



AKDENİZ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ



Gizem ERMUMCU

ÜNİVERSİTE ÖĞRENCİLERİNDE DİJİTAL MAHREMİYET FARKINDALIĞI VE
SİBER MAĞDURİYET ARASINDAKİ İLİŞKİNİN İNCELENMESİ

Sosyal Hizmet Anabilim Dalı
Yüksek Lisans Tezi

Antalya, 2025



AKDENİZ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ



Gizem ERMUMCU

ÜNİVERSİTE ÖĞRENCİLERİNDE DİJİTAL MAHREMİYET FARKINDALIĞI VE
SİBER MAĞDURİYET ARASINDAKİ İLİŞKİNİN İNCELENMESİ

Danışman

Doç. Dr. Sinem Burcu UĞUR

İkinci Danışman

Dr. Öğr. Üyesi Nehir YASAN AK

Sosyal Hizmet Anabilim Dalı

Yüksek Lisans Tezi

Antalya, 2025

T.C.
Akdeniz Üniversitesi
Sosyal Bilimler Enstitüsü Müdürlüğüne,

Gizem ERMUMCU'nun bu çalışması, jürimiz tarafından Sosyal Hizmet Anabilim Dalı Yüksek Lisans Programı tezi olarak kabul edilmiştir.

Başkan : Prof. Dr. Arif AYTEKİN (İmza)

Üye (Danışman) : Doç. Dr. Sinem Burcu UĞUR (İmza)

Üye : Doç. Dr. Elif BAŞ (İmza)

Üye : (İmza)

Üye : (İmza)

Tez Başlığı: Üniversite Öğrencilerinde Dijital Mahremiyet Farkındalığı ve Siber Mağduriyet Arasındaki İlişkinin İncelenmesi

Onay: Yukarıdaki imzaların, adı geçen öğretim üyelerine ait olduğunu onaylarım.

Tez Savunma Tarihi :27/06/2025

Mezuniyet Tarihi : 31/07/2025

AKADEMİK BEYAN

Yüksek Lisans Tezi olarak sunduğum “Üniversite Öğrencilerinde Dijital Mahremiyet Farkındalığı ve Siber Mağduriyet Arasındaki İlişkinin İncelenmesi” adlı bu çalışmanın, akademik kural ve etik değerlere uygun bir biçimde tarafımdan yazıldığını, yararlandığım bütün eserlerin kaynakçada gösterildiğini ve çalışma içerisinde bu eserlere atıf yapıldığını belirtir; bunu şerefimle doğrularım.

Gizem ERMUMCU





T.C.
AKDENİZ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ



23/07/2025

TEZ ÇALIŞMASI ORJİNALLİK RAPORU BEYAN BELGESİ

Öğrenci Bilgileri	
Adı-Soyadı	Gizem ERMUMCU
Öğrenci Numarası	202252107003
Anabilim Dalı	Sosyal Hizmet
Programı	Yüksek Lisans
Danışman Öğretim Üyesi Bilgileri	
Unvanı, Adı-Soyadı	Doç. Dr. Sinem Burcu UĞUR
Doktora Tez/Yüksek Lisans Tez/Dönem Projesi Başlığı	Üniversite Öğrencilerinde Dijital Mahremiyet Farkındalığı ve Siber Mağduriyet Arasındaki İlişkinin İncelenmesi
Turnitin Bilgileri	
Ödev Numarası	2719418757
Rapor Tarihi	23/07/2025
Benzerlik Oranı	Alıntılar hariç: %.8.... Alıntılar dahil: %.9....
SOSYAL BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜNE,	
Yukarıda bilgileri bulunan öğrenciye ait tez çalışmasının a) Kapak sayfası, b) Giriş, c) Ana Bölümler ve d) Sonuç kısımlarından oluşan toplam 90 sayfalık kısmına ilişkin olarak Turnitin adlı intihal tespit programından Sosyal Bilimler Enstitüsü Tez Çalışması Orijinallik Raporu Alınması ve Kullanılması Uygulama Esaslarında belirlenen filtrelemeler uygulanarak yukarıdaki detayları verilen ve ekte sunulan rapor alınmıştır. Danışman tarafından uygun olan seçenek işaretlenmelidir: () Benzerlik oranları belirlenen limitleri aşmıyor ise: Yukarıda yer alan beyanın ve ekte sunulan Tez Çalışması Orijinallik Raporunun doğruluğunu onaylarım. () Benzerlik oranları belirlenen limitleri aşıyor, ancak tez/dönem projesi danışmanı intihal yapılmadığı kanısında ise: Yukarıda yer alan beyanın ve ekte sunulan Tez Çalışması Orijinallik Raporunun doğruluğunu onaylar ve Uygulama Esaslarında öngörülen yüzdeleri sınırlarının aşılmasına karşın, aşağıda belirtilen gerekçe ile intihal yapılmadığı kanısında olduğumu beyan ederim.	
Gerekçe:	
Benzerlik taraması yukarıda verilen ölçütlere uygun olarak tarafımda yapılmıştır. İlgili tezin orijinallik raporunun uygun olduğunu beyan ederim. Danışman Öğretim Üyesi Doç. Dr. Sinem Burcu UĞUR	

İÇİNDEKİLER

ŞEKİLLER LİSTESİ	v
TABLolar LİSTESİ	vi
KISALTMALAR LİSTESİ	vii
TANIMLAR LİSTESİ	viii
ÖZET	ix
SUMMARY	x
TEŞEKKÜR / ÖNSÖZ.....	xi
GİRİŞ.....	1

BİRİNCİ BÖLÜM

ARAŞTIRMANIN KAVRAMSAL TEMELLERİ

1.1. Mahremiyet Kavramı ve Gelişimi	5
1.1.1. Mahremiyetin Tanımı ve Tarihsel Gelişimi.....	6
1.1.2. Mahremiyetin Türleri ve Boyutları.....	7
1.2. Dijital Mahremiyet Kavramı	8
1.2.1. Dijital Mahremiyetin Tanımı ve Önemi	9
1.2.2. Dijital Mahremiyetin Boyutları	11
1.2.2.1. Bilgi (Veri) Mahremiyeti	12
1.2.2.2. İletişim Mahremiyeti.....	12
1.2.2.3. Davranışsal Mahremiyet / Dijital Ayak İzi	13
1.2.2.4. Mekânsal Mahremiyet (Dijital Uzamda)	13
1.2.3. Dijital Mahremiyetin İhlal Riskleri ve Korunma Stratejileri.....	14
1.3. Dijital Mahremiyet Farkındalığı.....	16
1.3.1. Farkındalık Kavramı ve Bileşenleri.....	16
1.3.2. Gençlerde Dijital Mahremiyet Farkındalığı ve Koruma Davranışları	16
1.3.2.1. Sosyo-Demografik Değişkenlere Göre Mahremiyet Farkındalığı	17
1.3.2.2. İnternet Kullanım Alışkanlıkları ve Mahremiyet Farkındalığı	19
1.4. Siber Zorbalık ve Siber Mağduriyet	22
1.4.1. Siber Zorbalık: Dijital Mağduriyetin Kaynağı Olarak Bir Şiddet Biçimi	23
1.4.2. Siber Mağduriyet Tanımı ve Tarihsel Kökeni	24

1.4.3. Siber Mağduriyet Türleri	25
1.4.4. Siber Mağduriyet Nedenleri.....	26
1.4.5. Siber Mağduriyet Sonuçları	28

İKİNCİ BÖLÜM

KURAMSAL ÇERÇEVE: GÜÇLENDİRME KURAMI BAĞLAMINDA DİJİTAL MAHREMİYET VE MAĞDURİYET

2.1. Güçlendirme Kuramı: Tanım ve Temel Kavramları	31
2.2. Gençlerde Dijital Farkındalık ve Bireysel Güçlenme.....	33
2.3. Güçlenmenin Zorbalık ve Mağduriyetle Mücadelede Rolü	35
2.4. Güçlendirme Kuramının Bu Araştırmaya Uyarlanması	38

ÜÇÜNCÜ BÖLÜM

ARAŞTIRMANIN TASARIMI VE VERİLERİN ÇÖZÜMLENMESİ

3.1. Araştırmanın Konusu, Önemi ve Amacı	40
3.2. Araştırmanın Yöntemi	43
3.2.1. Araştırmanın Modeli.....	43
3.2.2. Araştırma Evren ve Örneklemi	44
3.2.3. Veri Toplama Süreci	45
3.2.3.1. Veri Toplama Araçları	45
3.2.3.1.1. Demografik Bilgiler Bölümü.....	46
3.2.3.1.2. Üniversite Öğrencileri İçin Sanal Zorbalık/Mağduriyet Envanteri	46
3.2.3.1.3. Çevrim İçi Mahremiyet Farkındalık Ölçeği	47
3.2.4. Araştırma Etiği.....	48
3.2.5. Veri Analizi.....	49
3.2.6. Araştırmanın Varsayım ve Sınırlılıkları	50
3.3. Araştırma Bulgularının Değerlendirilmesi	51
3.3.1. Sosyo-Demografik Özelliklere ve İnternet Kullanım Alışkanlıklarına İlişkin Bulgular	51
3.3.2. Araştırma Sorusu 1: Üniversite Öğrencilerinin Siber Zorbalık/Mağduriyet ve Çevrim İçi Mahremiyet Farkındalık Düzeyleri	57

3.3.2.1. Üniversite Öğrencilerinin Siber Zorbalık ve Siber Mağduriyet Seviyeleri	57
3.3.2.2. Üniversite Öğrencilerinin Çevrim İçi Mahremiyet Farkındalık Seviyeleri	58
3.3.3. Araştırma Sorusu 2: Üniversite Öğrencilerinin Siber Zorbalık ve Mağduriyet ile Çevrimiçi Mahremiyet Genel ve Alt Boyut Puanları Arasında İlişki.....	60
3.3.4. Araştırma Sorusu 3: Üniversite Öğrencilerinin Sanal Zorbalık/Mağduriyet ve Çevrim İçi Mahremiyet Farkındalık Genel ve Alt Boyut Puanlarının Cinsiyete Göre Farklılaşması	61
3.3.4.1.1. Üniversite Öğrencilerinin Sanal Zorbalık ve Sanal Mağduriyet Puanlarının Cinsiyete Göre Farklılaşması	62
3.3.4.1.2. Üniversite Öğrencilerinin Çevrim İçi Mahremiyet Farkındalık Genel ve Alt Boyut Puanlarının Cinsiyete Göre Farklılaşması	62
3.3.5. Araştırma Sorusu 4: Üniversite Öğrencilerinin Sanal Zorbalık/Mağduriyet ve Çevrim İçi Mahremiyet Farkındalık Genel ve Alt Boyut Puanlarının Sınıf Düzeylerine Göre Farklılaşması.....	63
3.3.5.1. Üniversite Öğrencilerinin Sanal Zorbalık ve Sanal Mağduriyet Puanlarının Sınıf Düzeyine Göre Farklılaşması.....	63
3.3.5.2. Üniversite Öğrencilerinin Çevrim İçi Mahremiyet Farkındalık Genel ve Alt Boyut Puanlarının Sınıf Düzeyine Göre Farklılaşması.....	64
3.3.6. Araştırma Sorusu 5: Üniversite Öğrencilerinin Çeşitli Değişkenler (Demografik Özellikler ve İnternet Kullanım Alışkanlıkları) ile Sanal Zorbalık/Mağduriyet ve Çevrim İçi Mahremiyet Farkındalık Puanları Arasındaki İlişki	65
3.3.6.1. Üniversite Öğrencilerinin Yaşları ile Sanal Zorbalık, Sanal Mağduriyet, Çevrim İçi Mahremiyet Farkındalık Genel ve Alt Boyut Puanları Arasındaki İlişki	66
3.3.6.2. Üniversite Öğrencilerinin Günlük İnternet Kullanım Süreleri ile Sanal Zorbalık, Sanal Mağduriyet, Çevrim İçi Mahremiyet Farkındalık Genel ve Alt Boyut Puanları Arasındaki İlişki	66
3.3.6.3. Üniversite Öğrencilerinin Akademik İnternet Kullanım ile Sanal Zorbalık, Sanal Mağduriyet, Çevrim İçi Mahremiyet Farkındalık Genel ve Alt Boyut Puanları Arasındaki İlişki	67
3.3.6.4. Üniversite Öğrencilerinin Sosyal Medya Kullanım Süreleri ile Sanal Zorbalık, Sanal mağduriyet, Çevrim İçi Mahremiyet Farkındalık Genel ve Alt Boyut Puanları Arasındaki İlişki.....	68
3.4. Tartışma	69

SONUÇ	77
KAYNAKÇA.....	80
EK 1- Kişisel Bilgi Formu	100
EK 2- Üniversite Öğrencileri İçin Siber Zorbalık/Mağduriyet Ölçeği.....	101
EK 3- Çevrimiçi Mahremiyet Farkındalık Ölçeği.....	102
ÖZGEÇMİŞ	103



ŞEKİLLER LİSTESİ

Şekil 3.1 Üniversite öğrencilerinin internete girme araçlarının kullanım dağılımı.....53



TABLOLAR LİSTESİ

Tablo 3.1 Veri Toplama Araçları.....	46
Tablo 3.2 SZ/SM Envanterinin Örnek Maddeleri.....	47
Tablo 3.3 ÇMFÖ Örnek Maddeleri	48
Tablo 3.4 Katılımcıların Sosyo-Demografik Özelliklerine ve İnternet Kullanım Alışkanlıklarına Göre Dağılımı (N = 560).....	52
Tablo 3.5 Katılımcıların İnternete Erişim Sağladığı Cihazların Dağılımı (N = 560).....	53
Tablo 3.6 Katılımcıların Kullandıkları Sosyal Medya Platformları (N = 560).....	54
Tablo 3.7 Katılımcıların İnternet Kullanım Amaçlarına Göre Dağılımı (N = 560)	55
Tablo 3.8 Katılımcıların Sosyal Medya Kullanım Amaçlarına Göre Dağılımı (N = 560).....	56
Tablo 3.9 Siber Zorbalık ve Siber Mağduriyet Envanterinin Maddelerinin Tanımlayıcı İstatistik Değerleri.....	58
Tablo 3.10 Çevrim İçi Mahremiyet Farkındalık Ölçeği Maddelerinin Tanımlayıcı İstatistik Değerleri.....	59
Tablo 3.11 Üniversite Öğrencilerinin Siber Zorbalık ve Mağduriyet ile Çevrim İçi Mahremiyet Genel ve Alt Boyut Puanları Arasında İlişki Tablosu	61
Tablo 3.12 Üniversite Öğrencilerinin Cinsiyetlerine Göre Sanal Zorbalık ve Sanal Mağduriyet Puanları Arasında Karşılaştırma Tablosu.....	62
Tablo 3.13 Üniversite Öğrencilerinin Cinsiyetlerine Göre Çevrim İçi Mahremiyet Genel ve Alt Boyutları Puanları Arasında Karşılaştırma Tablosu	63
Tablo 3.14 Üniversite Öğrencilerinin Sınıf Düzeylerine göre Çevrim İçi Mahremiyet Genel ve Alt Boyutları Puanları Arasında Karşılaştırma Tablosu	64
Tablo 3.15 Üniversite Öğrencilerinin Sınıf Düzeylerine göre Çevrim İçi Mahremiyet Genel ve Alt Boyutları Puanları Arasında Karşılaştırma Tablosu	65
Tablo 3.16 Üniversite Öğrencilerinin Yaşları ile Sanal Zorbalık, Sanal Mağduriyet, Çevrim İçi Mahremiyet Farkındalık Genel ve Alt Boyut Puanları Arasındaki İlişki.....	66
Tablo 3.17 Üniversite Öğrencilerinin Günlük İnternet Kullanım Süreleri ile Sanal Zorbalık, Sanal Mağduriyet, Çevrim İçi Mahremiyet Farkındalık Genel ve Alt Boyut Puanları Arasındaki İlişki	67
Tablo 3.18 Üniversite Öğrencilerinin Akademik İnternet Kullanım Süreleri ile Sanal Zorbalık, Sanal Mağduriyet, Çevrim İçi Mahremiyet Farkındalık Genel ve Alt Boyut Puanları Arasındaki İlişki	68
Tablo 3.19 Üniversite Öğrencilerinin Akademik İnternet Kullanım Süreleri ile Sanal Zorbalık, Sanal Mağduriyet, Çevrim İçi Mahremiyet Farkındalık Genel ve Alt Boyut Puanları Arasındaki İlişki	69

KISALTMALAR LİSTESİ

Bu araştırmada kullanılmış kısaltmalar, açıklamaları ile aşağıda verilmiştir.

BTK: Bilgi Teknolojileri ve İletişim Kurumu

ÇMFÖ: Çevrim İçi Mahremiyet Farkındalık Ölçeği

DM: Dijital Mahremiyet

DMF: Dijital Mahremiyet Farkındalığı

KBF: Kişisel Bilgi Formu

KVKK: Kişisel Verilerin Korunması Kanunu

SM: Siber Mağduriyet

SZ: Siber Zorbalık

SZMÖ: Siber Zorbalık/Mağduriyet Ölçeği

TANIMLAR LİSTESİ

Bu başlık altında araştırmada yer alan değişkenler tanımlanmıştır.

Mahremiyet: Mahremiyet, bireylerin kişisel bilgilerini, düşüncelerini ve davranışlarını diğer bireylerden koruma hakkı olarak tanımlanmaktadır (Westin, 1967).

Dijital Mahremiyet: Dijital mahremiyet, bireylerin çevrim içi ortamda dijital kimliklerinin ve kişisel verilerinin gizliliğini ve güvenliğini koruma hakkı olarak tanımlanmaktadır (Solove, 2008).

Farkındalık: Farkındalık, bireylerin çevrelerindeki olaylara ve durumlara dikkat etme ve kendi içsel deneyimleri ile bilinçli bir şekilde bunları anlama yeteneği olarak adlandırılmaktadır (Kabat-Zinn, 2013).

Dijital Mahremiyet Farkındalığı: Dijital mahremiyet farkındalığı, bireylerin dijital ortamda bulunurken kişisel verilerinin nasıl toplandığının, kullanıldığının ve paylaşıldığının bilincinde olmaları olarak tanımlanmaktadır (Paine vd., 2007).

Mağduriyet: Mağduriyet, bireylerin bir olay veya durum nedeniyle zarar görmesi, haksızlığa uğraması ya da olumsuz etkilenmesi olarak tanımlanmaktadır (Tapley & Davies, 2020).

Siber Mağduriyet: Siber mağduriyet, teknolojik araçları kullanırken bireylerin dijital ortamda, özellikle internet ve sosyal medya platformlarında, siber saldırılar, dolandırıcılıklar, kimlik hırsızlığı ya da diğer kötü niyetli eylemlere maruz kalarak zarar görmesi durumu olarak tanımlanmaktadır (Kowalski vd., 2014).

ÖZET

Bu araştırmanın amacı üniversite öğrencilerinin dijital mahremiyet farkındalıkları ve siber mağduriyetleri arasındaki ilişkiyi incelemektir. Bu kapsamda üniversite öğrencilerinin dijital mahremiyet farkındalıkları ve siber zorbalık sonucu ortaya çıkan siber mağduriyet değişkenleri cinsiyet, sınıf düzeyleri, günlük internet kullanım süreleri ve kullanılan sosyal medya platformlarına göre farklılaşıp farklılaşmadığı tespit edilmiştir. Aynı zamanda sosyal hizmet bakış açısıyla dijital mahremiyet farkındalığının güçlendirme kuramındaki yeri ele alınmıştır. Araştırma deseninde betimsel ve ilişkisel tarama modelleri tercih edilmiştir. Araştırmanın katılımcılarını 560 üniversite genci oluşturmaktadır. Araştırma verilerinin toplanmasında Kişisel Bilgi Formu ile birlikte Siber Zorbalık Ölçeği ve Çevrim İçi Mahremiyet Farkındalık Ölçeği kullanılmıştır. Araştırma sonucunda üniversite öğrencilerinin dijital mahremiyet farkındalıkları ile siber mağduriyetleri arasında düşük pozitif bir ilişki olduğu ortaya çıkmıştır. Bununla birlikte siber zorbalık ve siber mağduriyet arasında pozitif orta düzeyde bir ilişki olduğu saptanmıştır. Siber mahremiyet farkındalığı ve siber mağduriyetin cinsiyete, internetin kullanım süresine ve sosyal medya platformlarına göre anlamlı olarak farklılaştığı gözlemlenmiştir.

Anahtar Kelimeler: Dijital Mahremiyet Farkındalığı; Siber Mağduriyet; Siber Zorbalık; Üniversite Öğrencileri; Güçlendirme Kuramı

SUMMARY

INVESTIGATION OF THE RELATIONSHIP BETWEEN DIGITAL PRIVACY AWARENESS AND CYBER VICTIMIZATION AMONG UNIVERSITY STUDENTS

The aim of this study is to examine the relationship between university students' awareness of digital privacy and their experiences of cyber victimization. In this context, the study investigates whether digital privacy awareness and cyber victimization -emerging as a result of cyberbullying- differ according to gender, academic year, daily internet usage duration, and the social media platforms used. Additionally, from a social work perspective, the role of digital privacy awareness within the empowerment theory is explored. A descriptive and relational survey model was employed in the research design. The study sample consists of 560 university students. Data were collected using a Personal Information Form, the Revised Cyberbullying/Cyber Victimization Inventory for University Students, and the Online Privacy Awareness Scale. The findings reveal a low positive correlation between university students' digital privacy awareness and their levels of cyber victimization. Furthermore, a moderate positive relationship was found between cyberbullying and cyber victimization. Digital privacy awareness and cyber victimization were observed to differ significantly based on gender, duration of internet use, and the social media platforms utilized.

Keywords: Digital Privacy Awareness; Cyber Victimization; Cyberbullying; University Students; Empowerment Theory

TEŞEKKÜR / ÖNSÖZ

Bu çalışmada üniversite öğrencilerinin dijital mahremiyet farkındalığı ve siber mağduriyet arasındaki ilişki incelenmiştir. Aynı zamanda sosyal hizmet perspektifinden dijital mağduriyet farkındalığı ve siber mağduriyet güçlendirme kuramı bağlamında ele alınarak literatüre önemli bir katkı sağlayacağı düşünülmektedir.

Tezimin her adımında bana yol gösteren, emeğini ve desteğini hiçbir zaman esirgemeyen, sabırlı, anlayışlı ve en büyük şanslarımdan olan tez danışmanlarım Doç. Dr. Sinem Burcu UĞUR ve Dr. Öğr. Üyesi Nehir YASAN AK'a, tez savunmamda yer almayı kabul ederek kıymetli katkılarda bulunan saygıdeğer hocalarım Prof. Dr. Arif AYTEKİN ve Doç. Dr. Elif BAŞ'a sonsuz teşekkürlerimi sunarım. Ayrıca yüksek lisansa başlamam için beni teşvik eden değerli hocalarım Prof. Dr. Hüsne DEMİREL ve Arş. Gör. Ayşe Nur PEKASIL'a şükran borçlu olduğumu belirtmek isterim.

Tüm hayatım boyunca her koşulda maddi ve manevi olarak beni sonsuz destekleyen, önemseyen, seven, düştüğüm zaman ayağa kaldıran, her zaman yanımda olan ve varlıklarıyla beni güçlendiren annem Serpil ERMUMCU ve babam Ömer ERMUMCU'ya, sevgili ablam Gözde FİDANBOY ve biricik yeğenim Berra FİDANBOY'a, yüksek lisans maceramda bana manevi olarak desteğini hiç esirgemeyen canım arkadaşlarım Recep Baki OKAY ve Buse SARIKAMIŞ'a ve daha sayamadığım bütün sevdiklerime teşekkür ederim. İyi ki varsınız ve iyi ki hep yanımdaydınız.

Gizem ERMUMCU

Antalya 2025

GİRİŞ

İnsan sosyal bir varlıktır ve var olduğu andan itibaren sosyalleşmeye ihtiyaç duymaktadır. Bu sosyalleşme ihtiyacını giderme sürecinde kullandığı araçlar da zaman zaman değişikliğe uğramaktadır. Bireyler günümüzde bu ihtiyacını teknoloji ve internetin yaygınlaşması ile sıklıkla dijital yollarla karşılamaktadır. Özellikle gençler iletişim, bilgi edinme ve kişisel gelişim gibi ihtiyaçlarını sosyal medya platformları ile gidermeye başlamıştır (Hou vd., 2019). Teknolojik aletlerdeki gelişmeler ve bilhassa akıllı telefonların, tabletlerin kullanımının yaygınlaşmasının internet ve sosyal medya uygulamalarında vakit geçirmeyi teşvik ettiği düşünülmektedir (Zivnuska vd., 2019).

Günümüzde bilgi ve iletişim teknolojilerine ulaşımın artması hayatımızı kolaylaştırmakla birlikte, bazı sorunları da beraberinde getirmekte ve dijital dünyadaki sosyalleşme oldukça tehlikeli bir hal alabilmektedir. Çünkü dijital ortamdaki her bir paylaşım herkes tarafından oldukça kolay ulaşılabilir bir bilgi demektir. Bu nedenle bireylerin özellikle de ergen ve gençlerin dijital ortamda hangi bilgileri edindikleri, hangi bilgileri kimlerle ne boyutta paylaştıkları, mahremiyetlerinin ne kadar farkında oldukları ve mahremiyetlerini nasıl korudukları oldukça önemli noktalardır.

Dijital mahremiyet kavramı bilgi edinmek, iletişim kurmak veya başka amaçlarla internette bulunan kişilerin korunması için alınabilecek önlemler olarak tanımlanabilmektedir (Wu vd., 2011). Gün geçtikçe verileri gizlemek zorlaşmaktadır. Bu nedenle bireyler dijital mahremiyetleri konusunda endişelenmekte, dijital kimliklerini korumada zorluk yaşamaya başlamaları ile bıkkınlık hissetmekte ve zamanla bu konu üzerinde durmamaktadır (Choi, Park & Jung, 2018). Ayrıca bireyler çoğu zaman bağımsız olduklarını düşünerek mahremiyetlerinin bozulması hakkında kaygılanmamakta veya mahremiyetlerinin kaybolduğunu fark etmemektedir (Kalaman, 2017).

