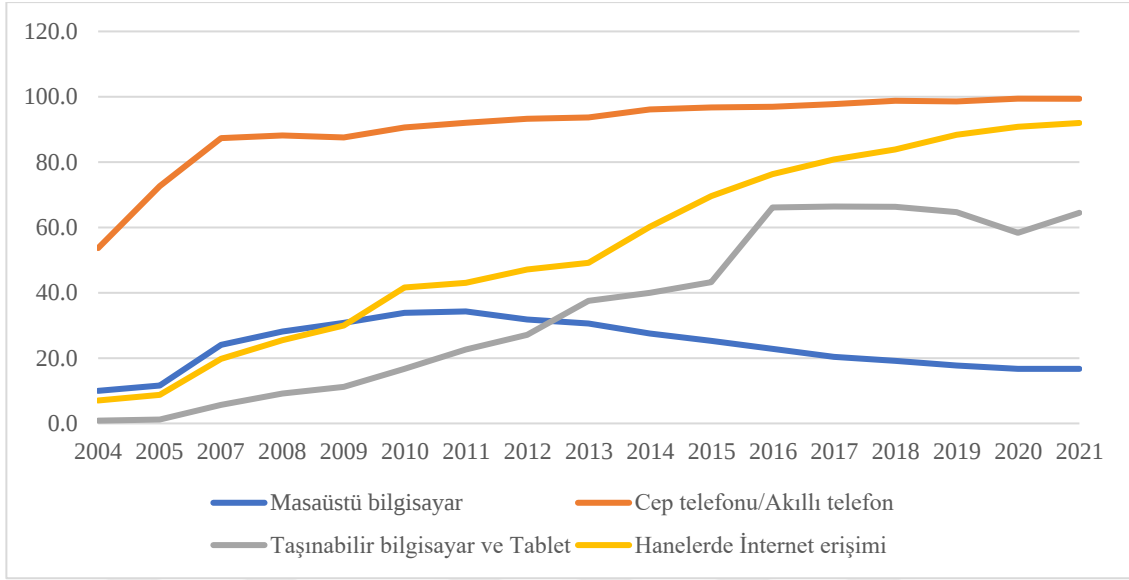


Grafikte Kullanılan Veriler: (BTK, 2013, 2014, 2015, 2021)

Yukarıdaki grafik, mobil geniş bant internet hizmetinin Türkiye’deki toplam geniş bant internet abonelikleri ile benzer bir oranda arttığını gösterir. Türkiye’deki yaklaşık 82,3 milyon geniş bant internet abonesinin 65,6 milyonu mobil internet abonelerinden oluşmaktadır (BTK, 2021). Bu veriler, Türkiye’deki bireylerin internet kullanımının büyük oranda mobil cihazlar üzerinden gerçekleştiğini işaret eder.

Hanelerin yüzde 92’sinin internete erişimi olduğu Türkiye’de, enformasyon ve iletişim teknolojilerinin hanelerdeki bulunma oranları da ağ toplumu kapsamında incelenebilir. Masaüstü bilgisayar sahipliği; 2004’te yüzde 10, 2011’de ise yüzde 34,3’tür. Bu tarihten itibaren düşüş eğilimi gösteren masaüstü bilgisayar sahipliği, 2021 yılında sadece yüzde 16,8’dir (TÜİK, 2021c). Aşağıdaki grafik, hanelerdeki internet erişimi ile cep telefonu, masaüstü ve taşınabilir bilgisayar bulunma oranlarını göstermektedir.

Şekil 2.4: Yıllara Göre Hanelerdeki EİT Teknolojileri Bulunma Oranları



Grafikte Kullanılan Veriler: (TÜİK, 2021c)

Grafiğe dayanarak, Türkiye’deki neredeyse tüm hanelerde cep telefonu ya da akıllı telefon bulunduğu söylenebilir. Masaüstü bilgisayar sahipliği üstünlüğünü 2012 sonrasında taşınabilir bilgisayar ve tabletlere bırakmıştır. Hanehalkı Bilişim Teknolojileri (BT) Kullanım Araştırması’ndaki veriler aynı zamanda, bireysel olarak cep telefonu kullanım oranının 2021 yılında yüzde 96’ya (erkek %98,3 – kadın %93,7) ulaştığını gösterir (TÜİK, 2021c).

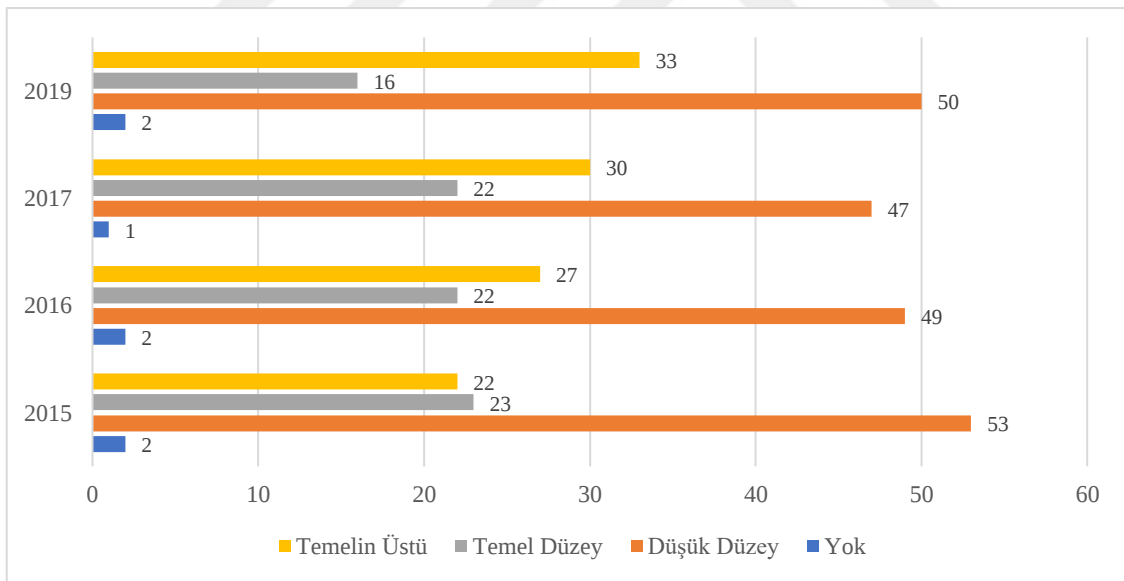
Ağ toplumu ve kitle toplumu ayırımında, hanehalkı genişliklerini de değerlendiren van Dijk’e göre (2017), kitle toplumlarında hanehalkı geniş aileyle büyük, ağ toplumlarında ise çeşitli aile ilişkileriyle küçüktür. Buna bağlı olarak temel iletişim türü de ilkinde yüz yüze, ikincisinde ise artan biçimde EİT’ler ile dolayımlandırılmıştır. Bu yaklaşımdan hareketle, Türkiye’yi bir ağ toplumu olarak değerlendirmek için hanehalkı büyüklüğü istatistiklerine başvurulabilir. Bu veriler, 2008 yılında 4 olan ortalama hanehalkı büyüklüğünün, on iki yıl içerisinde 3,30’a gerilediğini ve 2014 yılında yüzde 13,9 olan yalnız yaşayan fertlerden oluşan tek kişilik hanehalklarının oranının 2020 yılında yüzde 17,9’a yükseldiğini gösterir (TÜİK, 2021b).

Dünya genelindeki 41 şehrin, EİT olgunluğuna ve sürdürülebilir kentsel gelişimdeki performanslarına göre sıralandığı Networked Society City Index’te yer bulan İstanbul, son iki ölçüm döneminde beş sıra yükselir. 2014 yılında 27. Sırada olan şehir 2016’da 22. sıraya yükselmiştir (Networked Society Lab, 2016). Bir diğer uluslararası

endeks olan Network Readiness Index'te ise Türkiye, 57. sırada yer almaktadır. Bu endekste kullanılan göstergelerden EİT becerilerinde 111. ve internet kullanımındaki cinsiyet eşitsizliğinde 81. sırada yer alan Türkiye, e-ticaret mevzuatı göstergesinde ise ilk sırada yer alır (Dutta & Lanvin, 2020).

Hem TÜİK ve BTK'nın hem de uluslararası organizasyonların sağladığı istatistiki veriler dikkate alındığında, Türkiye'deki erişim temelli dijital bölünmenin büyük oranda kapandığı söylenebilir. Türkiye'deki bireylerin yüzde 82'den fazlasının internete erişimi ve yüzde 96'dan fazlasının ise cep telefonu vardır. EİT'lere erişimin yaygınlaşması, erişim temelli dijital bölünmeyi birleştirse de ikinci düzey ve kullanım becerilerinden kaynaklanan dijital bölünmeyi beraberinde getirir. Eurostat verileri, Türkiye'de son üç ay içerisinde internet kullanan bireylerin dijital beceri düzeylerine ilişkin istatistikler sağlar. Aşağıdaki grafikte, 2015-2019 yılları arasındaki dijital beceri düzeyi oranları yer almaktadır.

Şekil 2.5: Türkiye'de Son Üç Ay İçerisinde İnternet Kullanan Bireylerin Dijital Beceri Düzeyleri

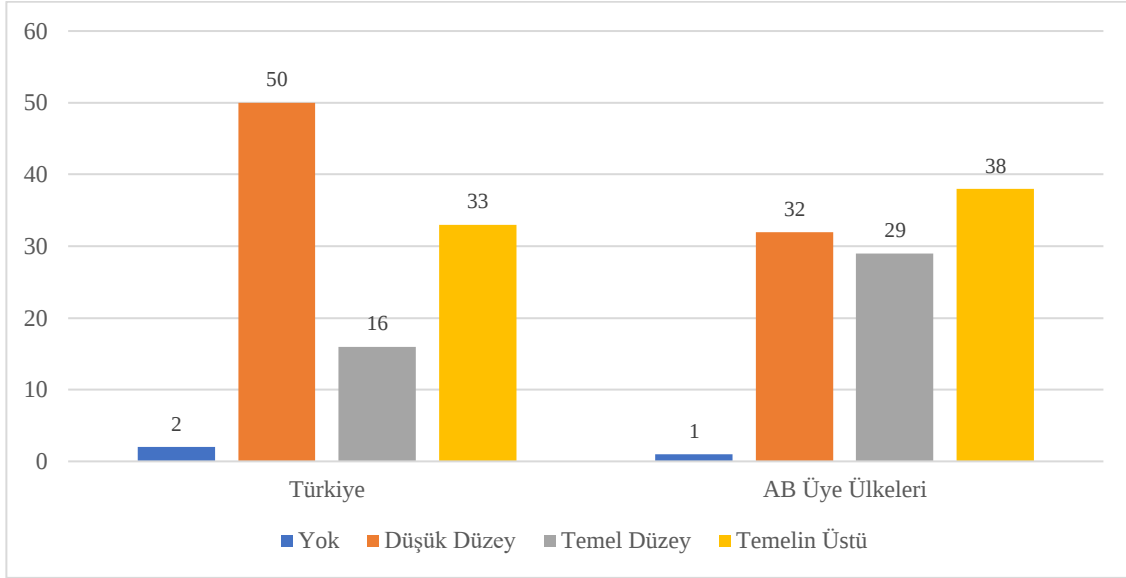


Grafikte Kullanılan Veriler: (Eurostat, 2021)

Yukarıdaki grafik, Türkiye'de internet kullanan bireylerin yarısının, sadece düşük düzey dijital becerileri olduğunu, yüzde 2'sinin de hiçbir dijital becerisi olmadığını göstermektedir. Her ne kadar temelin üzerinde becerilere sahip olan bireylerde yüzde 11'lik bir artış söz konusu olsa da düşük becerilere sahip bireylerin oranı, halen yüzde 50

civarındadır. Aşağıdaki grafik ise, 2019 yılında Türkiye ve AB üye ülkeleri ortalamalarını karşılaştırmaktadır.

Şekil 2.6: Türkiye ve AB Ülkelerinde Son Üç Ay İçerisinde İnternet Kullanan Bireylerin Dijital Beceri Düzeyleri (2019)



Grafikte Kullanılan Veriler: (Eurostat, 2021)

Grafığe dayanarak, Türkiye’deki internet kullanıcılarının, AB ülkelerindekilere göre daha düşük dijital becerilere sahip olduğu söylenebilir. Bu farklılıklar yaş ve eğitim düzeyi değişkenleri ile daha da belirginleşmektedir.

Türkiye’nin ağ toplumuna entegrasyonu için büyük oranda kapanan erişim temelli dijital bölünmeden sonra, yukarıdaki istatistik, grafik ve tablolarda gösterilen verilerin de işaret ettiği gibi, beceri temelli dijital bölünmeyi çözecek politikalara ihtiyaç duyduğu söylenebilir. Aşağıdaki başlıkta, bu bağlamda değerlendirilebilecek kavramlar olan dijital vatandaşlık, dijital okuryazarlık ve dijital beceriler, yetkinlikler konularına değinilmiştir.

2.2. Dijital Vatandaşlık

Genel olarak, bireyler ile ulus devletler arasındaki ilişki olarak kavramsallaştırılan vatandaşlık, olaylar ve durumlar hakkında kitle iletişim araçları aracılığıyla bilgilendirilen ve seçim süreçlerine katılmakla yükümlü olan “görevli vatandaş” kavramlarına dayanır (Bennett, 2008; Pangrazio & Sefton-Green, 2021). Başka bir ifade ile bir ülkeye vatandaşlık bağı ile bağlı olarak, devletin anayasada tanımladığı haklardan yararlanabilen bireylere vatandaş denir. Günümüzde internet teknolojilerinin gelişmesiyle vatandaşlık kavramının değiştiği söylenebilir (Çubukcu & Bayzan, 2013).

Siber topluluklara erişimde dijital teknolojilerden yararlanılması, dijital vatandaşlık kavramını gündeme getirir (Elçiçek vd., 2018). Mancini'ye göre (1999) internetin siyasal iletişim alanına giriş yapması ile birlikte gündeme gelen dijital vatandaş, siyasi partilerin arabuluculuğunu atlayarak ve partilerin rolünü daha da zayıflatarak vatandaşlar, liderler ve yetkililer arasındaki doğrudan etkileşim olasılığını şekillendirir.

Dijital vatandaşlık; hem devlet portallarını, sosyal ağ ve çevrim içi alışveriş sitelerini birer eyalet ya da imparatorlukmuş gibi kabul ederek bu oluşumlar içerisinde bireylerin çeşitli rollere ve işlevlere sahip oluşuna hem de yeni ve değişen seçim sistemleri ve sivil forumlar yoluyla klasik geleneksel vatandaşlık eylemlerinin dönüşümüne atıfta bulunur (Pangrazio & Sefton-Green, 2021). Isin ve Ruppert da (2020) dijital vatandaşların, ortaya koydukları dijital eylemlerle ortaya çıktığını ifade ederler. Lyon'a (2018) göre ise dijital vatandaşlar, işlerin yapıldığı aracın internet olduğu her yerde karşımıza çıkarlar.

En açık ve sade ifadesi ile dijital vatandaşlık; topluma çevrim içi katılma yeteneği olarak tanımlanabilir ve sosyal içermeye (*social inclusion*) için bir ön koşul olarak değerlendirilebilir (Mossberger vd., 2008). Mossberger'e göre (2009); çevrim içi topluma katılım, bilgi teknolojisine düzenli erişimi ve teknolojinin etkin kullanımını gerektirir. Başka bir ifade ile dijital vatandaşlar, interneti her gün kullananlardır. Kavram, dijital içeriği yorumlayarak, anlayarak ve güvenilirliğini değerlendirerek; uygun araçlarla üreterek, araştırarak ve iletişim kurarak; dijital dünyanın etik fırsatları ve zorlukları hakkında eleştirel düşünerek ve çevrim içi olarak güvenli, sorumlu, saygılı seçimler yaparak teknolojiyi yetkin bir şekilde kullanma yeteneği olarak da tanımlanabilir (Çubukcu & Bayzan, 2013; Isman & Canan Gungoren, 2014). Bu bağlamda dijital vatandaşlık, vatandaşların dijital araçları kullanmaları ve çeşitli dijital ortamlarda çalışabilmeleri için gerekli nitelikleri kapsar (Searson vd., 2015). Bu açıdan bakıldığında dijital vatandaş, geniş bir yetkinlik yelpazesinin geliştirilmesi yoluyla, yerel, ulusal veya küresel boyuttaki hem çevrim içi hem de çevrim dışı topluluklara aktif, olumlu ve sorumlu bir şekilde katılabilen kişidir (Richardson & Milovidov, 2019). Bazı araştırmacılar da dijital vatandaşlığa, internete özgü yetenekler ve öz yeterlilik açısından yaklaşır. Bu açıdan, dijital vatandaşlığın temel yetkinliği olarak başkalarıyla iş birliği yapma ve iletişim kurma becerisinin internet öz-yeterliliği ve bilgi okuryazarlığı ile doğrudan ilişkili olduğu söylenebilir (Kim & Choi, 2018).

Ribble ve Bailey (2007), dijital vatandaşlığın teknoloji kullanımına ilişkin uygun, sorumlu davranış normları olarak tanımlanabileceğini ifade ederler ve dijital vatandaşlık ve teknoloji kullanımı, istismarı ve kötüye kullanımı konularının karmaşıklığını anlamının bir yolu olarak, dijital vatandaşlığı oluşturan dokuz unsur belirlerler. Tanımı, daha somut ve işlevsel hale getiren bu dokuz unsur, dijital vatandaşlık için bir çerçeve sağlar (Erdem & Koçyiğit, 2019).

Ribble ve Bailey'nin dijital vatandaşlık çerçevesini oluşturan dokuz unsur ve bu unsurların dahil olduğu üç kategori şu şekilde sıralanır (Öztürk, 2021):

- Kendine ve diğer insanlara saygı (*respect for self and other people*)
 - Dijital erişim (*digital access*)
 - Dijital görgü kuralları (*digital etiquette*)
 - Dijital hukuk (*digital law*)
- Kendini eğitime ve diğer insanlarla bağlantı kurma (*self-education and connecting with other people*)
 - Dijital iletişim (*digital communication*)
 - Dijital okuryazarlık (*digital literacy*)
 - Dijital ticaret (*digital commerce*)
- Kendini ve diğer insanları koruma (*protecting self and other people*)
 - Dijital haklar ve sorumluluklar (*digital rights and responsibilities*)
 - Dijital sağlık ve zindelik (*digital health and wellness*)
 - Dijital güvenlik (*digital security*)

Dijital katılım, topluma tam elektronik katılıma, dijital ticaret mal ve hizmetlerin çevrim içi alım-satımına ve dijital iletişim de elektronik olarak bireyler arasında enformasyon alışverişine vurgu yapar. Ribble ve Bailey, dijital vatandaşlığın bir bileşeni olarak dijital okuryazarlığı, dijital teknolojileri kullanma kapasitesi ve bu teknolojileri ne zaman ve nasıl kullanacağını bilme şeklinde tanımlarlar. Dijital görgü kuralları, dijital teknoloji kullanıcılarının diğer kullanıcılardan bekledikleri davranış standartları olarak ifade edilebilir. Dijital hukuk, teknoloji kullanımını yöneten yasal hak ve kısıtlamaları; dijital hak ve sorumluluklar ise, tüm dijital teknoloji kullanıcılarına tanınan ayrıcalıklar ve özgürlükler ve bunlarla birlikte gelen davranışsal beklentileri kapsar. Dijital sağlık ve zindelik bileşeni, fiziksel ve psikolojik iyi olma halinin dijital teknoloji kullanımına ilişkin unsurlarına; dijital güvenlik bileşeni ise, tüm teknoloji kullanıcılarının kişisel

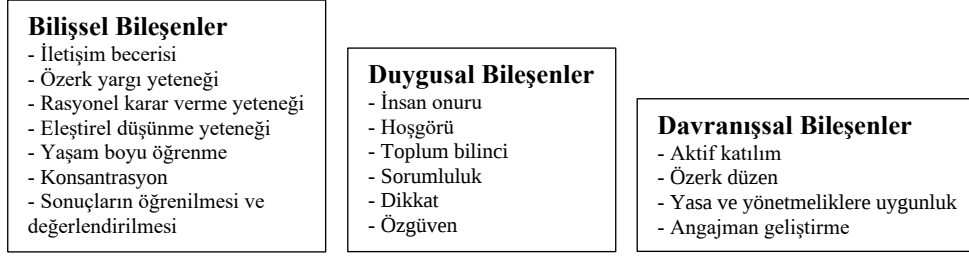
güvenliklerini ve ağlarının güvenliğini garanti altına almak için alması gereken önleme vurgu yapar (Ribble, 2012).

Alberta Education tarafından hazırlanan raporda, dijital vatandaşlık konusuna ilişkin eğitim politikalarının geliştirilmesi için Ribble ve Bailey'nin dokuz bileşenine, özellikle mobil internet teknolojisi ve bulut bilişimdeki gelişmeler dikkate alınarak, iki bileşen daha eklenmesi önerilir: (1) bulut bilişim (*cloud computing*) ve (2) kişisel olarak sahip olunan cihazlar (*personally owned devices*). Bulut bilişim, verileri depolamak, yönetmek ve işlemek için internet üzerinden uzak sunucuların kullanılmasını ifade eder. Bulut bilişimin kullanımı oldukça kolay olsa da işleyişindeki detayları anlamak oldukça zordur. Kişisel olarak sahip olunan cihazlar ya da kendi cihazını yanında getir bileşeni ise öğrencilerin kendilerine ait ve sürekli erişime sahip oldukları EİT'leri okullarına getirmeleri ve bu cihazların kendi eğitimleri için uyarlanmasını kapsar (Alberta Education, 2012).

Jones ve Mitchell (2016), Ribble ve Bailey'den farklı olarak dijital okuryazarlık eğitimi ve siber zorbalığın önlenmesi konusunu dijital vatandaşlık eğitiminden ayrı tutmayı önerirler ve dijital vatandaşlık eğitiminin gençlerin (1) başkalarına karşı saygılı ve hoşgörülü davranışlar sergilemesini ve (2) sivil katılım faaliyetlerini artırmak için internet kaynaklarını kullanmasını sağlamaya odaklanması gerektiğini belirtirler. Araştırmacılar, bu iki hedefi dikkate alarak dijital okuryazarlığı, “saygılı, hoşgörülü çevrim içi davranış ve çevrim içi sivil katılım faaliyetlerinin bir kombinasyonu (örneğin, topluluğa veya diğer gençlere yardımcı olacak bilgi bulma; becerileri paylaşma)” şeklinde tanımlarlar (L. M. Jones & Mitchell, 2016, s. 2073).

MINDtheGaps (2021) adlı Erasmus+ projesi kapsamında hazırlanan el kitabında, gençlerin dijital vatandaş olarak eğitilmesine odaklanılır ve kavramın çok boyutluluğuna vurgu yapılır. Kitapta dijital vatandaşlık için üç boyut on yedi bileşenden oluşan bir konsept önerilir.

Şekil 2.7: Dijital Vatandaşlık Boyutları



Kaynak: (MINDtheGaps, 2021)

International Society for Technology in Education kuruluşunun; öğrenme, öğretme ve liderlikte yenilik ve mükemmellik için bir çerçeve görevi gören ISTE Standartları; öğrencilerin sahip olması gereken dijital vatandaşlık yetkinliklerine de değinir. Bu standartlara göre öğrenciler, dijital dünyada yaşamanın, öğrenmenin ve çalışmanın getirdiği hak, yükümlülük ve olanakları bilirler; güvenli, yasal ve etik biçimde davranırlar ve bu tür davranışlara örnek olurlar. Öğrenciler ayrıca (1) kendi dijital kimliklerine ve itibarlarına sahip çıkarlar ve dijital dünyada yaptıklarının kalıcı olduğunun bilincinde olurlar; (2) çevrim içi sosyal iletişim sırasında ve ağdaki cihazları kullanırken olumlu, güvenli, yasal ve etik davranış sergilerler; (3) fikri mülkiyetin anlamını kavrarlar ve başkalarının fikir ürünlerini kullanırken ve paylaşırken fikir haklarına karşı yükümlülüklerinin bilincinde olurlar ve (4) kendi verilerini, dijital mahremiyeti ve güvenliğini koruyacak şekilde düzenlerler ve çevrim içi işlemleri izlemek için kullanılan veri toplama teknolojisinin bilincinde olurlar (ISTE, 2018).

Greenhow ve Robelia (2009), literatürdeki tanımlar ışığında, dijital vatandaşlığı uygulama becerilerinin, sosyal ve politik konulardaki farkındalıkları geliştirmeyi ve kamusal hayata çevrim içi katılımı içerdiğini belirtirler. Araştırmacılar; kaliteli çevrim içi katılımın, gizlilik ayarlarını yaparak, yasal bir şekilde müzik ve diğer medya dosyalarını indirerek, sosyal ağları güvenli bir şekilde kullanarak, çevrim içi topluluklara saygılı mesajlar göndererek ve başkalarını sorumlu çevrim içi davranışlar sergilemeye teşvik ederek dijital ortak alanlarda kendisinin ve başkalarının haklarına ve sorumluluklarına saygı göstermeyi gerektirdiğini ifade ederler. Avrupa Konseyi için hazırlanan dijital vatandaşlık eğitimi el kitabında ise dijital vatandaşlık ve dijital etkileşimin “yaratma, tüketme, paylaşma, oynama ve sosyalleşmeden araştırma, iletişim kurma, öğrenme ve çalışmaya kadar çok çeşitli faaliyetleri” içerdiği ve yetkin dijital vatandaşların; “öğrenme, çalışma, istihdam edilebilirlik, boş zaman, topluma dahil olma ve topluma katılım ile ilgili

yeni ve günlük zorluklara, insan haklarına ve kültürlerarası farklılıklara” saygı göstererek karşı koyabilecekleri ifade edilir (Richardson & Milovidov, 2019, ss. 10-11).

Ağ toplumlarında bireyler, dijital teknolojilerin aracılık ettiği bir dünyada yaşamaktadırlar ve bu toplumlarda bireylerin dijital vatandaş olması, vatandaşlık haklarından yararlanabilmeleri açısından önemlidir. Günümüz toplumunda sadece dijital araçları kullanmak değil, dijital dünyanın içinde var olmak esastır (Karakuş Yılmaz, 2020). Çağdaş kültüre tam katılım, sadece medya mesajlarını tüketmeyi değil, aynı zamanda onları üretmeyi ve paylaşmayı da gerektirir. Bireylerin dijital vatandaşlık vaadini yerine getirebilmeleri için dili, grafik tasarımı, görüntüleri ve sesleri kullanarak mesaj oluşturma becerisini içeren multimedya iletişim becerileri edinmeleri ve bu becerileri, topluluklarının sivil yaşamına katılmak için nasıl kullanacaklarını bilmeleri gerekir (Hobbs, 2010). Bu gereklilikler, dijital okuryazarlık ile ilişkilidir. Dijital vatandaşlık, düzenli ve etkin internet erişimi ile teknolojiyi kullanma becerisi gerektirir (Mossberger vd., 2012). Bu bağlamda, dijital vatandaş olabilmek ve dijital haklarını talep edip koruyabilmek için bireyin dijital okuryazar olmasının en temel gereklilik olduğu söylenebilir. Çünkü bireyler, dijital okuryazar değilse dijital haklarını talep edemez ve topluma katılamazlar (Pangrazio & Sefton-Green, 2021). Bir sonraki başlıkta, dijital vatandaş olmak için edinilmesi gereken dijital okuryazarlık yetkinliği ele alınmıştır.

2.3. Dijital Okuryazarlık

Ağ toplumunda yaşayan dijital vatandaşların, bu ekosistem içerisinde birey olabilmeleri ve temel haklarını talep edip kullanabilmeleri için dijital ortam ve platformları etkin kullanması, risk ve fırsatların farkında olması, dijital ortamlarda karşılaşabileceği tehlikelerden kendini koruması, etik davranması ve bu ortamlar içinde üretme, pazarlama, paylaşma, öğrenme, yaşama ve tüketme gibi yeteneklere sahip olması gereklidir. Tüm bu gereklilikler ise dijital okuryazarlık ile ilişkilidir (Sağıroğlu vd., 2020b). Kavram, ilk olarak Paul Gilster tarafından önerilmiştir (Üstündağ vd., 2017). Gilster (1997) dijital okuryazarlığı kısaca, ağa bağlı bilgisayar kaynaklarına erişme ve bunları kullanma yeteneği olarak tanımlar. Hobbs ve Coiro (2019) dijital okuryazarlığı, günlük yaşamın bir parçası olan enformasyon ve iletişim teknolojilerinde süregelen değişikliklere yanıt veren, genişletilmiş bir okuryazarlık kavramsallaştırması olarak görürler. En basit ifadesi ile ise dijital okuryazarlık, bireyin dijital çağda hayatta kalma becerisidir (Eshet-Alkalai, 2004).

Dijital okuryazarlık, giderek dijitalleşen bir kültürde yaşayanlar için önemli bir yetkinliktir. Dijital okuryazarlık, bireylere sosyal, kültürel, ekonomik ve entelektüel yaşamda aktif rol almalarına yardımcı olacak beceri, bilgi ve anlayışı kazandırır. Bu beceriler, farklı biçim ve formatlarda anlam oluşturma ve paylaşma, etkili bir şekilde üretme, iş birliği yapma ve iletişim kurma yeteneği ve dijital teknolojilerin bu süreçleri desteklemek için en iyi nasıl ve ne zaman kullanılabileceğini anlama olarak sıralanabilir (Hague & Payton, 2010). Hindistan Bilgisayar Okuryazarlığı Misyonu (ICSM) tarafından yapılan tanım, dijital okuryazarlık ile ilgili daha somut beceriler ortaya koyar. ICSM'ye göre dijital okuryazarlık, bir kişinin bilgisayar, tablet, akıllı telefon gibi dijital cihazları kullanma ve e-posta gönderip alma, internette gezinme, devlet hizmetlerini alma, yeni bilgiler edinme ve çevrim içi işlemler yapma yeteneğidir (akt. Mahapatra, 2020). Slovenya Hükümeti tarafından 2016 yılında yayınlanan strateji raporunda ise dijital okuryazarlık, dijital topluma katılım için bir ön koşul olarak kabul edilmiş ve yalnızca dijital okuryazar veya e-yetkin vatandaşların tam olarak dijital iletişim kurabileceği, modern EİT'leri kullanabileceği, farklı yaşam koşulları için yeni beceriler geliştirebileceği, yenilikçi ve yaratıcı olabileceği belirtilmiştir (Republic of Slovenia, 2016). İngiltere'de yayınlanan bir raporda ise dijital okuryazarlık, “sorunları çözmek, yenilikçi projeler üretmek, iletişimi geliştirmek ve dijital dünyanın zorluklarına hazırlanmak için dijital araçları kullanma gücü” olarak tanımlanmıştır (THE Consultancy, 2021).

Lankshear ve Knobel (2015), dijital okuryazarlık tanımlamalarının iki ana tür altında değerlendirilebileceğini söyler. Bunlar (1) kavramsal tanımlar ve (2) dijital okuryazarlığı ulusal ve uluslararası boyutta standart hale getirmeye yönelik standardize edilmiş işlem kümeleridir. Paul Gilster'in; “bilgisayar tarafından transfer edilebilen bilgileri anlama ve daha da önemlisi bu bilgileri değerlendirme ve çeşitli formatlara entegre etme becerisi” tanımı (Pool, 1997), kavramsal tanımlar kategorisinde yer alır. Standardize edilmiş işlemler olarak dijital okuryazarlık tanımları, belirli görevler, performanslar, becerilerin gösterimi vb. açısından dijital okuryazar olmanın içerdiği şeyleri işlevselleştirme ve bunları genel kabul için standart bir set haline getirme girişimlerine atıfta bulunur (Lankshear & Knobel, 2015). Bu türdeki tanımların, bilgisayar okuryazarlığı, enformasyon ve iletişim teknolojileri okuryazarlığı tanımlamaları ile örtüştüğü ve dijital okuryazarlık tanımı ile tam olarak örtüşmediği

söylenabilir. Gilster'in (1997) ifade ettiği gibi, dijital okuryazar olmak, sadece "tuş vuruşlarında (*keystrokes*) değil fikirlerde ustalaşmayı" ve uyanık, dikkatli ve ihtiyatlı olmayı (*wariness*) gerektirir. Pietraß da (2009) hümanist ve işlevsel kavram ayrımına vurgu yapar ve sadece tekniğe dayalı ve fonksiyonel dijital okuryazarlık kavramsallaştırmalarının, sanal topluma başarılı bir şekilde katılım için gereken kapasitelerin anlaşılmasını zorlaştırdığını belirtir. İşlevsel olmayan bir bakış açısından dijital okuryazarlık kavramsallaştırması, (1) araca değil kullanıcıya odaklanmayı, (2) tüketen bir kullanımdan daha üretken bir kullanıma geçişi hesaba katmayı ve (3) uygulayıcılar tarafından kullanılabilme potansiyeline sahip olmayı gerektirir (Pietraß, 2009, s. 140).

DigEuLit adlı Avrupa Birliği projesi, kapsamlı bir dijital okuryazarlık çerçevesini literatüre kazandırmıştır. Bu çerçeveye göre dijital okuryazarlık:

- i. *İş, öğrenme, boş zaman ve günlük yaşamın diğer yönlerini kapsayan yaşam durumlarına gömülü başarılı dijital eylemleri gerçekleştirebilmeyi içerir;*
- ii. *Birey için kendi özel yaşam durumuna göre değişebilen ve ayrıca bireyin yaşam durumu geliştikçe gelişen, yaşam boyu devam eden bir süreçtir;*
- iii. *EİT okuryazarlığından (ICT literacy) daha geniştir ve bilgi okuryazarlığı, medya okuryazarlığı ve görsel okuryazarlık gibi birkaç ilgili "okuryazarlıktan" alınan unsurları içerir;*
- iv. *Bilgi, teknik, tutum ve kişisel niteliklerin edinilmesini ve kullanılmasını, yaşam görevlerinin çözümünde dijital eylemleri planlama, yürütme ve değerlendirme yeteneğini ve kişinin kendi dijital okuryazarlık gelişimini yansıtmaya yeteneğini içerir (Martin, 2005).*

Projedeki araştırmacılar, dijital okuryazarlığın kapsamını belirleyen çerçeve ile literatürdeki diğer tanım ve nitelendirmeleri de dikkate alarak şu tanımları yaparlar:

Dijital okuryazarlık, bireylerin dijital araçları ve imkanları, dijital kaynakları tanımlamak, erişmek, yönetmek, entegre etmek, değerlendirmek, analiz etmek ve sentezlemek; yeni bilgiler edinmek, medya ifadeleri oluşturmak ve diğer bireylerle çeşitli yaşam durumları içerisinde, yapıcı sosyal eylemi mümkün kılmak ve bu süreci yansıtmak için iletişim kurmak amacıyla uygun şekilde

kullanma farkındalığı, tutumu ve yeteneğidir (Martin & Grudziecki, 2006, s. 255).

Rene Hobbs (2010), Aspen Institute ve John S. and James L. Knight Foundation için hazırladığı raporda, dijital ‘medya’ okuryazarlığı kavramını kullanır ve kavramı oldukça kapsayıcı bir şekilde ele alarak; “medyaya doymuş, bilgi açısından zengin toplumlara tam katılım için gerekli olan yaşam becerilerinin bir bütünü” şeklinde tanımlar. Raporda, dijital medya okuryazarı olan bireyin sahip olması gereken beceriler şu şekilde sıralanır:

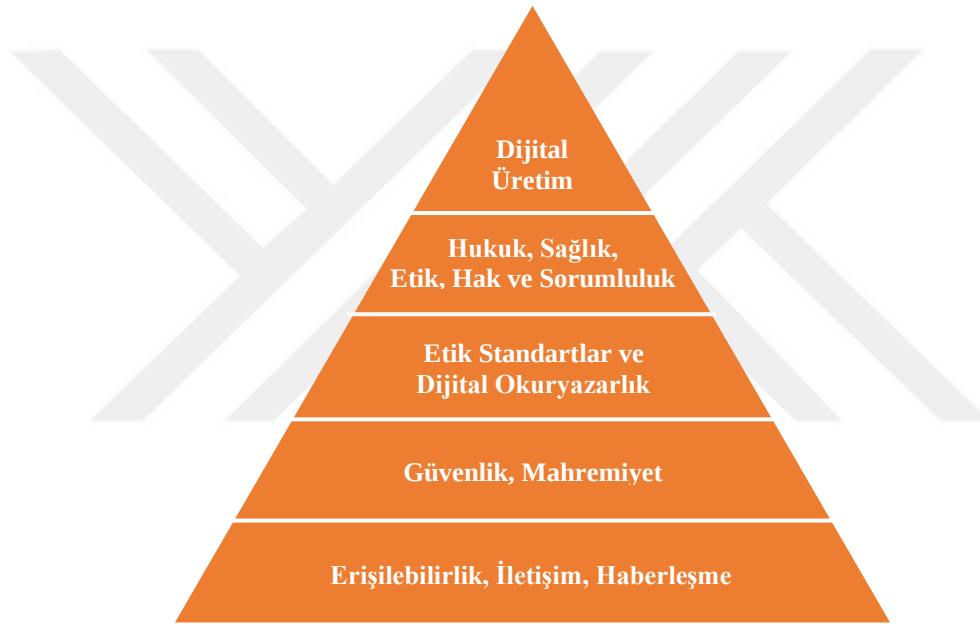
- *Materyalleri bulup paylaşarak, bilgi ve fikirleri anlayarak sorumlu seçimler yapma ve bilgiye erişme,*
- *Yazarın, amacı ve bakış açısını belirleyerek, içeriğin kalitesini ve güvenilirliğini değerlendirerek mesajları çeşitli biçimlerde analiz etme,*
- *Dil, görüntü, ses ve yeni dijital araç ve teknolojilerden yararlanarak çeşitli biçimlerde içerik oluşturma,*
- *Sosyal sorumluluk ve etik ilkeleri uygulayarak kendi iletişim davranışlarını yansıtma,*
- *Ailede, işyerinde ve toplumda bilgiyi paylaşmak ve sorunları çözmek için bireysel olarak veya iş birliği içinde çalışarak ve bir topluluğun üyesi olarak sosyal eylemde bulunma (Hobbs, 2010)*

Dijital okuryazarlık -ve onunla ilişkilendirilebilecek medya okuryazarlığı, medya yeterliliği ve e-beceriler gibi ilgili terimler- bilgi toplumundan faydalanabilmek için gereklidir (O’Neill & Dinh, 2012). Bireylerin, dijital ortamlarda etkin bir şekilde çalışabilmeleri için gerekli olan bilişsel, sosyolojik ve duygusal becerileri içeren dijital okuryazarlık; dijital dünyayı anlamayı, teknolojiyi etkin ve verimli bir şekilde kullanabilmeyi, onun sunduğu fırsatlardan yararlanırken karşılaşılabilecek risklerin de bilincinde olmayı ve tehditlere karşı kendini korumayı içerir (Sağıroğlu vd., 2020a). Bu açıdan, dijital okuryazarlığın içerdiği dijital becerilerin bir çeşit dijital teknoloji kaynaklı riskleri önleme aracı olduğu da söylenebilir (Rodríguez-de-Dios vd., 2016). Dijital okuryazarlığın geliştirilmesi, günümüzün çağdaş toplumunda eğitimin kaçınılmaz bir parçasıdır (Ng, 2012a). Avrupa Dijital Gündemi de özellikle çocukların internet kullanımını göz önünde bulundurarak, dijital okuryazarlığın önemine dikkat çeker. Dijital okuryazarlığın geliştirilmesi, ulusal dijital stratejiler ve ekonomik iyileştirme için esastır

ve dijital vatandaşlık becerilerinin geliştirilmesi için de gereklidir (O'Neill & Dinh, 2012). Gilster (1997) ise internetin yaygınlaşması ile dijital okuryazarlığın araba kullanmak için ihtiyaç duyulan ehliyet kadar önemli hale geldiğini vurgular. OECD üye ülkelerinin çoğunun, dijital okuryazarlığı eğitim gündemlerine almış olmaları da (Van der Vlies, 2020) dijital okuryazarlığa verilen önem için dikkate değer bir işarettir.

Dijital okuryazarlığın kapsamının etkin, güvenli, doğru ve etik kullanımı içerdiği söyleyen Sağıroğlu ve ekip arkadaşları (2020b), Maslow'un ihtiyaçlar hiyerarşisini, dijital okuryazarlık açısından ele alarak aşağıdaki piramidi oluşturmuşlardır.

Şekil 2.8: Maslow İhtiyaçlar Hiyerarşisi ve Dijital Okuryazarlık



Kaynak: (Sağıroğlu vd., 2020b, s. 24)

Araştırmacılar bu uyarlamalarını takiben, dijital okuryazarlığın gerekli ama yeterli olmadığını söylerler ve dijital “okur-yazar-sever-üretir-paylaşır-yönetir-satar” kavramını önerirler. Bunun sağlanması için bireylerin dijital ortamlarda üretmeyi, bilgi ve tecrübeyi değere dönüştürmeyi, ihtiyaç duyacakları yetenek ve becerileri edinmeye çalışmayı, doğru ve yanlış ayırt edebilmeyi, mahremiyete saygı göstermeyi, dijital dünyada karşılaşılabilecekleri tehditlerin farkında olmayı ve önlem almayı, bilgi güvenliğine önem vermeyi, etik davranmayı ve sadece tüketen değil aynı zamanda üreten kullanıcılar olmayı öğrenmesi gereklidir (Sağıroğlu vd., 2020b, s. 25).

Ağ toplumuna katılımın ve ağ toplumuna dönüşümün artması, ekonomik, sosyal ve kültürel alanların dijitalleşmesini beraberinde getirmiştir. Özellikle Covid-19

pandemisi ve onu takip eden süreç, dünya ekonomik sisteminin dijitalleşmesini hızlandırmış ve bu dijital dünya ekonomisi, hali hazırda sorun teşkil eden dijital bölünmenin genişlemesine neden olmuştur. Öğrenciler, aileler ve işyerleri, neredeyse tamamen dijital yollarla faaliyete geçirildikçe, dijital okuryazarlık seviyeleri arasındaki bölünme daha görünür olmuştur (THE Consultancy, 2021). Dijital okuryazarlıklar arasındaki bu dengesizliğin, beraberinde toplumsal eşitsizliği getireceği tahmin edilebilir. Bireylerin dijital teknolojilerine erişimleri arasındaki eşitsizliğe vurgu yapan dijital bölünmenin (OECD, 2001); EİT kullanımlarının artması, internet erişiminin ucuzlaması ve özellikle mobil internet hizmetlerinin tüketicilerin kullanımına sunulmasının da etkisiyle yaygınlaşması sonucunda kapandığı; ancak beraberinde başka bir dijital bölünmeyi getirdiği söylenebilir. İkinci seviye dijital bölünme olarak nitelendirilen bu eşitsizlikler ise bireylerin EİT’leri kullanma şekilleri ve becerileri arasındaki farklılıklara dikkat çeker (van Dijk, 2009; Mossberger, 2009; van Deursen & van Dijk, 2010, 2011, 2014). Dijital teknolojilere erişim eşitsizliğinin tamamen olmasa da büyük ölçüde ortadan kaldırılması, toplumsal eşitliği sağlamak için dijital okuryazarlık seviyeleri arasındaki dengesizliği çözülmesi gereken temel sorunlardan biri haline getirir.

2.3.1. Dijital Okuryazarlığı Oluşturan Okuryazarlıklar

Dijital okuryazarlık kavramı, diğer okuryazarlıklardan sonra geliştirilmiştir ve bu nedenle, onlardan yararlandığı söylenebilir. Dijital okuryazarlık, bilgi okuryazarlığı veya medya okuryazarlığı ile ilgili yönleri içerir (Rodríguez-de-Dios vd., 2016). Farklı okuryazarlıklar arasındaki ilişkiyi netleştirmek için okuryazarlık konseptlerinin ulaşılmaya çalıştığı sonuçlara bakılabilir. Bu noktada, medya okuryazarlığı ile eleştirel medya tüketicilerine, bilgi okuryazarlığı ile bilgiyi bulma ve seçme konusunda yetkin kullanıcılara, haber medya okuryazarlığı ile de haber içeriğine eleştirel olarak yaklaşım tüketebilecek bireylere ulaşmak hedeflenirken dijital okuryazarlık ile dijital medyanın eleştirel, güvenli ve bağımsız kullanıcılarının yetiştirilmesi beklenir (Rodríguez-de-Dios vd., 2018).

Ng de (2012b), dijital teknolojilerin son yıllardaki gelişiminin, literatürdeki okuryazarlık tanımlamalarının sayısını artırdığını ve EİT okuryazarlığı, enformasyon teknolojisi okuryazarlığı, ağ okuryazarlığı, çevrim içi okuryazarlık, multimedya okuryazarlığı gibi tanımlamalarının yapıldığını söyler. Gutiérrez-Martín ve Tyner de (2012), akademisyenlerin EİT’leri kullanmada ustalaşmayı “dijital okuryazarlık”,

medyaya yönelik eleştirel yaklaşımları da “medya okuryazarlığı” olarak tanımladıklarını ancak ikisi arasındaki ayrımı net belirleyemediklerini vurgular. Benzer şekilde Bawden (2001); okuryazarlık literatüründe bilgi/enformasyon okuryazarlığı ile ilişkili altı farklı kavramın, eşanlamlı olarak birbirlerinin yerine kullanıldığı söyler. Bu kavramlar; bilgi okuryazarlığı, bilgisayar (enformasyon teknolojileri, elektronik bilgi) okuryazarlığı, kütüphane okuryazarlığı, medya okuryazarlığı, ağ (internet) okuryazarlığı ve dijital okuryazarlıktır. Jin ve çalışma arkadaşlarının (2020) tanımlamasına göre ise dijital okuryazarlık; çeşitli şekillerde bilgisayar okuryazarlığı, EİT okuryazarlığı, bilgi okuryazarlığı ve medya okuryazarlığı olarak adlandırılan yetkinlikleri içerir.

Reddy ve ekip arkadaşları (2020), yaptıkları literatür değerlendirmesine dayanarak dijital okuryazarlık tartışmalarının 1960’lı yıllarda görsel okuryazarlık kavramı ile başladığını; teknolojik gelişmeler sonucunda teknoloji okuryazarlığı kavramının yaygınlaştığını; özellikle kişisel bilgisayarların yaygınlaşması ve grafik arayüzlerin geliştirilmesi ile bilgisayar okuryazarlığının gündeme geldiğini ve 1990’lı yılların sonuna kadar bu kavramın daha yaygın olduğunu ifade eder. Araştırmacılar, bu kavramın yerini önce EİT okuryazarlığına, daha sonra ise dijital teknolojilerin artan kullanımını kapsamak ve tanımlamak için çok daha geniş bir terime duyulan ihtiyaç neticesinde dijital okuryazarlığa bıraktığını ifade ederler. Genel olarak, dijital okuryazarlık, EİT okuryazarlığından daha geniş bir teknoloji yelpazesıyla ilişkili olarak kullanılır, ancak terimler önemli ölçüde örtüşmektedir ve sıklıkla birbirinin yerine kullanılmaktadır (Australian Council for Educational Research, 2016).

Özetle, farklı okuryazarlık tanımlamalarının birbirleri yerine kullanılabildiği ya da birbirlerini kapsayan özelliklere sahip olduğu söylenebilir. Bu çalışmada, aşağıda değinilen okuryazarlıklar dijital okuryazarlık şemsiyesi altında değerlendirilmektedir.

2.3.1.1. Bilgisayar Okuryazarlığı

Bilgisayar okuryazarlığı, bireyin bilgiye dayalı bir toplumda işlev görebilmek için bilgisayarlarla yapabilmesi ve bilgisayarlar hakkında bilmesi gereken her şey; doğrudan veya dolaylı olarak bilgisayarları içeren, belirli bir sosyal rol içinde etkin bir şekilde işlev görmek için kişinin ihtiyaç duyduğu anlayış, beceri ve tutum (akt. Bawden, 2001) veya sıradan eğitilmiş insanların, işte ve özel yaşamlarında etkin bir şekilde çalışabilmeleri için bilgisayarlar hakkında sahip olmaları gereken bilgi ve becerilerin özeti (Haigh, 1985)

şeklinde tanımlanabilir. Horton (akt. Bawden, 2001) ise daha basit bir ifade ile bilgisayar okuryazarlığını, bireyin, makinenin neler yapabileceğine ve yapamayacağına dair anlayışını artırmakla ilgili olduğunu söyler. Okuryazarlığın okuma ve yazma yeteneği anlamına geldiğini hatırlatan Luehrmann (1981) da bilgisayar okuryazarlığının aynı zamanda “bilgi işlem yapma” yeteneği anlamına geldiğini ifade eder. Van Dyke (1987) ise farklı bilgisayar okuryazarlığı tanımlarına dayanarak dört bileşen listeler: (1) bilgisayarlar ve veri işleme ile ilgili temel aşinalık (bilgisayar farkındalığı), (2) programları kullanma becerisi, (3) programlama yeteneği ve (4) bilgisayarlı sistemlerin hangi yollarla sosyal düzene entegre edildiğine dair bilgi birikimi.

Zhang ve Espinoza (1997), yirminci yüzyılın sonlarında, bilgisayar teknolojisindeki hızlı gelişmelerin, eğitimcileri müfredat değişikliklerine ve öğrencileri bilgisayar okuryazarı olarak eğitmeye zorladığını söyler ve özellikle beşerî ve sosyal bilimlerdeki öğrencilerin; (1) toplumda artan bilgi-işlem becerisi talebi ve (2) mevcut yetersiz bilgisayar becerilerinin farkındalığı ile (3) bilgisayar becerilerini, bu disiplinlerdeki temel bilgiler için ana faktörler olarak algılayarak bilgisayar okuryazarı olma ihtiyacı hissettiklerini belirtir.

2.3.1.2. Enformasyon ve İletişim Teknolojileri Okuryazarlığı

Enformasyon ve iletişim teknolojileri okuryazarlığı, bilgi okuryazarlığı ve teknoloji okuryazarlığı fikirleri arasında köprü kuran bir kavramdır (Katz, 2007). EİT okuryazarlığı; bilgi toplumuna katılmak, bilgi toplumunun bir parçası olmak için bilgiye erişmek, yönetmek, bütünleştirmek, değerlendirmek ve oluşturmak için dijital teknolojileri, iletişim araçlarını ve/veya ağlarını kullanmaktır (International ICT Literacy Panel, 2002). Avustralya’da hazırlanan bir raporda ise EİT okuryazarlığı, bireylerin bilgiye erişmek, yönetmek, bütünleştirmek, değerlendirmek, yeni anlayışlar geliştirmek, topluma etkin bir şekilde katılmak ve başkalarıyla iletişim kurmak için EİT’leri uygun şekilde kullanma yeteneği olarak nitelendirilir (Ainley vd., 2010). ETS, EİT okuryazarlığı için yedi farklı yetkinlik ya da bileşen sıralar. Bunlar; (1) tanımlama (*define*), (2) erişme (*access*), (3) yönetme (*manage*), (4) bütünleştirme (*integrate*), (5) değerlendirme (*evaluate*), (6) üretme (*create*) ve (7) iletişim kurmadır (*communicate*). ETS ayrıca, bu yetkinliklerin temelini oluşturan iki farklı bilgi ve beceri seti olduğunu öne sürer: bilişsel yeterlilikler ve teknik yeterlilikler. Bilişsel yeterlilik (*cognitive proficiency*), günlük yaşamdaki okuryazarlık, aritmetik, problem çözme ve uzamsal/görsel okuryazarlık gibi

temel becerileri kapsarken teknik yeterlilik (*technical proficiency*) ise donanım, yazılım, ağlar ve dijital teknoloji unsurları hakkında temel bilgileri içeren dijital okuryazarlığın temel bileşenlerini kapsar (International ICT Literacy Panel, 2002; Ng, 2012a).

2.3.1.3. Bilgi Okuryazarlığı

İlk olarak Zurkowski tarafından kullanılan bilgi okuryazarlığı kavramı, bilginin etkin kullanımı ve özellikle problem çözme ile ilişkilendirilir. Zurkowski'ye göre (akt. Bawden, 2001), bilgi kaynaklarını kendi işlerinde kullanmak konusunda eğitilmiş kişilere bilgi okuryazarı denilebilir. Doyle ise (1992) bilgi okuryazarlığını, çeşitli kaynaklardan gelen bilgilere erişme, bunları değerlendirme ve kullanma yeteneği olarak tanımlar. Shapiro ve Hughes'a (1996) göre bilgi okuryazarlığı, eski bilgisayar okuryazarlığını ve daha geniş, daha hümanist bir tür eleştirel kavrayışı kapsar ve yedi boyutta incelenebilir. Bunlar; araç okuryazarlığı, kaynak okuryazarlığı, sosyal-yapısal okuryazarlık, araştırma okuryazarlığı, yayınlama okuryazarlığı, gelişen teknolojiler okuryazarlığı ve eleştirel okuryazarlıktır.

Kurbanoğlu (2010), ilk bilgi okuryazarlığı tanımlamalarının daha çok bilgiyi bulma ve kullanma becerilerinden söz ettiğini, daha sonra yapılan tanımların ise “bilgi ihtiyacını tanımlama, bilgiyi bulma, kullanma, değerlendirme, iletme gibi bilgi problemi çözmenin tüm aşamaları” kapsadığına dikkat çeker. Çalışmasında, bilgi okuryazarlığının diğer okuryazarlık türlerini etkileyen bir doğası olduğunu ve bilgi okuryazarlığı becerilerinin, bir bireyin diğer okuryazarlık becerilerini geliştirmesinde rolü olduğunu söyleyen Kurbanoğlu'na göre bilgi okuryazarlığı, bir beceriler bütünüdür:

Bilgi ihtiyacını fark etme, bilgi ihtiyacını tanımlama, bilgi arama stratejileri geliştirme, bilgi arama, bulma, seçme, değerlendirme, kullanma, sınıflama, düzenleme, yorumlama, yeni bilgiyi mevcut bilgiyle bütünleştirme ve iletme gibi bilgi becerilerinin; muhakeme yürütebilme, karar verebilme, problem çözebilme, analitik düşünebilme, eleştirel düşünebilme, sentez yapabilme, yaratıcı düşünebilme, yeni bilgi üretebilme, geçmiş deneyimlerden yararlanarak bilgi ve beceri transferi yapabilme ve bilgiyi içselleştirme gibi üst düzey düşünme becerilerinin; iletişim, ekip çalışması, işbirliği, kişisel motivasyon, uyum sağlama gibi bireysel becerilerin; fonksiyonel okuryazarlık, bilgisayar okuryazarlığı, ağ okuryazarlığı kütüphane okuryazarlığı, medya okuryazarlığı, görsel okuryazarlık

gibi çeşitli okuryazarlık becerilerinin birleşiminden oluşur (Kurbanoglu, 2010, s. 743).

Bilgi okuryazarlığını, dijital teknolojileri kapsayacak şekilde genişleten dijital bilgi okuryazarlığı (*digital information literacy*) kavramı da mevcut okuryazarlık literatüründe yer alan bir kavramdır. Sparks, Katz ve Beile'nin (2016) ETS için hazırladıkları raporda, DBO'nun genelde çeşitli dijital teknoloji bağlamlarında bilgi edinme, anlama, değerlendirme ve kullanma becerisi olarak tanımlandığını ve yükseköğretimde ve küresel ağ ekonomisinde başarı için gerekli görülen kritik derecede önemli bir beceri olarak nitelendirildiğini ifade ederler. Araştırmacılar, DBO'yu bir şemsiye kavram olarak ele alarak farklı araştırmacı ya da kurumlar tarafından hazırlanan on iki farklı okuryazarlık tanımını, kapsadığı bileşenlere göre değerlendirirler. Bu bileşenler, EİT okuryazarlığı başlığında değinilen tanımda vurgu yapılan yedi bileşendir. Ortaya koydukları sentezlenmiş tanımda, DBO'yu dijital teknoloji aracılığıyla bilgiyi araştırma, organize etme ve sentezleme yeteneği de dahil olmak üzere; bilgi sorunlarını çözmek için enformasyon ve iletişim teknolojilerinin uygun kullanımı yoluyla ve bu tür bilgilerin kullanımını çevreleyen etik/yasal konular hakkında temel bir anlayışa sahip olarak bir bilgi toplumunda işlev görme yeteneği şeklinde tanımlamayı önerirler.

2.3.1.4. İnternet Okuryazarlığı

İnternet okuryazarlığı, en kapsamlı hali ile akıllı telefonlar, tabletler, kişisel bilgisayarlar gibi çok çeşitli dijital cihazlarda kullanılan bilgi, beceri ve davranışlar olarak tanımlanabilir (Bauer & Mohseni Ahooei, 2018). İnternet okuryazarlığı tanımları, internet okuryazarlığının çevrim içi bilgi ve iletişim içeriğine erişme, anlama, eleştirme ve oluşturma yeteneği olduğu noktasında birleşmektedir (Uğraş, 2020).

van Deursen ve van Dijk'in internet becerileri için oluşturdukları çerçeve de internet okuryazarlığı başlığı altında ele alınabilir. Bu çerçevede araştırmacılar, dört farklı internet becerisi belirlerler: (1) operasyonel (*operational*), (2) biçimsel (*formal*), (3) bilgisel (*informational*) ve (4) stratejik (*strategic*) internet becerileri. İlk beceri seti; web tarayıcısını açmak, bir URL yazmak, sık kullanılanlar bölümüne sayfa eklemek gibi operasyonel görevleri içerirken ikincisi ise internet üzerinde yönünü kaybetmeme yeteneğine vurgu yapar. Üçüncü ve dördüncü beceri türleri ise araçtan gelen içeriğe ilişkindir. Bilgisel beceriler, bilgi aramak için doğru siteyi seçme, arama kriterlerini

belirleme ve sonuçları değerlendirme gibi görevleri kapsarken dördüncü beceri türü olan stratejik internet becerileri ise en basit ifade ile belirli bir hedefe yönelik bir yönelim geliştirerek ve bu hedef için doğru adımları atarak internetten yararlanabilmeyi sağlar (van Deursen & van Dijk, 2010).

Dijital Beceriler (*Digital Skills*) adlı kitaplarında van Deursen ve van Dijk, diğer tüm dijital medyalarla bağlantılı en baskın dijital ortam haline gelmesi sebebiyle internet becerilerine odaklanırlar. Bu kitapta, yukarıda aktarılan çerçeveden farklı olarak iki beceri türü daha eklerler: iletişim becerileri ve içerik üretme becerileri. İletişim becerileri, anlam inşa etmek, anlamak ve değiş tokuş etmek için mesajları kodlama ve kodunu çözme yeteneği olarak tanımlanır. İçerik üretme becerileri ise, internette yayınlanmak üzere kabul edilebilir kalitede içerik oluşturmak için gereken becerileri içerir (van Dijk & van Deursen, 2014). Araştırmacıların oluşturdukları dijital beceri çerçevesi aşağıda detaylı olarak ele alınmıştır.

2.3.1.5. Medya Okuryazarlığı

Diğer okuryazarlık konseptlerinden farklı olarak medya okuryazarlığının halen bir şemsiye kavram görevi gördüğü söylenebilir (Hobbs, 1998; Koltay, 2011). Literatüre göre, medya okuryazarı bir kişi hem basılı hem de elektronik medyanın kodunu çözebilir, değerlendirebilir, analiz edebilir ve içerik üretebilir. Medya okuryazarlığının temel amacı, tüm medya ile eleştirel bir özerklik ilişkisinin sağlanmasıdır. “Medya okuryazarlığı eğitimindeki vurgular, bilinçli vatandaşlık, estetik takdir ve ifade, sosyal savunuculuk, benlik saygısı ve tüketici yetkinliği dahil olmak üzere geniş bir yelpazede yer almaktadır (Aufderheide, 1993).” Avrupa Komisyonu tarafından önerilen tanıma göre medya okuryazarlığı; genel olarak medyaya erişme, medyanın ve medya içeriklerinin farklı yönlerini anlama ve eleştirel olarak değerlendirme ve çeşitli bağlamlarda iletişim oluşturma yeteneğidir (European Commission, 2007). Medya okuryazarlığı, medyanın toplumdaki rolünün anlaşılmasının yanı sıra demokratik bir ülkenin vatandaşları için gerekli olan temel sorgulama ve kendini ifade etme becerilerini de sağlar (akt. Hobbs, 2016).