Dijital ortamdaki mahremiyetin yok olması çok sayıda mağduriyetin yaşanmasına zemin hazırlamaktadır. İnternet kullanımında herhangi bir denetleyicinin olmaması, anonim bir biçimde sosyal medyada var olunabilmesi, bilgilerin kopyalanabilir halde mevcut bulunması ve pornografik içeriklere kolaylıkla ulaşılabilmesi sebebiyle gerçekleşen siber saldırılar sonucunda siber mağduriyet kavramı ortaya çıkmıştır (Fujita & Ruffa, 2019).

Siber mağduriyet dijital ortamda teknolojik aletler kullanılarak bireyi kasten küçük düşürmek ve bu bireye zarar vermek şeklinde tanımlanabilmektedir (Brown, Demaray & Secord, 2014). Siber mağduriyet yaşayan birey fiziksel, psikolojik ve duygusal olarak olumsuz

etkilenebilmekte ve birey olumsuz davranışlarda bulunabilmektedir. Örneğin siber mağduriyet sonucu madde bağımlılığına sürüklenen bireylerin varlığından söz edilebilmektedir (Mitchell vd., 2011).

Dijital ortama erişilebilen her yerde siber mağduriyet yaşanabildiği, fiziksel bir mekân gerekmediği için siber mağdur kendini her ortamda savunmasız hissedebilmektedir (Slonje, Smith & Frisen, 2013). Bütün ortamlarda kendini savunmasız ve çaresiz hisseden mağdur sosyal ortamlardan da kendini geri çekebilme, yalnız kalmayı tercih edebilmektedir (Martinez-Martinez vd., 2020). Ayrıca siber mağduriyetin ergenlikten ilk yetişkinliğe geçiş döneminde olan üniversite yıllarında yaşanması ile bireyler oldukça önemli yıkımlar yaşayabilmektedir. Bu dönemde bireyin kendisinin farkına varması, deneyimlediği olumsuz tecrübelerin üstesinden gelmesi ve kendine uygun ahlak anlayışı geliştirmesi beklenmektedir. Ancak yaşanan mağduriyet ile bu gelişim görevleri olumsuz etkilenebilmektedir (Strohmeier, Karna & Salmivalli, 2010). Bu nedenle dijital mahremiyet farkındalığı ve siber mağduriyet arasında anlamlı bir ilişkinin olduğu öngörüldüğünden, üniversite döneminde de dijital mahremiyet farkındalığının oldukça önemli olduğu düşünülmektedir. Bu düşünceden yola çıkarak bu çalışmada üniversite öğrencilerinin dijital mahremiyet farkındalıkları ile siber mağduriyet ve arasındaki ilişkinin incelenmesi amaçlanmaktadır.

Literatürde, dijital mahremiyet farkındalığı ve siber mağduriyet arasındaki ilişkiyi inceleyen sınırlı sayıda araştırma bulunmaktadır. Çoğunlukla bu iki kavram birbirinden bağımsız olarak ele alınmış olup, aralarındaki potansiyel ilişkiyi keşfetmeye yönelik çalışmalar oldukça azdır. Bu tez, dijital mahremiyet farkındalığının, üniversite öğrencilerinin siber mağduriyet yaşama risklerini nasıl etkileyebileceğini ortaya koymayı amaçlamaktadır. Yapılacak bu araştırma, literatürdeki önemli bir boşluğu dolduracak ve dijital mahremiyet farkındalığının artırılmasına yönelik stratejilerin geliştirilmesine katkı sağlayacaktır.

Ayrıca, bu çalışmanın özgünlüğü, dijital mahremiyet ve siber mağduriyet arasındaki ilişkiyi sosyal hizmet perspektifinden ele almasıyla pekişmektedir. Dijital mahremiyet, bireylerin çevrim içi dünyada kişisel sınırlarını koruma yetilerini geliştirmeleri açısından kritik bir öneme sahiptir. Ancak bu farkındalık düzeyi, sosyal hizmet uzmanlarının uygulayacakları müdahaleler için de önemli bir temel teşkil etmektedir. Bu bağlamda, gençlerin dijital ortamda daha güvenli bir şekilde var olmalarını sağlamak amacıyla farkındalıklarını artırmaya yönelik stratejilerin geliştirilmesi gerekmektedir.

Tez, üç ana bölümden oluşmaktadır. İlk bölümde, dijital mahremiyet ve siber mağduriyet kavramları teorik bir çerçevede ele alınarak, bu kavramların tarihsel gelişimleri, boyutları ve birey üzerindeki etkileri tartışılacaktır. İkinci bölümde, dijital mahremiyet

farkındalığı ve siber mağduriyet arasındaki ilişki, güçlendirme kuramı perspektifinden analiz edilecektir. Son olarak, üçüncü bölümde, araştırma tasarımı, kullanılan yöntemler, bulgular ve bu bulguların tartışması sunulacaktır. Bu yapı, çalışmanın kapsamını daha anlaşılır kılacak ve araştırmanın önemli bulgularına ışık tutacaktır.



BİRİNCİ BÖLÜM

ARAŞTIRMANIN KAVRAMSAL TEMELLERİ

Günümüzde dijitalleşme bireysel ve toplumsal yaşamımızı şekillendirmektedir. Dolayısıyla bireylerin dijital dünyadaki varoluş biçimleri, mahremiyet algıları ve karşılaştıkları tehlikeler değişmektedir. Bu değişim sosyal hizmet disiplini açısından da oldukça önemli hale gelmektedir. Özellikle genç bireylerin yoğun olarak bulunduğu dijital ortamlarda diğer bireyler ile kurdukları ilişkiler, gençlerin kimlik gelişimleri, sosyal bağları ve psikososyal iyi olma halleri üzerinden doğrudan etkili olmaktadır. Bu kapsamda dijital mahremiyetin, yalnızca teknik bir durum olmadığı görülmektedir. Dijital mahremiyet, bireylerin kendilerini ifade etme, korunma ve sosyal güvenlik alanlarında güçlenme süreçleri ile yakından ilişkili bir olgudur.

Üniversite öğrencisi olan genç yetişkinler, dijital teknolojileri yoğun olarak kullanan bireyler arasında yer almaktadır. Özellikle sosyal medya, çevrim içi iletişim ve bilgi paylaşım platformlarını sıklıkla kullanmaktadırlar. Fakat bu çokça yaşanan dijital etkileşim, beraberinde çeşitli riskleri de getirmektedir. Bireylerin mahrem bilgilerini kontrolsüzce paylaşımı, özel yaşamalarının ihlaline, çevrim içi zorbalık ve siber mağduriyet gibi durumların yaşanmasına yol açabilmektedir. Bireylerin dijital farkındalığının yetersizliği ile yaşanan bu sorunlar daha da derinleşebilmektedir. Ayrıca dijital mahremiyet konusunda farkındalığı düşük bireylerin, siber zorbalığa maruz kalma ve mağdur olma ihtimalleri de artmaktadır.

Bu çalışma ile üniversite öğrencilerinin dijital mahremiyet farkındalık düzeyleri ve siber mağduriyet seviyeleri arasındaki ilişkiyi incelemek amaçlanmaktadır. Aynı zamanda bu iki değişkenin sosyal hizmet perspektifinden nasıl değerlendirileceği de ele alınacaktır. Bu bağlamda dijital mahremiyet farkındalığının genç bireylerin kendi sınırlarını belirleme, tehditleri tanıma ve çevrim içi ortamlarda kendilerini koruma kapasiteleri üzerindeki etkisi değerlendirilecektir. Bu sayede sosyal hizmet uygulamalarında güçlendirme müdahalelerine temel oluşturacak veriler elde edilmesi hedeflenmektedir.

Bu doğrultuda bu bölüm içerisinde, araştırmanın kavramsal temellerini oluşturan başlıca kavramlara yer verilmiştir. İlk olarak mahremiyet kavramı, tarihsel ve kuramsal boyutları açıklanmış; ardından dijital mahremiyetin ne anlama geldiği anlatılarak hangi boyutları içerdiği ve gençlerde nasıl tezahür ettiği ele alınmıştır. Daha sonrasında farkındalık kavramı tanımlanarak özellikle dijital ortamdaki mahremiyet farkındalığı ile ilişkili biçimde değerlendirilmiştir. Aynı zamanda bireyin kendi haklarının farkında olması ve koruyucu stratejiler geliştirebilmesi ile farkındalık arasındaki bağ tartışılmıştır.

Bu kavramsal bölümün amacı, araştırmanın dayandığı temel kavramları açıklığa kavuşturarak dijital mahremiyet ile siber mağduriyet arasındaki ilişkinin daha derinlikli anlaşılmasına zemin hazırlamaktır. Bununla birlikte sosyal hizmet bağlamında, bireylerin çevrim içi ortamlarda karşılaştığı sorunlara karşı güçlenmelerine hizmet edecek kuramsal bir yapı da bu temel üzerinde inşa edilecektir.

1.1. Mahremiyet Kavramı ve Gelişimi

Bu başlık altında dijital mahremiyet farkındalığı ve siber mağduriyet arasındaki ilişkinin kuramsal zeminini oluşturan en temel kavramlardan biri olan mahremiyet, tarihsel ve kuramsal yönleriyle ele alınmıştır. Çalışmanın temel problemlerinden biri olan “genç bireylerin dijital mahremiyet farkındalığı düzeylerinin ne olduğu ve bunun siber mağduriyetle nasıl bir ilişki içinde olduğu” sorusu, mahremiyet kavramının sadece dijitalleşme çerçevesinde değil, aynı zamanda bireyin toplumsal ilişkilerinde nasıl yapılandığı ve sınırlandığı yönleriyle de irdelenmesini gerekli kılmaktadır.

Tarihsel, kültürel, etik ve toplumsal kodlarla iç içe geçmiş çok katmanlı bir olgu olan mahremiyet, yalnızca bireysel bir tercih veya özel hayatın gizliliği olarak değerlendirilebilecek bir kavram değildir. Bu sebeple mahremiyetin tarihsel gelişimi, türleri, boyutları ve işlevleri bir bütün olarak ele alınmalıdır. Böylelikle kavramın dijital düzlemde nasıl dönüşüme uğradığı ve bireyin bu dönüşüm karşısında nasıl konumlandığı kolaylıkla anamlandırılabilir.

Bu bağlamda öncelikle mahremiyet kavramının tarihsel gelişimi, kültürel kapsamdaki anlam çeşitliliği ve birey-toplum ilişkilerindeki yeri incelenmiştir. Daha sonra mahremiyetin bilgi, beden, iletişim ve mekânsal gibi çeşitli türleri ele alınmış; bu türlerin bireyin öznel sınırlarını nasıl belirlediği tartışılmıştır. Bu çok boyutlu yapının anlatılması ile bireylerin dijital ortamlarda karşılaştıkları ihlal şekilleri ve bu ihlallere karşı geliştirdikleri farkındalık düzeylerinin daha iyi açıklanabilmesi için zemin sağlanmıştır.

Araştırmanın sosyal hizmet disiplini içinde yer alması sebebiyle mahremiyet, mesleki etik, müdahale ilkeleri ve birey haklarının korunması açısından da ele alınmaktadır. Sosyal hizmet uzmanları tarafından bireyin mahremiyetine saygı göstermek, sadece mahremiyeti korumak değildir. Aynı anda bireyin mahremiyet sınırlarını tanıma, ifade etme ve savunma kapasitesini destekleyerek güçlendirmektir. Bu yönüyle mahremiyet, yalnızca özel alanın korunması anlamına gelmemektedir. Buna ek olarak bireyin güçlenmesi için de temel bir ön koşuldur.

Bu sebeple bu kısımda sırasıyla mahremiyetin tarihsel ve kavramsal gelişimi, mahremiyetin türleri ve boyutları ile sosyal hizmet bağlamında mahremiyetin işlevi başlıkları

altında kavramın teorik temelleri sunulmuş, dijital mahremiyete geçiş için kuramsal bir arka plan oluşturulmuştur.

1.1.1. Mahremiyetin Tanımı ve Tarihsel Gelişimi

Mahremiyet, yüzyıllar öncesine dayanan bir kavramdır. İlk olarak 16.-17. yüzyıllarda karşımıza çıkmaktadır (Aries & Duby, 2007). Bu kavram sosyal-kültürel ve siyasal alanda meydana gelen değişimler ile paralellik gösterdiği için kentleşme ve kitle toplumunun ortaya çıkması ile mahremiyet kavramı da değişime uğramıştır. 18. yüzyılda evlerdeki bireyselleşme ile oda kavramı ortaya çıkmış evdeki mahremiyet alanları değişmiştir. 19. yüzyılda ise bireyin kişisel yaşamının kendine özel olma durumu gündeme gelmiştir. Daha sonraki yıllarda da modernleşme mahremiyeti etkilemiş, geliştirmiş ve dönüştürmüştür.

Mahremiyet olgusu, kavramsal olarak geniş bir anlam çeşitliliğine sahiptir. Bu nedenle, kelimenin köküne bakarak kavramı anlamaya çalışmak oldukça önemlidir. Öncelikle Arapça olan “haram” kelimesi ile bu kelimeden türetilen “mahrem” kavramları incelenmelidir. Haram “yasaklanmış koruluk, yasak bölge; dince yasak edilmiş, din kurallarına aykırı olan; dinen sorumluluk çağına ulaşmış olan herkese, Allah’ın yapılmasını kesin olarak yasakladığı söz ve davranış” (Komisyon, 2019) olarak tanımlanmaktadır. Mahrem kelimesi ise “başkalarından saklanan, başkaları tarafından görülmesi, bilinmesi, duyulması istenmeyen, gizli” (Yörükan, 2024) anlamına gelmektedir. Ayrıca dinsel boyutu da olan mahrem kavramı “1. Saygıya ve gizlenmeye değer şey. 2. Herkesin bilmesi gerekmeyen şey. 3. Aralarındaki kan bağının yakınlığından dolayı birbirleri ile evlenmeleri yasak olan çok yakın akrabalar.” (Komisyon, 2019) anlamlarını da içermektedir.

Mahremiyet kavramı, Türkçe Sözlükte (Türk Dil Kurumu, 2025) “gizlilik” olarak tanımlanmaktadır. Özdemir (2020) mahremiyeti “taşınamayan, satılamayan ve devredilemeyen özel bir mülkiyet” olarak ele alırken Şişman (2020) ise “Mahremiyet, paylaşmak istemediğim, başkasından sakındığım, koruduğum, tuttuğum günlüklerden aşk mektuplarına varıncaya kadar her şeyi kapsar. Bu ‘her şey’ bana ait dünyanın parçasıdır.” diyerek kapsayıcı bir tanım yapmaktadır.

İlk kez 1890’da bir makalede hak olarak mahremiyeti işleyen Warren ve Amerikalı yargıç Brandeis ise bu kavramı şu şekilde tanımlamaktadır: Bireyin yalnız bırakılma hakkı ve özgür insanlar tarafından en çok değer verilen hak (Öz & Kılıç, 2020).

1972 yılında Londra’da düzenlenen Mahremiyet Komitesi Raporu’nda mahremiyetin iki boyutunun olduğu ifade edilmektedir. İlk boyut bireysel, ailevi ve yakın çevresi ile bireyin kurduğu ilişkiye onun izni olmadan dahil olunmaması ile ilgiliyken diğer boyut bireye ait özel

bilgilerin kimlerle hangi düzeyde paylaşılacağına kararının yine bireye ait olduğu ile ilgilidir (Vincent, 2022).

Hak olmanın yanı sıra mahremiyet demokratik bilinç (Özbudun, 2025) ve özgürlük (Levent, 2015) konularını kapsamakta, ayrıca kültürel ve toplumsal (Bağlı, 2011) kodları da içermektedir. Belirtildiği üzere mahremiyet yalnızca bireyin özel alanı ile ilgili değildir. Aynı zamanda bireyin içerisinde yaşadığı toplum ve kültürle yakından ilişkili bir olgudur. Dolayısıyla mahremiyet bilinci, bireyin kendi sınırlarını tanıması ve başkalarının sınırlarına saygı göstermesiyle gelişen bir demokratik bilincin parçasını oluşturmaktadır. Benzer şekilde mahremiyetin bireyin özgürlüğünün bir uzantısı olduğu görülmektedir. Diğer bireylerin yaşamlarına müdahale edilmemesi özgür bir toplumun oluşması için de bir yapı taşıdır. Öte yandan bireylerin toplum içinde nasıl davranması gerektiğini belirleyen normlar olarak tanımlanan toplumsal kod ve bir toplumun değerleri, inançları, gelenekleri ve davranışlarını belirleyen kültürel kodlar bireyin mahremiyeti nasıl algıladığını da büyük ölçüde şekillendirmektedir. Görüldüğü üzere mahremiyet hem bireysel hem de toplumsal düzeyde çok katmanlı bir kavramdır. Bu yönleriyle hak, bilinç, özgürlük ve kültürel değerlerle iç içe geçmekte ve bunlar göz önünde tutularak ele alınması gereken bir kavram olduğu ifade edilebilmektedir.

1.1.2. Mahremiyetin Türleri ve Boyutları

Mahremiyetin boyutları üzerine farklı araştırmacılar çeşitli sınıflandırmalar önermiştir. Örneğin Fischer-Hübner (1998) mahremiyeti üç temel boyutta ele almaktadır: Bölgesel mahremiyet (territorial privacy), bireyin fiziksel çevresinin korunmasıyla ilgilidir; birey mahremiyeti (privacy of the person), bedensel dokunulmazlık ve kişinin fiziksel bütünlüğüne saygı bağlamında değerlendirilir; bilgi mahremiyeti (informational privacy) ise bireyin kişisel verilerinin toplanması, işlenmesi ve paylaşılması süreçlerini kapsar.

Baysal Berkup (2015) beden mahremiyeti, cinsellik ve kadın-erkek ilişkileri, ev ve aile yaşamı, dini-siyasi görüş mahremiyeti olmak üzere mahremiyetin dört boyuta sahip olduğunu ifade etmektedir.

Alan Westin mahremiyeti bireyin kendisi hakkında hangi bilginin, ne zaman, nasıl ve ne ölçüde başkalarına aktarılacağına karar verme yetkisi olarak tanımlar. Mahremiyeti hem iletişimsel bir süreç hem de bireyin özerkliğini sağlayan bir mekanizma olarak konumlandırılan bu yaklaşımda da mahremiyet dört temel boyutta sınıflandırılır:

Yalnızlık (Solitude): Bireyin, fiziksel ve psikolojik olarak diğer bireylerden tamamen ayrıldığı, gözlemlenmediği ve kendiyle baş başa kaldığı durumdur. Bu boyut, bireyin içsel dünyasını yeniden düzenlemesi ve kişisel bütünlüğünü koruması açısından önemlidir.

Yakınlık/Samimiyet (Intimacy): Bireyin belirli kişilerle (örneğin aile üyeleri, eş, arkadaş) samimi ve özel bir ilişki kurma ihtiyacını ifade eder. Mahremiyetin bu boyutu, güvene dayalı ilişkilerin gelişimini destekler. **Anonimlik (Anonymity):** Kişinin kamusal alanda tanınmadan var olma hakkını ifade eder. Birey, kalabalık içinde görünmeden ve izlenmeden hareket edebilmeyi ister. Bu da bireyin özgürlük duygusu ve ifade alanı açısından kritiktir. **Kendini Muhafaza Etme (Reserve):** Bireyin, duygu ve düşüncelerini ne ölçüde paylaşacağını denetleme ihtiyacıdır. Bu, kişinin iç dünyasını dış müdahalelerden korumasına imkân tanıyan zihinsel bir mesafeyi ifade eder (Westin, 1967).

Bu grupta, alanyazında çoğunlukla “mahremiyetin boyutları” adı altında ele alınmaktadır. Ancak mahremiyetin türlerini tanımlamaya yönelik sınıflamalar olarak da karşımıza çıkabilmektedir. Bireyin bedenine, bilgi ve iletişimine veya mekânsal mahremiyeti gibi alt dallar vurgu yapılmaktadır. Bu da bireyin hayatındaki çeşitli mahremiyet şekillerinin, farklı sosyal ortamlarda nasıl anlam kazandığını ve nasıl korunması gerektiğini ortaya koymaktadır. Bu yaklaşım, mahremiyetin yalnızca tekil bir alanla sınırlı olmadığını, aksine bireyin çoklu sınırlarını içine alan karmaşık bir sistem olduğunu göstermektedir.

Açıkça belirtildiği üzere, mahremiyet sadece bireysel bir tercih ya da basit bir gizlilik sorunu değildir. Aynı zamanda tarihsel, kültürel, dini, etik ve toplumsal çerçevede birbirinin içine geçmiş çok katmalı bir sistemdir. Dolayısıyla mahremiyet kavramının da tek bir tanımı yoktur. Zaman içerisinde farklılaşan ve çeşitlenen birden fazla tanımla karşımıza çıkan mahremiyet olgusu, bireyin hem fiziksel hem de psikolojik sınırlarının belirlenmesi ile öznelliğini koruma ve toplumsal dengeyi kurma işlevlerini üstlenmektedir. Bu sebeple mahremiyeti bütünüyle ele alarak anlamak, bireyin yaşamını ve haklarını nasıl deneyimlediğini çözümleyebilmek açısından oldukça önemlidir. Günümüz dünyasında, dijital teknolojilerin hayatımızın her alanında kullanılmaya başlanması ile bireylerin mahremiyetle kurduğu ilişki önemli bir dönüşüm geçirmektedir. Bu olay da bir sonraki kısımda dijital mahremiyetin tanımına odaklanılmasını gerekli kılmaktadır.

1.2. Dijital Mahremiyet Kavramı

Dijital mahremiyet, daha önce de belirtildiği üzere, yalnızca bireysel bir tercih alanı değildir, bireyin kendi sınırlarını belirleyebilme, haklarını tanıma ve bu hakları koruyabilme kapasitesidir. Bu çalışmada da dijital mahremiyet bu yönleri ile ele alınmaktadır. Dijital mahremiyet konusu, sosyal hizmetin temel hedeflerinden biri olan bireyin güçlendirilmesi ilkesiyle doğrudan örtüşmektedir. Düşük dijital mahremiyet farkındalığına sahip bireyler çevrim içi ortamlarda daha kırılgan hale gelebilmekte, kişisel verileri ihlal edilebilmekte veya

rızaları dışında izlenebilmektedir. Bunlar da siber zorbalığa uğrayarak mağduriyet yaşamaları ihtimalini yükseltmektedir. Dolayısıyla bu kavram, çalışmanın hem problem alanını hem de çözüm önerilerini şekillendiren ana hatlardan birini oluşturmaktadır.

Bu bölümde yer verilen başlıklar, dijital mahremiyet kavramını çok boyutlu biçimde ele almak amacıyla yapılandırılmıştır. İlk olarak dijital mahremiyetin tanımı ve günümüz koşullarında neden kritik önemde olduğu ortaya konmuş, ardından dijital mahremiyetin hangi boyutlardan oluştuğu -örneğin bilişsel, davranışsal, yapısal vb.- ele alınarak bireylerin dijital ortamlarda nasıl bir mahremiyet algısı geliştirdiği açıklanmıştır. Son olarak, bireylerin dijital ortamlarda hangi tür mahremiyet riskleriyle karşı karşıya olduğu ve bu risklere karşı bireysel veya kurumsal düzeyde hangi korunma stratejilerinin geliştirilebileceği ele alınmıştır. Böylelikle bu başlık hem mahremiyet farkındalığını artırmak hem de siber mağduriyet risklerini azaltmak açısından önemli bir değerlendirme alanı sunmaktadır.

Bu bağlamda ele alınan her bir başlık, çalışmanın temel araştırma soruları olan “üniversite öğrencilerinin dijital mahremiyet farkındalık düzeyleri nedir?” ve “bu farkındalık ile siber mağduriyet düzeyi arasında bir ilişki var mıdır?” sorularını kavramsal düzeyde anlamak ve açıklamak amacıyla düzenlenmiştir.

1.2.1. Dijital Mahremiyetin Tanımı ve Önemi

Geleneksel mahremiyet bireyin fiziksel sınırlarını ve özel yaşam alanlarını korumaya yöneliktir. Dijital mahremiyet ise bireyin çevrim içi ortamlarda paylaştığı bilgi, içerik ve etkileşimlerin kontrolünü ifade etmektedir. Dijital mahremiyet; bireyin hangi kişisel verisinin, kimler tarafından ne amaçlarla ve ne ölçüde erişileceğine karar verme hakkı olarak tanımlanabilmektedir. Dijital mahremiyet olgusu, bireyin çevrim içi ortamda görünürlüğünü yönetebilme kapasitesi ile de doğrudan ilişkilidir. Ayrıca teknolojik gelişmeler ile bireysel yaşantılar bu denli entegre olmuşken mahremiyetin yalnızca fiziksel veya yüz yüze ilişkiler düzeyinde tartışılmayacağı da görülmektedir. Özellikle sosyal medya, mesajlaşma uygulamaları ve çevrim içi içerik platformlarının yaygınlaşması ile dijital mahremiyet çağdaş sosyal ilişkilerin ayrılmaz bir parçası olmuştur. Fakat günümüzde mahremiyet sıkça ihlal edilen bir sorun haline de gelmiştir.

Teknoloji her geçen gün gelişmekte ve değişmektedir. Kültürel ve toplumsal normlar ile bağlantılı olan teknoloji beraberinde toplumu, insani ilişkiler ve davranışları da değiştirmektedir. Dolayısıyla insanların kendi elleriyle geliştirdiği iletişim teknolojilerinin bir noktadan sonra insan kontrolünden çıkarak insanları ve toplumu dönüştürmeye başladığı açıkça görülmektedir (McLuhan & Powers, 2020).