Yukarıda bahsedilen okuryazarlık konseptlerinin birbirlerinden ayrıldığı ve farklılaştığı noktaların net olmadığı söylenebilir. Örneğin, Bawden (2001) medya okuryazarlığı ile bilgi okuryazarlığı arasında bariz bir örtüşme olduğuna değinir. Jin ve

çalışma arkadaşlarının, literatürden uyarladıkları dijital okuryazarlık tanımları da bu iç içe geçmişliği gösterir. Bu iç içe geçmişlik, araştırmacıları tüm okuryazarlıkları kapsayan bir çatı okuryazarlık arayışına yönlendirir. Örneğin Uğraş'a göre; bilgi okuryazarlığı diğer okuryazarlık türleri için ortak bir zemin oluşturmaktadır ve tüm okuryazarlıklar yerine kullanılabilir bir kavramdır (Uğraş, 2020). Başka bir ifade ile Uğraş'a göre bilgi okuryazarlığı, günümüz dijital vatandaşlarının ihtiyaç duyduğu tüm okuryazarlık tanımlarını kapsayabilecek şemsiye bir kavramdır. Covello'ya (2010) göre ise bu görev, dijital okuryazarlık kavramındadır: Dijital okuryazarlık, bilgi okuryazarlığı, bilgisayar okuryazarlığı, medya okuryazarlığı, iletişim okuryazarlığı, görsel okuryazarlık gibi bir dizi karmaşık ve bütünleşik alt okuryazarlıklar için bir çatı kavramdır (Nascimbeni & Vosloo, 2019; Reddy vd., 2020). Benzer bir şekilde Martin de (2006) dijital okuryazarlığın; bilgi okuryazarlığı, medya okuryazarlığı, teknoloji okuryazarlığı ve görsel okuryazarlık gibi diğer okuryazarlıkların yakınsamasına (*convergence*) dayandığını ifade eder. Literatüre dayanarak bu çalışmada şemsiye kavram olarak dijital okuryazarlık tercih edilmiştir.

2.3.2. Dijital Okuryazarlık Boyutları

Literatürde, araştırmacıların dijital okuryazarlığı farklı boyutlara ayırarak incelediği görülür. Eshet-Alkalai beş, Martin üç, Buckingham dört, Ng üç ve Rodríguez-de-Dios ve Igartua beş dijital okuryazarlık boyutu (yetkinliği, becerisi ya da alt okuryazarlığı) tanımlarlar.

Eshet-Alkalai'nin beş boyutlu dijital okuryazarlığı; (1) foto-görsel okuryazarlık (*photo-visual literacy*), (2) yeniden üretim okuryazarlığı (*reproduction literacy*), (3) dallandırma okuryazarlığı (*branching literacy*), (4) bilgi okuryazarlığı (*information literacy*) ve (5) sosyo-duygusal okuryazarlıktan (*socio-emotional literacy*) oluşur. Eshet-Alkalai, kullanıcıların grafik kullanıcı ara yüzleri ile çalışırken, sezgisel ve özgürce “okumalarına” ve görsel olarak temsil edilen talimatları ve mesajları anlamalarına yardımcı olan, benzersiz bir dijital okuryazarlık biçimi olarak foto-görsel okuryazarlığı kullandıklarını ileri sürer. “Foto-görsel okuryazarlığı olan insanlar, görsel mesajları kolayca ve akıcı bir şekilde çözmelerine ve anlamalarına yardımcı olan iyi bir görsel hafızaya ve güçlü sezgisel-ilişkisel düşünceye sahiptir (Eshet-Alkalai, 2004, s. 95).” İkinci boyutu oluşturan yeniden üretim okuryazarlığı, hali hazırda mevcut olan bağımsız bilgi parçalarını bütünleştirerek anlamlı, özgün ve yaratıcı bir çalışma veya yorum

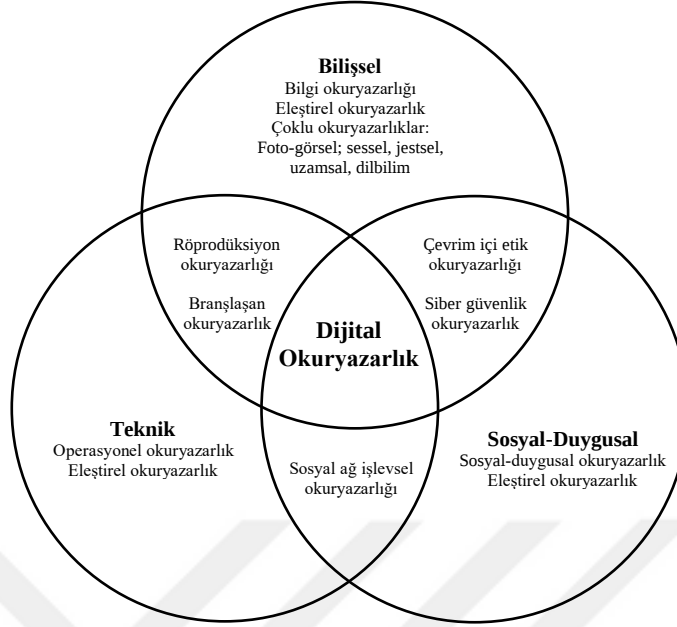
yaratma yeteneğidir. Eshet-Alkalai modelinin üçüncü boyutu olan dallandırma ya da hipermedya okuryazarlığı ile kastedilen “hiperuzayı karakterize eden şeritlerin labirentinde gezinirken yolunu kaybetmekten kaçınma” yeteneği ve çok boyutlu uzamsal oryantasyon duygusudur. Bu modelde kullanıldığı şekliyle bilgi okuryazarlığı, bireylerin bilgiyi eğitilmiş ve etkili bir şekilde değerlendirmek için kullandıkları bilişsel becerileri ifade eder. Son boyut olan sosyo-duygusal okuryazarlık ise, bireylerin eleştirel, analitik ve olgun olmasını ve yüksek seviyede bilgi okuryazarlığına ve dallandırma okuryazarlığına sahip olmalarını gerektirir. Eshet-Alkalai, siber uzayın sosyo-duygusal okuryazar kullanıcılarının, dijital iletişimin avantajlarından yararlanmanın yanı sıra tuzaklarından da nasıl kaçınılacağını bildiklerini söyler (Eshet-Alkalai, 2004). Bu açıdan beşinci boyutun, bir bakıma siber güvenliğe atıfta bulunduğu ifade edilebilir.

Dijital okuryazarlık için bir tanım ve çerçevenin oluşturulması hedeflenen DigEuLit projesinde, üç aşamadan oluşan bir katılım modeli önerilir. Bu aşamalar; (1) dijital yeterlilikler, (2) dijital kullanımlar ve (3) dijital dönüşümdür. Sistemin temeli olan ilk aşama, dijitalle ilgili bilgi, anlayış, tutum ve becerilerden oluşur. İkinci aşama olan dijital kullanımlar, merkezi ve en önemli düzey olarak nitelendirilebilir. Bu düzey, topluluk kültürünün bir parçası olan bireye, gruba veya kuruluşa özgü dijital kullanımlar bütününe mümkün kılan belirli profesyonel dijital yetkinliğin uygulanmasıdır. En üst düzey olan dijital dönüşüm ise bireysel, grup ya da kuruluş düzeyinde gerçekleşebilir. Geliştirilen dijital kullanımlar, yeniliğe ve yaratıcılığa olanak sağladığında ve önemli bir değişimi teşvik ettiğinde elde edilirler (Martin, 2006).

Buckingham (2015), medya okuryazarlığının beraberinde getirdiği eleştireliliğe vurgu yapar ve medya okuryazarlığının temel bileşenleri olarak kabul edilen dört geniş kavramsal yönün oluşturduğu kavramsal çerçevenin, dijital medya için de halen yararlı bir araç sağlamaya devam ettiğini söyler. Bu açıdan bakıldığında, Buckingham’ın dijital okuryazarlık çerçevesi dört boyut içerir: (1) temsil, (2) dil, (3) üretim ve (4) izleyici/kitledir (Ryberg & Georgsen, 2010).

Wan Ng'nin (2012b) tanımladığı üç boyut; teknik (*technical*), bilişsel (*cognitive*) ve sosyal-duygusal (*social-emotional*) olarak sıralanır. Bu boyutların birbirleri ile etkileşimi de alt boyutlar üretir. Aşağıdaki şekilde bu boyutlar görülebilir.

Şekil 2.9: Dijital Okuryazarlık Boyutları



Kaynak: (Ng, 2012a, s. 56)

Rodríguez-de-Dios ve Igartua ise beş boyutlu bir dijital okuryazarlık çerçevesi oluştururlar. Araştırmacılara göre dijital okuryazar olan bireyde; (1) teknolojik ve araçsal beceri, (2) iletişim becerisi, (3) bilgi/enformasyon becerisi, (4) eleştirel beceri (*critical skill*) ve (5) güvenlik becerisi olmalıdır. İlk boyut, dijital teknolojileri etkin bir şekilde kullanmayı içerir. Bu beceri, kullanıcının, farklı yazılım ve donanımlarla çalışabilmesine ve yeniliklere sorunsuz uyum sağlayabilmesine veya belirli bir amaç için hangi yazılımın en uygun olduğunu ayırt etmesini mümkün kılar. İkinci boyut, örneğin bir e-postayı okuma ve anlama veya iletişimcinin niyetini yargılayabilme becerisini kapsayan iletişim becerisidir. Bilgi becerisi, bilgiyi bulma, elde etme ve uygunluğunu değerlendirme yeteneğini ifade eder ve günlük hayatta sürekli kullanıldığı için önemlidir. Dördüncü boyut ise bu elde edilen bilgileri eleştirel olarak analiz edebilme becerisidir. Son boyut olan güvenlik becerisi ise, etkileşimli iletişimi risk ve tehlike olmadan kullanabilmeyi kapsar. Bu beceriye sahip olan bireyler, örneğin, dijital itibarlarını nasıl yöneteceklerini veya çevrim içi olarak mevcut olan kişisel bilgilerinin gizliliğini nasıl koruyacaklarını bilebilirler (Rodríguez-de-Dios & Igartua, 2016, s. 60).

2.3.3. Dijital Beceriler, Dijital Yeterlilikler

İnternet erişiminin yaygınlaşması ile dünya ülkeleri, birer birer ağ toplumu statüsü kazanırlar. Ağ toplumuna katılım, toplumsal haklardan faydalanma ve sorumluluklarını

yerine getirme gibi temel vatandaşlık özellikleri, dijital vatandaşlık kavramını gündeme getirir. Dijital bir vatandaş olabilmenin ise dijital okuryazarlık seviyesinin yükseltilmesi ile mümkün olduğu ifade edilebilir. Yukarıda da değinildiği gibi, pek çok boyut ve alt okuryazarlıklardan oluşan dijital okuryazarlık, belirli dijital becerileri kazanmayı ve dijital olarak yetkin olmayı gerektirir. Bu başlık, dijital okuryazar olmak için kazanılması gereken bu dijital becerilere ayrılmıştır.

Bazen dijital yeterlilikler, yetkinlikler (*digital competences*) olarak da adlandırılan dijital beceriler (*digital skills*), bir bireyin kişisel ve profesyonel yaşamındaki hedeflere ulaşmak için gerek duyduğu EİT kullanma bilgi ve becerilerini kapsar (Commission on Science and Technology for Development, 2018). Bu yetkinlikler, sadece teknik becerileri değil, aynı zamanda kişilerarası beceriler ve iletişim becerileri gibi bilişsel olmayan becerileri ve bilişsel becerileri de içerir (ITU, 2020a). Dijital beceriler olarak nitelendirilen becerilerin birçoğu, yalnızca beceri değil, aynı zamanda davranışlar, uzmanlıklar, teknik bilgi, çalışma alışkanlıkları, karakter özellikleri, eğilimler ve eleştirel anlayışların bir kombinasyonu olan bir dizi farklı yetenek anlamına gelir (Broadband Commission for Sustainable Development, 2017).

OECD için hazırlanan raporda, dijital okuryazarlığa yapılan vurgu ile hangi becerilerin kastedildiği ele alınmış ve (1) dijital bir çağda yaşamak ve çalışmak için gereken genel beceriler ile (2) teknolojileri kullanabilmek için gereken özel beceriler arasında bir ayırmadan söz edilebileceği belirtilmiştir. Aynı raporda, dijital becerilerin tam olarak ne olduğu konusunda devam eden bir tartışma olduğu vurgulanır (Van der Vlies, 2020). Daha önceki bir OECD yayınında, operasyonel beceriler, bilgi navigasyon becerileri, sosyal beceriler ve yaratıcı beceriler şeklinde dört kategoriye atıfta bulunulur. İlk iki kategori, bilgisayar ve interneti kullanmak için gerekli olan teknik ve bilişsel becerilerle ilgili iken son iki kategori ise, çevrim içi iletişim ve etkileşim kurma, dijital sosyal sermaye oluşturma ve çevrim içi kaliteli içerik oluşturma ve paylaşma becerisiyle ilgilidir (Hooft Graafland, 2018; Van der Vlies, 2020) Dünya Ekonomik Forumu'nun iş dünyasının geleceğine ilişkin raporunda ise 2022 yılında beceri taleplerinin analitik düşünme ve inovasyon; aktif öğrenme; yaratıcılık, özgünlük ve inisiyatif; teknoloji tasarımı ve programlama; eleştirel düşünme ve analiz; karmaşık sorunları çözme; liderlik ve sosyal etki; duygusal zeka; akıl yürütme; sorun çözme ve fikir üretme ve sistem analizi

ve değerlendirme gibi becerilere odaklanacağı ifade edilir (World Economic Forum, 2018).

Aşağıda ulusal ve uluslararası iş birlikleri ile oluşturulan dört farklı dijital yetkinlik, dijital beceri çerçevesine değinilmiştir.

2.3.3.1. Vatandaşlar için Dijital Yetkinlik Çerçevesi (DigComp)

DigComp kısa adlı “*Vatandaşlar için Dijital Yeterlilik Çerçevesi*”, bireylerin dijital yeterliliğini geliştirmek için bir araç sunar. İlk olarak 2013 yılında yayınlanan çerçevenin, 2016 yılında terminoloji ve kavramsal modeli güncellenen bir versiyonu yayınlanmış ve DigComp 2.0 olarak adlandırılmıştır. 2017 yılında ise en güncel sürüm olan DigComp 2.1 yayınlanmış ve üç yeterlilik düzeyli model daha ayrıntılı sekiz düzeyli bir modele dönüştürülmüştür (Carretero vd., 2017).

Çerçevede, sekiz yeterlilik seviyesi ve beş yetkinlik alanı tanımlaması yapılmıştır. Bu beş yetkinlik alanı içerisinde toplamda yirmi bir farklı yetkinlik bulunmaktadır. Aşağıdaki tablo bu yetkinlik alanlarını ve yetkinlikleri listelemektedir.

Tablo 2.8: DigComp Yetkinlik Alanları ve Yetkinlikleri

Yetkinlik Alanı	Yetkinlikler
1. Bilgi ve Veri Okuryazarlığı (Information and data literacy)	1.1 Verileri, bilgileri ve dijital içeriği tarama, arama, filtreleme 1.2 Veri, bilgi ve dijital içeriğin değerlendirilmesi 1.3 Verileri, bilgileri ve dijital içeriği yönetme
2. İletişim ve İş Birliği (Communication and collaboration)	2.1 Dijital teknolojiler aracılığıyla etkileşim 2.2 Dijital teknolojiler aracılığıyla paylaşım 2.3 Dijital teknolojiler aracılığıyla vatandaşlığa dahil olmak 2.4 Dijital teknolojiler aracılığıyla iş birliği 2.5 Netiket 2.6 Dijital kimliği yönetme
3. Dijital İçerik Oluşturma (Digital content creation)	3.1 Dijital içerik geliştirme 3.2 Dijital içeriğin bütünleştirilmesi ve yeniden detaylandırılması 3.3 Telif hakkı ve lisanslama 3.4 Programlama
4. Güvenlik (Safety)	4.1 Cihazların korunması 4.2 Kişisel verilerin ve gizliliğin korunması 4.3 Sağlığın ve esenliğin korunması 4.4 Çevrenin korunması
5. Sorun Çözme (Problem Solving)	5.1 Teknik sorunları çözme 5.2 İhtiyaçların ve teknolojik yanıtların belirlenmesi 5.3 Dijital teknolojileri yaratıcı bir şekilde kullanmak

Yetkinlik Alanı	Yetkinlikler
	5.4 Dijital yeterlilik boşluklarını belirleme

Kaynak: (Carretero vd., 2017; Eken, 2021)

Çerçevenin ilk versiyonu temel, orta ve ileri olmak üzere üç yeterlilik seviyesine sahipken 2.1’de seviye sayısı sekiz olmuştur. Proje yürütücülerine göre daha geniş ve daha detaylı yeterlilik seviyeleri, öğrenme ve eğitim materyallerinin geliştirilmesini destekler ve aynı zamanda vatandaşların yeterliliklerinin, kariyer rehberliğinin ve işyerinde terfilerinin gelişimini değerlendirmek için gerekli olan araçların tasarlanmasına da yardımcı olur (Carretero vd., 2017). Aşağıdaki tablo, bu sekiz seviyeyi niteleyen anahtar temaları işaret etmektedir.

Tablo 2.9: Yeterlilik Düzeylerini Öne Çıkaran Ana Anahtar Kelimeler

DigComp 1.0'daki Seviyeler	DigComp 2.0'daki Seviyeler	Görevlerin Karmaşıklığı	Otonomi	Bilişsel Alan
Temel (Foundational)	1	Basit görevler	Yönlendirme ile	Hatırlama
	2	Basit görevler	Otonomi ve gerektiğinde yönlendirme	Hatırlama
Orta (Intermediate)	3	İyi tanımlanmış ve rutin görevler ile kolay sorunlar	Kendi başına	Anlama
	4	Görevler ile iyi tanımlanmış ve rutin olmayan sorunlar	Bağımsız ve ihtiyaçlara göre	Anlama
İleri (Advanced)	5	Farklı görevler ve sorunlar	Başkalarını yönlendirme	Uygulama
	6	En uygun görevler	Karmaşık bir bağlamda başkalarına uyum sağlayabilme	Değerlendirme
Uzmanlaşma (Highly Specialised)	7	Karmaşık sorunları sınırlı çözümlerle giderme	Mesleki pratiklere katkıda bulunma ve başkalarına rehberlik etmek için entegre olma	Oluşturma
	8	Etkileşimli birçok faktörle karmaşık sorunları çözme	Alana yeni fikirler ve süreçler önerme	Oluşturma

Kaynak: (Carretero vd., 2017, s. 13)

DigComp'ta yer alan, toplamda yirmi bir farklı yetkinlik için her bir yetkinlik seviyesine karşılık gelen beceriler de ayrı ayrı tanımlanmıştır. Örneğin, birinci yetkinlik alanının ilk yetkinliğine temel düzeyde sahip olan bir bireyden, bilgi ihtiyaçlarını belirleyebilmesi, dijital ortamlarda basit bir arama ile veri, bilgi ve içerik bulabilmesi ve basit kişisel arama stratejilerini belirleyebilmesi beklenir. Aynı yetkinliğin en yüksek seviyesine sahip bir birey ise tarama, arama ile ilgili etkileşimli birçok faktörle karmaşık sorunları gidermek için çözümler oluşabilir; veri, bilgi ve dijital içeriği kaydedebilir ve filtreleyebilir ve alana yeni fikirler ve süreçler önerebilir (Carretero vd., 2017).

UNESCO tarafından yürütülen ve kırktan fazla dijital okuryazarlık çerçevesine yönelik teknik incelemeler sonucu elde edilen Dijital Okuryazarlık Küresel Çerçevesi'nde (*Digital Literacy Global Framework*), DigComp'a birkaç ekleme yapılması önerilir. Bu çerçevede, DigComp'taki beş yetkinlik alanına; “cihazlar ve yazılım operasyonları” ve “kariyerle ilgili yetkinlikler” şeklinde iki yeni yetkinlik alanı ve sorun çözme yetkinlik alanı içerisine de “hesaplamalı düşünme” şeklinde bir yetkinlik eklemesi yapılır (ITU, 2020a). “İnsanların, dijital teknolojilere ilişkin sorunları çözmenin algoritmik, hesaplamalı doğası hakkında bir anlayışa sahip olmaları giderek daha önemli hale geldiğinden” bu çerçeveye, hesaplamalı düşünme yetkinliği dahil edilmiştir (UNESCO, 2018).

UNESCO'nun katkısına ek olarak, orijinal çerçevede yapılacak güncellemeler için Ocak 2021'de bir katkı çağrısı yapılmış ve DigComp 2.2'nin, 2022 yılının ilk aylarında yayınlanacağı ilan edilmiştir (European Commission, 2021).

2.3.3.2. Dijital Becerilerden Somut Sonuçlara (DiSTO)

Dijital becerilere yönelik bir diğer çerçeve ise London School of Economics'te yürütülen, Dijital Becerilerden Somut Sonuçlara (*Digital Skills to Tangible Outcomes, DiSTO*) adlı proje içerisinde geliştirilmiştir. Proje ile insanların dijital becerilerinin, dijital katılımlarının ve EİT kullanımlarının ölçüm modelleri geliştirilmiş ve iyileştirilmiştir (ITU, 2020a). Araştırma yürütücüleri, internet becerilerini dijital katılımın önemli bir parçası olarak görürler ve projede bir dizi yeni internet becerisi ölçütü önermeye odaklanırlar. Gerçekleştirdikleri ölçek geliştirme çalışmaları sonucunda, beş faktörlü bir internet becerileri ölçeği oluştururlar: (1) operasyonel beceriler, (2) mobil beceriler, (3) bilgi navigasyonu becerileri, (4) sosyal beceriler ve (5) yaratıcı beceriler. İndirilen bir

dosyayı ve tarayıcıda yeni bir sekmeyi nasıl açacağını, kısa yolları nasıl kullanacağını, bir web sitesini sık kullanılanlara eklemeyi bilme gibi beceriler operasyonel beceriler içerisinde değerlendirilir. Mobil beceriler ise mobil cihazlara uygulama indirme ve kurmayı bilmeyi kapsar. Rehberden bir arkadaşı silmeyi ve hangi bilginin internette paylaşılıp paylaşılamayacağını bilmek, sosyal beceriler arasında değerlendirilir. Son olarak yaratıcı beceriler ise var olan çevrim içi içerikleri kullanarak yeni içerikler üretmeyi, başkaları tarafından üretilen içeriklerde küçük değişiklikler yapmayı ve bir web sitesi tasarlamayı bilmeyi içermektedir (van Deursen vd., 2014).

DiSTO projesi içerisinde yer alan van Dijk ve van Deursen, yayınladıkları *Digital Skills* adlı kitapta, projedekinden farklı olarak altı beceri türü belirlerler. Dijital beceriler çerçevesini oluşturan bu altı temel beceri; (1) operasyonel beceriler, (2) biçimsel beceriler, (3) bilgi becerileri, (4) iletişim becerileri, (5) içerik üretme becerileri ve (6) stratejik beceriler şeklinde sıralanır. Operasyonel beceriler, teknik yeterliliğe atıfta bulunurken biçimsel beceriler ise internette gezinme becerisini kapsar. Bilgi becerileri ile kastedilen, arama yapma, arama sonuçları arasında değerlendirme ve seçim yapma becerisidir. Mesajlaşma, tweet gönderme ve çeşitli pek çok internet tabanlı iletişim kanalını kullanma gibi beceriler, iletişim becerilerini oluşturur. İçerik üretme becerisi ise Web 2.0 ile mümkün olan, kullanıcı tarafından üretilen içeriğe atıfta bulunur. Çerçeveedeki son beceri türü olan stratejik beceriler, bireylerin içeriğe ilişkin ve onların belirli bir hedef doğrultusunda dijital medyayı kullanmalarına imkân veren becerilerdir (van Dijk & van Deursen, 2014).

Tablo 2.10: İnternet Becerisi Çerçevesi

Beceri Kategorisi	Beceri Türü	Beceriler
Araca İlişkin	Operasyonel	- İnternetteki araç çubuklarını, düğmelerini ve menülerini tanıma ve çalıştırma - İnternette bulunan farklı türde kullanıcı giriş alanları kullanabilme - İnternette açılan veya kaydedilen farklı dosya biçimlerini yönetebilme
	Biçimsel	- Metinler, resimler, menüler, e-postalar veya uygulamalar gibi farklı biçimlerde gömülü köprüleri kullanarak internette gezinme - Gezinme sırasında konum hissini koruma, yani - Bir web sitesinde veya çevrim içi platformda gezinirken yönünü kaybetmeme - Web siteleri veya çevrim içi platformlar arasında gezinirken yönünü kaybetmeme

Beceri Kategorisi	Beceri Türü	Beceriler
İçeriğe İlişkin	Bilgi	- Arama sonuçları, çevrim içi tartışmalar, kişisel profiller, e-postalar veya kişiler gibi listeleri açarken ve bunlara göz atarken yönünü kaybetmeme - İhtiyaç duyulan bilgiye - Bilgi problemini tanımlayarak, - Bilgi aramak için bir web sitesi ya da arama sistemi seçerek - Arama seçeneklerini ya da sorgularını tanımlayarak - Web siteleri veya arama sonuçları arasından bilgiyi seçerek - Bilgi kaynaklarını değerlendirerek ulaşma
	İletişim	- Kişileri çevrim içi olarak arama, seçme, değerlendirme ve eyleme geçme - Mesajları çevrim içi olarak kodlama: Anlam oluşturma - Mesajları çevrim içi olarak çözme: Anlamı kavrama - Çevrim içi mesaj gönderip alma: Anlam alışverişi - Çevrim içi ortamda dikkat çekme - Çevrim içi kimlikler için profiller oluşturma - Performans: Keşif veya doğaçlama için alternatif çevrim içi kimlikleri benimseme yeteneği - Oyun ve simülasyon: Daha iyi karar verebilmek için çevrim içi deney yapma kapasitesi - Kolektif zekâ: Bireyler arası ağ oluşturmada bilgiyi bir araya getirme ve başkalarıyla anlam alışverişinde bulunma sosyal yeteneği - Müzakere: Başkalarının kastettiklerini anlarken kararlara varmak ve işlemleri gerçekleştirmek için anlam alışverişinde bulunma yeteneği
	İçerik Üretme	- Uygun (minimum kalite seviyesinde) ve etkili veya çekici - Metin içeriği, - Müzik ve video içeriği, - Fotoğraf veya resim içeriği, - Multimedya içeriği - Remikslenmiş (birbirleri ile karıştırılmış) içerikler üretme
	Stratejik	- Belirli bir hedefe yönelik bir yönelim geliştirme - Bu hedefe ulaşmak için doğru adımları atma - Bu hedefe ulaşmak için doğru kararları vermek ve sonunda - Hedefe ulaşmanın getirdiği faydaların elde edilmesi

Kaynak: (van Dijk & van Deursen, 2014, s. 42)

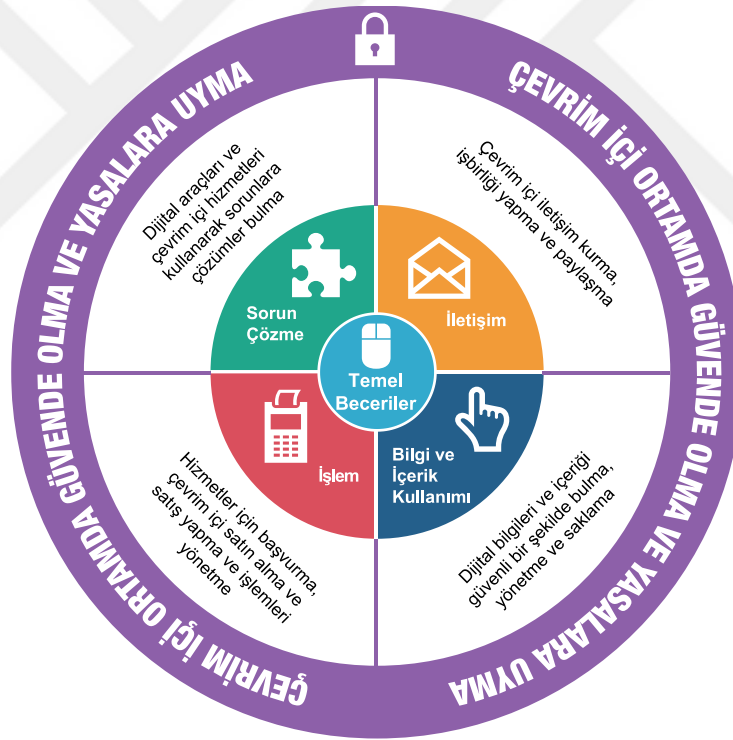
van Dijk ve van Deursen, belirledikleri altı beceri türünün iki ana kategoride ele alınabileceğini ifade ederler: araca ilişkin beceriler (*medium-related*) ve içeriğe ilişkin beceriler (*content-related*). Bu açıdan, operasyonel ve biçimsel beceriler, araca ilişkin beceri olarak değerlendirilir. Diğer dört beceri ise içeriğe ilişkin becerilerdir. Araca ilişkin beceriler, medya kullanımının teknik özelliklerini hesaba katarken, içeriğe ilişkin beceriler, medya tarafından sağlanan ve kullanıcılar tarafından üretilen içeriği etkileyen becerileri kapsar. Bu beceriler arasındaki ayrım, sıralı ve koşulludur. Başka bir şekilde ifade edilirse, bu beceriler, birbirlerinin arkasına ve üstüne gelir. Örneğin, içerikle ilgili

becerilerin gerçekleştirilmesi, araçla ilgili becerilere hâkim olmayı ve stratejik becerilerde etkin olmak da bilgi ve iletişim becerilerine sahip olmayı gerektirir (van Dijk & van Deursen, 2014).

2.3.3.3. Temel Dijital Beceriler Çerçevesi

Temel Dijital Beceriler Çerçevesi (*The Essential Digital Skills Framework*), bugünün ve geleceğin dijital dünyasına katılmak, katkıda bulunmak ve dijital dünyadan güvenli bir şekilde yararlanmak için gereken becerileri tanımlar. Bu çerçevede, iletişim (*communication*), bilgi ve içerik kullanımı (*handling information and content*), işlem yapma (*transacting*), sorun çözme (*problem solving*) ve çevrim içi ortamda güvende olma ve yasalara uyma (*being safe and legal online*) şeklinde beş farklı kategori yer almaktadır (Department for Education, 2018).

Şekil 2.10: Temel Dijital Beceriler Çerçevesi Diyagramı



Kaynak: (Department for Education, 2018)

Yukarıdaki diyagram, çerçevede yer alan beceri kategorilerine ilişkin temel bilgileri içermektedir. Çerçevede, sıralanan beş kategoriye ek olarak, şu anda dijital teknolojiyi kullanmayan veya sınırlı şekillerde kullananlar için gerekli olan temel (*foundational*) beceriler de tanımlanır. Bu becerilere sahip kişilerin, aynı zamanda dijital

teknolojiyle bağlantı kurma motivasyonuna ve güvenine sahip olacağı varsayılabilir. Çerçeve tanımlanan iletişim becerileri, çevrim içi olarak iletişim kurma, iş birliği yapma ve paylaşma becerisini işaret ederken bilgi ve içerik kullanma kategorisi, bilgiye güvenli bir şekilde ulaşma, bilgiyi yönetme ve saklama becerilerini kapsar (Department for Education, 2018).

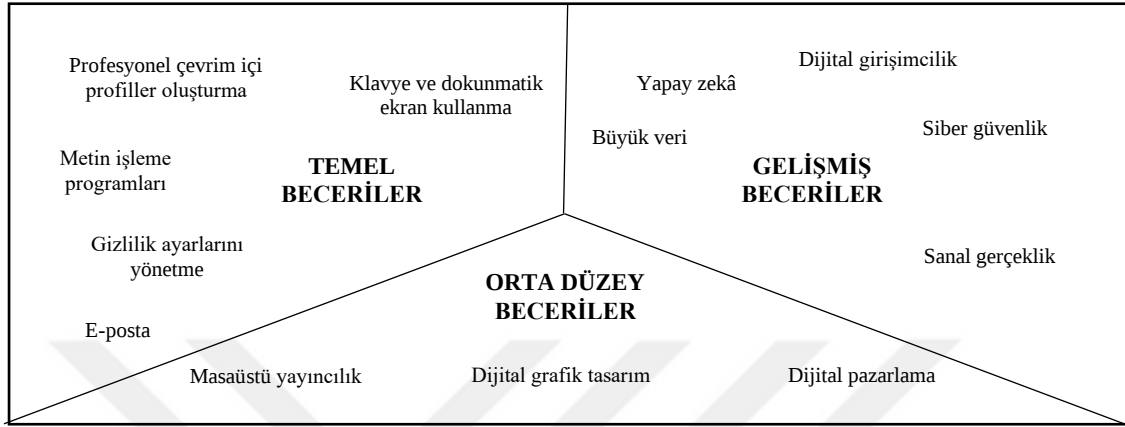
Temel Dijital Beceriler Çerçevesi'ndeki beş kategori, yaşam ve iş hayatı olarak iki farklı üst kategori içerisinde ayrı ayrı değerlendirilir. En temel ya da basit beceriler, bir cihazı kapatıp açma, uygulama kullanma ve fare kullanma gibi toplamda yedi, yaşam için dijital beceriler fotoğraf yükleyebilme, metin işleme programlarını kullanabilme gibi yirmi dokuz; iş hayatı için dijital beceriler ise dijital iş birliği araçlarını kullanabilme, profesyonel sosyal ağlarda profil oluşturabilme ve dijital kayıt ve dosyaları yönetebilme gibi on yedi görevi kapsar. Çerçeveye göre, en temel becerilere sahip olmak, yedi görevin tamamını da yerine getirebilmeyi gerektirir (Lloyds Banking Group, 2019).

2.3.3.4. ITU Dijital Beceri Seviyeleri

Uluslararası Telekomünikasyon Birliği (ITU), *Digital Skills Toolkit* adlı çalışmada, dijital becerileri üç seviyede değerlendiren bir çerçeve oluşturur: (1) temel, (2) orta düzey ve (3) gelişmiş. Temel dijital beceri seviyesi, toplumda minimum düzeyde işlev görmeyi sağlar. Temel beceriler, donanımı (klavye ve dokunmatik ekranları kullanma), yazılımı (metin işleme, bilgisayarlarda dosyaları yönetme, cep telefonlarında gizlilik ayarlarını yönetme) ve temel çevrim içi işlemleri (e-posta gönderme, arama veya çevrim içi bir form doldurma) kapsar. Aynı zamanda temel beceriler, başkaları ile iletişim kurmayı ve kamusal, ticari veya finansal hizmetlere erişmeyi sağlar. Orta düzey beceriler, teknolojiyi eleştirel olarak değerlendirme veya içerik oluşturma becerisi de dahil olmak üzere, dijital teknolojileri daha anlamlı ve faydalı şekillerde kullanmayı sağlayan becerilerdir. Bu beceriler aynı zamanda; masaüstü yayıncılık, dijital grafik tasarım ve dijital pazarlama gibi işle ilgili işlevleri gerçekleştirmek için gereken becerileri de kapsar. Gelişmiş beceri seviyesi ise, bilgisayar programlama ve ağ yönetimi gibi EİT mesleklerindeki uzmanların ihtiyaç duyduğu beceri setlerini içerir. Geleneksel girişimciliği, yeni dijital teknolojilerle birleştiren dijital girişimcilik de gelişmiş beceri seviyesine sahip bireylerde aranan bir özelliktir. Dijital işletmeler, iş operasyonlarını iyileştirmek, yeni iş modelleri icat etmek, iş zekasını keskinleştirmek ve müşteri ve paydaşlarla etkileşim kurmak için sosyal medya, büyük veri analitiği, mobil ve bulut

çözümleri gibi yeni dijital teknolojileri yüksek yoğunlukta kullanımlarıyla karakterize edilirler (ITU, 2018a). Aşağıdaki şekil, üç beceri seviyesinin kapsadığı becerileri göstermektedir.

Şekil 2.11: Dijital Beceriler



Kaynak: (ITU, 2018a)

2.4. Literatürdeki Araştırmalar

Kuhlemeier ve Hemker (2007), öğrencilerin evlerinde internet ve bilgisayar kullanmalarının, okul için ihtiyaç duydukları dijital beceriler üzerindeki etkisini araştıran bir çalışma gerçekleştirirler. Çalışmada, Hollanda'daki 68 farklı okulda okuyan, 13-15 yaş arasındaki 2500'den fazla öğrencinin, internet ve bilgisayar becerileri ölçülmüş ve öğrencilerin arka planlarının etkisi de dikkate alınarak, evde erişim ve kullanımın internet ve bilgisayar becerileri üzerindeki etkisi incelenmiştir. Araştırma sonucunda, üniversite öncesi eğitimdeki öğrencilerin, üçüncü sınıf öğrencilerinin ve azınlık olmayan öğrencilerin, sırasıyla meslek öncesi eğitimdeki öğrencilere, birinci sınıf öğrencilerine ve azınlık öğrencilerine göre daha iyi internet becerilerine ve daha avantajlı ev bilgisayar kullanımına sahip oldukları ve kızların internet becerilerinin, erkeklerinkinden küçük bir miktar az olduğu sonucuna ulaşılmıştır.

van Deursen ve van Dijk, 2007 ve 2008 yıllarında katılımcıların internet becerilerini ölçmek için, iki performans testini içeren bir araştırma yürütmüşlerdir. Toplamda 218 kişinin katıldığı araştırma sonucunda araştırmacılar, katılımcıların operasyonel ve biçimsel internet becerileri seviyesinin oldukça yüksek, ancak bilgi ve stratejik internet becerileri seviyesinin kuşku uyandırıcı olduğunu söylerler. Eğitim, tüm beceri seviyeleri üzerinde katkı sağlayıcı bir etkiye sahipken yaş, sadece operasyonel ve biçimsel internet becerileri ile ilişkilendirilebilir. Yürüttükleri çalışmaların sonuçlarını

yorumlayan araştırmacılar, orijinal dijital bölünmenin (bilgisayarlara ve internete erişimi olan ve olmayanlar arasındaki bölünme), interneti kullanma becerilerindeki farklılıkları içeren ikinci bir bölünme geliştirdiğini vurgularlar (van Deursen & van Dijk, 2011).

Aynı araştırma ekibinin, 2007 yılında 109 katılımcı ile gerçekleştirdiği çalışmada ise kullanıcıların çevrim içi davranışlarındaki beceri kaynaklı sorunlara dikkat çekilir. Çalışmanın verileri, katılımcılara uygulanan kısa anket ve performans testinden elde edilir. Sonuçları değerlendiren araştırmacılara göre, özellikle daha düşük eğitim seviyesine sahip ve daha yaşlı olan katılımcıların, operasyonel ve biçimsel becerilere ilişkin sorunları daha çok deneyimledikleri ve bu sebeple internet kullanımlarının sınırlandığını; bilgi becerileri açısından da yüksek eğitim seviyesine sahip olanların daha iyi performans gösterdiklerini ifade ederler. Ayrıca, yaşın bilgi becerisine ilişkin sorunlarla bir ilişkisi olmadığı, ancak alakasız arama sonuçları seçme üzerinde olumsuz bir etkisi olduğunu eklerler (van Deursen & van Dijk, 2009).

Avustralya’da on iki yıllık bir periyodu kapsayan dönemde, Ulusal Değerlendirme Programı ile altıncı ve onuncu sınıf öğrencilerinin EİT okuryazarlıklarını ölçen bir araştırma yürütülmüştür. Dört farklı zamanda (2005, 2008, 2011, 2014 ve 2017) yürütülen çalışmalara göre; 2011 ve 2014 yılları arasında hem 6. hem de 10. sınıf öğrencilerinin EİT okuryazarlığı performansında bir düşüş olduğu tespit edilmiştir. Projeyi yürüten araştırmacılar bu düşüşü, yaygınlaşan mobil teknolojilere atfedilebileceğini, ancak bunu söyleyebilmek için yapılan araştırmaların sayısının henüz çok az olduğunu belirtirler. Kapsamlı araştırmada ortaya çıkan bir diğer sonuç da erkek öğrencilerin, sürekli olarak EİT ile ilgili görevleri yaparken daha yüksek düzeyde ilgi, zevk ve güven ifade etmelerine rağmen, kızların hem 6. hem de 10. sınıfta erkeklerden daha iyi performans göstermeye devam etmeleridir (Fraillon vd., 2015). Cinsiyetler arasındaki bu farklılığın, 2017 yılında yapılan taramalarda da sürdüğü gözlemlenmiştir. 2017 yılındaki EİT okuryazarlığı ölçümlerinde hem 6. hem de 10. sınıf kız öğrencilerinin erkeklere oranla daha yüksek performans sergilerler (Fraillon vd., 2018).

Mossberger ve ekip arkadaşları (2012), evde geniş bant internet erişimi olan bireyler ile yalnızca mobil erişime sahip bireylerin internet kullanımlarını karşılaştırdıkları bir çalışma yürütürler. 2011 yılında, Şikago kentinde telefon yoluyla 3000 farklı katılımcıyla gerçekleştirilen anket çalışması ile akıllı telefon ve evde geniş

bant internet kullanıcılarının faaliyet ve becerilerini, bireysel düzeyde karşılaştırırlar. Araştırmacılar ayrıca kullandıkları çok düzeyli istatistiksel analizler ile şehrin 77 mahallesinde, evde geniş bant internet kullanımı, akıllı telefon kullanımı ve çevrim içi etkinlikleri tahmin etmeye çalışırlar. İstatistiki modellerin mahalle bağlamının, bireysel düzeydeki eşitsizlikleri şiddetlendirdiğini ifade eden araştırmacılar, sonuçların erişim kalitesinin bireysel yetenekler ve potansiyel kamu yararı için önemli olduğunu gösterdiğini ve bunun da geniş bant internet erişiminin devam eden önemini vurguladığını söylerler. Araştırma ve istatistiki analizler, çevrim içi beceriler ve etkinlikler de dahil olmak üzere, dijital vatandaşlık için farklı erişim biçimleri ile yetenekler arasında güçlü bir bağlantı olduğunu ve cep telefonlarının gençler ve azınlıklar arasında internete bağlanmanın popüler bir yolu haline geldiğini gösterir. Şikago'daki siyahi vatandaşların, akıllı telefon kullanıyor olma olasılıkları, beyazlardan daha yüksektir, ancak dezavantajlı kişiler için bir çözüm olarak mobil erişimin yaygın kabulüne rağmen, bu erişim türü ikinci sınıf bir erişim şekli olmaya devam etmektedir. Araştırmacılar analizler sonucunda, evde geniş bant internet erişiminin, dijital vatandaşlık için kritik bir öneme sahip olmaya devam ettiğini ve cep telefonu kullanımındaki büyümenin, çevrim içi katılımdaki eşitsizlikleri ortadan kaldırmadığının altını çizerler.

Zher (2017), PIAAC²¹ verilerini inceleyerek hazırladığı sunumda 34 OECD ülkesin dijital okuryazarlık seviyelerine göre sıralar. Bu sıralamaya göre; Türkiye, yüzde 74'lük düşük dijital okuryazarlık seviyesi ile 33. sırada yer alır. Türkiye'deki orta seviye dijital okuryazarlık ise sadece yüzde 23'tür. OECD ülkeleri arasında, en fazla orta ve yüksek düzey dijital okuryazara sahip olan ülkeler ise sırasıyla; Norveç, Danimarka, İsveç, Hollanda ve Finlandiya'dır.

Martens ve Hobbs (2015), medya okuryazarlığı eğitiminin sivil katılıma etkisini değerlendirdikleri çalışmada, 400 lise öğrencisinin medya okuryazarlığı programına katılımları ile akademik yetenek, internet kullanım sıklığı, bilgi toplama güdüler, haber ve reklam analiz becerileri ve sivil katılıma yönelik niyetleri arasındaki ilişkiyi araştırırlar. Bulgular, medya okuryazarlığı programındaki öğrencilerin, diğer öğrencilere göre önemli ölçüde daha yüksek medya bilgisine, haber ve reklam analizi becerisine ve

²¹ Programme for the International Assessment of Adult Competencies

medya bilgisi ve bilgi arama güdüsüne sahip olduklarını gösterir. Ayrıca bu beceriler, ergenlerin sivil katılıma yönelik niyetlerine bağımsız olarak katkıda bulunmaktadır.

2017-2018 yıllarında Polonya’da, 701 ilkokul öğretmeni üzerinde, dijital okuryazarlığın temel bir bileşeni olarak dijital güvenlik becerilerinin ölçümlenmesine yönelik bir araştırma yürütülmüştür. Tomczyk tarafından gerçekleştirilen araştırmaya göre, cinsiyet yeterlilik düzeyi açısından belirleyici bir faktör değildir ve dijital güvenlikle ilgili olarak öğretmenler arasında, Dunning-Kruger etkisi²² söz konusudur. Tomczyk, dijital okuryazarlığın cihazları ve web sitelerini kullanma, bilgiye erişme, verilerin güvenliğini sağlama, ekipman kurma ve yeni e-tehditlerle ilgili kendi bilgilerini güncelleme gibi teknik becerileri içeren çok yönlü bir yapı olmasının, dijital güvenlik göstergelerinin listelenmesini ve ölçülmesini zorlaştırdığını, ancak bir alandaki farkındalık ve okuryazarlık ne kadar yüksek olursa, diğer alanlardaki bilgi düzeyinin de o kadar yüksek olduğunu gözlemlediğini söyler (Tomczyk, 2020).

Rodríguez-de-Dios ve çalışma arkadaşları, ergenlerin dijital becerileri ile çevrim içi risk ve fırsatlar arasındaki ilişkiyi ve ebeveynlerin aracılığının (*parental mediation*), çevrim içi risk ve fırsatlara etkisini araştırdıkları bir çalışma yürütürler. Örneklemini 1.446 İspanyol ortaokul öğrencisinin oluşturduğu çalışmada, dijital olarak daha yetenekli ergenlerin daha fazla fırsat elde ettiğini ve daha fazla risk yaşadığını gösterir. Bulguları değerlendiren araştırmacılar, dijital okuryazarlığın, gençlerin daha fazla fırsat elde etmesine olanak sağladığı için önemli olduğunu ve ebeveynlerin kısıtlayıcı arabuluculuk yerine başka arabuluculuk yollarını seçmesi gerektiğini söylerler (Rodríguez-de-Dios vd., 2018).

Pala ve Başbüyük (2020), ortaokul öğrencilerinin dijital okuryazarlık seviyelerini tespit edecek bir ölçek geliştirme çalışması yürütürler. 2017-18 eğitim-öğretim yılında, Erzincan’daki 16 farklı ortaokulda eğitim gören 742 beşinci sınıf öğrencisi üzerinde yaptıkları çalışmalar sonucunda, yirmi bir maddenin dört faktöre dağıldığı bir ölçek elde ederler. Ölçekteki faktörler; bilgi işlem, iletişim, güvenlik ve problem çözme olarak adlandırılır.

²² Dunning-Kruger etkisi, psikolojide, belirli bir entelektüel veya sosyal alanda sınırlı bilgi veya yetkinliğe sahip kişilerin, nesnel kriterlere, akranlarının veya çevredeki insanların performansına göre bu alandaki kendi bilgi veya yeterliliklerini büyük ölçüde abarttığı bilişsel bir önyargıdır (Duignan, 2020).

Özsoy ve ekip arkadaşları (2020), dijital beceriler (*digital skills*) ile siyasal katılım arasındaki ilişkiyi aydınlatmaya yönelik bir araştırma yürütürler. Çalışmada, dört farklı dijital beceri alt türü (operasyonel, resmi, bilgilendirici ve stratejik) ile üç farklı siyasal katılım türü (çevrim içi, çevrim dışı ve sivil katılım) alt türü arasındaki ilişki araştırılır. Verileri, Türkiye'nin kuzeydoğusunda yaşayan 400 katılımcıya uygulanan performans testleri ve anketler aracılığıyla toplanan çalışma, her alt türden dijital becerinin, siyasi katılımı olumlu etkilediği göstermektedir. Dijital beceriler, en güçlü şekilde sivil ve çevrim içi siyasal katılımı tahmin ederken çevrim dışı siyasal katılım ile arasında bir ilişki yoktur.

Choi ve çalışma arkadaşları (2021), Bourdieu'nün sermaye teorisini ve dijital okuryazarlık literatürünü temel alarak bir çalışma gerçekleştirirler. 2018 yılında, Austin, Teksas'ta yaşayan 997 katılımcıya hem posta yoluyla hem de çevrim içi olarak uygulanan anket sonucunda, bireylerin “tekno-sermayesini” oluşturan üç teknolojik yetenek boyutu belirleyen araştırmacılar, temel sosyoekonomik göstergelerin yansıttığı kültürel ve ekonomik/finansal sermayenin farklı tekno-sermaye boyutları üzerindeki etkilerini analiz ederler. Araştırmacılar, anket verilerine uyguladıkları faktör analizleri sonucunda, bireylerin medya ve bilgi (bilgisayar, akıllı telefon ve internetle ilgili) yeteneklerinin, (1) temel yetenekler (*basic media and information capability*), (2) orta seviye iş ve bilgiye ilişkin yetenekler (*intermediate work/information-related capability*) ve (3) gelişmiş güvenlik ve katılım yetenekleri (*advanced security and participation capability*) olarak üç boyutta inceleyebileceği sonucuna ulaşırlar. Birinci boyut, bilgi teknolojilerini kullanarak dijital ortamda gezinmek için gereken çok temel becerileri içerirken ikincisi işyerlerinde veya okulda kullanılan daha karmaşık becerileri kapsar. Üçüncü boyut olan gelişmiş yetenekler ise, kişinin dijital alanlardaki mahremiyet ve güvenlik anlayışıyla ilgili daha karmaşık becerilerinin yanı sıra içerik üretimi ve kodlama gibi yaratıcı etkinlikleri de içerir. Araştırmada, eğitim ve gelirin bu yetenek boyutları (tekno-sermaye) üzerinde olumlu, yaşın ise olumsuz bir etkisi olduğu sonucuna ulaşılır. Araştırmacılar ayrıca, ırkın da bir rol oynadığını ve Hispaniklerin daha düşük, Asyalıların ise daha yüksek bir tekno-sermayeye sahip olduğunu eklerler. Son olarak araştırma sonuçlarına dayanılarak temel teknolojik yetenekleri (birinci boyut) edinmenin ileri tekno-sermayeyi (üçüncü boyut) açıklayan kilit bir faktör olduğu söylenebilir (J. R. Choi vd., 2021).

Castellví ve ekip arkadaşları, ilköğretim öğretmenliği öğrencilerinin dijital okuryazarlık yetenekleri ve sosyal problemlere yönelik tutumlarını inceledikleri araştırmalarında, eleştirel dijital okuryazarlık kavramına değinirler. Araştırmacılar, eleştirel dijital okuryazarlığı, bilgi aramak, çok modlu metinleri analiz etmek, bilgi üzerinde düşünmek, anlatılar ve karşı anlatılar oluşturmak ve radikal demokrasi ve küresel adalet arayışında sosyal olarak hareket etmek için gereken beceri ve tutumlar olarak görürler. 2017-18 akademik yılında, İspanya'daki beş farklı üniversitede ilköğretim öğretmenliği bölümünde okuyan 322 üçüncü ve dördüncü sınıf öğrencisi üzerinde yapılan araştırma, geleceğin öğretmenlerinin sosyal problemler hakkında, internette aldıkları bilgilere dayalı eleştirel söylemleri bir araya getirmekte zorlandıklarını ve şüphecilerin, kıyaslayanların, analiz edenlerin ve akıl yürütenlerin azınlıkta olduğunu gösterir (Castellví vd., 2020).

van Laar ve çalışma ortakları (2019), yirmi birinci yüzyılın dijital becerilerini belirleyen faktörleri ortaya koymak için bir çalışma gerçekleştirirler. Bilgi yoğun yaratıcı sektörlerde çalışan 1222 katılımcı üzerinde, Ekim-Aralık 2017 tarihinde gerçekleştirilen büyük çaplı anket çalışmasında, potansiyel kişisel, motivasyonel ve sosyal belirleyiciler üzerinden dijital beceri düzeyindeki farklılıkların açıklanması amaçlanmıştır. Çalışma sonucunda, her bir dijital beceriye ait seviyenin, benzersiz bir dizi belirleyici tarafından açıklandığı ve her birinin geliştirilmesi için benzersiz bir yaklaşım gerektiği görülür. Örneğin, kendi kendine öğrenme belirleyicisi bilgi, iş birliği ve problem çözme dijital beceri düzeylerine katkıda bulunurken iletişim, yaratıcılık ve eleştirel düşünme becerilerine bir etkisi yoktur. Araştırmacılara göre, bireysel çalışan düzeyinde hangi faktörlerin becerilerin gelişimini etkilediğini anlamak, uygun girişimlerin tasarlanması için önemlidir. Çünkü araştırma sonuçlarına göre, beceriler farklı bireysel arka plan değişkenlerine bağlı olarak değişiklik göstermekte ve bu durum da beceri geliştirme önündeki başka bir engeli vurgulamaktadır. Her bir becerinin gelişimi, sadece öğrenilme sırasını değil aynı zamanda farklı bir dizi belirleyicinin de hesaba katılmasını gerektirir (van Laar vd., 2019, s. 100).

van Laar ve ekibi, bilgi yoğun yaratıcı sektörlerde çalışan bireyler üzerinde gerçekleştirdikleri diğer araştırmada ise performansa dayalı bir yaklaşım benimserler ve anket formu ile değil doğrudan katılımcıların performanslarını gözlemlerler. Örneklemi Hollanda'da, belirtilen sektörlerde çeşitli pozisyonlarda çalışan 45 erkek ve 42 kadının

oluşturduğu araştırmada, 1 Nisan – 15 Ağustos 2018 tarihleri arasında gerçekleştirilen performans testlerinden elde edilen veriler sonucunda, katılımcıların en çok dijital bilgi değerlendirme ve problem çözme becerilerinde zorlandıklarını gösterir. Araştırmacılar, katılımcıların çevrim içi olarak eriştikleri bilgileri, nadiren tekrar kontrol ettiklerini ve yalnızca oldukça küçük bir yüzdesinin, problemlere birden fazla çözüm önerebildiğini belirtirler. Araştırmacılar, problem çözme becerisine ilişkin bulguların, endişe verici olduğunu vurgularlar (van Laar vd., 2020).

Jackman ve meslektaşları (2021), dijital beceri farklılıklarının geleceğin eğitimindeki önemine dikkat çektikleri çalışmalarında, DQ Institute (2020) tarafından yürütülen ve 30 farklı ülkeden 145.000 çocuğun katıldığı, 2020 Child Online Safety Index araştırmasına atıfta bulunarak 8-12 yaş arasındaki çocukların yüzde 60'ının siber zorbalık, oyun oynama bozukluğu ve şiddet gibi siber riskler, yüzde 39'unun ise itibar riskleri ile karşı karşıya kaldıklarına dikkat çekerler. Araştırmacılar, bu risklerin dijital beceri eğitiminin aciliyetine dikkat çekerler ve Coalition for Digital Intelligence tarafından, yakın zamanda başlatılan 1 Milyar Dijital Beceri Projesi'ne değinirler.

AB tarafından finanse edilen, Doğu Ortaklığı Sivil Toplum Grubu için hazırlanan raporda, Doğu Ortaklığı ülkelerindeki dijital okuryazarlık düzeyinin, Covid-19 salgını sürecindeki durumu ele alınmış ve gelişmemiş internet altyapıları, güvenli olmayan siber alan, dezenformasyona yüksek oranda maruz kalma ve yetersiz dijital okuryazarlık seviyelerinin etkisi ile bu ülkeler için salgın sürecinin oldukça zorlayıcı olduğu ifade edilmiştir. Raporda değinilen verilere göre, Gürcistan'ın yaklaşık yarısı (%47) ve Ermenistan'daki bireylerin üçte biri (%34), bilgisayar kullanmak için gereken temel bilgiye sahip değildir. Ukrayna nüfusunun yüzde 53'ünün, dijital beceri seviyesi ise temel becerilerin altındadır ve ülkedeki altı kişiden biri ise herhangi bir dijital beceriye sahip değildir. Diğer bir Doğu Ortaklığı ülkesi olan Azerbaycan'da ise ankete katılan bireylerin yaklaşık dörtte biri (%22,7), sohbet için interneti kullanırken, sadece yüzde 17'si ekli dosyalar içeren e-postalar gönderdiklerini ve yüzde 18,2'si bilgiye ulaşmak için arama motorlarını kullandıklarını belirtmiştir (Akhvlediani, 2021).

Birleşik Krallık'ta, yetişkinlerin dijital beceri seviyelerini tespit etmek için, periyodik olarak saha araştırmaları yürütülmektedir. Bu araştırmalarda, dijital beceriler altında değinilen “Temel Dijital Beceriler Çerçevesi”nin sunduğu kategoriler ve ölçekler

kullanılmaktadır. 2021 yılında üçüncüsü gerçekleştirilen araştırmaya, 18 yaş üstü 4000 yetişkin katılmıştır. Salgın sürecindeki sokağa çıkma kısıtlamaları nedeniyle, bu yıl ilk defa tüm anketleri telefon yoluyla gerçekleştirilen araştırmanın sonuç raporuna göre, İngiltere’de yaklaşık 2 milyon insan daha dijital dünyaya katılım sağlamıştır (*digital inclusion*). Toplamda yaklaşık 11 milyon insan ise temel dijital becerilere sahip olmadıkları için dezavantajlı konumdadırlar. Hatta bu grubun yüzde 91’i, en basit becerilere dahi sahip değildirlar. Bu en basit beceriler, cihazı Wi-Fi ağına bağlama, internette gezinmek için bir tarayıcı açma, cihazı açıp kendi profiline erişim sağlama gibi görevleri yerine getirebilmeyi kapsar. Bu basit becerilere dahi sahip olmayan gruptakiler genellikle, 65 yaş üstü bireylerden, engellilerden ve resmi niteliklere sahip olmayanlardan oluşmaktadır. Çalışmada, en basit becerilere sahip olma ile yaş arasında bir korelasyon olduğu sonucuna ulaşılmıştır (Lloyds Banking Group, 2021).

Literatürdeki araştırmalar değerlendirildiğinde, dijital okuryazarlık seviyelerinin tespiti ile ilgili araştırmaların çoğunun örneklemini, ergenlerin ve üniversite öğrencilerin oluşturulduğu görülmektedir. Dijital vatandaşlık ile ilgili araştırmaların büyük çoğunluğu ise öğrencilerin, eğitim yöneticilerinin, öğretmen adaylarının ve öğretmenlerin dijital vatandaşlık düzeylerini veya algılarını belirlemeye yöneliktir. Bu tema dışında kalan araştırmalar ise; (1) dijital vatandaşlık kavramının veya unsurlarının tanıtılmasına yönelik çalışmalar, (2) müfredatları dijital vatandaşlık çerçevesinde inceleyen araştırmalar ve (3) dijital vatandaşlık öğretimi ve unsurları üzerine yapılan çalışmalardır (Öztürk, 2021).

ÜÇÜNCÜ BÖLÜM

KAYSERİ KIR NÜFUSUNUN DİJİTAL OKURYAZARLIK DÜZEYİ ve ÇEVİRİM İÇİ MAHREMİYET YÖNELİMLERİ

Bu bölümde, mevcut araştırmanın metodolojisi, yöntemi, sınırlılıkları ve kapsamına ilişkin beyanlar ve örneklemden toplanan veriler üzerinde yapılan analizler sonucu elde edilen bulgular yer almaktadır. Öncelikli olarak araştırmanın amacı, araştırma soruları ve bu sorulara paralel olarak literatürle ilişkili olarak kurulan hipotezler ifade edilmiş, daha sonra bu hipotezleri test etmek için kullanılan istatistiki testler basitçe açıklanmıştır. Bulgular başlığı ise araştırmada kullanılan her üç ölçeğe ilişkin hem betimsel hem de karşılaştırmalı istatistikleri içermektedir.

3.1. Araştırmanın Sorunu

Enformasyon ve iletişim teknolojilerinin (EİT) yaygınlaşması, bu teknolojilere erişimi olanlar ile olmayanlar arasındaki ayrımı (dijital bölünme) ortadan kaldırmaktadır. Cep telefonu kullanan kişi sayısı, internete erişimi olan hanehalkı sayısı ve mobil internet hizmetini kullanan kişi sayısını gösteren istatistikler, bu savı desteklemektedir. EİT'lere erişim, her ne kadar dijital bölünmenin erişim kaynaklı ayağını ortadan kaldırırsa da kullanım becerilerinden kaynaklanan bölünme (ikinci düzey dijital bölünme), halen güncel bir sorundur.

TÜİK'in yayınladığı en güncel istatistiklere göre, Türkiye nüfusunun yüzde 82,6'sı internet kullanmakta ve tüm hanelerin yüzde 92'si internete erişim sağlamaktadır (TÜİK, 2021c). Ancak, dijital yetenekler açısından bakıldığında, internete erişimi olanların neredeyse yarısı, düşük dijital yeteneklere sahiptir. 2019 yılı verilerine göre, Türkiye'de son üç ayda internete erişim sağlayan nüfusun yüzde 50'si, düşük dijital yeteneklere sahiptir (Eurostat, 2021). Düşük dijital yeteneklerle internet kullanmak, mahremiyet başta olmak üzere ekonomik riskleri de beraberinde getirir. Bireyler

arasındaki dijital yetenek farklılıkları aynı zamanda ikinci düzey dijital bölünmenin de kaynağıdır (van Deursen & van Dijk, 2014).