İletişim teknolojilerinden en popüler olanı sosyal medya platformlarında bu gelişim ve dönüşümler kolaylıkla gözlemlenebilmektedir. Teknolojik araçların gün geçtikçe daha ucuz ve ulaşılabilir olması bu platformları daha popüler hale getirerek bu platformların daha çok yaygınlaşmasına yol açmaktadır. Bu dijital ortamlar da bireylerin maddi ve manevi değer yargılarının değişip dönüşmesinde oldukça önemli bir rol oynamaktadır.

Teknoloji kaynaklı değer yargıların değişmesiyle birlikte mahremiyet algısının da gelişip dönüşmesi kaçınılmaz hale gelmiştir (Vatandaş, 2020). İnternetin ve dijital platformların kullanımının artması ile kişisel mahremiyet alanında bir devrim yaşanmakta, süratli bir biçimde mahremiyet olgusunun geçerliliğini kaybettiği bir evreye girilmektedir.

Dijital ortamdaki kullanıcıların, kendilerine ait her bilgiyi kolaylıkla paylaşabilmeleri sebebi ile bireylerin kişisel alanlarına yönelik saldırılar oldukça basit bir hal almıştır. Önceleri kişisel fotoğraf ve videolarının başka bir yere servis edilmesinden, konuşmalarının dinlenmesinden, nüfus verilerinin güvenliğinden endişe duyan, mahremiyetinin yitirilmesi konusunda panikleyen ve hatta mahremiyeti için yasal düzenleme talep eden bireylerin günümüzde bu panik ve kaygılarının dağıldığı görülmektedir (Yüksel, 2003). Bu panik ve endişe yerini beğenilme ve kabul görme arzusu ile başka istek ve beklentilere bırakmıştır. Bir başka ifadeyle dijital platformların bireylerde oluşturduğu “beğenilme ve onaylanma arzusu” mahremiyet kaygılarının önüne geçmektedir.

Dijital dünyada mahrem olan birçok şeyin kolaylıkla hiçbir çekince yaşanmadan paylaşılabilir olması, özel yaşamın transparan bir hale gelmesi mahremiyetin silikleşmeye ve kaybolmaya başladığının bir göstergesidir (Vatandaş, 2020). Mahremiyetin yok olması bu dünya ile içli dışlı olan bireyler özellikle de çocuk ve gençler için tehdit oluşturmaktadır (Gülderen, Çetinkaya & Keser, 2016). Mahremiyetin olmadığı ortamda çeşitli mağduriyetlerin yaşanması oldukça kolaydır. Özellikle çevrim içi ortamlarda genç bireylerin karşılaştığı siber riskler dikkate alındığında, mahremiyetin birey için taşıdığı önem dijital çağda daha da hayati hale gelmektedir.

Bu noktada mahremiyetin birey için yalnızca bir hak değil, aynı zamanda çok boyutlu bir işlev gördüğü unutulmamalıdır. Westin (1967), mahremiyetin dört temel işleve sahip olduğunu belirtmektedir: Kişisel özerklik (bireyin kendine ait kararlar alabilmesi), duygusal rahatlama (toplumsal rollerden uzaklaşarak kendini yeniden düzenleme), öz-değerlendirme (kişisel iç görüş kazanımı) ve sınırlı-korumalı iletişim (iletişimde denetim gücü elde etme). Aynı zamanda, Görmen Şen’e (2024) göre mahremiyet; toplumsal ilişkileri düzenleme, demokratik bilinç geliştirme, bireyin özgürlük ve itibarını güvence altına alma gibi işlevlere de sahiptir. Bu

noktada mahremiyet olgusu, bireysel, kültürel, toplumsal ve politik düzeyde çok katmanlı roller üstlenmektedir.

Nitekim literatürde mahremiyetin toplumsal düzeni sağlamada işlevsel olduğu vurgulanmaktadır (Rachels, 1975). Bireyler çoğunlukla yalnız kaldıklarında sergiledikleri davranışları, toplum içinde göstermemekte; bu da mahremiyetin yalnızca bireysel ilişkileri değil, toplumsal etkileşimleri de düzenlediğini göstermektedir (Yörükan, 2024). Mahremiyetin bu düzenleyici rolü, demokratik toplumlarda daha da kritik hâle gelir. Gavison'a (1980) göre mahremiyet, demokratik görüşlerin gelişebilmesi için vazgeçilmez bir koşuldur; çünkü birlikte yaşam kültürünün temelini bireylerin sınırlarına saygı oluşturur.

Toplumsal sistemlerin büyümesi ve bireyler arası iletişimin daha karmaşık hâle gelmesiyle birlikte, mahremiyetin iletişim süreçlerindeki işlevi de ön plana çıkmaktadır. Yüksel'in (2003) belirttiği üzere, bireyler iletişim kurarken kimi zaman üçüncü kişilerin bu iletişime dâhil olmasını istemeyebilir; burada da devreye mahremiyetin sunduğu denetim gücü girer. Birey, kimlerle ne zaman ve nasıl iletişim kuracağına kendi iradesiyle karar verebilmekte, böylece hem özel bilgilerini hem de toplumsal itibarını koruyabilmektedir. Lokke'ye (2018) göre ise bireyin itibarı, toplumdaki yerini belirler ve bu da özgürlüğünün bir parçası olarak değerlendirilir.

Mahremiyetin bu çok katmanlı işlevleri elbette yalnızca dijital ortamlara özgü değildir; bireyin toplumsal yaşamda sınırlarını koruyabildiği her bağlamda işlevseldir. Ancak bu işlevlerin dijitalleşmeyle birlikte görünürlüğü ve kırılganlığı artmış, özellikle genç bireyler açısından yeni risk alanları ortaya çıkarmıştır. Dolayısıyla bu çalışmada, mahremiyetin söz konusu işlevlerinin dijital ortam bağlamında nasıl anlam kazandığı üzerinde durulmaktadır. Bu bağlamda dijital mahremiyet, yalnızca teknik bir güvenlik sorunu değil; bireyin sınırlarını koruyarak güçlenmesini, özerkliğini ve toplumsal konumunu sürdürebilmesini sağlayan temel bir unsurdur.

1.2.2. Dijital Mahremiyetin Boyutları

Dijital mahremiyet, bireyin çevrim içi dünyada varlığını kontrol etme ve kişisel verilerini koruma potansiyeli olarak açıklanan çok katmanlı bir yapıdır. Bu çok katmanlı yapının hangi alanlarda nasıl ortaya çıktığını sistematik şekilde değerlendirilmesi gerekmektedir. Tezin probleminde dikkat çekilen dijital mahremiyet farkındalığı ile siber mağduriyet arasındaki ilişkisinin anlaşılabilmesi için bireylerin hangi alanlarda mahremiyet hakkına sahip olduklarını öğrenmeleri ve bu alanları koruyabilme becerilerini keşfedebilmeleri oldukça önemlidir. Bu sebeple dijital mahremiyetin sadece bir ilke olmadığı; bilgi paylaşımı,

iletiřim, dijital iz takibi ve çevrim içi alan yönetimi gibi özgül boyutlara ayrılarak incelenmesinin gerekli olduđu fark edilmektedir. Bu başlık altında da dijital mahremiyetin temel boyutları açıklanmış, bireylerin çevrim içi ortamlarda karşılaştığı risklerin nerelerde yoğunlaştığı ve farkındalığın hangi alanlarda kritik hâle geldiğı üzerinde durulmuştur.

1.2.2.1. Bilgi (Veri) Mahremiyeti

Bilgi (veri) mahremiyeti, bireylerin dijital ortamlarda kendisine ait kişisel verilerin toplanması, saklanması, işlenmesi ve paylaşılması süreçleri üzerinde kontrol ve denetim hakkına sahip olması anlamına gelmektedir. Özellikle dijitalleşmenin hız kazandığı çağımızda bireylerin kimlik bilgileri, dijital ortamdaki davranışları ve paylaşımları giderek daha fazla görünür hâle gelmektedir. Bu durum da kişisel verilerin mahremiyetle olan ilişkisini dah ada karmaşıklaştırmaktadır. 6698 sayılı Kişisel Verilerin Korunması Kanunu'na (KVKK) göre kişisel veri, “kimliğı belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi” olarak tanımlanmaktadır. Bu tanıma göre, kişisel veriler yalnızca ad, soyad, T.C. kimlik numarası gibi temel bilgileri değil, ayrıca parmak izi, konum verileri, sosyal medya paylaşımları ve dijital etkileşim geçmişı gibi bütün bilgileri kapsamaktadır (KVKK, md. 3; Tan & Pivot, 2015). Bu tür bilgilerin çevrim içi dünyada bireyin rızası dışında toplanması ve dolaşıma girmesi, veri mahremiyetinin ihlali anlamına gelmektedir. Yüksel'e (2003) göre, bireyler dijital ortamlarda kendi mahremiyetlerinin yanı sıra farkında olmadan başkalarının mahremiyetlerini de ihlal edebilmektedir. Nitekim dijital ortamda yayınlanan bir görsel ya da konum bilgisi, yalnızca bireyin değil, ailesinin ya da yakın çevresinin kişisel alanına dair verilerin ifşasına neden olabilmektedir (Güllük, 2014). Görüldüğü üzere bilgi mahremiyeti bireysel bir koruma alanı değildir, aynı zamanda toplumsal düzlemde de dikkat edilmesi gereken bir hak alanıdır. Dolayısıyla dijital mahremiyetin bu boyutu, bireyin hem özel hayatını hem de saygınlığını tehdit edebilecek düzeyde etkili olabilmesi nedeniyle teknik, hukuki ve ahlaki açılardan ele alınmalı ve korunmalıdır (Çalık, 2018).

1.2.2.2. İletişim Mahremiyeti

İletişim mahremiyeti, bireyin kimlerle, ne zaman ve hangi içerikle iletişim kuracağıının üçüncü kişilerce izlenmemesi ve bu iletişimin bireysel kontrol altında kalması olarak açıklanabilmektedir. Mahremiyetin bu boyutu; mesajlaşma uygulamaları, e-posta, sesli ve görüntülü aramalar gibi bireysel iletişim araçları üzerinden yürütölen bütün özel haberleşmeleri içermektedir. Bu boyutta iletişimdeki içeriğın yanı sıra iletişimin zamanı, sıklığı ve kiminle kurulduğı bilgisi de önemli sayılmaktadır. Bireyin iletişim trafiğı üzerindeki kontrolünü

kaybetmesi, yalnızca mahremiyet ihlali olarak düşünülmemelidir. Bu durum bireyde psikolojik güvenlik kaybına yol açabilmekte ve bireyin çevrim içi istismara açık hâle gelmesi riskini taşımaktadır. Özellikle gençlerin dijital ortamlarda özel mesajlarının izinsiz şekilde üçüncü kişilerce ifşa edilmesi, siber zorbalık, tehdit veya sosyal dışlanma gibi sonuçlar doğurabilmektedir. Bu doğrultuda iletişim mahremiyeti, sadece bireysel özgürlük açısından değerlendirilmemelidir. İletişim mahremiyeti aynı zamanda sosyal güvenliğin de önemli bir bileşeni olarak ele alınmalıdır.

1.2.2.3. Davranışsal Mahremiyet / Dijital Ayak İzi

Davranışsal mahremiyet (dijital ayak izi) ise, bireylerin hangi siteleri ziyaret ettiği, ne zaman çevrim içi olduğu, neleri beğendiği, hangi içeriklerle ne kadar süre etkileşimde bulunduğu gibi dijital ortamlarda gerçekleştirdikleri faaliyetleri kapsamaktadır ve bireylerin bu dijital izlerinin izlenmesi ve analiz edilmesine karşı korunma hakkını ifade etmektedir. Bu boyut ile bireylerin dijital ayak izleri üzerinden oluşturulan davranışsal profillerin, bireyin bilgisi ve rızası dışında kullanılması tehlikesine odaklanılmaktadır (Goethals vd., 2025). Yaşadığımız dijital çağda bireylerin farkında olmadan çevrim içi dünyaya bıraktığı veriler, onların özel yaşamı, inançları, tercihlerine dair hassas çıkarımlar yapılmasına olanak tanımaktadır. Zuboff (2019), bu süreçleri “gözetim kapitalizmi” olarak adlandırmaktadır. Ayrıca bu gözetim kapitalizmi ile dijital davranışların izlenmesinin bireylerin yalnızca gizliliğini değil, özerkliğini ve özgür karar alma yetilerini de zedelediğini belirtmektedir. Tan ve Pivot’un aktardığına göre ise, çevrim içi ayak izleri üzerinden bireylerin cinsel yönelimi, siyasi inancı, sağlık durumu gibi mahrem alanlara dair çıkarımlar yapılabilmekte ve bu durum, bireyleri dijital ortamda manipülasyon, ayrımcılık ya da dışlanma gibi risklerle karşı karşıya bırakabilmektedir (Çalık, 2018). Bu bilgiler ışığında görülmektedir ki, davranışsal mahremiyet, yalnızca veri güvenliği ile ilgili değildir. Aynı zamanda bireyin düşünsel ve sosyal bütünlüğünü korumaya yönelik çok boyutlu bir mahremiyet alanını oluşturmaktadır.

1.2.2.4. Mekânsal Mahremiyet (Dijital Uzamda)

Son olarak mekânsal mahremiyete bakıldığında; konut, oda, aile içi çevre gibi özel alanların bireyin fiziksel yaşam alanını oluşturduğu ve bireylerin bu özel alanların gizliliğini koruma hakkına sahip olduğu görülmektedir. Dijital uzamda mekânsal mahremiyet ile bu hakkın dijitalleşmeyle beraber bireylerin sadece fiziksel değil, çevrim içi platformlarda inşa ettikleri dijital alanları da kapsayarak yeni bir anlam kazanmaya başladığı vurgulanmaktadır. Çalık (2018) sosyal medyanın kullanıcıların özel hayatlarına dair fotoğraf, video ve konum gibi

içerikleri paylaşımlarına imkân tanıdığını ve bu platformların geleneksel mekânsal mahremiyet anlayışının dönüşümüne neden olduğunu dile getirmektedir. Özellikle ev ortamına ilişkin paylaşımlar, bireyin ailesiyle beraber yaşamını sürdürdüğü alanları kamusal alana taşımakta hem kendisinin hem de çevresindekilerin özel alanlarını görünür hâle getirmektedir (Güllük, 2014). Yüksel (2003), bu tür paylaşımların mekânsal mahremiyetin bulanıklaşmasına ve bireyin çevrim içi alanlarının dışarıdan müdahaleye açık hâle gelmesine zemin hazırladığını belirtmektedir. Bu durumda dijital mekânsal mahremiyetin, bireyin fiziksel alanlarıyla birlikte dijital varlığını da koruyabilmesi ve sınırlarını bilinçli şekilde belirleyebilmesi açısından kritik öneme sahip olduğu ileri sürülebilmektedir.

Özetle, dijital mahremiyet çok boyutlu bir yapıya sahiptir ve bilgi, iletişim, davranışsal ve mekânsal mahremiyet gibi farklı alanlarda bireyin dijital ortamdaki varlığını doğrudan etkileyen unsurlar barındırmaktadır. Bu boyutların her biri, bireyin çevrim içi dünyada sınırlarını ne ölçüde tanıyabildiği ve bu sınırlara ne ölçüde sahip çıkabildiğiyle ilgilenmektedir. Dolayısıyla, dijital mahremiyet farkındalığını değerlendirmek için genel bir kavrayış yetmemektedir. Bireyin bu özgül boyutlara ilişkin bilgi ve bilinç düzeyi, bireyin farkındalığı ile doğrudan ilişkilidir. Bu sebeple bu konu da önem arz etmektedir.

Tüm bunlara rağmen bireyin dijital ortamdaki sınırları tanınması ve korunması, her zaman kendi kontrolünde gerçekleşmemektedir. Bireyler çevrim içi dünyada çeşitli tehdit ve ihlaller nedeniyle siber taciz, kişisel veri sızdırılması, dijital gözetim ya da çevrim içi manipülasyon gibi risklerle baş başa kalabilmektedir. Budan dolayı bir sonraki başlıkta, dijital mahremiyetin günümüzde ne tür tehditlerle karşı karşıya kaldığı ve bireylerin bu tehditlere karşı hangi bireysel ya da kurumsal korunma stratejilerini geliştirebildiği değerlendirilmiştir.

1.2.3. Dijital Mahremiyetin İhlal Riskleri ve Korunma Stratejileri

Dijital mahremiyetin sadece kavramsal bir hak olarak tanımlanması yeterli olmamaktadır. Dijital mahremiyet, aynı zamanda bireylerin ne tür risklerle karşı karşıya kalabileceğini ve karşılaştığı bu risklerden nasıl korunabileceğini sistemli ve bilinçli şekilde ele almayı gerektiren kritik bir alandır. Özellikle gençlerin çevrim içi ortamlarda yoğun şekilde varlığını sürdürüyor olmaları onları kişisel veri sızıntısı, siber taciz, gözetim ve kimlik hırsızlığı gibi dijital tehditlere karşı açık hedef konumuna getirebilmektedir. Bu nedenle dijital mahremiyetin korunmasına yönelik hem bireysel hem de kurumsal düzeyde çeşitli stratejilerin geliştirilmesi zorunlu hale gelmiştir.

Mahremiyet İhlallerinin Dijital Biçimleri:

İnternet, bireylerin iletişim kurma, bilgiye erişme ve kendilerini ifade etme biçimlerini köklü biçimde dönüştürmüştür; ancak bu dönüşüm aynı zamanda yeni türden mahremiyet ihlallerine de zemin hazırlamıştır. Literatürde çevrim içi ortamlarda maruz kalınan mağduriyetler arasında dijital dolandırıcılık ve hırsızlık, siber takip ve taciz, özel yaşamın ifşası, bilgi kirliliği, internet bağımlılığı, kaba ve nefret söylemleri yer almaktadır (Mitchell, Finkelhor & Wolak, 2003; Özkaya, 2023). Bu tehditlerin ortak yönü, bireylerin rızası olmaksızın özel bilgilerinin ifşa edilmesi veya manipüle edilmesidir. Özellikle genç bireylerin sosyal medya kullanım sıklığı ve dijital iz bırakma eğilimleri, onları bu tür ihlaller açısından daha kırılgan bir konuma taşımaktadır.

Bireysel Korunma Stratejileri:

Dijital mahremiyetin korunmasında bireylere önemli sorumluluklar düşmektedir. Mahremiyet ihlallerinden kaçınmak için kişisel verilerin paylaşımında dikkatli olunmalı, çevrim içi platformların gizlilik politikaları dikkatle incelenmeli ve kullanıcıların güvenlik ayarlarını bilinçli biçimde yapılandırılmaları sağlanmalıdır. Dijital okuryazarlık, bu bağlamda yalnızca teknik becerileri değil, aynı zamanda bireyin çevrim içi ortamda karşılaşılabileceği riskleri tanıma ve uygun tepki geliştirme yeteneğini de kapsamaktadır (Diler, 2014). Ayrıca gelişim dönemine uygun dijital mahremiyet eğitimi, bireylerin çocukluk ve ergenlik döneminden itibaren bu konuda bilinçli davranışlar geliştirmesine katkı sunmaktadır (Canbay & Sağıroğlu, 2020).

Kurumsal ve Hukuki Yaklaşımlar:

Bireysel çabaların yanı sıra, dijital mahremiyetin etkili biçimde korunması için kurumsal ve yasal düzenlemeler de büyük önem taşımaktadır. İnternet ortamında bireyleri koruma sorumluluğu yalnızca bireyin kendisine değil, aynı zamanda devlete ve ilgili kurumlara da aittir. Türkiye’de bu sorumluluk büyük ölçüde Bilgi Teknolojileri ve İletişim Kurumu (BTK) tarafından yürütülmekte olup; kişisel verilerin korunmasına yönelik düzenlemeler 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) kapsamında şekillenmektedir (Gürkan, 2013). Bu tür yapısal ve düzenleyici önlemler, bireylerin mahremiyet haklarını gözetme açısından bir güvenlik çerçevesi sunmaktadır.

Dijital mahremiyetin ihlal edilme şekilleri, sadece bireylerin bilgi güvenliğini etkilememektedir. Ayrıca bireylerin psikolojik bütünlüğünü, sosyal ilişkilerini ve öz saygısını da tehdit edebilmektedir. Dolayısıyla çevrim içi ortamda karşılaşılan risklerin tanınarak bu risklere karşı etkili bireysel, kurumsal ve yasal stratejilerin geliştirilmesi hem bireyin haklarını korumak hem de dijital farkındalığı güçlendirmek amacıyla temel bir gereklilik hâline

gelmiştir. Bir sonraki başlıkta, bu gerekliliğin en önemli bileşenlerinden biri olan dijital mahremiyet farkındalığı kavramı üzerinde durulmuş ve bu farkındalığın bireylerin çevrim içi deneyimlerini nasıl şekillendirdiği tartışılmıştır.

1.3. Dijital Mahremiyet Farkındalığı

Dijital mahremiyet farkındalığını daha iyi anlamlandırabilmek amacıyla öncelikle farkındalık kavramı ve bileşenlerini açıklamak önemlidir. Bu nedenle bu başlık altında öncelikle farkındalık kavramı ve bileşenlerine değinilmiş daha sonra gençlerde dijital mahremiyet farkındalığı ve koruma davranışları ele alınmıştır. Son olarak da farkındalığın bireysel güçlenmeye katkısı açıklanmıştır.

1.3.1. Farkındalık Kavramı ve Bileşenleri

Farkındalık; bireylerin düşünceleri, duyguları, davranışları ve çevresi hakkında bilinçli olma hali olarak ifade edilebilmektedir. Yargısız biçimde şu ana odaklanabilmek için dikkatini toplayabilmek olarak da tanımlanabilmektedir (Kabat-Zinn, 2013).

Deneyimin yargılayıcı olmadan izlenmesi, kasıtlı dikkat ve öz-sorgulama olarak açıklanan farkındalık bir bilinç durumudur (Diaz, 2022). Bu bilinç durumu iki bileşeni içermektedir. Bu bileşenler: yargılayıcı olmayan kabul ve yönlendirilmiş dikkattir. Bu iki bileşen sayesinde bireylerin bilişsel ve zihinsel sağlıkları olumlu etkilenebilmekte ve çeşitli etkinliklerde performansları artabilmektedir (Fey, 2019).

Farkındalık tanımlarının çeşitliliği nedeniyle bu iki bileşenden başka bileşenlerden de söz edilmektedir. Bu bileşenden bazılarının şimdiye odaklı dikkat, içsel gözlem, yargılamama ve kabul olduğu söylenebilmektedir (Çatak & Ögel, 2010). Ayrıca Shapiro ve meslektaşları (2006) farkındalığın temel bileşenlerinin tutum, dikkat ve niyet olduğunu öne sürmektedir. Tutum bileşeninin yargısız olma, güven, sabır, zorlayıcı olmama ve merak gibi unsurları içerdiğini savunmaktadırlar (Bishop vd., 2004). İkinci bileşen olan dikkati odaklanmış, yayılmış ve sürdürülebilir olarak tanımlayarak bir uyarandan diğerine dikkati çevirebilme becerisini de kapsadığını belirtmişlerdir (Burke, 2010). Niyeti ise dikkati odaklama, sürdürme ve başka yöne odaklanma niyeti gibi geniş bir yelpazede ele almaktadırlar (Bishop vd., 2004).

1.3.2. Gençlerde Dijital Mahremiyet Farkındalığı ve Koruma Davranışları

Bu kısımda, dijital mahremiyetin gençler üzerindeki yansımaları farkındalık düzeyleri ve koruma davranışları işlenmiştir. Üniversite çağındaki gençler hem teknolojik araçları çokça kullanmakta hem de gelişimsel olarak kimlik arayışında olabilmektedirler. Bu sebeple gençler

mahremiyet sınırlarının en hassas biçimde şekillendiği gruplardan birini oluşturmaktadırlar. Bu doğrultuda bu başlıkta, tezin temel problemlerinden biri olan dijital mahremiyet farkındalığının düzeyi ve bunun bireylerin dijital ortamlarda maruz kalabileceği risklerle ilişkisi incelenmiştir. Araştırmanın amacının, genç bireylerin -özellikle üniversite öğrencilerinin- dijital mahremiyet konusundaki farkındalık düzeyleri ve bu bağlamda sergiledikleri koruyucu davranış örüntülerinin daha iyi anlaşılabilmesi olması nedeniyle literatürde yer alan diğer çalışmalar irdelenerek bu araştırmaların bulgularına başvurulmuştur. Böylelikle aşağıda hem Türkiye’de hem de uluslararası alanda bu konuda yapılmış çalışmaların bazı öne çıkan bulguları tematik olarak sunulmuştur.

1.3.2.1. Sosyo-Demografik Değişkenlere Göre Mahremiyet Farkındalığı

Dijital mahremiyet farkındalığı bireyler arasında homojen bir biçimde dağılmamakta; cinsiyet, yaş, eğitim düzeyi, internet deneyimi, kültürel değerler gibi demografik faktörlere göre anlamlı farklılıklar göstermektedir (Cho, Rivera-Sánchez ve Lim, 2009).

Bu değişkenlere ilişkin farklılıklar, bireylerin dijital ortamda mahremiyetlerini algılamaları, ihlal risklerini değerlendirmeleri ve koruyucu davranışlar geliştirmeleri üzerinde doğrudan etkilidir (Choi, Park & Jung, 2018).

Literatür tarandığında dijital mahremiyet farkındalığını etkileyen sosyo-demografik değişkenler arasında yaşın önemli unsurlardan biri olduğu görülmektedir. Bu doğrultuda farklı yaş gruplarıyla yürütülen çeşitli çalışmalar incelendiğinde, yaşa bağlı olarak mahremiyet algısının, bu algıya yönelik endişelerin ve bireylerin gizlilik ihlallerine karşı geliştirdikleri korunma stratejilerinin farklılık gösterdiği ortaya çıkmaktadır. Örneğin, Bietz ve arkadaşları (2019) farklı yaş gruplarının gizliliğe ilişkin farklı tutum ve yaklaşımlar sergilediğini belirtirken De Wolf (2019) yaş ilerledikçe bireylerin kişisel mahremiyeti daha etkin biçimde yönetebildiklerini ifade etmiştir. Benzer şekilde, Çaycı ve Karagülle’nin (2014) yürüttüğü çalışmada X, Y ve Z kuşaklarının mahremiyet algıları karşılaştırılmış ve Z kuşağının mahremiyet algısının diğer kuşaklara göre daha yüksek olduğu, bu kuşağın gerçek ve sanal dünyadaki mahremiyet sınırlarını benzer şekilde değerlendirdiği belirtilmiştir. Aynı çalışmada, Z kuşağının özel bilgilerini korumak amacıyla sahte hesaplar oluşturma gibi stratejiler geliştirebildiği de aktarılmıştır.

Ancak bu tez çalışmasında, araştırmanın amacı ve örneklem yapısı gereği yaş değişkeni ayrı bir başlık altında tematik olarak ele alınmamakta ve sabit bir değişken olarak kabul edilmektedir. Çalışma, yalnızca üniversite öğrencilerinden oluşan genç bir yaş grubuna odaklanmaktadır. Bu yaş grubu içerisinde belirleyici olan cinsiyet, eğitim düzeyi gibi diğer

sosyo-demografik deęişkenler çerçevesinde bir araştırma yürütölmektedir. Buna baęlı olarak, dijital mahremiyet farkındalıęına ve korunma davranışlarına ilişkin tüm tartışmalar, yaşı deęişkeni sabit tutularak deęerlendirilmiş hem alanyazından aktarılan örnekler hem de elde edilen sonuçlar bu yaşı grubuna özgü bağlamda yorumlanmıştır.

Cinsiyet, sosyo-demografik deęişkenler arasında dijital mahremiyet farkındalıęını etkileyen önemli bir unsurdur. Bireyin dijital ortamlarda mahremiyet algısı ve koruma yönünde geliştirdięi tutumlar, cinsiyet temelli olarak anlamlı farklılıklar gösterebilmektedir. Literatürde dijital mahremiyet farkındalıęının cinsiyet temelli olarak anlamlı biçimde farklılaştıęını gösteren çok sayıda araştırma bulunmaktadır.

Örneęin yürütölen bir çalışmada (Sepetci, 2017), genç bireylerin sosyal medya uygulamalarının gizlilik politikalarını çoęunlukla okumadıkları ve mahremiyet ihlali riski taşıyan paylaşımları sıklıkla yaptıkları belirlenmiştir. Ancak aynı çalışmada, kadın katılımcıların erkeklere kıyasla mahremiyete daha fazla önem verdikleri ve daha temkinli bir dijital davranış sergiledikleri vurgulanmıştır. Çakır ve meslektaşlarının (2015) öęretmen adaylarıyla gerçekleştirdięi araştırma, yüksek eğitim düzeyine sahip bireylerde genel olarak gizlilik farkındalıęının yüksek olduęunu göstermiş; bununla birlikte kadın katılımcıların farkındalık düzeylerinin erkeklere kıyasla anlamlı düzeyde daha yüksek olduęunu saptamıştır. Bu durum, eğitim seviyesi yükseldikçe genel risk farkındalıęı artsa bile, cinsiyet temelli farklılıkların korunduęunu göstermektedir. Yurt ii- yurt dışı alanyazında kadın öęrencilerin erkek öęrencilere kıyasla çevrim ii mahremiyet farkındalıklarının yüksek olduęunu, dijital mahremiyetlerine daha fazla önem verdiklerini ve gizlilikle ilgili önlemleri daha dikkatli uyguladıklarını ortaya koyan pek çok çalışma (De Wolf, 2019; Topbaşı & Gazi, 2016; Töngel, 2020) mevcuttur.

Genç kadınların dijital ortamda mahremiyet konusuna erkeklere kıyasla daha duyarlı yaklaştıkları, risk algılarının erkeklerden daha yüksek olduęu ve daha sık koruyucu stratejiler benimsediklerini ortaya koyan bu çalışmalar, mahremiyet farkındalıęında toplumsal cinsiyet rolleriyle şekillenen algı ve tutumların da biçimlendirici bir role sahip olduęunu göstermektedir.

Eğitim düzeyi, bireyin dijital ortamlardaki davranışlarını şekillendiren temel deęişkenlerden bir dięeridir. Birey, eğitim yoluyla yalnızca teknik bilgi deęil; aynı zamanda eleştirel düşünme, öngörü geliştirme ve haklarının farkına varma gibi yetkinlikler de edinir. Literatürde, eğitim düzeyinin artmasıyla birlikte dijital mahremiyet farkındalıęının da yükseldięi, bireylerin kişisel veri güvenlięi, gizlilik ayarları ve çevrim ii davranışlar konusunda daha bilinli tercihler yaptıęı görölmektedir. Eğitim, aynı zamanda bireyde sosyal

sorumluluk, öz denetim ve risk algısının gelişmesini sağlayarak, dijital ortamda daha koruyucu ve öngörülü stratejiler benimsenmesine zemin hazırlamaktadır.

Nitekim gerek ulusal gerekse uluslararası alanda yürütülen çalışmalar, eğitim düzeyinin dijital mahremiyet farkındalığı üzerinde belirgin bir fark yarattığını ortaya koymaktadır. Yürütülen bir çalışmada (Korucu & Gürkez, 2019) bireylerin çevrim içi mahremiyet farkındalıkları ile eğitim seviyesi (sınıf düzeyi) arasında anlamlı bir ilişki olduğunu ortaya konulurken; bir başka araştırmanın (Kantar Özkes, 2023) bulguları, eğitim düzeyi yükseldikçe mahremiyet farkındalığının da istatistiksel olarak anlamlı biçimde arttığını göstermektedir. Bu çalışmada bireylerin dijital mahremiyet farkındalıklarının yıllar içinde artış gösterdiği, bu farkındalık artışının en önemli belirleyicilerinden birinin eğitim düzeyi olduğu ortaya konmuştur.

Benzer şekilde, bir başka çalışmada (Türten, 2018), katılımcıların eğitim hayatları boyunca edindikleri dijital mahremiyet bilgisi sayesinde sosyal medya kullanımlarında mahremiyete yönelik daha yüksek bir duyarlılık geliştirdikleri; bu farkındalığın da onları daha temkinli ve koruyucu dijital davranışlar geliştirmeye yönlendirdiği anlaşılmaktadır.

Bir başka çalışmada (Boerman vd., 2018) eğitim düzeyi yüksek olan bireylerin çevrim içi mahremiyetlerini korumaya yönelik çerezleri silme, tarayıcı geçmişini temizleme veya veri paylaşımını reddetme türünden davranışları, bilinçli ve sistematik bir korunma stratejisi olarak uyguladıkları anlaşılmıştır. Bu bulgulara dayanarak, artan eğitim seviyesiyle birlikte dijital mahremiyet farkındalığının yalnızca bilişsel değil, aynı zamanda davranışsal düzeyde de güçlendiği ifade edilebilir.

Küresel ve ulusal sahaya dayalı bu bulgular dijital mahremiyet farkındalığının bireylerin yaş, cinsiyet, eğitim düzeyi gibi sosyo-demografik özelliklerinden etkilendiğini göstermektedir. Bu değişkenler, bireylerin çevrim içi riskleri nasıl algıladığını ve bu risklere karşı nasıl stratejiler geliştirdiğini belirlemede önemli bir rol oynamaktadır.

1.3.2.2. İnternet Kullanım Alışkanlıkları ve Mahremiyet Farkındalığı

Gençlerin yoğun olarak kullandığı dijital ortamların başında sosyal medya platformları gelmektedir. Bireyler bu platformlar aracılığıyla hem kendilerini ifade etmekte hem de çeşitli sosyal ilişkiler kurabilmektedir. Dolayısıyla bireylerin mahremiyet farkındalıklarının sınıandığı temel ortamları da bu platformlar oluşturmaktadır. Yapılan çalışmalar ile mahremiyet farkındalığına dair çarpıcı sonuçlar ortaya konmakta ve dijital ortamda korunma stratejilerine yönelik bilgiler sunulmaktadır. Aşağıda örneklenen bu çalışmalarda korunma stratejilerinin bilgi düzeyi, kullanım alışkanlıkları ve kişisel risk algısına göre değişkenlik gösterdiği ifade

edilmektedir. Özellikle sosyal medyada geçirilen sürenin artması, gizlilik ayarlarının kullanımında dikkatsizlik ve mahremiyet ihlallerine rağmen platform kullanımının devam etmesi gibi sonuçlar, dijital mahremiyet farkındalığının ne derece davranışa dönüştüğü sorusunu da gündeme getirmektedir.

Çalışmalar, genç bireylerin dijital mahremiyet farkındalığına sahip olduklarını düşündüklerini, ancak bu farkındalığın çoğu zaman yüzeysel kaldığını göstermektedir. Örneğin Eroğlu'nun (2018) çalışmasında üniversite öğrencilerinin kişisel verilerin ne olduğu konusunda kendilerine güvendikleri ancak bu verileri net şekilde tanımlamakta zorlandıkları tespit edilmiştir. Çalışmalar (Cho vd., 2009) çevrim içi gizliliğin küresel düzeyde çoğu internet kullanıcılarını etkileyen önemli bir endişe olduğunu; bununla birlikte gençlerin kişisel verilerin korunmasına yönelik yasal düzenlemeler hakkında yeterli bilgiye sahip olmadıklarını ve bu bakımdan da kaygıların davranışlarını değiştirmediklerini (Altıntaş Var, 2022) ortaya koymaktadır. Örneğin yürütülen bir başka çalışmada (Debatin vd., 2009) gizliliğin kendileri için endişe kaynağı olduğunu belirten gençlerin Facebook'a büyük miktarda kişisel bilgi yükledikleri ortaya konulmuştur.

Farkındalığın düzeyini etkileyen en belirgin değişkenler arasında sosyal medya kullanım süresi, interneti kullanma amacı, arkadaş sayısı ve deneyimlenen gizlilik ihlalleri yer almaktadır. Mevcut çalışmaların en önemli bulgularından biri, internette-sosyal medya platformlarında geçirilen süre ile mahremiyet farkındalığı arasında ilişkidir. Örneğin Korucu ve Gürkez (2019) çalışmalarında, internet bağlantılı mobil cihaz kullanım süresi arttıkça mahremiyet farkındalığının azalarak daha riskli dijital davranışların gözlemlendiğini ortaya koyarken; Topbaş ve Gazi (2016) ise çalışmalarında bunun tam tersi bulgular elde etmiş; gençlerin sosyal medya kullanım süreleri ile gizlilik farkındalıkları arasında pozitif bir ilişki olduğu sonucuna varmıştır. Söz konusu çalışmada olumsuz bir gizlilik deneyiminin bu farkındalığı artırdığı, bu deneyimden “ders” çıkaran gençlerin sonrasında gizliliğe daha fazla önem verdikleri anlaşılmıştır. Bir başka anlatımla internette geçirilen süre olumsuz deneyim riskini artırırken bu deneyimler ise farkındalık ve korunma arzusu kazandırır görünmektedir. Çalışmalar arasındaki bu farklılık, bazı çalışmalarda internetin kullanım amacıyla ilişkilendirilmiştir. Nitekim Öz'ün (2014) araştırması, sosyal medyayı haber takibi için kullanan bireylerin daha yüksek gizlilik farkındalığına sahip olduğunu ortaya koymuştur.

Sosyal çevrenin genişliği de farkındalık üzerinde etkili görünmektedir. Topbaş ve Gazi (2016), sosyal medya arkadaş sayısı arttıkça bireylerin gizliliğe verdikleri önemin azaldığını belirtmiştir. Bu bulgu, dijital görünürlüğün artmasının mahremiyet sınırlarını zayıflatabileceğine işaret etmektedir.

Sahaya dayalı bu araştırma bulguları, sosyo-demografik değişkenlerin yanı sıra dijital deneyimler, interneti kullanım biçimleri, sosyal medya platformlarındaki görünürlük ve network genişliği gibi değişkenlerin gençlerin mahremiyet farkındalıkları üzerinde etkili unsurlar olduğunu ortaya koymaktadır. Mevcut bulgular gençlerin çoğu zaman mahremiyetin farkında olduklarını düşünme eğilimde olduklarını ancak; bu farkındalığın bilgi düzeyi ve davranışa yansıma açısından yüzeysel kaldığını göstermektedir. Bir başka anlatımla, gençler tarafından mahremiyetin sakıncalı ihlallerle ilişkili olduğu algılansa da bu algı her zaman bilinçli ve tutarlı bir dijital davranışla desteklenmemektedir. Ancak buna rağmen, dijital mahremiyet farkındalığına sahip bireylerin, risklere karşı daha koruyucu stratejiler geliştirebildiklerini gösteren çalışmalar (Davis & James, 2012) mevcuttur.

Örneğin Öz'ün yürüttüğü çalışmada (2014) mahremiyet farkındalığının artmasıyla birlikte gençlerin bazı sosyal medya hesaplarını kapatma ihtimalinin güçlendiği belirlenmiştir. Benzer şekilde yürütülen bir başka çalışmada (Boerman vd., 2018) kişisel bilgilerinin toplanması, kullanılması ve paylaşılmasını ciddi bir mahremiyet sorunu olarak algılama eğilimindeki gençlerin çevrim içi gizliliklerini nadiren koruyamadıkları, çerezleri reddetme-silme ve tarayıcı geçmişini silme gibi davranışların da çevrim içi gizliliklerini koruma stratejileri olduğu anlaşılmıştır. Bir başka çalışmada (Dowd, 2011) ise öz yeterlik/yeteneklerin, mahremiyeti kaybı endişesi ile mücadele stratejisi oluşturduğu anlaşılmıştır. Bu çalışmada internet-sosyal medya kullanıcısı gençlerin çevrim içi mahremiyetleri konusunda endişe duydukları, mahremiyet ihlalinin itibarlarını zedeleyebileceğini düşündükleri ve çevrim içi mahremiyetlerini yönetmek için ise kendi yeteneklerine güvendikleri ortaya konmuştur.

Öte yandan, farkındalığın korunma davranışı geliştirmede ortaya koyan çalışmalar da mevcuttur. Örneğin yürütülen bir çalışmada (Aslanyürek, 2016) genç internet kullanıcılarının çevrim içi gizlilik ve güvenlik ihlalleri karşısında yüksek farkındalığa sahip oldukları; buna karşın ihlallerin varlığına rağmen internet kullanımını azaltma eğilimi göstermedikleri tespit edilmiştir. Benzer şekilde, bir başka çalışmada (Sepetci, 2017) sosyal medya platformlarının güvensiz olduğunu düşünme eğilimi yüksek olan genç kullanıcıların bu buna rağmen paylaşım sıklıklarının yüksek olduğu ve kişisel bilgilerini, aile ve diğer kişilerin fotoğraflarını paylaşarak riski göze aldıkları belirlenmiştir. Başka bir çalışmada ise (Youn, 2009) bireylerin gizlilik endişelerinin, bilginin ifşa edilmesinden doğan risk algısına bağlı olarak arttığı; ancak bu bilginin kendilerine fayda sağlayacağına inandıklarında ise bilgilerini paylaşmakta sakınca görmedikleri anlaşılmıştır. Bu durumda odaklanılan kazançlar, korunma davranışının geliştirilmesine engel oluşturur görünmektedir. Bu durum, bireylerin farkındalık düzeyleri yüksek olsa dahi, çeşitli psikolojik, sosyal veya pragmatik gerekçelerle bilinçli

biçimde korunma davranışından uzak durabildiklerini göstermektedir. Örneğin sosyal kabul görme arzusu, dijital görünürlük isteği, fayda beklentisi veya “bana bir şey olmaz” algısı gibi unsurlar, bireyin mevcut riskleri bilmesine rağmen riskli dijital davranışları sürdürme iradesini kullanarak bilinçli olarak korunmama yönünde bir tutum gerçekleştirmesinde etkili olabilir.

Erişilen tüm bu bulgular bir arada değerlendirildiğinde, mahremiyet farkındalığının çok boyutlu ve değişken bir yapıda olduğu görülmektedir. Farkındalık düzeyinin bireylerin çevrim içi dünyadaki davranışlarını doğrudan şekillendirdiği tespit edilmektedir. Fakat bu davranışların her zaman korunma stratejilerine dönüşmediği de anlaşılmaktadır. Sosyo-demografik değişkenlerle beraber sosyal medya deneyimleri, kullanım alışkanlıkları ve bireysel motivasyonlar bireylerin mahremiyet farkındalığını şekillendirmektedir. Aynı zamanda bu farkındalığın bireyin koruma eğilimlerinin niteliğini belirlediği de ifade edilmelidir. Bu bakımdan dijital mahremiyetin yalnızca bilişsel düzeyde ele alınmasının yeterli olmadığı, bilişsel düzeyin yanı sıra bireylerin tutum ve davranışlarının da değerlendirilmesi gerektiği anlaşılmaktadır.

1.4. Siber Zorbalık ve Siber Mağduriyet

Yaşamın her alanında dijital teknolojilerin kullanılmaya başlamasıyla beraber bireylerin sosyal ilişkileri, etkileşim şekilleri ve iletişim alanları da önemli bir değişim geçirmiştir. Sosyal medya platformlarının çoğalması ve yaygınlaşması ile çevrim içi dünya bireysel ifade alanı haline gelmiştir ve bu, bireylerin hem görünürlüklerinin hem de kırılganlıklarının artmasına yol açmıştır. Böylece geleneksel şiddet türleri dijital ortama taşınmış ve yeni mağduriyet alanları ortaya çıkmıştır. Bu kapsamda da en sık karşılaşılan dijital tehditler siber zorbalık ve bunun doğurduğu siber mağduriyet olmuştur.

Dolayısıyla bu başlık altında mahremiyet farkındalığı ile doğrudan ilişkili olan siber zorbalık ve siber mağduriyet kavramları ele alınacaktır. Ancak bu araştırmanın temel odak noktası, Araştırmanın temel odak noktası, bireylerin dijital mahremiyet farkındalıklarının siber mağduriyet düzeyleriyle ilişkisini anlamaya yöneliktir. Bu nedenle bu kavramların incelenme biçimi, tezin problemi, amacı ve kuramsal çerçevesi doğrultusunda yapılandırılmıştır.

Siber zorbalık bu çalışmada bir kavram olarak ele alınmakla beraber, daha çok *mağduriyet yaratan bir etki alanı* bağlamında değerlendirilmiştir. Diğer bir deyişle, siber zorbalığın biçimlerinden daha ziyade, bu zorbalığın bireyde yarattığı mağduriyet durumları ve bu durumların bireyin dijital mahremiyet sınırlarıyla ilişkisi merkeze alınmıştır.

Siber mağduriyet ise bu bölümün temel kavramı olarak çok boyutlu şekilde ele alınmıştır. Mağduriyet kavramının tarihsel ve sosyolojik arka planı, dijitalleşme ile birlikte nasıl bir değişim geçirdiği, hangi türlere ayrıldığı ve bireysel sonuçları bu kapsamda incelenmiştir.

Bu çerçevede, siber zorbalık kısaca tanımlanarak mahremiyet ihlali ile nasıl kesiştiği ortaya konulmuş; ardından siber mağduriyet kavramı tarihsel kökeni, türleri, nedenleri ve sonuçlarıyla daha ayrıntılı olarak incelenmiş. Böylelikle bir sonraki bölümde ortaya konacak olan ilişki analizi için kavramsal bir temel oluşturulmuştur.

1.4.1. Siber Zorbalık: Dijital Mağduriyetin Kaynağı Olarak Bir Şiddet Biçimi

Siber zorbalık, dijital ortamda bireylere zarar verme amacı ile bilgisayar, cep telefonu gibi internetin yoğun olarak kullanıldığı elektronik araçlar ile kasıtlı ve sürekli gerçekleştirilen eylemler olarak tanımlanmaktadır (Willard, 2007; Hinduja & Patchin, 2010).

Dijital araçların yaygınlaşması ile mesajlaşma ve sosyal medyada paylaşım yapma gibi yollarla bireyler bilgi, görüntü ve ses dosyalarını diğer bireylere kolaylıkla gönderebilmektedir. Bu durum da zorbanın mağdura kolayca ulaşmasını sağlayabilmektedir. Ayrıca dijital ortamdaki bu dosyaların başkaları tarafından yayılma ihtimali de oldukça yüksektir (Slonje, Smith & Frisen, 2013). Görülmektedir ki dijital ortamda yayınlanan çeşitli bilgiler mahremiyet ihlaline yol açmakta ve bireyin siber zorbalığa uğrama olasılığını arttırmaktadır.

Günümüzde teknoloji ve internet kullanımının artması ile siber zorbalık yapan ve siber zorbalığa maruz kalan mağdurların sayısının da artış gösterdiği raporlanmaktadır (von Marées & Petermann, 2012). Siber zorbalık konusunda yapılan çalışmalara bakıldığında da özellikle ergenlik ve genç yetişkinlik dönemlerinde bireylerin siber zorbalığa maruz kalma ve zorba olma ihtimalinin fazla olduğu ifade edilmektedir (Šmahel ve Ševc'íková, 2009). Bu tür zorba davranışların genellikle gençler arasında, daha çok tanıdıkları bireylere yönelik olduğu ve çoğunlukla sosyal ağlar aracılığıyla gerçekleştirdikleri belirtilmektedir (Willard, 2007).

Genç yetişkinler üzerinde görülme olasılığının fazla olması sebebiyle siber zorbalığın gençler üzerindeki etkisinin incelenmesinin oldukça önemli hale geldiği görülmektedir. Sosyal medya platformlarına herhangi bir zaman kısıtlaması olmadan 24 saat erişim sağlanabilmektedir. Bu nedenle siber zorbalığa maruz kalan gencin her an zorbalık yaşayabilirim düşüncesiyle anksiyete düzeyinde artış görülebilmektedir (Raskauskas & Stoltz, 2007). Bununla beraber genç birey sosyal kaygı geliştirebilmekte ve arkadaşlarından, okulundan, iş hayatından ve ailesinden uzaklaşabilmektedir (Martínez-Monteagudo vd., 2020; Ybarra & Mitchell, 2004). Bu uzaklaşma sonucunda da depresyon gibi ciddi psikolojik sorunlar yaşayabilmektedir (Reed vd., 2015).

Siber zorbalık nedeniyle mağduriyet yaşayan gençler, kendilerine ve çevrelerine olan güveni yitirebilmekte, yakın ilişkiler ve ikili ilişkilerde sorunlar yaşayabilmektedir (Pyzalski, 2012). Ayrıca bireyin benlik saygısında da bir azalma görülebilmektedir. Benlik saygısı azalan gencin kendisine ve çevresine karşı daha agresif bir tutum sergileyebildiği ve daha öfkeli olabileceği dile getirilmektedir (Beran & Li, 2005). Bu durum genci yalnızlığa sürükleyebilmekte ve sosyal hayattan kendini soyutlayan gencin daha ileri safhalarda intihara kalkışmasına sebep olabilmektedir (Heiman & Olenik Shemesh, 2019; Hinduja & Patchin, 2010).

Siber zorbalığın mağdurların yaşamlarında oldukça önemli sorunlara yol açtığı gözlemlenmektedir. Siber zorbalığa maruz kalma süresi, şiddeti ve tekrarlanma sıklığı arttığında mağdurların daha yüksek düzeyde ve daha olumsuz etkilere neden olduğu da vurgulanmaktadır (Safaria, Tentama & Suyono, 2016). Dolayısıyla bireylerin kritik yaşam dönemlerinden biri olan gençlik yıllarında siber zorbalık ile karşılaşarak mağdur olmalarının çok önemli bir sorun olduğu söylenebilmektedir.

Özetle, teknolojik gelişmeler ile dijital ortamda bireylerarası etkileşimin artması, şiddet biçimlerinin de yeni platformlara kaymasına zemin hazırlamıştır. Böylece dijital dünyada ortaya çıkan siber zorbalık; kasıtlı, tekrarlayan ve zarar veren eylemlerin tamamı olarak açıklanabilmektedir. Bireylerin maruz kaldığı siber zorbalık, sadece duygusal veya psikolojik zarar vermemektedir. Aynı zamanda bireyin mahremiyetine yönelik ciddi ihlalleri de kapsamaktadır. Sosyal medya ve diğer iletişim platformlarında özel bilgilerin izinsiz paylaşılması, tehdit, dışlanma ve alay gibi davranışlar siber mağduriyeti ortaya çıkarmaktadır. Bu dijital platformlarda yoğun olarak yer alan genç bireyler de bu olumsuz davranışlardan etkilenmektedir. Bu sebeple bu çalışmada siber zorbalık olgusu, doğrudan siber mağduriyetin kaynaklarından biri olarak ele alınmakta ve dijital mahremiyet farkındalığı ile ilişkili şekilde değerlendirilmektedir.

1.4.2. Siber Mağduriyet Tanımı ve Tarihsel Kökeni

Siber mağduriyet dijital ortamda bireylerin siber saldırılara maruz kalması anlamına gelmektedir (Wright & Li, 2013). Bireyler internetin bulunduğu her ortamda bu saldırılara maruz kalarak mağduriyet yaşayabilmektedir (Gini, Card & Pozzoli, 2018). Sosyal medya platformlarının 2000'li yıllarda hayatımızda yer edinmeye başlaması ile siber mağduriyet kavramı da ortaya çıkmıştır (Wang vd., 2010).