EİT kullanımının yaygınlaşması ve ağ toplumuna katılımın genişlemesi, dijital yetenekler bakımından yetersiz kalan vatandaşlar açısından sorunsaldır. Ayrıca, bu çalışmanın odaklandığı kırsal kesimde yaşayan vatandaşların, bu ağ toplumunda geçirdikleri süre dikkate alındığında, sorunun daha da derinleştiği söylenebilir. Çünkü kırsal kesimde karşılaşılabilecek altyapı ve erişim sorunları, özellikle mobil internet teknolojilerindeki gelişmeler sonucunda azalmış ve kırsal bölgelerde yaşayan vatandaşların EİT kullanımları artmıştır. Ağ toplumu ile tanışmaları, kent merkezlerinde ikamet eden bireylere göre daha yeni olan kırsal mahallelerde yaşayan bireylerin, bu yeni tanışıklığın bir sonucu olarak düşük dijital becerilere sahip olduğu ve bu düşük beceri düzeyi sebebiyle EİT kullanımlarının, özellikle mahremiyet ve kişisel bilgilerin güvenliği açısından riskler taşıdığı söylenebilir.

Bu bilgiler ışığında, bu araştırmanın sorununu, kırsal kesimde yaşayan ve EİT kullanan vatandaşların dijital okuryazarlık seviyelerinin tespit edilmesi ve mahremiyet yönelimleri ile dijital okuryazarlık seviyeleri arasında, anlamlı bir ilişki olup olmadığı oluşturmaktadır.

3.2. Araştırmanın Amacı

Araştırmanın sorununa paralel olarak, bu çalışmanın en temel amacı, kırsal kesimde yaşayan ve EİT'leri kullanmaya kentte yaşayanlara kıyasla daha yakın bir geçmişte başlayan bireylerin, bu teknolojilerle ve bu teknolojiler aracılığıyla kurdukları etkileşimleri, çevrim içi mahremiyet ve dijital okuryazarlık çerçevesinde ele almaktır.

Hızla kendini yenileyen EİT'lere erişebilmek, dijital bölünmenin ilk ayağını ortadan kaldırırsa da bu ayrımın tamamen ortadan kalkabilmesi için, bireylerin bu teknolojileri kullanma becerisine, başka bir şekilde ifade edilirse, dijital okuryazar olmaya ihtiyaçları vardır. Geleneksel olarak, yüz yüze iletişimin daha yaygın olduğu kırsal bölgelerde EİT kullanımının yaygınlaşması, bu teknolojilerle dolayımlanan iletişimi ve etkileşimi artırmaktadır. EİT kullanımındaki artış, dijital beceriler ve dijital okuryazarlıkla desteklenmediği takdirde, başta çevrim içi mahremiyet kaynaklı sorunlar olmak üzere çeşitli riskler yaratabilir. Bu bağlamda araştırmanın amacı; kırsal kesimde yaşayan bireylerin dijital okuryazarlık düzeylerini tespit etmek ve bu değişken ile başta

çevrim içi mahremiyet yönelimleri olmak üzere EİT kullanım sıklıkları gibi diğer değişkenlerle olan ilişkisini ortaya çıkarmaktır.

3.3. Araştırmanın Önemi

Literatürdeki çevrim içi mahremiyet araştırmaları, genellikle üniversite öğrencilerine ve kentte yaşayan nüfusa odaklanmaktadır. Kırsal bölgelerde yaşayan bireylerin internet kullanımlarına, bu kullanım pratiklerinden kaynaklanabilecek sorunlara ve risklere odaklanan araştırmalar ise oldukça azdır. Literatürdeki boşluğun yanı sıra, bu bölgelerde ikamet eden bireylere ilişkin sabit internet (ev interneti) hizmeti aboneliği, mobil internet hizmeti aboneliği, akıllı cep telefonu kullanım sıklığı gibi verileri barındıran istatistikî bilgiler de oldukça sınırlıdır.

Bunun yanı sıra, literatürde mahremiyet yönelimleri, çevrim içi mahremiyet endişeleri ve dijital okuryazarlık ile ilgili ayrı ayrı araştırmalar bulunmasına rağmen, dijital okuryazarlık seviyeleri ile mahremiyet yönelimleri arasındaki ilişkiyi açıklamaya çalışan bir araştırmaya rastlanmamıştır. Bu araştırma, çevrim içi mahremiyet yönelimleri ile dijital okuryazarlık arasındaki ilişkiye odaklanması ve araştırma evrenini kırsal bölgelerde yaşayan bireylerin oluşturması bakımından önemlidir. Bunun yanı sıra bu araştırma, kırsal bölgelerde yaşayan bireylerin EİT kullanımlarını betimleyecek istatistikler oluşturması bakımından da önemlidir.

3.4. Araştırma Soruları ve Hipotezleri

Kayseri'nin dört büyük (merkez) ilçesi dışındaki ilçelerinde, 2012'deki yasal düzenlemeden önce köy ve belde statüsünde olan mahallelerde yaşayan ve EİT kullanan nüfusu, evren olarak alan bu araştırmada cevabı aranan sorular ve bu sorulardan ve literatürden hareketle öne sürülen hipotezler aşağıda listelenmiştir:

AS 1: Köylerde yaşayan EİT kullanıcılarının dijital okuryazarlık düzeyi nedir?

Literatürde eşit olmayan zamansal, maddi, zihinsel, sosyal ve kültürel kaynaklara sahip kişilerin, dijital becerilerde ustalık da dahil olmak üzere, dijital medyaya az ya da çok erişimi açısından ayrıldıklarına değinilmektedir (van Dijk & van Deursen, 2014). Benzer şekilde, dijital beceriler bakımından sosyo-ekonomik geçmiş, statü ve uzak coğrafi konumlara ilişkin dikkati hak eden farklılıklardan söz edilebilir (Fraillon vd., 2015). Avustralya'daki altıncı ve onuncu sınıf öğrencileri üzerinde yapılan EİT becerileri testlerinde, büyükşehir okullarından gelen öğrenciler daha yüksek puanlar alırken uzak

okullardan gelen öğrenciler ise en düşük puanları almıştır ve bu farklılık istatistiksel açıdan anlamlıdır (Fraillon vd., 2018). Başka bir araştırmada ise EİT okuryazarlığının, arka plan değişkenleri ile (sınıf düzeyi, okul türü, ailenin kültürel sermayesi) ilişkili olduğu sonucuna ulaşılmıştır. Bu araştırmada, ailelerin kültürel sermayesinin öğrencilerin EİT okuryazarlık düzeyleri arasındaki farklılıkları arttırdığı görülür (Senkbeil vd., 2013).

Literatürdeki bu sonuçlara dayanarak aşağıdaki hipotez oluşturulmuştur.

H1: Köylerde yaşayan EİT kullanıcılarının dijital okuryazarlık düzeyleri düşüktür.

AS 1a: Bu düzey cinsiyetler arasında farklılık gösterir mi?

AS 1b: Bu düzey dijital göçmenler ve dijital yerliler arasında farklılık gösterir mi?

AS 1c: Bu düzey eğitim seviyelerine göre farklılık gösterir mi?

AS 1d: İnternete ilk erişim tarihi ile dijital okuryazarlık düzeyi arasında bir ilişki var mı?

AS 1e: Dijital okuryazarlık düzeyi ile ilk cep telefonu ve ilk akıllı cep telefonu edinme tarihleri arasında bir ilişki var mı?

AS 1f: Dijital okuryazarlık düzeyi ile sosyal medya kullanım sıklıkları arasında bir ilişki var mı?

AS 1g: Dijital okuryazarlık düzeyi ile internetten alışveriş yapıp yapmama tercihi arasında bir ilişki var mı?

Literatürdeki araştırmalar, kadınların kendi beceri düzeylerini önemli ölçüde daha düşük olarak değerlendirdiklerini göstermektedir. Ancak bu farklılık, sadece kadın ve erkeklerin kendi çevrim içi becerilerine ilişkin öz değerlendirmelerinde oluşmaktadır. Ölçülen gerçek yeteneklerde ise belirgin bir fark yoktur (Hargittai & Shafer, 2006). Hatta, Avustralya’da orta okul ve lise öğrencileri (6 ve 10. sınıf) üzerinde yapılan EİT okuryazarlığı araştırmasında, her iki sınıfta da kız öğrenciler erkeklerden daha iyi performans göstermiştir ve bu fark istatistiksel olarak anlamlıdır (Fraillon vd., 2018). Literatürdeki bu sonuçlara rağmen, Türkiye OECD ülkeleri arasında, özellikle ileri yaştaki yetişkinlerde olmak üzere, bilgi işleme becerilerinde cinsiyete dayalı farklılıkların en yüksek olduğu ülkelerden biridir (Çalışma ve Sosyal Güvenlik Bakanlığı, 2016).

van Laar ve arkadaşları (2019), literatürdeki genel kanının, tüm yaşamları boyunca internete maruz kalmaları sebebiyle genç nesillerin dijital olarak daha yetenekli

oldukları yönünde olduğunu ifade ederler. Eğitim faktörü de dijital beceriler üzerinde etkilidir. Araştırmalar, eğitim düzeyinin daha yüksek dijital becerilerle sonuçlandığını doğrulamaktadır (van Deursen vd., 2011).

İnternete daha eski bir kullanıcısı olma ve akıllı cep telefonunu daha erken edinmiş olma gibi değişkenlerin, dijital okuryazarlık düzeylerinde olumlu bir etkisi olduğu söylenebilir. Avustralya’da yapılan bir araştırmada, yüksek seviyede dijital cihaz deneyimi ile daha yüksek EİT okuryazarlığı seviyesi ile ilişkilendirilir (Fraillon vd., 2018).

Literatüre dayanarak yukarıdaki araştırma soruları için aşağıdaki hipotezler oluşturulmuştur.

H2: Kadın ve erkek katılımcıların dijital okuryazarlık düzeyleri farklıdır.

H3: Erkeklerin dijital okuryazarlık düzeyi kadınlara kıyasla daha yüksektir.

H4: Dijital göçmenler ve dijital yerlilerin dijital okuryazarlık düzeyleri farklıdır.

H5: Yaş ile dijital okuryazarlık seviyesi arasında negatif yönde bir ilişki vardır.

H6: Eğitim seviyesi ile dijital okuryazarlık seviyesi arasında pozitif yönde bir ilişki vardır.

H7: İnterneti daha erken kullanmaya başlayanların dijital okuryazarlık düzeyi daha yüksektir.

H8: Akıllı cep telefonlarını daha erken edinen katılımcıların dijital okuryazarlık düzeyi daha yüksektir.

AS 2: Köylerde yaşayan EİT kullanıcılarının mahremiyet yönelimleri nasıldır?

AS 2a: Bu yönelim, cinsiyetler arasında farklılık gösterir mi?

AS 2b: Bu yönelim, yaş grupları arasında farklılık gösterir mi?

AS 2c: Bu yönelim, eğitim düzeyine göre farklılık gösterir mi?

AS 2d: Bu yönelim, internete ilk erişim tarihine göre farklılık gösterir mi?

AS 2e: Sosyal medya ve anlık mesajlaşma programlarında kullanılan ayarlar ile mahremiyet yönelimleri arasında bir ilişki var mı?

AS 2f: Bu yönelim, sosyal ağ siteleri ve/veya uygulamalarını kullanma sıklıklarına göre farklılık gösterir mi?

AS 2g: Bu yönelim, internetten alışveriş yapanlar ve yapmayanlar arasında farklılık gösterir mi?

AS2h: Kimlik ögelerini sosyal medyada paylaşılanlar ve paylaşmayanlar arasında mahremiyet yönelimleri açısından anlamlı bir farklılık var mı?

AS 2i: Akıllı cep telefonunda şifre kullanımı ile mahremiyet yönelimi arasında bir ilişki var mı?

Petronio'nun (2002) İMY teorisine göre, bireyler mahremiyetlerini kimi kurallara göre yönetir. Bu kurallarının belirlenmesinde etkili olan değişkenlerden biri cinsiyettir. Literatürde, mahremiyet endişesinin kadınlarda erkeklere oranla daha yüksek olduğunu işaret eden araştırmalar mevcuttur (Fogel & Nehmad, 2009; Hoy & Milne, 2010; Taddicken, 2014). Ayrıca, 2012-2015 yılları arasında gerçekleştirilen bir AB projesinin verileri üzerinde yapılan analizlerde, bireysel mahremiyet tercihlerinin yaş, cinsiyet ve eğitim durumuna göre değişkenlik gösterdiği görülmüştür (Potoglou vd., 2017). Bu bulgulardan hareketle aşağıdaki hipotezler oluşturulmuştur.

H9: Kadın ve erkek EİT kullanıcılarının mahremiyet yönelimleri farklıdır.

H10: Mahremiyet yönelimleri yaşa göre farklılık gösterir.

H11: Mahremiyet yönelimleri eğitim düzeyine göre farklılık gösterir.

H12: İnternette alışveriş yapanlar ile yapmayanların mahremiyet yönelimleri farklıdır.

AS 3: Köylerde yaşayan EİT kullanıcıları sosyal medya uygulamaları, kamu kurum ve kuruluşlarının e-hizmetler için geliştirdikleri uygulamaları (dijital vatandaşlık uygulamaları) ve internet (ev ya da mobil), cep telefonu, bilgisayar (laptop ya da masaüstü), tablet ve televizyon gibi teknolojileri ne sıklıkta kullanıyorlar?

AS 3a: Sosyal ağ siteleri ve/veya uygulamalarını kullanma sıklıkları nedir?

AS 3b: Cep telefonlarını kullanma sıklıkları nedir?

AS 3c: Bu cihaz, teknoloji veya uygulamaları kullanma sıklıkları 2020 Covid-19 salgını öncesine kıyasla farklılık gösterdi mi?

AS 3d: Köylerde yaşayan EİT kullanıcıları arasında en yaygın kullanılan sosyal ağ siteleri ve/veya uygulamaları hangileridir?

AS 3e: Kamu hizmeti uygulamalarını kullanma sıklıkları ne kadardır?

AS 3f: Bu teknolojileri kullanım sıklıkları cinsiyete göre farklılık gösterir mi?

AS 3g: Bu teknolojileri kullanma sıklıkları yaşa göre farklılık gösterir mi?

H13: Köylerde yaşayan EİT kullanıcılarının uygulama, cihaz ve teknoloji kullanım sıklıkları cinsiyete göre anlamlı bir farklılık gösterir.

H14: Köylerde yaşayan EİT kullanıcılarının uygulama, cihaz ve teknoloji kullanım sıklıkları yaşa göre anlamlı bir farklılık gösterir.

AS 4: Köylerde yaşayan EİT kullanıcıları ne kadar süredir bu teknolojileri kullanıyorlar?

AS 4a: İlk cep telefonlarını ne zaman aldılar?

AS 4b: İlk akıllı cep telefonlarını ne zaman aldılar?

AS 4c: Sabit hatlı internet (ev interneti) ya da mobil internet abonelikleri var mı?

AS 4d: İnternete ilk ne zaman bağlandılar?

AS 4e: İnternete ilk defa hangi cihazla eriştiler?

AS4f: Bu teknolojilere ve cihazlara erişim tarihi cinsiyete ve yaşa göre farklılık gösterir mi?

AS 5: Köylerde yaşayan EİT kullanıcılarının dijital okuryazarlık düzeyleri ile mahremiyet yönelimleri arasında istatistiksel olarak anlamlı bir ilişki var mıdır?

H15: Dijital okuryazarlık düzeyi ile mahremiyet yönelimi arasında istatistiksel olarak anlamlı ve pozitif yönlü bir ilişki vardır.

AS 6: Köylerde yaşayan EİT kullanıcılarının dijital okuryazarlık düzeyleri ile dijital vatandaşlık düzeyleri arasında bir ilişki var mıdır?

H16: Dijital okuryazarlık düzeyi ile dijital vatandaşlık düzeyi arasında istatistiksel olarak anlamlı ve pozitif yönlü bir ilişki vardır.

AS 7: Dijital vatandaşlık düzeyi ile mahremiyet yönelimleri arasında istatistiksel olarak anlamlı bir ilişki var mıdır?

AS 8: Köylerde yaşayan EİT kullanıcılarının sosyal medyada ve genel olarak internette kişisel bilgilerini paylaşma oranları nedir?

AS 8a: Bu oranlar, cinsiyetler arasında farklılık gösterir mi?

AS 8b: Bu oranlar, dijital göçmenler ve dijital yerliler arasında farklılık gösterir mi?

AS 8c: Bu oranlar, mahremiyet yönelimlerinin alt boyutlarına göre farklılık gösterir mi?

AS 9: Köylerde yaşayan EİT kullanıcıları bu teknolojiler aracılığı ile kimlerle iletişim kurarlar?

3.5. Araştırmanın Kapsam ve Sınırlılıkları

Araştırmanın evrenini Kayseri'nin kırsal nüfusu oluşturmaktadır. Bu sebeple araştırma, Kayseri ilinin kırsal mahallelerinde yaşayan bireyleri kapsamaktadır. Ayrıca kullanılan olasılık dışı örnekleme yöntemi, tüm evrene genelleme imkanının önünde bir engeldir. Literatürde hem dijital okuryazarlık düzeyi ile çevrim içi mahremiyet yönelimlerini birbirleri ile ilişkileri bağlamında inceleyen hem de bu araştırmayı kırsal nüfus üzerinden yapan başka araştırma yoktur. Bu karşılaştırmaya ilişkin hipotez üretmek için referans olabilecek literatürün olmayışı araştırmanın bir diğer sınırlılığıdır.

Araştırma örnekleminin kadın-erkek dağılımı, cinsiyetler arasında karşılaştırma yapmak için yeterli olsa da eşit ya da eşite yakın bir dağılım göstermediği için bir sınırlılık yaratmaktadır. Aynı zamanda, bulgular kısmında da ele alınacağı gibi, araştırmadaki kullanılan çevrim içi mahremiyet yönelimleri ölçeği ile elde edilen veriler, normal dağılım göstermediği için, bu ölçeğin kullanıldığı analizlerde parametrik olmayan testler kullanılmıştır. Bu testlerin parametrik olanlara kıyasla, daha zayıf sonuçlar sağladığı bilinmektedir. Ayrıca parametrik olmayan testler ile yapılan analizler, evrene genellenemez (Geray, 2014). Bu da araştırmanın bildirilmesi gereken bir sınırlılığıdır.

Araştırmada kullanılan ölçeklerin tamamı, farklı dil ve kültürler için oluşturulan ve daha sonra Türkçeye uyarlanan ölçeklerdir. Her ne kadar bu ölçekler, adaptasyon çalışmaları ile geçerlilik ve güvenilirliklerini ispatlamış olsalar da mevcut çalışmanın örnekleme hitap eden yapıda değillerdir. Aşağıdaki faktör analizlerinde de bahsedildiği gibi, on altı madde ile dört boyuta dağılması beklenen mahremiyet yönelimleri ölçeğinin, öngörüldüğü gibi bir faktör dağılımı sergilememesinin nedeni de ölçeğin orijinal örnekleme ile mevcut örneklemin sosyo-ekonomik ve kültürel farklılığıdır. Bu sebeple, ölçeğin dört maddesi çıkarılmış ve dört faktörlü dağılım sağlanmıştır.

Dijital becerilerin ölçülmesi ile ilgili olarak üç farklı ölçüm metodundan söz edilebilir: (1) öz değerlendirme (*self-assessments*), (2) bilgiye dayalı değerlendirme (*knowledge-based assessment*) ve (3) performansa dayalı değerlendirme (*performance-based assessment*). İlk yöntemde, katılımcılardan kendi bilgi, yetenek, güven veya kullanım düzeylerini derecelendirmelerini isteyerek ölçüm yapılır. İkinci yöntemde,

olgusal veya prosedürel bilgi ile ilgili sorular kullanarak beceriler test edilir. Değerlendirme sonuçları, genellikle çoktan seçmeli sorulara verilen bir dizi yanıt olarak sunulur ve öz değerlendirmelere kıyasla, daha doğru bir tablo sunabilir. Performansa dayalı değerlendirme ise tarayıcılar ve metin işleme yazılımları gibi araçlar kullanarak, gerçek durumlarda gerçek dijital beceri performansını ölçer. Bu yöntem, dijital becerileri ölçmenin en geçerli yolu olarak nitelendirilebilir (ITU, 2020a). Bu çalışmada, dijital okuryazarlığın ölçülmesi için, on maddelik bir öz-değerlendirme anketi kullanılmış olması, çalışmanın bir diğer sınırlılığıdır.

Tüm dünyayı etkisi altına alan ve 2020 yılının Mart ayından itibaren Türkiye’de görülmeye başlanan Sars-Cov-2 virüsü kaynaklı Covid-19 hastalığı, bu çalışmanın 2020 yılı içerisinde yapılması planlanan saha araştırmasının ertelenmesine neden olmuştur. Salgın ayrıca, sahada yapılması öngörülen derinlemesine mülakatlara da hem araştırmacı hem de katılımcı sağlığı açısından engel olmuştur ve araştırmanın verilerini, sahada 374 kişiye uygulanan anketler ile sınırlamıştır.

3.6. Araştırmanın Yöntemi

Araştırmada kullanılan veriler, yüz yüze anket araştırması yöntemi ile elde edilmiştir. Tarihsel olarak, kullanımı en yaygın anket araştırmaları olan yüz yüze anket araştırmalarının, telefon, posta veya çevrim içi anket araştırmalarına kıyasla en temel farkı, katılımcı ile anketçi arasındaki doğrudan kişisel iletişimidir (Stockemer, 2019). Standart prosedürler kullanarak bireylerden sistematik bilgi toplamayı içeren anket araştırmasında, araştırma evreninden (rastgele veya temsili) bir örneklem seçilir ve seçilen örnekleme tutumlar, algılar veya davranışlar hakkında bir veya birkaç soru sorulur (Stockemer, 2019). Tarama araştırması da olarak nitelendirilen bu yöntem, sosyal bilimlerdeki pozitivist yaklaşım içerisinde geliştirilmiştir ve doğası gereği istatistiksel veriler üretir (Neuman, 2010b). Araştırmada katılımcılardan sadece bir kez veri toplandığı için kesitsel, katılımcılara önceden yaşamış oldukları deneyimlere ilişkin sorular içerdiği için de geçmişe dönük tarama araştırması olarak nitelendirilebilir (Büyüköztürk vd., 2014).

Araştırmada kullanılan anket formu, üç farklı ölçek ve kullanım sıklıklarını ölçmek için beşli likert; paylaşım tercihleri için evet-hayır; yaş ve tarih bilgileri için nümerik açık uçlu ve eğitim, cinsiyet gibi değişkenler için de kategorik sorular

içermektedir. Tarama araştırması, 18 Ağustos 2021 – 30 Ağustos 2021 tarihleri arasında Kayseri'nin kırsal mahallelerinde gerçekleştirilmiştir. Anketler, hizmet alımı prosedürleri uygulanarak anlaşma sağlanan bir araştırma şirketi tarafından istihdam edilen 7 anketçi tarafından uygulanmıştır. Anketçiler, araştırma şirketi tarafından sağlanan tablet cihazlara yüklenen soru formunu katılımcılara okumuş ve katılımcının verdiği cevapları doğrudan işlemişlerdir. Bu yöntem hem kâğıt israfını ortadan kaldırması hem de saha araştırması sonrası veri girişi sürecini ve bu süreçte oluşabilecek kodlama hatalarını ortadan kaldırması açısından faydalıdır.

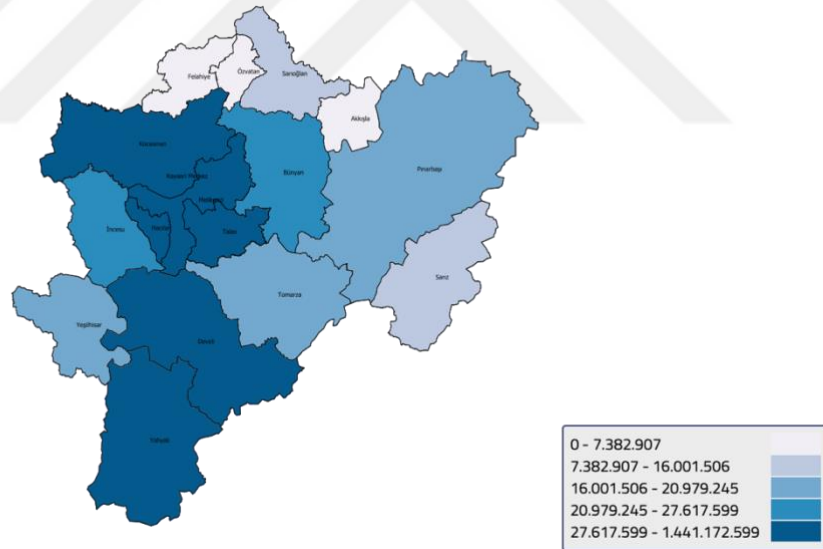
3.7. Araştırmanın Evreni ve Örneklemi

2012 yılında yürürlüğe giren, 6360 sayılı kanunun birinci maddesinin üçüncü fıkrası ile büyükşehirlere bağlı ilçelerin mülki sınırları içerisinde yer alan köy ve belde belediyelerinin tüzel kişiliği kaldırılmış ve köyler, mahalle olarak bağlı bulundukları ilçenin belediyesine dahil edilmiştir (On Dört İlde Büyükşehir Belediyesi ve Yirmi Yedi İlçe Kurulması İle Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun, 2012). Yapılan bu değişiklik ile Türkiye'deki hiçbir büyükşehir belediyesine bağlı köy kalmamıştır. Mevzuatta yapılan bu değişiklik öncesinde, yani 2012 yılında, ülke nüfusunun yaklaşık yüzde 23'ü, köy ve beldelerde yaşamaktadır. Bir sonraki yılın istatistiklerinde ise bu oran yüzde 8,7'ye düşmüştür (TÜİK, 2021a). Türkiye'nin kırsal nüfusunda yaşanan bu dramatik azalmanın, sadece istatistiki boyutta olduğu söylenebilir. Çünkü köy statüsünden mahalle statüsüne geçen ikametgâh noktalarında, böyle bir azalma söz konusu değildir.

2012 yılı öncesinde, Kayseri'deki tüm ilçelerde toplam 424 köy bulunmaktadır. Yasa sonrası, bu köylerin neredeyse tamamı (413), mahalle statüsü kazanmış, 11 tanesi ise kapatılmıştır. Adrese Dayalı Nüfus Kayıt Sistemi verilerine bakıldığında, kapatılan köy/mahalleler ile ilgili olarak 2017 yılından bu yana bir nüfus istatistiği yoktur. Bu durumda, bu araştırmanın evrenini, Kayseri ili sınırları içerisinde yer alan, dört merkez ilçe (Melikgazi, Kocasinan, Hacılar ve Talas) dışındaki on iki ilçede bulunan ve 2020 yılı mahalli nüfus verilerine göre, en az 14 (Kozluca) ve en fazla 3374 (Palas) kişinin yaşadığı, 384 mahallede ikamet eden, toplamda 117.918 kişi içerisindeki EİT kullanıcıları oluşturmaktadır.

Dağınık bir yapıda olan bu evrende, verilerin toplanacağı örneklemin seçiminde, önce bir alt küme olarak anketin uygulanabileceği ilçeler ve köyler belirlenmiştir. Nihai örnekleme unsurlarını içinde barındıran ilçe ve köyler, geçici olarak örneklem unsuru olarak değerlendirilmiştir (Neuman, 2010a). Bu yöntem, küme örneklemin ilk aşaması olarak değerlendirilebilir, ancak araştırma örneklemini, küme örneklemin önerdiği şekilde rastlantısal belirlenmemiştir. Araştırma, kırsal kesimde yaşayan ve EİT kullanan, internete düzenli olarak bağlanan katılımcıları hedeflediği için anketin uygulanacağı ilçe ve köylerin belirlenmesinde, Sanayi ve Ticaret Bakanlığı'nca yürütülen Türkiye'de Kentsel ve Kırsal Yerleşim Sistemleri Araştırması'nın (YER-SİS) sağladığı, mobil sinyal yoğunlukları haritaları, ilçelerin sosyo-ekonomik gelişmişlik sıralamaları (SEGE) ve TÜİK'in Adrese Dayalı Nüfus Kayıt Sistemi'nden çekilen mahalle nüfusları dikkate alınmıştır. Bu sebeple, ilçe ve mahallelerin seçiminde kullanılan yöntem, amaçlı -kasti- örnekleme yöntemi olarak ifade edilebilir.

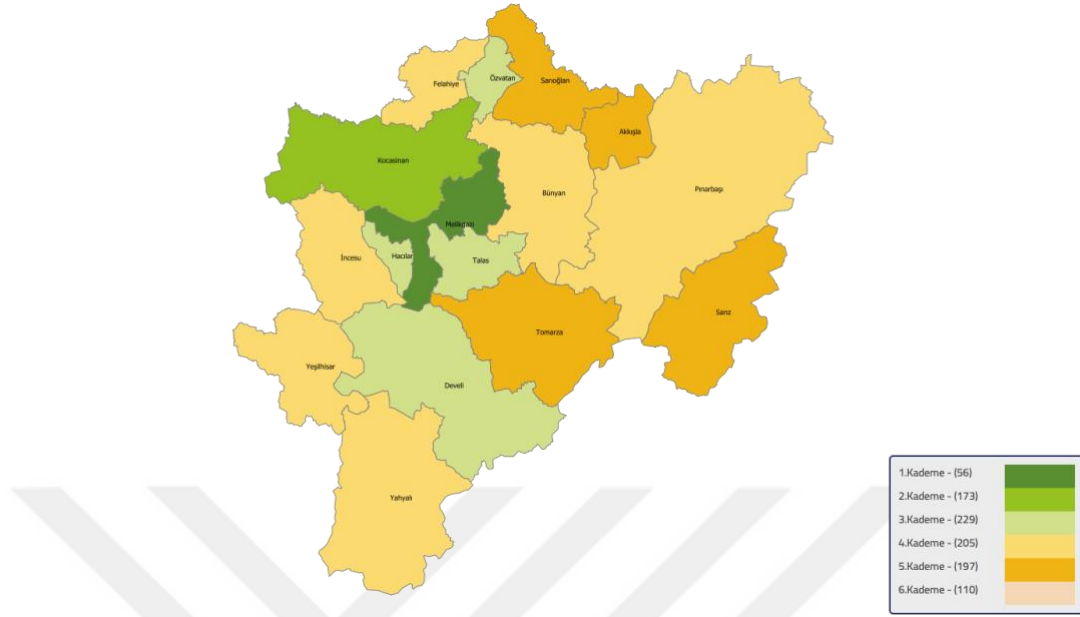
Şekil 3.1: Kayseri İlçelerindeki Mobil Sinyal Yoğunlukları



Kaynak: (Sanayi ve Teknoloji Bakanlığı, 2020)

Yukarıdaki harita, Kayseri'nin ilçelerindeki mobil sinyal yoğunluklarını göstermektedir. Merkez dört ilçe dışında, mobil sinyalin en yoğun olduğu ilçeler; Develi ve Yahyalı'dır. Sinyal yoğunluğunun en düşük olduğu ilçeler ise Akkışla, Felahiye ve Özvatan'dır. Bu sinyal yoğunluklarının, ilçenin nüfusu ile ilişkili olduğu söylenebilir.

Şekil 3.2: Kayseri İlçelerinin Sosyo-Ekonomik Gelişmişlik Kademeleri



Kaynak: (Sanayi ve Teknoloji Bakanlığı, 2020)

Kayseri'nin on altı ilçesinin sosyo-ekonomik gelişmişlik kademelerini gösteren haritada, en koyu yeşil renkle gösterilen ve Türkiye'nin en gelişmiş 38. ilçesi olan Melikgazi ile onu takip eden Kocasinan (151.), Talas (252.) ve Hacılar (289.) ilçeleri bu çalışma evrenine dahil değildir. İlçelerin, SEGE-2017'deki sıralamaları dikkate alınarak; üç, dört ve beşinci kategoriden ikişer ilçe örnekleme dahil edilmiştir. Bu ilçeler; Özvatan, Develi, İncesu, Bünyan, Sarıoğlu ve Tomarza'dır (Yılmaz vd., 2019, s. 102). İlçelerin seçiminde, amaçlı -kasti- örnekleme yöntemi kullanılmıştır. Bu yöntemde, araştırmacı önceki bilgi, deneyim ve gözlemlerden faydalanarak araştırmanın amacına uygun olan birimleri örnekleme dahil eder (Ural & Kılıç, 2013).

SEGE kademelerine göre belirlenen bu ilçelerden, çalışma evrenine dahil olabilecek kriterlere sahip olan (2012 öncesi köy ve belde olan) mahalleler arasından on sekiz tanesi, nüfus yoğunlukları ve mobil sinyal haritalarındaki sinyal yoğunluklarının dikkate, alındığı amaçlı örnekleme yöntemi ile belirlenmiştir. Mahalleler belirlendikten sonra, ilgili mahallelerde (eski köy ve beldeler) kolayda örneklem yöntemi ile örneklem oluşturulmuştur. Olasılık dışı örnekleme yöntemlerinden olan kolayda örnekleme (*convenience sampling*), bireylerin hazırda bulundukları için seçildiği bir tekniktir. Birincil seçim kriteri, bilgi alma kolaylığı ile ilgilidir (Stockemer, 2019). Bu örnekleme

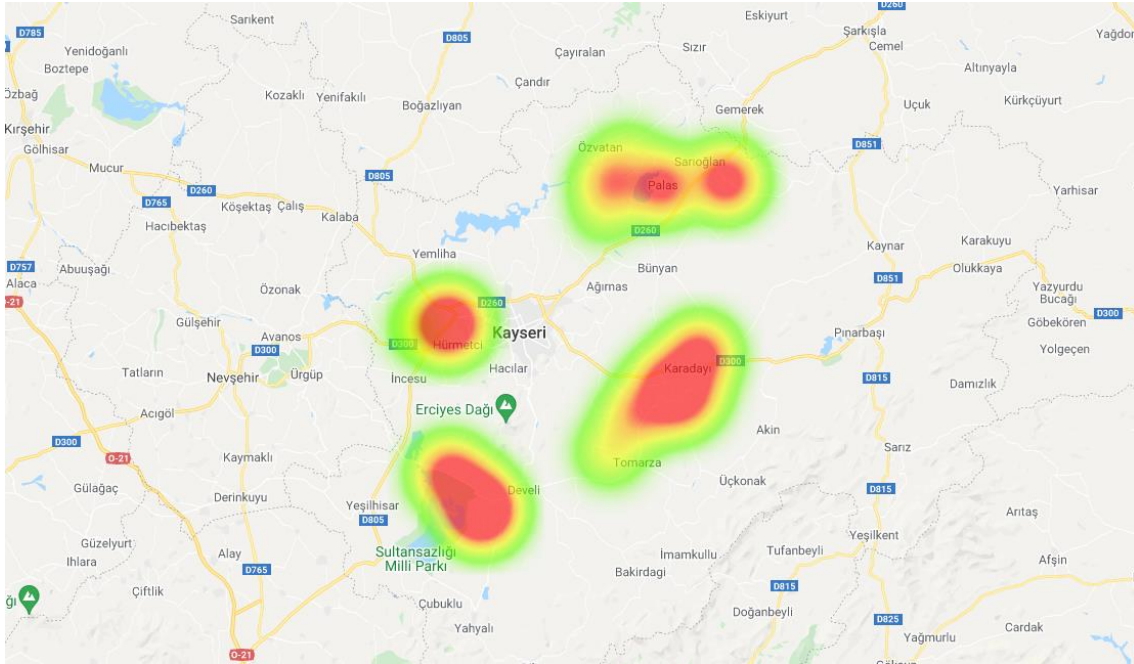
yöntemi, kazara ya da elverişli örnekleme yöntemi olarak anılmaktadır ve bu yöntemde temel amaç, zaman, para ve işgücü kaybını önlemektir (Büyüköztürk vd., 2014). Araştırma büyük oranda, internet ve akıllı cep telefonu kullanımına ilişkin olduğu için anket formunun başına, “Akıllı telefonunuz var mı?” sorusu eklenmiş ve bu soruya hayır cevabını verenler örnekleme dahil edilmemiştir.

Tablo 3.1: Örnekleme Dahil Edilen İlçeler ve Toplam Katılımcı Sayıları

İlçe	SEGE Kademesi	SEGE Sırası	Katılımcı Sayısı	Oran (%)
Özvatan	3	394	15	4.0%
Develi	3	405	55	14.7%
İncesu	4	502	25	6.7%
Bünyan	4	581	85	22.7%
Sarıoğlu	5	696	111	29.7%
Tomarza	5	713	83	22.2%
TOPLAM			374	100%

Yukarıdaki tablo, örnekleme dahil edilen ilçeler ve bu ilçelerdeki toplam katılımcı sayısını göstermektedir. Aşağıdaki harita ise anketlerin uygulandığı noktaların koordinat bilgileri ile oluşturulan ısı haritasıdır.

Şekil 3.3: Araştırmanın Uygulandığı Konumların Oluşturduğu Isı Haritası



Aktarılan bilgiler doğrultusunda, araştırmanın örneklemini, Kayseri'nin altı farklı ilçesinde 2012 öncesinde köy ya da belde statüsünde olan mahallelerinde ikamet eden ve akıllı telefona sahip olan 374 kişi oluşturmaktadır. Örneklem ile ilgili detaylar, bulgular başlığı altında paylaşılmıştır.

3.8. Araştırmanın Bilimsel Etiğe Uygunluğu

Bu araştırma, Erciyes Üniversitesi Sosyal ve Beşerî Bilimler Etik Kurulu'na yapılan 326 numaralı başvuruya istinaden, 29.06.2021 tarihli kurul toplantısında görüşülmüş ve etik açıdan uygun bulunmuştur.

3.9. Kullanılan Ölçekler ve Soru Formu

Araştırma için oluşturulan soru formunda, Baruh ve Cemalcılar (2014) tarafından geliştirilen ve Baruh, Bal ve Cemalcılar (2015) tarafından İstanbul'daki bir vakıf üniversitesinde okuyan 379 Twitter kullanıcısı öğrenci üzerinde gerçekleştirilen uygulama ile Türkçeye uyarlanan çok boyutlu mahremiyet yönelimi ölçeği (*multidimensional privacy orientation scale*), Ng'nin (2012b) geliştirdiği ve Üstündağ, Güneş ve Bahçivan (2017) tarafından Türkçeye uyarlanan dijital okuryazarlık ölçeği (*digital literacy scale*) ve Choi, Glassman ve Cristol'ün (2017) geliştirdikleri ve Erdem ve Koçyiğit (2019) tarafından Türkçeye uyarlanan, dijital vatandaşlık ölçeğinin beş maddesi (*digital citizenship scale*) kullanılmıştır.

Çok boyutlu mahremiyet yönelimi ölçeği, dört farklı yönelim boyutu tanımlar: (1) bir hak olarak mahremiyet (*belief in the value of privacy as a right*), (2) kendi enformasyonel mahremiyetine ilişkin kaygı (*concern about own informational privacy*), (3) başkalarının mahremiyetine ilişkin kaygı (*concern about privacy of others*) ve (4) diğer ihtimalli mahremiyet (*other-contingent privacy*) (Baruh & Cemalcılar, 2014, s. 169; Baruh vd., 2015; Livberber Göçmen, 2018, s. 120). Ölçekten elde edilen veriler, üç farklı mahremiyet kümesi tanımlar: (1) mahremiyet savunucuları (*privacy advocates*), (2) mahremiyet bireycileri (*privacy individualists*) ve (3) mahremiyet umursamazları (*privacy indifferents*). Mahremiyet savunucuları, kendi mahremiyetleri ile diğer insanların mahremiyetleri için de endişe duyanları tanımlarken mahremiyet bireycileri çoğunlukla sadece kendi mahremiyetleri ile ilgili endişeler taşırlar. Mahremiyet umursamazlarının ise yukarıdaki dört boyutun tümünde, diğer iki gruptan daha düşük skor alanlardan oluşur (Baruh & Cemalcılar, 2014).

Araştırmada, dijital okuryazarlık ölçeğindeki bazı maddeler, araştırma örneklemine hitap edebilmesi için değiştirilmiştir. Ölçeğin dokuzuncu maddesindeki “bilgi ve iletişim teknolojileri, bir projede çalışma ve diğer öğrenme etkinlikleri konusunda akranlarımla daha iyi işbirliği yapmamı sağlar” ve onuncu maddesindeki “üniversitedeki çalışmalarında, arkadaşlarımla internet üzerinden (ör. Skype, Facebook, Bloglar aracılığıyla) sıklıkla yardımlaşırım” ifadeleri, sırasıyla “bilgi ve iletişim teknolojileri, yakın çevremle ve akranlarımla daha iyi işbirliği yapmamı ve iletişim kurmamı sağlar” ve “yakın çevremle, akranlarımla ya da arkadaşlarımla internet üzerinden (ör. Facebook, Twitter, WhatsApp, Bloglar aracılığıyla) sıklıkla yardımlaşırım” şeklinde değiştirilmiştir.

Soru formunda, yukarıda değinilen ölçeklerin yanı sıra, Stutzman’ın kimlik öğelerinden hangilerinin sosyal ağ profillerinde ve genel olarak internette paylaşıldığını belirlemek için, katılımcılara ad-soyad, e-posta adresi, yaşanılan şehir, telefon numarası, eğitim durumu, cinsiyet, memleket, doğum tarihi, fotoğraf, meslek, ilişki durumu, ilgi alanları ve siyasi görüş bilgilerini paylaşp paylaşmadıklarını belirleyen on üç evet-hayır sorusu yöneltilmiştir. Sosyal ağ sitelerinin ilk dönemlerinde, Stutzman (2006) tarafından belirlenen yirmi altı maddelik kimlik öğeleri listesi, EİT kullanıcılarının kendileri hakkında hangi bilgileri paylaştığını belirlemek için faydalı bir referans noktası oluşturur.

Araştırmada kullanılan soru formunda, katılımcıların hangi sosyal medya, anlık mesajlaşma ve kamu hizmeti uygulamalarını ve internet (ev ya da mobil), cep telefonu, bilgisayar (dizüstü ya da masaüstü), tablet ve televizyon gibi teknoloji ve cihazlardan hangilerini ne sıklıkla kullandıklarını belirlemek için, beşli ölçekte (hiç kullanmam – her zaman kullanırım) on sekiz soru sorulmuştur. Bu soruları takiben katılımcılara, Covid-19 salgını sonrasında bu kullanımlarında bir değişiklik (azalma veya artma) olup olmadığı sorusu da yöneltilmiştir. Böylece, araştırmanın öneri safhasında öngörülmesi mümkün olmayan ve tüm dünyayı etkisi altına alan bu talihsiz gelişmenin, katılımcıların kullanımlarına olan etkisi de tespit edilmiştir.

Soru formunda, ölçeklerden bağımsız olarak ve özellikle çok boyutlu mahremiyet ölçeği ile ölçülen yönelimlerin, kullanıcı davranışlarına yansımaları ortaya koymak için katılımcılara, sosyal medya uygulamalarında gizliliği korumak için sunulan, varsayılan seçenekleri değiştirip değiştirmedikleri (hiçbirini değiştirmedim – tamamını değiştirdim)

ve bu uygulamalarda oluřturdukları profillerinin, kimler tarafından görülebilir olduđu sorulmuřtur. Katılımcılara, mahremiyet davranıřları ile iliřkili olabileceđi düşünölen, cep telefonunda řifre kullanımı ve bu řifrenin kimlerle paylařıldıđı ile anlık mesajlařma uygulamalarındaki (WhatsApp, BİP, Telegram vb.) son görölme ve mavi tik gibi özelliklerin kullanımına ve internetten alışveriş yapıp yapmadıklarına iliřkin beř soru sorulmuřtur.

Soru formu, katılımcıların anlık mesajlařma uygulamaları aracılıđıyla kimlerle iletiřim kurduđunu belirlemeyi amaçlayan bir soru da içermektedir. Soru, annemle, babamla, kardeşlerimle, eşimle, evlatlarımla, arkadaşlarımla, aynı köyde ikamet ettiđimiz akrabalarımla, řehir dıřında ikamet eden akrabalarımla ve yurt dıřında ikamet eden akrabalarımla řeklinde, dokuz farklı seçenek içermektedir.

Arařtırmada kullanılan soru formu ile ilgili olarak son değinilmesi gereken nokta, formda yer alan ve katılımcıların ne kadar süredir internet, cep telefonu ve akıllı telefon kullandıklarını belirlemeyi hedefleyen sorulardır. Bu sorulardan elde edilen bulgular, katılımcıların dijital okuryazarlık seviyeleri ile iliřkisi aćısından değeriendirilmiřtir.

3.10. Güvenilirlik ve Geçerlilik

Arařtırmada kullanılan dijital okuryazarlık ölçeđi (Ng, 2012b), Üstündađ ve arkadaşları tarafından (2017) Türkçeye uyarlanmıřtır. Bu ölçek adaptasyonu çalışması sonucu, on maddenin toplam Cronbach Alpha güvenilirlik skoru 0.86'dır ve yapılan keřfedici faktör analizine (EFA) göre, varyansın yüzde 40'ını aćıklayan tek bir faktör oluřmuřtur. Bu çalışmada ise, ölçeđin bazı ifadeleri çalışma örneklemine hitap edecek řekilde değıştirilmiř ve 374 kiřiye uygulanmıřtır. Çalışma sonucu bu ölçek ile toplanan verilere uygulanan güvenilirlik analizine göre Cronbach Alpha 0.861'dir.

Mahremiyet yönelimlerini, dört farklı boyutta ölçen ve Baruh ve Cemalcılar (2014) tarafından geliřtirilen ölçek, Baruh vd. (2015), Kezer vd. (2016) ve Livberber-Göçmen (2018) tarafından kullanılmıř ve bu çalışmalardaki Cronbach Alpha değeriileri ile güvenilir ve geçerli olduđunu göstermiřtir. Ölçekteki tüm boyutlara iliřkin Cronbach Alpha değeriilerini içeren tablo ařađıdadır.

Tablo 3.2: Çok Boyutlu Mahremiyet Yönelimleri Ölçeği'nin Cronbach Alpha Skorları

Boyutlar	Baruh ve Cemalcılar (2014)	Baruh vd. (2015)	Kezer vd. (2016)	Livberber-Göçmen (2018)	Bu Çalışma
Bir hak olarak mahremiyet	0.83	0.831	0.83	0.675	0.793
Kendi mahremiyetine ilişkin kaygı	0.83	0.831	0.83	0.758	0.673
Başkalarının mahremiyetine ilişkin kaygı	0.88	0.702	0.88	0.732	0.810
Diğer ihtimalli mahremiyet	0.85	0.691	0.86	0.794	0.845

Kaynak: (Baruh vd., 2015; Baruh & Cemalcılar, 2014; Kezer vd., 2016; Livberber Göçmen, 2018)

Choi ve arkadaşları (2017) tarafından geliştirilen ve Erdem ve Koçyiğit (2019) tarafından Türkçeye adapte edilen dijital vatandaşlık ölçeği, on sekiz maddeye ve beş farklı faktöre sahiptir. Orijinal ölçek 0.88, Türkçe adaptasyonu ise 0.87 Cronbach Alpha değeri ile güvenilirliklidir. Ancak bu ölçekteki maddelerin çoğunda yer alan ifadelerin, bu araştırmanın örneklemini üzerinde bir karşılık bulacağı düşünülmeyişi için, sadece beş maddesi kullanılmıştır. Bu beş maddenin Cronbach Alpha değeri ise 0.805 olarak hesaplanmıştır.

3.11. Verilerin Analizinde Kullanılan İstatistik Testler

Araştırmada sonucu elde edilen veriler, yüklenici firma tarafından kodlanmış bir şekilde Excel formatında araştırmacıya teslim edilmiştir. Bu veriler, IBM SPSS Statistics for Mac 28 uygulamasında gerekli değişken tanımlamalarının yapılmasının ardından içeri aktarılmış ve bu program ile analiz edilmiştir. Normal dağılım gösteren değişkenler için parametrik testler, normallik varsayımını sağlamayan mahremiyet yönelimleri ölçeğinin dahil olduğu analizler için de parametrik olmayan testler kullanılmıştır. Parametrik testler, "bir popülasyon hakkındaki tanımlayıcı istatistikler" olarak da bilinen bir parametreye dayanan testlerdir. En yaygın olarak kullanılan parametre, normal olduğunu varsaydığımız bir popülasyondan alınan ortalama (*mean*) ve onunla ilişkili olan standart sapmadır (*standart deviation*). Parametrik olmayan testler ise (*non-parametric*) normallik varsayımının ihlal edildiği durumlarda kullanılır ve bu testlerde ortalama dikkate alınmaz. Parametrik olmayan testler, parametrik testler kadar güçlü değildir ve bu prosedürleri kullanarak istatistiksel anlam bulmak daha zordur (George & Mallery, 2020).

3.11.1. Frekans (Sıklık) Analizi

Frekans analizi, tek değişkenli sayısal verileri tanımlamanın en kolay yoludur. En basit örneği, bir araştırmaya katılan katılımcıların cinsiyetlerinin, kabaca sayısal ve yüzdesel dağılımlarının elde edilmesidir (Neuman, 2010b). Bu analiz yöntemi ile değişkenlerin yüzde ve frekanslarının ayrı ayrı tablolar halinde gösterilmesinin yanı sıra mod, medyan, ortalama ve standart sapma gibi değişkenlere ilişkin betimsel istatistikler de sağlanabilir (Ural & Kılıç, 2013). Frekans analizleri, tüm SPSS prosedürlerinin en basitlerinden ve en kullanışlılarından biri olarak nitelendirilebilir. Frekanslar komutu, belirli bir kategorideki örneklerin sayısının basitçe toplanmasıdır (George & Mallery, 2020). Bu analizin temel amacı, araştırmacının toplanan verileri anlamlandırmasına yardımcı olmaktır (Ho, 2017).

3.11.2. Faktör Analizi

Değişken sayısını azaltmak için kullanılan faktör analizi, gözlemlenen ya da ölçülen değişkenler arasından temel değişkenler ya da faktörler tanımlanmasını sağlar (Ural & Kılıç, 2013). Başka bir ifade ile faktör analizi, birbiriyle ilişkili değişkenler arasındaki ilişkiyi temsil etmek için kullanılabilecek az sayıda faktörü belirlemek amacıyla kullanılır. Bu analizi yapmak için dört temel adım gerekir: (1) Analizde kullanılacak tüm değişkenlerin bir korelasyon matrisinin hesaplanması, (2) faktörlerin seçilmesi, (3) daha anlaşılır bir faktör yapısı oluşturmak için faktörlerin döndürülmesi ve (4) sonuçların yorumlanması (George & Mallery, 2020).

3.11.3. İki Adımlı Küme (Two-Step Cluster) Analizi

Faktör analizi ile benzer yönleri bulunan küme analizi, vakaları gruplar halinde birleştirmek için kullanılır. Daha açık bir şekilde ifade edilirse küme analizi, öncelikle her bir öznenin veya vakanın, belirli bir değişkenler grubundaki skorlarını, özneleri veya vakaları gruplandırmak (kümelemek) için kriter olarak kullanmak niyetiyle tasarlanmıştır. Faktör analizinde ilişkili değişkenler bir araya getirilerek bir faktör ile temsil edilirken küme analizinde ise vakalar (*cases*) bir araya getirilip kümeler oluşturulur (George & Mallery, 2020). Bu analiz yöntemi ile katılımcılar veya diğer varlıklar, araştırmacı tarafından belirlenen özellikler referans alınarak sınıflandırılır. “Ortaya çıkan kümeler, yüksek iç (küme içi) homojenlik ve yüksek dış (kümeler arası) heterojenlik sergilemelidir (Hair vd., 2014).” İki adımlı küme analizi IBM SPSS Statistics programının 23. versiyonu ile kullanıma sunulmuştur. Testin ilk adımında, ön-kümeleme

yapılır ve analiz edilen öznitelik uzayındaki yoğun bölgelere dayalı olarak sıralı bir yaklaşım kullanılır. İkinci adımda ise bu ön kümeler, tek bir küme olana kadar adım adım istatistiksel olarak birleştirilir (Benassi vd., 2020).

3.11.4. Pearson ve Spearman Korelasyon Analizleri

Korelasyon, iki değişken arasındaki ilişkiyi tanımlar ve istatistikte en çok kullanılan yöntemlerden biridir (Geray, 2014). Diğer istatistiksel analizlerden farklı olarak korelasyon analizinde, değişkenlerin test öncesi bağımlı ve bağımsız olarak belirlenmesine, tasnif edilmesine gerek yoktur. Bu analiz, iki değişken arasındaki ilişkinin düzeyini ve yönünü belirlemek için kullanılır. Analiz, “r” harfi ile ifade edilen korelasyon katsayısını hesaplar ve bu değer -1 ve +1 arasında bir sayı ile ifade edilir. Pozitif korelasyon katsayısı iki değişken arasında pozitif yönlü bir ilişkiyi, negatif katsayı ise negatif yönlü bir ilişkiyi işaret eder (Ural & Kılıç, 2013). Başka bir şekilde ifade etmek gerekirse korelasyon analizi, iki değişken arasındaki ilişkinin (1) büyüklüğünü (gücünü) ve (2) yönünü (pozitif-negatif) ortaya koyar (Ho, 2017). İki değişken arasındaki basit ve doğrusal korelasyonu belirlemek için kullanılan korelasyon analizi, aynı zamanda Pearson r olarak da adlandırılır. Pearson testi, değişkenler normal dağıldığında uygulanır. Değişkenlerin normallik varsayımını karşılamadığı durumlarda ise Spearman korelasyon testi kullanılır. Korelasyon sayısının 1’e eşit olması mükemmel korelasyonu işaret eder. Bu durum, bir değişkenin diğer değişkenden tam olarak tahmin edilebilir olduğunu gösterir. Ancak bu tip korelasyonlar, sosyal bilimlerde bulunamazlar (George & Mallery, 2020).

3.11.5. Ki-Kare Analizi

Ki-Kare analizi, bir araştırma sonucunda elde edilen (gözlenen) frekanslar ile beklenen (teorik varsayımsal) frekanslar arasındaki farkın, anlamlı olup olmadığını test eder. Tek örneklem Ki-Kare testinde, tek bir gruba ait tek bir değişkenin gözlenen ve beklenen frekanslarının uyumu test edilirken iki farklı gruba ilişkin frekansların karşılaştırıldığı Ki-Kare bağımsızlık testinde ise iki değişken arasında anlamlı bir ilişki olup olmadığı ya da iki değişkenin anlamlı bir farklılık gösterip göstermediği test edilir (Ural & Kılıç, 2013). Bir değişken için beklenen değer, SPSS tarafından hesaplanır ve iki değişkenin birbirinden bağımsız olduğu varsayımına dayanır. Beklenen değer için verilebilecek en basit örnek, 70 erkek ve 30 kadından oluşan bir örneklemde yer alan 10

Asyalının beklenen cinsiyet dağılımının 7 erkek ve 3 kadın olmasıdır (George & Mallery, 2020).

3.11.6. Ortalama Karşılaştırma Analizleri

3.11.6.1. Tek Örneklem t-Testi

Tek örneklem t-Testi, belirli bir değişkene ilişkin olarak öngörülen ya da hesaplanan ortalama ile araştırmada ölçülen ortalama arasında, belirli güven düzeylerinde anlamlı farklılık olup olmadığını test etmek için kullanılır (Ural & Kılıç, 2013). Bu test yöntemi, bir dağılımın ortalamasının önceden ayarlanmış bazı değerlerden (*test values*) önemli ölçüde farklı olup olmadığını test etmek için tasarlanmıştır (George & Mallery, 2020).

3.11.6.2. Bağımsız Örneklem t-Testi

Bağımsız örneklem t-Testi ile örneklem ortalamalarının farklılık gösterip göstermediğine dair yeterli kanıt olup olmadığı tespit edilmeye çalışılır (George & Mallery, 2020). Tek örneklem t-Testi'nin iki farklı örneklem için uygulanan versiyonu olan bağımsız örneklem t-Testi (*independent samples t-Test*), iki farklı grubun bağımlı bir değişkene ait ortalamalarının karşılaştırıldığı ve iki grup arasında istatistiksel açıdan anlamlı ve önemli bir farklılık olup olmadığını test eden bir yöntemdir (Ural & Kılıç, 2013). “Erkekler ve kadınlar, standart bir başarı testinde performans açısından farklılık gösteriyor mu?” sorusu bu test ile cevaplanabilecek araştırma sorularına bir örnektir (Ho, 2017).

3.11.6.3. Mann-Whitney U Testi

Bağımsız iki örneklemin ortalamaları karşılaştırılırken en yaygın kullanılan testlerden biri olan Mann-Whitney U testi, bağımsız örneklem t-Testi'nin parametrik olmayan alternatifidir. Test ile bir değişkenin iki farklı grup arasında farklılaşıp farklılaşmadığı kontrol edilir (Ural & Kılıç, 2013). Mann-Whitney U testi, Wilcoxon sıra toplamı testinin, bağımsız iki örneği karşılaştırmaya yarayan versiyonu olarak da bilinir ve zaman zaman Mann-Whitney-Wilcoxon olarak da adlandırılır (Krzywinski & Altman, 2014). U testi, bir örneklemden aldığı puanların, başka bir bağımsız örneklemin puanlarından önemli ölçüde daha yüksek sıralanıp (*rank*) sıralanmadığını görmek için kullanılan parametrik olmayan bir testtir (Norris & Qureshi, 2012). Bu test, bağımsız örneklem t-testi ile yaklaşık olarak aynı sonucu verir (Cleophas & Zwinderman, 2016).

3.11.6.4. Tek Faktörlü Varyans Analizi (One-Way ANOVA)

Tek yönlü ya da faktörlü varyans analizi, en kolay t testleri ile karşılaştırılarak açıklanabilir (George & Mallery, 2020). Bağımsız örneklem t-Testi, iki grubun ortalamaları arasındaki farkı tespit etmekle sınırlıdır. İki ya da daha fazla bağımsız grubun ortalamaları arasındaki farklılığı tespit etmek için tek faktörlü varyans analizi (*One-Way ANOVA*) kullanılır. Bu test, F testi olarak da bilinmektedir (Ural & Kılıç, 2013). Testin adında yer alan tek yön ile teste ilişkin bir ön koşul ifade edilmektedir. Bu testteki bağımlı değişken, her zaman sürekli bir değişkenden, bağımsız değişken ise her zaman kategorik bir değişkenden oluşmalıdır (George & Mallery, 2020). Bağımsız örneklem t testinin bir uzantısı olan ANOVA, anlamlı bir sonuç vermesi, araştırmacıya birbirinden önemli ölçüde farklı en az iki grup ortalaması olduğu çıkarımını yapma şansı verir. Farklılığın hangi iki grup arasında gerçekleştiği ise Post Hoc testleri ile tespit edilir. En az anlamlı fark (LSD) testi, Tukey dürüst anlamlı fark (HSD) testi ve Scheffé testi popüler Post Hoc testleridir (Ho, 2017).

3.11.6.5. Kruskal -Wallis H Testi

Tek faktörlü varyans analizinin parametrik olmayan ve normal dağılmayan verilerde kullanılabilen alternatifi olan Kruskal-Wallis H testi, iki ya da daha fazla grubun bağımlı bir değişkene ilişkin ortalamalarının karşılaştırılması ve gruplar arasında anlamlı bir farklılık olup olmadığını test eder. Bu test, iki grup arasındaki farklılığı ölçmek için kullanıldığında Mann-Whitney U testi ile aynı sonuçları verir (Ural & Kılıç, 2013). Bu test, ikiden daha fazla bağımsız örneklem için sıralanmış ortalama puanların önemli ölçüde farklılık gösterip göstermediğini belirlemek için kullanılan parametrik olmayan bir testtir (Norris & Qureshi, 2012).

3.12.Bulgular

3.12.1. Örneklemeye İlişkin Demografik Bilgiler

Kayseri'nin altı farklı ilçesindeki on sekiz farklı mahallede, 18.08.2021 – 30.08.2021 tarihleri arasında gerçekleştirilen araştırmaya, toplamda 374 kişi katılmıştır. Katılımcıların yaklaşık yüzde 40'ı, daha öncesinde köy statüsünde olan mahallerde ikamet ederken kalanı, belde statüsündeki mahallelerde yaşamaktadır.

Araştırmayı sahada uygulayan yedi anketçinin, katılımcılara yönelttiği ilk soru “akıllı telefonunuz var mı?” olmuştur. Bu soruya evet yanıtını veren ve araştırmaya katılmayı kabul eden katılımcıların 77'si kadın ve 297'si erkektir. Bu dengesiz dağılımın

sebebi, araştırmanın uygulandığı mahallelerde akıllı telefon kullanan kadın sayısının az olması olarak değerlendirilebilir. TÜİK'in en güncel istatistiklerine göre; tüm nüfus genelinde cep telefonu kullanımı, kadınlar arasında erkeklere oranla yaklaşık olarak yüzde 4 daha azdır (TÜİK, 2021c). Genellenemeyecek ve gözlemsel bir bulgu olsa da anketçilerin örnekleme dahil edilen mahallelerde, akıllı telefon kullanan kadın kullanıcıya daha az rastlamış olmaları, bu farklılığın kırsal bölgelerde daha fazla olduğunun bir göstergesi olarak yorumlanabilir. Katılımcıların yüzde 52,7'si evli, yüzde 45,7'si ise bekarıdır.

Tablo 3.3: Katılımcıların Demografik Özellikleri

Demografik Özellikler	Kategori	Sayı	Oran (%)
İkamet Edilen Mahalle	Köy	152	40.6
	Belde	222	59.4
Cinsiyet	Kadın	77	20.6
	Erkek	297	79.4
Medeni Hal	Evli	197	52.7
	Bekar	171	45.7
	Dul	5	1.3
	Boşanmış	1	0.3
	Çiftçi	32	8.6
Meslek	Ev Hanımı	44	11.8
	Esnaf	56	15.0
	İşçi	74	19.8
	Öğrenci	73	19.5
	Memur	22	5.9
	İşsiz/İş Arayan	7	1.9
	Emekli	24	6.4
	Diğer	42	11.2
	İlkokul Mezunu	112	29.9
	Ortaokul Mezunu	80	21.4
Eğitim	Lise Mezunu	133	35.6
	Üniversite Mezunu	39	10.4
	Lisansüstü	10	2.7
Yaş	18-24	121	32.4
	25-34	59	15.8

Demografik Özellikler	Kategori	Sayı	Oran (%)
	35-44	76	20.3
	45-54	62	16.6
	55-64	34	9.1
	65-74	17	4.5
	75+	5	1.3
Dijital Yerli – Dijital Göçmen	Dijital Yerli	159	42.5
	Dijital Göçmen	215	57.5

Katılımcılardan, yaşları yerine doğum yılı bilgileri açık uçlu soru olarak talep edilmiş ve toplanan veriler SPSS programında “Compute Variable” komutu ile 2021’den çıkartılarak katılımcıların yaşı hesaplanmıştır. Daha sonra katılımcılar, hesaplanan yaşları ile hem yedi farklı yaş kategorisine hem de dijital göçmen (30+) ve dijital yerli (18-29) olarak iki farklı kategoriye dağıtılmıştır. Araştırmaya katılanların yüzde 42.5’i dijital yerli, yüzde 57.5’i ise dijital göçmen olarak sınıflandırılmıştır²³. Katılımcıların yaklaşık yüzde 32’si, 18-24, yüzde 20’si ise 35-44 yaş aralığındadır.

Katılımcıların yaklaşık yüzde 50’si, ilköğretim ve ortaokul mezunlarından oluşmaktadır. Örneklemdekilerin yüzde 35.6’sı lise ve yaklaşık yüzde 10’u ise üniversite mezunudur. Araştırmanın gerçekleştirildiği il olan Kayseri’nin eğitim istatistikleri, her ne kadar mahalle ve kırsal alan sınırlandırması olmaksızın tüm il nüfusuna ilişkin bir tablo sunsa da örneklemin eğitim düzeyi dağılımını değerlendirmek için önemli bir referanstır. TÜİK’in Ulusal Eğitim İstatistikleri Veri Tabanı, 2020 verilerine göre, Kayseri’deki 15 yaş ve üzerindeki nüfusun yaklaşık yüzde 49’u ilköğretim, ilköğretim veya ortaokul mezunudur (TÜİK, 2020). Bu oran, örnekleme ise yaklaşık yüzde 50’dir.

Örneklem ile ilgili değinilmesi gereken bir diğer bilgi de katılımcıların meslekleridir. Örneklem içerisindeki en yaygın meslekler işçilik ve öğrenciliktir.

²³ Dijital teknolojiler ile büyüyen kuşak ile daha önceki kuşakları nitelendirmek için kullanılan dijital yerli ve dijital göçmen (*digital native and digital immigrant*) kavramları, ilk olarak Marc Prensky (2001a, 2001b) tarafından kullanılır. Prensky, 2001 yılına ait makalesinde, o dönemin yeni öğrencilerini nitelendirmek için bu kavramsallaştırmayı önerir. Kalaman (2016, s. 131), doktora tez çalışmasında, internetin 1993’te kullanılmaya başladığını hatırlatarak Türkiye’deki dijital yerlilerin yaklaşık olarak 23 yaşında olduklarını belirtir. İki çalışma arasındaki yıl farkı dikkate alınarak bu çalışmada, 18-29 yaş arasındaki katılımcılar dijital yerli, 30 ve üzeri yaşında olanlar ise dijital göçmen olarak kategorize edilmiştir.

Katılımcıların yüzde 15'i esnaflardan oluşurken sadece yüzde 8,6'sı çiftçidir. Mesleğini diğer olarak belirten katılımcıların sekizi inşaat sektöründe çalıştıklarını belirtmiş, dördü veteriner olduğunu, üçü şoförlük yaptığını ve diğer üçü de terzilik yaptığını ifade etmiştir.

3.12.2. Cihaz, Teknoloji ve Uygulama Kullanımlarına İlişkin Bulgular

Araştırmada, katılımcılardan Facebook, Twitter, Instagram, Snapchat, Tiktok, LinkedIn ve YouTube gibi sosyal medya uygulamalarını; BİP ve Telegram gibi anlık mesajlaşma programlarını; E-Devlet, MHRS (Merkezi Hekim Randevu Sistemi), HES (Hayat Eve Sığar) ve E-Nabız gibi kamu hizmeti uygulamalarını ve internet, cep telefonu, bilgisayar, tablet ve televizyon gibi teknolojileri kullanma sıklıklarını bir (hiç kullanmam) ve beş (her zaman kullanırım) arasında bir değerle belirtmeleri istenmiştir. Bu soruya paralel olarak, katılımcılardan aynı cihaz, teknoloji ve uygulamaları kullanma sıklıklarının, 2020 Covid-19 salgını öncesine göre değişip değişmediği de sorulmuştur.

Elde edilen bulgulara göre, kırsal kesimde en çok kullanılan sosyal medya uygulamaları; Instagram ($\bar{X}=2.9037$), Facebook ($\bar{X}=2.7166$) ve YouTube'dur ($\bar{X}=2.5936$). Profesyonel sosyal iş ağı ve sosyal paylaşım platformu olan LinkedIn ve bir diğer sosyal medya uygulaması olan SnapChat'in, örneklem içerisindeki kullanımı oldukça düşüktür. Literatürdeki diğer çalışmalara bakıldığında, bu iki uygulamanın kullanımının, sadece kırsal kesimde değil tüm nüfus için düşük olduğu söylenebilir. Aynı şekilde, Instagram kullanımı, şehir merkezlerinde yapılan araştırmalarda da en sık kullanılan sosyal medya araçlarından biridir (Livberber Göçmen, 2018). Üniversite öğrencileri üzerinde yapılan bir diğer araştırmada da öğrenciler arasında en sık kullanılan sosyal medya araçları; Instagram ($\bar{X}=3.92$), YouTube ($\bar{X}=3.89$) ve Twitter ($\bar{X}=2.53$) olarak belirlenmiştir (Balcı vd., 2019, s. 965). Kent merkezlerinde, 2018 yılında yapılan araştırmada; Facebook, WhatsApp ve Instagram'dan sonra en sık kullanılan ($\bar{X}=3.41$) sosyal medya aracıdır ve bu araştırmadakine benzer bir tablo oluşturur; ancak üniversite öğrencilerinin Facebook kullanım sıklıkları ($\bar{X}=1.80$) ile karşılaştırıldığında, kırsal bölgede yaşayan bireylerin Facebook kullanımları ($\bar{X}=2.7166$) daha fazladır (Livberber Göçmen, 2018, s. 133; Balcı vd., 2019, s. 965). Devlet uygulamaları incelendiğinde ise en yaygın kullanılan kamu hizmeti uygulamasının E-Devlet olduğu görülmektedir.

Tablo 3.4: Uygulama, Cihaz ve Teknoloji Kullanım Sıklıkları

Uygulama, Cihaz ve Teknolojiler	N	Ortalama ($\bar{X}$)	Standart Sapma	Çarpıklık	Basıklık
Facebook	374	2.7166	1.54638	.237	-1.415
Twitter	374	1.5775	1.20683	1.942	2.335
Instagram	374	2.9037	1.73787	.050	-1.734
TikTok	374	2.0321	1.54435	1.070	-.541
YouTube	374	2.5936	1.57581	.331	-1.439
SnapChat	374	1.3235	.94323	2.994	7.949
LinkedIn	374	1.0856	.53123	6.558	43.040
BİP	374	1.2326	.72260	3.560	13.034
Telegram (ve diğer anlık mesajlaşma uygulamaları) ²⁴	374	2.3128	1.69244	.689	-1.310
E-Devlet	374	2.2995	1.24101	.516	-.652
Hayat Evet Sığar	374	2.0374	1.25285	.817	-.490
MHRS	374	1.6578	1.09372	1.477	1.182
E-Nabız	374	1.6872	1.08413	1.371	.866
İnternet	374	4.0080	1.34321	-1.209	.189
Cep Telefonu	374	4.4198	.97019	-1.844	3.038
Bilgisayar	374	1.7968	1.35670	1.448	.596
Tablet	374	1.3342	.94233	2.979	7.928
Televizyon	374	3.0963	1.45213	-.121	-1.307

Araştırmaya katılanların neredeyse yüzde 90'ı (334), bir anlık mesajlaşma (*instant messaging*) uygulaması, yaklaşık yüzde 79'u da (295) bir sosyal medya uygulaması kullanmaktadır. Katılımcıların kullanım sıklıklarına ilişkin verilere göre; Telegram ve diğer anlık mesajlaşma uygulamaları Instagram, Facebook ve YouTube'dan sonra en yaygın kullanılan uygulamalardır. Tüm dünya genelinde en yaygın kullanılan anlık mesajlaşma uygulaması olan WhatsApp'ın, 2021 yılının başında duyurduğu kullanıcı sözleşmesi değişikliği nedeni ile kullanıcı sayılarında bir düşüş gözlemlenmiş ve Telegram ile birlikte, yerli anlık mesajlaşma uygulaması olan BİP'in kullanıcı sayıları

²⁴ Katılımcıların, WhatsApp kullanım sıklıklarını da bu soruda ifade ettikleri düşünülmektedir. Bu sebeple WhatsApp ve diğer anlık mesajlaşma uygulamalarının karşılaştırmak bu çalışma için olası değildir.

artmıştır (Çavuş, 2021; Ulukan, 2021). Bu artışa rağmen, Kayseri kırsalından alınan örnekleme, BİP kullanımı oldukça düşüktür ($\bar{X}=1.2326$).

Katılımcıların en sık kullandıkları cihaz, cep telefonu ($\bar{X}=4.4198$), en az kullandıkları cihazlar ise tablet ($\bar{X}=1.3342$) ve bilgisayardır ($\bar{X}=1.7968$). Televizyon ve internet kullanımları incelendiğinde ise katılımcıların televizyona kıyasla interneti daha sık kullandıkları görülmektedir. Bu veri, kullanım tercihlerinin geleneksel medyadan yeni medyaya yönelmesinin, kırsal bölgeler için de geçerli olduğunu gösteriyor olabilir.

Uygulama, cihaz ve teknoloji kullanımının cinsiyete ve dijital yerli-göçmen ayrımına göre analiz edildiğinde, kategoriler arası istatistiksel olarak anlamlı farklılıklar gözlemlenmektedir. Tabachnick ve ekip arkadaşları (2019), çarpıklık ve basıklık değerleri ± 1.5 arasında olan değişkenlere parametrik testlerin uygulanabilir olduğunu; George ve Mallery (2020, s. 114) ise, çoğu durumda $\pm 2,0$ arasındaki bir değer de kabul edilebilir olduğunu ifade ederler. Bu sebeple aşağıdaki tabloda, çarpıklık ve basıklık değerleri ± 2 arasında olan değişkenler için Bağımsız Örneklem t Testi kullanılmış ve kategoriler arasındaki farklılık analiz edilmiştir.

Tablo 3.5: Cinsiyete Göre Uygulama ve Teknoloji Kullanım Farklılığı

Uygulama ve Teknolojiler	Cinsiyet	N	Ortalama ($\bar{X}$)	Standart Sapma	t Değeri	Sig.
Facebook	Kadın	77	1.7922	1.21761	-7.061	<.001
	Erkek	297	2.9562	1.53389		
Twitter	Kadın	77	1.3766	1.13600	Z:-2.491	.013
	Erkek	297	1.6296	1.22096		
Instagram	Kadın	77	2.7532	1.71798	-.852	.395
	Erkek	297	2.9428	1.74374		
TikTok	Kadın	77	1.5844	1.16247	-3.477	<.001
	Erkek	297	2.1481	1.61023		
YouTube	Kadın	77	2.3117	1.51536	-1.767	.078
	Erkek	297	2.6667	1.58541		
Telegram (ve diğer anlık mesajlaşma uygulamaları)	Kadın	77	2.6364	1.79846	1.800	.075
	Erkek	297	2.2290	1.65671		
E-Devlet	Kadın	77	1.9351	1.20675	-2.920	.004
	Erkek	297	2.3939	1.23424		
Hayat Evet Sığar	Kadın	77	1.9610	1.20789	-.600	.549

Uygulama ve Teknolojiler	Cinsiyet	N	Ortalama ($\bar{X}$)	Standart Sapma	t Değeri	Sig.
MHRS	Erkek	297	2.0572	1.26548	1.347	.181
	Kadın	77	1.8182	1.20008		
E-Nabız	Erkek	297	1.6162	1.06264	.482	.630
	Kadın	77	1.7403	1.06873		
İnternet	Erkek	297	1.6734	1.08945	-2.261	.024
	Kadın	77	3.7013	1.36753		
Cep Telefonu	Erkek	297	4.0875	1.32762	Z:-1.868	.062
	Kadın	77	4.2857	.99812		
Bilgisayar	Erkek	297	4.4545	.96148	-.598	.550
	Kadın	77	1.7143	1.19050		
Televizyon	Erkek	297	1.8182	1.39761	-1.270	.205
	Kadın	77	2.9091	1.33950		
	Erkek	297	3.1448	1.47819		

Bağımsız örneklemeler için uygulanan testlere göre, cinsiyetler arasındaki Facebook ($t=-7.061$, $p<.001$), TikTok ($t=-3.477$, $p<.001$) ve E-Devlet ($t=-2.920$, $p=.004$) kullanım sıklığı farkı, istatistiksel olarak anlamlıdır. Facebook kullanımları arasındaki bu farklılık, şehir merkezlerinde yapılan araştırmalarda ($t=-9.33$, $p=.000$) ve üniversite öğrencileri üzerinde yapılan çalışmalarda da gözlemlenmiştir (Livberber Göçmen, 2018; Balcı vd., 2019). Bahsi geçen üniversite öğrencileri üzerindeki araştırmada Instagram kullanımı, cinsiyetler arasında anlamlı farklılık göstermekte ve kadınlar tarafından daha çok kullanılmaktadır. Bu farklılığın, iki çalışmanın örneklemelerinin sosyo-ekonomik olarak oldukça farklı olmasından kaynaklandığı söylenebilir. Twitter ve cep telefonu kullanım sıklığına ilişkin karşılaştırma, veriler normallik varsayımını sağlamadığı için Mann-Whitney U testi ile yapılmıştır ve aradaki farkın Twitter için anlamlı ($Z=-2.491$, $p=.016$), cep telefonu için ise istatistiksel olarak anlamlı olmadığı sonucuna ($Z=-1.868$, $p=.062$) ulaşılmıştır. İnternet kullanımlarında ise kadın ve erkek katılımcılar arasında bir farklılık olduğu görülmektedir ($t=-2.261$, $p=.024$). Bu bilgiler ışığında H13 hipotezi kabul edilmiştir.

Tablo 3.6: Dijital Yerli ve Dijital Göçmen Kategorilerine Göre Uygulama ve Teknoloji Kullanım Farklılığı

Uygulama ve Teknolojiler	Kategori	N	Ortalama ($\bar{X}$)	Standart Sapma	t Değeri	Sig.
Facebook	D. Yerli	159	2.5786	1.50267	-1.486	.138
	D. Göçmen	215	2.8186	1.57362		
Twitter	D. Yerli	159	1.8679	1.42364	Z:-3.876	<.001
	D. Göçmen	215	1.3628	.96602		
Instagram	D. Yerli	159	3.9434	1.44628	11.684	<.001
	D. Göçmen	215	2.1349	1.52409		
TikTok	D. Yerli	159	2.5975	1.72149	6.114	<.001
	D. Göçmen	215	1.6140	1.24735		
YouTube	D. Yerli	159	3.2453	1.52081	7.351	<.001
	D. Göçmen	215	2.1116	1.43930		
Telegram (ve diğer anlık mesajlaşma uygulamaları)	D. Yerli	159	2.8616	1.80883	5.444	<.001
	D. Göçmen	215	1.9070	1.47904		
E-Devlet	D. Yerli	159	2.3082	1.26766	.117	.907
	D. Göçmen	215	2.2930	1.22387		
Hayat Evet Sığar	D. Yerli	159	2.1195	1.25972	1.090	.277
	D. Göçmen	215	1.9767	1.24721		
MHRS	D. Yerli	159	1.7044	1.15591	.709	.479
	D. Göçmen	215	1.6233	1.04677		
E-Nabız	D. Yerli	159	1.8302	1.15401	2.165	.031
	D. Göçmen	215	1.5814	1.01927		
İnternet	D. Yerli	159	4.4591	.97916	6.176	<.001
	D. Göçmen	215	3.6744	1.47441		
Cep Telefonu	D. Yerli	159	4.6415	.78983	Z:-4.078	<.001
	D. Göçmen	215	4.2558	1.05664		
Bilgisayar	D. Yerli	159	2.0063	1.42090	2.550	.011
	D. Göçmen	215	1.6419	1.28874		
Televizyon	D. Yerli	159	2.5912	1.40620	-6.055	<.001
	D. Göçmen	215	3.4698	1.37323		

Kullanım sıklıkları dijital yerli ve dijital göçmen kategorileri arasında cinsiyete oranla daha fazla farklılık göstermektedir. Yapılan analizlere göre; dijital yerliler Twitter ($Z=-3.876$, $p<.001$), Instagram ($t=11.684$, $p<.001$), TikTok ($t=6.114$, $p<.001$), YouTube ($t=7.351$, $p<.001$) ile Telegram ve diğer anlık mesajlaşma uygulamalarını ($t=5.444$, $p<.001$) dijital göçmenlere oranla daha fazla kullanmaktadır. Z, t ve p değerlerine bakıldığında, bu farklılıkların istatistiksel olarak anlamlı olduğu görülmektedir. Çoğu kamu hizmeti uygulamasının kullanım sıklıkları arasında, anlamlı bir farklılık yoktur. Sadece E-Nabız adlı uygulamanın kullanım sıklığı, kategoriler arasında farklılık göstermektedir ($t=2.165$, $p=.031$).

Teknoloji kullanımları incelendiğinde, dijital yerlilerin interneti ($t=6.176$, $p<.001$) ve bilgisayarı ($t=2.550$, $p=.011$) dijital göçmenlere kıyasla daha fazla kullandıkları söylenebilir. Bu farklılık, yaşlıların gençlere oranla, sınırlı bilgisayar maruziyeti ile açıklanabilir. Ayrıca dijital göçmenlerin bilgisayar bilgisi eksikliği, Web 2.0 teknolojileri gibi yeni bilgisayar kavramlarını görselleştirmekte ve kavramakta zorlanmaları ve bilgisayar deneyimi eksiklikleri nedeniyle, mahremiyet ve güven sorunları gibi olumsuz teknoloji algıları taşımaları da (Arfaa & Wang, 2016, s. 174) bu farklılığın temelini oluşturduğu söylenebilir. Dijital göçmenlerin taşıdığı söylenebilecek bu algı, geleneksel medya aracı olan televizyonu ($t=-6.055$, $p<.001$) dijital yerlilere göre daha fazla kullanmalarını da açıklayabilir. Cep telefonu kullanımları arasındaki farkı test etmek için kullanılan Mann-Whitney U testine göre, dijital yerliler dijital göçmenlere göre daha sık ($Z=-4.078$, $p<.001$) cep telefonu kullanmaktadır. Cep telefonu ve internet, dijital göçmenlerin en sık kullandığı EİT'lerdir. Literatürde, bu cihazların dijital göçmenler arasındaki yaygın kullanımına ilişkin bulgular mevcuttur (Castro Rojas vd., 2016, s. 204). Literatürdeki çalışmalar ve bu araştırmadaki bulgulara dayanarak H14 hipotezi kabul edilmiştir.

2020 yılının başından itibaren tüm dünyayı etkisi altına alan ve pek çok ülkede sokağa çıkma kısıtlamaları, hatta tam kapanmaların uygulanması ile devam eden Covid-19 salgını, bireylerin medya tüketimlerini de etkilemiştir. Bu etkiyi ölçmek için katılımcılardan, yukarıda incelenen sosyal medya uygulaması, cihaz ve teknolojileri kullanma sıklıklarının salgın öncesine göre değişip değişmediğini, “artık daha az kullanıyorum”, “hayır, bir değişiklik olmadı” ve “evet, eskisine göre daha fazla

kullanıyorum” seçeneklerinden biri ile ifade etmeleri istenmiştir. Salgının, kullanım sıklıkları üzerindeki etkisini belirginleştirmek için; uygulama, cihaz ve teknoloji kullanım sıklıklarına “hiç kullanmam” yanıtını veren katılımcıların, ilgili madde için pandemi sürecindeki değişim sorusuna verdikleri yanıt, aşağıdaki frekans analizlerinin dışında bırakılmıştır. Çünkü bir cihaz için, “hiç kullanmam” yanıtını veren katılımcıların büyük bir kısmı, “hayır, bir değişiklik olmadı” seçeneğini tercih etmiştir.

Tablo 3.7: Cihaz, Uygulama ve Teknoloji Kullanımının Pandemi Sürecindeki Değişimi

Uygulama, Cihaz ve Teknolojiler	Daha Sık Kullanım		Değişiklik Yok		Daha Az Kullanım	
	N	Oran (%)	N	Oran (%)	N	Oran (%)
Facebook	99	41.1	135	56.0	7	2.9
Twitter	38	45.8	44	53.0	1	1.2
Instagram	113	50.4	103	46.0	8	3.6
TikTok	67	50.8	60	45.5	5	3.8
YouTube	100	46.3	111	51.4	5	2.3
Telegram (ve diğer anlık mesajlaşma uygulamaları)	75	48.7	76	49.4	3	1.9
E-Devlet	53	23.1	172	75.1	4	1.7
Hayat Evet Sığar	73	41.7	101	57.7	1	.6
MHRS	33	28.9	81	71.1	-	-
E-Nabız	35	28.2	85	68.5	4	3.2
İnternet	193	58.0	137	41.1	3	.9
Cep Telefonu	197	54.3	161	44.4	5	1.4
Bilgisayar	48	42.1	64	56.1	2	1.8
Tablet	19	35.8	32	60.4	2	3.8
Televizyon	103	34.9	178	60.3	14	4.7

Tabloda listelenen uygulama, cihaz ve teknolojileri az da olsa kullandıklarını ifade eden kullanıcılar arasında internet, kullanımı, salgın sürecinde en fazla artan teknoloji olmuştur. Örneklemdeki internet kullanıcıların yüzde 58’i, artık daha fazla internet kullandıklarını belirtmişlerdir. Katılımcıların 197’si, cep telefonlarını pandemi sürecinde daha sık kullandıklarını, yaklaşık yarısı (178) ise televizyon kullanımlarında bir değişiklik olmadığını belirtmiştir. Bu sonuç, 65 yaş ve üzeri bireylerin, pandemi sürecindeki enformasyon arama pratiklerine yönelik araştırmada elde edilen bulgularla paralellik göstermektedir (Binark vd., 2020). Ancak Amerika’da yapılan araştırmada ise,

televizyon içeriği tüketimi tüm jenerasyonlarda bir düşüş içindedir. Buna rağmen, Türkiye’deki yaşlı nüfusun televizyon izleme davranışlarına benzer şekilde, 1947-1965 yıllarında doğanları kapsayan ve “boomers” kuşağı olarak nitelendirilen kategorideki bireylerin yüzde 29.6’sı, televizyon kullanma pratiklerini değiştirmemiştir (Lu, 2021). Amerika’da yapılan Dijital Medya Trendleri araştırmasında da hem “X” kuşağı olarak ifade edilen 1966-1982 doğumlular hem de “boomers” adı verilen kuşağın, sırasıyla; yüzde 29’u ve yüzde 39’u için en sevdikleri eğlence aktivitesi, evde televizyon programları ve filmleri izlemektir. Aynı şekilde, bu iki kuşak, habere erişim için de televizyonu tercih etmektedir (Deloitte Center for Technology, Media & Telecommunications, 2021).

RTÜK (2018) tarafından yapılan araştırmalarda, ortalama televizyon izleme süresinin 2006-2018 yılları arasında yaklaşık iki saat azaldığı ve 3 saat 34 dakika olduğu görülmektedir. TİAK’ın (2021) yayınladığı araştırmaya göre ise 2018 yılında Türkiye’deki ortalama televizyon izleme süresi 4 saat 18 dakikadır ve bu ortalama 2020 yılında 4 saat 33 dakikaya yükselmiştir. Televizyon izleme sürelerindeki bu yükseliş, salgın süreci ile açıklanmaktadır. TİAK’ın araştırmasını destekler şekilde, bu araştırmadaki katılımcıların yaklaşık yüzde 35’i de salgın sonrasında televizyonu daha fazla izlediğini ifade etmiştir.

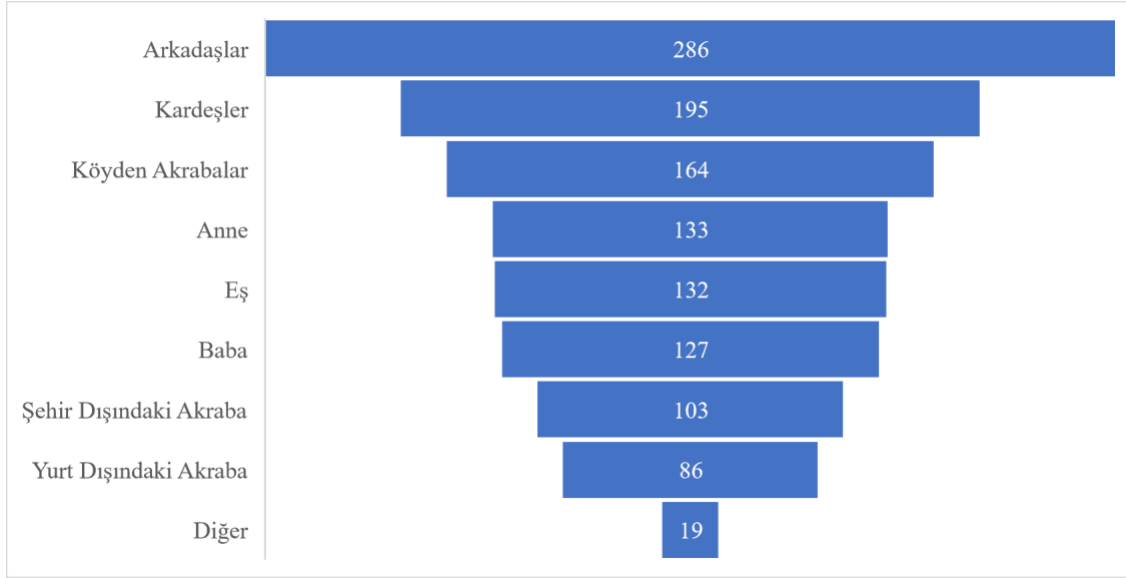
Sosyal medya uygulamalarının kullanım sıklığı da salgın sürecinde artış göstermiştir. Katılımcılar arasındaki YouTube kullanıcılarının yüzde 46’sı, Instagram kullanıcılarının yüzde 50.4’ü ve TikTok kullanıcılarının yaklaşık yüzde 51’i, bu uygulamaları artık daha sık kullanmaktadırlar. TikTok kullanımındaki bu artış, sadece bu araştırmanın örnekleme ile sınırlı değildir. Bu uygulama, evde kal çağrıları ile birlikte artan eğlenceye yönelik talebi, “ustalıkla karşılmasıyla” tüm dünya genelinde kullanım sıklığını artırmış ve en yüksek kullanıcı etkinliğine sahip sosyal uygulama olmuştur (Clapp, 2021).

3.12.3. Anlık Mesajlaşma Programları ile Kurulan İletişimlere İlişkin Bulgular

Neredeyse yüzde 90’ı (334), bir anlık mesajlaşma uygulaması kullanan örnekleme, bu uygulamalar ile kimlerle iletişim kurduğu sorusu da çoktan çok seçmeli şekilde yöneltilmiştir. Katılımcılara, “WhatsApp, BİP ya da diğer anlık mesajlaşma programları üzerinden kimlerle iletişim kurarsınız?” sorusu sorulmuş ve “annemle,

babamla, kardeşlerimle, eşimle, evlatlarımla, arkadaşlarımla, aynı köyde ikamet ettiğimiz akrabalarımla, şehir dışında ikamet eden akrabalarımla ve yurt dışında ikamet eden akrabalarımla” seçenekleri işaretlemeleri istenmiştir.

Şekil 3.4: Anlık Mesajlaşma Uygulamaları ile Kurulan İletişim



Yukarıdaki grafik, katılımcıların anlık mesajlaşma uygulamaları ile en çok arkadaşları ve en az da yurt dışındaki akrabaları ile iletişim kurduğunu göstermektedir. Katılımcıların yaklaşık yüzde 77’si arkadaşlarıyla, yaklaşık yüzde 52’si kardeşleriyle ve yaklaşık yüzde 44’ü de aynı mahallede (köy/belde) yaşadıkları akrabaları ile iletişim kurmaktadır.

Tablo 3.8: Kategorilere Göre Anlık Mesajlaşma Uygulamaları ile Kurulan İletişim

İletişim Kurulan Kişi	Cinsiyet		Dijital Yerli – Göçmen	
	Kadın	Erkek	Yerli	Göçmen
Anne	44.4%	38.5%	57.9%	24.7%
Baba	43.1%	36.6%	55.9%	23.1%
Kardeşler	76.4%	53.4%	52.0%	63.7%
Eş	41.7%	38.9%	17.1%	58.2%
Evlatlar	44.4%	30.9%	8.6%	54.9%
Arkadaşlar	75.0%	88.5%	90.8%	81.3%
Aynı Mahalledeki Akrabalar	45.8%	50.0%	41.4%	55.5%
Şehir Dışındaki Akrabalar	31.9%	30.5%	31.6%	30.2%
Yurt Dışındaki Akrabalar	25.0%	26.0%	25.0%	26.4%

İletişim Kurulan Kişi	Cinsiyet		Dijital Yerli – Göçmen	
	Kadın	Erkek	Yerli	Göçmen
Diğer	6.9%	5.3%	4.6%	6.6%

Katılımcılar arasında tüm kategorilerde, anlık mesajlaşma uygulamaları ile en fazla iletişim kurulan kişiler arkadaşlardır. Kadınların yüzde 76.4'ü kardeşleri, yaklaşık yüzde 46'sı ise aynı mahalledeki akrabaları ile iletişim kurmak için anlık mesajlaşma uygulamalarını kullanmaktadırlar. Dijital yerlilerin neredeyse yüzde 91'i, arkadaşları ile iletişim kurmak için bu uygulamaları kullandıklarını belirtmiştir.

3.12.4. EİT Maruziyeti Süresine ve İnternet Aboneliklerine İlişkin Bulgular

Araştırmada, katılımcıların EİT teknolojilerine maruziyet süreleri ve ne kadar yıldır bu teknolojileri kullanıyor olduklarının, araştırmadaki dijital okuryazarlık, dijital vatandaşlık ve mahremiyet yönelimleri gibi bağımlı değişkenler üzerinde etkisini tespit etmek için, internete ilk olarak hangi yıl bağlandıkları, ilk cep telefonu ve ilk akıllı telefonlarını ne zaman aldıkları açık uçlu olarak sorulmuştur. Soru, katılımcıların yakın geçmişlerine ilişkin bir tarihi hatırlamalarını ve yıl olarak belirtmelerini gerektirmektedir. Katılımcılardan bazıları, bu tarihleri ifade ederken, muhtemelen tam olarak hatırlayamadıkları için, gerçek dışı tarihler bildirmişlerdir. Bu tarihler, ortalamaları etkilememesi için analizden çıkarılmıştır. İnternet sorusu için, Türkiye'de internetin bir hizmet olarak kullanılmaya başladığı yıl olan 1996'dan daha erken; cep telefonu sorusu için Türkiye'de cep telefonunun ilk kullanılmaya başladığı yıl olan 1994'ten daha erken ve akıllı telefon sorusu için de, her ne kadar diğerleri gibi net bir tanımlaması ve tarihlendirmesi olmasa da ilk akıllı telefon, ya da akıllı telefon kategorisi için bir kilometre taşı olarak nitelendirilebilecek olan, ilk iPhone modelinin piyasaya çıktığı 2007 yılından daha erken cevaplar, ortalamalara dahil edilmemiştir.

Tablo 3.9: Cinsiyete Göre İlk EİT Kullanımı Tarihleri

Uygulama ve Teknolojiler	Cinsiyet	N	Ortalama ($\bar{X}$)	Standart Sapma	t Değeri	Sig.
İnternet	Kadın	76	2014.39	4.761	4.639	<.001
	Erkek	289	2011.18	5.518		
Cep Telefonu	Kadın	77	2010.36	6.044	4.202	<.001
	Erkek	288	2006.78	6.795		

Uygulama ve Teknolojiler	Cinsiyet	N	Ortalama ($\bar{X}$)	Standart Sapma	t Değeri	Sig.
Akıllı Telefon	Kadın	75	2015.15	3.332	2.071	.039
	Erkek	271	2014.21	3.502		

Cinsiyete göre internete ilk bağlanma tarihi, ilk cep telefonunu ve ilk akıllı telefonu satın alma tarihleri incelendiğinde; kadınların, her üç teknolojiyi de erkeklere oranla daha geç kullanmaya başladığı görülmektedir. EİT teknolojilerini kullanmaya başlama tarihleri, cinsiyetler arasında istatistiksel olarak anlamlı bir farklılık gösterir ($t=4.639$, $p<.001$; $t=4.202$, $p<.001$; $t=2.071$, $p=.039$). Farklılık her ne kadar istatistiksel olarak anlamlı görünse de örneklemdaki kadın-erkek oranı dengesizliği de dikkate alınmalıdır. Frekans analizi sonucu elde edilen ortalamalara göre; örneklemin internete ilk olarak 2011-2012 ($\bar{X}=2011.85$) yıllarında bağlandıkları, ilk cep telefonlarını 2007-2008 ($\bar{X}=2007.54$) ve ilk akıllı cep telefonlarını da 2013-2014 ($\bar{X}=2014.41$) yılları arasında satın aldıkları söylenebilir.

İnternete ilk bağlandıkları cihaza ilişkin soruya, katılımcıların yüzde 26.2'si evdeki bilgisayar, yüzde 16'sı internet kafe ve yaklaşık yüzde 53'ü de cep telefonu yanıtını vermiştir. Hatırlamıyorum veya diğer seçeneğini işaretleyen katılımcıların oranı ise yüzde 4.8'dir. Aşağıdaki tabloda, katılımcıların sahip oldukları internet aboneliklerine ilişkin bilgiler yer almaktadır.

Tablo 3.10: Katılımcıların İnternet Abonelikleri

Abonelik Türü	N	Oran (%)
Abonelik Yok	27	7.2
Sadece Ev İnterneti Aboneliği	18	4.8
Sadece Mobil İnternet Aboneliği	111	29.7
Hem Ev Hem Mobil İnternet Aboneliği	218	58.3
TOPLAM	374	100.0

Tablo incelendiğinde, katılımcıların en az yüzde 88'inin, cep telefonu ya da mobil cihazlardan internete bağlandığı söylenebilir. van Dijk'e (2017) atıfta bulunarak ve bu verileri dikkate alarak mobil internet teknolojisinin "ağ toplumunu, dünyadaki en uzak yerlere ve en derin deliklere doğru" genişlettiği söylenebilir. Türkiye'de yapılan başka bir araştırmada da katılımcıların yüzde 83.3'ü, cep telefonundan internete bağlandıklarını

belirtmiştir (Kalaman, 2016). Literatürde, sadece mobil internet abonesi olmanın dijital vatandaşlık için yeterli olmadığına değinilmektedir. Mossberger ve çalışma arkadaşlarının (2012) Şikago kentinde yaptıkları araştırmada, dezavantajlı kişiler için bir çözüm olarak mobil erişimin önemli olduğuna değinirler. Araştırmacılar, sadece bu erişim türüne sahip olmayı, ikinci sınıf bir erişim şekli olarak nitelendirirler ve cep telefonu kullanımındaki büyümenin çevrim içi katılımdaki eşitsizlikleri ortadan kaldırmadığının altını çizerler. Aynı araştırmada, evde geniş bant internet erişiminin, dijital vatandaşlık için kritik bir öneme sahip olmaya devam ettiği vurgulanır. Çalışmaya katılanların yüzde 60'tan fazlasının ev interneti kullanıyor olması, dijital vatandaşlık için önemli bir gelişmedir.

Araştırma elde edilen veriler, katılımcıların yüzde 60'tan fazlasının, 2011 ve sonrasında internet kullanmaya başladıklarını göstermektedir. Başka bir ifade ile Kayseri'nin kırsal mahallelerinde oturan ve akıllı telefon kullanan bireylerden alınan örneklemin çoğunluğu, sadece on yıldır, yaklaşık yüzde 29'u da son beş yıldır internet kullanmaktadır. Katılımcıların yarısından fazlasının ilk internet deneyiminin cep telefonu üzerinden olması ve yüzde 88'inin mobil internet abonesi oluşu da dikkate alındığında örneklemin internete penetrasyonunun, oldukça yeni bir gelişme olduğu söylenebilir. Bu görece yeni katılım, dijital okuryazarlık ve dijital becerilerle desteklenmediği takdirde, başta mahremiyet olmak üzere çeşitli riskli EİT kullanımlarına zemin hazırlayabilir. Aşağıda katılımcıların hem sosyal medya hem de anlık mesajlaşma uygulamalarındaki, kimi gizlilik ayarı tercihleri ve internette paylaştıkları kişisel bilgilerine ilişkin bulgular yer almaktadır.

3.12.5. Mahremiyet Tercihlerine ve Kişisel Bilgi Paylaşımlarına İlişkin Bulgular

Sosyal medya uygulamaları kullanıcılarına, kendileri hakkında paylaştıkları ve paylaşacakları içerikler ile ilgili olarak kişisel mahremiyetlerini korumaya yardımcı olacak kimi tercihler sunarlar. Bu ayarların yardımı ile kullanıcılar, paylaştıkları içeriklerin kimler tarafından görülebileceğini kontrol edebilirler. Bu gizlilik tercihleri için, sosyal ağ sitelerinin belirlediği varsayılan ayarlar mevcuttur. Örneğin Ekim 2021 verilerine göre; en fazla aktif kullanıcıya sahip olan Facebook (We Are Social, 2021), 2014 yılına kadar varsayılan gizlilik tercihi "herkese açık" (*public*) olarak belirlemiş ve bu ayarı değiştirmeyenlerin gönderileri, herkes tarafından görülebilir şekilde

paylaşmıştır. Daha sonra, mahremiyet tartışmalarının da etkisiyle Facebook, yeni üyeler için bu ayarı, varsayılan olarak “sadece arkadaşlar” (*friends only*) şeklinde belirlemiştir (Hamburger, 2014). Ancak bu varsayılan ayar, Instagram için halen herkese açık durumdadır.

Facebook, Instagram, TikTok ve YouTube sosyal platformları ve WhatsApp gibi anlık mesajlaşma yazılımlarını sıklıkla kullandığı görülen katılımcıların, bu servisleri kullanırken yukarıda bahsedilen gizlilik ayarlarını değiştirip değiştirmedikleri ve bu platformlardaki profilleri ve yaptıkları paylaşımların erişilebilirliği ile ilgili tercihlerini tespit etmek, hem katılımcıların bu ayarlar hakkındaki farkındalığını anlamak hem de mahremiyet yönelimleri ile ilişkisini incelemek açısından gereklidir. Bu sebeple, katılımcılara sosyal medya uygulamalarında (Facebook, Instagram, Twitter vb.), gizliliği korumak için sunulan varsayılan seçenekleri, değiştirip değiştirmedikleri sorulmuş ve sosyal medya profilleri ile ilgili olarak; (1) hesabım gizli, sadece onayladığım takipçiler paylaşımlarımı görebiliyor, (2) hesabım herkese açık, ama kişisel paylaşımlarımı sadece “Yakın Arkadaşlar” kategorisindekilere ya da belirlediğim arkadaş gruplarına açık olarak paylaşıyorum ve (3) hesabım herkese açık ve paylaştıklarımı herkes görebilir seçeneklerinden birini işaretlemeleri istenmiştir.

Tablo 3.11: Sosyal Medya Uygulamalarındaki Varsayılan Gizlilik Ayarlarını Değiştirme Oranları

Seçenek	N	Oran (%)
Hiç değiştirmeyenler	112	29.9
Birazını değiştirenler	106	28.3
Tamamını değiştirenler	156	41.7
TOPLAM	374	100.0

Kayseri’nin kırsal mahallelerinde yaşayan bireylerden alınan örneklemin yaklaşık yüzde 70’i, varsayılan gizlilik ayarlarını az da olsa değiştirerek kendi tercihlerini belirlemiştir. Türkiye’de yapılan bir diğer araştırmada ise katılımcıların yüzde 55.6’sı, Facebook gizlilik ayarlarını düzenlediklerini belirtmiştir (Kalaman, 2016). Yukarıda aktarıldığı gibi bu varsayılan ayarlar, platformdan platforma farklılık göstermektedir. Bu sebeple, kullanıcılara ayrıca kendi profillerine ilişkin olarak üç seçenekli bir soru

yöneltilmiş ve kendi durumlarına en uygun olan seçeneği işaretlemeleri istenmiştir. Aşağıdaki tablo, soldaki ifadelere seçen katılımcı sayılarını göstermektedir.

Tablo 3.12: Sosyal Medya Uygulamalarındaki Profil ve Gönderilerin Görünürlüğü

İfadeler	Cinsiyet		Dijital Yerli – Göçmen		TOPLAM
	Kadın	Erkek	Yerli	Göçmen	
Hesabım gizli, sadece onayladığım takipçiler paylaşımlarımı görebiliyor	34 (%63)	130 (%53.9)	101 (%68.2)	63 (%42.9)	164 (%55.6)
Hesabım herkese açık, ama kişisel paylaşımlarımı sadece “Yakın Arkadaşlar” kategorisindekilere ya da belirlediğim arkadaş gruplarına açık olarak paylaşıyorum	12 (%22.2)	20 (%8.3)	10 (%6.8)	22 (%15)	32 (%10.8)
Hesabım herkese açık ve paylaştıklarımı herkes görebilir.	8 (%14.8)	91 (%37.8)	37 (%25)	62 (%42.2)	99 (%33.6)
TOPLAM	54	241	148	147	295

Katılımcılar arasındaki sosyal medya kullanıcılarının, kendi hesaplarının gizlilik ayarlarına ilişkin beyanları incelendiğinde, yaklaşık yüzde 55’inin profillerinin, sadece kendileri tarafından onaylanan takipçi ya da arkadaşlar tarafından görülebilir olduğu ve yaklaşık yüzde 33’ünün ise herkese açık olduğu görülmektedir. Kadınlar ve dijital yerliler, profillerini erkekler ve dijital göçmenlere göre daha fazla gizli tutmaktadırlar. Kategoriler arasındaki farklılıklar için yapılan Ki-Kare analizlerine göre; hem cinsiyetler arasında (Pearson Chi-Square=15.450, df=2, $p<.001$) hem de dijital yerli ile dijital göçmenler arasında (Pearson Chi-Square=19.615, df=2, $p<.001$) sosyal medya hesaplarının görünürlük ayarları açısından istatistiksel olarak anlamlı bir farklılık vardır. Enformasyon ve iletişim teknolojileri profesyonelleri üzerinde yapılan bir diğer araştırmada da katılımcıların mahremiyet durumlarına ilişkin olarak cinsiyetler arasında anlamlı bir farklılık gözlemlenmiştir ($t=2.003$, $p=0.046$) (Külcü & Henkoğlu, 2014, s. 766). Literatürdeki Facebook kullanımı ile ilgili olarak yapılan diğer araştırmalarda, kadınların kendilerini koruyacak proaktif davranışlar gösterme ihtimallerinin, erkeklere göre daha fazla olacağı belirtilmiştir (Hoy & Milne, 2010; Saeri vd., 2014; Baruh vd., 2017). Elde edilen bulgular, genç kullanıcıların daha yetenekli sosyal ağ kullanıcıları

oldukları ve yaşlılara göre mahremiyet ayarlarını değiştirme ihtimallerinin, daha yüksek olduğuna ilişkin bulgular (Brandtzæg vd., 2010) ile paraleldir.

Katılımcılara, WhatsApp ve diğer anlık mesajlaşma uygulamasında bulunan “son görülme” ve “mavi tik” özellikleri ile ilgili olarak iki soru yöneltilmiş ve bu özellikleri kullanıp kullanmadıkları tespit edilmiştir. Uygulamadaki, son çevrim içi olma zamanının tüm kişi listenize görünebilir olduğu ve gönderilen mesajın okunup okunmadığını belirten mavi tik işaretçisi, kimi kullanıcılar tarafından kendi mahremiyetlerini korumak amacıyla devre dışı bırakılmaktadır. İki özellik de varsayılan olarak kullanılabilir durumdadır ve kullanıcılar değiştirmedeği sürece, son görülme tarih ve saatleri ile mesajları okuyup okumadıklarını belirten mavi tik, iki yönlü olarak kullanılmaktadır. Katılımcılara, bu özelliği kullanıp kullanmadıkları veya bu özellikten haberleri olup olmadığı sorulmuş ve aşağıdaki sonuçlar elde edilmiştir.

Tablo 3.13: Cinsiyet ve Yaşa Göre Son Görülme ve Mavi Tik Özelliklerinin Kullanımı

	Son Görülme Özelliği			Mavi Tik Özelliği		
	Açık	Kapalı	Bilmiyor	Açık	Kapalı	Bilmiyor
Kadın (N)	18	38	16	7	47	18
Kadın (%)	25.0	52.8	22.2	9.7	65.3	25.0
Erkek (N)	56	166	40	41	179	42
Erkek (%)	21.4	63.4	15.3	15.6	68.3	16.0
Dijital Yerli (N)	50	96	6	32	113	7
Dijital Yerli (%)	32.9	63.2	3.9	21.1	74.3	4.6
Dijital Göçmen (N)	24	108	50	16	113	53
Dijital Göçmen (%)	13.2	59.3	27.5	8.8	62.1	29.1
TOPLAM (%)	22.2	61.1	16.8	14.4	67.7	18.0

Katılımcıların yaklaşık yüzde 17’si, son görülme özelliğini ve yüzde 18’i de mavi tik özelliğini bilmediklerini ifade etmişlerdir. Varsayılan olarak bu özelliklerin açık konumda olduğu düşünüldüğünde, katılımcıların yüzde 39’unun, son görülme ve yüzde 32’sinin de mavi tik özelliğini kullandığı söylenebilir. İki özellik karşılaştırıldığında, mavi tik özelliğinin, son görülme özelliğine göre daha fazla devre dışı bırakıldığı görülmektedir. Verilere bakarak, katılımcıların yüzde 68’inin, kendilerine gelen mesajların okunup okunmadığının bilinmesini istemediği söylenebilir. Kategoriler arasındaki farklılıkları test etmek için yapılan Ki-Kare analizlerine göre; her iki özelliğin

kullanımı için de cinsiyetler arasında anlamlı bir farklılığa rastlanmamıştır (Pearson Chi-Square=3.000, df=2, p=.223 ve Pearson Chi-Square=3.987, df=2, p=.136). Dijital yerli ve dijital göçmenler karşılaştırıldığında ise hem son görülme özelliğinin (Pearson Chi-Square=42.057, df=2, p<.001) hem de mavi tik özelliğinin (Pearson Chi-Square=38.214, df=2, p<.001) kullanımları arasında anlamlı bir farklılık görülmektedir.

Katılımcıların kişisel mahremiyetleri ile ilişkilendirilebilecek bir diğer değişken de kullandıkları akıllı telefonlarda, bir şifre kullanıp kullanmadıkları ve bu şifrenin kimler tarafından bilindiğidir. Bu sebeple katılımcılara, akıllı telefonlarında bir şifre kullanıp kullanmadıklarına ilişkin olarak bir evet-hayır sorusu ve cevapları evet ise bu şifrenin kimler tarafından bilindiğine ilişkin çoktan çok seçmeli bir soru sorulmuştur.

Tablo 3.14: Cinsiyet ve Yaşa Göre Akıllı Telefonlarda Şifre Kullanımı

Kategoriler	Evet	Hayır	Şifreleri Kimseyle Paylaşmayanlar
Kadın (N)	50	27	18
Kadın (%)	64.9	35.1	36
Erkek (N)	211	86	157
Erkek (%)	71.0	29.0	74.4
Dijital Yerli (N)	142	17	109
Dijital Yerli (%)	89.3	10.7	76.8
Dijital Göçmen (N)	119	96	66
Dijital Göçmen (%)	55.3	44.7	55.5
TOPLAM (%)	69.8	30.2	58.7

Veriler incelendiğinde, katılımcıların yaklaşık yüzde 70'inin bir şifre kullandığı, ancak sadece yaklaşık yüzde 58'inin bu şifreyi kimseyle paylaşmadığı görülmektedir. Akıllı telefonlarının şifrelerini kendilerine saklayan kategoriler, yüzde 76.8 ile dijital yerliler ve yaklaşık yüzde 74.4 ile erkeklerdir. Dijital göçmenler ise dijital yerlilere oranla hem daha az şifre kullanmakta (%55.3) hem de şifre kullananların sadece yüzde 55.5'i bu şifreyi kimseyle paylaşmamaktadır. Bu sonuç, Petronio'nun İMY teorisindeki, yetişkinlikte genişleyen mahremiyet sınırlarının, bireyler yaşlandıkça daralacağı yönündeki öngörüsünü destekler niteliktedir. Petronio bu daralmada, yaşlıların giderek artan güvenlik ihtiyaçlarının etkili olduğunu belirtir ve yaşlıların finansal meselelerini yönetecek ve sağlık sorunları ile ilgilenecek birisine ya da birilerine ihtiyaç

duyabileceğini söyler (Petronio, 2002; Petronio & Kovach, 1997). Bu teoriye dayanarak dijital göçmenlerin, akıllı telefonlarında yaşayabilecekleri sorunlarla ilgilenebilecekleri birisi ya da birilerine ihtiyaç duyduğu ve bu sebeple hem daha az şifre kullandıkları hem de kullandıkları şifreyi daha fazla paylaşma eğiliminde oldukları söylenebilir. Akıllı telefon şifrelerinin, kimlerle paylaşıldığına ilişkin bulgular ise aşağıdadır.

Tablo 3.15: Cinsiyet ve Yaşa Göre Akıllı Telefonlarda Kullanılan Şifrenin Paylaşımı

Kategoriler	Anne-Baba	Çocuklar	Eş	Çevredeki Çoğu Kişi	Diğer
Kadın (N)	5	13	12	10	5
Kadın (%)	10.0%	26.0%	24.0%	20.0%	10.0%
Erkek (N)	8	19	30	12	9
Erkek (%)	3.8%	9.0%	14.2%	5.7%	4.3%
Dijital Yerli (N)	10	1	8	10	9
Dijital Yerli (%)	7.0%	0.7%	5.6%	7.0%	6.3%
Dijital Göçmen (N)	3	31	34	12	5
Dijital Göçmen (%)	2.5%	26.1%	28.6%	10.1%	4.2%
TOPLAM (%)	4.4%	10.7%	14.1%	7.4%	4.7%

Tablo incelendiğinde, akıllı telefon şifrelerinin çocuklar ve eşlerle paylaşıldığı görülmektedir. Bu paylaşım tercihi, dijital göçmen ve kadınlarda, dijital yerli ve erkeklere göre oldukça fazladır. Bu sonuç, Petronio'nun (2002) mahremiyet sınırlarının, bireyler yaşlandıkça daralacağı yönündeki savını desteklemektedir. Diğer tercihini işaretleyen katılımcılar genellikle, arkadaş, kardeş ve kuzenlerinin akıllı telefon şifrelerini bildiklerini beyan etmişlerdir.

Katılımcılara, kişisel bilgilerini sosyal medyada ve genel olarak internette paylaşıp paylaşmadıklarına ilişkin sorular yöneltilmiştir. Bu sorular, Stutzman (2006) tarafından belirlenen, yirmi altı maddelik kimlik öğeleri listesindeki on üç maddeden oluşmaktadır. Katılımcılardan, ad-soyad, e-posta adresi, yaşanılan şehir, telefon numarası, eğitim durumu, cinsiyet, memleket, doğum tarihi, fotoğraf, meslek, ilişki durumu, ilgi alanları ve siyasi görüş bilgilerini internette paylaşıp paylaşmadıklarını belirtmeleri istenmiş ve aşağıdaki bulgular elde edilmiştir.

Tablo 3.16: Kimlik Öğelerinin Paylaşılma Oranları

Kimlik Öğeleri	Evet		Hayır		TOPLAM
	N	%	N	%	N
Gerçek Ad	305	81.6	69	18.4	374
E-Posta Adresi	198	52.9	176	47.1	374
Yaşanılan Yer	217	58.0	157	42.0	374
Telefon Numarası	190	50.8	184	49.2	374
Eğitim	171	45.7	203	54.3	374
Cinsiyet	251	67.1	123	32.9	374
Memleket	224	59.9	150	40.1	374
Doğum Yılı	206	55.1	168	44.9	374
Fotoğraflar	249	66.6	125	33.4	374
Meslek	168	44.9	206	55.1	374
İlişki Durumu	137	36.6	237	63.4	374
İlgi Alanları	139	37.2	235	62.8	374
Siyasi Görüş	63	16.8	311	83.2	374

Kayseri'nin kırsal mahallelerinden alınan 374 kişilik örneklemin, sosyal medyada ve genel olarak internette en çok paylaştığı beş kimlik ögesi; gerçek ad (%81.6), cinsiyet (%67.1), fotoğraflar (%66.6), memleket (%59.9) ve yaşanılan yerdir (%58). En az paylaşılan kimlik öğeleri ise; siyasi görüş (%83.2), ilişki durumu (%63.4) ve ilgi alanlarıdır (%62.8). En çok paylaşılan kimlik öğeleri, literatürdeki araştırmalar ile kısmen paralellik göstermektedir (Stutzman, 2006; Kalaman, 2016; Livberber Göçmen, 2018). Üniversite öğrencileri üzerinde yapılan araştırmalarda, en az paylaşılan kimlik ögesi telefon numarası iken (Stutzman, 2006) bu araştırmada telefon numarası, katılımcıların yaklaşık yüzde 51'i tarafından paylaşılmaktadır. Bu sonuç, soruda ifade edilen “genel olarak internette” vurgusunun bir sonucu olabilir. Benzer şekilde, Türkiye’de yapılan diğer bir araştırmada da iletişim bilgileri paylaşımı, yaklaşık yüzde 24’tür (Livberber Göçmen, 2018, s. 136). Bir diğer araştırmada, siyasi görüşünü Facebook’ta hiç paylaşmayanların oranı yüzde 46.2, sadece arkadaşları ile paylaşanların oranı ise yaklaşık yüzde 30’dur (A. Zengin vd., 2015, ss. 129-130). Enformasyon ve iletişim teknolojileri profesyonellerinden oluşan bir örnekleme, katılımcıların yüzde 95’inden fazlasının; adres, telefon numarası, doğum tarihi, ilham kaynağı kişiler, spor, politik görüş ve dini

görüş gibi kişisel bilgileri herkese açık olarak paylaşmadığı ve katılımcılar için fotoğraflar, yaşanılan şehir ve iş/okul bilgisinin ise en az mahrem kabul edilen bilgiler olduğu sonucuna ulaşılmıştır (Külcü & Henkoğlu, 2014). Külcü ve Henkoğlu'nun adı geçen çalışmasından farklı olarak mevcut çalışmada, eğitim ve meslek bilgisinin paylaşım oranları yüzde 45 civarındadır.

Katılımcıların kimlik öğelerini paylaşma tercihlerinin, cinsiyete ve yaşa göre anlamlı bir farklılık gösterip göstermediğini test etmek için kullanılan Ki-Kare analizlerine göre; cinsiyetler arasında gerçek ad (Pearson Chi-Square=1.565, df=1, p=.211) ve telefon (Pearson Chi-Square=2.449, df=1, p=.118) bilgilerinin paylaşımında anlamlı bir farklılık görülmemiştir. Dijital göçmen ve dijital yerliler arasında ise yaşanılan yer (Pearson Chi-Square=1.483, df=1, p=.223), telefon (Pearson Chi-Square=2.646, df=1, p=.104), eğitim düzeyi (Pearson Chi-Square=3.039, df=1, p=.081), memleket (Pearson Chi-Square=3.503, df=1, p=.061), doğum yılı (Pearson Chi-Square=.089, df=1, p=.765), meslek (Pearson Chi-Square=.008, df=1, p=.929), ilgi alanları (Pearson Chi-Square=.396, df=1, p=.529) ve siyasi görüş (Pearson Chi-Square=1.118, df=1, p=.290) paylaşımları anlamlı bir farklılık göstermez.

Tablo 3.17: Kimlik Öğelerinin Paylaşılma Oranının Cinsiyete Göre Karşılaştırması

Kimlik Öğeleri	Cinsiyet	Evet		Hayır		Ki-Kare
		N	%	N	%	
E-Posta Adresi	Kadın	30	39.0%	47	61.0%	7.607, df=1, p=.006
	Erkek	168	56.6%	129	43.4%	
Yaşanılan Yer	Kadın	23	29.9%	54	70.1%	31.549, df=1, p<.001
	Erkek	194	65.3%	103	34.7%	
Eğitim	Kadın	19	24.7%	58	75.3%	17.307, df=1, p<.001
	Erkek	152	51.2%	145	48.8%	
Cinsiyet	Kadın	37	48.1%	40	51.9%	15.960, df=1, p<.001
	Erkek	214	72.1%	83	27.9%	
Memleket	Kadın	29	37.7%	48	62.3%	19.949, df=1, p<.001
	Erkek	195	65.7%	102	34.3%	
Doğum Yılı	Kadın	26	33.8%	51	66.2%	17.803, df=1, p<.001
	Erkek	180	60.6%	117	39.4%	
Fotoğraflar	Kadın	34	44.2%	43	55.8%	21.907, df=1, p<.001
	Erkek	215	72.4%	82	27.6%	

Kimlik Öğeleri	Cinsiyet	Evet		Hayır		Ki-Kare
		N	%	N	%	
Meslek	Kadın	18	23.4%	59	76.6%	18.188, df=1, p<.001
	Erkek	150	50.5%	147	49.5%	
İlişki Durumu	Kadın	13	16.9%	64	83.1%	16.290, df=1, p<.001
	Erkek	124	41.8%	173	58.2%	
İlgi Alanları	Kadın	13	16.9%	64	83.1%	17.081, df=1, p<.001
	Erkek	126	42.4%	171	57.6%	
Siyasi Görüş	Kadın	1	1.3%	76	98.7%	16.730, df=1, p<.001
	Erkek	62	20.9%	235	79.1%	

Yukarıdaki tabloda yer alan tüm kimlik öğeleri incelendiğinde; erkeklerin kadınlara oranla bu bilgileri daha çok paylaştıkları görülmektedir. Tabloda yer alan tüm kimlik öğelerinde, cinsiyetler arasındaki farklılık anlamlıdır. Literatürde, kadınların, sosyal ağ sitelerine gönderilen kişisel bilgilerin, farklı amaçlarla kullanılabileceğinin bilincinde olmanın önemli olduğuna inandıklarına ilişkin bulgular (Hoy & Milne, 2010), bu farklılığı açıklayabilir. Mevcut sonuçlara paralel olarak, literatürde erkeklerin kadınlara oranla politik ve dini görüşlerini daha fazla paylaştıkları görülmektedir (Nosko vd., 2010). Literatürde, doğum tarihi (1,262, df=1, p=,261) ve yaşanan yer (2,843, df=1, p=,092) paylaşımlarının, anlamlı farklılıklar göstermediği çalışmalar mevcuttur (Livberber Göçmen, 2018). Farklılıklar, mevcut çalışmadaki kadın-erkek katılımcı oranının dengesizliğinden kaynaklanıyor olabilir.