Siber mağduriyet kavramının hayatımıza girme nedenini anlayabilmek için geleneksel mağduriyetten farkının anlaşılması oldukça önemlidir (Dağlı, 2024). Geleneksel mağduriyette

saldırıyı gerçekleştiren zorba kişi ile mağdurun aynı ortamda bulunması gerekliken siber mağduriyette böyle bir zorunluluk yoktur. Bu nedenle zorbanın mağdura ulaşabilmesi siber mağduriyette daha kolaydır. Ayrıca dijital ortamda zorbanın kimliğini gizleyebiliyor olması siber mağduriyet ve geleneksel mağduriyetin arasındaki bir diğer farktır (Salmon vd., 2018). Siber mağduriyetin bir başka farkı ise mağdurun hiç tanımadığı kişiler tarafından zorbalanabiliyor olmasıdır (Beran & Li, 2007). Zorbanın kimliğinin gizlenebilir olması ve mağduru tanımıyor olması ile geleneksel zorbalığa göre siber saldırılarda mağdurun daha fazla üzerine gidebilmekte, zorba tarafından daha büyük ve olumsuz bir güç gösterisi yapabilmektedir (DePaolis & Williford, 2015). Bu farklar geleneksel zorbalığa maruz kalmasına oranla mağdurun daha kötü hissetmesine ve daha travmatik deneyimler yaşamasına neden olabilmektedir (Jackson & Cohen, 2012). Böylece mağdur yaşadığı travmanın etkisi ile uzun süre bunu atlatamayıp daha büyük yıkımlar yaşayabilmektedir (Wigderson & Lynch, 2013).

Günümüzde dijital platformlar sayesinde insanlar arası erişim ve etkileşim çok kolay hale gelmiştir. Bu dijital platformların yeni yeni kullanılmaya başlandığı zamanlar bu durum oldukça olumlu bir gelişme olarak yorumlanmıştır (Reid & Weigle, 2014). Çünkü bireylere uzak mesafedeki tanıdıkları ile görüşebilme imkânı verilmiştir. Ancak sosyal medyanın yaygınlaşması ve bireylerin tanımadığı kişiler ile de etkileşime girmeye başlamasıyla bu durum tersine dönmüştür. Çeşitli siber saldırılar ile çok sayıda kişi mağdur edilmiştir (Naslund vd., 2020).

1.4.3. Siber Mağduriyet Türleri

Teknoloji ve internet kullanımının yaygınlaşması ile bireylerin yaşadığı siber mağduriyetler her geçen gün artmaktadır (Sontag vd., 2011). Bu nedenle önemli bir sorun haline gelen siber mağduriyet konusunda çalışmalar yapılmaktadır. Alanyazın tarandığında siber mağduriyetin türlerinin olduğuna dair bilgilere ulaşılmaktadır. Bu bilgiler ışığında siber mağduriyetin türlerinin üç başlık altında toplandığı görülmektedir (Schwartz vd., 1997).

Pasif Mağdur: Pasif mağdurlar siber zorbalık karşısında seslerini çıkarmamakta ve bu durumu kabullenmektedirler. Bu zorbalığı kabullenip pasif bir tutum sergilemelerinde mağdurların mizacı büyük bir rol oynayabilmektedir (Pellegrini, 1998). Mağduriyetin bu türünde zorbalık yapan bireyler ise mağdurların pasif kalmasından güç alarak saldırılarına devam edebilmektedirler (Bernstein & Watson, 1997).

Saldırgan Mağdur: Bu türdeki mağdurlar yaşadıkları mağduriyet nedeniyle tepki göstererek bu durumdan kurtulmak ve zorba bireye ders vermek amacıyla onunla

inatlaşabilmektedirler (Toblin vd., 2005). Böylece siber zorbalar ya saldırılarına bir son vermekte ya da tam tersi şekilde daha çok öfkelenerek mağduru daha çok köşeye sıkıştırmaya çalışabilmektedir (Fung, 2012).

Olası Mağdur: Siber mağduriyet yaşayan bazı bireyler bu durumu gizleme eğiliminde olabilmektedir. Dolayısıyla bu bireyler için tam olarak bir mağdur tanımı yapılamamaktadır. Bu nedenle mağduriyet yaşayıp yaşamadıkları tam olarak bilinmeyen bireyler bu türün içerisinde değerlendirilmektedir (Malesky, 2007). Bu kategoride yer alan bireyler genellikle zorbadan kaçınmakta ve özellikle fiziksel alanlarda zorba ile karşılaşmamaya çalışmaktadır (Greenbaum vd., 2015).

1.4.4. Siber Mağduriyet Nedenleri

Bireylerin siber mağdur olma ihtimalini arttıran çok sayıda sebep bulunmaktadır. Bu sebeplerden ilki bireylerin çeşitli ihtiyaçlarını internet ile gidermeye çalışmaları gelmektedir (Bruin, Meppelink & Bögels, 2015). Örneğin fizyolojik bir ihtiyaç olan açlığı yemek yapma veya sipariş etme uygulamaları, sevgi ve ait hissetme ihtiyaçlarını arkadaşlık uygulamaları üzerinden gidermeye çalışabilmektedir. Aynı zamanda öğrenme ihtiyacını gidermek için çeşitli öğrenme uygulamaları da oldukça yaygın şekilde kullanılmaktadır (Wong, 2020). Bunların yanında bireylerin sosyalleşme ihtiyacını karşılamak için günümüzde sosyal medya platformlarında sıklıkla vakit geçirdiği de bilinmektedir.

Sosyal medya platformları özellikle ergenlik ve yetişkinlik dönemlerinde çokça tercih edilen yerlerdir (Al-Garadi vd., 2019). Başta zararsız gibi görünen sosyal medya yanlış kullanıldığı takdirde bireylerin siber mağduriyet yaşama ihtimalinin oldukça yüksek olduğu platformlardır (Whittaker & Kowalski, 2015). Sosyal medya platformlarında konuşulan kişinin tanıdık olup olmadığına dikkat edilmeli, karşıdakinin sahte bir hesap olabileceği akıldan çıkarılmamalıdır (Barlett vd., 2018). Aksi takdirde yanlış kişiler ile bilgi alışverişinde bulunmak siber mağduriyet riskini arttıran bir diğer nedendir (Agustina, 2015). Ayrıca dijital platformlarda özel bilgilerin, konumun, fotoğraf ve videoların dikkatsizce paylaşılması mağduriyet yaşama ihtimalini arttırmaktadır (Song, Lynch & Cochran, 2015).

Özellikle çocuk ve gençlerin ailelerinin dikkatsizliği ve ebeveyn-çocuk arasındaki iletişim eksikliği de siber mağduriyete davetiye çıkarabilmektedir (Alvarez-Garcia vd., 2019). Görüldüğü üzere aile bu konuda önemli bir faktördür. Ailenin yanı sıra bireylerin psikolojik durumları da mağduriyet konusunda önem arz etmektedir. Örneğin düşük özgüvene sahip bireylerin mağduriyet yaşama ihtimali oldukça yüksektir (Burger & Bachmann, 2021). Düşük özgüveni nedeniyle sosyal ortamlarda kendini gösteremeyen bireyler sosyal medya

uygulamalarına yönelmekte ve burada içerikler yayınlatabilmektedir. Yaptığı paylaşımlar ile siber zorbaların hedefi haline gelebilmekte ve özgüveni daha çok düşülebilmektedir (Varghese & Pistole, 2017).

Bireylerin kendilerini yalnız hissetmesi ile sosyal medyaya yönelmesi de oldukça sık rastlanan bir durumdur. Bireyin amacı yeni arkadaşlıklar edinmektir (Heiman & Olenik-Shemesh, 2022)F. Ancak bu durum olumsuz sonuçlar doğurabileceği için tanıştığı kişilere verdiği kişisel bilgileri ve profilindeki paylaşımlarına dikkat etmelidir (Matthews vd., 2022).

Siber mağduriyete neden olan bir diğer psikolojik faktör ise depresyon ve kaygı bozukluğudur (Tran, vd., 2023). Bu bireyler, özellikle kaygı bozukluğuna sahip olanlar, yaşadıkları anksiyete nedeniyle sosyal ortamdan çok dijital platformlara yönelebilmektedir (Landoll vd., 2015). Dolayısıyla gerçeklikten çok sanal alemde vakit geçirmeye başlamaları ile bu bireylerin siber mağduriyet yaşama ihtimalleri de orantılı olarak artmaktadır.

Bireyin siber mağduriyet yaşamasında etkili olan faktörlerden biri de içinde bulunduğu kültürel normlardır. Toplumun kültürel yapısı, bireylere belirli rol ve sorumluluklar yüklemekte; özellikle toplumsal cinsiyet rolleri kadın ve erkeklere farklı davranış kalıpları atfetmektedir. Bu roller doğrultusunda kadınlar genellikle daha uyumlu, kırılgan ve ilişki odaklı bireyler olarak tanımlanırken; erkekler güçlü, saldırgan ve dışa dönük özelliklerle özdeşleştirilmektedir (Mishna vd., 2020). Bu durum, kadınları siber ortamlarda daha savunmasız hale getirebilmektedir. Siber zorbalık bağlamında yapılan araştırmalar, erkeklerin zorbalık davranışlarında daha aktif bir rol üstlendiğini ve kadınlara göre daha fazla siber zorba davranışta bulunduğunu ortaya koymaktadır. Öte yandan, kadınların siber mağduriyet yaşama oranı erkeklere kıyasla daha yüksektir. Ayrıca, toplumsal rollerin etkisiyle erkekler mağduriyet deneyimlerini ifade etmekte zorlanabilirken; kadınlar yaşadıkları zorbalıkları paylaşma ve destek arama konusunda daha isteklidir (Wright & Wachs, 2020).

Kültürel normların yol açtığı bir diğer siber sorun, mizah adı altında gerçekleştirilen zorbalık davranışlarıdır. Toplumda kadınlardan daha empatik ve destekleyici olmaları beklenirken, mizah çoğunlukla erkeklikle ilişkilendirilen bir özellik olarak öne çıkmaktadır. Bu durum, toplumsal cinsiyet rollerinin etkisiyle mizah anlayışının erkekliğe özgü bir alan gibi görülmesine neden olmakta ve kimi zaman bu anlayış, sınır ihlallerini meşrulaştıran bir araca dönüşebilmektedir. Zorbalık, çoğu zaman şaka veya espri kılıfına bürünerek mağdurlara yöneltilmekte ve bu tür davranışlar, mağdur açısından psikolojik baskı ve aşağılamayı içeren bir zorbalık biçimi hâlini alabilmektedir (Mishna vd., 2020). Bu tür durumlarda, şakanın hedefi olan bireyler davranışa itiraz ettiklerinde sıklıkla “aşırı hassas” ya da “mızımız” olmakla suçlanmakta; böylece hem zorbalık meşrulaştırılmakta hem de mağdurun yaşadığı deneyim

görünmez kılınmaktadır. Özellikle erkekler arasında saldırgan, sınırları zorlayan ve alaycı mizah biçimleri “erkeklik göstergesi” olarak kabul edilmekte ve bu nedenle söz konusu davranışlar yaygın biçimde sürdürülmektedir (Wright & Wachs, 2020). Oysa mağdurlar, bu tür zorbalık karşısında derin psikolojik ve duygusal etkiler yaşayabilmektedir (Herry & Mulvey, 2022). Dolayısıyla toplumsal cinsiyet rolleri yalnızca zorbalık davranışlarını değil, aynı zamanda bu davranışlara verilen tepkileri de şekillendirmekte; böylece şiddet ve zorbalık kültürel düzeyde yeniden üretilmektedir.

1.4.5. Siber Mağduriyet Sonuçları

Siber mağduriyet bireyleri fiziksel, psikolojik, sosyal, duygusal, davranışsal ve akademik yönden etkileyerek mağdurlar üzerinde olumsuz sonuçlara zemin hazırlamaktadır (Brown, Demaray & Secord, 2014). Bireylerin hayatını doğrudan ve dolaylı olarak etkileyen siber mağduriyetin bu olumsuz sonuçları psikolojik, sosyal, duygusal ve davranışsal olmak üzere dört temel başlık altında incelenebilmektedir (Dağlı, 2024).

Psikolojik Sonuçlar: Mağdur bireylerin yaşadığı psikolojik sonuçların en önemlilerinden biri depresyondur. Siber mağdurların depresyonu yaşama oranı mağduriyet yaşamamış bireylere göre daha yüksektir (Medrano, Lopez & Gamez-Guadix, 2018). Bireyin kendini psikolojik açıdan iyi hissetmemesi olarak tanımlanan depresyon uzun süre devam edebilmekte ve bireyin yaşamını olumsuz etkileyebilmektedir (Ramsey, DiLalla & McCrary, 2016). Dijital ortamda zorbalık yapılan materyalin defalarca paylaşılabiliyor olması mağduriyetin artmasına ve hatta mağdurun depresyonunun derinleşmesine neden olabilmektedir. Derinleşen bu depresyon profesyonel bir destek ile çözülmezse birey kendine zarar verme ve intihar etme gibi eylemlere yol açabilmektedir (Mitchell vd., 2011).

Diğer bir psikolojik sonuç, zorbanın anonim olması nedeniyle mağdurun çevresine güvenmemesinden kaynaklanmaktadır (Tokunaga, 2010). Bu güvensizlik sonucunda bireyin zamanla kendine güveni yok olabilmekte ve öz saygısını da yitirebilmektedir (Al Qudah vd., 2020). Aynı zamanda bu bireyde anksiyete görülme ihtimali de artmaktadır (Wright & Wachs, 2019). Birey bunlar sonucunda sürekli yalnız kalmayı isteyebilmektedir. Tüm bunlar sonucunda birey kendini sosyal hayattan soyutlayarak daha çok yalnız kalmaya çalışabilmektedir. Bu da çeşitli psikolojik rahatsızlıkları beraberinde getirebilmektedir (Zhu vd., 2021).

Sosyal Sonuçlar: Siber mağduriyet, bireylerin çevresi ile olan ilişkisine zarar vermektedir. Ergen ve gençlerin sosyal çevresi genellikle okul olmaktadır. Zorba okuldan veya okul çevresinden biri ise mağdur okul kaygısı veya okul terki yaşamaktadır (Wolke, Lee &

Guy, 2017). Okulları bu sebeple güvenli bulmayan siber mağdurlar kendini korumak için tehlikeli aletler taşımaktadır (Martinez-Martinez vd., 2020). Bu durum da daha olumsuz sonuçlar doğurabilmektedir. Dolayısıyla mağdur en önemli sosyal ortamından kopmakta ve akademik başarısı düşmektedir (Wang vd., 2014). Akademik başarısı düşen mağdurun tüm hayatının olumsuz bir yöne evrilme riski de oluşmaktadır.

Duygusal Sonuçlar: Siber mağduriyet üzüntü, öfke, hayal kırıklığı, utanç, çaresizlik ve korku duygularını tetiklemektedir (Patchin & Hinduja, 2006). Bu duyguların yoğun şekilde yaşanması bireyin mağduriyetten kurtulmasını engelleyebilmekte ve mağdurun hayatını zorlaştırabilmektedir. Mağdur bu duygular sebebiyle yaşamdan zevk alamama ve hayatta kalmak için istek duymama gibi sorunlar yaşayabilmektedir (Trompeter, Bussey & Fitzpatrick, 2018). Bu nedenle bu duyguların aşılmasında psikolojik destek çok önemlidir (Ryan & Curwen, 2013).

Davranışsal Sonuçlar: Siber mağduriyet kaynaklı uyku bozukluğu önemli bir davranışsal sonuçtur. Genellikle siber mağdurların uyku düzenleri bozulmakta (Lin vd., 2020) ve kabuslar görerek uyanmaya başlamaktadırlar (Fekih-Romdhane vd., 2023).

Diğer bir önemli davranışsal sonuç ise yeme bozukluğudur. Mağdur zorbalık sonrası tamamen yemeden kesilebilmekte veya duygusal yeme bozukluğu yaşayabilmektedir (Yusuf vd., 2021). Siber mağdurun zorbalık ile anoreksiya nervroza ya da bulimia nervroza gibi ileri yeme bozuklukları da tetiklenebilmektedir (Marco vd., 2018). Siber mağduriyet sonucunda bireyin beden algısı bozulabilmekte ve estetik ameliyatlara ve zayıflama haplarına yönelmesiyle kendine kalıcı zararlar verebilmektedir (Day vd., 2022).

Görülüyor ki zorbanın kimliğini saklayabiliyor olması, dijital dünyada zaman ve mekân sınırının olmaması gibi yönleriyle geleneksel mağduriyetten ayrılan siber mağduriyet bireyin psikolojik, fiziksel ve sosyal işlevselliğini olumsuz yönde etkilemektedir. Bireyde meydana gelen bu olumsuzlukların dolaylı olarak toplumu da etkilediği alındığında dijital mahremiyet farkındalığı konusunun ne kadar önemli olduğu bir kez daha gözler önüne serilmektedir.

Ulusal ve uluslararası literatür, dijital mahremiyet farkındalığının oldukça düşük seyrettiğini (Eroğlu, 2018; Altıntaş Var, 2022); buna karşılık mahremiyet farkındalığının çevrim içi alanlardaki riskler karşısında “kalkan” oluşturabildiğini (Öz, 2014; Boerman vd., 2018) ortaya koymaktadır. Mahremiyet bilinci sayesinde birey dijital dünyada tehditleri kolaylıkla tanıyabilmekte ve bu tehditlere karşı önlem alabilmektedir. Ayrıca dijital mahremiyet farkındalığı ile bireyler siber zorbalığa karşı daha dirençli olabilmekte ve böylece siber mağduriyet risklerini azaltabilmektedir.

Dolayısıyla bireylerin dijital mahremiyet konusunda bilinçli olmaları, siber zorbalık ve siber mağduriyet bağlamında önemli bir adımdır. Zorbalık ve mağduriyet olasılığını azaltan mahremiyet farkındalığı, bireylerin dijital ortamda daha güçlü, kontrollü ve bilinçli hissetmesine katkıda bulunmaktadır.

Dijitalleşmenin mahremiyet üzerindeki izlerinin giderek arttığı günümüzde, sosyal hizmet alanında bu konunun yalnızca geleneksel biçimleriyle değil, dijital bağlamda da değerlendirilmesi gerektiği anlaşılmaktadır. Zira dijitalleşen dünyada bireylerin çevrim içi ortamlarda görünürlüklerinin artması, mahremiyet kavramını geleneksel sınırların ötesine taşıyarak daha karmaşık ve çok katmanlı bir hâle getirmektedir. Özellikle sosyal medya, çevrim içi iletişim platformları ve dijital uygulamalar yoluyla bireylerin kişisel ve özel bilgilerini paylaşma şekilleri değişmekte ve bu durum yeni türden risklerin ve ihlallerin ortaya çıkmasına zemin hazırlamaktadır.

Mahremiyet ihlali, bireylerde kırılabilirlik, güven kaybı, yalnızlık, utanma, değersizlik ve dışlanma gibi güçlü duygusal tepkileri beraberinde getirebilmektedir. Bu sebep doğrultusunda sosyal hizmet uygulamalarında bireyin mahremiyeti oldukça önemli bir konu olarak ele alınmaktadır. Ayrıca bireyin rızası olmadan kişisel bilgilerinin paylaşılması, yaşamına müdahale edilmesi veya sınırlarının ihlal edilmesi ciddi bir etik sorun da teşkil etmektedir. Böylece, mahremiyetin korunması, bireyin hem danışmanlık ilişkisi içinde güven duymasını hem de kendi yaşamı üzerindeki denetim duygusunu korumasını sağlamaktadır.

Sosyal hizmet disiplininin temelini bireyin onuruna, öznel sınırlarına ve yaşam haklarına saygıyı merkeze alan hak temelli bir yaklaşım oluşturmaktadır (Turner, 2017). Bu yaklaşım ile mahremiyet, yalnızca etik bir kural veya yasal bir unsur olarak görülememektedir. Sosyal hizmet perspektifinde mahremiyet, bireyin varoluşunu, öznelliğini ve toplum içindeki konumunu şekillendiren temel bir olgudur. Ayrıca bireylerle yürütülen danışmanlık, destek ve müdahale süreçlerinde, kişinin fiziksel, psikolojik ve dijital alanına saygı göstermek sosyal hizmet uzmanı için mesleki bir yükümlülüktür.

Sosyal hizmet açısından sadece bireyin mahremiyetinin korunması yeterli değildir. Sosyal hizmet disiplinine göre, bireyin kendi mahrem sınırlarını tanıyabilmesi, bu sınırları başkalarına karşı ifade edebilmesi ve ihlal durumunda destek talep edebilmesi de oldukça önemlidir. Bireyin bu şekilde bir güç kazanacağı düşünülmektedir. Bireyin, kendi özel alanına ilişkin kararları alabilmesi, bu kararları savunabilmesi ve gerektiğinde müdahaleye sınır çizebilmesi, onu yalnızca mağdur olmaktan çıkarıp aktör hâline getirmektedir. Bu da sosyal hizmetin güçlendirici rolü açısından elzemdir. Bu noktada mahremiyetin, bireysel özerkliğin ve hak temelli sosyal hizmet yaklaşımının temel taşlarından biri olduğu söylenebilmektedir.

İKİNCİ BÖLÜM

KURAMSAL ÇERÇEVE: GÜÇLENDİRME KURAMI BAĞLAMINDA DİJİTAL MAHREMİYET VE MAĞDURİYET

Genç bireylerin günümüzde siber mağduriyete açık bir hedef haline gelmesi ile, bu araştırmanın zemini olan güçlendirme kuramının önemi artmaktadır. Güçlendirme, bireyin hayatındaki zorluklara karşı direnç geliştirmesi ve haklarını koruyabilmesi süreci olarak tanımlandığında, siber mağduriyet karşısında bireyin korunabilirliğini artıran en önemli unsurlardan birinin de dijital mahremiyet farkındalığı olduğu görülmektedir.

Güçlendirme sürecinde dijital mahremiyet farkındalığının öneminin anlaşılması ile bu bölümde öncelikle güçlendirme kuramının tanımı ve temel kavramları anlatılarak gençlerde dijital mahremiyet farkındalığı ve bireysel güçlenmenin önemi vurgulanmıştır. Daha sonrasında güçlenmenin zorbalık ve mağduriyet ile mücadeledeki rolü açıklanıp güçlendirme kuramının bu çalışmadaki yeri ortaya konmuştur.

2.1. Güçlendirme Kuramı: Tanım ve Temel Kavramları

Güçlendirme Kuramı, “bireylere, ailelere, gruplara ve topluluklara bireysel, bireyler arası, sosyo-ekonomik ve politik güçlerini arttırma ve durumlarını iyileştirmeleri yönünde bir etki geliştirme süreci” olarak tanımlanmaktadır (Barker, 2014).

Bu yaklaşım, toplumda var olan kaynaklar üzerinde farklı güç ve kontrol seviyelerine sahip grupların olduğunu varsayan bir çatışma modeline dayanmaktadır (Fay, 1987). Bu nedenle öncelikle güç kavramının açıklanması önem kazanmaktadır. Greene ve Lee (2002)’ye göre güç, bireyin yoğun stresle karşılaşsa dahi işlevselliğini sürdürebilmesi, belirgin bir travma ile karşı karşıya kaldığında kendini toparlayabilmesi, zorlukları gelişim için kullanabilmesi ve sosyal destekleri bir dirençlilik kaynağı olarak değerlendirebilmesidir. Kısacası güç, bireyin tecrübe ettikleri ile başa çıkabilme kapasitesi olarak ifade edilebilmektedir.

Güç, gelişimi ve çözümleri güdüleme potansiyeline sahiptir (Saleebey, 2013) ve hem bireyin kendisinde hem de yaşadığı toplulukta bulunabilmektedir (Rapp & Goscha, 2004). Örneğin bireylerin bilgi birikimleri, yetenekleri, ümitleri, kararlılığı, merakı, tutkuları, geçmiş yaşamındaki başarıları, sorun çözmeye dair geçmiş girişimleri, kişiler arası ilişkileri, yaşamını sürdürdüğü toplum, sosyo-politik destekleri ve daha birçoğu birer güç olarak görülebilmektedir. Ayrıca bireyin yaşadığı yaralayıcı ve zorlayıcı olan travma, istismar ve hastalık gibi olayların

da bir güç, bir fırsat kaynağı teşkil edebileceği de güçlendirme yaklaşımının temel varsayımlarındandır (Teater, 2015).

Bu kuramın yapı taşlarından olan diğer kavramlar ise benlik saygısı, özyeterlik, öğrenilmiş çaresizlik, kontrol odağıdır. Benlik saygısı, bireyin kendine duyduğu saygıdır (Doğan & Eryılmaz, 2013). Bireyin kendi hakkında geliştirdiği olumlu düşüncelerin tümü olarak da açıklanabilmektedir. Bir diğer önemli kavram olan özyeterlik, bireyin yaşadığı durumlarla başa çıkabilme yetisine yönelik inancı olarak tanımlanabilmektedir (Bandura, 1997). Öğrenilmiş çaresizlik ise, bireylerin zamanla gerçekleştirdikleri eylemler ve sonuçları arasında bir bağlantı olmadığını görerek durumlar karşısında hiçbir kontrolünün olmadığına inanmasıdır (Seligman, 1975).

Tanımlanacak olan son kavram kontrol odağı terimidir. Kontrol odağı, bireylerin yaşam koşullarına dair kontrol mekanizmalarına yönelik tutumlarıdır ve bu tutumlar ikiye ayrılmaktadır (Greene, Lee & Hoffpauir, 2005): İçsel ve Dışsal Kontrol Odağı. İçsel kontrol odağına göre bireyler kendi yaşamlarını kendilerinin kontrol ettiklerine inanırken dışsal kontrol odağına göre, bireyler hayatlarının kader, şans veya iktidar sahipleri tarafından kontrol altında tutulduğunu düşünmektedir.