Tablo 3.18: Kimlik Öğelerinin Paylaşılma Oranının Yaşa Göre Karşılaştırması

Kimlik Öğeleri	Kategori	Evet		Hayır		Ki-Kare
		N	%	N	%	
Gerçek Ad	Dijital Yerli	140	88.1%	19	11.9%	7.766, df=1, p=.005
	Dijital Göçmen	165	76.7%	50	23.3%	
E-Posta Adresi	Dijital Yerli	106	66.7%	53	33.3%	20.915, df=1, p<.001
	Dijital Göçmen	92	42.8%	123	57.2%	
Cinsiyet	Dijital Yerli	122	76.7%	37	23.3%	11.590, df=1, p<.001
	Dijital Göçmen	129	60.0%	86	40.0%	
Fotoğraflar	Dijital Yerli	127	79.9%	32	20.1%	21.976, df=1, p<.001
	Dijital Göçmen	122	56.7%	93	43.3%	

Kimlik Öğeleri	Kategori	Evet		Hayır		Ki-Kare
		N	%	N	%	
İlişki Durumu	Dijital Yerli	49	30.8%	110	69.2%	4.027, df=1, p=.045
	Dijital Göçmen	88	40.9%	127	59.1%	

Dijital göçmen ve dijital yerlilerin, sosyal medyada ve genel olarak internette paylaştıkları kimlik öğelerine ilişkin Ki-Kare analizlerine göre; ilişki durumu dışındaki tüm öğeleri, dijital yerlilerin daha çok paylaştığı görülmektedir. İlişki durumunun paylaşılması, dijital göçmenler arasında daha yaygındır, ancak aradaki farklılık, diğer öğelerde olduğu kadar güçlü değildir (Pearson Chi-Square=4.027, df=1, p=.045).

İnternette alışveriş yapma yapmama tercihi de katılımcıların kendi mahremiyetlerine ilişkin olarak belirledikleri bir tutum olarak değerlendirilebilir. Bu sebeple katılımcılara, internette alışveriş yapma yapmadıkları da sorulmuştur. Katılımcıların yüzde 43.6'sı (163), internette alışveriş yaptığını, yüzde 56.4'ü de (211) yapmadığını belirtmiştir. Bu oran, 2021 verilerine göre Türkiye genelinde yüzde 44.3'tür (TÜİK, 2021c). Örneklem içerisinde, internette alışveriş yapma pratiği, cinsiyetler arasında anlamlı bir farklılık göstermemektedir (Pearson Chi-Square=.021, df=1, p=.885). Dijital yerliler ise dijital göçmenlere kıyasla, daha fazla internette alışveriş yapmaktadırlar ve aradaki farklılık, 0.01 düzeyinde anlamlıdır (Pearson Chi-Square=41.945, df=1, p<.001).

3.12.6. Mahremiyet Yönelimlerine İlişkin Bulgular

Araştırmada, Baruh ve Cemalcılar (2014) tarafından geliştirilen ve Baruh ve meslektaşları (2015) tarafından Türkçeye uyarlanan, çok boyutlu mahremiyet yönelimi ölçeği kullanılmıştır. On altı maddeden oluşan ölçek, dört farklı yönelim boyutu oluşturur. Bu boyutlar, (1) bir hak olarak mahremiyet (*privacy as a right*), (2) kendi enformasyonel mahremiyetine ilişkin kaygı (*concern about own informational privacy*), (3) başkalarının mahremiyetine ilişkin kaygı (*concern about privacy of others*) ve (4) diğer ihtimalli mahremiyet (*other-contingent privacy*) şeklinde sıralanır (Baruh & Cemalcılar, 2014, s. 169; Baruh vd., 2015; Livberber Göçmen, 2018, s. 120). Bu araştırmada, ölçeğin geliştirildiği ve kullanıldığı örneklemelere göre, sosyo-ekonomik olarak oldukça farklıdır. Bu sebeple, ölçek tarafından öngörülen faktör dağılımları, ölçekten dört madde çıkarılarak sağlanabilmektedir. “*Kişisel bilgilerimi istediğimden daha*

fazla kişi ile paylaşmış olmak beni kaygılandırıyor”, “kimlik bilgilerini paylaşmanın sonuçları hakkında endişeliyim (kaygılıyım)”, “başkalarının mahremiyetine saygı, sosyal ilişkilerde önemli bir öncelik olmalıdır” ve “çevremdeki insanların kendi hayatlarının mahremiyetine (gizliliğine) ne kadar özen gösterdikleri benim özelimin ne kadar korunabileceğini etkiler” maddeleri, farklı faktörlere yüklendiği için çıkarılmış ve aşağıdaki faktör analizi yapılmıştır.

Tablo 3.19: Çok Boyutlu Mahremiyet Yönelimleri Ölçeği Faktör Analizi

Maddeler	Faktörler			
	1	2	3	4
İnsanlar kişisel verilerin suistimal edilmesine karşı yasal olarak korunmalıdırlar.	-.892			
Mahremiyet (gizlilik) ile ilgili yasalar, kişilerin özel yaşamlarını koruyacak şekilde güçlendirilmelidir.	-.684			
Eğer bugün bir anayasa yazacak olsaydım büyük ihtimalle kişisel mahremiyeti temel hak olarak eklerdim.	-.433			
Etrafımdakilerin özel hayatım hakkında gereğinden fazla bilgiye sahip olduklarından endişeliyim (kaygılıyım).		.888		
Kişisel bilgilerimin detaylarını birisiyle paylaştığım zaman diğer insanlarla bunları paylaşacağı hakkında endişe duyarım.		.687		
Kendileri dikkat etmiyorsa bile, başkalarının mahremiyetine saygı göstermek benim için önemlidir.			.770	
Kendimin mahremiyeti kadar diğer insanların mahremiyetine de değer veriyorum.			.653	
Başkalarının özel hayatlarına karışmamak için her zaman elimden geleni yaparım.			.685	
Bir kişi kendi mahremiyetini korumaya özen göstermiyorsa bile, ben elimden geldiğince o kişinin özel yaşamına burun sokmamaya çalışırım.			.605	
Kendi özel yaşamları hakkındaki detayları herkesle paylaşan birine sırdaş olarak güvenemem.				.807
Özel hayatımın mahremiyetinin güvende olması için, arkadaşlarımla da kendi özel hayatları hakkında dikkatli olması gerekir.				.879
Kendi özel hayatını korumaya özen göstermeyen kişilerin benim özel hayatıma saygı göstereceğine güvenmiyorum.				.898

Çok boyutlu mahremiyet yönelimleri ölçeği ile toplanan ve dört faktör oluşturan veriler kullanılarak örneklem farklı alt boyutlara ayrılabilir. Baruh ve Cemalcılar (2014), mahremiyet alt boyutlarını belirlemek için, “Two-Step Cluster” analizi kullanmış ve üç farklı küme elde etmiştir. Ölçeğin kullanıldığı diğer bir çalışmada, aynı analiz ile beş

küme elde edilmiştir (Baruh vd., 2015). Livberber Göçmen (2018) ise kümeleme analizi yerine ölçekten alınan ortalama skoru; 0-49, 50-79 ve 80+ şeklinde kategorize ederek bu kümeleri oluşturmuştur. Bu çalışmadaki mahremiyet alt boyutlarını belirlemek için de orijinal ölçekte olduğu gibi iki adımlı küme (*Two-Step Cluster*) analizi tercih edilmiş ve örneklem, mahremiyet yönelimi boyutlarına göre üç farklı kümeye dağılmıştır. Analiz, üç kümeli modelin ortalama uyum ve ayrılma siluet ölçüsünü (*average silhouette measure of cohesion and separation*) 0.6 olarak vermiş ve iyi bir uyuma sahip olduğunu göstermiştir.

Tablo 3.20: Çok Boyutlu Mahremiyet Yönelimleri Ölçeği Alt Boyutları ve Ortalama Ölçek Puanları

Alt Boyutlar	Sayı	%	Ortalama	Standart Sapma
Mahremiyet Savunucuları	93	24.9	4.70	.23
Mahremiyet Bireycileri	233	62.3	3.98	,11
Mahremiyet İlımlıları	48	12.8	3.51	.66
TOPLAM	374	100	4.10	.47

Yapılan kümeleme analizi sonucu örneklem, tüm boyutlardan en yüksek puan alan, mahremiyet savunucuları; ortalama puana sahip ve en kalabalık grup olan mahremiyet bireycileri ve en küçük ve en az puanı alan mahremiyet ılımlıları olarak üçe ayrılmıştır. Diğer çalışmalardan farklı olarak, en düşük mahremiyet yönelimi puanına sahip grup, mahremiyet “umursamazları” değil “ılımlıları” olarak nitelendirilmiştir. Çünkü, bu grup mevcut örneklemdeki en düşük skora sahip olsa da mahremiyet ılımlılarının ortalaması ölçeğin kullanıldığı diğer çalışmalardaki ortalamalara kıyasla, halen oldukça yüksektir.

Tablo 3.21: Çok Boyutlu Mahremiyet Yönelimleri Ölçeği Z Skorları ile Alt Boyutların Karşılaştırılması

Boyutlar	Mahremiyet Savunucuları	Mahremiyet Bireycileri	Mahremiyet İlımlıları
Bir Hak Olarak Mahremiyet	1.14257	-.26525	-.92617
Kendi Mahremiyetine İlişkin Kaygı	.88888	.06106	-2.01861
Başkalarının Mahremiyetine İlişkin Kaygı	1.11079	-.28188	-.78388
Diğer İhtimalli Mahremiyet	1,10393	-.32155	-.57801

Tablo incelendiğinde, mahremiyet ılımlılarının, kendi mahremiyetlerine ilişkin kaygılarının, başkalarının mahremiyetlerine ilişkin kaygıdan düşük olduğu görülmektedir. Kendi mahremiyetine ilişkin kaygı boyutunun, tüm gruplarda en düşük boyutu oluşturması, bu boyuttaki iki maddenin, faktör analizi sırasında çıkarılmış olmasından kaynaklanmaktadır. Aşağıda ölçekten elden edilen veriler, farklı bağımsız değişkenlere göre ele alınmaktadır.

3.12.6.1. Cinsiyete Göre Mahremiyet Yönelimi Boyutları

Petronio'nun (2002) İMY teorisine göre; bireyler, mahremiyetlerini yönettikleri kuralları, kültürel beklentiler, cinsiyet, bağlam ve risk-fayda oranı gibi kriterlerden etkilenerek geliştirirler. Literatürdeki araştırmalar, mahremiyet endişesinin, kadınlarda erkeklere oranla daha yüksek olduğunu işaret etmektedir (Fogel & Nehmad, 2009; Hoy & Milne, 2010; Taddicken, 2014). Araştırmada kullanılan çok boyutlu mahremiyet yönelimleri ölçeği ile elde edilen bulgular, kadın ve erkek arasında farklı boyutlarda anlamlı farklılıkları işaret etmektedir.

Tablo 3.22: Mahremiyet Yönelimi Boyutlarının Cinsiyete Göre Karşılaştırması

Boyutlar	Cinsiyet	Ortalama Sıra	Mann-Whitney U	Z ve p
Bir Hak Olarak Mahremiyet	Kadın	159.40	9271.000	Z=-2.845, p=.004
	Erkek	194.78		
Kendi Mahremiyetine İlişkin Kaygı	Kadın	184.03	11167.000	Z=-.351, p=.726
	Erkek	188.40		
Başkalarının Mahremiyetine İlişkin Kaygı	Kadın	165.95	9775.500	Z=-2.170, p=.030
	Erkek	193.09		
Diğer İhtimalli Mahremiyet	Kadın	171.34	10190.500	Z=-1.665, p=.096
	Erkek	191.69		
Ölçek Ortalaması	Kadın	170.66	10138.000	Z=-1.575, p=.115
	Erkek	191.87		

Uygulanan Mann-Whitney U testi sonuçlarına göre, ölçek genelinde cinsiyetler arasında anlamlı bir farklılığa rastlanmazken (Z=-1.575, p=.115), bir hak olarak mahremiyet (Z=-2.845, p=.004) ve başkalarının mahremiyetine ilişkin kaygı (Z=-2.170, p=.030) boyutlarında, anlamlı bir farklılıktan söz edilebilir. Kendi mahremiyetine ilişkin

kaygı boyutunun ortalamalarına bakıldığında (kadın $\bar{X}$ =3.9156, erkek $\bar{X}$ =3.8872), kadınların daha fazla kaygı duydukları görülsede bu fark, literatürdeki araştırmalardan farklı olarak anlamlı değildir. Ancak mahremiyet yönelimleri alt boyutlarının, cinsiyetler arasındaki dağılımının, anlamlı olup olmadığı test etmek için yapılan analiz, cinsiyetler arasında istatistiksel açıdan anlamlı bir farklılık göstermektedir (Pearson Chi-Square=10.360, df=2, p=.006). Bu bilgiler ışığında, H9 hipotezi kısmen kabul edilmiştir.

3.12.6.2. Yaşa Göre Mahremiyet Yönelimi Boyutları

Literatürdeki araştırmalar, mahremiyet endişesinin, yaşa göre değişkenlik gösterdiğini ve yaşlı katılımcıların çevrim içi mahremiyet konusunda, daha endişeli olduklarını ortaya koymaktadır (Paine vd., 2007). 18-40, 41-65 ve 65+ olmak üzere, üç farklı yaş kategorisi üzerinde yapılan ve çok boyutlu mahremiyet yönelimleri ölçeğinin kullanıldığı bir araştırmada ise yaş gruplarının, çevrim içi mahremiyet okuryazarlığı, mahremiyet endişesi ve davranışları açısından farklılaştığını gösterir (Kezer vd., 2016).

Tablo 3.23: Mahremiyet Yönelimi Boyutlarının Dijital Göçmen - Dijital Yerli Değişkenine Göre Karşılaştırması

Boyutlar	Cinsiyet	Ortalama Sıra	Mann-Whitney U	Z ve p
Bir Hak Olarak Mahremiyet	D. Yerli	184.95	16687.500	Z=-.436, p=.663
	D. Göçmen	189.38		
Kendi Mahremiyetine İlişkin Kaygı	D. Yerli	179.33	15794.000	Z=-1.392, p=.164
	D. Göçmen	193.54		
Başkalarının Mahremiyetine İlişkin Kaygı	D. Yerli	179.62	15839.500	Z=-1.341, p=.180
	D. Göçmen	193.33		
Diğer İhtimali Mahremiyet	D. Yerli	181.75	16177.500	Z=-1.002, p=.316
	D. Göçmen	191.76		
Ölçek Ortalaması	D. Yerli	174.67	15052.000	Z=-2.027, p=.043
	D. Göçmen	196.99		

Mann-Whitney U analizlerine göre; hiçbir mahremiyet boyutunda anlamlı bir farklılık görülmemektedir. Ancak ölçek geneline bakıldığında, çok güçlü olmasa da dijital göçmen ve dijital yerliler arasında anlamlı bir farklılık (Z=-2.027, p=.043) görülmektedir. Faktör ortalamaları incelendiğinde, tüm faktörlerde, dijital göçmenlerin daha yüksek ortalamalara sahip oldukları görülmektedir. Ancak bu fark, anlamlı değildir.

Bu sonuç, Konya ve İzmir’de yapılan araştırmalardan farklıdır (Livberber Göçmen, 2018). Bu farklılığın, hem örneklemin literatürdeki araştırmalardaki örnekleme kıyasla farklı bir sosyo-demografik yapıya mensup olması hem de dijital yerli nüfusunun yaşlanması ile ilişkisi olabilir. Bu sebeple, yaş gruplarını karşılaştırmak için, Kruskal-Wallis Test uygulanmış ve yedi farklı yaş grubu kategorisi arasında anlamlı farklılıklar gözlemlenmiştir.

Tablo 3.24: Mahremiyet Yönelimi Boyutlarının Yaş Gruplarına Göre Karşılaştırması

Boyutlar	Kruskal-Wallis	df ve p
Bir Hak Olarak Mahremiyet	13.350	df=6, p=.038
Kendi Mahremiyetine İlişkin Kaygı	13.532	df=6, p=.035
Başkalarının Mahremiyetine İlişkin Kaygı	21.132	df=6, p=.002
Diğer İhtimalli Mahremiyet	14.629	df=6, p=.023
Ölçek Ortalaması	17.882	df=6, p=.007

Dijital yerli (18-29) – dijital göçmen (30+) ayrımı yerine örneklem, yedi farklı yaş kategorisine bölündüğünde, yapılan analizler her mahremiyet yönelimi boyutunda istatistiksel olarak anlamlı bir farklılığı işaret etmektedir. Bu sonuç, literatürdeki, yaşlıların gençlere göre daha fazla mahremiyet endişesi taşıdığı yönündeki bulgularla paralellik gösterir (Kezer vd., 2016; Aydın, 2018). Elde edilen bulgular, H10 hipotezini desteklemektedir.

3.12.6.3. Eğitim Durumuna Göre Mahremiyet Yönelimi Boyutları

Literatürdeki, eğitim seviyesindeki farklılıkların, mahremiyet endişesine ve mahremiyet yönelimlerine etkisine ilişkin farklı sonuçlar bulunmaktadır. AB’de yapılan bir araştırmada, eğitim düzeyi farklılıklarının mahremiyet erozyonuna ilişkin endişelerde büyük bir farklılık yaratmadığı tespit edilmiştir (Strauß, 2015). Mahremiyet yönelimlerinin araştırıldığı bir çalışmada ise, sadece diğer ihtimalli mahremiyet boyutu ile eğitim arasında anlamlı bir ilişki bulunmuştur ($F=3.524$, $p=.015$) (Livberber Göçmen, 2018). Kalaman (2016) ise, çalışmasının sonuçlarını değerlendirirken; üniversite, yüksek lisans ve doktora düzeyinde bireylerin, lise düzeyinde kişilere göre mahremiyetlerini daha

az ifşa ettiklerini ifade eder. Beş eğitim düzeyi ile yapılan Kruskal-Wallis testi sonuçlarına göre, ölçek ortalamasında olmasa da mahremiyet boyutlarında anlamlı farklılıklar gözlemlenmektedir.

Tablo 3.25: Mahremiyet Yönelimi Boyutlarının Eğitim Düzeyine Göre Karşılaştırması

Boyutlar	Eğitim Düzeyi	N	Ortalama Sıra	Kruskal-Wallis	df ve p
Bir Hak Olarak Mahremiyet	İlkokul	112	161.57	13.090	df=4, p=.011
	Ortaokul	80	197.16		
	Lise	133	193.59		
	Üniversite	39	213.05		
	Lisansüstü	10	220.10		
Kendi Mahremiyetine İlişkin Kaygı	İlkokul	112	186.04	.852	df=4, p=.931
	Ortaokul	80	185.73		
	Lise	133	185.41		
	Üniversite	39	200.05		
	Lisansüstü	10	196.95		
Başkalarının Mahremiyetine İlişkin Kaygı	İlkokul	112	170.05	9.917	df=4, p=.042
	Ortaokul	80	189.52		
	Lise	133	189.12		
	Üniversite	39	212.78		
	Lisansüstü	10	246.70		
Diğer İhtimalli Mahremiyet	İlkokul	112	168.33	12.091	df=4, p=.017
	Ortaokul	80	203.73		
	Lise	133	182.71		
	Üniversite	39	217.74		
	Lisansüstü	10	218.10		
Ölçek Ortalaması	İlkokul	112	173.12	5.914	df=4, p=.206
	Ortaokul	80	191.55		
	Lise	133	188.22		
	Üniversite	39	203.88		
	Lisansüstü	10	242.75		

Analiz sonuçlarına göre, bir hak olarak mahremiyet ve diğer ihtimalli mahremiyet boyutlarında, eğitim düzeyine göre anlamlı bir farklılık olduğu gözlemlenmektedir. Başkalarının mahremiyetine ilişkin kaygı boyutu için, düşük de olsa istatistiksel olarak

anlamli bir farklılık bulunduđu söylenebilir (9.917, df=4, p=.042). Kendi mahremiyetine ilişkin kaygı boyutu, eğitim düzeyleri arasında farklılık göstermemektedir. Başka bir ifade ile mahremiyete yönelik kaygılar ile eğitim düzeyi arasında bir ilişki olmadığı görölmektedir. Analiz, meslekler açısından tekrarlandığında ise, benzer şekilde kendi mahremiyetine ilişkin kaygı boyutu dışındaki tüm boyutlarda ve ölçek genelinde istatistiksel olarak anlamlı farklılıklar bulunmuştur (p<.001). Livberber Göçmen'in (2018) çalışmasında, eğitim düzeyi açısından sadece diğer ihtimalli mahremiyet boyutunda anlamlı bir farklılığa rastlanmış, (F=3.524, p=.015) meslek değişkeninde ise farklılık göstermeyen tek boyut, başkalarının mahremiyetine ilişkin kaygı olmuştur (F=1.691, p=.071). Verilere dayanarak, H11 hipotezi kısmen kabul edilmiştir.

3.12.6.4. EİT Maruziyet Sürelerine Göre Mahremiyet Yönelimi Boyutları

Paine ve mesai arkadaşları (2007, ss. 533-534), bireyler ne kadar çok çevrim içi deneyime sahip olursa olası gizlilik tehditleri hakkında, o kadar çok bilgi sahibi olacağını ve kendilerini korumak için nasıl harekete geçeceklerini, o kadar çok bileceklerini söyler. Bu önerme ile ilişkili olarak katılımcılara, internete ilk bağlandıkları yıl, ilk cep telefonlarını ve ilk akıllı telefonlarını aldıkları yıl sorulmuş ve bu değişkenlerin, mahremiyet boyutları üzerindeki etkilerini incelemek için Spearman korelasyon testi kullanılmıştır.

Tablo 3.26: Mahremiyet Yönelimi Boyutları ile EİT Maruziyet Süreleri Arasındaki İlişkiyi Gösteren Korelasyon Analizi

		1	2	3	4	Ortalama
İlk İnternet	Correlation Coefficient	-.180**	-.126*	-.132*	-.169**	-.156**
	Sig. (2-tailed)	<.001	.016	.011	.001	.003
	N	365	365	365	365	365
İlk Cep Telefonu	Correlation Coefficient	-.146**	-.187**	-.159**	-.155**	-.208**
	Sig. (2-tailed)	.005	<.001	.002	.003	<.001
	N	365	365	365	365	365
İlk Akıllı Telefon	Correlation Coefficient	-.166**	-.140**	-.203**	-.197**	-.171**
	Sig. (2-tailed)	.002	.009	<.001	<.001	.001
	N	346	346	346	346	346

** Correlation is significant at the 0.01 level (2-tailed). | * Correlation is significant at the 0.05 level (2-tailed).

Tablo incelendiğinde, EİT maruziyet süreleri ile tüm mahremiyet boyutları arasında anlamlı düzeyde ilişki olduğu görülmektedir. İki kaygı boyutunun, ilk internete bağlanma tarihi ile olan ilişkisi dışında tüm korelasyonlar, 0.01 anlamlılık düzeyine sahiptir. Literatürde, internet kullanım tecrübelerinin çevrim içi mahremiyet endişeleri üzerinde anlamlı bir etkisi olmadığına ilişkin bir araştırma mevcuttur (Alfred, 2014, s. 84). Ancak sözü edilen araştırmada, kullanıcıların internet kullanım tecrübeleri, tek bir soru ile ölçülmüş ve katılımcıların kendi deneyim seviyelerini, üç seçenek arasından seçim yaparak belirlemeleri sağlanmıştır. Mevcut çalışmada elde edilen sonuç hem farklı ölçüm şekli hem de farklı örneklem özellikleri ile açıklanabilir.

3.12.6.5. Gizlilik Ayarları Tercihlerine Göre Mahremiyet Yönelimi Boyutları

Katılımcılar, hem sosyal medya hesaplarında paylaştıkları bilgilerin erişilebilirliğini, hem anlık mesajlaşma uygulamalarındaki son görülme ve mavi tik özelliklerini, hem de akıllı telefonlarına koydukları şifre ile cihazlarının güvenliğini ve mahremiyetini sağlamaya çalışırlar. Katılımcıların bu tercihlerindeki değişikliklerin, mahremiyet yönelimi boyutları ile ilişkili olup olmadığını test etmek için, Kruskal-Wallis ve Mann-Whitney U testleri kullanılmış ve aşağıdaki sonuçlar elde edilmiştir.

Tablo 3.27: Mahremiyet Yönelimi Boyutlarının Sosyal Medya Profillerindeki Gizlilik Tercihlerine Göre Karşılaştırması

Boyutlar	Profile Erişim	N	Ortalama Sıra	Kruskal-Wallis	df ve p
Bir Hak Olarak Mahremiyet	Arkadaşlar	164	148.27	6.109	df=2, p=.047
	İzin Verilen Yakın Arkadaşlar	32	118.28		
	Herkes	99	157.16		
Kendi Mahremiyetine İlişkin Kaygı	Arkadaşlar	164	146.17	.228	df=2, p=.892
	İzin Verilen Yakın Arkadaşlar	32	148.42		
	Herkes	99	150.89		
Başkalarının Mahremiyetine İlişkin Kaygı	Arkadaşlar	164	144.36	7.965	df=2, p=.019
	İzin Verilen Yakın Arkadaşlar	32	120.17		
	Herkes	99	163.03		
Diğer İhtimalli Mahremiyet	Arkadaşlar	164	143.22	7.669	df=2, p=.022
	İzin Verilen Yakın Arkadaşlar	32	124.53		
	Herkes	99	163.50		
	Arkadaşlar	164	143.91	5.049	

Boyutlar	Profile Erişim	N	Ortalama Sıra	Kruskal-Wallis	df ve p
Ölçek Ortalaması	İzin Verilen Yakın Arkadaşlar	32	126.95		df=2, p=.080
	Herkes	99	161.58		

Katılımcıların sosyal medya profillerindeki bilgilere, kimlerin erişebildiğine dair yaptığı tercihler ile başkalarının mahremiyetine ilişkin kaygı ve diğer ihtimalli mahremiyet boyutlarında, istatistiksel olarak anlamlı bir farklılık söz konusudur. Bir hak olarak mahremiyet boyutu ile olan farklılık ise anlamlı olsa da düzeyi oldukça düşüktür ($p=.047$). Akıllı cep telefonlarında şifre kullanma tercihi ile sadece diğer ihtimalli mahremiyet boyutu arasında anlamlı bir farklılık gözlemlenmiştir (12944.000, $Z=-2.125$, $p=.034$). Anlık mesajlaşma programlarındaki son görülme ve mavi tik özelliklerinin kullanımı ile yapılan karşılaştırmalar, kendi mahremiyetine ilişkin kaygı boyutu dışındaki tüm boyutlarda, anlamlı bir şekilde farklılaşmaktadır.

Tablo 3.28: Mahremiyet Yönelimi Boyutlarının Anlık Mesajlaşma Uygulamalarındaki Son Görülme Özelliğinin Kullanımına Göre Karşılaştırması

Boyutlar	Kullanım Tercihi	N	Ortalama Sıra	Kruskal-Wallis	df ve p
Bir Hak Olarak Mahremiyet	Kullanıyor	74	173.36	27.036	df=2, p<.001
	Devre Dışı	204	180.41		
	Bilgisi Yok	56	112.72		
Kendi Mahremiyetine İlişkin Kaygı	Kullanıyor	74	155.97	3.721	df=2, p=.156
	Devre Dışı	204	174.83		
	Bilgisi Yok	56	156.03		
Başkalarının Mahremiyetine İlişkin Kaygı	Kullanıyor	74	179.59	12.992	df=2, p=.002
	Devre Dışı	204	173.60		
	Bilgisi Yok	56	129.29		
Diğer İhtimalli Mahremiyet	Kullanıyor	74	177.53	21.066	df=2, p<.001
	Devre Dışı	204	176.96		
	Bilgisi Yok	56	119.78		
Ölçek Ortalaması	Kullanıyor	74	171.57	17.265	df=2, p<.001
	Devre Dışı	204	178.98		
	Bilgisi Yok	56	120.29		

Kruskal-Wallis testi sonuçları, anlık mesajlaşma uygulamalarındaki son görülme özelliğini kullananlar, kullanmayanlar ve bu özellik hakkında bilgisi olmayanlar arasında mahremiyet yönelimi boyutları ve genel ölçek açısından istatistiksel olarak anlamlı farklılık olduğunu göstermektedir.

Tablo 3.29: Mahremiyet Yönelimi Boyutlarının Anlık Mesajlaşma Uygulamalarındaki Mavi Tik Özelliğinin Kullanımına Göre Karşılaştırması

Boyutlar	Kullanım Tercihi	N	Ortalama Sıra	Kruskal-Wallis	df ve p
Bir Hak Olarak Mahremiyet	Kullanıyor	48	180.68	30.626	df=2, p<.001
	Devre Dışı	226	179.64		
	Bilgisi Yok	60	111.22		
Kendi Mahremiyetine İlişkin Kaygı	Kullanıyor	48	162.10	2.298	df=2, p=.317
	Devre Dışı	226	172.23		
	Bilgisi Yok	60	153.99		
Başkalarının Mahremiyetine İlişkin Kaygı	Kullanıyor	48	179.76	13.688	df=2, p=.001
	Devre Dışı	226	174.94		
	Bilgisi Yok	60	129.68		
Diğer İhtimalli Mahremiyet	Kullanıyor	48	176.66	23.017	df=2, p<.001
	Devre Dışı	226	178.25		
	Bilgisi Yok	60	119.67		
Ölçek Ortalaması	Kullanıyor	48	176.60	16.289	df=2, p<.001
	Devre Dışı	226	177.36		
	Bilgisi Yok	60	123.09		

Son görülme özelliğindeki sonuçlara paralel olarak mavi tik özelliğinin kullanımı ile mahremiyet yönelimlerinin iki boyutu arasında, istatistiksel olarak 0.01 anlamlılık düzeyinde, bir diğer boyutu ile de 0.05 anlamlılık düzeyinde farklılık vardır. Akıllı telefonlarda şifre kullanımı, sadece diğer ihtimalli mahremiyet boyutunda anlamlı bir farklılık yaratmaktadır (U=12944.000, Z=-2.125, p=.034).

3.12.6.6. İnternette Paylaşılan Bilgilere Göre Mahremiyet Yönelimi Boyutları

Katılımcılara, kişisel bilgilerini sosyal medyada ve genel olarak internette paylaşıp paylaşmadıklarına ilişkin yöneltilen sorularda, Stutzman'ın (2006) belirlediği, yirmi altı maddelik kimlik öğeleri listesindeki on üç madde kullanılmış ve bu sorulara

verilen evet ya da hayır cevapları ile mahremiyet yönelimi boyutları arasında bir ilişki olup olmadığı incelenmiştir. On üç ögenin mahremiyet yönelimleri boyutlarında ve genel olarak ölçeğin tamamında, anlamlı bir farklılık göstermediği, ayrı ayrı Mann-Whitney U testi ile analiz edilmiştir. Gerçek ad bilgisinin paylaşılması, sadece bir hak olarak mahremiyet boyutunda (Mann-Whitney U=8729.000, Z=-2.459, p=.014), yaşanılan yer (Mann-Whitney U=14817.500, Z=-2.432, p=.015) ve meslek bilgisinin (Mann-Whitney U=15282.500, Z=-2.200, p=.028) paylaşımı diğer ihtimalli mahremiyet boyutunda anlamlı bir farklılığı işaret etmektedir. E-posta adresi, telefon numarası, cinsiyet, doğum yılı ve ilişki durumu hiçbir mahremiyet yönelimi boyutu ile anlamlı bir farklılık göstermezken, eğitim bilgilerinin ve fotoğrafların paylaşımı ile mahremiyet yönelimi boyutları arasında anlamlı bir farklılık bulunmaktadır.

Tablo 3.30: Mahremiyet Yönelimi Boyutlarının Eğitim Düzeyinin Paylaşılmasına Göre Karşılaştırması

Boyutlar	Eğitim Bilgisi	N	Ortalama Sıra	Mann-Whitney U	Z ve p
Bir Hak Olarak Mahremiyet	Paylaşıyor	171	201.79	14912.500	Z=-2.609, p=.009
	Paylaşmıyor	203	175.46		
Kendi Mahremiyetine İlişkin Kaygı	Paylaşıyor	171	195.77	15942.500	Z=-1.504, p=.133
	Paylaşmıyor	203	180.53		
Başkalarının Mahremiyetine İlişkin Kaygı	Paylaşıyor	171	203.25	14662.500	Z=-2.861, p=.004
	Paylaşmıyor	203	174.23		
Diğer İhtimalli Mahremiyet	Paylaşıyor	171	209.19	13648.000	Z=-4.030, p<.001
	Paylaşmıyor	203	169.23		
Ölçek Ortalaması	Paylaşıyor	171	207.03	14017.500	Z=-3.292, p<.001
	Paylaşmıyor	203	171.05		

Tablo 3.31: Mahremiyet Yönelimi Boyutlarının Fotoğrafların Paylaşılmasına Göre Karşılaştırması

Boyutlar	Fotoğraf	N	Ortalama Sıra	Mann-Whitney U	Z ve p
Bir Hak Olarak Mahremiyet	Paylaşıyor	249	199.03	12690.500	Z=-3.237, p=.001
	Paylaşmıyor	125	164.52		
Kendi Mahremiyetine İlişkin Kaygı	Paylaşıyor	249	191.04	14681.500	Z=-.990, p=.322
	Paylaşmıyor	125	180.45		

Boyutlar	Fotoğraf	N	Ortalama Sıra	Mann-Whitney U	Z ve p
Başkalarının Mahremiyetine İlişkin Kaygı	Paylaşıyor	249	196.97	13205.500	Z=-2.643, p=.008
	Paylaşmıyor	125	168.64		
Diğer İhtimalli Mahremiyet	Paylaşıyor	249	199.26	12633.500	Z=-3.361, p<.001
	Paylaşmıyor	125	164.07		
Ölçek Ortalaması	Paylaşıyor	249	197.15	13158.500	Z=-2.503, p=.012
	Paylaşmıyor	125	168.27		

Mann-Whitney U analizlerine göre hem eğitim bilgisinin hem de fotoğrafların paylaşımı, kendi mahremiyetine ilişkin kaygı boyutu dışında tüm mahremiyet yönelimi boyutlarında ve ölçek genelinde anlamlı bir farklılık olduğunu göstermektedir. Bu farklılık, her iki değişken için de diğer ihtimalli mahremiyet boyutunda, 0.01 anlamlılık düzeyindedir. Diğer mahremiyet yönelimi araştırmasında ise, eğitim durumunun paylaşımı, sadece diğer ihtimalli mahremiyet boyutu ile anlamlı bir farklılık ($F=4.037$, $p=.045$) göstermektedir (Livberber Göçmen, 2018). Bu farklılık, iki araştırmanın örneklemini arasındaki eğitim düzeyi farklılığından kaynaklanıyor olabilir. Livberber Göçmen'in örnekleminin yüzde 80'den fazlası lise ve üniversite mezunu iken bu çalışmada, lise ve üniversite mezunu örneklemin yüzde 50'sinden daha azdır.

3.12.6.7. Sosyal Ağ Sitesi ve Teknoloji Kullanım Sıklıkları ile İnternette Alışveriş Yapma Tercihlerine Göre Mahremiyet Yönelimi Boyutları

Paine ve mesai arkadaşlarının (2007, ss. 533-534), bireylerin çevrim içi deneyimleri ile mahremiyetlerini koruma konusunda nasıl hareket edeceklerine ilişkin bilgileri arasında ilişki olduğuna ilişkin önermesi ile ilişkili olarak çeşitli sosyal medya uygulaması ve EİT'lerin kullanım düzeyi ile mahremiyet yönelimi boyutları arasında bir korelasyon olduğu düşünülebilir. Bunu test etmek için Spearman korelasyon testi kullanılmıştır. Analiz sonuçları bilgisayar, tablet ve televizyon gibi cihazlar ve Instagram, SnapChat, TikTok, LinkedIn ve BİP uygulamalarının kullanım sıklığı ile mahremiyet yönelimleri arasında anlamlı bir ilişki olmadığını göstermektedir. Kullanım sıklıkları ile mahremiyet yönelimi boyutları arasındaki farklılığı test etmek için yaptığı ANOVA testleri sonucu Livberber Göçmen (2018) de Instagram kullanım düzeyi ile hiçbir mahremiyet yönelimi boyutu arasında anlamlı bir farklılığa rastlamamıştır. Aşağıdaki tabloda ise farklı anlamlılık düzeylerindeki korelasyonlar görülmektedir.

Tablo 3.32: Mahremiyet Yönelimi Boyutları ile Sosyal Medya ve EİT Kullanım Sıklıkları Arasındaki İlişkiyi Gösteren Korelasyon Analizi

		1	2	3	4	Ortalama
Facebook	Correlation Coefficient	.103*	.067	.078	.164**	.104*
	Sig. (2-tailed)	.046	.198	.132	.001	.044
	N	374	374	374	374	374
Twitter	Correlation Coefficient	.201**	.104*	.181**	.189**	.174**
	Sig. (2-tailed)	<.001	.044	<.001	<.001	<.001
	N	374	374	374	374	374
YouTube	Correlation Coefficient	.179**	.074	.062	.095	.091
	Sig. (2-tailed)	<.001	.156	.234	.066	.079
	N	374	374	374	374	374
Telegram, WhatsApp vd.	Correlation Coefficient	-.178**	-.114*	-.233**	-.208**	-.214**
	Sig. (2-tailed)	<.001	.028	<.001	<.001	<.001
	N	374	374	374	374	374
E-Devlet	Correlation Coefficient	.239**	.134**	.162**	.220**	.195**
	Sig. (2-tailed)	<.001	.009	.002	<.001	<.001
	N	374	374	374	374	374
HES	Correlation Coefficient	.173**	.191**	.192**	.216**	.199**
	Sig. (2-tailed)	<.001	<.001	<.001	<.001	<.001
	N	374	374	374	374	374
İnternet	Correlation Coefficient	.240**	.085	.206**	.196**	.183**
	Sig. (2-tailed)	<.001	.100	<.001	<.001	<.001
	N	374	374	374	374	374
Cep Telefonu	Correlation Coefficient	.127*	.037	.129*	.129*	.091
	Sig. (2-tailed)	.014	.474	.013	.013	.080
	N	374	374	374	374	374

** Correlation is significant at the 0.01 level (2-tailed).

* Correlation is significant at the 0.05 level (2-tailed).

Korelasyon tablosuna göre, Facebook kullanım sıklığı, kaygı boyutları dışındaki iki boyut ile 0.05 ve 0.01 anlamlılık düzeyinde ilişkilidir. Twitter kullanım sıklığı, kendi mahremiyetine ilişkin kaygı boyutunda 0.05, diğer üç boyutta ise 0.01 anlamlılık düzeyinde ilişkilidir. Twitter kullanımının yükselmesi ile mahremiyet yönelimleri ölçeğinde de bir yükselme olduğu söylenebilir. YouTube kullanımı ile sadece bir hak olarak mahremiyet boyutu arasında anlamlı bir ilişki vardır ($p<.001$). Tabloda görülen tek

negatif yönlü korelasyon, Telegram, WhatsApp ve diğer anlık mesajlaşma uygulamalarının kullanımı sıklıkları değişkenindedir. Spearman korelasyon analizi sonuçlarına göre; anlık mesajlaşma uygulaması kullanım sıklığı ile kendi mahremiyetine ilişkin kaygı boyutu arasında 0.05, diğer tüm boyutlar ile 0.01 anlamlılık düzeyinde negatif yönde bir ilişki vardır. Başka bir ifade ile bu uygulamalardaki kullanım artışı, mahremiyet yönelimlerini olumsuz yönde etkilemektedir.

Kamu uygulamaları olan E-Devlet ve Hayat Eve Sığar'ın (HES) kullanım sıklıkları ile mahremiyet yönelimi boyutları arasında, güçlü korelasyonlar olduğu görülmektedir. Bu uygulamaları daha sık kullananlar, dört mahremiyet boyutunda ve ölçek genelinde daha yüksek ortalamalara sahiptir. Özellikle salgın sonrası, 2021 yılı itibarıyla başlayan aşılama sürecinde kullanımı artan MHRS uygulamasının kullanım sıklığı ile sadece başkalarının mahremiyetine ilişkin kaygı boyutunda (Correlation Coefficient=.108, $p=.037$) ve diğer bir kamu sağlık uygulaması olan E-Nabız'ın kullanımı ile bir hak olarak mahremiyet (Correlation Coefficient=.106, $p=.040$) ve kendi mahremiyetine ilişkin kaygı (Correlation Coefficient=.103, $p=.048$) boyutlarında düşük düzeyde bir ilişki vardır.

EİT kullanım sıklıklarının, mahremiyet yönelimleri ile ilişkisi internet ve cep telefonu kullanım sıklıkları üzerinde anlamlı bir boyut kazanmaktadır. Spearman analizlerine bakıldığında, internet ve cep telefonu kullanım sıklıklarının, kendi mahremiyetine ilişkin kaygı boyutu hariç tüm boyutlarla istatistiksel olarak anlamlı bir ilişkisi olduğu görülür. İnternet kullanımı ile bir hak olarak mahremiyet, başkalarının mahremiyetine ilişkin kaygı ve diğer ihtimalli mahremiyet boyutları arasında 0.01 anlamlılık düzeyinde ve pozitif yönde bir ilişki vardır. Cep telefonu kullanımında ise aynı boyutlarla bir ilişki söz konusudur ama anlamlılık düzeyi 0.05'tir.

Katılımcıların, internetten alışveriş yapıp yapmama tercihleri ile mahremiyet yönelimleri arasında bir ilişki olup olmadığı da test edilmiştir. Mann-Whitney U testinden elde edilen sonuçlara göre; internetten alışveriş yapma veya yapmama tercihi ile bir hak olarak mahremiyet ($U=14622.500$, $Z=-2.760$, $p=.006$) ve başkalarının mahremiyetine ilişkin kaygı ($U=15161.500$, $Z=-2.171$, $p=.030$) boyutlarında anlamlı bir farklılık olduğu söylenebilir. Bu sonuç, Dinev ve Hart'ın (2005) mahremiyet endişeleri ile çevrim içi

alışveriş yapma niyeti arasında, negatif yönlü bir korelasyon olduğuna ilişkin bulguları ile örtüşmektedir. Bilgiler ışığında, H12 hipotezi kısmen kabul edilmiştir.

3.12.7. Dijital Okuryazarlık ve Dijital Vatandaşlık Düzeyine İlişkin Bulgular

Ülkelerin dijital okuryazarlık düzeylerine ilişkin, Eurostat'ın sağladığı istatistikler mevcuttur. Ancak bu veriler, çok az ülkede kent-kır ayrımına izin vermektedir ve Türkiye'ye ilişkin veriler de sadece tüm nüfusu temsil etmekte, kırsal bölge özelinde bir değerlendirmeye izin vermemektedir. Kayseri'nin kırsal mahallerinde yaşayan nüfus içerisinde alınan 374 kişilik örneklemin, dijital okuryazarlık düzeylerini belirlemek için on maddelik bir ölçek kullanılmıştır. On maddelik ölçekten elde edilen bulgular, Türkiye'deki kırsal bölgelerde yaşayan bireylerin dijital okuryazarlık düzeyleri açısından betimsel bir niteliğe sahiptir.

Tablo 3.33: Dijital Okuryazarlık Ölçeği Betimsel İstatistikleri

Maddeler	Ortalama ($\bar{X}$)	Standart Sapma	Min-Max
Kullandığım teknolojilerle ilgili karşılaştığım teknik problemleri (telefonun/bilgisayarın takılması, internete bağlanamaması gibi) nasıl çözeceğimi bilirim.	3.2647	1.07717	1-5
Yeni teknolojileri kolayca öğrenebilirim.	3.5080	.97072	1-5
Önemli yeni teknolojileri takip ederim.	3.3209	1.04522	1-5
Birçok farklı teknoloji hakkında bilgi sahibiyim.	3.2112	1.03855	1-5
Bilgi ve iletişim teknolojilerini iletişim kurma ve bilgiye erişme amaçlı kullanmak ve edindiğim bilgileri sergileyebileceğim dijital içerikler (Facebook, Twitter, Instagram paylaşımları, wikiler, bloglar, yorumlar) üretmek için gereken teknik becerilere sahibim.	3.1979	1.20027	1-5
Bilgi ve iletişim teknolojileri konusunda sahip olduğum beceriler (akıllı cep telefonunu sorun yaşamadan kullanma, sosyal medyada içerik paylaşma, fotoğraf çekme vb.) yeterlidir.	3.4091	1.02307	1-5
İnternette bilgi edinmek için yaptığım arama ve değerlendirmelerde kendime güvenirim.	3.5241	1.00038	1-5
Siber güvenlik, webde arama ve internette sahtecilik ile ilişkili konular hakkında bilgi sahibiyim.	3.3289	1.11839	1-5
Yakın çevremle, akranlarımla ya da arkadaşlarımla internet üzerinden (ör. Facebook, Twitter, WhatsApp, Bloglar aracılığıyla) sıklıkla yardımlaşırım.	3.7086	.93090	1-5
TOPLAM	3.4267	.68647	1-5

Ölçek maddeleri arasında en düşük ortalama ($\bar{X}=3.1979$), bilgi ve iletişim teknolojileri aracılığıyla kazanılan bilgileri sergilemek için dijital içerik üretebilmeye ilişkindir. İkinci en düşük ortalama, “birçok farklı teknoloji hakkında bilgi sahibiyim” ifadesinde görülmektedir ($\bar{X}=3.2112$). Ölçekteki en yüksek ortalama ise, internet üzerinden yardımlaşma ve iletişim kurma maddesinde görülmektedir ($\bar{X}=3.7086$). Bu bilgiler ışığında, kırsal mahallelerde yaşayan katılımcıların, internet aracılığıyla yakınları, arkadaşları ve akranlarıyla iletişim kurmakta zorlanmadığı, ancak kendi bilgi ve becerilerini sergileyebilecekleri dijital içerikler üretme ve yeni teknolojiler hakkında, yetersiz oldukları söylenebilir.

Araştırma örnekleminin dijital okuryazarlık düzeyinin, ortalama dijital okuryazarlık düzeyinin altında olup olmadığını test edebilmek için, tek örneklem t testi kullanılmıştır. Bu testi gerçekleştirebilmek için gerekli olan test değeri, Ng’ye (2012b) ait dijital okuryazarlık ölçeğinin, farklı Türkçe adaptasyonları ile yapılan çalışmalarda ortalamar kullanılarak elde edilmiştir. Ölçeğin, bu çalışmada kullanılan ve on maddeden oluşan versiyonu ile öğretmen adayları üzerinde yapılan araştırmada, ölçeğe verilen cevapların ortalaması 3.654’tür (Üstündağ vd., 2017). Orijinal ölçeği on yedi madde olarak Türkçeye adapte eden Hamutoğlu ve ekip arkadaşlarının (2017) kullanıldığı ve meslek yüksekokulu öğrencilerinin dijital okuryazarlık düzeylerinin araştırıldığı çalışmada, ölçeğin ortalaması 63.40’tır (Uyar, 2021). Ölçeğin, on yedi maddeden oluştuğu dikkate alındığında, bir maddenin ortalaması 3.729 (63.40/17) olarak hesaplanabilir. Aynı on yedi maddelik ölçeğin, okul öğrencisi öğretmeni adayları üzerinde kullanıldığı çalışmada ise ortalama puan 65.60’tır (Bay, 2021). Aynı şekilde hesaplandığında, bir maddenin ortalamasının 3.858 (65.60/17) olduğu görülür. Bu ortalamalar arasında en düşük değer olan 3.654, test değeri olarak belirlenmiştir.

Tablo 3.34: Tüm Katılımcıların Dijital Okuryazarlık Düzeyi için Tek Örneklem t Testi

Test Değeri: 3.654	N	Ortalama ($\bar{X}$)	Standart Sapma	Ortalama Standart Sapma
DOÖ Ortalaması	374	3.4267	.68647	.03550
	t	df	p Değeri	Ortalama Farkı
DOÖ Ortalaması	-6.402	373	<.001	-.22726

Uygulanan tek örneklem t testi, ortalamalar arasında 0.01 anlamlılık düzeyinde farklılık olduğunu işaret etmektedir. Ancak, bu karşılaştırma test değerinin elde edildiği çalışmalardaki yaş ortalaması ile mevcut araştırmadaki yaş ortalaması dikkate alındığında, geçerliliği tartışmalı hale gelmektedir. Bu sebeple aynı test, mevcut örneklemdeki dijital yerliler özelinde tekrar edilmiş ve aşağıdaki sonuçlar elde edilmiştir.

Tablo 3.35: Dijital Yerlilerin Dijital Okuryazarlık Düzeyi için Tek Örneklem t Testi

Test Değeri: 3.654	N	Ortalama ($\bar{X}$)	Standart Sapma	Ortalama Standart Sapma
DOÖ Ortalaması	159	3.6862	.53147	.04215
	t	df	p Değeri	Ortalama Farkı
DOÖ Ortalaması	.763	158	.447	.03216

Test, sadece örneklem içerisindeki dijital yerliler üzerinde uygulandığında, kırsalda yaşayan dijital yerliler ile diğer örneklem arasında anlamlı bir farklılığa rastlanmamaktadır. Bu durumda, kırsal bölgelerde yaşayan EİT kullanıcılarının dijital okuryazarlık düzeylerinin düşük olduğu, ama bu hipotezin, dijital yerli kategorisi özelinde desteklenmediği görülmektedir. Başka bir ifade ile H1 hipotezi örneklem geneli için kabul edilmiş, dijital yerliler özelinde ise reddedilmiştir.

Tablo 3.36: Dijital Vatandaşlık Ölçeği Betimsel İstatistikleri

Maddeler	Ortalama ($\bar{X}$)	Standart Sapma	Min-Max
İhtiyacım olan bilgiyi bulmak için interneti kullanırım.	3.8102	.88406	1-5
Benim için faydalı olan uygulamaları internetten bulabilir ve indirebilirim.	3.7647	.95656	1-5
Dijital teknolojileri (akıllı telefon, tablet, bilgisayar vb.) kullanarak ne zaman istersem internete erişebilirim.	3.8075	.86663	1-5
Sosyal ya da politik konularda interneti kullanarak daha çok bilgi edinirim.	3.6123	1.00239	1-5
Düşüncelerimi, hislerimi, görüşlerimi ifade etmek için internette özgün mesaj, ses, görüntü ya da videolar paylaşıyorum.	3.2754	1.22380	1-5
TOPLAM	3.6540	.74616	1-5

Choi, Glassman ve Cristol'un (2017) geliştirdikleri ve Türkçeye adaptasyonu Erdem ve Koçyiğit (2019) tarafından gerçekleştirilen dijital vatandaşlık ölçeğinin, beş maddesine verilen cevaplar sonucu elde edilen betimsel istatistikler; katılımcıların

interneti bilgiye erişim ve iletişim kurma açısından kullanmada, internet üzerinde kendilerini ifade edecek içerikler ve kendi bilgilerini sergileyecek dijital ürünler üretmeye kıyasla kendilerine daha fazla güvendiklerini göstermektedir. Dijital vatandaşlık ölçeğindeki en düşük ortalama, “düşüncelerimi, hislerimi, görüşlerimi ifade etmek için internette özgün mesaj, ses, görüntü ya da videolar paylaşırım” maddesindedir ($\bar{X}$ =3.2754). Aşağıda, dijital okuryazarlık ve dijital vatandaşlık düzeyleri farklı değişkenlere göre karşılaştırılmaktadır.

Tablo 3.37: Dijital Okuryazarlık ve Dijital Vatandaşlık Ölçeklerinin Çarpıklık ve Basıklık Değerleri

Ölçekler	N	Çarpıklık	Çarpıklık Standart Hatası	Basıklık	Basıklık Standart Hatası
Dijital Okuryazarlık	374	-.580	.126	-.133	.252
Dijital Vatandaşlık	374	-1.223	.126	1.753	.252

Dijital okuryazarlık ölçeğinin çarpıklık ve basıklık değerleri, Tabachnick ve mesai arkadaşlarının (2019) önerdiği ± 1.5 aralığı arasındadır ve parametrik testlere uygundur. Sadece beş maddesi kullanılan dijital vatandaşlık ölçeğinin basıklık değeri ise 1.753’tür. George ve Mallery (2020, s. 114), çarpıklık ve basıklık değerlerinin ± 1 aralığında olmasının psikometrik amaçlar için mükemmel kabul edilebileceğini, ancak çoğu durumda, ± 2 arasındaki bir değer de kabul edilebilir olduğunu ifade ederler. Buradan hareketle, her iki ölçek ile yapılan analizlerde (çok boyutlu mahremiyet yönelimleri ölçeği ile yapılan korelasyon analizleri hariç) parametrik testler kullanılmıştır.

3.12.7.1. Cinsiyete Göre Dijital Okuryazarlık ve Dijital Vatandaşlık Düzeyleri

Kayseri’nin kırsal mahallelerinde yaşayan ve akıllı telefon kullananlar arasından seçilen örneklem içerisinde, dijital okuryazarlık ve dijital vatandaşlık düzeylerinin cinsiyetler arasında farklılık gösterip göstermediğini test etmek için, bağımsız örneklem t testi kullanılmış ve aşağıdaki sonuçlar elde edilmiştir.

Tablo 3.38: Cinsiyete Göre Dijital Okuryazarlık ve Dijital Vatandaşlık Düzeyleri

Ölçekler	Cinsiyet	N	Ortalama ($\bar{X}$)	Standart Sapma	t Değeri	df ve p Değeri
Dijital Okuryazarlık	Kadın	77	3.4740	.64897	.678	df=372, p=.498
	Erkek	297	3.4145	.69639		
Dijital Vatandaşlık	Kadın	77	3.5584	.76388	-1.262	df=.208
	Erkek	297	3.6788	.74079		

T testi sonuçlarına göre, erkekler ve kadınlar arasında hem dijital okuryazarlık hem de dijital vatandaşlık düzeyi açısından anlamlı bir farklılık yoktur ($p>0.05$). Kadınların dijital okuryazarlık düzeyleri, erkeklerden az da olsa daha fazladır, ancak bu farklılık, istatistiksel açıdan anlamlı değildir. Benzer şekilde, dijital vatandaşlık düzeyinde de anlamlı bir farklılık gözlemlenmese de erkeklerin ortalaması, kadınlara kıyasla daha yüksektir. Literatürde, kadınların kendi beceri düzeylerini, önemli ölçüde daha düşük olarak değerlendirdikleri, ancak bu farklılığın sadece kadın ve erkeklerin kendi çevrim içi becerilerine ilişkin öz değerlendirmelerinde görüldüğü ve ölçülen gerçek yeteneklerde belirgin bir farklılığın olmadığı ifade edilmektedir (Hargittai & Shafer, 2006). Başka bir ifade ile cinsiyet, dijital yeterlilik düzeyi açısından belirleyici bir faktör değildir (Tomczyk, 2020). Avustralya’da yapılan EİT okuryazarlığı araştırmalarında ise, kız öğrencilerin erkeklere oranda daha iyi performansla sahip oldukları görülmüştür (Fraillon vd., 2018). Türkiye özelinde düşünüldüğünde ise, özellikle ileri yaştaki yetişkinlerde olmak üzere, bilgi işleme becerilerinde, cinsiyete dayalı farklılıkların söz konusu olduğunu işaret eden sonuçlar mevcuttur (Çalışma ve Sosyal Güvenlik Bakanlığı, 2016). Tüm bunlara rağmen, Türkiye’de yapılan diğer dijital okuryazarlık ölçümlerinde, cinsiyetler arasında dijital okuryazarlık düzeyi açısından anlamlı bir farklılık bulunmadığı görülmektedir (Bay, 2021; Ergin & Bozdağ, 2021; Uyar, 2021). Literatürdeki çalışmalar ve elde edilen bulgulara dayanarak H2 ve H3 hipotezleri reddedilmiştir.

3.12.7.2. Yaşa Göre Dijital Okuryazarlık ve Dijital Vatandaşlık Düzeyleri

Dijital okuryazarlık ve dijital vatandaşlık düzeylerinin, yaşa göre farklılaştığını göstermek için hem bağımsız örneklem için t testi hem de tek faktörlü varyans analizi (Anova) kullanılmış ve aşağıdaki sonuçlar elde edilmiştir.

Tablo 3.39: Dijital Yerli ve Dijital Göçmen Ayırımına Göre Dijital Okuryazarlık ve Dijital Vatandaşlık Düzeyleri

Ölçekler	Kategori	N	Ortalama ($\bar{X}$)	Standart Sapma	t Değeri	df ve p Değeri
Dijital Okuryazarlık	D. Yerli	159	3.6862	.53147	6.945	df=371.976, p<.001
	D. Göçmen	215	3.2349	.72514		
Dijital Vatandaşlık	D. Yerli	159	3.8730	.53977	5.356	df=366.165, p<.001
	D. Göçmen	215	3.4921	.83268		

Test sonuçları, her iki ölçekte de istatistiksel olarak 0.01 anlamlılık düzeyinde farklılığa işaret etmektedir. Başka bir ifade ile dijital yerli ve dijital göçmenlerin hem dijital okuryazarlık düzeyleri hem de dijital vatandaşlık düzeyleri birbirlerinden anlamlı ölçüde farklıdır. Dijital yerliler, göçmenlere göre, daha fazla dijital okuryazarlık ve dijital vatandaşlık becerisine sahiptirler. Testlerden elde edilen sonuçlar, tüm yaşamları boyunca internete maruz kalmaları sebebiyle, genç nesillerin dijital olarak daha yetenekli oldukları yönündeki genel kanıyı destekler niteliktedir (van Laar vd., 2019).

Testler, dijital yerli – dijital göçmen ayırımının dışında, yaş grubu kategorileri arasında da anlamlı bir farklılık olduğunu göstermektedir.

Tablo 3.40: Yaş Gruplarına Göre Dijital Okuryazarlık ve Dijital Vatandaşlık Düzeyleri

		Sum of Squares	df	Mean Square	F Değeri	P Değeri
Dijital Okuryazarlık Ortalaması	Between Groups	34.735	6	5.789	15.064	<.001
	Within Groups	141.038	367	.384		
	Total	175.773	373			
Dijital Vatandaşlık Ortalaması	Between Groups	48.111	6	8.018	18.443	<.001
	Within Groups	159.558	367	.435		
	Total	207.669	373			

Anova testi sonuçları, belirlenen yedi farklı yaş grubu arasında, dijital okuryazarlık ve dijital vatandaşlık düzeyleri açısından anlamlı bir farklılık olduğunu göstermektedir ve bu farklılık istatistiksel olarak anlamlıdır (p<0.01). Dijital okuryazarlık ve dijital vatandaşlık ile yaş değişkeni arasındaki ilişkiyi açıklamak için kullanılan Pearson korelasyon analizi sonuçlarına göre, yaş arttıkça hem dijital okuryazarlık düzeyi

(Pearson Correlation=-.425, $p<0.01$) hem de dijital vatandaşlık düzeyi (Pearson Correlation=-.413, $p<0.01$) düşmektedir. Bu sonuç, Choi ve arkadaşlarının (2021), yaşın tekno-kapital olarak ifade ettikleri dijital becerilere olumsuz bir etkisi olduğu sonucu ile paraleldir. Yapılan analizlere dayanarak, H4 ve H5 hipotezleri kabul edilmiştir.

3.12.7.3. Eğitim Durumuna Göre Dijital Okuryazarlık ve Dijital Vatandaşlık Düzeyleri

Eğitim faktörünün de dijital beceriler üzerinde etkili olduğu bilinmektedir. Literatürdeki araştırmalar, eğitim düzeyindeki artışın, daha yüksek dijital becerilerle sonuçlandığını doğrulamaktadır (van Deursen vd., 2011).

Tablo 3.41: Eğitim Düzeyine Göre Dijital Okuryazarlık ve Dijital Vatandaşlık

		Düzeyleri				
		Sum of Squares	df	Mean Square	F Değeri	P Değeri
Dijital Okuryazarlık Ortalaması	Between Groups	33.021	4	8.255	21.339	<.001
	Within Groups	142.752	369	.387		
	Total	175.773	373			
Dijital Vatandaşlık Ortalaması	Between Groups	35.678	4	8.919	19.136	<.001
	Within Groups	171.991	369	.466		
	Total	207.669	373			

Anova testi sonuçları incelendiğinde, her iki ölçek için de farklı eğitim düzeyindeki bireylerin ortalamalarının, birbirlerinden 0.01 anlamlılık derecesinde farklı olduğu görülmektedir. Farklılığın, en çok nereden kaynaklandığını anlamak için uygulanan Post Hoc LSD testi sonuçlarına göre; ilkokul mezunları tüm diğer eğitim düzeylerindeki bireyler ile güçlü anlamlılık düzeyinde bir farklılık göstermektedir ($p<.001$). Sonuçlar, Choi ve arkadaşlarının (2021), eğitim ve gelirin, bu yetenek boyutları (tekno-sermaye) üzerinde olumlu etkisi olduğuna ilişkin bulgularını desteklemektedir. Bulgular ışığında, H6 hipotezi kabul edilmiştir.