Güçlendirme yaklaşımının temelleri sosyal, ekonomik ve kültürel yönden dezavantajlı bireylerle çalışan eğitimciler ve topluluk psikologları tarafından atılmıştır. Çoğunlukla Paulo Freire'nin (1972) eğitim felsefesine dayanan Güçlendirme Yaklaşımı, dezavantajlı veya baskı altındaki bireylerin güçlenmeleri için sosyal eşitsizlik konusunda bilinçlenmeleri ve sosyal eşitsizliğin sağlanacağı konusunda güvenlerinin artması gerektiği düşüncesinden beslenmektedir.

İlk zamanlarda Güçlendirme Kuramı'ndan doğrudan bahsedilmese de Jane Addams ve Hull House sosyal adalet ve hak temelli gerçekleştirdikleri çalışmalar ile Güçlendirmenin ilk uygulamalarını hayata geçirmeye başlamışlardır (Cankurtaran, Akoğlu & Sakarya, 2020). Güçlendirme Yaklaşımı'nın Sosyal Hizmet'te popüler hale gelmesi ise Solomon'un 1976'da Black Empowerment kitabı ile olmuştur (Gutierrez, 1990). Bu kitabın yayınlanması ile Güçlendirme Sosyal Hizmet alanında yaygın şekilde kullanılmaya başlanmıştır.

Sosyal Hizmet bakış açısıyla, Güçlendirme Yaklaşımı ile bireyde istenen değişimin gerçekleşmesi için yapılacak müdahalede müracaatçının güçleri üzerinde durulması gerektiği savunulmaktadır ve dolayısıyla bu kuram ilk olarak klinik Sosyal Hizmet uygulamalarında kullanılmıştır (Duyan, Özgür Sayar & Özbulut, 2008).

Sosyal Hizmet mesleğinde mikro, mezzo ve makro müdahale alanlarında uygulanabilen Güçlendirme; bireylere, ailelere ve topluluklara, içlerinde ve çevrelerinde sahip oldukları

kaynakları ve araçları keşfetmeleri ve bu kaynakları kullanmaları için destek olmaktadır (Thompson, 2007). Güçlendirme müdahaleleri ile müracaatçıların kendi hayatlarını kontrol etmeleri, baskıcı uygulamalara karşı güçlü olmaları, eleştirel düşünceye sahip olmaları, kendilerine güvenlerinin artması ile kendi haklarının savunucuları olmaları amaçlanmaktadır. Kısacası amaç, güçlendirme ile kendi kendine yetebilen bireylerin sayısının arttırmasına katkıda bulunmaktır (Erbay, 2019). Bireyin güçlenmesi ile dolaylı olarak toplumlar ve toplum da güçlenme imkânı bulabilecektir.

Görüldüğü üzere güçlendirmenin odağı uyum sağlamak değil, bireylerin, grupların ve toplumların güçlenmesini sağlayarak sorunlar karşında iyileştirme kapasitesini arttırmaktır (Gutierrez, 1990).

Sosyal hizmet uzmanları genelci bir bakış açısıyla çerçevelenen güçlendirme yaklaşımı ile birçok müracaatçı ile farklı ortamlardaki sorunlara müdahale edebilmektedir. Ancak uygulama esnasında belirlenecek yol, ortam ve koşullar, müracaatçının kişiliği ve şartlar farklı olabilmektedir. Dolayısıyla yapılan müdahale de bireye özeldir.

Güçlendirme yaklaşımına göre her müracaatçı yaşam kalitesini iyileştirmek için gelişime açık, kaynaklarını arttırabilecek potansiyeli olan, yeterliliğe sahip, güçlü yönleri ve kapasiteleri bulunan bireylerdir (Whitmore, 1988) ve her birey kendi yaşamının uzmanıdır (Cankurtaran, Akoğlu & Sakarya, 2020). Dolayısıyla güçlendirme müracaatçı ve sosyal hizmet uzmanı ile iş birliği içerisinde yürütülen bir müdahale yöntemidir (Thompson, 2007). Sosyal hizmet uzmanları müracaatçıların tanımladığı güçlü yönleri, değişime ve motivasyonlarına odaklanmaktadır (Lee, 2001). Güçlendirme hayat boyu devam eden bir süreçtir (Whitmore, 1988). Bu nedenle sosyal hizmet uzmanlarının müracaatçının katılımını sağlamaya çalışması da oldukça önemlidir (Tuncay, 2009).

Özetle sosyal hizmet perspektifine göre güçlendirme yaklaşımı ile; müracaatçının bakış açısına öncelik verilerek müracaatçı ile işbirliği yapılmalı, müracaatçının aktif katılımı sağlanmalı, müracaatçının istekleri, amaçları ve hedefleri keşfedilmeli, müracaatçının güçlü yönleri ve güç ilişkileri konusunda farkındalık geliştirmesi sağlanmalı, müracaatçı özyeterliliği konusunda bilinçlendirilmeli, müracaatçının kendi kaderini tayin etme ve söz söyleme hakkı verilmeli, müracaatçının özerk bir birey olduğu kabul edilerek bağımsızlığı teşvik edilmelidir.

2.2. Gençlerde Dijital Farkındalık ve Bireysel Güçlenme

Güçlendirme, bireylerin yaşamları hakkında söz hakkı kazandığı, hayatının kontrolünü eline aldığı bir süreçtir. Kişisel güçlendirme, bireyin yeterlilik duygusunu ve becerilerini pekiştirmektedir. Değişime etki etme gücünün ve yeterliliğinin farkına varmasını sağlamaktadır

(Anuradha, 2004). Bireysel güçlendirme sürecinde müracaatçı ve sosyal hizmet uzmanının ilişkisi ve iletişimi oldukça önemlidir. Bu süreçte müracaatçının bakış açısıyla var olan durumu görebilmek, müracaatçının bu durumu nasıl yorumladığının farkına varabilmek de mühimdir (Askheim, 2003).

Bireyin kendi güçsüz yanlarını ve bu yanlarının yaşamlarındaki etkileri anlamaları bireysel güçlenme açısından önemlidir. Çünkü birey güçsüz yönlerine göre kendi değer ve inançlarını inceleyerek potansiyel güçler ortaya çıkarabilmektedir. Bireysel güçlü yanları keşfetmek, benzer duygular ve sorunlar yaşayan diğer bireyleri de anlayabilmenin önemli bir parçasıdır.

Bireysel güçler; bireylerin kişisel özellikleri, sorun çözme ve karar alma becerileri, fiziksel kaynakları gibi çeşitli şekilde sıralanabilmektedir. Bu sıralamada yer alabilecek bir diğer bireysel güç ise dijital mahremiyet farkındalığıdır.

Dijital mahremiyet farkındalığı, kısacası bireyin dijital ortamda karşısına çıkabilecek veri güvenliği tehditlerini tanıyabilme ve bu tehditlere bilinçli olarak tepki verebilme kapasitesi olarak tanımlanabilmektedir (Park, 2013). Birey dijital mahremiyetinin farkına vardığında, kişisel verilerinin nasıl toplandığı, kullanıldığı ve paylaşıldığı konusunda daha bilinçli kararlar verebilmektedir. Bu durum da bireyin çevrim içi ortamda edilgen bir kullanıcıdan ziyade aktif özne haline gelmesini sağlamaktadır (Westin, 1967). Aktif özne haline gelen birey dijital ortamdaki sınırlarını oldukça iyi belirleyebilmek ve bu sınırları kolaylıkla koruyabilmektedir.

Güçlenme kavramı ile bireyin kendi yaşamı üzerindeki kontrolü kurabilmesi yakından ilişkilidir. Dolayısıyla dijital ortamda bireyin dijital farkındalığa sahip olup kendi sınırlarını çizebilmesi bireysel güçlenme açısından da oldukça önemlidir.

Dijital mahremiyet farkındalığı, bireyin sadece dijital güvenliği için önemli değildir. Aynı zamanda dijital mahremiyet farkındalığı bireyin iyi olma halini de destekler (Özen, 2017). Bu yönüyle dijital mahremiyet farkındalığına sahip bireylerin psikolojik iyi olma hali konusunda da güçlenmiş olduğu bilinmektedir. Bununla birlikte dijital mahremiyet farkındalığı bireyde eleştirel düşünme becerisinin de gelişmesinde önemli bir rol oynamaktadır. Birey, farkındalığı sayesinde dijital okuryazarlığını arttırabilir (Talan & Aktürk 2021), kullandığı uygulamaların veri politikalarını okuyup analiz ettikçe dijital hakları konusunda kendisini geliştirebilmektedir (Karakuş Yılmaz, 2020). Bu sayede çevrim içi dünyada kendisini çeşitli tehditlere karşı koruyabilmekte ve dijital ortamdaki bireysel güçlenmesine katkı sağlayabilmektedir.

Görüldüğü üzere, dijital mahremiyet farkındalığı bireyi çok yönlü şekilde güçlendiren bir araç olabilmektedir. Kendi verilerinin üzerinde söz sahibi olan birey, hem dijital ortamda

daha güvenli şekilde hareket edebilme becerisi kazanabilir hem de gerektiğinde haklarını kolaylıkla savunabilme yeterliliğine kavuşabilir.

2.3. Güçlenmenin Zorbalık ve Mağduriyetle Mücadelede Rolü

Kızdırma-kışkırtma, taciz, karalama- iftira, taklit etme, ifşa etme, dışlama, rahatsız edici mesaj ve aramalar yapma şeklinde görülebilen siber zorbalık ve bunun sonucunda yaşanan siber mağduriyet ile mücadelede güçlenme yaklaşımı oldukça önemlidir. Bunlarla mücadelede güçlenmenin rolünü anlayabilmek için öncelikle siber zorbalık ve siber mağduriyetin yaygınlığına göz atılmalıdır.

Siber zorbalığın ve siber mağduriyetin gençler arasında yaygınlığını belirlemek amacıyla çok sayıda çalışma yürütülmektedir. Bu çalışmalardan biri olan ve Lai ile meslektaşları (2017) tarafından yapılan araştırmada Malezya'daki üniversite öğrencileri arasında siber zorbalığın yaygınlığı incelenmektedir. Bu çalışmaya katılan 712 devlet/özel üniversite öğrencisinin 470'inin (%66) daha önce siber zorbalığa maruz kaldığı tespit edilmiştir. Cinsiyet yönünden ele alındığında ise kadın katılımcıların 264'ü (%56,2), erkek katılımcıların 206'sı (%43,8) siber zorbalık yaşadığını belirtmektedir. Buna göre erkeklere oranla kadınların siber zorbalığı daha çok yaşadığı belirlenmiştir.

Bir diğer araştırma West'in (2015) üniversite öğrencileri üzerinde gerçekleştirdiği çalışmadır. Bu araştırmada 93 (%1,9) katılımcı siber zorbalık davranışında bulunduğunu ifade etmektedir. Ayrıca bu çalışmada bu katılımcıların %44,4'ünün bir defa, %25'nin 2-3 kez, %5,6'sının 4-6 defa, %1,4'ünün 7-10 kez ve %23,6'sının 10'dan fazla zorbalık davranışını tekrarladığı belirtilmektedir.

Türkiye'deki literatüre bakıldığında Dilmaç (2009) tarafından Selçuk Üniversitesi öğrencileri ile yürütülen bir araştırma olduğu görülmektedir. Mevcut araştırmaya göre öğrencilerin %22,5'i en az bir defa çevrim içi ortamda zorba davranışlarda bulunurken %55,3'ü en az bir kez siber zorbalık mağduru olduğunu belirtmektedir. Aynı zamanda bu çalışmada erkek katılımcıların kadın katılımcılara oranla daha fazla siber zorbalık davranışında bulunduğu tespit edilmektedir.

Son olarak Bayram ve Sayılı'nın (2013) yaptığı araştırma irdelendiğinde, 612 üniversite öğrencisi gencin bu çalışmaya katıldığı belirtilmektedir. Bu öğrencilerin son 6 ay içerisinde %27,8'ine çirkin adlarla hitap edildiği, %22,4'ünün kasıtlı olarak aktivitelerden dışlandığı, %30,6'sının siber ortamlarda zorbalık gördüğü tespit edilmektedir. Aynı çalışmada son 6 ay içinde katılımcıların %23,5'inin en az bir kez birine çirkin adlarla hitap ettiği, %19'unun kasıtlı olarak birini dışladığı ve %22,9'unun siber ortamda birini zorbaladığı görülmektedir.

İncelenen birkaç araştırma sonucunda görüldüğü üzere, siber zorbalık ve siber mağduriyet dünya genelinde ve ülkemizde gençler arasında yaygın bir sorundur. Bu sorunun da gençlerin refahını olumsuz açıdan etkilediğine dikkat çekilmektedir.

Siber zorbalığın ve siber mağduriyetin gençler üzerinde duygusal, ruhsal, sosyal ve akademik pek çok etkisi bulunmaktadır. Bu etkilerin başlıcaları; depresyon ve kaygı bozuklukları, benlik saygısında düşüş, özgüvende azalma, yeme bozuklukları, kronik hastalıklarda görülen semptomların yaşanması, nörolojik bozukluklar, uyku sorunları, bağımlılık yapıcı madde kullanımı, sosyal izolasyon, evden kaçma, devamsızlık, akademik başarıda düşüş, iş hayatında gerileme, intihardır (Mason, 2008; Burnukara & Uçanok, 2012; Kowalski, 2014).

Siber zorbalık nedeniyle mağdur olan bireyler en temelde mutsuzluk ve çaresizlik duyguları ile baş etmektedirler (Eroğlu & Peker, 2011). Aynı şekilde bu bireylerde öfke ve üzüntü duygularını da yoğun olarak yaşadıkları görülmektedir. Bu duyguları fazlaca yaşarken aşağılanma ve nefret duygularını ise daha az yaşadıkları tespit edilmiştir (Şahin vd., 2010). Bunların yanında siber zorbalık davranışının eğlence amacıyla gerçekleştirildiğini düşünerek mutlu olan bireylerin var olduğu da görülmektedir (Türkileri, 2012).

Genellikle maddi ve manevi çöküş yaşayan mağdur gençler savunmasız, dışlanmış, hayal kırıklığına uğramış hissedebilmektedirler. Özellikle yalnızlık ile baş başa kalabilmekte, aile ve arkadaşları ile problemler yaşayabilmekte, sosyal ilişki ve iletişim kurmakta zorlanabilmektedirler. Bu nedenle öfke nöbetleri de geçirebilmektedirler (Serin, 2012). Bunun yanında mağdur bireyler başlarına gelen olayları saklama eğilimde de olabilmektedir. Böylece şaşkınlık ve korkunun etkisi altında işlevi olmayan yollara da başvurabilmektedirler (Abaido, 2020). Tüm bu etkilerin sonucunda birey siber zorba veya istismarcı da olabilmektedir. Aslında bu da yaşadığı mağduriyet ile bir baş etme yöntemi olarak görülmektedir (Karaca, Mutlu & Gencer, 2021).

Anlaşıldığı üzere siber zorbalık ve siber mağduriyet gençler arasında oldukça yaygındır ve bu mağduriyetin gençlerde çeşitli etkileri olduğu da fark edilmektedir. Siber zorbalık nedeniyle yaşanan çok sayıda etkiyi de içinde barındıran bu siber mağduriyet sürecinde dijital mahremiyet farkındalığının önemi de bir kez daha gözlemlenebilmektedir. Özellikle gençlerle gerçekleştirilen çalışmalar, mahremiyet bilincinin artmasının siber zorbalık ve mağduriyet oranlarını da azalttığını göstermektedir (Livingstone & Haddon, 2009).

Mahremiyet farkındalığı önceki bölümlerde değinildiği üzere, bireylerin kişisel bilgilerinin dijital ortamda nasıl toplandığının, korunduğunun ve dağıtıldığının bilincinde olma düzeyleri olarak ifade edilebilmektedir (Tanışık & Bal, 2024). Zorbalık ise hedef seçilen kişiye

yönelik korkutma, kızdırma veya utandırma amacıyla tekrarlı davranışlarda bulunmak olarak tanımlanabilmektedir (UNİCEF, 2025). Hedef seçilen kişinin veya grubun çevrim içi ortamda rahatsız edilmesi ve bunun sonucunda maddi ve manevi zarara uğraması ise mağduriyet olarak açıklanabilmektedir (Karaca, Mutlu & Gencer, 2021).

Dijital mahremiyet farkındalığı, bireylerin bilgi sahibi olmalarıyla sınırlı değildir. Ayrıca çevrim içi ortamlarda kendilerini koruma, sınırlarını belirleme ve bu sınırları sürdürebilme yetkinliklerini de içeren bir bilinç durumu olarak ifade edilmektedir. Bu bakımdan farkındalık, bireylerin çevrim içi dünyada karşılaşılabileceği potansiyel riskleri öngörebilmesi, bu risklere karşı savunma mekanizmaları geliştirebilmesi ve böylece bireysel mahremiyet alanını koruyabilmesi açısından kritik bir işleve sahiptir.

Bireyin dijital ortamda neyi, ne zaman ve kimlerle paylaşacağını seçme iradesi yalnızca teknik bir beceri değildir. Aynı zamanda öz denetim, sorumluluk ve özsaygı ile yakından ilişkili psikososyal bir yetkinliktir. Dolayısıyla, dijital mahremiyet farkındalığı yüksek bireyler, hak ihlallerini tanıma ve bu ihlallere karşı edilgen değil, etken bir rol oynayabilmektedir. Yani, sessiz kalmayarak karşı karşıya kaldığı ihlaller konusunda etkin, kararlı ve güçlü bir tutum sergileyebilmektedir.

Mahremiyet farkındalığı olan genç, tehditleri görebildiği için riskler karşısında daha dirençli ve korunaklıdır. Siber riskler karşısında kendini koruma becerisine sahip olduğu için dijital ortamda güç kazanmaktadır. Dijital mahremiyet farkındalığı yüksek olan birey, çevrim içi tehditlere karşı strateji geliştirerek tepki verebilmekte ve kendi dijital güvenliğini sağlayabilmektedir. Bu yönüyle gençler siber ortamda edilgen değil, etken bir özne konumuna geçmektedir.

Siber mağduriyet olgusu, bireyin güçlenme düzeyiyle yakından ilişkilidir. Bireylerin siber zorbalık ve siber mağduriyet yaşamaları düşük farkındalık seviyeleri ile ilgili olabilmektedir. Dolayısıyla siber zorbalık ve siber mağduriyet yaşayan gençlerin benlik saygılarını geri kazanmaları, sosyal destek sistemlerinde çektikleri yoksunluğa son verilmesi gibi daha birçok etkinin ortadan kaldırılması güçlendirme yaklaşımı ile gençlerin bireysel kapasiteleri desteklenerek mümkün olabilmektedir. Bu çalışma bağlamında da güçlendirme ile dijital mahremiyet farkındalığı kazandırılan gencin psikososyal iyilik halinin olumlu yönde değişiminin sağlanabileceği düşünülmektedir.

Bu perspektif ile farkındalığın, bireysel güçlenmenin ana unsurlarından biri olduğu görülmektedir. Güçlenme, bireyin kendi hayatı üzerinde denetimini artıran, haklarını savunabilmeyi mümkün kılan ve kişisel kararlarını daha bilinçli şekilde almasına imkân veren

dinamik bir süreçtir. Görülmektedir ki siber zorbalık ve siber mağduriyet gibi tehditlere karşı farkındalık temel bir dayanak oluşturmaktadır.

2.4. Güçlendirme Kuramının Bu Araştırmaya Uyarlanması

Bu çalışmada gençlerin dijital ortamda siber zorbalık ve siber mağduriyet yaşamamaları amacıyla çevrim içi dünyadaki hak ve sınırlarını tanımaları, bu haklar ve mahremiyetleri üzerinde kontrol sahibi olmaları ve olası tehditlere karşı farkındalıklı geliştirebilmeleri için bir araştırma yürütülmektedir. Bu çalışma kapsamında dijital mahremiyet farkındalığının bireysel güçlenmenin önemli bir dalı olduğu düşünülmektedir. Bu kapsamda üniversitede öğrencilerinin dijital mahremiyet farkındalık düzeyleri ile siber mağduriyet deneyimleri arasında anlamlı bir ilişki olup olmadığı bu araştırma ile incelenerek çevrim içi ortamda bireysel güçlenme açısından güçlendirme kuramının önemi vurgulanmaktadır.

Gerçekleştirilen bu çalışmanın problem soruları, güçlendirme yaklaşımı ile doğrudan ilişkilidir. Örneğin, araştırmanın temel sorusu olan “Üniversite öğrencilerinin dijital mahremiyet farkındalığı ve siber mağduriyet arasında anlamlı bir ilişki var mıdır?” ın cevabı güçlendirme yaklaşımı ile verilebilmektedir. Bu kurama göre, gençlerin mahremiyet farkındalığı konusunda güçlendikçe, siber mağduriyet yaşama olasılıkları azalabilmektedir.

Güçlendirme yaklaşımı, bireysel güç kaynaklarının (bilgi, farkındalık, öz yeterlik vb.) bireyin davranışlarını nasıl etkilediği ile ilgilendiği için “Dijital mahremiyet farkındalığı siber mağduriyeti yordamakta mıdır?” sorusuna da cevap verebilmektedir. Buna göre farkındalık, siber mağduriyet düzeyini öngörebilmektedir.

Bu araştırmanın problem sorularından diğer ikisi de şunlardır: “Üniversite öğrencilerinin dijital mahremiyet farkındalık düzeyleri cinsiyete göre farklılaşmakta mıdır?” ve “Üniversite öğrencilerinin dijital mahremiyet farkındalık düzeyleri yaşa göre farklılaşmakta mıdır?”. Güçlendirmen kuramı, güçlenmenin bireysel, kişilerarası ve toplumsal düzeylerde gerçekleştiğini varsaymaktadır. Bu nedenle cinsiyet ve yaş, bireyin hayatını sürdürdüğü toplumda güç ilişkilerini etkileyen faktörlerdendir. Dolayısıyla bireylerin cinsiyeti ve yaşı yaşam deneyimlerini, dijital tehlikelerle baş etme kapasitelerini etkileyebilmektedir. Kadın ve erkeğin yaşama bakış açıları farklı olduğundan güçlenme süreçleri de farklı olabilmektedir. Ayrıca güçlendirme süreci yaş ile gelişim gösterebileceği için yaşın artması ile dijital alanda güçlenmenin de artacağı düşünülmektedir.

Güçlendirme kuramı, “Üniversite öğrencilerinin dijital mahremiyet farkındalık düzeyleri öğrenim görülen bölüme göre farklılaşmakta mıdır?” ve “Üniversite öğrencilerinin dijital mahremiyet farkındalık düzeyleri sınıf düzeyine göre farklılaşmakta mıdır?” soruları ile

de kesişmektedir. Eğitim alanı, bireyin teknoloji ile kurduğu ilişkiyi şekillendirebilmektedir. Örneğin bilişim, iletişim gibi bölümlerde okuyan gençler çevrim içi mahremiyet ve veri güvenliği konularına daha hâkim olabilmektedir. Dolayısıyla akademik bağlam bireyin dijital farkındalık düzeyini etkileyerek güçlenmesine katkı sağlayabilmektedir. Bireyin sınıf düzeyinin artması ile bilgi birikimi de artmaktadır. Gençlerdeki bu kademeli olarak bilgi artışı bireysel güçlenmeyi de destekleyebilmektedir.

Araştırmanın son sorusu olan “Üniversite öğrencilerinin dijital mahremiyet farkındalık düzeyleri interneti günlük kullanma sıklığına göre farklılaşmakta mıdır?” da güçlendirme yaklaşımı ile açıklanabilmektedir. Güçlendirmeye göre, birey çevresi ile etkileşim içerisinde ve internet de etkileşimde bulunduğu kaynaklardan biridir. İnternete daha çok vakit geçiren bireyin dijital tehditlere daha fazla maruz kaldığı ve bunun sayesinde dijital riskler hakkında daha fazla bilgiyi öğrenme fırsatı elde ettiği düşünülmektedir. Bu da kullanım sıklığı arttıkça farkındalığın yani güçlenmenin artabileceğini göstermektedir.

Sonuç olarak tüm bu soruların merkezinde yer alan dijital mahremiyet farkındalığı olgusu, bireyin dijital ortamda güçlü ve özne olarak var olabilmesinin anahtarı olabilmektedir. Ayrıca güçlendirme kuramı ile bireyin çevrim içi ortamda kendini koruma potansiyelini geliştirmesini, özerkliğini desteklemesini ve siber risklere karşı daha dirençli hale gelmesini sağlayan psikososyal bir temel sunulmaktadır. Bu doğrultuda bu çalışma, güçlendirme kuramının sunduğu çerçeveden faydalanarak, gençlerin dijital mahremiyet farkındalığı konusunda güçlenme süreçlerini açıklama, anlama ve karşılaştırma açısından önemli bir zemin sağlamaktadır.

ÜÇÜNCÜ BÖLÜM

ARAŞTIRMANIN TASARIMI VE VERİLERİN ÇÖZÜMLENMESİ

3.1. Araştırmanın Konusu, Önemi ve Amacı

Üniversite dönemi, bireylerin kimlik gelişimlerinin yanı sıra sosyal ve mesleki rollerini şekillendirdikleri kritik bir evredir. Erikson'un (1976) psikososyal gelişim kuramına göre bu dönem, "yakınlığa karşı yalıtılmışlık" evresi olarak tanımlanmakta ve bireylerden mesleki eğitim alma, işe yerleşme, eş seçimi, evlilik ve yakın ilişkileri sürdürme gibi önemli gelişimsel görevleri yerine getirmeleri beklenmektedir. Benzer şekilde, Orlofsky ve mestaktaşlarına (1973) göre de bu süreçte bireyler hem mesleki hem de kişisel sorumluluklar üstlenerek yetişkinlik rollerini benimsemeye başlar. Günümüzde bu beklentiler geçerliliğini korumakla birlikte, bireylerin bu süreçleri deneyimleme biçimleri dijitalleşme ile önemli ölçüde dönüşmüştür. Özellikle üniversite öğrencileri, bu beklentileri karşılamak ve sosyal rollerini inşa etmek amacıyla çevrim içi platformları aktif olarak kullanmakta; böylece dijital ortamlar, gelişimsel sürecin ayrılmaz bir parçası hâline gelmektedir (Neelakandan vd., 2020).