3.12.7.4. EİT Maruziyet Sürelerine Göre Dijital Okuryazarlık ve Dijital Vatandaşlık Düzeyleri

Dijital yerli ve dijital göçmen ayrımı ile ilişkili olarak, bireylerin; interneti, cep telefonunu ve akıllı telefonu daha erken kullanmaya başlamaları, onların dijital becerileri üzerinde olumlu bir etkiye sahiptir. Literatürde, yüksek seviyede dijital cihaz deneyimi

olanların, daha yüksek EİT okuryazarlığı seviyesine sahip olduğunu gösteren araştırmalar mevcuttur (Fraillon vd., 2018). Değişkenler arasındaki ilişkiyi test etmek için Pearson korelasyon testi uygulanmış ve aşağıdaki bulgular elde edilmiştir.

Tablo 3.42: EİT Maruziyet Süreleri ile Dijital Okuryazarlık ve Dijital Vatandaşlık Düzeyleri Arasındaki Korelasyon

		İlk İnternet	İlk Cep Telefonu	İlk Akıllı Telefon
Dijital Okuryazarlık	Pearson Correlation	-.211**	.107*	-.250**
	Sig. (2-tailed)	<.001	.042	<.001
	N	365	365	346
Dijital Vatandaşlık	Pearson Correlation	-.293**	-.028	-.318**
	Sig. (2-tailed)	<.001	.588	<.001
	N	365	365	346

** Correlation is significant at the 0.01 level (2-tailed).

* Correlation is significant at the 0.05 level (2-tailed).

Analiz sonuçları, internete daha erken bir tarihte bağlanmış olmanın hem dijital okuryazarlık hem de dijital vatandaşlık düzeyleri üzerinde pozitif bir etkisi olduğunu gösterir. Başka bir ifade ile internete ilk bağlanılan tarih ile ölçek düzeyleri arasında, 0.01 anlamlılık düzeyinde negatif yönlü bir ilişki vardır. Aynı düzeyde anlamlı ilişki, ilk akıllı cep telefonunu edinme tarihinde de görülmektedir. Örneklemdeki bireyler, ilk akıllı cep telefonlarını ne kadar erken edinirlerse, dijital okuryazarlık ve dijital vatandaşlık düzeyleri o kadar yüksek olmaktadır. İlk cep telefonunun edinilme tarihi, dijital vatandaşlık düzeyi ile anlamlı bir ilişki göstermezken ($p=.588$) dijital okuryazarlık düzeyi ile gösterdiği ilişki hem 0.05 anlamlılık düzeyindedir ($p=.042$) hem de diğer değişkenlerden farklı olarak pozitif yönlüdür. Yapılan analizler sonucunda H7 ve H8 hipotezleri kabul edilmiştir.

3.12.7.5. Sosyal Ağ Sitesi ve Teknoloji Kullanım Sıklıkları ile İnternette Alışveriş Yapma Tercihlerine Göre Dijital Okuryazarlık ve Dijital Vatandaşlık Düzeyleri

Araştırmada, internet ile daha erken bir tarihte tanışan ve akıllı cep telefonu kullanmaya daha önce başlayan bireylerin, dijital okuryazarlık ve dijital vatandaşlık düzeylerinin daha yüksek olduğuna dair istatistiki bulgular elde edilmiştir. Bu bulgulara ek olarak dijital okuryazarlık ve dijital vatandaşlık düzeylerinin EİT'lerin ve çeşitli sosyal medya uygulamalarının kullanım sıklıklarına bağlı olarak değişip değişmediği de test

edilmiştir. Katılımcıların, çeşitli sosyal medya uygulamaları ve EİT'leri kullanma sıklıkları ile dijital okuryazarlık ve dijital vatandaşlık düzeyleri arasındaki ilişkiyi analiz etmek için, Pearson ve Spearman korelasyon testleri kullanılmıştır.

Tablo 3.43: Sosyal Medya ve EİT Kullanım Sıklıkları ile Dijital Okuryazarlık ve Dijital Vatandaşlık Düzeyleri Arasındaki Korelasyon

Uygulama, Cihaz ve Teknolojiler		Dijital Okuryazarlık	Dijital Vatandaşlık
Facebook	Pearson Correlation	.220**	.266**
	Sig. (2-tailed)	<.001	<.001
Twitter	Pearson Correlation	.297**	.242**
	Sig. (2-tailed)	<.001	<.001
Instagram	Pearson Correlation	.421**	.368**
	Sig. (2-tailed)	<.001	<.001
TikTok	Pearson Correlation	.234**	.182**
	Sig. (2-tailed)	<.001	<.001
YouTube	Pearson Correlation	.354**	.360**
	Sig. (2-tailed)	<.001	<.001
SnapChat	Correlation Coefficient	.266**	.109*
	Sig. (2-tailed)	<.001	.035
LinkedIn	Correlation Coefficient	.149**	.046
	Sig. (2-tailed)	.004	.372
BİP	Correlation Coefficient	.158**	.073
	Sig. (2-tailed)	.002	.162
Telegram ve diğer anlık mesajlaşma uygulamaları	Pearson Correlation	.282**	.162**
	Sig. (2-tailed)	<.001	.002
E-Devlet	Pearson Correlation	.202**	.258**
	Sig. (2-tailed)	<.001	<.001
Hayat Eve Sığar (HES)	Pearson Correlation	.167**	.204**
	Sig. (2-tailed)	.001	<.001
Merkezi Hekim Randevu Sistemi (MHRS)	Pearson Correlation	.240**	.175**
	Sig. (2-tailed)	<.001	<.001
E-Nabız	Pearson Correlation	.246**	.238**
	Sig. (2-tailed)	<.001	<.001
İnternet	Pearson Correlation	.481**	.454**
	Sig. (2-tailed)	<.001	<.001
Cep Telefonu	Correlation Coefficient	.339**	.304**

Uygulama, Cihaz ve Teknolojiler		Dijital Okuryazarlık	Dijital Vatandaşlık
	Sig. (2-tailed)	<.001	<.001
Bilgisayar	Pearson Correlation	.321**	.262**
	Sig. (2-tailed)	<.001	<.001
Tablet	Correlation Coefficient	.183**	.165**
	Sig. (2-tailed)	<.001	.001
Televizyon	Pearson Correlation	-.136**	-.044
	Sig. (2-tailed)	.008	.397

** Correlation is significant at the 0.01 level (2-tailed).

* Correlation is significant at the 0.05 level (2-tailed).

Korelasyon analizinden elde edilen veriler incelendiğinde, dijital okuryazarlık düzeyi ile tablodaki tüm değişkenler arasında istatistiksel olarak anlamlı bir ilişki olduğu görülür. Dijital okuryazarlık düzeyi ile en yüksek korelasyona sahip olan değişken, internet (Pearson Correlation=.481) ve Instagram (Pearson Correlation=.421) kullanım sıklığıdır. Dijital okuryazarlık düzeyi, tüm değişkenler ile 0.01 anlamlılık düzeyinde ilişkilidir. Bu ilişkilerin yönü, sadece televizyon kullanım sıklığında değişmektedir. Başka bir ifade ile televizyon kullanım sıklığı arttığında, dijital okuryazarlık düzeyinin düştüğü söylenebilir (Pearson Correlation=-.136, p=.008).

Dijital okuryazarlık düzeyinde olduğu gibi, dijital vatandaşlık ölçeği de tablodaki değişkenler ile çeşitli düzeylerde korelasyon sergilemektedir. Ancak LinkedIn, BİP ve televizyon kullanımları ile dijital vatandaşlık düzeyi arasında anlamlı bir ilişki yoktur. Özellikle LinkedIn, SnapChat ve BİP uygulamalarının, örneklem içerisindeki kullanımlarının, oldukça düşük olduğu hatırlandığında, bu sonuç şaşırtıcı olmamaktadır. Diğer ölçekte olduğu gibi, internet kullanım sıklığı dijital vatandaşlık düzeyi ile en güçlü ve pozitif yönlü korelasyonu oluşturmaktadır (Pearson Correlation=.454). Literatürde, bilgisayarlı olanlar ve olmayanlar (t=2.639, p=.009) ile evde interneti olanlar ve olmayanlar (t=4.963, p=.000) arasında dijital okuryazarlık düzeyi açısından anlamlı bir farklılık olduğunu gösteren sonuçlar yer almaktadır (Uyar, 2021).

Dijital okuryazarlık ve dijital vatandaşlık düzeylerinin, internetten alışveriş yapanlar ve yapmayanlar arasında farklılaşıp farklılaşmadığını test etmek için bağımsız örneklem t testi uygulanmıştır ve internetten alışveriş yapmayı tercih eden bireylerin, dijital okuryazarlık ve dijital vatandaşlık düzeylerinin daha yüksek olduğu görülmüştür.

Tablo 3.44: İnternette Alışveriş Yapma Tercihine Göre Dijital Okuryazarlık ve Dijital Vatandaşlık Düzeyleri

Ölçekler	İnternette Alışveriş	N	Ortalama ($\bar{X}$)	Standart Sapma	t Değeri	df ve p Değeri
Dijital Okuryazarlık	Evet	163	3.7141	.53332	7.923	df=371.731, p<.001
	Hayır	211	3.2047	.70991		
Dijital Vatandaşlık	Evet	163	3.9239	.50928	6.867	df=355.233, p<.001
	Hayır	211	3.4455	.82981		

Bağımsız örneklem t testi sonucunda, internette alışveriş yapıp yapmama tercihinin, her iki düzeyde de istatistiksel olarak 0.01 anlamlılıkta bir farklılık oluşturduğu görülmüştür. Örneklem içerisinde, dijital okuryazarlık düzeyi düşük olanların, internette alışveriş yapmayı tercih etmedikleri söylenebilir.

3.12.8. Mahremiyet Yönelimleri ile Dijital Okuryazarlık ve Dijital Vatandaşlık Düzeyi Arasındaki İlişki

Kayseri'nin kırsal mahallelerinde yaşayan ve akıllı cep telefonu kullanan bireyler üzerinde gerçekleştirilen araştırmanın üç bağımlı değişkenini oluşturan mahremiyet yönelimleri boyutları, dijital okuryazarlık ve dijital vatandaşlık arasında bir ilişki olup olmadığı test edilmiş ve aşağıdaki korelasyon tablosu oluşturulmuştur.

Tablo 3.45: Mahremiyet Yönelimi Boyutları ile Dijital Okuryazarlık ve Dijital Vatandaşlık Düzeyleri Arasındaki Korelasyon

Mahremiyet Yönelimleri		Dijital Okuryazarlık	Dijital Vatandaşlık
Bir Hak Olarak Mahremiyet	Correlation Coefficient	.199**	.255**
	Sig. (2-tailed)	<.001	<.001
Kendi Mahremiyetine İlişkin Kaygı	Correlation Coefficient	.099	.097
	Sig. (2-tailed)	.056	.062
Başkalarının Mahremiyetine İlişkin Kaygı	Correlation Coefficient	.162**	.221**
	Sig. (2-tailed)	.002	<.001
Diğer İhtimalli Mahremiyet	Correlation Coefficient	.171**	.253**
	Sig. (2-tailed)	<.001	<.001
Çok Boyutlu Mahremiyet Yönelimleri Ölçeği	Correlation Coefficient	.165**	.231**
	Sig. (2-tailed)	.001	<.001

** Correlation is significant at the 0.01 level (2-tailed).

Spearman korelasyon analizleri, dijital okuryazarlık düzeyi ile mahremiyet yönelimlerinin üç boyutu arasında, istatistiksel olarak anlamlı ve güçlü bir ilişki olduğunu göstermektedir. Kendi mahremiyetine ilişkin kaygı boyutu ile ne dijital okuryazarlık ne de dijital vatandaşlık düzeyi ile anlamlı bir korelasyon sergilememektedir. Bu boyut, daha önceki testlerde de farklılaşmanın en az görüldüğü boyuttur. Mahremiyet yönelimleri ölçeği, bir bütün olarak değerlendirildiğinde ise yine her iki değişken ile 0.01 anlamlılık düzeyinde ilişki kurmaktadır. Bir hak olarak mahremiyet, başkalarının mahremiyetine ilişkin kaygı ve diğer ihtimalli mahremiyet boyutları, dijital okuryazarlık düzeyi ile olduğu gibi dijital vatandaşlık düzeyi ile de istatistiksel açıdan ilişkilidir. Başka bir ifade ile dijital okuryazarlık ve dijital vatandaşlık düzeyindeki artış üç mahremiyet boyutunda da artışla sonuçlanmaktadır. Literatürde, internet okuryazarlığı ile mahremiyet endişeleri arasında negatif yönlü bir ilişki olduğunu işaret eden bir araştırmada, bu durumun iki farklı şekilde yorumlanabileceği belirtilir: Bireyler, internet kaynaklı tehlikelerle baş edebilme kabiliyetine sahip oldukları için, daha az mahremiyet endişesi duyabilir ya da sahip oldukları internet ve ona bağlı sistemlere ilişkin bilgi ve deneyim ile temel güvenlik açıklarına ve sistemin güvensizliklerine ilişkin farkındalıkları nedeniyle daha fazla mahremiyet endişelerine sahip olabilirler (Dinev & Hart, 2005, s. 19). Yapılan analizlere dayanarak H15 hipotezi kabul edilmiştir.

Tablo 3.46: Mahremiyet Yönelimi Alt Boyutlarına Göre Dijital Okuryazarlık ve Dijital Vatandaşlık Düzeyleri

Alt Boyutlar	Dijital Okuryazarlık		Dijital Vatandaşlık	
	Ortalama (X̄)	Standart Sapma	Ortalama (X̄)	Standart Sapma
Mahremiyet Savunucuları	3.56	.83	3.81	.77
Mahremiyet Bireycileri	3.40	.73	3.59	.71
Mahremiyet Ilımlıları	3.27	.73	3.64	.84

Dijital okuryazarlık ve dijital vatandaşlık düzeyleri, mahremiyet yönelimi ölçeği faktörlerinde alınan puanla belirlenen alt boyutlarına göre incelendiğinde, mahremiyet savunucularının, örneklem içerisindeki en yüksek dijital okuryazarlık ($\bar{X}=3.56$) ve dijital vatandaşlık ($\bar{X}=3.81$) düzeyine sahip olduğu görülmektedir. Alt boyutlar arasında, dijital okuryazarlık ve dijital vatandaşlık düzeyleri açısından anlamlı bir farklılık olup olmadığını test etmek için Anova testi kullanılmış ve mahremiyet alt boyutları arasında,

dijital okuryazarlık düzeyleri açısından oldukça düşük düzeyde ama istatistiksel olarak anlamlı bir farklılık olduğu görülmüştür ($F=3.210$, $p=.041$). Farklılığın, hangi iki alt boyuttan kaynaklandığını ortaya koymak için yapılan Post Hoc LSD testine göre; mahremiyet savunucuları ile mahremiyet ılımlıları arasındaki farklılık, diğer eşleşmelere oranla daha fazladır (Mean Difference=.29153, Std Error=.12129, $p=.017$). Dijital vatandaşlık düzeyinde ise alt boyutlar arasında istatistiksel açıdan anlamlı bir farklılık yoktur ($F=2.840$, $p=.060$).

Çalışma kapsamında yapılan son korelasyon testi ise, yukarıdaki pek çok karşılaştırmada, birbirleriyle oldukça ilişkili olduğunu gösteren dijital okuryazarlık ve dijital vatandaşlık düzeylerine ilişkindir. Uygulanan Pearson korelasyon testine göre, bu iki değişken arasında istatistiksel açıdan 0.01 anlamlılık düzeyinde pozitif yönlü bir ilişki vardır (Pearson Correlation=.516, $p<0.01$). Birbiri ile oldukça ilişkili olan bu iki olguyu ölçen ölçeklerin, bu derecede bir korelasyon ortaya koyması önemli bir göstergedir. Bu korelasyon analizine dayanarak H16 hipotezi kabul edilmiştir.

SONUÇ ve ÖNERİLER

İnternet ve mobil iletişim teknolojilerinin kullanımının tüm dünyada yaygınlaşması, çeyrek asır önce hayal edilmesi bile zor olan bir etkileşim ortamı oluşturmuştur. Bu etkileşim, insanların iletişim kurma, sosyalleşme, alışveriş yapma, itibar ya da popülerlik kazanma, oyun oynama, eğlenme ve öğrenme pratiklerini değiştirmiştir. Hatta internetin, bireylerin gündelik yaşamlarındaki pek çok aktiviteyi dönüştürdüğü söylenebilir. İlk defa duyulan bir kelimenin anlamını öğrenmek için, kitaplıkta duran kalın sözlüğe değil, cebe sığacak kadar ince olan akıllı telefona başvurulur. Akşam hazırlanacak yemek için alternatif fikirler, mutfak çekmecesinde duran tarif defterinden değil, YouTube'daki yemek kanallarından edinilir. Güncel haberler, gazete ya da televizyonlardan değil, internetteki haber sitelerinden ya da Twitter'dan takip edilir. Üstelik bu örnekler, sadece ilk akla gelenlerdir ve çeşitlendirilebilirler. Kısacası internet, insanların gündelik hayatını dönüştürmektedir. Bu dönüşümün daha iyi bir toplumsal yaşama doğru mu, yoksa karanlık ve distopik bir geleceğe doğru mu gerçekleştiği ise, farklı bakış açılarıyla değerlendirilebilir: Bardak hem boş hem de doludur.

Paul Gilster, 1997 gibi erken bir tarihte, teknoloji ve internetin, insan hayatını değiştirmesinin kaçınılmaz olduğunu söylemiştir. Kökleri 1969 yılına kadar uzanan ve yaklaşık olarak otuz yıldır, “sıradan” insanlar tarafından kullanılabilen internetin toplumsal yaşamdaki güncel önemi ve halihazırda gündelik hayatlarda yarattığı dönüşüm düşünüldüğünde, bu öngörünün haklılığı ortaya çıkmaktadır. İnternet artık işlerin takip edilmesinde ve bankacılık dahil pek çok hizmetin yürütülmesinde yeri doldurulamayacak bir pozisyon kazanmıştır. Merkezi olmayan, birbirine pek çok alternatif yol ile bağlanabilen ve dağınık yapıdaki birimlerin çeşitli protokoller ile birbirine bağlandığı bir ağ olarak internet, sadece gündelik hayat pratiklerini değil, toplumsal örgütlenme biçimini de dönüştürmektedir. Bu dönüşüm, kitle toplumundan ağ toplumuna doğru olmaktadır.

Aslında, ağ tipi örgütlenme, insanlık tarihindeki eski bir pratik olsa da, internet ağı ile bambaşka bir boyut kazanmıştır (Castells, 2010b). Bu ağ yapılanması, toplumlardaki örgütlenmelerin hem bireysel hem toplumsal düzeyde gerçekleşmesini

mümkün kılan bir yapıdır. Ağ toplumu kavramsallaştırmasının temeli, bu yapıya dayanmaktadır. Sadeleştirilmiş bir ifade ile ağ toplumu, en küçük birimlerini grup ya organizasyonların değil bireylerin oluşturduğu toplumlardır. Bu toplumlarda birimler arası iletişim, artan bir şekilde dijital teknolojiler ile dolaylanmaktadır. Bu yapılanma şekli, henüz tüm toplumlar için geçerli değildir. Yine de bu sosyal yapı, bir şekilde herkesi etkilemektedir. Dünyanın her yerinde, insan yaşamını şekillendiren ve kontrol eden finansal piyasalardan üretim, yönetim, mal ve hizmetlerin dağıtımına bilim, teknoloji, iletişim, kültür, sanat ve spor faaliyetlerden uluslararası sivil toplum örgütlenmelerine kadar pek çok faaliyet alanı, küresel ağlarda organize edilmektedir (Castells, 2004a) ve bu durum kaçınılmaz olarak tüm dünyayı etkilemektedir. van Dijk'in “ağların dışsallığı” kanunu ile anlatmak istediği de tam olarak budur. Dünya toplumları, ağın bir parçası olsalar da olmasalar da bu yapılanmadan etkilenmektedirler. Bu etkinin, olumlu bir yönde ilerlemesi de ağ toplumuna nitelikli entegrasyona ve dijital vatandaşların sayısının artmasına bağlıdır.

İnternete erişim, ağ toplumuna entegrasyonun ve ağa eklemlenmenin temel bir göstergesi olarak değerlendirilebilir. Bu bakımdan, 2021 itibariyle, dünya nüfusunun yaklaşık yüzde 65'inin internete erişebiliyor oluşu, önemli bir gelişmedir. Ancak internet erişimi, tek başına geçerli bir gösterge olarak kabul edilse bile, ağ toplumu içerisindeki fırsat eşitliğinin sağlanması açısından yeterli sayılmaz. Çünkü ağ toplumu, çelişki ve mücadelelerden muaf değildir (Castells, 2010a). Bu toplumun altyapılarını oluşturan ağlar, toplum içerisindeki mevcut yapıları güçlendirme eğilimine sahiptir (van Dijk, 2017). Başka bir ifadeyle, kitle toplumlarının ağ toplumlarına dönüşmeleri, fırsat eşitliği ve demokrasiyi tek başına garanti altına alacak bir gelişme değildir. van Dijk, ağ toplumuna ilişkin özellikleri, belirlediği yedi kanun ile nitelendirmiştir. Özellikle ağ genişlemesi ve ağlardaki güç kanunları, ağ toplumunun bir ütopya olmadığını ve sosyal mücadelenin devam ettiğini işaret etmektedir. Bu toplum yapısı, üç temel katmandan oluşmaktadır: enformasyon seçkinleri, katılanlar ve dışlanmışlar.

Ağ toplumlarının en avantajlı ve ayrıcalıklı katmanı olan enformasyon seçkinleri, yüksek eğitim ve gelir düzeyine sahip olan ve EİT'leri etkin bir şekilde kullanarak toplumdaki tüm önemli kararların alınmasında rol oynayan kişilerden oluşmaktadır (van Dijk, 2006). İkinci ve üzerinde ağırlıklı olarak durulması gereken katman ise katılanlardan oluşmaktadır. Bu katman, en kalabalık katmandır ve EİT kullanımları iş

veya eğitim değil eğlence odaklıdır. van Dijk (2017), bu katmandakilerin kullanım becerileri ve kullanım çeşitliliklerinin enformasyon seçkinlerine kıyasla daha az olduğunu ifade eder. Ağ toplumlarında enformasyon seçkinleri, üretici ve söz sahibi, katılan çoğunluk ise çoğunlukla tüketici ve nadiren söz sahibidir. Dünya nüfusunun internete erişiminin her geçen gün arttığı dikkate alındığında, ağ toplumunun katılanlar katmanının daha da kalabalıklaştığı söylenebilir. Ağ toplumuna katılımın artması gibi olumlu bir gelişmenin arkasındaki sorunları ifade etmek için, tekrar ağın kanunlarına dönmek gerekmektedir. Ağ genişlemesi kanununa göre, ağlardaki birim ve düğüm noktalarındaki artış, ağın daha büyük hale gelmesine ve bir bakıma ağlardaki birimlerin, birbirlerine görünmez olmalarına neden olur. Oluşan bu sorun, aracı sistemler ile çözülür. Aracı sistemler ise, enformasyon seçkinlerinin kontrolündedir. Hatırlanması gereken ikinci kanun ise, ağlardaki güç kanunudur. Bu kanuna göre; halihazırda daha fazla bağlantıya sahip olan birimlerin (enformasyon seçkinleri), daha fazla bağlantı kurma olasılığı daha yüksektir ve buna karşılık, ağdaki çoğu birim (katılan çoğunluk) sadece birkaç bağlantıya sahiptir. Başka bir ifade ile ağ toplumunda bağlantı fırsatları, normal dağılmamaktadır.

Katmanlı yapı, ağ toplumunun yarattığı tek sorun değildir. Yukarıda da değinildiği gibi ağ toplumunun en temel ve en güçlü ağı olarak internet, gündelik hayat pratiklerinden kişilerarası ilişkilere pek çok geleneksel deneyimi dönüştürmektedir. Yeni biri ile tanışmak, onunla arkadaş olmak, beklenmedik kişilerle beklenmedik anlarda iletişim kurmak, ağ üzerindeki “aracı” uygulamalar (sosyal ağ siteleri) sayesinde çok kolaylaşmıştır. Bunun bir sonucu olarak EİT’ler ile dolayımlanan kişilerarası iletişim miktarı, her geçen gün artmaktadır. İnternet, kendisinden önce sağlanması mümkün olmayan temaslara ve tanışıklıklara gebedir. Dolayımlanan bu iletişimin kapsamı, birimler arası ile sınırlı değildir. Bu teknolojiler sayesinde bir kişi, mesajını milyonlarca kişiye ulaştırabilmektedir. Ancak, bu karşılıklı konuşma ortamı, kusursuz değildir. İlk sorun, dikkatin sınırlılığı kanunu ile açıklanabilir. Kullanıcı temelli içerik üretimi yapısıyla internet, herkese içerik üretme ve mesajlarını yayınlama şansı verse de bu mesajların görülme ve dikkate alınma olasılığı, dikkatin sınırlılığı nedeniyle düşüktür. Daha açık bir şekilde ifade edilirse, internette herkes, bir şey söyleyebilmekte ama çok az kişi söylediğini başkalarına dinletebilmektedir. İkinci sorun ise, internet yolu ile kolayca kurulan temaların ve arkadaşlıkların benzer bir kolaylıkla ortadan kaldırılabilmesidir.

Temasların kolayca ortadan kaldırılabılır oluşu, Bauman’a göre; gerçek diyalogun önünde duran bir engeldir: Sosyal medya, diyalog kurmayı öğretmemektedir. Çünkü bu ağlarda, anlaşmazlıktan kaçınmak çok kolaydır. İnsanların çoğunun, sosyal medyayı, bir araya gelmek veya ufuklarını genişletmek yerine, kendi seslerinin yankıları olan sesleri duyacakları, kendi yüzlerinin yansıması olan yüzleri görecekleri bir konfor alanı yaratmak için kullandığını söyleyen Bauman, sosyal medyanın çok kullanışlı ve keyifli bir tuzak olduğunu ifade etmektedir (Koçak, 2016). Bu “tuzak” içerisinde topluluklar, ferdi “bağlanma” ve “bağlantıyı kesme” karar ve dürtüleri ile oluşturulmakta, parçalanmakta, genişlemekte ve küçülmektedirler (Bauman, 2014). Bauman’a göre akışkan modernitenin koşullarına uygun bir şekilde yaşayan insanların, ağın gelişini kutlaması ve bu yapıyı eski tip topluluklara yeğlemesinin nedeni, internet ile kurulan iletişimin değişken, kırılgan ve durdurulamaz bir şekilde parçalanmaya yatkın oluşudur.

Ağ toplumu içerisinde karşılaşılan bir diğer sorun, en basit ifade ile “yüzeyselleşme” olarak nitelendirilebilir. Kullanıcı temelli içerik üretimini müjdeleyen Web 2.0 devrimi, çok geçmeden sindirilmesi ve bireysel olarak işlenip özümsemesi zorlaşan boyutta bir enformasyon yığını oluşturmuştur. Bu boyutta bir enformasyon kümesi içerisinde, talep edilen bilgi parçacığına ulaşmak hem sınırlı dikkatler nedeniyle zorlaşmakta hem de ağlardaki güç kanununun etkisiyle kolaylaşmaktadır. Ancak bu kolaylık, sadece araçlar (arama motorları) tarafından belirlenen ve onların süzgecinden geçen bilgilere ulaşım ile sınırlıdır. Bu noktada, tekrar Bauman’a başvurulabilir. Bauman’a göre, “daha fazla bilginin “erişilebilir” olması için ödediğimiz bedel, anlam içeriğinin daralması” ve bilginin önem ve değerindeki büyük azalmadır (Bauman, 2014). Pettman, özellikle sosyal medya çerçevesinde bu yüzeyselleşmeyi, “sonsuz dikkat dağınıklığı” metaforu ile açıklar. Dikkati cezbeden pek çok farklı hikâyenin dolaşımda oluşu, birincil haberlerin kolaylıkla kontrol edilmesini sağlar. “Örneğin, insan hakları meseleleri gibi, potansiyel açıdan tarihsel öneme sahip olabilecek konular, artık sevimli bir hayvan ya da itici bir ünlünün yer aldığı homojen ve boş dijital alana sıkıştırılmıştır (ve tersi de geçerlidir) (Pettman, 2017, s. 36).” Değerli bilginin, diğer dikkat dağıtıcı ve eğlendirici içerikler arasında kaybolması, Huxley’nin “*Cesur Yeni Dünya*”sını çağrıştırmaktadır. Doğru ve nitelikli bilgi, halen internette bir yerlerdedir, ancak onlara ulaşmak zordur. Ağlardaki güç ve ağların genişlemesi kanunları tekrar karşımıza çıkmaktadır.

Ağ toplumlarında, temel iletişim türünün artan bir biçimde dolayımlanmış olması, temel sosyalleşme pratiklerinin de bu ağlar üzerinde gerçekleşmesini beraberinde getirmektedir. Bu ağlar aracılığıyla sosyalleşebilmek için bireyler, kendi varlıklarını bu ağlarda temsil edecek profiller oluşturmaktadırlar. Ağ üzerinde kimlikler oluşturmak, kimi kişisel bilgilerin bu ağlar üzerinde dolaşıma sokulmasını ya da istenildiği an erişilebilir olmasını gerektirmektedir. Bu süreç, aynı zamanda bir itibar yönetimi ve üretimini de kapsamaktadır. Ağ toplumunun en küçük birimleri olarak bireyler, dijital ağlarda kendi kimlikleri ile var olmaya, bu varlıkları üzerinden sosyalleşmeye ve itibarlarını korumaya çalışmaktadırlar. Bu durum, ağ toplumuna faturalandırılabilir bir diğer sorun olan mahremiyet sorununu gündeme getirmektedir. Üstelik bu sorun, bireylerin zorlanması ile değil sürece gönüllü katılımları ile meydana gelmektedir.

Bireyler sosyalleşebilmek için, ağ üzerinde kendi kimliklerini oluşturmaya ve kendi itibarlarını düzenlemeye zorlanmazlar. Bu durumda da mahremiyet hakkının gaspından çok, bir vazgeçişten söz edilebilir. Bireyler, arzu ettikleri kadar mahremiyeti, arzu ettikleri şekilde elde ederler. Bu değerlendirme iki açıdan sorunludur. İlk sorun, bireylerin bu sosyalleşme pratiğine, bir bakıma zorla yönlendirildiklerinin görmezden gelinmesidir. Bauman (2014), kadın ya da erkek, çocuk ya da yetişkin, fakir ya da zengin her bireyin; kendi bireysel varlıklarını tüm diğer bireylerinkiyle kıyaslamaya davet edildiğini, itildiğini ve bu kıyaslamalar için cezbedildiğini işaret eder. Benzer şekilde McGrath da (2012), “mümkün olan en fazla sayıda insanın ruh halimizi, nerede olduğumuzu, fikirlerimizi, planlarımızı ve hatta ahiretle olan ilişkimizi bilmesini sağlamanın, çoğumuz için sosyal bir gereklilik haline” geldiğini savunur. Niedzwiecki (2019) ise, bireyleri bu davranışa yönlendiren sebepleri; ruhun başka bir ruha ulaşma ve hayatın anlamını paylaşma çabası ve popüler kültürün enjekte ettiği ilgi çekme ve farkına varılma arzusu ile açıklar. Bireylerin, ağlar üzerinde kendi kişisel bilgileri ile bulunmaları, ağların dışsallığı kanunu ile açıklanabilir. Yeterince bireyin sisteme dahil olması, geride kalanların üzerinde ağ etkisi diye nitelendirilen bir baskı oluşturur. Kısacası, bireylerin bir bakıma, bu sosyalleşme formuna zorlandıkları söylenebilir. Mahremiyete ilişkin değerlendirmenin ikinci sorunu, ise bireylerin vazgeçtikleri hakkında yeterli farkındalığa sahip olmayışları ile ilgilidir.

Ağ toplumunun altyapısını oluşturan EİT’lerin, kalıcılık, yoğunluk, görünmezlik, tarafsızlık, erişilebilirlik, birleştirilebilirlik ve uzaklık özellikleri (K. S. Jones, 2003)

vazgeçilen mahremiyetin sınırlarını bulanıklaştırmaktadır. Teknolojilerin sahip olduğu bu özellikler, yukarıda bahsedilen sebeplerle mahremiyet ikinci plana itilirken görmezden gelinebilmektedir. Bireylerin, bilinçli ya da bilinçsiz olarak bıraktıkları dijital ayak izleri, bireylerin öngöremediği kadar kalıcı ve erişilebilir durumdadır. Üstelik bu ayak izlerinin önemli bir kısmını da bireyler farkında olmadan oluşturmaktadırlar. Üst veri (*metadata*) olarak adlandırılan bu veriler, bireylerin bilinçli paylaşımlarına ilişkin farkında olmadan ürettikleri verilerdir. Bir araya getirilen (birleştirilebilirlik) üst verilerin de bir içerik olduğu ve bir tablo ortaya koyduğu söylenebilir (Democracy Now, 2012). İlişkili olarak, Buchanan ve arkadaşları (2007), yeni teknolojilerin bilgi toplumunu oluşturduğunu, ancak bu “bilginin” sadece nesnelerle ilişkili olmadığını ve çoğunun insanlar hakkında, onların bilgisi ya da rızası olmadan toplanan bilgiler olduğunu söylerler. Kısacası bireyler, hizmetlere erişim, sosyalleşme ve hatta güvende hissedebilme gibi gerekçelerle mahremiyetlerinden vazgeçerlerken ağ teknolojilerinin sahip olduğu gömülü özelliklerin farkına varmayabilir ya da görmezden gelebilir. Bu farkındalık eksikliği ya da görmezden geliş, bireylerin mahremiyetine, kendi göze aldıklarından çok daha fazla zarar vermektedir.

Bardağın boş tarafına odaklanarak, ağ toplumunun katmanlı, fırsat eşitliğinden uzak ve mahremiyeti aşındıran bir sosyal organizasyon olduğunu savunmak mümkündür. Ancak, karamsarlığı bir kenara bırakıp ağ toplumu ve beraberinde getirdiği fırsatlar ön plana alındığında, daha olumlu bir bakış yakalanabilir. Ağ toplumunun bu katmanlı yapısının üstesinden gelmek, daha doğrusu, teraziye olabildiğince dengelemek ve fırsat eşitliği yaratmak için yapılması gereken, sadece ağ toplumuna katılımı arttırmak değil, katılanların da birer enformasyon seçkinine dönüşmesini sağlamaktır. Bu hedef, her şeyden önce ağ üzerinde sadece tüketmeyi değil, üretebilmeyi gerektirmektedir. Bu noktada, üzerinde durulması gereken, iç içe geçerek birbirini tamamlayan dijital vatandaşlık ve dijital okuryazarlık kavramlarıdır.

Ağ toplumuna katılanların, bu ağ üzerindeki iş yapış ve “hayatta kalma becerilerinin” artırılması ve pozisyonlarının olabildiğince enformasyon seçkinlerininine yaklaştırılması, fırsat eşitliğini sağlayabilir. Bireylerin, dijital vatandaş olabilmeleri; dili, grafik tasarımı, görüntüleri ve sesleri kullanarak mesaj oluşturma becerisini içeren multimedya iletişim becerileri edinmelerine ve bu becerileri sivil yaşama katılmak için nasıl kullanacaklarını bilmelerine bağlıdır (Hobbs, 2010). Çünkü bireyler, dijital haklarını

talep etmek ve topluma katılmak için bu becerilere ihtiyaç duymaktadır (Pangrazio & Sefton-Green, 2021). Bu bakımdan, ağ toplumuna mensup bireylerin dijital vatandaş olabilmeleri ve bu unvan için gereken dijital okuryazarlık becerilerini edinmeleri, bu toplum yapılanması içerisindeki avantajlarını arttırmak ve risklerden sakınmak için oldukça önemlidir.

Dijital vatandaşlık, düzenli ve etkin internet erişimi ile teknolojiyi kullanma becerisi gerektirir (Mossberger vd., 2012). Dijital vatandaş olabilmek ve dijital hakları talep edip koruyabilmek için, bireylerin birer dijital okuryazara dönüşmesi gerekmektedir. Dijital okuryazarlık ve onu kazanmak için gereken dijital beceriler, ağa erişimin bir sorun olmaktan çıktığı (erişim düzeyindeki dijital bölünmenin kapandığı) bir dönemde, ağ toplumunun katmanlı yapısına şekil veren temel bir değişkene dönüşmüştür. Artık toplumda görülen dijital bölünme, erişim düzeyinde değil, beceri düzeyindedir. Sosyo-ekonomik farklılıklar, kültürel ve ekonomik sermaye farklılıkları ve eşitsizlikler, artık ağa erişimde değil beceriler üzerinde belirleyici bir faktör haline gelmiştir.

Ağ toplumlarında yaşayan vatandaşların, dijital dünyada “hayatta kalmaları”, birer dijital vatandaş ve dijital okuryazar olmalarına bağlıdır. Bu sebeple, ağ toplumunun distopik tablosuna çizilen karanlık resmi aydınlatmak için, özellikle ağa yeni eklemlenen ve ağ toplumunun en kalabalık katmanını oluşturan “katılanların”, dijital okuryazarlık becerileri ile donatılması gerekmektedir. Ağa yeni katılım trendini, pozitif yönde etkileyen faktörler dikkate alındığında, dijital okuryazar olması gereken kişilerin sayısı hızla artmaktadır.

Ağ toplumuna zemin hazırlayan mikro-elektronikteki gelişmeler ve dijitalleşme gibi temeller dışında, geçtiğimiz yıllarda meydana gelen toplumsal ve teknolojik gelişmeler de ağa katılım trendini hızlandırmıştır. Bu gelişmelerden ilki, mobil internet hizmetinin yaygınlaşmasıdır. Bu hizmet, altyapı oluşturma sorunu yaşanan bölgelerin dahi ağa eklemlenmesini sağlamıştır. 2020 yılında yaşanan beklenmedik, ancak ağa katılımı etkileyen diğer gelişme de küresel boyuttaki Covid-19 salgınıdır. Salgın ekonomik, toplumsal ve psikolojik etkilerin yanında, tüm dünyada uzunca bir süre uygulanan sokağa çıkma kısıtlamaları nedeniyle ağa katılımı da arttırmıştır. Salgının ağa etkisi, sadece yeni katılımcılar kazandırması olmamıştır. Bireylerin ağ üzerinde geçirdikleri süre, harcadıkları zaman da dramatik bir şekilde artmıştır. Sadece salgın

sürecinde gerçekleşen yeni katılımların ve salgının bir bakıma mecbur bıraktığı yeni sosyalleşme yöntemlerinin bile, dijital okuryazar olmayan bireylerin mahremiyet başta olmak üzere pek çok risk ile karşı karşıya kalmasına neden olmuştur.

Ağ toplumuna entegrasyonu, kırsal bölgeler özelinde düşündüğümüzde ise ağın genişlemesinde etkili olan temel gelişme, salgından çok mobil internet teknolojisinin yaygınlaşması ve ucuzlamasıdır. Hizmet kalitesinin daha iyi olduğu kentsel alanlar ile hizmet ve altyapı yetersizliği çeken kırsal alanlar arasındaki farklılık, kırsal dijital bölünme olarak nitelendirilmektedir (Townsend vd., 2013). Mobil internet teknolojisinin yaygınlaşması, kırsal bölgelerin internet erişim olanaklarını artırmış olsa da bu bölünmeyi ortadan kaldıramamıştır (Meachem & Herald-Tribune, 2020; Vogels, 2021). Dünya genelinde, kentlerde yaşayanların internete erişim oranı yüzde 72 iken kırsal bölgelerde yaşayanların erişim oranı sadece yüzde 37'dir. Bu oranlar arasındaki fark, gelişmiş ülkelerde kapanırken gelişmekte olan ülkelerde artmaktadır (ITU, 2020c, s. 6). Halen bir kırsal ceza söz konusu olsa da kırsal bölgelerde yaşayan ve internete kentte yaşayanlara kıyasla daha yakın bir geçmişte katılan bireylerin sayısı az değildir.

Ağ toplumunun beraberinde getirdiği çelişkilerden kurtulmak için, dijital vatandaşların sayısını arttırmanın ve dijital okuryazarlık becerilerini kazanmanın önemine değinmiştik. Hizmetlere ve altyapıya olan coğrafi uzaklık ve ağa görece yeni katılımdan kaynaklı tecrübe eksiklikleri gibi faktörler dikkate alındığında, kırsal bölgelerde yaşayanlar için bu yetkinliklerin daha önemli olduğunu söyleyebiliriz. Çünkü ağ toplumunun katmanlı yapısı dikkate alındığında, halihazırda kırsal ceza ile karşı karşıya olan bu azınlığın, yeni eklemlendikleri ağ üzerinde mevcut dezavantajlı hallerini sürdürme ihtimalleri kentlerde yaşayanlara göre çok daha yüksektir. Bu sebeple, ağ toplumunu, daha demokratik bir sosyal organizasyon haline getirmek için kırsal bölgelerin de araştırma gündemlerine dahil edilmesi önemlidir.

Ağ toplumuna katılımı ve dijital okuryazarlık düzeyini, ülke özelinde ele aldığımızda, Türkiye'nin son on yıl içerisinde internete erişim sağlayan nüfusunu, yaklaşık yüzde 40 artırdığı görülmektedir. 2021 itibariyle, ülke genelindeki hanelerin yüzde 92'si internete erişebilmektedir. Bu oran, Avrupa ortalamasının altında, ancak dünya ortalamasının yaklaşık yüzde 30 üzerindedir. İnternetin topluma nüfuzunun, bu denli artmasının tek başına yeterli ve umut verici bir gösterge olmadığını tekrar

hatırlatmak gerekmektedir. Katmanlı ağ toplumunun oluşturacağı potansiyel eşitsizlikler ile mücadele için göz önünde bulundurulması gereken şey, dijital okuryazarlık düzeyleridir. Eurostat tarafından yayınlanan, dijital becerilere ilişkin istatistikler Türkiye’de internet kullanan nüfusun yaklaşık yarısının, düşük düzey dijital becerilere sahip olduğunu göstermektedir. Bu veri, internete erişimdeki artışın oluşturduğu olumlu tablodaki en büyük sorundur. Değerlendirme çerçevemizi, Türkiye’deki kırsal bölgelere ve bu bölgelerde yaşayan bireylerle sınırlarsak, bu sorun daha da anlam kazanmaktadır. Eurostat verileri, Türkiye’de kent-kır karşılaştırmasına izin vermese de diğer ülkelerin verilerine dayanarak bu bölgelerde yaşayan vatandaşların daha düşük dijital becerilere sahip olduğu çıkarımı yapılabilir.

Enformasyon ve iletişim teknolojilerine yönelik deneyimleri sınırlı olan, bu teknolojilerle yeni tanışan bireylerin, popüler kültürün enjekte ettiği ilgi çekme ve farkına varılma arzusunun da etkisi ile kendi kişisel bilgilerini daha fazla ifşa edecekleri ve mahremiyetlerini daha fazla risk altında bırakacakları iddia edilebilir. Bu bakımdan, kırsal bölgelerde yaşayan ve interneti yeni kullanmaya başlayan bireylerin, dijital okuryazarlık düzeylerinin ve “yabancıları oldukları” bu siber uzayda sosyalleşirken kendi mahremiyetlerinin, ne kadarından vazgeçebileceklerinin tespit edilmesi, sorunun boyutunu belirlemek ve çözüm için gereken politikaları geliştirmek için birinci adımdır.

Bu tez çalışması da bu ilk adımı atmak adına; kırsal bölgede yaşayan, özellikle mobil geniş bant internet hizmetinin yaygınlaşmasının etkisi ile internete katılımları artan ve internet tabanlı hizmetleri kullanmaya başlayan bireyleri merkezine almaktadır. Kayseri’nin altı farklı ilçesinde yer alan, on sekiz kırsal mahallede gerçekleştirilen bu yüz yüze anket araştırması, yukarıda yapılan değerlendirmelerin bazılarını doğrulayan ve bazı ön kabulleri yanlışlayan çıktılar sunmaktadır.

Çalışma sonucu elde edilen bulgular, ağ toplumunun katmanlı yapısı içerisinde, “dışlanan azınlıktan katılan çoğunluğa” geçiş yapan ve kırsalda bulunmanın mevcut dezavantajlarını deneyimleyen bireylerin, tecrübe eksiklikleri nedeniyle daha düşük dijital becerilere sahip oldukları ve ağa kenttekilere kıyasla daha yakın bir tarihte katıldıkları ön kabullerinin, mevcut örneklem için geçerli olduğunu göstermektedir. Ortalama olarak araştırma örnekleminin, internete ilk bağlandığı tarih 2011-2012 yıllarıdır. Bu, yaklaşık olarak, on yıllık bir internet deneyimi anlamına gelmektedir ve bu

bölgelerdeki internet kullanımının, görece yeni bir deneyim olduğunu göstermektedir. Bu öngörüü destekleyen bir diğer bulgu da örneklemin yüzde 50'den fazlasının, internete ilk olarak cep telefonu ile bağlanmış olmalarıdır. Örneklemin dijital okuryazarlık düzeyi ise, dijital okuryazarlık ölçeğinin kullanıldığı diğer araştırmalardaki ortalama düzeylerden daha düşüktür. Bu da diğer ön kabulün geçerliliğini işaret etmektedir.

Ağ toplumunun düşük dijital becerilere sahip yeni üyelerinin, bu yeni ortamda yaşayabilecekleri sorunlardan biri, mahremiyetlerinin kendi istek ve kontrollerin dışında açığa çıkmasıdır. Bu sebeple araştırmada, katılımcıların, hem sosyal medya ve internette paylaştıkları kişisel bilgiler ve kullandıkları gizlilik tercihleri hem de mahremiyet yönelimleri belirlenmiştir. Öngörülenin aksine katılımcılar, düşük dijital okuryazarlık düzeylerine rağmen hem kişisel bilgilerini daha az paylaşmaktadırlar hem de mahremiyet konusunda beklenildiğinden daha hassas ve dikkatlidirler. Mahremiyet yönelimleri ölçeğinden elde edilen dört farklı faktörün ortalaması kullanılarak yapılan kümeleme analizi, örnekleme üç kümeye ayırmıştır. Ancak en düşük ortalamalara sahip kümenin dahi mahremiyet yönelimi ortalaması, literatürdeki sonuçlardan daha yüksektir. Bu sebeple, mevcut örneklem içerisinde, “mahremiyet umursamazları” şeklinde nitelendirilebilecek bir kesimin olmadığı söylenebilir. Örneklem, mahremiyet savunucuları, bireycileri ve ılımlıları olarak üçe ayrılmıştır. Başka bir ifade ile, kırsal bölgelerde yaşayan katılımcıların mahremiyet yönelim düzeyleri, genel olarak yüksektir.

Araştırma sonucu elde edilen bulgular, örneklemin, mahremiyete yönelik endişelerinin yüksek olduğunu göstermektedir. Başka bir ifade ile Kayseri'nin kırsal mahallelerinde yaşayan katılımcıların, dijital okuryazarlık düzeyleri düşük olsa da mahremiyetleri ile ilgili duydukları endişeler, onları riskli davranışlar ve paylaşımlardan uzak tutmaktadır. İlişkili bir sonuç olarak, örneklemin yaklaşık yüzde 44'ü internetten alışveriş yapmaktadır.

Örneklemin ağ toplumuna entegrasyonunu işaret eden bir diğer çıktı ise internet kullanım sıklığının televizyondan daha fazla olmasıdır. Bu sonuç, ağ toplumuna entegrasyonda geleneksel medyadan yeni medyaya geçişin, kırsal bölgelerde de anlam kazanmaya başladığını gösteriyor olabilir.

Elde edilen bulgular incelendiğinde, örneklemin genel olarak, dijital okuryazarlık düzeylerinin düşük ve mahremiyet yönelimlerinin ise yüksek olduğunu söylemek

mümkündür. Ağ toplumunun bu yeni üyeleri arasında, cinsiyet, eğitim, yaş ve EİT kullanım sıklıkları gibi bağımsız değişkenlere göre bir farklılaşma olup olmadığını ve buna bağlı olarak farklı risk gruplarının varlığını belirlemek için yapılan analizler, dikkate değer sonuçlar ortaya koymaktadır.

Örneklem ile ilgili olarak ilk değinilmesi gereken, cinsiyet değişkeninin akıllı telefon kullanımı ile olan ilişkisidir. Araştırmaya katılacakları belirlemek için yüz yüze anket çalışmasının ilk sorusu, “akıllı telefonunuz var mı?” olarak belirlenmiş ve hayır cevabını verenler örnekleme dahil edilmemiştir. Sahada gerçekleştirilen kolayda örnekleme sırasında, bu eleyici soruya “evet” cevabını vererek araştırmaya dahil olan kadın sayısı, sadece 77’dir. Bu durum, araştırma örneklemindeki kadın-erkek dağılımını olumsuz yönde etkilemektedir. Aynı zamanda, sahada akıllı telefon kullanan kadınlara daha az rastlanmış olması, genellenemeyecek ve sadece gözleme dayalı bir bulgu olsa da Kayseri’nin kırsal mahallelerinde akıllı telefon kullanımı açısından cinsiyetler arasında bir dengesizlik olduğunu göstermektedir. Bu dengesizlik, örnekleme dahil olan kadınların, interneti, cep telefonunu ve akıllı telefonu ilk kullanmaya başladığı tarihler için de geçerlidir. Örneklemdeki kadınlar, ilk internet bağlantılarını ve cep telefonlarını, erkeklere göre yaklaşık üç yıl, ilk akıllı telefonlarını ise yaklaşık bir yıl daha geç edinmişlerdir.

Araştırmada kullanım sıklığı ölçülen uygulama ve cihazlar içerisinde, sadece anlık mesajlaşma uygulamaları (WhatsApp, Telegram vb.) kadınlar tarafından daha sık kullanılsa da aradaki fark anlamlılık ölçütlerini sağlamamaktadır. Buna karşılık, Facebook, TikTok ve E-Devlet kullanımları, cinsiyetler arasında farklılık göstermekte ve erkekler tarafından daha sık kullanılmaktadır. E-Devlet kullanımındaki 0.01 anlamlılık düzeyindeki farklılık, dijital vatandaşlık çerçevesinde değerlendirildiğinde olumsuz bir sonuçtur.

Cinsiyetin, gizlilik tercihleri ve internette bilgi paylaşımı üzerinde de bir etkisi olduğu söylenebilir. Örneklemdeki kadınların yaklaşık sadece yüzde 15’i, sosyal medya profillerini herkesin görünümüne açık bir şekilde kullanırken erkeklerde bu oran yüzde 37.8’dir. Akıllı telefonlarda şifre kullanımı ise, bu sonuçlara zıt bir şekilde erkeklerde daha fazladır. Erkeklerin yüzde 71’i, bir şifre kullanmakta ve yaklaşık yüzde 74’ü de bu şifreyi kimseyle paylaşmamaktadır. Kadınlarda ise bu oranlar sırasıyla, yaklaşık yüzde

65 ve 36'dır. İlişkili bir diğer bulgu olarak anlık mesajlaşma uygulamalarındaki son görülme ve mavi tik özelliklerinin kullanım tercihleri ise cinsiyetler arasında farklılık göstermemektedir. Bu iki özelliğin de örneklemin en az yüzde 61'i tarafından devre dışı bırakılmış olması, dikkat çeken bir sonuçtur. Katılımcılar, en son ne zaman çevrim içi olduklarının ve mesajları okuyup okumadıklarının bilgisini, kendi mahremiyet sınırları içerisinde kalması gerektiğini düşünmekte ve ayarlamalarını buna göre yapmaktadırlar.

İnternet üzerinde kişisel bilgilerin paylaşılması açısından, literatürdeki sonuçları destekleyecek şekilde, cinsiyetler arasında belirgin bir farklılığa rastlanmıştır. Katılımcılar arasında, on üç kimlik ögesinin tümünü erkekler kadınlara oranla daha çok paylaşmaktadır. Bu farklılık, sadece gerçek ad ve telefon bilgisinin paylaşımında anlamlı değildir. Örneklemdaki kadınların, internette kişisel bilgilerini paylaşmada daha temkinli davrandıkları görülmektedir.

Kadınların bu temkinli tutumlarının, kendi mahremiyet endişelerine de yansıdığı görülmektedir. Aradaki fark, istatistiksel açıdan anlamlı olmasa da kadınların kendi mahremiyetine ilişkin kaygı boyutundaki ortalamaları erkeklerden fazladır. Buna karşılık, diğer tüm boyutlarda ve ölçek genelinde, erkeklerin mahremiyet yönelimi ortalamaları kadınlardan daha yüksektir. Farklılıklar, sadece bir hak olarak mahremiyet ve başkalarının mahremiyetine ilişkin kaygı boyutlarında anlamlıdır. Mahremiyet yönelimleri ve özellikle de kendi mahremiyetine ilişkin kaygı boyutu, sadece cinsiyet değişkeninde değil, diğer tüm bağımsız değişkenlerde de farklılık göstermemektedir. Örneklemin mahremiyet yönelimleri ve kaygı düzeylerinin eğitim, cinsiyet, yaş ve gizlilik ayarlarına göre farklılık göstermemesi, bu bağımlı değişkenlerin, tüm kategoriler için benzer düzeylerde olduğunu işaret etmektedir. Başka bir ifade ile kırsal bölgelerde yaşayan katılımcıların kendi mahremiyetlerine ilişkin kaygıları, her eğitim düzeyinde, her cinsiyette ve her gizlilik tercihinde benzer yoğunluktadır.

Cinsiyet değişkeni, dijital okuryazarlık ve dijital vatandaşlık düzeyleri için de farklılık yaratan bir faktör değildir. Kadınların dijital okuryazarlık düzeyi, erkeklere kıyasla daha yüksek; dijital vatandaşlık düzeyi ise daha düşüktür. Ancak iki değişken için de aradaki fark anlamlı değildir. EİT kullanmaya başlayan kadınlar ve erkekler arasında, dijital okuryazarlık ve dijital vatandaşlık düzeyleri açısından bir farklılık yoktur. Ancak, örnekleme dahil edilen ve akıllı telefon kullandığını söyleyen kadın sayısının erkeklere

oranla çok düşük oluşu, erişim kaynaklı dijital bölünmenin, cinsiyetler arasındaki varlığının bir göstergesi olarak değerlendirilebilir. Başka bir ifade ile kırsal bölgelerde cinsiyetler arası dijital bölünme, halen birinci düzeyde geçerliliğini korumaktadır.

Araştırmada, 18-29 yaş aralığındaki katılımcılar dijital yerli; 30 ve üzeri yaşındakiler ise dijital göçmen olarak sınıflandırılmış ve bu sınıflandırmanın bağımlı değişkenler üzerindeki etkisi incelenmiştir. Bu sınıflandırma ile yapılan testler sonucunda, dijital yerli ve dijital göçmen ayrımının, cinsiyete oranla daha belirleyici bir faktör olduğunu söylemek mümkündür.

Facebook dışındaki tüm sosyal medya uygulamaları (Twitter, Instagram, TikTok, YouTube ile WhatsApp, Telegram gibi anlık mesajlaşma uygulamaları), dijital yerliler tarafından daha sık kullanılmaktadır. Kamu hizmeti uygulamaları açısından iki kategori arasında, anlamlı bir farklılık gözlenmemesi, yaş faktörüne bakılmaksızın herkesin E-Devlet, Hayat Eve Sığar ve MHRS gibi uygulamaları benzer sıklıklarda kullandığını göstermektedir. İlk kullanıcılarını üniversite öğrencilerinin oluşturduğu Facebook'un, artık dijital yerliler tarafından daha az kullanıldığı ve dijital göçmenlerin bu sosyal medya aracını daha sık kullandığı görülmektedir, ancak farklılık anlamlı değildir. Kullanım sıklıkları ile ilgili en dikkat çekici sonuç, geleneksel medya araçlarından televizyonun, dijital göçmenler tarafından çok daha sık kullanılmasıdır ($p<.001$). Bu bulgu, dijital göçmenlerin, interneti kullanmaya başlasalar da halen geleneksel medya araçlarını daha yoğun kullandıklarının bir göstergesidir. Bilgisayar kullanımı, her iki kategoride de oldukça düşüktür. Buna rağmen dijital yerliler, bilgisayarı, dijital göçmenlere göre daha fazla kullanmaktadırlar. Benzer şekilde, dijital yerlilerin internet ve cep telefonu kullanımları da daha yüksektir.

Literatürdeki araştırmalarda, yaşlıların gençlere göre mahremiyetlerini daha fazla önemsedikleri ve mahremiyetlerini korumak için daha çok önlem aldıkları gözlemlenmektedir. Ancak bu araştırmanın örneklemi özelinde, dijital yerlilerin, gizlilik ayarları konusunda, dijital göçmenlere kıyasla daha temkinli olduğu görülmektedir. Dijital yerlilerin yaklaşık yüzde 68'i, sosyal medya hesaplarını sadece arkadaşlarının erişimine açarken dörtte biri herkese açık bir şekilde kullanmaktadır. Dijital göçmenlerde ise bu oranlar sırasıyla; yaklaşık yüzde 43 ve 42'dir. Anlık mesajlaşma uygulamalarında bulunan özelliklerin kullanımlarındaki farklılıklar da istatistiksel olarak anlamlıdır. Her

ne kadar dijital yerliler, her iki özelliği de dijital göçmenlere kıyasla daha fazla kullandıklarını söyleseler de dijital göçmenlerin en az yüzde 27'si, bu özellikleri bilmediklerini ifade etmişlerdir. Bu özelliklerin varsayılan olarak açık olduğu dikkate alındığında, dijital göçmenlerin bu özellikleri daha sık kullandığı görülmektedir. Bu iki bulguyla paralel şekilde hem akıllı telefonlarda şifre kullanımı hem de bu şifreyi kimseyle paylaşmama tercihi, dijital yerlilerde daha yüksektir. Dijital göçmenlerin, akıllı telefonlarında daha az şifre kullanıyor oluşu ve bu şifreyi daha fazla paylaşma eğiliminde olmaları, Petronio'nun İMY teorisine atıfta bulunarak teorik bir zemine oturtulabilir. Bu teori, giderek artan güvenlik ihtiyaçları, finansal meselelerini yönetecek ve sağlık sorunları ile ilgilenecek birisine ya da birilerine ihtiyaç duymaları neticesinde, yaşlıların mahremiyet sınırlarının daralacağını varsaymaktadır.

İnternette kişisel bilgilerin paylaşılması konusunda, ölçülen on üç kimlik ögesinin sekizi için, dijital yerli ve dijital göçmenler arasında anlamlı bir farklılık söz konusu değildir. Gerçek ad, e-posta adresi, cinsiyet ve fotoğraflar dijital yerliler tarafından, ilişki durumu ise dijital göçmenler tarafından daha sık paylaşılmaktadır. Her ne kadar dijital yerlilerin internette daha fazla kişisel bilgi paylaştığı görülse de gizlilik ayarları konusundaki tutumları nedeniyle, örneklem içerisindeki dijital yerlilerin daha temkinli olduğu söylenebilir. Aradaki fark istatistiksel olarak anlamlı olmasa da dijital göçmenlerin telefon bilgilerini, dijital yerlilere göre daha fazla paylaşıyor olmaları, dijital göçmenlerin daha riskli bir kullanım sergilediklerini göstermektedir.

Dijital yerli ve dijital göçmenler arasındaki gizlilik tercihleri ve internette kişisel bilgi paylaşımlarına ilişkin bu farklılıklar, mahremiyet yönelimleri boyutlarına yansımamıştır. Ölçeğin dört boyutunda da iki kategori arasında anlamlı bir farklılık görülmezken sadece ölçek genelinde oldukça düşük düzeyde bir farklılık görülmektedir. Tüm boyutlarda ve ölçek ortalamasında, dijital göçmenlerin ortalamaları daha yüksektir. Dijital göçmenlerin mahremiyete ilişkin davranışları (gizlilik tercihleri) ile tutumları arasında bir tutarsızlık olduğu söylenebilir. Bu durum, literatürde mahremiyet paradoksu olarak anılmaktadır.

Çalışma örneklemini içerisinde, yaşın mahremiyet yönelimleri üzerindeki etkisini keşfetmek için, dijital göçmen ve dijital yerli ayrımının yeterli olmadığı görülmüştür. Bu durum, dijital yerlilerin de artık 30 yaşına dayanmış olmalarından kaynaklanıyor olabilir.

Bu ayrımın, geçen her yıl ayrımını yitireceği söylenebilir. Bu sebeple, örnekleme yedi farklı yaş grubuna bölerek yapılan karşılaştırmalar, her mahremiyet yönelimi boyutunda istatistiksel açıdan anlamlı farklılıkların olduğunu göstermiştir.

Dijital okuryazarlık ve dijital vatandaşlık düzeyleri, dijital yerli ve dijital göçmenler arasında yüksek anlamlılık düzeyinde farklılaşmaktadır. Tahmin edilen ve literatürde, hayatlarının daha erken bir döneminde teknolojiler ile tanışmaları ile açıklanan bir sonuç olarak, dijital yerlilerin hem dijital okuryazarlık hem de dijital vatandaşlık düzeyleri, göçmenlere göre oldukça yüksektir. Bu sonucu doğrulayan bir diğer bulgu da yaş ile dijital okuryazarlık düzeyi arasındaki negatif yönlü korelasyondur.

Araştırmadaki bağımsız değişkenlerden olan eğitim düzeyi, mahremiyet yöneliminin üç boyutu içerisinde, anlamlı bir şekilde farklılaşmaktadır. Kendi mahremiyetine ilişkin kaygı boyutunda bir farklılaşma görülmemesi ve başkasının mahremiyetine ilişkin kaygı boyutundaki farklılığında düşük düzeyde olması, örneklem içerisinde mahremiyete ilişkin kaygıların, her grup için eşit düzeyde seyrettiğini göstermektedir. Konu dijital okuryazarlık ve dijital vatandaşlık olduğunda ise, eğitim düzeyi çok daha güçlü bir farklılaştırıcı faktördür.

Literatürdeki, bireylerin sahip olduğu çevrim içi deneyimleri ne kadar fazla olursa olası gizlilik tehditleri hakkında daha fazla bilgi sahibi olacakları ve kendilerini korumak için nasıl hareket edeceklerini daha fazla bileceklerine ilişkin sonuçlara paralel olarak, internet ile daha erken bir tarihte tanışan, ilk cep telefonunu ve ilk akıllı telefonunu daha erken edinenler, mahremiyet konusunda daha hassastır. EİT'leri edinme tarihleri ile dört mahremiyet boyutu arasında da negatif yönlü bir korelasyona rastlanmıştır. Çevrim içi deneyime ilişkin olarak sosyal medya uygulamaları ve EİT kullanım sıklıkları da genel olarak (kendi mahremiyetine ilişkin kaygı boyutu dışında) mahremiyet yönelimleri ile ilişkilidir. Bu ilişkilerin çoğu, pozitif yönlü iken anlık mesajlaşma uygulaması kullanım sıklığı ile mahremiyet yönelim boyutları arasında, negatif yönde güçlü bir ilişki vardır. Başka bir ifade ile bu uygulamalardaki kullanım artışı, mahremiyet yönelimlerini olumsuz yönde etkilemektedir.

EİT maruziyet sürelerinin, dijital okuryazarlık ve dijital vatandaşlık düzeyleri üzerinde de açıklayıcı bir etkisi olduğu söylenebilir. Katılımcılar, internete ne kadar erken bağlandılarsa ve akıllı telefonlarını ne kadar erken edindilerse dijital okuryazarlık

düzeyleri de o kadar yüksektir. Bu etki, katılımcıların EİT ve uygulama kullanım sıklıklarında da görülmektedir. Korelasyon analizlerinde en çok dikkat çeken sonuç, dijital okuryazarlık düzeyi ile diğer tüm cihaz ve uygulama kullanımları arasında pozitif yönlü bir korelasyon söz konusu iken televizyon kullanım sıklığı ile negatif yönlü bir korelasyon gözlemlenmesidir. Bu, düşük dijital okuryazarlık düzeyine sahip katılımcıların, halen televizyonu temel medya tüketim aracı olarak tercih ettiklerini göstermektedir.

Çalışmanın çıktıları, dijital okuryazarlık ya da dijital vatandaşlık düzeyi yüksekliğinin, mahremiyet yönelimi boyutlarına da yansıdığını göstermektedir. Kendi mahremiyetine ilişkin kaygı boyutu dışındaki üç mahremiyet yönelimi boyutu da bu düzeylerle güçlü bir korelasyon göstermektedir. Daha açık ifade etmek gerekirse, bir katılımcının, dijital okuryazarlık düzeyinin yüksek olması, onun mahremiyet yöneliminin de daha yüksek olacağını göstermektedir. Mahremiyet yönelimi alt boyutları arasında da en yüksek dijital okuryazarlık düzeyine sahip olanlar, “mahremiyet savunucuları” kümesidir. Bu sonucu değerlendirerek, bireylerin dijital okuryazarlık düzeylerini yükseltecek çalışmaların, onları ağ toplumunun mahremiyete yönelik risklerine karşı daha farkında ve temkinli hale getireceği söylenebilir. Dijital okuryazarlık düzeyi düşük olan katılımcıların, internetten alışveriş yapmayı tercih etmemesi de çalışmada elde edilen olumlu bir sonuçtur. Bu tercih, dijital okuryazarlığı düşük olan katılımcıların, çevrim içi dolandırıcılık riskleri ile karşılaşma ihtimallerini azaltmaktadır. Çünkü yeterli bilgi ve beceriye sahip olmayan bireyler, internetten alışveriş yaptıklarında kolaylıkla kandırılabilir ve dolandırılabilirler.

Bu tez çalışmasının saha araştırması sürecinin, yaklaşık bir yıl ertelenmesine ve sadece yüz yüze uygulanan anketlerden elde edilen verilerle sınırlanmasına neden olan Covid-19 salgını, katılımcıların sosyal medya ve kamu hizmeti uygulamaları ve cihaz ya da teknoloji kullanımlarını da etkilemiştir. Araştırma katılımcılarının yüzde 58’i, interneti ve yaklaşık yüzde 54’ü de cep telefonlarını, salgın sonrasında daha fazla kullanmaya başlamışlardır. Salgında kullanımı en çok artan sosyal medya uygulamaları ise, TikTok ve Instagram olmuştur. TikTok uygulamasının kullanıcı sayısı, salgın sürecinde dünya genelinde bir artış göstermiştir ve bu artış, kırsal bölgelerdeki kullanıcılarda da gözlemlenmektedir.

Tüm bulgular bir arada değerlendirildiğinde, örnekleme oluşturan 374 kişinin, internet ile olan tanışıklığının, büyük oranda son on yıl içerisinde gerçekleştiği, yüzde 53'ünün ilk internet bağlantılarını bir cep telefonu ile sağladığı görülmektedir. Ağ toplumuna katılımlarının, kent merkezlerinde yaşayanlara oranla daha yeni olduğu ve dijital okuryazarlık düzeylerinin düşük olduğu görülmektedir. Ağ üzerinde en kolay karşı karşıya kalabilecekleri risk olan mahremiyet kaybı ve kişisel bilgilerin açığa çıkması sorunu ile ilgili katılımcıların, beklenenden daha temkinli oldukları görülmektedir. Ancak özellikle eğitim düzeyi düşük dijital göçmenlerin, diğer gruplara göre daha risk altında oldukları anlaşılmaktadır. Dijital okuryazarlık ve dijital vatandaşlık ölçeklerinin maddeleri teker teker incelendiğinde, katılımcıların internetten bilgiye erişmekte ve internet aracılığıyla iletişim kurmakta kendilerine güvendikleri, ancak kendi içerik ve bilgilerini üretmede daha çekingen kaldıkları görülmektedir. Bu durum, örneklemin ağ toplumuna tam entegrasyonu önünde bir engel olarak yorumlanabilir. Örnekleme, dijital ihtiyaçlar hiyerarşisinin ilk birkaç basamağını kısmen sağlasa da dijital üretim konusunda sıkıntı çekmektedir.

Literatürdeki araştırmalar, istatistikler ve bu araştırmadan elde edilen sonuçlar göz önünde bulundurularak hem gelecek araştırmacılar hem de politika yapıcılar için bazı öneriler sunulabilir.

- Türkiye, ağ toplumuna entegrasyonun ilk adımı olan internete erişimi önemli ölçüde sağlamıştır. Buradan sonra yapılması gereken, ağ toplumuna katılan vatandaşların, dijital okuryazarlık düzeylerinin yükseltilmesi ve birer enformasyon seçkinine dönüştürülmesidir. Yukarıdaki istatistik, grafik ve tablolarda gösterilen verilerin de işaret ettiği gibi, beceri temelli dijital bölünmeyi çözecek politikalara ihtiyaç duyulmaktadır. Bu politikalar, öncelikli olarak eğitim seviyesi düşük dijital göçmenleri, daha sonra kırsal bölgede yaşayan vatandaşları ve son olarak da tüm nüfusu kapsamalıdır.

- Özellikle kırsal bölgelerde yaşayan ve cep telefonu hatlarını (SIM kartlarını) bir akıllı telefona ilk defa takan, ilk kez internet paketi alan/açtıran ve/veya ilk defa cep telefonu hattı alan vatandaşlara, dijital okuryazarlık beceri ve farkındalıklarını arttırıcı ve bilgilendirici doküman veya içerik sağlanmalıdır.

- Öncelikli olarak kırsal bölgelerde ve daha sonra da tüm nüfus için, bilgisayar kullanımının yaygınlaştırılması gerekmektedir. Çünkü bilgisayar, bir bakıma ağ toplumu

içerisindeki temel dijital üretim aracıdır. Bilgisayar kullanımı, ağ toplumunda istihdam edilmeyi de kolaylaştırmaktadır. Akıllı telefon ve tablet gibi cihazlar da dijital üretime izin verse de nitelikli dijital içerikler için bilgisayar kullanımı zorunludur.

- İnternette alışveriş yapmak, özellikle şehir merkezlerinden uzakta olan kırsal bölgeler için coğrafi kimi dezavantajları kapatabilir. Örneğin kent merkezinde yaşayan biri, bir tekstil markasının alışveriş merkezindeki mağazasına giderek istediği ürüne kolayca erişebilir ve isterse aynı ürünü, aynı fiyata, o markanın internet sitesinden de sipariş edebilir. Kırsal bölgelerde yaşayanlar için, ilk alternatif oldukça masraflı olacaktır. İkinci alternatif, bu vatandaşlar için bir fırsattır. Bu sebeple, kırsal bölgelerde internette alışverişin yaygınlaştırılması için çeşitli eğitimler ve bilgilendirme toplantıları düzenlenmelidir. Analiz sonuçları, dijital okuryazarlık düzeyi düşük olanların internette alışveriş yapmadığını göstermektedir. Bu çıktıdan hareketle, dijital okuryazar olmayan bireylere öncelik verilmelidir.

- Dijital okuryazarlık düzeyinin yükseltilmesi ve dijital vatandaşlık bilincinin kazandırılması için, özellikle kırsal bölgelerdeki ve daha sonra tüm ülkedeki ilkokullarda, dijital vatandaşlık ve dijital okuryazarlık derslerinin müfredata eklenmesi nitelikli bir gelişme sağlayabilir. Bu sebeple, ilkokul müfredatlarında, bu kapsamda bir düzenleme yapılması önerilmektedir. Dijital teknolojilerin sürekli geliştiği göz önüne alındığında, bu teknolojiler ile ilgili yetkinlik oluşturma sürecinin hem evde hem okulda, örgün ve yaygın eğitim ortamlarında erken çocukluk döneminden itibaren başlaması gereken yaşam boyu bir süreç (Richardson & Milovidov, 2019) olduğu dikkate alındığında, bu derslerin içeriklerinin de düzenli olarak güncellenmesi gerekmektedir.

- Araştırma evreninden kolayda örnekleme ile seçilen katılımcılar arasında, kadın katılımcıların sayısının azlığı dikkat çekmektedir. Bu durum, ilgili evren içerisinde, akıllı telefon kullanan kadın sayısının erkeklere oranla az olduğuna bir işaret olarak değerlendirilebilir. Bu sebeple hem cinsiyet eşitliğini sağlamak hem de kadınların da ağ toplumuna entegrasyonunda ilk adımı atmak için, kırsal bölgelerde yaşayan kadınların da akıllı telefon kullanımına yönlendirecek çalışmalar yapılabilir. Kırsal bölgelerde yapılan başka bir araştırma, sosyal ağ sitesi kullanımlarının, kadınlara çeşitli ilgi alanlarına bağlı sosyal katılım fırsatları verdiğini ve sosyal ağların kadınları topluluklarının kültürel ve sosyal yaşamına katılmaya teşvik ettiğini göstermektedir (Vega Caro vd., 2015). Sosyal

katılımlarına faydasının yanında, ebeveynlerin EİT kullanıcısı olmasının, yetiştirecekleri çocukların dijital dünyadaki pozisyonları üzerinde de etkisi bulunmaktadır.

- Korelasyon analizleri, daha sık televizyon izleyenlerin daha düşük dijital okuryazarlık düzeylerine sahip olduklarını göstermektedir. Bu sonuç, dijital okuryazarlık düzeyi düşük vatandaşlara ulaşmak ve onların dijital becerilerini ve dijital vatandaşlık konusundaki farkındalıklarını arttırmak için, televizyonun kullanılmasının verimli olacağını göstermektedir. Bu sebeple, televizyonlarda prime time saatlerinde yayınlanacak dijital okuryazarlık ve dijital vatandaşlık ile ilişkili kamu spotları ya da belgeseller çekilmelidir.

- Araştırmada mahremiyet yönelimleri ve dijital okuryazarlık düzeyleri ile ilgili ölçekler yardımı ile çeşitli nicel veriler toplanmıştır. Özellikle mahremiyet konusunun sahip olduğu derinlik, sadece nicel verilere dayanarak bir çıkarımda bulunmayı güçleştirmektedir. Bu sebeple daha sonraki araştırmacılara, mahremiyet konusu ile ilgili ölçekleri, odak grup ya da derinlemesine mülakatlarla desteklemeleri ve nicel yöntemlerle bütünleşik olarak nitel bir araştırma modeli kurgulamaları önerilmektedir.

- Araştırmada, kişisel beyan (*self-report*) yöntemi ile ve çoğunlukla beşli likert ölçeğinde veri toplanmıştır. Saha araştırması süreci, kentlerde yaşayan veya üniversitede okuyan örneklemelerden farklı bir sosyo-ekonomik konumda olan, kırsal bölge nüfusu için bir ifadeye belirli bir oranda katılma ve katılmamanın alışık olmadıkları bir pratik olduğu görülmüştür. Bu sebeple gelecekte, kırsal bölgelerde ya da düşük eğitim düzeyine sahip bir örnekleme yapılacak araştırmalarda, evet-hayır soruları ya da bilgilerini test edecek doğru-yanlış soruları yöneltilerek bir ölçüm yapılması önerilebilir.

- Araştırmada, katılımcıların internette paylaştıkları bilgiler, yine kişisel beyan ile toplanmıştır. Bu verileri doğrulamak ve daha net bir tablo elde etmek için gelecek araştırmalarda gerekli tüm etik kurul izinleri ve kişisel rıza beyanları alınarak katılımcıların doğrudan sosyal ağ profilinin incelenmesi, daha geçerli sonuçlar sağlayabilir.

- Dijital okuryazarlık gibi, dijital tecrübe ve bilgiye dayanan bir değişkenin de kişisel beyan yerine bilgi testleri ya da doğrudan laboratuvar ortamında uygulamalı olarak değerlendirilmesi, daha net ve bireyin kendisini değerlendirirken adil olamaması gibi sorunlardan (*Dunning-Kruger effect*) arındırılmış bir sonuç çıkaracaktır.

Altında yatan teknoloji mahremiyeti korumaya değil, “bilgileri transfer etme” prensibine dayanan internette (Fischer-Hübner, 1998; Garfinkel & Spafford, 2002) artık geleneksel olarak kabul ettiğimiz mahremiyet kuralları, yavaş yavaş geçerliliğini yitirmekte ve daha önce çizdiğimiz mahremiyet sınırları, her geçen gün daha da silikleşmektedir. Altında yatan tasarım prensibi, bilginin dolaşımı ve depolanmasına dayandığı için bu sonucun uygulamanın doğasında var olduğu söylenebilir. 1890 yılında tartışılan mahremiyet, fotoğraf ve magazin basınının verdiği zarara odaklanmaktadır. Şimdiki süreç ile karşılaştırıldığında ise bu zarar, ufacık bir kum tanesidir. Sadece bu bile, mahremiyet yönelimlerimizde bir dönüşüm olduğunu göstermektedir. Yeni neslin internete yönelik tutum ve davranışları gözlemlendiğinde ise tablo daha da netleşmektedir. Özellikle 2010 sonrası doğan nesil, YouTube videoları ile büyümekte ve bu mecraya içerik üretmeye özenmektedir. Niedzwiecki’nin söylediği gibi, kişisel alanlarımızı ve anlarımızı böylesine paylaşmamızda, popüler kültürün etkisi barizdir. Belki de gelecek nesiller, farklı bir yakınlık kurma pratiği geliştirecekler ve şu an yakınlık kurmak için sadece yakınlarımızla paylaştığımız özel alanları, herkesin erişimine açık tutmayı normalleştirecektir. Yine de, yapılması gereken, Gilster’in (1997) ifade ettiği gibi, dijital okuryazar olarak sadece tuş vuruşlarında (*keystrokes*) değil, fikirlerde ustalaşmak; uyanık, dikkatli ve ihtiyatlı olmayı (*wariness*) elden bırakmamaktır. Hem kendimiz hem de yetiştireceğimiz kuşaklar için...

KAYNAKÇA

- Acquisti, A. (2010). Joint wpisp-wpie roundtable: The economics of personal data and privacy: 30 years after the oecd privacy guidelines. *The Economics of Personal Data and the Economics of Privacy*, 24.
- Acquisti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the facebook. İçinde G. Danezis & P. Golle (Ed.), *Privacy Enhancing Technologies* (C. 4258, ss. 36-58). Springer Berlin Heidelberg. https://doi.org/10.1007/11957454_3
- Acquisti, A., & Gross, R. (2009). Predicting social security numbers from public data. *Proceedings of the National Academy of Sciences*, 106(27), 10975-10980. <https://doi.org/10.1073/pnas.0904891106>
- Ainley, J., Fraillon, J., Freeman, C., & Ministerial Council for Education, Early Childhood Development and Youth Affairs (MCEECDYA). (2010). *National assessment program: ICT literacy years 6 & 10* (Sy 2008; National Assessment Program). Ministerial Council for Education, Early Childhood Development and Youth Affairs. https://www.nap.edu.au/_resources/2008_nap_ictl_public_report.pdf
- Akdeniz, Y., Taylor, N. W., & Walker, C. (2001). Bigbrother.gov.uk: State surveillance in the age of information and rights. *Criminal Law Review*, February, 73-90. <https://doi.org/10.2139/ssrn.3181278>
- Akhvlediani, T. (2021). *Digital literacy in times of the covid-19 in the eastern partnership countries* [EaP CSF COVID-19 Policy Paper]. Eastern Partnership Civil Society Forum. <https://eufordigital.eu/library/digital-literacy-in-times-of-covid-19-in-the-eap-countries/>
- Akikol, R. (2018). Kadın dijital göçmenlerin facebook kullanımı ve mahremiyet ilişkisi. *Connectist: Istanbul University Journal of Communication Sciences*, 54, 1-36.
- Alakurt, T. (2017). Adaptation of online privacy concern scale into turkish culture. *Pegem Eğitim ve Öğretim Dergisi*, 7(4), 611-636. <https://doi.org/10.14527/pegegog.2017.022>

- Alberta Education. (2012). *Digital citizenship policy development guide*. School Technology Branch. <http://education.alberta.ca/admin/technology.aspx>
- Alfred, D. N. K. (2014). *Online privacy issues: Awareness, attitudes and perceptions amongst internet users in egypt* [Yüksek Lisans Tezi]. The American University in Cairo.
- Alkeinay, N. Y., & Norwawi, N. Md. (2014). User oriented privacy model for social networks. *Procedia - Social and Behavioral Sciences*, 129, 191-197. <https://doi.org/10.1016/j.sbspro.2014.03.666>
- Altman, I. (1976). Privacy: A conceptual analysis. *Environment and Behavior*, 8(1), 141-141. <https://doi.org/10.1177/001391657600800108>
- Altman, I. (1977). Privacy regulation: Culturally universal or culturally specific? *Journal of Social Issues*, 33(3), 66-84. <https://doi.org/10.1111/j.1540-4560.1977.tb01883.x>
- Altman, I., Vinsel, A., & Brown, B. B. (1981). Dialectic conceptions in social psychology: An application to social penetration and privacy regulation. İçinde *Advances in Experimental Social Psychology* (C. 14, ss. 107-160). Elsevier. [https://doi.org/10.1016/S0065-2601\(08\)60371-8](https://doi.org/10.1016/S0065-2601(08)60371-8)
- Andrejevic, M., & Burdon, M. (2015). Defining the sensor society. *Television & New Media*, 16(1), 19-36. <https://doi.org/10.1177/1527476414541552>
- Angwin, J. (2015). *Dragnet nation: A quest for privacy, security, and freedom in a world of relentless surveillance*.
- Antón, A. I., Earp, J. B., & Young, J. D. (2010). How internet users' privacy concerns have evolved since 2002. *IEEE Security and Privacy*, 8(1), 21-27. <https://doi.org/10.1109/MSP.2010.38>
- Arfaa, J., & Wang, Y. (2016). Elder adults utilizing social networking sites on mobile platforms. İçinde J. Zhou & G. Salvendy (Ed.), *Human Aspects of IT for the Aged Population. Healthy and Active Aging* (C. 9755, ss. 167-175). Springer International Publishing. https://doi.org/10.1007/978-3-319-39949-2_16
- Aufderheide, P. (1993). *Media literacy: A report of the National Leadership Conference on Media Literacy* (1. bs). The Aspen Institute.

- Austin, L. (2003). Privacy and the question of technology. *Law and Philosophy*, 22(2), 119-166.
- Australian Council for Educational Research. (2016). *A global measure of digital and ICT literacy skills* (ED/GEMR/MRT/2016/P1/4; Global Education Monitoring Report). United Nations.
- Avrupa Birliği Türkiye Delegasyonu. (2012). *Avrupa birliği temel haklar bildirgesi*. <https://www.avrupa.info.tr/tr/avrupa-birligi-temel-haklar-bildirgesi-708>
- Aybay, R. (2006). *Açıklamalı insan hakları evrensel bildirisi*. Türkiye Barolar Birliği.
- Aydın, A. E. (2018). *Gözetim toplumunda tüketici: Tüketici mahremiyeti üzerine bir araştırma* [Doktora Tezi]. Muğla Sıtkı Koçman Üniversitesi Sosyal Bilimler Enstitüsü.
- Balcı, Ş., Bal, E., & Delal, Ö. (2019). Instagram kullanım alışkanlıkları ve motivasyonları ile narsisizm arasında bir bağlantı var mı? Üniversite gençliği araştırması. *Erciyes İletişim Dergisi*, 6(2), 955-974. <https://doi.org/10.17680/erciyesiletisim.543430>
- Ball, K., Haggerty, K. D., & Lyon, D. (Ed.). (2012). *Routledge handbook of surveillance studies*. Routledge.
- Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday*, 11(9). <https://doi.org/10.5210/fm.v11i9.1394>
- Baruh, L., Bal, H. M., & Cemalcılar, Z. (2015). A multidimensional privacy orientation scale: Development and validation with turkish twitter users. İçinde B. Akdenizli (Ed.), *Digital transformations in Turkey: Current perspectives in communication studies* (ss. 3-20). Lexington Books.
- Baruh, L., & Cemalcılar, Z. (2014). It is more than personal: Development and validation of a multidimensional privacy orientation scale. *Personality and Individual Differences*, 70, 165-170. <https://doi.org/10.1016/j.paid.2014.06.042>
- Baruh, L., Secinti, E., & Cemalcılar, Z. (2017). Online privacy concerns and privacy management: A meta-analytical review: privacy concerns meta-analysis. *Journal of Communication*, 67(1), 26-53. <https://doi.org/10.1111/jcom.12276>
- Bauer, A. T., & Mohseni Ahooei, E. (2018). Rearticulating internet literacy. *Journal of Cyberspace Studies*, 2(1). <https://doi.org/10.22059/jcss.2018.245833.1012>

- Bauman, Z. (2014). *Modernite, kapitalizm, sosyalizm: Küresel çağda sosyal eşitsizlik* (F. D. Ergun, Çev.; 2. bs). Say.
- Bauman, Z., & Lyon, D. (2013). *Akışkan gözetim* (E. Yılmaz, Çev.; 1. bs). Ayrıntı Yayınları.
- Bawden, D. (2001). Information and digital literacies: A review of concepts. *Journal of Documentation*, 57(2), 218-259. <https://doi.org/10.1108/EUM0000000007083>
- Bay, D. N. (2021). Okul öncesi öğretmen adaylarının dijital okuryazarlık düzeyleri. *Mustafa Kemal Üniversitesi Eğitim Fakültesi Dergisi*, 5(7), 172-187.
- Benassi, M., Garofalo, S., Ambrosini, F., Sant'Angelo, R. P., Raggini, R., De Paoli, G., Ravani, C., Giovagnoli, S., Orsoni, M., & Piraccini, G. (2020). Using two-step cluster analysis and latent class cluster analysis to classify the cognitive heterogeneity of cross-diagnostic psychiatric inpatients. *Frontiers in Psychology*, 11, 1085. <https://doi.org/10.3389/fpsyg.2020.01085>
- Bennett, W. L. (2008). Changing citizenship in the digital age. İçinde W. L. Bennett (Ed.), *Civic Life Online: Learning How Digital Media Can Engage Youth* (ss. 1-24). The MIT Press.
- Bentham, J. (1969). *A bentham reader* (M. P. Mack, Ed.). Pegasus.
- Bentham, J., Watkin, C. P., & Werret, S. (2016). *Panoptikon: Gözün iktidarı* (B. Çoban & Z. Özarslan, Ed.; 2. bs). Su Yayınları.
- Berkup, S. B. (2015). *Sosyal ağlarda bireysel mahremiyet paylaşımı: X ve y kuşakları arasında karşılaştırmalı bir analiz* [Doktora Tezi]. Ege Üniversitesi Sosyal Bilimler Enstitüsü.
- Bigo, D. (2008). Globalized (in)security: The field and the ban-opticon. İçinde *Terror, insecurity and liberty: Illiberal practices of liberal regimes after 9/11* (ss. 10-48). Routledge.
- Binark, M., Arun, Ö., Özsoy, D., Kandemir, B., & Şahinkaya, G. (2020). *Covid-19 sürecinde yaşlıların enformasyon arayışı ve enformasyon değerlendirmesi: TÜBİTAK SOBAG 120K613 no'lu araştırma projesi*. Yaşlanma Çalışmaları Derneği Yayınları. http://www.senex.org.tr/wp-content/uploads/Covid19_SenexKitap.pdf

- Botan, C. (1996). Communication work and electronic surveillance: A model for predicting panoptic effects. *Communication Monographs*, 63(4), 293-313. <https://doi.org/10.1080/03637759609376396>
- Boyd, D. (2008). Why youth heart social network sites: The role of networked publics in teenage social life. İçinde D. Buckingham (Ed.), *Youth, Identity, and Digital Media* (ss. 119-142). The MIT Press. <https://doi.org/10.31219/osf.io/22hq2>
- Boyd, D., & Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication*, 13(1), 210-230. <https://doi.org/10.1111/j.1083-6101.2007.00393.x>
- Boyd, D., & Heer, J. (2006). Profiles as conversation: Networked identity performance on friendster. *Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06)*, 59c-59c. <https://doi.org/10.1109/HICSS.2006.394>
- Boyne, R. (2000). Post-panopticism. *Economy and Society*, 29(2), 285-307. <https://doi.org/10.1080/030851400360505>
- Brandtzæg, P. B., & Lüders, M. (2009). *Privacy 2.0: Personal and consumer protection in the new media reality* (Sy A12979; s. 86). The Norwegian Consumer Council.
- Brandtzæg, P. B., Lüders, M., & Skjetne, J. H. (2010). Too many facebook “friends”? Content sharing and sociability versus the need for privacy in social network sites. *International Journal of Human-Computer Interaction*, 26(11-12), 1006-1030. <https://doi.org/10.1080/10447318.2010.516719>
- Broadband Commission for Sustainable Development. (2017). *Working group on education: Digital skills for life and work 2017* (s. 128). <https://broadbandcommission.org/publication/digital-skills-for-life-and-work/>
- Bruno, F. (2012). Surveillance and participation on Web 2.0. İçinde *Routledge Handbook of Surveillance Studies*. Routledge. https://doi.org/10.4324/9780203814949.ch3_5_b
- BT Bilgi Teknolojileri. (2018, Şubat 12). General data protection regulation (GDPR) ve 6698 sayılı kişisel verilerin korunması kanunu (KVKK). *BT Bilgi Teknolojileri*. <https://btbilgi.com.tr/kvkk-ve-gdpr/general-data-protection-regulation-gdpr-6698-sayili-kisisel-verilerin-korunmasi-kanunu-kvkk/>

- BTK. (2013). *Elektronik haberleşme sektörüne ilişkin il bazında yıllık istatistik bülteni 2013*. Bilgi Teknolojileri ve İletişim Kurumu. <https://www.btk.gov.tr/uploads/pages/slug/ehsyib-2007-2012.pdf>
- BTK. (2014). *Elektronik haberleşme sektörüne ilişkin il bazında yıllık istatistik bülteni 2014*. Bilgi Teknolojileri ve İletişim Kurumu. <https://www.btk.gov.tr/uploads/pages/slug/ehsyib-2008-2013.pdf>
- BTK. (2015). *Elektronik haberleşme sektörüne ilişkin il bazında yıllık istatistik bülteni 2015*. Bilgi Teknolojileri ve İletişim Kurumu. <https://www.btk.gov.tr/uploads/pages/slug/ehsyib-2009-2014.pdf>
- BTK. (2021). *Elektronik haberleşme sektörüne ilişkin il bazında yıllık istatistik bülteni 2021*. Bilgi Teknolojileri ve İletişim Kurumu. <https://www.btk.gov.tr/uploads/pages/yillik-il-istatistikleri/elektronik-haberlesme-sektorune-iliskin-il-bazinda-yillik-istatistik-bulteni.pdf>
- Buchanan, T., Paine, C., Joinson, A. N., & Reips, U.-D. (2007). Development of measures of online privacy concern and protection for use on the Internet. *Journal of the American Society for Information Science and Technology*, 58(2), 157-165. <https://doi.org/10.1002/asi.20459>
- Buckingham, D. (2015). Defining digital literacy. *Nordic Journal of Digital Literacy*, 2006-2016, 21-34. https://doi.org/10.1007/978-3-531-92133-4_4
- Budak, H. (2016). *Yeni çağ yeni medya ve mahremiyetin yeni sınırları* [Doktora Tezi]. Selçuk Üniversitesi Sosyal Bilimler Enstitüsü.
- Budak, H. (2018). Sosyal medya iletişiminde mahremiyetin serüveni. *İnsan ve Toplum Bilimleri Araştırmaları Dergisi*, 7(1), 146-170. <https://doi.org/10.15869/itobiad.350161>
- Burgoon, J. K. (1982). Privacy and communication. *Annals of the International Communication Association*, 6(1), 206-249. <https://doi.org/10.1080/23808985.1982.11678499>
- Burgoon, J. K., Parrott, R., Le Poire, B. A., Kelley, D. L., Walther, J. B., & Perry, D. (1989). Maintaining and restoring privacy through communication in different types of relationships. *Journal of Social and Personal Relationships*, 6(2), 131-158. <https://doi.org/10.1177/026540758900600201>

- BusinessWorld. (2018, Mayıs 12). *Rural internet penetration still lagging*.
<https://www.bworldonline.com/rural-internet-penetration-still-lagging-sws/>
- Büyüköztürk, Ş., Kılıç Çakmak, E., Akgün, Ö. E., Karadeniz, Ş., & Demirel, F. (2014).
Bilimsel araştırma yöntemleri (17. bs). Pegem Akademi.
- Cairncross, F. (2002). The death of distance. *RSA Journal*, 149(5502), 40-47.
- Campbell, J. E., & Carlson, M. (2002). Panopticon.com: Online surveillance and the commodification of privacy. *Journal of Broadcasting & Electronic Media*, 46(4), 586-606. https://doi.org/10.1207/s15506878jobem4604_6
- Cardoso, G. (2005). Societies in transition to the network society. İçinde M. Castells & G. Cardoso (Ed.), *The Network Society From Knowledge to Policy* (ss. 23-). Center for Transatlantic Relations.
- Carretero, S., Vuorikari, R., Punie, Y., European Commission, & Joint Research Centre. (2017). *DigComp 2.1 the digital competence framework for citizens with eight proficiency levels and examples of use*.
- Castells, M. (2002). *The internet galaxy*. Oxford University Press.
<https://doi.org/10.1093/acprof:oso/9780199255771.001.0001>
- Castells, M. (2004a). Informationalism, networks, and the network society: A theoretical blueprint. İçinde M. Castells (Ed.), *The network society: A cross-cultural perspective* (ss. 3-45). Edward Elgar Pub.
- Castells, M. (Ed.). (2004b). *The network society: A cross-cultural perspective*. Edward Elgar Pub.
- Castells, M. (2005). The network society from knowledge to policy. İçinde M. Castells & G. Cardoso (Ed.), *The Network Society From Knowledge to Policy* (ss. 3-21). Center for Transatlantic Relations.
- Castells, M. (2010a). *End of millennium* (2nd ed., with new preface). Blackwell Publishers.
- Castells, M. (2010b). *The power of identity* (2nd ed., with a new preface). Wiley-Blackwell.
- Castells, M. (2010c). *The rise of the network society* (2nd ed., with a new pref). Wiley-Blackwell.

- Castellví, J., Díez-Bedmar, M.-C., & Santisteban, A. (2020). Pre-service teachers' critical digital literacy skills and attitudes to address social problems. *Social Sciences*, 9(8), 134. <https://doi.org/10.3390/socsci9080134>
- Castro Rojas, M. D., Bygholm, A., & Hansen, T. G. B. (2016). Using information and communication technologies to promote healthy aging in costa rica: Challenges and opportunities. İçinde J. Zhou & G. Salvendy (Ed.), *Human Aspects of IT for the Aged Population. Healthy and Active Aging* (C. 9755, ss. 194-206). Springer International Publishing. https://doi.org/10.1007/978-3-319-39949-2_19
- Chen, C. (2018, Şubat 7). *Report: Internet usage in rural communities on the rise—Chinadaily.com.cn*.
<http://www.chinadaily.com.cn/a/201807/02/WS5b3992b0a3103349141e01d2.html>
- Chen, X., & Michael, K. (2012). Privacy issues and solutions in social network sites. *IEEE Technology and Society Magazine*, 31(4), 43-53. <https://doi.org/10.1109/MTS.2012.2225674>
- Choi, J. R., Straubhaar, J., Skouras, M., Park, S., Santillana, M., & Strover, S. (2021). Techno-capital: Theorizing media and information literacy through information technology capabilities. *New Media & Society*, 23(7), 1989-2011. <https://doi.org/10.1177/1461444820925800>
- Choi, M., Glassman, M., & Cristol, D. (2017). What it means to be a citizen in the internet age: Development of a reliable and valid digital citizenship scale. *Computers & Education*, 107, 100-112. <https://doi.org/10.1016/j.compedu.2017.01.002>
- Christakis, N. A., & Fowler, J. H. (2007). The Spread of Obesity in a Large Social Network over 32 Years. *The New England Journal of Medicine*, 357(4), 370-379.
- Christakis, N. A., & Fowler, J. H. (2011). *Connected: The surprising power of our social networks and how they shape our lives, how your friends' friends' friends affect everything you feel, think, and do*. Little, Brown Spark.
- Christofides, E., Muise, A., & Desmarais, S. (2009). Information disclosure and control on facebook: Are they two sides of the same coin or two different processes?

- CyberPsychology & Behavior*, 12(3), 341-345.
<https://doi.org/10.1089/cpb.2008.0226>
- Christofides, E., Muise, A., & Desmarais, S. (2012). Hey mom, what's on your facebook? Comparing facebook disclosure and privacy in adolescents and adults. *Social Psychological and Personality Science*, 3(1), 48-54.
<https://doi.org/10.1177/1948550611408619>
- Clapp, R. (2021, Nisan 30). *COVID-19 causes digital consumption to rise by over 30%, forming new and lasting consumer habits* | WARC.
<http://origin.warc.com/newsandopinion/opinion/covid-19-causes-digital-consumption-to-rise-by-over-30-forming-new-and-lasting-consumer-habits/en-gb/4209>
- Clarke, R. (1988). Information technology and dataveillance. *Communications of the ACM*, 31(5), 498-512. <https://doi.org/10.1145/42411.42413>
- Cleophas, T. J., & Zwinderman, A. H. (2016). *SPSS for starters and 2nd levelers*. Springer International Publishing. <https://doi.org/10.1007/978-3-319-20600-4>
- Colvile, R. (2013). *Eric Schmidt interview: 'You have to fight for your privacy or you will lose it'—Telegraph*. <https://www.telegraph.co.uk/technology/eric-schmidt/10076175/Eric-Schmidt-interview-You-have-to-fight-for-your-privacy-or-you-will-lose-it.html>
- Commission on Science and Technology for Development. (2018). *Building digital competencies to benefit from existing and emerging technologies, with a special focus on gender and youth dimensions* (Report of the Secretary General E/CN.16/2018/3). United Nations. https://unctad.org/system/files/official-document/ecn162018d3_en.pdf
- Conklin, K. R. (1976). Privacy: Should there be a right to it? *Educational Theory*, 26(3), 263-270. <https://doi.org/10.1111/j.1741-5446.1976.tb00734.x>
- Council of the European Union. (2010). *Avrupa insan hakları sözleşmesi*. Avrupa İnsan Hakları Mahkemesi. https://www.echr.coe.int/Documents/Convention_TUR.pdf
- Charter of fundamental rights of the european union, 2012/C 326/02 (2012). <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN>

- Covello, S. (2010). *A review of digital literacy assessment instruments*.
https://www.academia.edu/7935447/A_Review_of_Digital_Literacy_Assessment_Instruments?auto=download
- Çalışma ve Sosyal Güvenlik Bakanlığı. (2016). *Türkiye—Ülke notu—Beceriler önemlidir: Yetişkin becerileri araştırmasının kapsamlı sonuçları*. OECD.
<https://www.oecd.org/skills/piaac/Skills-Matter-Turkey-Turkish-version.pdf>
- Çavuş, N. (2021, Ağustos 1). *Whatsapp kullanabilmek için güncellemeyi kabul etmek zorunlu*. Webtekno. <https://www.webtekno.com/whatsapp-yeni-sozlesme-turkiyede-zorunlu-h104599.html>
- Çayır, F. (2020). *Covid-19 sürecinde temas takip uygulamaları ve kişisel verilerin korunması* (1. bs). Alternatif Bilişim Derneği.
<https://ekitap.alternatifbilisim.org/covid-19-temas-takip-uygulamaları/>
<https://ekitap.alternatifbilisim.org/pdf/covid-19-temas-takip.pdf>
- Çubukcu, A., & Bayzan, Ş. (2013). Türkiye’de dijital vatandaşlık algısı ve bu algıyı internetin bilinçli, güvenli ve etkin kullanımı ile artırma yöntemleri. *Middle Eastern & African Journal of Educational Research*, 5(1), 148-174.
- D. Haggerty, Richard V. Ericson, K. (2000). The surveillant assemblage. *British Journal of Sociology*, 51(4), 605-622. <https://doi.org/10.1080/00071310020015280>
- De Wolf, R., Willaert, K., & Pierson, J. (2014). Managing privacy boundaries together: Exploring individual and group privacy management strategies in Facebook. *Computers in Human Behavior*, 35, 444-454.
<https://doi.org/10.1016/j.chb.2014.03.010>
- Debatin, B., Lovejoy, J. P., Horn, A.-K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication*, 15(1), 83-108.
<https://doi.org/10.1111/j.1083-6101.2009.01494.x>
- DeCew, J. W. (1997). *In pursuit of privacy*. Cornell University Press; JSTOR.
<http://www.jstor.org/stable/10.7591/j.ctv75d3zc>
- Deloitte Center for Technology, Media & Telecommunications. (2021). *Digital media trends, 15th edition: Courting the consumer in a world of choice* (s. 28) [Deloitte Insights]. Deloitte.

<https://www2.deloitte.com/us/en/insights/industry/technology/digital-media-trends-consumption-habits-survey/summary.html>

Democracy Now. (2012, Nisan 23). “*We don’t live in a free country*”: Jacob Appelbaum on being target of widespread gov’t surveillance. Democracy Now! http://www.democracynow.org/2012/4/20/we_do_not_live_in_a

Denizer, M. C. (2019). Türkiye’de ilk dönem internet servis sağlayıcıları: Bir arşiv denemesi. İçinde E. Saka (Ed.), *Türkiye İnternet Tarihi*. Alternatif Bilişim Derneği. https://ekitap.alternatifbilisim.org/files/ymc5_turkiye_internet_tarihi.pdf

Department for Education. (2018). *Essential digital skills framework*. <https://www.gov.uk/government/publications/essential-digital-skills-framework>

Dinev, T., & Hart, P. (2003). Privacy concerns and internet use: A model of trade-off factors. *Academy of Management Proceedings*, 2003(1), D1-D6. <https://doi.org/10.5465/ambpp.2003.13792464>

Dinev, T., & Hart, P. (2005). Internet privacy concerns and social awareness as determinants of intention to transact. *International Journal of Electronic Commerce*, 10(2), 7-29. <https://doi.org/10.2753/JEC1086-4415100201>

Directive 95/46/EC of the European Parliament and of the Council, EUR-Lex—31995L0046—EN (1995). <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046>

Doyle, A. (2011). Revisiting the synopticon: Reconsidering mathiesen’s ‘the viewer society’ in the age of web 2.0. *Theoretical Criminology*, 15(3), 283-299. <https://doi.org/10.1177/1362480610396645>

Doyle, C. S. (1992). *Outcome measures for information literacy within the national education goals of 1990*. National Forum on Information Literacy. <https://eric.ed.gov/?id=ED351033>

DQ Institute. (2020). *2020 child online safety index*. DQ Institute. <https://www.dqinstitute.org/child-online-safety-index/>

Duerr, H. P. (1999). *Uygarlaşma sürecinin miti: I çıplaklık ve utanç* (1. bs). Dost Kitabevi.

- Duerr, H. P. (2004). *Uygarlaşma sürecinin miti: İi mahremiyet* (M. Tüzel, Çev.; 1. bs). Dost Kitabevi.
- Duignan, B. (2020). Dunning-kruger effect. İçinde *Encyclopedia Britannica*. <https://www.britannica.com/science/Dunning-Kruger-effect>
- D’Urso, S. C. (2006). Who’s watching us at work? Toward a structural–perceptual model of electronic monitoring and surveillance in organizations. *Communication Theory*, 16(3), 281-303. <https://doi.org/10.1111/j.1468-2885.2006.00271.x>
- Dutta, S., & Lanvin, B. (Ed.). (2020). *The network readiness index 2020 accelerating digital transformation in a post-covid global economy*. Portulans Institute. https://networkreadinessindex.org/wp-content/uploads/2020/11/NRI-2020-V8_28-11-2020.pdf
- Earp, J. B., Anton, A. I., Aiman-Smith, L., & Stufflebeam, W. H. (2005). Examining internet privacy policies within the context of user privacy values. *IEEE Transactions on Engineering Management*, 52(2), 227-237. <https://doi.org/10.1109/TEM.2005.844927>
- Eggers, D. (2017). *Çember* (H. Balkara, Çev.; 4. bs). Siren Yayınları.
- Eken, M. (2021). Literatür ve sahanın kesişiminde dijital göçmenler için dijital yetkinlikler. *Erciyes İletişim Dergisi*, 8(2), 813-846. <https://doi.org/10.17680/erciyesiletisim.969495>
- Elçiçek, M., Erdemci, H., & Karal, H. (2018). Examining the relationship between the levels of digital citizenship and social presence for the graduate students having online education. *Turkish Online Journal of Distance Education*, 19(1), 203-214. <https://doi.org/10.17718/tojde.382801>
- Elias, N. (2009). *Uygarlık süreci cilt 2* (E. Özbek, Çev.; 4. bs). İletişim Yayınları.
- Elias, N. (2016). *Uygarlık süreci cilt 1* (E. Ateşman, Çev.; 6. bs). İletişim Yayınları.
- Ellison, N. B., Steinfield, C., & Lampe, C. (2007). The benefits of facebook “friends:” social capital and college students’ use of online social network sites. *Journal of Computer-Mediated Communication*, 12(4), 1143-1168. <https://doi.org/10.1111/j.1083-6101.2007.00367.x>
- Ellison, N. B., Vitak, J., Steinfield, C., Gray, R., & Lampe, C. (2011). Negotiating privacy concerns and social capital needs in a social media environment. İçinde

- S. Trepte & L. Reinecke (Ed.), *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web* (ss. 19-32). Springer.
<http://link.springer.com/10.1007/978-3-642-21521-6>
- Erdem, C., & Koçyiğit, M. (2019). Exploring undergraduates' digital citizenship levels: Adaptation of the digital citizenship scale to turkish. *Malaysian Online Journal of Educational Technology*, 7(3), 22-38.
<https://doi.org/10.17220/mojet.2019.03.003>
- Ergin, M., & Bozdağ, B. (2021). Examination of digital literacy levels of the sports sciences faculty students. *The Online Journal of Recreation and Sport*, 10(2), 24-36. <https://doi.org/10.22282/ojrs.2021.82>
- Esguerra, R. (2009, Aralık 10). *Google ceo eric schmidt dismisses the importance of privacy*. Electronic Frontier Foundation.
<https://www.eff.org/deeplinks/2009/12/google-ceo-eric-schmidt-dismisses-privacy>
- Eshet-Alkalai, Y. (2004). Digital literacy: A conceptual framework for survival skills in the digital era. *Journal of Educational Multimedia and Hypermedia*, 13(1), 93-106.
- Etzioni, A. (2000). The right to privacy vs. The common good. *USA Today Magazine*, 129(2664), 24. f6h.
- European Commission. (2007). *A European approach to media literacy in the digital environment*. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52007DC0833&from=en>
- European Commission. (2021). *DigComp*. EU Science Hub - European Commission.
<https://ec.europa.eu/jrc/en/digcomp>
- European Union (Ed.). (2010). *Data protection in the European Union: The role of national data protection authorities*. Publications Office of the European Union.
- Eurostat. (2021, Mayıs 25). *Individuals' level of digital skills*. Eurostat.
https://appsso.eurostat.ec.europa.eu/nui/show.do?query=BOOKMARK_DS-601368_QID_-183C6548_UID_-3F171EB0&layout=TIME,C,X,0;GEO,L,Y,0;INDIC_IS,L,Z,0;IND_TYPE,L,Z,1;UNIT,L,Z,2;INDICATORS,C,Z,3;&zSelection=DS-

601368IND_TYPE,IND_TOTAL;DS-601368INDIC_IS,I_DSK_B;DS-
 601368INDICATORS,OBS_FLAG;DS-
 601368UNIT,PC_IND_IU3;&rankName1=UNIT_1_2_-
 1_2&rankName2=INDICATORS_1_2_-1_2&rankName3=INDIC-IS_1_2_-
 1_2&rankName4=IND-TYPE_1_2_-
 1_2&rankName5=TIME_1_0_0_0&rankName6=GEO_1_2_0_1&sortC=ASC_-
 1_FIRST&rStp=&cStp=&rDCh=&cDCh=&rDM=true&cDM=true&footnes=fal
 se&empty=false&wai=false&time_mode=ROLLING&time_most_recent=true&
 lang=EN&cfo=%23%23%23%2C%23%23%23.%23%23%23

- Fischer-Hübner, S. (1998). Privacy and security at risk in the global information society. *Information, Communication & Society*, 1(4), 420-441. <https://doi.org/10.1080/13691189809358981>
- Fogel, J., & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior*, 25(1), 153-160. <https://doi.org/10.1016/j.chb.2008.08.006>
- Foucault, M. (1992). *Hapishanenin doğuşu* (M. A. Kılıçbay, Çev.; 1. bs). İmge Kitabevi.
- Fox, M. (2013, Şubat 22). Alan F. Westin, who transformed privacy debate before the web era, dies at 83. *The New York Times*. <https://www.nytimes.com/2013/02/23/us/alan-f-westin-scholar-who-defined-right-to-privacy-dies-at-83.html>
- Fraillon, J., Gebhardt, E., Friedman, T., Duckworth, D., O'Malley, K., & Vernon, K. (2018). *NAP sample assessment ICT literacy: Years 6 and 10*. Australian Curriculum, Assessment and Reporting. https://www.nap.edu.au/docs/default-source/default-document-library/2017napictlreport_final.pdf?sfvrsn=2
- Fraillon, J., Schulz, W., Gebhardt, E., & Ainley, J. (2015). *National assessment program: ICT literacy years 6 & 10* (Sy 2014; National Assessment Program). Australian Curriculum, Assessment and Reporting Authority. https://www.nap.edu.au/_resources/D15_8761__NAP-ICT_2014_Public_Report_Final.pdf

- Fuchs, C. (2011). New media, web 2.0 and surveillance: Web 2.0 surveillance. *Sociology Compass*, 5(2), 134-147. <https://doi.org/10.1111/j.1751-9020.2010.00354.x>
- Furini, M., Mirri, S., Montangero, M., & Prandi, C. (2020). Privacy perception when using smartphone applications. *Mobile Networks and Applications*, 25, 1055-1061. <https://doi.org/10.1007/s11036-020-01529-z>
- Furnell, S. (2005). Why users cannot use security. *Computers & Security*, 24(4), 274-279. <https://doi.org/10.1016/j.cose.2005.04.003>
- Gandy, O. H. (1993). *The panoptic sort: A political economy of personal information*. Westview.
- Gangadharbatla, H. (2008). Facebook me: Collective self-esteem, need to belong, and internet self-efficacy as predictors of the igeneration's attitudes toward social networking sites. *Journal of Interactive Advertising*, 8(2), 5-15. <https://doi.org/10.1080/15252019.2008.10722138>
- Garfinkel, S., & Spafford, G. (2002). *Web security, privacy and commerce* (2nd ed. expanded & updated). O'Reilly.
- George, D., & Mallery, P. (2020). *IBM SPSS statistics 26 step by step: A simple guide and reference* (Sixteenth edition). Routledge, Taylor & Francis Group.
- Geray, H. (2014). *Toplumsal arařtırmalarda nicel ve nitel yöntemlere giriş* (1. bs). Umuttepe Yayınları.
- Gerke, S., Shachar, C., Chai, P. R., & Cohen, I. G. (2020). Regulatory, safety, and privacy concerns of home monitoring technologies during COVID-19. *Nature Medicine*, 26(8), 1176-1182. <https://doi.org/10.1038/s41591-020-0994-1>
- Gilster, P. (1997). *Digital literacy*. Wiley Computer Pub.
- Giner, S. (2001). Mass society: History of the concept. İinde N. J. Smelser & P. B. Baltes (Ed.), *International Encyclopedia of the Social & Behavioral Sciences* (ss. 9368-9372). Pergamon. <https://doi.org/10.1016/B0-08-043076-7/00130-3>
- Goffman, E. (2014). *Günlük yaşamda benliğin sunumu* (B. Cezar, Çev.; 3. bs). Metis Yayınları.
- Goffman, E. (2017). *Kamusal alanda ilişkiler: Toplu yaşamın mikro incelemeleri* (M. F. Karakaya, Çev.; 1. bs). Heretik.

- Gordon, D. R. (1987). The electronic panopticon: A case study of the development of the national criminal records system. *Politics & Society*, 15(4), 483-511. <https://doi.org/10.1177/003232928701500404>
- Govani, T., & Pashley, H. (2005). *Student awareness of the privacy implications when using facebook*. <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.95.6108&rep=rep1&type=pdf>
- Gökalier, E., & Saatçioğlu, E. (2020). Sosyal büyük veri ekseninde kişisel gizlilik sorunsalı: Türkiye’de eğitilmiş ve kentli sosyal ağ kullanıcılarının gizlilik sorunlarına yaklaşımları. *Connectist: Istanbul University Journal of Communication Sciences*, 133-167. <https://doi.org/10.26650/CONNECTIST2020-0085>
- Göle, N. (2016). *Modern mahrem: Medeniyet ve örtünme* (13. bs). Metis Yayınları.
- Greenhow, C., & Robelia, B. (2009). Informal learning and identity formation in online social networks. *Learning, Media and Technology*, 34(2), 119-140. <https://doi.org/10.1080/17439880902923580>
- Gross, R., & Acquisti, A. (2005). Information revelation and privacy in online social networks. *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society - WPES '05*, 71. <https://doi.org/10.1145/1102199.1102214>
- Gutiérrez-Martín, A., & Tyner, K. (2012). Media education, media literacy and digital competence. *Comunicar*, 19(38), 31-39. <https://doi.org/10.3916/C38-2012-02-03>
- Güngör, M., & Evren, G. (2002). *İnternet sektörü ve Türkiye incelemeleri*. Bilgi Teknolojileri ve İletişim Kurumu. <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjdzrH5uYr0AhXbiP0HHS7dAYEQFnoECAMQAAQ&url=https%3A%2F%2Fwww.btk.gov.tr%2Fuploads%2Fpages%2Fslug%2Finternet-sektoru-ve-turkiye-incelemeleri.pdf&usg=AOvVaw3piOgkoiZiGHh9SrgIrbqD>
- Güven, S. K., & Kovanlıkaya, C. (2008). Postmodern rear window: Facebook. *İçinde 6th International Symposium Communication in the Millenium-Proceedings Book* (C. 1, ss. 481-496).

https://www.academia.edu/1389923/POSTMODERN_REAR_WINDOW_FAC_EBOOK

- Haber, E., & Tamò-Larrieux, A. (2020). Privacy and security by design: Comparing the EU and Israeli approaches to embedding privacy and security. *Computer Law & Security Review*, 37, 105409. <https://doi.org/10.1016/j.clsr.2020.105409>
- Hacettepe Üniversitesi Nüfus Etütleri Enstitüsü. (2004). *Türkiye nüfus ve sağlık araştırması, 2003*. Hacettepe Üniversitesi.
- Hague, C., & Payton, S. (2010). *Digital literacy across the curriculum*. Futurelab. <https://www.nfer.ac.uk/publications/futl06/futl06.pdf>
- Haigh, R. W. (1985). Planning for computer literacy. *The Journal of Higher Education*, 56(2), 161. <https://doi.org/10.2307/1981664>
- Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2014). *Multivariate data analysis* (7. ed., Pearson new internat. ed). Pearson.
- Hallinan, D., Friedewald, M., & McCarthy, P. (2012). Citizens' perceptions of data protection and privacy in Europe. *Computer Law & Security Review*, 28(3), 263-272. <https://doi.org/10.1016/j.clsr.2012.03.005>
- Hamburger, E. (2014, Mayıs 22). *Facebook increases privacy on all new posts by default*. The Verge. <https://www.theverge.com/2014/5/22/5739744/facebook-changes-default-privacy-of-posts-from-public-to-friends>
- Hamutoğlu, N. B., Canan Güngören, Ö., Kaya Uyanık, G., & Gür Erdoğan, D. (2017). Dijital okuryazarlık ölçeği: Türkçe'ye uyarlama çalışması. *Ege Eğitim Dergisi*, 18(1), 408-429. <https://doi.org/10.12984/egedfd.295306>
- Hargittai, E., & Shafer, S. (2006). Differences in actual and perceived online skills: The role of gender. *Social Science Quarterly*, 87(2), 432-448. <https://doi.org/10.1111/j.1540-6237.2006.00389.x>
- He, J., & Chu, W. W. (2008). Protecting private information in online social networks. İçinde H. Chen & C. C. Yang (Ed.), *Intelligence and Security Informatics* (C. 135, ss. 249-273). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-540-69209-6_14

- Henderson, S., & Gilding, M. (2004). 'I've never clicked this much with anyone in my life': Trust and hyperpersonal communication in online friendships. *New Media & Society*, 6(4), 487-506. <https://doi.org/10.1177/146144804044331>
- Henson, B., Reyns, B. W., & Fisher, B. S. (2011). Security in the 21st century: Examining the link between online social network activity, privacy, and interpersonal victimization. *Criminal Justice Review*, 36(3), 253-268. <https://doi.org/10.1177/0734016811399421>
- Heravi, A., Mubarak, S., & Raymond Choo, K.-K. (2018). Information privacy in online social networks: Uses and gratification perspective. *Computers in Human Behavior*, 84, 441-459. <https://doi.org/10.1016/j.chb.2018.03.016>
- Hindman, M. S. (2009). *The myth of digital democracy*. Princeton University Press.
- Ho, R. (2017). *Understanding statistics for the social sciences with IBM SPSS*. CRC Press.
- Hobbs, R. (1998). The seven great debates in the media literacy movement. *Journal of Communication*, 48(1), 16-32.
- Hobbs, R. (2010). *Digital and media literacy a plan of action*. Aspen Institute and John S. and James L. Knight Foundation.
- Hobbs, R. (Ed.). (2016). *Exploring the roots of digital and media literacy through personal narrative*. Temple University Press. <https://doi.org/10.2307/j.ctvrf898z>
- Hobbs, R., & Coiro, J. (2019). Design features of a professional development program in digital literacy. *Journal of Adolescent & Adult Literacy*, 62(4), 401-409. <https://doi.org/10.1002/jaal.907>
- Hofstede, G. (2002). *Culture's consequences comparing values, behaviors, institutions, and organizations across nations*. SAGE. https://books.google.com.tr/books?hl=tr&lr&id=9HE-DQAAQBAJ&oi=fnd&pg=PP1&ots=ILv7pMz_PP&sig=nVfbm_yrGvgmeIzuzLxJYspUyTI&redir_esc=y&pli=1#v=onepage&q&f=false
- Hooft Graafland, J. (2018). *New technologies and 21st century children: Recent trends and outcomes* (OECD Education Working Papers Sy 179; OECD Education Working Papers, C. 179). <https://doi.org/10.1787/e071a505-en>

- Hough, M. G. (2009). Keeping it to ourselves: Technology, privacy, and the loss of reserve. *Technology in Society*, 31(4), 406-413. <https://doi.org/10.1016/j.techsoc.2009.10.005>
- Hoy, M. G., & Milne, G. (2010). Gender differences in privacy-related measures for young adult facebook users. *Journal of Interactive Advertising*, 10(2), 28-45. <https://doi.org/10.1080/15252019.2010.10722168>
- International ICT Literacy Panel. (2002). *Digital transformation: A framework for ICT literacy* (ETS Report of the International ICT Literacy Panel, s. 42). Educational Testing Service (ETS).
- Internet World Stats. (2021). *World internet users statistics and 2021 world population stats*. <https://www.internetworldstats.com/stats.htm>
- Isin, E. F., & Ruppert, E. S. (2020). *Being digital citizens* (Second edition). Rowman & Littlefield International.
- Isman, A., & Canan Gungoren, O. (2014). Digital citizenship. *The Turkish Online Journal of Educational Technology*, 13(1).
- ISTE. (2018). *ISTE standards*. International Society for Technology in Education. <https://www.iste.org/iste-standards>
- İlkiz, F. (2013, Nisan 8). *Büyük umutlar ve kişisel veriler*. Bianet - Bağımsız İletişim Ağı. <https://www.bianet.org/bianet/hukuk/145662-buyuk-umutlar-ve-kisisel-veriler>
- ITU. (2018a). *Digital skills toolkit*. International Telecommunication Union. <http://handle.itu.int/11.1002/pub/8110cd77-en>
- ITU. (2018b). *Measuring the information society report 2018 volume 1* (C. 1). International Telecommunication Union. <https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2018/MISR-2018-Vol-1-E.pdf>
- ITU. (2020a). *Digital skills assessment guidebook*.
- ITU. (2020b). *ITU world telecommunication/ICT indicators database*. ITU. <https://www.itu.int:443/en/ITU-D/Statistics/Pages/stat/default.aspx>
- ITU. (2020c). *Measuring digital development facts and figures 2020*. International Telecommunication Union. <https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2020.pdf>

- İzgi, M. C. (2009). *Etik açıdan yaşlı mahremiyeti: Huzurevi örneğinde hizmet alanlar ve verenler açısından bir değerlendirme* [Doktora Tezi, Ankara Üniversitesi]. <http://acikarsiv.ankara.edu.tr/browse/27778/>
- Jackman, J. A., Gentile, D. A., Cho, N.-J., & Park, Y. (2021). Addressing the digital skills gap for future education. *Nature Human Behaviour*, 5(5), 542-545. <https://doi.org/10.1038/s41562-021-01074-z>
- Jeanneney, J.-N. (2006). *Başlangıcından günümüze medya tarihi* (E. Atuk, Çev.; 2. bs). Yapı Kredi Yayınları.
- Jin, K.-Y., Reichert, F., Cagasan, L. P., de la Torre, J., & Law, N. (2020). Measuring digital literacy across three age cohorts: Exploring test dimensionality and performance differences. *Computers & Education*, 157. <https://doi.org/10.1016/j.compedu.2020.103968>
- Jones, E. E., & Archer, R. L. (1976). Are there special effects of personalistic self-disclosure? *Journal of Experimental Social Psychology*, 12(2), 180-193. [https://doi.org/10.1016/0022-1031\(76\)90069-X](https://doi.org/10.1016/0022-1031(76)90069-X)
- Jones, H., & Soltren, J. H. (2005). *Facebook: Threats to privacy*. <http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall05-papers/facebook.pdf>
- Jones, K. S. (2003). Privacy: What's different now? *Interdisciplinary Science Reviews*, 28(4), 287-292. <https://doi.org/10.1179/030801803225008677>
- Jones, L. M., & Mitchell, K. J. (2016). Defining and measuring youth digital citizenship. *New Media & Society*, 18(9), 2063-2079. <https://doi.org/10.1177/1461444815577797>
- Jourard, S. M. (1966). Some psychological aspects of privacy. *Law and Contemporary Problems*, 31(2), 307. <https://doi.org/10.2307/1190673>
- Jourard, S. M., & Lasakow, P. (1958). Some factors in self-disclosure. *The Journal of Abnormal and Social Psychology*, 56(1), 91-98. <https://doi.org/10.1037/h0043357>
- Kalaman, S. (2016). *Sosyokültürel, ekonomik ve siyasi boyutlarıyla yeni medyada mahremiyetin dönüşümü: Facebook örneği* [Doktora Tezi]. Ege Üniversitesi Sosyal Bilimler Enstitüsü.