Dijitalleşmenin gençlerin yaşam tarzlarına ve gelişimsel görevlerini yerine getirme biçimlerine etkisi yalnızca sosyal etkileşimlerle sınırlı kalmamakta, aynı zamanda bireylerin çevrim içi ortamlardaki mahremiyet ihtiyaçlarını da gündeme getirmektedir. Bireylerin yaşam tarzlarının ve çeşitli beklentilerini gerçekleştirme yollarının dijital ortamlara kayması, dijital mahremiyet konusunu günümüzde giderek daha önemli hâle getirmiştir. Literatür taramaları, dijital mahremiyet konusunda yapılan çalışmaların arttığını göstermektedir. Türkiye'de yürütülen çalışmaların büyük çoğunluğunda üniversite öğrencileri örneklem grubunu oluşturmakta ve bu araştırmalarda dijital mahremiyet; sosyal medya bağımlılığı (Ahmedi, 2023), ekran bağımlılığı (Avcı & Kayıran, 2023) ve dijital okuryazarlık becerileri (Okumuş & Atılğan, 2021) gibi değişkenlerle birlikte ele alınmaktadır (Baritçi, 2023; Karadaş & Kara, 2021; Sine Nazlı & Akcaoğlu Erdem, 2023). Öte yandan, yurt dışında gerçekleştirilen çalışmalarda ise genellikle ileri yaş gruplarına odaklanılmakta ve dijital mahremiyetin eğitim (Robertson & Muirhead, 2022), ekonomi (Goldfarb & Que, 2023), sağlık (Mahadik vd., 2024) ve ruhsal sağlık (Lustgarten vd., 2020) gibi çeşitli bağlamlarla ilişkisi incelenmektedir (Aly vd., 2024; Kropczynski vd., 2021; Zhang vd., 2024). Bu bağlamda hem yerel hem de küresel düzeyde farklı değişkenlerle ilişkilendirilen dijital mahremiyet kavramını üniversite öğrencileri özelinde siber mağduriyetle birlikte ele alan bu çalışmanın, literatüre bütüncül bir bakış açısı kazandıracağı düşünülmektedir.

Üniversite öğrencilerinin dijital ortamlarda geçirdikleri zamanın artması, bu ortamlarla ilgili riskleri de beraberinde getirmektedir. Bu risklerden biri de dijital mahremiyetin ihlal edilmesiyle ortaya çıkan siber mağduriyetlerdir. Literatür incelendiğinde, dijital mahremiyet farkındalığına yönelik çok sayıda çalışmanın yapıldığı görülmektedir. Türkiye’de yürütülen araştırmalarda, genellikle üniversite öğrencileri örneklem alınmakta ve dijital mahremiyet; sosyal medya bağımlılığı (Ahmedi, 2023), ekran bağımlılığı (Avcı & Kayıran, 2023) ve dijital okuryazarlık becerileri (Okumuş & Atılğan, 2021) gibi değişkenlerle ilişkilendirilerek incelenmektedir (Karadaş & Kara, 2021; Baritçi, 2023; Sine Nazlı & Akcaoğlu Erdem, 2023). Öte yandan, yurt dışı literatürde ise çoğunlukla yaşlı bireyler üzerinde durulmakta (Kropczynski vd., 2021; Zhang vd., 2024; Aly vd., 2024) ve bu bireylerin dijital mahremiyet farkındalıkları; eğitim (Robertson & Muirhead, 2022), ekonomi (Goldfarb & Que, 2023), sağlık (Mahadik vd., 2024) ve ruhsal sağlık (Lustgarten vd., 2020) gibi alanlarla ilişkilendirilerek ele alınmaktadır. Tüm bu çalışmalar değerlendirildiğinde, dijital mahremiyetin farklı yaş ve toplumsal gruplar için farklı boyutlarıyla ele alındığı, ancak bu farkındalığın siber mağduriyetle doğrudan ilişkisini inceleyen çalışmaların sınırlı olduğu anlaşılmaktadır. Bu bağlamda, dijital mahremiyet farkındalığını üniversite öğrencileri özelinde siber mağduriyet değişkeni ile birlikte ele alan bu çalışmanın, alanyazına önemli bir katkı sunması beklenmektedir.

Dijital mahremiyet farkındalığı, bireylerin çevrim içi ortamlarda kişisel bilgilerini kimlik hırsızlığı, dolandırıcılık, siber saldırılar ve benzeri kötü niyetli girişimlere karşı bilinçli bir şekilde koruma çabasıdır (Gültekin, 2024). Bu farkındalığın eksikliği, bireyleri maddi ya da manevi zarara uğratabilecek siber mağduriyet durumlarına açık hâle getirmektedir (Arıcak, Tanrıkuş & Kınay, 2012). Siber mağduriyete maruz kalan bireylerin hem başkalarına hem de kendilerine olan güvenlerinde azalma, duygu düzenleme güçlüğü ve davranış kontrolünde zayıflama gibi olumsuz sonuçlar yaşadıkları ifade edilmektedir (Robalo & Abdul Rahim, 2023). Bu tür olumsuz deneyimler, bireylerin genel bilinçli farkındalık düzeylerinde de düşüşe yol açabilmektedir (Liu, Liu & Yuan, 2021). Her yaş grubunda önemli bir sorun teşkil eden siber mağduriyet, özellikle kimlik gelişiminin tamamlanmadığı üniversite döneminde daha hassas bir risk faktörü olarak öne çıkmaktadır. Bu nedenle, üniversite öğrencilerinin dijital mahremiyet farkındalıklarının değerlendirilmesi, siber mağduriyetin önlenmesinde önemli bir adım olarak görülmektedir. Bireylerin farkındalık düzeylerinin artması, olası mağduriyetlerin azaltılmasına katkı sağlayabilir.

Literatür tarandığında, bireylerin dijital mahremiyet farkındalığına ilişkin çeşitli çalışmaların gerçekleştirildiği görülmektedir. Örneğin öğretmen adaylarıyla yapılan bir araştırmada, bu bireylerin ortalamanın üzerinde bir dijital mahremiyet farkındalığına sahip

oldukları belirlenmiştir (Çakır vd., 2015). Benzer şekilde, Avcı ve Kayıran (2023)'ın üniversite öğrencileriyle yürüttüğü çalışmada da çevrim içi mahremiyet düzeylerinin yüksek olduğu rapor edilmiştir. Ancak, Eroğlu (2018)'nin gerçekleştirdiği bir başka çalışmada, üniversite öğrencilerinin kişisel veri ve gizlilik algılarının yeterince gelişmemiş olduğu ve bu alanda bilgi eksikliklerinin bulunduğu vurgulanmıştır. Semiz Türkoğlu (2018) ise teknolojik araçların yaygınlaşmasının bireylerin mahremiyetlerinden ödün vermelerine neden olduğunu ifade etmektedir. Ayrıca, Agosto ve Abbas (2017) tarafından yapılan araştırmada da dijital mahremiyet bilincinin gelişiminin zaman aldığına dikkat çekilmiştir. Bu bulgular, dijital mahremiyet farkındalığının bireyler arasında farklılık gösterebildiğini ve bu konunun daha derinlemesine araştırılması gerektiğini ortaya koymaktadır.

Mevcut araştırmalar, dijital mahremiyet farkındalığı düşük bireylerin sayısının azımsanamayacak düzeyde olduğunu ve bu durumun siber mağduriyet riskini artırdığını göstermektedir. Özellikle üniversite öğrencileri gibi dijital ortamlarla yoğun etkileşim içinde olan grupların, kişisel verilerinin korunmasına yönelik bilinçlerinin yüksek olması gerekmektedir. Alanyazın incelendiğinde, dijital mahremiyet farkındalığı ile siber mağduriyet arasındaki ilişkiye odaklanan çalışmaların sınırlı sayıda olduğu dikkat çekmektedir. Bu nedenle, bu araştırma söz konusu boşluğu doldurmayı amaçlamakta olup, ileride yapılacak çalışmalara da yön vererek literatüre katkı sunması hedeflenmektedir.

Bu bilgiler ışığında, mevcut çalışmanın temel amacı, üniversite öğrencilerinin dijital mahremiyet farkındalığı ile siber mağduriyet düzeyleri arasındaki ilişkiyi incelemektir. Bununla birlikte, öğrencilerin siber zorbalık, siber mağduriyet ve çevrim içi mahremiyet farkındalık düzeylerinin (genel ve alt boyutlar) belirlenmesi de araştırmanın hedefleri arasındadır. Ayrıca, öğrencilerin cinsiyetlerine ve sınıf düzeylerine göre bu değişkenlerde anlamlı bir farklılık olup olmadığını ortaya koymak ve yaş, günlük internet kullanımı, akademik internet kullanımı ve sosyal medya kullanımı gibi bireysel değişkenlerle olan ilişkileri analiz etmek de çalışmanın amaçları arasında yer almaktadır. Bu doğrultuda, araştırma aşağıdaki sorulara yanıt aramaktadır:

1. Üniversite öğrencilerinin siber zorbalık, siber mağduriyet ve çevrim içi mahremiyet farkındalık (genel ve alt boyutlar) düzeyleri nasıldır?
2. Üniversite öğrencilerinin siber zorbalık ve siber mağduriyet düzeyleri ile çevrim içi mahremiyet farkındalık (genel ve alt boyutlar) düzeyleri arasında anlamlı bir ilişki var mıdır?
3. Üniversite öğrencilerinin cinsiyetleri siber zorbalık, siber mağduriyet ve çevrim içi mahremiyet farkındalık (genel ve alt boyutlar) puanlarında farklılık yaratmakta mıdır?

4. Üniversite öğrencilerinin sınıf düzeyleri siber zorbalık, siber mağduriyet ve çevrim içi mahremiyet farkındalık (genel ve alt boyutlar) puanlarında farklılık yaratmakta mıdır?
5. Üniversite öğrencilerinin çeşitli değişkenleri (demografik özellikleri ve internet kullanım alışkanlıkları) ile siber zorbalık, siber mağduriyet ve çevrim içi mahremiyet farkındalık (genel ve alt boyutlar) düzeyleri arasında anlamlı bir ilişki var mıdır?
 - a. Yaşları?
 - b. Günlük internet kullanım süreleri?
 - c. Akademik internet kullanım süreleri?
 - d. Sosyal medya kullanım süreleri?

Son yıllarda dijital mahremiyet farkındalığına yönelik hem yurt içinde hem de yurt dışında çeşitli araştırmalar gerçekleştirilmiştir. Bu çalışmalar incelendiğinde, özellikle ergen ve genç bireylerin dijital mahremiyet konusundaki farkındalık düzeylerinin sorgulandığı görülmektedir. Bu araştırma da üniversite öğrencilerinin dijital mahremiyet farkındalığı düzeyleri ile bu farkındalığın siber mağduriyetle olan ilişkisini incelemeyi amaçlamaktadır. Alan yazın tarandığında, dijital mahremiyet farkındalığı ile siber mağduriyet arasındaki ilişkiyi konu alan yeterli sayıda çalışmanın bulunmadığı dikkat çekmektedir. Bu bağlamda, çalışmanın üniversite öğrencileri örnekleminde gerçekleştirilmesi ve farklı fakültelerden katılımcılarla veri toplanması, daha güçlü ve genellenebilir bulgulara ulaşılmasına katkı sağlayacaktır. Böylece, araştırmanın dijital mahremiyet alanına özgün bir katkı sunacağı ve literatürdeki boşluğu dolduracağı öngörülmektedir.

3.2. Araştırmanın Yöntemi

3.2.1. Araştırmanın Modeli

Bu çalışmada, sosyal medya bağımlılığı, siber zorbalık, siber mağduriyet ve çevrim içi mahremiyet farkındalık değişkenleri arasındaki ilişkileri incelemek amacıyla nicel araştırma yöntemlerinden biri olan ilişkisel araştırma modeli kullanılmıştır. İlişkisel araştırma deseni, araştırmacının iki ya da daha fazla değişken arasındaki doğal ilişkileri inceleyerek bu ilişkilerin yönünü ve derecesini belirlemeyi hedeflediği bir yöntemdir. Bu doğrultuda araştırmada, değişkenler üzerinde herhangi bir müdahalede bulunulmadan, var olan durumlar kendi doğal bağlamında ele alınmış ve aralarındaki potansiyel bağlantılar ortaya konmaya çalışılmıştır (Creswell, 2012; Frankel, Wallen & Hyun, 2012).

Bu kapsamda, öğrencilerin dijital mahremiyet farkındalığı düzeyleriyle siber zorbalık/mağduriyet deneyimleri arasındaki ilişki analiz edilmiş; ayrıca öğrencilerin sosyo-

demografik değişkenlerine göre anlamlı farklılıklar olup olmadığı araştırılmıştır. Araştırmada ilişkisel araştırma modelinin tercih edilmesinin temel nedeni, çalışmanın hem mevcut durumun kapsamlı biçimde betimlenmesine hem de değişkenler arasındaki ilişkinin yönüne ve gücüne dair bulgular elde edilmesine olanak tanımasıdır. Böylece, yalnızca öğrencilerin dijital mahremiyet farkındalıklarının hangi düzeyde olduğunun belirlenmesinin ötesine geçilerek, bu farkındalık düzeylerinin siber mağduriyet riskiyle nasıl bir ilişki içinde olduğu da detaylı biçimde incelenmiştir.

3.2.2. Araştırma Evren ve Örneklemi

Gençlik dönemi, dijital teknolojilerin en yoğun ve yaygın şekilde kullanıldığı yaş aralığını temsil etmektedir. Bu sebeple üniversite öğrencilerinin bu araştırmanın konusu olan dijital mahremiyet farkındalığı ve siber mağduriyet değişkenleriyle doğrudan ilişki kurabilecek en uygun grubu oluşturduğu düşünülmektedir. Bu bakımdan araştırmanın problematiği ve amacı kapsamında özellikle sosyal medya ve internet kullanım deneyimi olan genç bireylerin çalışmaya dâhil edilmesi hedeflenmiştir. Böylelikle araştırmanın evrenini, 2024-2025 eğitim-öğretim yılında Türkiye’de farklı üniversitelerde öğrenim gören lisans düzeyindeki öğrenciler oluşturmaktadır. Çalışmada yer alan öğrenciler, çeşitli fakülte ve bölümlerden seçilmiştir.

Araştırma kapsamında, Türkiye'deki farklı üniversitelerde öğrenim gören toplam 560 lisans öğrencisinden veri toplanmıştır. Katılımcıların büyük çoğunluğu %68,8 ile Akdeniz Üniversitesi’ne kayıtlı öğrencilerden oluşmaktadır. Bunu %26,6 ile Amasya Üniversitesi takip etmekte, kalan %4,6’lık kısmı ise Bilkent Üniversitesi, İstanbul Kent Üniversitesi, Kilis 7 Aralık Üniversitesi ve Iğdır Üniversitesi gibi çeşitli üniversitelerden gelen katılımcılar oluşturmaktadır.

Bölüm bazında incelendiğinde, öğrencilerin 30’u aşkın farklı lisans programında öğrenim görmekte olduğu görülmektedir. Örneklemde en yüksek katılım %34,8 ile Sosyal Hizmetler bölümünden gerçekleşmiştir. Bu oranı %17,7 ile Rehberlik ve Psikolojik Danışmanlık, %11,4 ile Yönetim Bilişim Sistemleri, %7,5 ile Türkçe Öğretmenliği ve %6,3 ile Felsefe bölümleri takip etmektedir. Katılımcıların geri kalanı; sosyoloji, tarih, İngilizce öğretmenliği, rekreasyon yönetimi, müzik öğretmenliği, bilgisayar programcılığı gibi çeşitli alanlarda dağılmıştır. Bu dağılım, araştırma verilerinin ağırlıklı olarak belirli bölümlerden elde edildiğini göstermekle birlikte, farklı akademik disiplinlerden öğrenci görüşlerinin de veri setine dahil edildiğini ortaya koymaktadır. Genel olarak, çalışmanın örneklemi hem üniversite hem de bölüm düzeyinde çeşitlilik göstermekle birlikte, bazı kurum ve programlarda yoğunlaşma gözlenmiştir. Bu durum, verilerin belirli bağlamlara özgü eğilimleri yansıttığını ve

elde edilen sonuçların bu örneklem yapısı çerçevesinde değerlendirilmesi gerektiğini göstermektedir.

Araştırmanın örnekleme, olasılıksız örnekleme yöntemlerinden biri olan *kolayda örnekleme* (convenience sampling) yöntemiyle belirlenmiştir. Bu yöntem, veri toplamanın hızlı ve pratik şekilde yürütülmesine olanak sağlamakta, aynı zamanda her bireyin örnekleme seçilme olasılığının eşit olması nedeniyle araştırma bulgularının evreni temsil etme gücünü artırmaktadır (Büyüköztürk vd., 2019). Uygulamada örneklem, gönüllülük esasına göre araştırmaya katılmayı kabul eden bireylerden oluşturulmuştur. Kolayda örnekleme yöntemiyle farklı üniversitelerden, fakültelerden ve bölümlerden öğrencilerin katılımının sağlanması, örneklemin demografik ve akademik çeşitliliğini artırmış ve dijital mahremiyet farkındalığı ile siber mağduriyet değişkenlerine ilişkin bulguların daha geniş bir çerçevede değerlendirilmesine olanak tanımıştır. Ancak bu örnekleme yönteminin, evreni tam anlamıyla temsil eden sonuçlar üretme kapasitesi sınırlı olmakla birlikte, elde edilen bulguların genel eğilimleri yansıtmaya gücüne katkı sağladığı düşünülmektedir (Creswell, 2012).

Araştırmada veri toplamak amacıyla kullanılan anketler, Google Forms üzerinden hazırlanmış ve katılımcılara çevrim içi yollarla ulaştırılmıştır. Kolayda örnekleme yöntemi kullanılarak internet üzerinden erişime açık olan öğrencilere ulaşılmış ve bu şekilde toplam 560 üniversite öğrencisinden veri toplanmıştır. Bu örnekleme yöntemi, Türkiye'nin farklı üniversite, fakülte ve bölümlerinden öğrencilerin katılım göstermesini mümkün kılarak örneklemin demografik ve akademik çeşitliliğini artırmıştır. Bu sayede, çalışmada ele alınan siber zorbalık, siber mağduriyet ve çevrim içi mahremiyet farkındalık düzeylerine ilişkin bulguların daha geniş bir perspektifte değerlendirilmesine olanak tanınmış ve sonuçların genel eğilimleri daha iyi yansıtabilmesi sağlanmıştır.

3.2.3. Veri Toplama Süreci

3.2.3.1. Veri Toplama Araçları

Bu araştırmada veri toplamak amacıyla birden fazla ölçme aracı kullanılmıştır: (1) Demografik Bilgiler Formu, (2) Siber Zorbalık (SZ)/Siber Mağduriyet (SM) Envanteri ve (3) Çevrim İçi Mahremiyet Farkındalık Ölçeği (ÇMFÖ). Kullanılan bu araçların ayrıntılı açıklamaları Tablo 3.1'de sunulmuştur.

Tablo 3.1 Veri Toplama Araçları

Araçlar	Değişkenler	Kaynak
Demografik Bilgiler Bölümü (12-soru)	- Cinsiyet, Yaş, Sınıf düzeyi, Üniversite, Bölüm- (5) - İnternet Kullanım Bilgileri- (7): Günlük internet kullanım süresi(saat), Günlük akademik amaçlı internet kullanım süresi (saat), Günlük sosyal medya kullanım süresi (saat), İnternet erişiminde kullanılan cihazlar, İnternet kullanım amaçları, Sosyal medya kullanım amaçları, Kullanılan sosyal medya platformları	Araştırmacı tarafından geliştirilmiştir.
Siber Zorbalık / Siber Mağduriyet Envanteri (11-madde)	- Siber Zorbalık - Siber Mağduriyet	Tanrıkulu & Erdur-Baker (2020)
Çevrim içi Mahremiyet Farkındalık Ölçeği (17-madde)	- Dikkat - Güvenlik - İletişim & Paylaşım	Korkmaz, Vergili & Karadaş (2021)

Mevcut çalışmada kullanılan veri toplama araçlarının tümüne Ekler’de yer verilmiştir.

3.2.3.1.1. Demografik Bilgiler Bölümü

Bu bölümde, katılımcıların demografik özellikleri ile internet kullanım alışkanlıklarına ilişkin bilgileri toplamak amacıyla toplam 12 soru yer almıştır. Demografik sorular; cinsiyet, yaş, sınıf düzeyi, üniversite ve bölüm bilgilerini içermektedir. İnternet kullanımına ilişkin sorular ise; günlük internet kullanım süresi (saat), günlük akademik amaçlı internet kullanımı süresi (saat) ve günlük sosyal medya kullanımı süresi (saat) değişkenleri kapsamaktadır. Ayrıca, katılımcıların internet erişiminde kullandıkları cihaz türleri, internet kullanım amaçları, sosyal medya kullanım amaçları ve tercih ettikleri sosyal medya platformlarına ilişkin sorular da bu bölümde yer almıştır.

3.2.3.1.2. Üniversite Öğrencileri İçin Sanal Zorbalık/Mağduriyet Envanteri

Üniversite öğrencilerinin çevrim içi ortamlarda ne ölçüde siber zorbalık yaptıklarını ya da bu tür davranışlara ne düzeyde maruz kaldıklarını belirlemek amacıyla, Tanrıkulu ve Erdur-Baker (2020) tarafından geliştirilen Üniversite Öğrencileri için Siber Zorbalık ve Mağduriyet Envanteri (Cyberbullying Inventory for University Students) kullanılmıştır. Ölçek, siber zorbalık ve siber mağduriyet olmak üzere iki alt boyuttan oluşmaktadır ve her iki alt boyutta da aynı 11 madde yer almaktadır. Katılımcılar, son altı ay içerisinde bu davranışları ne sıklıkta

yaşadıklarını ya da uyguladıklarını 4'lü Likert tipi bir derecelendirme ile yanıtlamaktadır: 1 = hiç, 2 = bir kez, 3 = iki-üç kez, 4 = üç kereden fazla.

Siber zorbalık alt boyutundaki ifadeler “Ben yaptım” şeklinde kurgulanırken, siber mağduriyet alt boyutundaki ifadeler “Bana yapıldı” biçimindedir. Her iki alt ölçek için teorik puan aralığı 11 ile 44 arasında değişmektedir. Ölçekte "bir kez" yanıt seçeneğinin özellikle korunması, davranışın siber zorbalık mı yoksa siber saldırganlık mı olduğunun ayırt edilmesini sağlamaktadır. Çünkü literatürde, siber zorbalığın tekrar eden davranışlar içermesi gerektiği, ancak siber saldırganlık için tek bir olayın yeterli olduğu belirtilmektedir (Vale vd., 2018). Örnek maddelere Tablo 3.2’de yer verilmiştir:

Tablo 3.2 SZ/SM Envanterinin Örnek Maddeleri

Alt boyut	Örnek madde
SZ (Ben yaptım.)	İnternette tehdit içeren, utandırıcı, kırıcı mesajlar göndermek.
SM (Bana yapıldı.)	İnternette tehdit içeren, utandırıcı, kırıcı mesajlar göndermek.
SZ (Ben yaptım.)	İnternette, cinsiyetini farklı göstererek karşı tarafı kandırmak.
SM (Bana yapıldı.)	İnternette, cinsiyetini farklı göstererek karşı tarafı kandırmak.

Her iki alt boyutta da daha yüksek puanlar, sırasıyla siber zorbalık yapma veya siber mağduriyet yaşama düzeyinin yüksek olduğunu göstermektedir. Ayrıca, ölçek sonuçları doğrultusunda katılımcılar siber zorba, siber mağdur hem zorba hem mağdur (zorba-mağdur) ya da hiçbirine dâhil olmayan bireyler olarak kategorize edilebilmektedir.

Ölçeğin iç tutarlılığı yüksek düzeydedir. Tanrıku ve Erdur-Baker (2020) tarafından raporlanan iç güvenilirlik katsayıları, siber zorbalık alt boyutu için .82, siber mağduriyet alt boyutu için ise .75 olarak bulunmuştur. Bu çalışmada ise, siber zorbalık alt boyutu için Cronbach alfa güvenilirlik katsayısı .82; siber mağduriyet alt boyutu için ise .85 olarak hesaplanmıştır. Her iki alt boyutta da Cronbach alfa değerlerinin .70’in üzerinde olması, ölçeğin güvenilirliğinin yeterli düzeyde olduğunu göstermektedir (Field, 2009)

3.2.3.1.3. Çevrim İçi Mahremiyet Farkındalık Ölçeği

Bu çalışmada, bireylerin çevrim içi ortamlardaki mahremiyet farkındalıklarının düzeyini belirlemek amacıyla, Korkmaz, Vergili ve Karadaş (2021) tarafından geliştirilen Çevrim İçi Mahremiyet Farkındalık Ölçeği (ÇMFÖ) kullanılmıştır. Ölçek, katılımcılardan son iki ay boyunca çevrim içi ortamda başkalarıyla etkileşim hâlindeyken verilen ifadelerin kendileri için ne sıklıkla geçerli olduğunu 5’li Likert tipi bir derecelendirme üzerinden belirtmelerini istemektedir. Orijinal formunda 0–4 arası puanlama sistemi kullanılırken, katılımcıların yanıt verme kolaylığını artırmak amacıyla bu sistem 1–5 arası bir ölçeğe dönüştürülmüştür. Yeni puanlamaya göre, 1 = hiçbir zaman, 2 = nadiren, 3 = bazen, 4 = sık sık,

5 = çok sık şeklinde düzenlenmiştir. Yapılan bu uyarlama yalnızca yanıt seçeneklerinin yeniden numaralandırılmasını kapsamaktadır; ölçeğin yapısal içeriğinde herhangi bir değişiklik yapılmamıştır.