- Kalaman, S. (2017). Yeni medya ve mahremiyetin dönüşümü facebook Türkiye örneği. *International Peer-Reviewed Journal of Communication And Humanities Research*, 0(14), 1-31. <https://doi.org/10.17361/UHIVE.2017.1.0011>
- Karakuş Yılmaz, T. (2020). Dijital haklar ve sorumluluklar. İçinde Ş. Sağıroğlu, H. İ. Bülbül, A. Kılıç, & M. Küçükali (Ed.), *Dijital Okuryazarlık: Araçlar, Metodolojiler, Uygulamalar ve Öneriler* (ss. 127-180). Nobel Akademik Yayıncılık.
- Karpel, M. A. (1980). Family secrets: I. conceptual and ethical issues in the relational context. ii. ethical and practical considerations in therapeutic management. *Family Process*, 19(3), 295-306. <https://doi.org/10.1111/j.1545-5300.1980.00295.x>
- Katz, I. R. (2007). Testing information literacy in digital environments: ETS's iskills assessment. *Information Technology and Libraries*, 26(3), 3. <https://doi.org/10.6017/ital.v26i3.3271>
- Kezer, M., Sevi, B., Cemalcılar, Z., & Baruh, L. (2016). Age differences in privacy attitudes, literacy and privacy management on Facebook. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 10(1). <https://doi.org/10.5817/CP2016-1-2>
- Khan, R., Kumar, P., Jayakody, D. N. K., & Liyanage, M. (2020). A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions. *IEEE Communications Surveys & Tutorials*, 22(1), 196-248. <https://doi.org/10.1109/COMST.2019.2933899>
- Kim, M., & Choi, D. (2018). Development of youth digital citizenship scale and implication for educational setting. *Educational Technology & Society*, 21(1), 155-171.
- Kişisel Verilerin Korunması Kanunu, 6698 (2016). <https://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf>
- Koçak, C. (2016, Ocak 28). *Zygmunt Bauman: "Sosyal medya bir tuzak"*. vesaire. <https://vesaire.org/zygmunt-bauman-sosyal-medya-bir-tuzak/>
- Kodak, D. (2018). Düşünsel modernitede mahremiyeti yeniden tanımlamak: Kuşaklararası bir araştırma. *Connectist: Istanbul University Journal of Communication Sciences*, 54, 85-116.

- Koltay, T. (2011). The media and the literacies: Media literacy, information literacy, digital literacy. *Media, Culture & Society*, 33(2), 211-221. <https://doi.org/10.1177/0163443710393382>
- Krzywinski, M., & Altman, N. (2014). Nonparametric tests. *Nature Methods*, 11(5), 467-468. <https://doi.org/10.1038/nmeth.2937>
- Kuhlemeier, H., & Hemker, B. (2007). The impact of computer use at home on students' Internet skills. *Computers & Education*, 49(2), 460-480. <https://doi.org/10.1016/j.compedu.2005.10.004>
- Kurbanoğlu, S. S. (2010). Bilgi okuryazarlığı: Kavramsal bir analiz. *Türk Kütüphaneciliği*, 24(4), 723-747.
- Külcü, Ö., & Henkoğlu, T. (2014). Privacy in social networks: An analysis of Facebook. *International Journal of Information Management*, 34(6), 761-769. <https://doi.org/10.1016/j.ijinfomgt.2014.07.006>
- Kütükoğlu, E. (2019). *Sosyal medyadaki mahremiyet algısının belirlenmesi: X, y ve z kuşakları üzerinde bir araştırma* [Doktora Tezi]. Erciyes Üniversitesi Sosyal Bilimler Enstitüsü.
- Lankshear, C., & Knobel, M. (2015). Digital literacy and digital literacies: *Nordic Journal of Digital Literacy*, 2006-2016, 13.
- Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues*, 33(3), 22-42. <https://doi.org/10.1111/j.1540-4560.1977.tb01880.x>
- Laurie, G. T. (2002). *Genetic privacy: A challenge to medico-legal norms*. Cambridge University Press.
- Lemieux, R. (2012). Fictional privacy among facebook users. *Psychological Reports*, 111(1), 289-292. <https://doi.org/10.2466/21.01.PR0.111.4.289-292>
- Litt, E. (2013). Understanding social network site users' privacy tool use. *Computers in Human Behavior*, 29(4), 1649-1656. <https://doi.org/10.1016/j.chb.2013.01.049>
- Liu, Z., & Wang, X. (2018). How to regulate individuals' privacy boundaries on social network sites: A cross-cultural comparison. *Information & Management*, 55(8), 1005-1023. <https://doi.org/10.1016/j.im.2018.05.006>

- Livberber Göçmen, T. (2018). *Toplumsal yaşamda bireylerin mahremiyet yönelimleri: Sosyal ağ kullanıcıları üzerine bir saha araştırması* [Doktora Tezi]. Selçuk Üniversitesi Sosyal Bilimler Enstitüsü.
- Livingstone, S. (2008). Taking risky opportunities in youthful content creation: Teenagers' use of social networking sites for intimacy, privacy and self-expression. *New Media & Society*, 10(3), 393-411. <https://doi.org/10.1177/1461444808089415>
- Liyanage, M., Salo, J., Braeken, A., Kumar, T., Seneviratne, S., & Ylianttila, M. (2018). 5G privacy: Scenarios and solutions. *2018 IEEE 5G World Forum (5GWF)*, 197-203. <https://doi.org/10.1109/5GWF.2018.8516981>
- Lloyds Banking Group. (2019). *Consumer digital index 2019*. https://www.lloydsbank.com/assets/media/pdfs/banking_with_us/whats-happening/lb-consumer-digital-index-2019-report.pdf
- Lloyds Banking Group. (2021). *Essential digital skills report 2021* (Sy 3; Benchmarking the Essential Digital Skills of the UK). https://www.lloydsbank.com/assets/media/pdfs/banking_with_us/whats-happening/210923-lb-essential-digital-skills-2021-report.pdf
- Løkke, E. (2018). *Mahremiyet dijital toplumda özel hayat* (1. bs). Koç Üniversitesi Yayınları.
- Lu, M. (2021, Haziran 22). *How media consumption evolved throughout covid-19*. Visual Capitalist. <https://www.visualcapitalist.com/how-media-consumption-evolved-throughout-covid-19/>
- Luehrmann, A. (1981). Computer literacy-what should it be? *The Mathematics Teacher*, 74(9), 682-686.
- Lyon, D. (1994). *The electronic eye: The rise of surveillance society*. University of Minnesota Press.
- Lyon, D. (2006). *Günlük hayatı kontrol etmek: Gözetlenen toplum* (G. Soykan, Çev.; 1. bs). Kalkedon Yayıncılık.
- Lyon, D. (2013). *Gözetim çalışmaları: Genel bir bakış* (A. Toprak, Çev.; 1. bs). Kalkedon Yayınları.
- Lyon, D. (2018). *The culture of surveillance: Watching as a way of life*. Polity.

- Mahapatra, S. K. (2020). Impact of digital technology training on english for science and technology teachers in india. *RELC Journal*, 51(1), 117-133. <https://doi.org/10.1177/0033688220907401>
- Malecki, E. J. (2003). Digital development in rural areas: Potentials and pitfalls. *Journal of Rural Studies*, 19(2), 201-214. [https://doi.org/10.1016/S0743-0167\(02\)00068-2](https://doi.org/10.1016/S0743-0167(02)00068-2)
- Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, 15(4), 336-355. <https://doi.org/10.1287/isre.1040.0032>
- Mancini, P. (1999). New frontiers in political professionalism. *Political Communication*, 16(3), 231-245. <https://doi.org/10.1080/105846099198604>
- Manning, R. C. (1997). Liberal and communitarian defenses of workplace privacy. *Journal of Business Ethics*, 16(8), 817-823. <https://doi.org/10.1023/A:1017976716129>
- Margulis, S. T. (2011). Three theories of privacy: An overview. İçinde S. Trepte & L. Reinecke (Ed.), *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web* (ss. 9-18). Springer. <http://link.springer.com/10.1007/978-3-642-21521-6>
- Martens, H., & Hobbs, R. (2015). How media literacy supports civic engagement in a digital age. *Atlantic Journal of Communication*, 23(2), 120-137. <https://doi.org/10.1080/15456870.2014.961636>
- Martin, A. (2005). DigEuLit: A European framework for digital literacy: A progress report. *Journal of ELiteracy*, 2, 130-136.
- Martin, A. (2006). A European framework for digital literacy. *Nordic Journal of Digital Literacy*, 1(02), 151-161. <https://doi.org/10.18261/ISSN1891-943X-2006-02-06>
- Martin, A., & Grudziecki, J. (2006). DigEuLit: Concepts and tools for digital literacy development. *Innovation in Teaching and Learning in Information and Computer Sciences*, 5(4), 249-267. <https://doi.org/10.11120/ital.2006.05040249>
- Marx, G. T. (1985). The surveillance society: The threat of 1984-style techniques. *The Futurist*, June, 21-26.

- Marx, G. T. (2004). What's new about the "new surveillance"?: Classifying for change and continuity. *Knowledge, Technology & Policy*, 17(1), 18-37. <https://doi.org/10.1007/BF02687074>
- Marx, G. T. (2016). *Windows into the soul: Surveillance and society in an age of high technology*. University of Chicago Press. <https://doi.org/10.7208/chicago/9780226286075.001.0001>
- Mathiesen, T. (1997). The viewer society: Michel Foucault's "panopticon" revisited. *Theoretical Criminology*, 1(2), 215-234. <https://doi.org/10.1177/1362480697001002003>
- Mcdonald, A. M., & Cranor, L. F. (2008). The cost of reading privacy policies. *I/S: A Journal of Law and Policy for the Information Society*, 4(3), 543-568.
- McGrath, J. (2012). Performing surveillance. *İçinde Routledge Handbook of Surveillance Studies*. Routledge. https://doi.org/10.4324/9780203814949.ch1_3_a
- Meachem, A., & Herald-Tribune, S. (2020, Temmuz 27). *Why some rural communities lack high-speed internet*. GovTech. <https://www.govtech.com/network/Why-Some-Rural-Communities-Lack-High-Speed-Internet.html>
- MINDtheGaps. (2021). *Youth digital citizenship education*. <https://www.salto-youth.net/tools/toolbox/tool/youth-digital-citizenship-education.2964/>
- Milgram, S. (1967). The small world problem. *Psychology Today*, 1(1), 61-67.
- 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. <https://doi.org/10.1002/dir.20009>
- Milne, G. R., & Gordon, M. E. (1993). Direct mail privacy-efficiency trade-offs within an implied social contract framework. *Journal of Public Policy & Marketing*, 12(2), 206-215. <https://doi.org/10.1177/074391569101200206>
- Momen, N., & Piekarska, M. (2017). Towards improving privacy awareness regarding apps' permissions. *ICDS 2017: The Eleventh International Conference on Digital Society and eGovernments*. ICDS 2017: The Eleventh International Conference on Digital Society and eGovernments.

- Mossberger, K. (2009). Toward digital citizenship: Addressing inequality in the information age. İçinde A. Chadwick & P. N. Howard (Ed.), *Routledge handbook of Internet politics* (ss. 173-185). Routledge.
- Mossberger, K., Tolbert, C. J., & Hamilton, A. (2012). Measuring digital citizenship: Mobile access and broadband. *International Journal of Communication*, 6, 2492-2528.
- Mossberger, K., Tolbert, C. J., & McNeal, R. S. (2008). *Digital citizenship: The internet, society, and participation*. MIT Press.
<http://site.ebrary.com/id/10194164>
- Munro, A. (2017). Mass society. İçinde *Encyclopedia Britannica*.
<https://www.britannica.com/topic/mass-society>
- Murakami Wood, D. (2013). What is global surveillance? Towards a relational political economy of the global surveillant assemblage. *Geoforum*, 49, 317-326.
<https://doi.org/10.1016/j.geoforum.2013.07.001>
- Mutlu, E. (2004). *İletişim sözlüğü* (4. bs). Bilim ve Sanat.
- Nascimbeni, F., & Vosloo, S. (2019). *Digital literacy for children: Exploring definitions and frameworks* (s. 41) [Scoping Paper]. United Nations Children's Fund (UNICEF).
- Nebeker, D. M., & Tatum, B. C. (1993). The effects of computer monitoring, standards, and rewards on work performance, job satisfaction, and stress. *Journal of Applied Social Psychology*, 23(7), 508-536. <https://doi.org/10.1111/j.1559-1816.1993.tb01101.x>
- Nemec Zlatolas, L., Welzer, T., Heričko, M., & Hölbl, M. (2015). Privacy antecedents for SNS self-disclosure: The case of Facebook. *Computers in Human Behavior*, 45, 158-167. <https://doi.org/10.1016/j.chb.2014.12.012>
- Networked Society Lab. (2016). *Networked society city index 2016*. Ericsson.
<https://www.ericsson.com/49ea27/assets/local/reports-papers/networked-society-insights/reports/2016-networked-society-city-index.pdf>
- Neuman, W. L. (2010a). *Toplumsal araştırma yöntemleri: Nitel ve nicel yaklaşımlar 1* (S. Özge, Çev.; 4. bs). Yayın Odası Yayınları.

- Neuman, W. L. (2010b). *Toplumsal araştırma yöntemleri: Nitel ve nicel yaklaşımlar 2* (S. Özge, Çev.; 4. bs). Yayın Odası Yayınları.
- Ng, W. (2012a). *Empowering scientific literacy through digital literacy and multiliteracies*. Nova Science Publishers, Inc; eBook Collection (EBSCOhost). <https://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=604021&lang=tr&site=eds-live&scope=site&authtype=uid>
- Ng, W. (2012b). Can we teach digital natives digital literacy? *Computers & Education*, 59(3), 1065-1078. <https://doi.org/10.1016/j.compedu.2012.04.016>
- Niedzviecki, H. (2019). *Dikizleme günlüğü: Kendimizi ve komşularımızı gözetlemeyi niçin bu kadar sevdik* (G. Gündüç, Çev.; 2. bs). Ayrıntı Yayınları.
- Noor, M. U. (2020). Indonesian millennial awareness to privacy and personal data protection on the internet. *DESIDOC Journal of Library & Information Technology*, 40(02), 431-436. <https://doi.org/10.14429/djlit.40.02.14969>
- Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, 41(1), 100-126. <https://doi.org/10.1111/j.1745-6606.2006.00070.x>
- Norris, G., & Qureshi, F. (2012). *Introduction to statistics with SPSS for the social sciences* (1st ed). Pearson.
- Nosko, A., Wood, E., & Molema, S. (2010). All about me: Disclosure in online social networking profiles: The case of FACEBOOK. *Computers in Human Behavior*, 26(3), 406-418. <https://doi.org/10.1016/j.chb.2009.11.012>
- OECD. (2001). *Understanding digital divide*. OECD Publications.
- OECD. (2003a). *Privacy online: Policy and practical guidance* (Sy JT00137976; Working Party on Information Security and Privacy).
- OECD. (2003b). *The OECD privacy framework*. OECD. <https://www.oecd.org/digital/ieconomy/privacy-guidelines.htm>
- O'Harrow, R. (2005). *No place to hide*. Free Press.
- On Dört İlde Büyükşehir Belediyesi ve Yirmi Yedi İlçe Kurulması İle Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun, 6360 (2012). <https://www.mevzuat.gov.tr/MevzuatMetin/1.5.6360.pdf>

- O'Neill, B., & Dinh, T. (2012). *Digital literacy, digital opportunities* (Digital Childhoods Working Paper Series). Technological University Dublin.
- American Convention on Human Rights, B-32 (1969).
https://www.oas.org/dil/treaties_b-32_american_convention_on_human_rights.pdf
- Orwell, G. (2009). *Bin dokuz yüz seksen dört* (N. Akgören, Çev.). Can Yayınları.
- Özsoy, D., Akbulut, E., Atılgan, S. S., & Muschert, G. (2020). Digital skills and political participation in northeast Anatolia, Turkey. *First Monday*, 25(7).
<https://doi.org/10.5210/fm.v25i7.10854>
- Öztürk, G. (2021). Digital citizenship and its teaching: A literature review. *Journal of Educational Technology & Online Learning*, 4(1), 31-45.
- Paine, C., Reips, U.-D., Stieger, S., Joinson, A., & Buchanan, T. (2007). Internet users' perceptions of 'privacy concerns' and 'privacy actions'. *International Journal of Human-Computer Studies*, 65(6), 526-536.
<https://doi.org/10.1016/j.ijhcs.2006.12.001>
- Pala, Ş. M., & Başbüyük, A. (2020). 10-12 yaş grubu öğrencileri için dijital okuryazarlık ölçeği geliştirme çalışması. *Mediterranean Journal of Educational Research*, 14(33), 542-565. <https://doi.org/10.29329/mjer.2020.272.25>
- Palen, L., & Dourish, P. (2003). Unpacking "privacy" for a networked world. *New Horizons*, 5, 8.
- Pangrazio, L., & Sefton-Green, J. (2021). Digital rights, digital citizenship and digital literacy: What's the difference? *Journal of New Approaches in Educational Research*, 10(1), 15. <https://doi.org/10.7821/naer.2021.1.616>
- Pavone, V., & Esposti, S. D. (2012). Public assessment of new surveillance-oriented security technologies: Beyond the trade-off between privacy and security. *Public Understanding of Science*, 21(5), 556-572.
<https://doi.org/10.1177/0963662510376886>
- Petronio, S. (2002). *Boundaries of privacy: Dialectics of disclosure*. State University of New York Press.

- Petronio, S., Ellemers, N., Giles, H., & Gallois, C. (1998). (Mis)communicating across boundaries: Interpersonal and intergroup considerations. *Communication Research*, 25(6), 571-595. <https://doi.org/10.1177/009365098025006001>
- Petronio, S., & Kovach, S. (1997). Managing privacy boundaries: Health providers' perceptions of resident care in Scottish nursing homes. *Journal of Applied Communication Research*, 25(2), 115-131. <https://doi.org/10.1080/00909889709365470>
- Petronio, S., & Martin, J. N. (1986). Ramifications of revealing private information: A gender gap. *Journal of Clinical Psychology*, 42(3), 499-506. [https://doi.org/10.1002/1097-4679\(198605\)42:3<499::AID-JCLP2270420317>3.0.CO;2-I](https://doi.org/10.1002/1097-4679(198605)42:3<499::AID-JCLP2270420317>3.0.CO;2-I)
- Petronio, S., Reeder, H. M., Hecht, M. L., & Ros-Mendoza, T. M. (1996). Disclosure of sexual abuse by children and adolescents. *Journal of Applied Communication Research*, 24(3), 181-199. <https://doi.org/10.1080/00909889609365450>
- Pettman, D. (2017). *Sonsuz dikkat dağınıklığı* (Y. Çetin, Çev.; 1. bs). Sel Yayıncılık.
- Pew Research Center. (2014). *The future of privacy* (s. 79). <http://www.pewInternet.org/2014/12/18/future-of-privacy/>
- Pietraß, M. (2009). Digital literacy as “framing”: Suggestions for an interactive approach based on e. Goffman's frame theory. *Nordic Journal of Digital Literacy*, 4(3-4), 131-142.
- Pool, C. R. (1997). A new digital literacy: A conversation with paul gilster. *Educational Leadership*, 55(3), 6-11.
- Portulans Institute. (2020). *Network readiness index*. Network Readiness Index. <https://networkreadinessindex.org/>
- Poster, M. (1990). *The mode of information: Poststructuralism and social context*. University of Chicago Press.
- Potoglou, D., Dunkerley, F., Patil, S., & Robinson, N. (2017). Public preferences for internet surveillance, data retention and privacy enhancing services: Evidence from a pan-European study. *Computers in Human Behavior*, 75, 811-825. <https://doi.org/10.1016/j.chb.2017.06.007>

- Prensky, M. (2001a). Digital natives, digital immigrants part 1. *On the Horizon*, 9(5), 1-6. <https://doi.org/10.1108/10748120110424816>
- Prensky, M. (2001b). Digital natives, digital immigrants part 2: Do they really think differently? *On the Horizon*, 9(6), 1-6. <https://doi.org/10.1108/10748120110424843>
- PRISE. (2008). *PRISE statement paper*. http://www.prise.oeaw.ac.at/docs/PRISE_Statement_Paper.pdf
- Rachels, J. (1975). Why privacy is important. *Philosophy & Public Affairs*, 4(4), 323-333. JSTOR.
- Raguse, M., Meints, M., Langfeldt, O., & Peissl, W. (2008). *Criteria for privacy enhancing security technologies*.
- Raynes-Goldie, K. (2010). Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook. *First Monday*. <https://doi.org/10.5210/fm.v15i1.2775>
- Raynes-Goldie, K. (2012). *Privacy in the age of Facebook* [Doktora Tezi]. Curtin University.
- Reddy, P., Sharma, B., & Chaudhary, K. (2020). Digital literacy: A review of literature. *International Journal of Technoethics*, 11(2), 65-94. <https://doi.org/10.4018/IJT.20200701.oa1>
- Republic of Slovenia. (2016). *Digital Slovenia 2020—Development strategy for the information society until 2020*. <https://www.gov.si/assets/ministrstva/MJU/DID/Digital-Slovenia-2020-Development-Strategy-for-the-Information-Society-until-2020.pdf>
- Ribble, M. (2012). Digital citizenship for educational change. *Kappa Delta Pi Record*, 48(4), 148-151. <https://doi.org/10.1080/00228958.2012.734015>
- Ribble, M., & Bailey, G. D. (2007). *Digital citizenship in schools* (1st ed). International Society for Technology in Education.
- Richardson, J., & Milovidov, E. (2019). *Digital citizenship education handbook: Being online, well-being online, rights online*. Council of Europe.
- Rodríguez-de-Dios, I., & Igartua, J.-J. (2016). Skills of digital literacy to address the risks of interactive communication: *Journal of Information Technology Research*, 9(1), 54-64. <https://doi.org/10.4018/JITR.2016010104>

- Rodríguez-de-Dios, I., Igartua, J.-J., & González-Vázquez, A. (2016). Development and validation of a digital literacy scale for teenagers. *Proceedings of the Fourth International Conference on Technological Ecosystems for Enhancing Multiculturality - TEEM '16*, 1067-1072. <https://doi.org/10.1145/3012430.3012648>
- Rodríguez-de-Dios, I., van Oosten, J. M. F., & Igartua, J.-J. (2018). A study of the relationship between parental mediation and adolescents' digital skills, online risks and online opportunities. *Computers in Human Behavior*, 82, 186-198. <https://doi.org/10.1016/j.chb.2018.01.012>
- Roessler, B., & Mokrosinska, D. (2013). Privacy and social interaction. *Philosophy & Social Criticism*, 39(8), 771-791. <https://doi.org/10.1177/0191453713494968>
- RTÜK. (2018). *Televizyon izleme eğilimleri araştırması—2018*. <https://www.rtuk.gov.tr/assets/Icerik/AltSiteler/televizyonizlemeegilimleriarastirmasi2018.pdf>
- Ryberg, T., & Georgsen, M. (2010). Enabling digital literacy: Development of meso-level pedagogical approaches. *Nordic Journal of Digital Literacy*, 5(02), 88-100. <https://doi.org/10.18261/ISSN1891-943X-2010-02-02>
- Saeri, A. K., Ogilvie, C., Macchia, S. T. L., Smith, J. R., & Louis, W. R. (2014). Predicting Facebook users' online privacy protection: Risk, trust, norm focus theory, and the theory of planned behavior. *The Journal of Social Psychology*, 154(4), 352-369. <https://doi.org/10.1080/00224545.2014.914881>
- Sağiroğlu, Ş., Bülbül, H. İ., Kılıç, A., & Küçükali, M. (Ed.). (2020a). *Dijital okuryazarlık: Araçlar, metodolojiler, uygulamalar ve öneriler*. Nobel Akademik Yayıncılık.
- Sağiroğlu, Ş., Bülbül, H. İ., Kılıç, A., & Küçükali, M. (2020b). Dijital okuryazarlık ve ötesi. İçinde *Dijital Okuryazarlık: Araçlar, Metodolojiler, Uygulamalar ve Öneriler* (ss. 1-46). Nobel Akademik Yayıncılık.
- Saka, E. (Ed.). (2019). *Türkiye internet tarihi*. Alternatif Bilişim Derneği. https://ekitap.alternatifbilisim.org/files/ymc5_turkiye_internet_tarihi.pdf
- Salemink, K., Strijker, D., & Bosworth, G. (2017). Rural development in the digital age: A systematic literature review on unequal ICT availability, adoption, and use in

- rural areas. *Journal of Rural Studies*, 54, 360-371.
<https://doi.org/10.1016/j.jrurstud.2015.09.001>
- Sanayi ve Teknoloji Bakanlığı. (2020). *Türkiye’de kentsel ve kırsal yerleşim sistemleri araştırması (YER-SİS)*. <https://yersis.gov.tr/web#>
- Schaub, F., Balebako, R., & Cranor, L. F. (2017). Designing effective privacy notices and controls. *IEEE Internet Computing*, 1-1.
<https://doi.org/10.1109/MIC.2017.265102930>
- Scheerder, A., van Deursen, A. J. A. M., & van Dijk, J. A. G. M. (2017). Determinants of Internet skills, uses and outcomes. A systematic review of the second- and third-level digital divide. *Telematics and Informatics*, 34(8), 1607-1624.
<https://doi.org/10.1016/j.tele.2017.07.007>
- Schneier, B. (2006, Mayıs 18). The eternal value of privacy. *Wired*.
<https://www.wired.com/2006/05/the-eternal-value-of-privacy/>
- Searson, M., Hancock, M., Soheil, N., & Shepherd, G. (2015). Digital citizenship within global contexts. *Education and Information Technologies*, 20(4), 729-741.
<https://doi.org/10.1007/s10639-015-9426-0>
- Semiz Türkoğlu, H. (2018). Sosyal medya üzerinden mahremiyet farkındalığı ve değişimin ölçülenmesine yönelik bir araştırma. *Connectist: Istanbul University Journal of Communication Sciences*, 54, 163-189.
<https://doi.org/10.26650/CONNECTIST408216>
- Senkbeil, M., Ihme, J. M., & Wittwer, J. (2013). The test of technological and information literacy (TILT) in the national educational panel study: Development, empirical testing, and evidence for validity. *Journal for Educational Research Online*, 5(2), 139-161.
- Sezen, A., & Erden, M. (2018). Mahremiyetin psiko-sosyal yansımaları. *Dicle Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 10(20). http://www.e-dusbed.com/InstitutionArchiveFiles/c305be46-4d62-e711-80f0-00224d68272d/4ce9b3d4-4f62-e711-80f0-00224d68272d/Cilt10Sayi20/9d7cff7e-735e-4f04-9c01-72a0b5c59de8_20180308004.pdf

- Shapiro, J. J., & Hughes, S. K. (1996). Information literacy as a liberal art. *Educom Review*, 31(2).
- Shils, E. (1966). Privacy: Its constitution and vicissitudes. *Law and Contemporary Problems*, 31(2), 281. <https://doi.org/10.2307/1190672>
- Śliwińska, J. (2017). The network society and new forms of engagement. *Adeptus*, 10. <https://doi.org/10.11649/a.1494>
- Smith, Dinev, & Xu. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, 35(4), 989. <https://doi.org/10.2307/41409970>
- Soffer, T., & Cohen, A. (2014). Privacy perception of adolescents in a digital world. *Bulletin of Science, Technology & Society*, 34(5-6), 145-158. <https://doi.org/10.1177/0270467615578408>
- Solove, D. J. (2011). *Nothing to hide: The false tradeoff between privacy and security*. Yale University Press.
- Sparks, J. R., Katz, I. R., & Beile, P. M. (2016). Assessing digital information literacy in higher education: A review of existing frameworks and assessments with recommendations for next-generation assessment: assessing digital information literacy in higher education. *ETS Research Report Series*, 2016(2), 1-33. <https://doi.org/10.1002/ets2.12118>
- Stefanick, L. (2011). *Controlling knowledge: Freedom of information and privacy protection in a networked world*. AU Press.
- Stockemer, D. (2019). *Quantitative methods for the social sciences: A practical introduction with examples in SPSS and Stata*. Springer International Publishing. <https://doi.org/10.1007/978-3-319-99118-4>
- Stone, E. F., Gueutal, H. G., Gardner, D. G., & McClure, S. (1983). A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations. *Journal of Applied Psychology*, 68(3), 459-468. <https://doi.org/10.1037/0021-9010.68.3.459>
- Stratford, J. S., & Stratford, J. (1999). Data protection and privacy in the United States and Europe. *IASSIST Quarterly*, 22(3), 17. <https://doi.org/10.29173/iq80>

- Strauß, S. (2015). *Citizen summits on privacy, security and surveillance: Synthesis report* (D 6.10). <http://surprise-project.eu/wp-content/uploads/2015/02/SurPRISE-D6.10-Synthesis-report.pdf>
- Strickland, L. S., & Hunt, L. E. (2005). Technology, security, and individual privacy: New tools, new threats, and new public perceptions. *Journal of the American Society for Information Science and Technology*, 56(3), 221-234. <https://doi.org/10.1002/asi.20122>
- 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.
- Stutzman, F., Gross, R., & Acquisti, A. (2013). Silent listeners: The evolution of privacy and disclosure on Facebook. *Journal of Privacy and Confidentiality*, 4(2). <https://doi.org/10.29012/jpc.v4i2.620>
- Tabachnick, B. G., Fidell, L. S., & Ullman, J. B. (2019). *Using multivariate statistics* (Seventh edition). Pearson.
- Taddicken, M. (2014). The privacy paradox in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self disclosure. *Journal of Computer-Mediated Communication*, 19(2), 248-273. <https://doi.org/10.1111/jcc4.12052>
- Taneja, A., Vitrano, J., & Gengo, N. J. (2014). Rationality-based beliefs affecting individual's attitude and intention to use privacy controls on Facebook: An empirical investigation. *Computers in Human Behavior*, 38, 159-173. <https://doi.org/10.1016/j.chb.2014.05.027>
- Tate, R. (2009). *Google CEO: Secrets are for filthy people*. Gawker. <http://gawker.com/5419271/google-ceo-secrets-are-for-filthy-people>
- THE Consultancy. (2021). *Digital literacy in the UK*. https://www.timeshighereducation.com/sites/default/files/digital_literacy_in_the_uk_the_consultancy_report.pdf
- The Gallup Organization. (2008). *Data protection in the European Union citizens' perceptions* (Analytical Report Sy 225; Flash Eurobarometer). Directorate-

General Justice, Freedom and Security.
http://ec.europa.eu/public_opinion/index_en.htm

The World Bank. (2021, Ekim 28). *Individuals using the Internet (% of population)*.
https://data.worldbank.org/indicator/IT.NET.USER.ZS?most_recent_year_desc=true

TİAK. (2021). *Televizyon izleme ölçümü 2020 yılı*.
<https://tiak.com.tr/upload/files/2020yillik.pdf>

TNS Opinion & Social. (2011). *Attitudes on data protection and electronic identity in the European Union* (Sy 359; Special Eurobarometer). Directorate-General Justice, Information Society & Media and Joint Research Centre.
http://ec.europa.eu/public_opinion/index_en.htm

Tomczyk, Ł. (2020). Skills in the area of digital safety as a key component of digital literacy among teachers. *Education and Information Technologies*, 25(1), 471-486. <https://doi.org/10.1007/s10639-019-09980-6>

Tong, S. T., Van Der Heide, B., Langwell, L., & Walther, J. B. (2008). Too much of a good thing? The relationship between number of friends and interpersonal impressions on facebook. *Journal of Computer-Mediated Communication*, 13(3), 531-549. <https://doi.org/10.1111/j.1083-6101.2008.00409.x>

Townsend, L., Sathiaselan, A., Fairhurst, G., & Wallace, C. (2013). Enhanced broadband access as a solution to the social and economic problems of the rural digital divide. *Local Economy: The Journal of the Local Economy Policy Unit*, 28(6), 580-595. <https://doi.org/10.1177/0269094213496974>

Tufekci, Z. (2008). Can you see me now? Audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology & Society*, 28(1), 20-36. <https://doi.org/10.1177/0270467607311484>

TÜİK. (2012). *İstatistik göstergeler 1923-2011*. Türkiye İstatistik Kurumu.

TÜİK. (2013, Ağustos 22). *Hanehalkı bilişim teknolojileri kullanım araştırması, 2013*.
TÜİK. [https://data.tuik.gov.tr/Bulten/Index?p=Hanehalki-Bilisim-Teknolojileri-\(BT\)-Kullanim-Arastirmasi-2013-13569](https://data.tuik.gov.tr/Bulten/Index?p=Hanehalki-Bilisim-Teknolojileri-(BT)-Kullanim-Arastirmasi-2013-13569)

TÜİK. (2020). *Ulusal eğitim istatistikleri veri tabanı*.
<https://biruni.tuik.gov.tr/medas/?kn=130&locale=tr>

- TÜİK. (2021a, Nisan 2). *Yıllara ve cinsiyete göre il / ilçe merkezleri ve belde / köy nüfusu, genel nüfus sayımları—ADNKS*.
<https://data.tuik.gov.tr/Kategori/GetKategori?p=nufus-ve-demografi-109&dil=1>
- TÜİK. (2021b, Haziran 5). *İstatistiklerle aile, 2020*. TÜİK Kurumsal.
<https://data.tuik.gov.tr/Bulten/Index?p=Istatistiklerle-Aile-2020-37251>
- TÜİK. (2021c, Ağustos 26). *Hanehalkı bilişim teknolojileri (BT) kullanım araştırması, 2021*. TÜİK Kurumsal. [https://data.tuik.gov.tr/Bulten/Index?p=Hanehalki-Bilisim-Teknolojileri-\(BT\)-Kullanim-Arastirmasi-2021-37437](https://data.tuik.gov.tr/Bulten/Index?p=Hanehalki-Bilisim-Teknolojileri-(BT)-Kullanim-Arastirmasi-2021-37437)
- Türk Ceza Kanunu, 5237 (2004).
<https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5237.pdf>
- Türk Dil Kurumu (Ed.). (2011). *Türkçe sözlük* (11. bs). Atatürk Kültür, Dil ve Tarih Yüksek Kurumu, Türk Dil Kurumu.
- Türkiye Cumhuriyeti Anayasası, (1982).
<https://www.mevzuat.gov.tr/MevzuatMetin/1.5.2709.pdf>
- Uğraş, T. (2020). Bilgi okuryazarlığı. İçinde Ş. Sağıroğlu, H. İ. Bülbül, A. Kılıç, & M. Küçükali (Ed.), *Dijital Okuryazarlık: Araçlar, Metodolojiler, Uygulamalar ve Öneriler* (ss. 47-67). Nobel Akademik Yayıncılık.
- Ulukan, G. (2021, Ocak 14). *11 günde WhatsApp, Telegram ve BiP'in kullanıcı sayılarının değişimi*. Webrazzi. <https://webrazzi.com/2021/01/14/11-gunde-whatsapp-telegram-ve-bip-in-kullanici-sayilarinin-degisimi/>
- UNDP (Ed.). (2020). *The next frontier: Human development and the Anthropocene*. United Nations Development Programme.
- UNESCO. (2018). *A global framework of reference on digital literacy skills for indicator 4.4.2* (UIS/2018/ICT/IP/51; Information Paper No. 51). UNESCO.
<http://uis.unesco.org/sites/default/files/documents/ip51-global-framework-reference-digital-literacy-skills-2018-en.pdf>
- United Nations Human Rights. (1966). *International covenant on civil and political rights*. OHCHR | International Covenant on Civil and Political Rights.
<https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>
- Ural, A., & Kılıç, İ. (2013). *Bilimsel araştırma süreci ve SPSS ile veri analizi* (4. bs). Detay Yayıncılık.

- Uyar, A. (2021). Meslek yüksekokulu öğrencilerinin dijital okuryazarlık düzeyleri. *International Journal of Contemporary Educational Studies (IntJCES)*, 7(1), 198-211.
- Üstündağ, M. T., Güneş, E., & Bahçivan, E. (2017). Turkish adaptation of digital literacy scale and investigating pre-service science teachers' digital literacy. *Journal of Education and Future*, 12, 19-29.
- Vaidhyanathan, S. (2011). *The Googlization of everything: And why we should worry*. University of California Press.
- Van der Vlies, R. (2020). *Digital strategies in education across OECD countries: Exploring education policies on digital technologies* (Sy JT03465236; OECD Education Working Papers No 226).
- van Deursen, A. J. A. M., Helsper, E. J., & Eynon, R. (2014). *Measuring digital skills: From digital skills to tangible outcomes project report* (s. 50) [Project Report]. www.oii.ox.ac.uk/research/projects/?id=112
- van Deursen, A. J. A. M., & van Dijk, J. A. G. M. (2009). Using the Internet: Skill related problems in users' online behavior. *Interacting with Computers*, 21(5-6), 393-402. <https://doi.org/10.1016/j.intcom.2009.06.005>
- van Deursen, A. J. A. M., & van Dijk, J. A. G. M. (2010). Measuring internet skills. *International Journal of Human-Computer Interaction*, 26(10), 891-916. <https://doi.org/10.1080/10447318.2010.496338>
- van Deursen, A. J. A. M., & van Dijk, J. A. G. M. (2011). Internet skills and the digital divide. *New Media & Society*, 13(6), 893-911. <https://doi.org/10.1177/1461444810386774>
- van Deursen, A. J. A. M., & van Dijk, J. A. G. M. (2014). The digital divide shifts to differences in usage. *New Media & Society*, 16(3), 507-526. <https://doi.org/10.1177/1461444813487959>
- van Deursen, A. J. A. M., & van Dijk, J. A. G. M. (2015). New media and the digital divide. İçinde J. D. Wright (Ed.), *International Encyclopedia of the Social & Behavioral Sciences* (ss. 787-792). Elsevier. <https://doi.org/10.1016/B978-0-08-097086-8.95086-4>

- van Deursen, A. J. A. M., van Dijk, J. A. G. M., & Peters, O. (2011). Rethinking internet skills: The contribution of gender, age, education, Internet experience, and hours online to medium- and content-related Internet skills. *Poetics*, 39(2), 125-144. <https://doi.org/10.1016/j.poetic.2011.02.001>
- van Dijk, J. A. G. M. (2006). *The network society: Social aspects of new media* (2nd ed). Sage Publications.
- van Dijk, J. A. G. M. (2009). One Europe, digitally divided. İçinde A. Chadwick & P. N. Howard (Ed.), *Routledge handbook of Internet politics* (ss. 288-304). Routledge.
- van Dijk, J. A. G. M. (2017). *Ağ toplumu* (Ö. Sakin, Çev.; 3. bs). Epsilon Yayıncılık.
- van Dijk, J. A. G. M., & van Deursen, A. J. A. M. (2014). *Digital skills*. Palgrave Macmillan US. <https://doi.org/10.1057/9781137437037>
- van Dyke, C. (1987). Taking “computer literacy” literally. *Communications of the ACM*, 30(5), 366-374. <https://doi.org/10.1145/22899.22901>
- van Kolschooten, H., & de Ruijter, A. (2020). Covid-19 and privacy in the European Union: A legal perspective on contact tracing. *Contemporary Security Policy*, 1-14. <https://doi.org/10.1080/13523260.2020.1771509>
- van Laar, E., van Deursen, A. J. A. M., van Dijk, J. A. G. M., & de Haan, J. (2019). Determinants of 21st-century digital skills: A large-scale survey among working professionals. *Computers in Human Behavior*, 100, 93-104. <https://doi.org/10.1016/j.chb.2019.06.017>
- van Laar, E., van Deursen, A. J. A. M., van Dijk, J. A. G. M., & de Haan, J. (2020). Measuring the levels of 21st-century digital skills among professionals working within the creative industries: A performance-based approach. *Poetics*, 81, 101434. <https://doi.org/10.1016/j.poetic.2020.101434>
- van Manen, M. (2010). The pedagogy of momus technologies: Facebook, privacy, and online intimacy. *Qualitative Health Research*, 20(8), 1023-1032. <https://doi.org/10.1177/1049732310364990>
- Vega Caro, L., Vico Bosch, A., & Rebollo Catalán, Á. (2015). Motivaciones de uso de las redes sociales para el desarrollo del capital social de las mujeres de entorno

- rural. *Revista ICONO14 Revista científica de Comunicación y Tecnologías emergentes*, 13(2), 142-162. <https://doi.org/10.7195/ri14.v13i2.839>
- Vincent, D. (2017). *Mahremiyet kısa bir tarih* (D. C. Başaraner, Çev.; 1. bs). Epos Yayınları.
- Vogels, E. A. (2021, Ağustos 19). Some digital divides persist between rural, urban and suburban America. *Pew Research Center*. <https://www.pewresearch.org/fact-tank/2021/08/19/some-digital-divides-persist-between-rural-urban-and-suburban-america/>
- Wacks, R. (2010). *Privacy: A very short introduction*. Oxford University Press; e000xww.
<http://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=303971&lang=tr&site=ehost-live>
- Waldo, J., Lin, H., & Millett, L. I. (Ed.). (2007). *Engaging privacy and information technology in a digital age*. National Academies Press.
- Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, 4(5), 193-220. JSTOR. <https://doi.org/10.2307/1321160>
- We Are Social. (2021, Ekim 21). *Social media users pass the 4.5 billion mark*. We Are Social UK. <https://wearesocial.com/uk/blog/2021/10/social-media-users-pass-the-4-5-billion-mark/>
- Westin, A. F. (1967). *Privacy and freedom*. Atheneum.
<https://archive.org/details/privacyfreedom00west>
- Westin, A. F. (2003). Social and political dimensions of privacy. *Journal of Social Issues*, 59(2), 431-453. <https://doi.org/10.1111/1540-4560.00072>
- Wheless, L. R., & Grotz, J. (1976). Conceptualization and measurement of reported self-disclosure. *Human Communication Research*, 2(4), 338-346.
<https://doi.org/10.1111/j.1468-2958.1976.tb00494.x>
- Wikipedia. (2020). Relational dialectics. İçinde *Wikipedia*.
https://en.wikipedia.org/w/index.php?title=Relational_dialectics&oldid=993357488

- Wikipedia. (2021). Six degrees of separation. İçinde *Wikipedia*.
https://en.wikipedia.org/w/index.php?title=Six_degrees_of_separation&oldid=1051200104
- Woolf, V. (2017). *Kendine ait bir oda* (S. Öncü, Çev.; 19. bs). İletişim Yayınları.
- World Economic Forum. (2018). *The future of jobs report* [Insight Report]. World Economic Forum.
http://www3.weforum.org/docs/WEF_Future_of_Jobs_2018.pdf.
- Yabancı, C., Akça, F., & Ulutaş, E. (2018). Çevrimiçi mahremiyet kaygısı ve duygusal zekâ arasındaki ilişkinin incelenmesi. *Connectist: Istanbul University Journal of Communication Sciences*, 54, 191-218.
<https://doi.org/10.26650/CONNECTIST406310>
- Yılmaz, F., Acar, S., Bilen Kazancık, L., Gültekin, L., Meydan, M. C., Özsan, M. E., & Işık, M. (2019). *İlçelerin sosyo-ekonomik gelişmişlik sıralaması araştırması SEGE-2017*. Türkiye Cumhuriyeti Sanayi ve Teknoloji Bakanlığı.
<https://yersis.gov.tr/web/File/ilce-sege-2017.pdf>
- Young, A. L., & Quan-Haase, A. (2013). Privacy protection strategies on Facebook. *Information, Communication & Society*, 16(4), 479-500.
<https://doi.org/10.1080/1369118X.2013.777757>
- Yücedağ, N. (2019). Kişisel verilerin korunması kanunu kapsamında genel ilkeler. *Kişisel Verileri Koruma Dergisi*, 1(1), 47-63.
- Yüksel Civelek, D. (2011). *Kişisel verilerin korunması ve bir kurumsal yapılanma önerisi* [Uzmanlık Tezi]. http://www.bilgitoplumu.gov.tr/wp-content/uploads/2014/04/Kisisel_Verilerin_Korunmasi-Dilek_Civelek-DPT_Uzmanlik_Tezi.pdf
- Yüksel, M. (2003). Mahremiyet hakkı ve sosyo—Tarihsel gelişimi. *Ankara Üniversitesi SBF Dergisi*, 58(01). https://doi.org/10.1501/SBFder_0000001619
- Yüksel, M. (2009). Mahremiyet hakkına ve bireysel özgürlüklere felsefi yaklaşımlar. *Ankara Üniversitesi SBF Dergisi*, 64(01), 275-298.
https://doi.org/10.1501/SBFder_0000002130
- Zengin, A., Zengin, G., & Altunbaş, H. (2015). Sosyal medya ve değişen mahremiyet “facebook mahremiyeti (Social media and the changing privacy “facebook

- privacy). *Gümüşhane Üniversitesi İletişim Fakültesi Elektronik Dergisi*, 3(2).
<https://doi.org/10.19145/guifd.11157>
- Zengin, M. O., & Zengin, İ. (2015). Facebook'ta güvenlik davranışı ve mahremiyet kaygısı: İstanbul'da yaşayan kullanıcılara ilişkin bir araştırma. *Uluslararası Hakemli İletişim ve Edebiyat Araştırmaları Dergisi*, 6, 1-33.
- Zhang, C., Sun, J., Zhu, X., & Fang, Y. (2010). Privacy and security for online social networks: Challenges and opportunities. *IEEE Network*, 24(4), 13-18.
<https://doi.org/10.1109/MNET.2010.5510913>
- Zhang, R., & Fu, J. S. (2020). Privacy management and self-disclosure on social network sites: The moderating effects of stress and gender. *Journal of Computer-Mediated Communication*, 25(3), 236-251. <https://doi.org/10.1093/jcmc/zmaa004>
- Zhang, Y., & Espinoza, S. (1997). Affiliations of computer self-efficacy and attitudes with need for learning computer skills. *Journal of Educational Computing Research*, 17(4), 371-383. <https://doi.org/10.2190/3GNY-APR6-51Q8-402N>
- Zhao, S., Grasmuck, S., & Martin, J. (2008). Identity construction on Facebook: Digital empowerment in anchored relationships. *Computers in Human Behavior*, 24(5), 1816-1836. <https://doi.org/10.1016/j.chb.2008.02.012>
- Zher, S. Y. (2017, Kasım). *Developing a digital literacy scale & measuring digital divide using PIAAC data*. 4th PIAAC International Conference Singapore 21- 23 November 2017. https://www.ial.edu.sg/content/dam/projects/tms/ial/Access-research/piaac/YeeZherSheng_SanChyeCheng_Developing%20a%20digital%20literacy%20scale%20and%20measuring%20digital%20divide%20using%20PIAAC%20data.pdf
- Zuboff, S. (1988). *In the age of the smart machine: The future of work and power*. Basic Books.

EKLER

EK 1: Araştırmada Kullanılan Anket Soruları

Merhaba. Bu saha araştırması, Erciyes Üniversitesi Sosyal Bilimler Enstitüsü İletişim Bilimleri Anabilim Dalı'nda, **Arş. Gör. Burak ÜNLÜ** tarafından hazırlanan doktora tezi için yapılmaktadır. Ankette kimlik bilgileriniz sorulmamaktadır. Bu çalışmaya katılmak tamamen gönüllülük esasına dayanmaktadır. Çalışmaya katılmama veya katıldıktan sonra herhangi bir anda çalışmadan çıkma hakkında sahipsiniz. Çalışmayı yanıtlamanız, **araştırmaya katılım için onam verdiğiniz biçiminde yorumlanacaktır**. Size verilen formlardaki soruları yanıtlarken kimsenin baskısı veya telkini altında olmayınız. Bu formlardan elde edilecek bilgiler tamamen araştırma amacı ile kullanılacaktır.

Zaman ayırdığınız ve bilimsel bir çalışmaya katkıda bulunduğunuz için teşekkür ederiz.

Aşağıda belirtilen ifadelere ne oranda katılıyorsunuz?	Hiç Katılmıyorum	Katılmıyorum	Kısmen Katılıyorum	Katılıyorum	Kesinlikle Katılıyorum
Kullandığım teknolojilerle ilgili karşılaştığım teknik problemleri (telefonun/bilgisayarın takılması, internete bağlanamaması gibi) nasıl çözeceğimi bilirim.	1	2	3	4	5
Yeni teknolojileri kolayca öğrenebilirim.	1	2	3	4	5
Önemli yeni teknolojileri takip ederim.	1	2	3	4	5
Birçok farklı teknoloji hakkında bilgi sahibiyim.	1	2	3	4	5
Bilgi ve iletişim teknolojilerini iletişim kurma ve bilgiye erişme amaçlı kullanmak ve edindiğim bilgileri sergileyebileceğim dijital içerikler (Facebook, Twitter, Instagram paylaşımları, wikiler, bloglar, yorumlar) üretmek için gereken teknik becerilere sahibim.	1	2	3	4	5
Bilgi ve iletişim teknolojileri konusunda sahip olduğum beceriler (akıllı cep telefonunu sorun yaşamadan kullanma, sosyal medyada içerik paylaşma, fotoğraf çekme vb.) yeterlidir.	1	2	3	4	5
İnternette bilgi edinmek için yaptığım arama ve değerlendirmelerde kendime güvenirim.	1	2	3	4	5
Siber güvenlik, webde arama ve internette sahtecilik ile ilişkili konular hakkında bilgi sahibiyim.	1	2	3	4	5
Bilgi ve iletişim teknolojileri, yakın çevremle ve akranlarımla daha iyi işbirliği yapmamı ve iletişim kurmamı sağlar.	1	2	3	4	5
Yakın çevremle, akranlarımla ya da arkadaşlarımla internet üzerinden (ör. Facebook, Twitter, WhatsApp, Bloglar aracılığıyla) sıklıkla yardımlaşırım.	1	2	3	4	5

Aşağıda belirtilen ifadelere ne oranda katılıyorsunuz?	Hiç Katılmıyorum	Katılmıyorum	Kısmen Katılmıyorum	Katılıyorum	Kesinlikle Katılıyorum
İnsanlar kişisel verilerin suistimal edilmesine karşı yasal olarak korunmalıdırlar.	1	2	3	4	5
Mahremiyet (gizlilik) ile ilgili yasalar, kişilerin özel yaşamlarını koruyacak şekilde güçlendirilmelidir.	1	2	3	4	5
Eğer bugün bir anayasa yazacak olsaydım büyük ihtimalle kişisel mahremiyeti temel hak olarak eklerdim.	1	2	3	4	5
Kişisel bilgilerimi istediğimden daha fazla kişi ile paylaşmış olmak beni kaygılandırıyor.	1	2	3	4	5
Kimlik bilgilerini paylaşmanın sonuçları hakkında endişeliyim (kaygılıyım).	1	2	3	4	5
Etrafımdakilerin özel hayatım hakkında gereğinden fazla bilgiye sahip olduklarından endişeliyim (kaygılıyım).	1	2	3	4	5
Kişisel bilgilerimin detaylarını birisiyle paylaştığım zaman diğer insanlarla bunları paylaşacağı hakkında endişe duyarım.	1	2	3	4	5
Kendileri dikkat etmiyorsa bile, başkalarının mahremiyetine saygı göstermek benim için önemlidir.	1	2	3	4	5
Kendimin mahremiyeti kadar diğer insanların mahremiyetine de değer veriyorum.	1	2	3	4	5
Başkalarının özel hayatlarına karışmamak için her zaman elimden geleni yaparım.	1	2	3	4	5
Başkalarının mahremiyetine saygı, sosyal ilişkilerde önemli bir öncelik olmalıdır.	1	2	3	4	5
Bir kişi kendi mahremiyetini korumaya özen göstermiyorsa bile, ben elimden geldiğince o kişinin özel yaşamına burun sokmamaya çalışırım.	1	2	3	4	5
Çevremdeki insanların kendi hayatlarının mahremiyetine (gizliliğine) ne kadar özen gösterdikleri benim özelimin ne kadar korunabileceğini etkiler.	1	2	3	4	5
Kendi özel yaşamları hakkındaki detayları herkesle paylaşan birine sırdaş olarak güvenemem .	1	2	3	4	5
Özel hayatımın mahremiyetinin güvende olması için, arkadaşlarımda kendi özel hayatları hakkında dikkatli olması gerekir.	1	2	3	4	5
Kendi özel hayatını korumaya özen göstermeyen kişilerin benim özel hayatıma saygı göstereceğine güvenmiyorum.	1	2	3	4	5

Sosyal medya kullanmıyorsanız aşağıdaki iki soruyu boş bırakınız.

Sosyal medya uygulamalarında (Facebook, Instagram, Twitter vb.) gizliliği korumak için sunulan varsayılan seçeneklerin...

() Hiçbirini değiştirmedim. () Birazını değiştirdim. () Tamamını değiştirdim.

Sosyal medya profilleriniz ile ilgili en uygun seçeneği işaretleyiniz. (Sosyal medya profilleriniz)

- () Hesabım gizli, sadece onayladığım takipçiler paylaşımlarımı görebiliyor.
 () Hesabım herkese açık, ama kişisel paylaşımlarımı sadece “Yakın Arkadaşlar” kategorisindekilere ya da belirlediğim arkadaş gruplarına açık olarak paylaşıyorum.
 () Hesabım herkese açık ve paylaştıklarımı herkes görebilir.

Aşağıdaki sosyal medya, anlık mesajlaşma ve kamu hizmeti uygulamaları ile teknolojilerden hangilerini, ne sıklıkla kullanıyorsunuz?	Hiç Kullanmam	Nadiren Kullanırım	Ara Sıra Kullanırım	Çoğu Zaman Kullanırım	Her Zaman Kullanırım
Facebook	1	2	3	4	5
Twitter	1	2	3	4	5
Instagram	1	2	3	4	5
Tiktok	1	2	3	4	5
YouTube	1	2	3	4	5
Snapchat	1	2	3	4	5
LinkedIn	1	2	3	4	5
BİP	1	2	3	4	5
Telegram (ve diğer anlık mesajlaşma uyg.)	1	2	3	4	5
E-Devlet	1	2	3	4	5
Hayat Eve Sığar	1	2	3	4	5
MHRS (Merkezi Hekim Randevu Sistemi)	1	2	3	4	5
E-Nabız	1	2	3	4	5
İnternet (ev ya da mobil)	1	2	3	4	5
Cep Telefonu	1	2	3	4	5
Bilgisayar (Laptop ya da Masaüstü)	1	2	3	4	5
Tablet	1	2	3	4	5
Televizyon	1	2	3	4	5

Bu uygulamaları ve teknolojileri kullanma sıklığınız pandemi sürecinde değişti mi?	Artık daha az kullanıyorum	Hayır, bir değişiklik olmadı.	Evet, eskisine göre daha fazla kullanıyorum
Facebook	1	2	3
Twitter	1	2	3
Instagram	1	2	3
Tiktok	1	2	3
YouTube	1	2	3
Snapchat	1	2	3
LinkedIn	1	2	3
BİP	1	2	3
Telegram (ve diğer anlık mesajlaşma uyg.)	1	2	3
E-Devlet	1	2	3
Hayat Eve Sığar	1	2	3
MHRS (Merkezi Hekim Randevu Sistemi)	1	2	3
E-Nabız	1	2	3
İnternet (ev ya da mobil)	1	2	3
Cep Telefonu	1	2	3
Bilgisayar (Laptop ya da Masaüstü)	1	2	3
Tablet	1	2	3
Televizyon	1	2	3

WhatsApp, BİP ya da diğer anlık mesajlaşma programlarından herhangi birini kullanmıyorsanız aşağıdaki üç soruyu boş bırakınız.

WhatsApp, BİP ya da diğer anlık mesajlaşma programlarındaki “Son Görülme” özelliğini...

- ☐ Devre dışı bıraktım.
- ☐ Kullanıyorum.
- ☐ Böyle bir özellik olduğunu bilmiyorum.

WhatsApp, BİP ya da diğer anlık mesajlaşma programlarındaki “mavi tik” (gönderilen mesajın okunup okunmadığını belirten işaret) özelliğini...

- ☐ Devre dışı bıraktım.
- ☐ Kullanıyorum.
- ☐ Böyle bir özellik olduğunu bilmiyorum.

WhatsApp, BİP ya da diğer anlık mesajlaşma programları üzerinden kimlerle iletişim kurarsınız?

(Birden fazla seçeneği işaretleyebilirsiniz)

- ☐ Annemle ☐ Babamla
- ☐ Kardeşlerimle ☐ Eşimle
- ☐ Evlatlarımla ☐ Arkadaşlarımla
- ☐ Aynı köyde ikamet ettiğimiz akrabalarımla ☐ Şehir dışında ikamet eden akrabalarımla
- ☐ Yurt dışında ikamet eden akrabalarımla

İnternete ilk ne zaman bağlandınız? (Yıl olarak belirtiniz) _____

İnternete ilk olarak hangi cihazla bağlandınız?

- ☐ Kendi evimdeki bilgisayardan
- ☐ İnternet Cafe’deki bilgisayardan
- ☐ Cep telefonumdan
- ☐ Hatırlamıyorum
- ☐ Diğer (lütfen belirtiniz) _____

Ev ya da mobil internet aboneliğiniz var mı?

- ☐ Hiçbir internet aboneliğim yok.
- ☐ Sadece ev interneti aboneliğim var.
- ☐ Sadece mobil internet (cep telefonu) aboneliğim var.
- ☐ Hem ev interneti hem de mobil internet aboneliğim var.

İlk cep telefonumu _____ yılında; ilk akıllı cep telefonumu da _____ yılında satın aldım.

Akıllı cep telefonunuzun bir şifresi var mı? ☐ Evet ☐ Hayır

Cihazınızı şifresiz kullanıyorsanız aşağıdaki soruyu boş bırakınız.

Şifrenizi sizden başka... (Birden fazla seçenek işaretleyebilirsiniz)

- ☐ Kimse bilmiyor.
- ☐ Annem ya da babam biliyor.
- ☐ Çocuklarım biliyor.
- ☐ Eşim biliyor.
- ☐ Çevremdeki çoğu kişi biliyor.

Sosyal ağ profillerinizde ve genel olarak internette aşağıdaki bilgilerden hangilerini paylaşıyorsunuz?	Hayır	Evet
Adınız, soyadınız	1	2
E-posta adresiniz	1	2
Yaşadığınız yer	1	2
Telefon numaranız	1	2
Eğitim durumunuz	1	2
Cinsiyetiniz	1	2
Memleketiniz	1	2
Doğum tarihiniz	1	2
Fotoğraflarınız	1	2
Mesleğiniz	1	2
İlişki durumunuz	1	2
İlgi alanlarınız	1	2
Siyasi görüşünüz	1	2

Aşağıda belirtilen ifadelere ne oranda katılıyorsunuz?	Hiç Katılmıyorum	Katılmıyorum	Kısmen Katılıyorum	Katılıyorum	Kesinlikle Katılıyorum
İhtiyacım olan bilgiyi bulmak için interneti kullanırım.	1	2	3	4	5
Benim için faydalı olan uygulamaları internette bulabilir ve indirebilirim.	1	2	3	4	5
Dijital teknolojileri (akıllı telefon, tablet, bilgisayar vb.) kullanarak ne zaman istersem internete erişebilirim.	1	2	3	4	5
Sosyal ya da politik konularda interneti kullanarak daha çok bilgi edinirim.	1	2	3	4	5
Düşüncelerimi, hislerimi, görüşlerimi ifade etmek için internette özgün mesaj, ses, görüntü ya da videolar paylaşıyorum.	1	2	3	4	5

İnternet üzerinden alışveriş yapar mısınız? () Evet () Hayır

Eğitim durumunuz

() İlkokul mezunu () Ortaokul mezunu () Lise mezunu
() Üniversite mezunu () Lisansüstü

Doğum yılınız: _____

Cinsiyetiniz: () Erkek () Kadın

Mesleğiniz: _____

Medeni haliniz: () Evli () Bekar () Diğer (Lütfen belirtiniz) _____

EK 2: Etik Kurul Onayı

Bu çalışma için etik kurul onayı Erciyes Üniversitesi Sosyal ve Beşerî Bilimler Etik Kurulu'nun 29/06/2021 tarihli ve 326 numaralı kararı ile alınmıştır.