Ölçek toplam 17 maddeden oluşmakta ve “Dikkat”, “Güvenlik” ve “İletişim & Paylaşım” olmak üzere üç alt boyut içermektedir. Bu boyutlar sırasıyla 7, 5 ve 5 maddeden meydana gelmektedir. Her bir alt boyut için örnek maddelere Tablo 3.3’te yer verilmiştir. Ayrıca, İletişim & Paylaşım alt boyutundaki maddeler olumsuz ifadeler içerdiği için bu maddeler ters yönde kodlanarak analiz edilmiştir.

Tablo 3.3 ÇMFÖ Örnek Maddeleri

Alt boyut/Madde sayısı	Örnek madde
Dikkat/ 7-madde	Kullandığım çevrim içi platformların gizlilik ayarlarını ve bildirim seçeneklerini düzenli olarak kontrol ederim.
Güvenlik/ 5-madde	İnternet sitelerinin kullandığı çerez (cookies) dosyalarının işlevi ve amacı hakkında bilgi sahibiyim.
İletişim&Paylaşım/ 5-madde	Çevrim içi ortamlarda tanımadığım kişilerle iletişim kurarım.

ÇMFÖ’den elde edilen verilerin güvenilirliği, Cronbach alfa iç tutarlılık katsayıları kullanılarak değerlendirilmiştir. Ölçeğin toplam Cronbach alfa güvenilirlik katsayısı önceki çalışmada .79 olarak bulunmuş; alt boyutlarda ise dikkat için .78, güvenlik için .70 ve iletişim & paylaşım için .71 değerleri elde edilmiştir. Bu çalışmada yapılan analizde ise ölçeğin toplam Cronbach alfa katsayısı .87 olarak hesaplanmış, alt boyutlar bazında güvenilirlik değerleri dikkat için .89, güvenlik için .86 ve iletişim & paylaşım için .75 olarak belirlenmiştir. Tüm bu katsayıların .70’in üzerinde olması, ölçeğin yeterli düzeyde güvenilir olduğunu göstermektedir (Field, 2009).

3.2.4. Araştırma Etiği

Bu çalışma, Akdeniz Üniversitesi Bilimsel Araştırma ve Yayın Etiği Kurulu’ndan 21.01.2025 tarihinde (Onay numarası.1119748) alınan onay doğrultusunda gerçekleştirilmiştir. Etik kurul onayı, araştırma sürecine başlanmadan önce temin edilmiş olup, veri toplama aşamaları ilgili kurulun onayı kapsamında yürütülmüştür.

Araştırmaya katılım tamamen gönüllülük esasına dayanmaktadır. Anket formunun başlangıcında katılımcılara çalışmanın amacı, kapsamı ve içeriğine ilişkin ayrıntılı bilgilendirme sunulmuş; elde edilecek verilerin yalnızca bilimsel amaçlarla kullanılacağı, kimlik bilgilerinin toplanmayacağı ve tüm yanıtların anonim olarak değerlendirileceği açıkça belirtilmiştir. Katılımcılar, bu bilgilendirme metnini okuyup onay verdikten sonra ankete erişim sağlamışlardır.

Katılımcıların istedikleri aşamada ankete katılımı sonlandırma hakları olduğu vurgulanmış; herhangi bir zorlama ya da yönlendirici uygulamaya başvurulmamıştır. Katılımcıların gizliliği ve veri güvenliği yüksek düzeyde korunmuş; toplanan tüm veriler yalnızca araştırma kapsamında analiz edilmiş ve üçüncü şahıslarla hiçbir şekilde paylaşılmamıştır.

3.2.5. Veri Analizi

Veri analizi IBM SPSS 22 programı kullanılarak gerçekleştirilmiştir. Öncelikle, katılımcıların demografik özelliklerine ve Siber Zorbalık, Siber Mağduriyet ve Çevrim içi Mahremiyet Farkındalık ölçeklerinin maddelerine ilişkin tanımlayıcı istatistikler raporlanmıştır. Çıkarımsal istatistiksel analizlere geçmeden önce, uygun analiz türünü belirlemek amacıyla verilerin normal dağılım gösterip göstermediği ve örneklem büyüklüğünün yeterliliği değerlendirilmiştir.

Normal dağılım varsayımı; çarpıklık ve basıklık değerlerinin ± 2 aralığında olması (George & Mallery, 2010), Kolmogorov-Smirnov ve Shapiro-Wilk testlerinin p değerlerinin .05'ten büyük olması (Field, 2009) ve histogram grafiklerinde gözlemlenen çan eğrisi formundaki dağılım ile değerlendirilmiştir. Bu kriterlere göre, Siber Zorbalık ve Siber Mağduriyet ölçekleri normal dağılım göstermemektedir. Çevrim içi Mahremiyet Farkındalık ölçeği ise çarpıklık ve basıklık değerleri ile histogram grafikleri incelendiğinde normal dağılım varsayımını karşılamaktadır.

Siber zorbalık, siber mağduriyet ve çevrim içi mahremiyet farkındalık değişkenleri arasındaki ilişkilerde, normal dağılım varsayımını karşılamayan değişkenlerin bulunması nedeniyle Spearman sıra farkları korelasyon katsayısı analizi tercih edilmiştir. Pallant (2017)'a göre, bu yöntemle elde edilen korelasyon katsayısının .40'ın altında olması, ilişki düzeyinin düşük olduğunu göstermektedir.

Siber Zorbalık ve Siber Mağduriyet değişkenlerinin normal dağılım göstermemesi nedeniyle, bu değişkenlerin yaş ve internet kullanım paterni ile olan ilişkileri Spearman korelasyon analizi ile; cinsiyet ile olan ilişkileri ise Mann-Whitney U testi ile incelenmiştir. Çevrim içi Mahremiyet Farkındalık ölçeği ve alt boyutlarının cinsiyet değişkenine göre karşılaştırılmasında ise normal dağılım varsayımının sağlanması ve her bir gruptaki örneklem büyüklüğünün yeterli olması ($N > 20$) (Tabachnick & Fidell, 2013) nedeniyle bağımsız örneklem *t*-testi uygulanmışken, ikiden fazla kategorisi olan sınıf düzeyi değişkeni için ise ANOVA yöntemi kullanılmıştır. Çalışmada kullanılan veri analiz tekniklerine göre örneklem büyüklüğünün yeterliliğini değerlendirmek amacıyla G-Power (v.3.1.9.4) yazılımı

kullanılmıştır. Spearman ve Pearson korelasyon analizleri için orta büyüklükte etki (.30), %5 hata payı ve %80 güç düzeyi esas alınarak yapılan analizde örneklemin en az 84 olması gerektiği hesaplanmıştır. Bağımsız örneklem t-testi için orta etki büyüklüğüne (.50) göre gerekli örneklem büyüklüğü toplam 128 katılımcı, dört grup arasındaki farkı incelemek için yapılan one-way ANOVA analizinde ise orta etki büyüklüğüne (.25) göre toplam 180 katılımcının gerekli olduğu belirlenmiştir. Mevcut örneklemin 560 kişi olması nedeniyle örneklemin tüm analizler için yeterli güçte olduğu görülmüştür. Tüm istatistiksel analizlerde anlamlılık düzeyi $p < .05$ olarak kabul edilmiştir.

3.2.6. Araştırmanın Varsayım ve Sınırlılıkları

Bütün araştırmalar belirli varsayımlar ve ön kabuller temelinde yürütülmektedir. Bu durum, çalışmanın bilimsel güvenirliğini etkilememektedir. Ulaşılan sonuçların yorumlanmasında dikkate alınması gereken koşullar vurgulanmaktadır. Bu araştırmada da dijital mahremiyet farkındalığı ve siber mağduriyet arasındaki ilişkiyi inceleme amacıyla, araştırma sürecini etkileyebilecek bazı temel varsayımlar kabul edilmiş ve çalışmanın kapsamını sınırlayan belirli koşullar tanımlanmıştır. Aşağıda, bu çalışmanın yürütülmesinde esas alınan varsayımlar ve sınırlılıklar ayrı ayrı belirtilmiştir.

Bu araştırmanın varsayımları şunlardır:

- Kullanılan veri toplama araçlarının (Kişisel Bilgi Formu, Siber Zorbalık/Mağduriyet Ölçeği ve Çevrim İçi Mahremiyet Farkındalık Ölçeği) geçerli ve güvenilir ölçümler sağladığı varsayılmaktadır.
- Katılımcıların, soruları dürüst ve içtenlikle yanıtladıkları kabul edilmektedir.
- Verilerin elde edildiği dönemde araştırma sonuçlarını etkileyebilecek tarihsel ya da çevresel faktörlerin etkisinin minimal düzeyde olduğu varsayılmaktadır.
- Ulaşılan örneklem sayısının, evreni temsil etme açısından yeterli olduğu kabul edilmektedir.

Araştırmanın sınırlılıkları ise şu şekildedir:

- Araştırma, yalnızca Kişisel Bilgi Formu Formu, Çevrim İçi Mahremiyet Farkındalık Ölçeği ve Siber Zorbalık/Mağduriyet Ölçeği'nden elde edilen verilerle sınırlıdır.
- Örneklem grubu, 2024-2025 eğitim-öğretim yılında üniversite öğrenimine devam eden öğrencilerle sınırlı tutulmuştur.
- Bulgular, veri toplama sürecinin gerçekleştiği 2024-2025 eğitim-öğretim yılı itibarıyla geçerli olan koşullarla sınırlıdır.

- Bu çalışmada elde edilen bulgular, sadece araştırmaya katılan üniversite öğrencilerinin özellikleri dikkate alınarak değerlendirilmiş; bulgular araştırmanın sınırlılıkları doğrultusunda değerlendirilmiştir.

3.3. Araştırma Bulgularının Değerlendirilmesi

Bu bölümde yürütülen araştırmanın bulgularına yer verilmiştir. İlk olarak, katılımcıların demografik özellikleri ile internet kullanım alışkanlıklarına ilişkin bulgular sunulmuştur. Ardından, üniversite öğrencilerinin siber zorbalık, siber mağduriyet ve çevrim içi mahremiyet farkındalık düzeylerine dair veriler ayrıntılı biçimde açıklanmıştır. Devamında, katılımcıların cinsiyetlerinin ve sınıf düzeylerinin siber zorbalık, siber mağduriyet ve çevrim içi mahremiyet farkındalık düzeylerinde anlamlı bir farklılık oluşturup oluşturmadığı değerlendirilmiştir. Son olarak, demografik özellikler ile internet kullanım alışkanlıklarının, öğrencilerin siber zorbalık, siber mağduriyet ve çevrim içi mahremiyet farkındalık düzeyleriyle olan ilişkileri incelenmiştir. Bulgular, araştırma sorularına sistematik bir biçimde yanıt verecek şekilde yapılandırılmıştır.

3.3.1. Sosyo-Demografik Özelliklere ve İnternet Kullanım Alışkanlıklarına İlişkin Bulgular

Bu bölümde, araştırma kapsamında elde edilen veriler doğrultusunda katılımcıların demografik özelliklerine ilişkin bulgular sunulmaktadır. Katılımcıların yaş, cinsiyet, sınıf düzeyi gibi değişkenlere ait dağılımlar tablolar hâlinde verilmiş ve bu bulgular betimsel istatistikler eşliğinde yorumlanmıştır.

Tablo 3.4'te katılımcıların demografik özelliklerine ilişkin betimleyici istatistikler sunulmuştur. Araştırmaya toplamda $n = 560$ üniversite öğrencisi katılmıştır. Katılımcıların %77.1'i ($n = 432$) kadın, %22.9'u ($n = 128$) erkektir. Sınıf düzeyi açısından incelendiğinde, katılımcıların %25.5'inin ($n = 143$) birinci sınıf, %34.8'inin ($n = 195$) ikinci sınıf, %17.1'inin ($n = 96$) üçüncü sınıf ve %22.5'inin ($n = 126$) dördüncü sınıf öğrencisi olduğu belirlenmiştir. Katılımcıların yaşları 17.0–53.0 aralığında değişmekte olup, yaş ortalaması $\bar{X} = 21.56$, standart sapması $SS = 4.32$ 'dir. Çalışmanın temel hedeflerinden biri, bireylerin dijital ortamlardaki mahremiyet farkındalıklarını etkileyebilecek olası davranış örüntülerini anlamaktır. Bu amaç doğrultusunda, günlük internet ve sosyal medya kullanım süreleri, en sık kullanılan dijital cihazlar, çevrim içi etkinliklerin türü ve sosyal medya platformlarının kullanım nedenleri gibi değişkenler ele alınmıştır. Mevcut çalışmada katılımcıların günlük toplam internet kullanım sürelerinin ortalaması $\bar{X} = 6.06$ saat ($SS = 3.13$), akademik internet kullanım sürelerinin ortalaması $\bar{X} = 2.17$ saat ($SS = 2.09$) ve sosyal medya kullanım sürelerinin ortalaması ise $\bar{X} =$

3.98 saat ($SS = 2.56$) olarak saptanmıştır. Ayrıca, günlük internet, akademik internet ve sosyal medya kullanım sürelerinin 0.0–24.0 saat aralığında değiştiği görülmektedir.

Tablo 3.4 Katılımcıların Sosyo-Demografik Özelliklerine ve İnternet Kullanım Alışkanlıklarına Göre Dağılımı (N = 560)

Değişken	f	%		
Cinsiyet				
Kadın	432		22.9	
Erkek	128		77.1	
Sınıf Düzeyi				
1. Sınıf	143		25.5	
2. Sınıf	195		34.8	
3. Sınıf	96		17.1	
4. Sınıf	126		22.5	
	$\bar{X}$	SS	Min	$Maks$
Yaş	21.56	4.32	17.0	53.0
Günlük İnternet Kullanım Süresi	6.06	3.13	1.0	24.0
Akademik İnternet Kullanım Süresi	2.17	2.09	0.0	24.0
Sosyal Medya Kullanım Süresi	3.98	2.56	0.0	24.0

f: Frekans; $\bar{X}$: aritmetik ortalama; SS: Standart Sapma; Min: Minimum; Maks: Maksimum

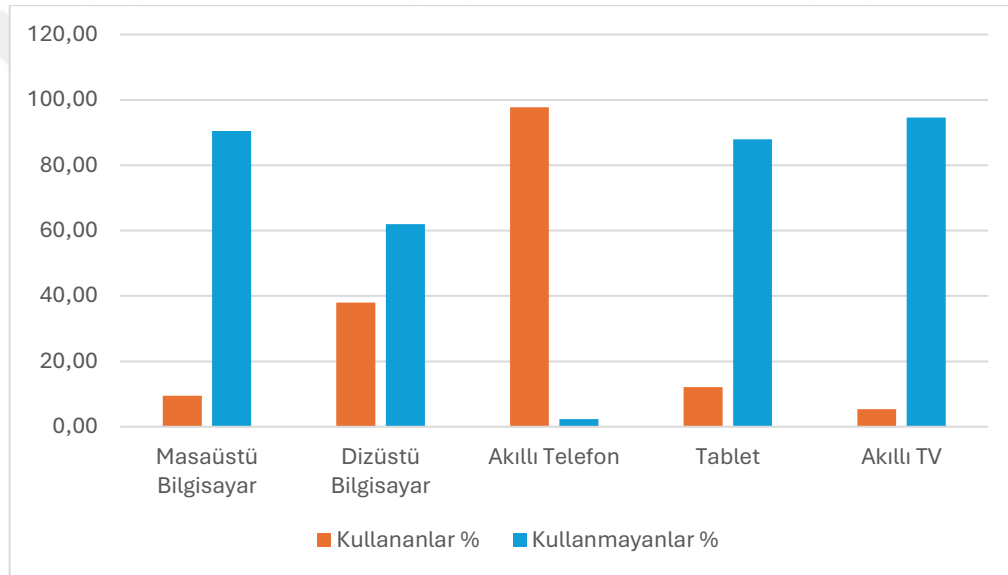
Katılımcıların büyük çoğunluğu (%97.7, $n = 547$) internete erişim için akıllı telefon kullanırken, yalnızca %2.3'lük ($n = 13$) bir kesim akıllı telefon kullanmamaktadır (bkz. Tablo 3.5). Dizüstü bilgisayar kullananların oranı %38.0 ($n = 213$), kullanmayanların oranı ise %62.0'dır ($n = 347$). Masaüstü bilgisayar kullanma oranı %9.5 ($n = 53$) iken, kullanmayanların oranı %90.5'tir ($n = 507$). Katılımcıların %12.1'i ($n = 68$) tablet kullanırken, %87.9'u ($n = 492$) kullanmamaktadır. Ayrıca akıllı TV kullanma oranı %5.4 ($n = 30$), kullanmayanların oranı ise %94.6 ($n = 530$) olarak belirlenmiştir.

Tablo 3.5 Katılımcıların İnternete Erişim Sağladığı Cihazların Dağılımı (N = 560)

İnternet Araçları	Kullananlar		Kullanmayanlar	
	<i>f</i>	%	<i>f</i>	%
Masaüstü Bilgisayar	53	9.5	507	90.5
Dizüstü Bilgisayar	213	38.0	347	62.0
Akıllı Telefon	547	97.7	13	2.3
Tablet	68	12.1	492	87.9
Akıllı TV	30	5.4	530	94.6

f: Frekans

Üniversite öğrencilerinin internete erişim sağladığı cihazlara ilişkin veriler, Şekil 3.1'de görsel olarak sunulmuştur.

**Şekil 3.1** Üniversite öğrencilerinin İnternete girme araçlarının kullanım dağılımı

Tablo 3.6'da katılımcıların sosyal medya platformlarını kullanma durumuna ilişkin frekans ve yüzde değerlerine yer verilmiştir. Katılımcıların büyük bir kısmının Instagram (%83.2; n = 466) ve WhatsApp (%81.4; n = 456) platformlarını aktif şekilde kullandığı görülmektedir. Bunu sırasıyla YouTube (%60.4; n = 338), Twitter (%25.7; n = 144) ve TikTok (%22.3; n = 125) takip etmektedir. Snapchat'i kullananların oranı %15.5 (n = 87) iken, Telegram (%3.6; n = 20) ve Facebook (%2.5; n = 14) kullanım oranlarının daha düşük seviyede olduğu belirlenmiştir.

Bunların yanı sıra, katılımcılar tarafından nadiren kullanılan diğer platformlar da bulunmaktadır (%1.6; n = 9). Bu gruptaki örnek cevaplar; Ekşi Sözlük, Sahibinden, ChatGPT, Spotify, Pinterest, Wattpad, Reddit ve Discord gibi platformları içermektedir.

Tablo 3.6 Katılımcıların Kullandıkları Sosyal Medya Platformları (N = 560)

Sosyal Medya Platformları	Kullananlar		Kullanmayanlar	
	<i>f</i>	%	<i>f</i>	%
Instagram	466	83.2	94	16.8
WhatsApp	456	81.4	104	18.6
You Tube	338	60.4	222	39.6
Twitter	144	25.7	416	74.3
TikTok	125	22.3	435	77.7
Snapchat	87	15.5	473	84.5
Telegram	20	3.6	540	96.4
Facebook	14	2.5	546	97.5
Diğer	9	1.6	551	98.4

f: Frekans

Tablo 3.7’de üniversite öğrencilerinin internet kullanım amaçlarına göre dağılımı verilmiştir. Üniversite öğrencilerinin büyük çoğunluğu interneti eğlence amacıyla (müzik dinleme, video veya film izleme; örneğin, YouTube, Netflix, Fizy, Spotify, PuhuTV vb.) kullandığını belirtmiştir (%82.7; $n = 463$). Bunu sırasıyla sosyal platformlarda fotoğraf ve video izleme ya da paylaşım yapma (%74.8; $n = 419$) ve öğrenme amacıyla bilgi paylaşma veya erişim sağlama (%51.1; $n = 286$) izlemektedir. Ayrıca üniversite öğrencilerinin %50.7’si ($n = 285$) çevrim içi alışveriş ve satış yapmak için interneti kullandığını bildirmiştir.

İnternet kullanım amaçları arasında en düşük orana sahip madde ise Kindle vb. üzerinden kitap okumadır (%7.9; $n = 44$). Üniversite öğrencilerinin %18.2’si ($n = 102$) kendi ilgi alanlarına yönelik web sitelerinde içerik okumakta, %31.1’i ($n = 174$) oyun oynamakta ve %38.6’sı ($n = 216$) interneti e-hizmetlerden (internet bankacılığı, hastane işlemleri vb.) yararlanmak için kullanmaktadır. Ayrıca öğrencilerin %46.1’i ($n = 258$) interneti haber, sağlık veya moda gibi konuları takip etmek için kullanırken, bu oran diğer kullanım amaçlarıyla kıyaslandığında orta düzeyde kalmaktadır.

Son olarak, üniversite öğrencilerinin %1.25’i ($n = 7$) diğer internet kullanım amaçlarını belirtmiş; bu grupta farklı oyun türlerinde vakit geçirme (Candycrush dışında), yapay zekâ araçlarını kullanma, PDF kitap indirip okuma, detaylı not çıkarmak için ChatGPT’den yardım alma, aktif e-ticaret ya da yayıncılık işleriyle uğraşma gibi örnekler yer almaktadır.

Tablo 3.7 Katılımcıların İnternet Kullanım Amaçlarına Göre Dağılımı ($N = 560$)

İnternet Kullanım Amaçları	Kullananlar		Kullanmayanlar	
	<i>f</i>	%	<i>f</i>	%
IA5. Eğlence (Müzik dinleme, Video/film izleme, (Youtube, Netflix, Fizy, Spotify, PuhuTV, Çevrim içi dizi/film siteleri vb.)	463	82.7	97	17.3
IA6. Instagram, Facebook gibi sosyal platformlarda fotoğraflara bakma / video izleme / paylaşım yapma	419	74.8	141	25.2
IA7. Öğrenme amaçlı, eğitimle ilgili bir şeyler paylaşma/ erişme	286	51.1	274	48.9
IA3. Çevrim içi alışveriş / satış yapmak (eBay, Gittigidiyor, Hepsiburada, Trendyol vb.)	285	50.7	276	49.3
IA2. İnternet'te haberler, gazeteler, sağlık, moda vb. ile ilgili bilgi arama/okuma	258	46.1	302	53.9
IA1. E hizmetler (internet bankacılığı, hastane işleri...)	216	38.6	344	61.4
IA4. Oyun oynama (Candycrush vb.)	174	31.1	386	68.9
IA9. İlgi alanlarınıza yönelik web sitelerinden bilgi okuma (Onedio, Listelist, Bilimfili, Düşünbil vb.)	102	18.2	458	81.8
IA8. Kindle vb. üzerinden kitap okumak.	44	7.9	516	92.1
Diğer	7	1.25	553	98.75

f: Frekans

Tablo 3.5'te belirtilen diğer internet kullanım amaçlarını detaylandırmak için yapılan incelemede, üniversite öğrencilerinin %1.25'inin ($n = 7$) Candycrush gibi klasik oyunlar yerine farklı tür oyunlar oynadığı, yapay zekâ araçlarını kullandığı, PDF formatında kitap indirip okuduğu ya da bu kitaplardan not çıkardığı, ayrıca detaylı notlar oluşturmak için ChatGPT'den faydalandığı görülmektedir. Buna ek olarak, bazı öğrencilerin aktif e-ticaret ya da yayıncılık faaliyetleriyle ilgilendikleri belirlenmiştir. Bu durum, üniversite öğrencilerinin interneti çok yönlü kullanarak hem akademik hem de kişisel gelişimlerine destekleyici çeşitli dijital araçlardan yararlandığını göstermektedir.

Tablo 3.8'de, üniversite öğrencilerinin sosyal medya kullanım amaçlarına göre dağılımı sunulmuştur. Bulgulara göre, katılımcıların büyük çoğunluğu WhatsApp aracılığıyla sosyalleşme ve sohbet etme amacıyla interneti kullanmaktadır (%83.2, $n = 475$). Bunu %74.4 ($n = 425$) oranıyla Facebook, Twitter, Instagram gibi platformlardan doğrudan mesajlaşarak etkileşimde bulunma izlemektedir. Ayrıca öğrencilerin %54.8'i ($n = 313$) sosyal medya paylaşımlarına yorum yaparak diğer insanlarla etkileşim kurduğunu belirtmiştir. Katılımcıların %46.9'u ($n = 268$) forumlarda mesaj (post) paylaşarak iletişim sağlamakta, %37.7'si ($n = 215$)

ise ilgi alanlarına yönelik web sitelerinde paylaşımlara yorum yapmaktadır. Flört uygulamaları aracılığıyla iletişim kuran öğrencilerin oranı %31.9 ($n = 182$) olarak bulunmuştur.

Tablo 3.8 Katılımcıların Sosyal Medya Kullanım Amaçlarına Göre Dağılımı ($N = 560$)

İnternet Kullanım Amaçları	Kullananlar		Kullanmayanlar	
	<i>f</i>	%	<i>f</i>	%
SA2. WhatsApp aracılığıyla sosyalleşme/ muhabbet etme amaçlı iletişim kurmak	475	83.2	96	16.8
SA1. Sosyal medya platformlarında doğrudan mesaj (DM) aracılığıyla etkileşime geçmek (Facebook, Twitter, Instagram vb. üzerinden)	425	74.4	146	25.6
SA3. Sosyal medya üzerinden, yapılan paylaşımlara diğer insanlarla etkileşim kurmak için yorum yapmak. (Facebook, Twitter, Instagram vb.)	313	54.8	258	45.2
SA4. İlgi alanınıza yönelik İnternet forumlarında diğer insanlarla iletişim kurmak için mesaj (post) paylaşmak (Donanım haber forum, Kadınlar kulübü, Ekşisözlük vb.)	268	46.9	303	53.1
SA5. Diğer insanlarla iletişim kurabilmek için ilgi alanlarınıza yönelik web sitelerinde yapılan paylaşımlara yorum yapmak (Onedio, Listelisi vb.)	215	37.7	356	62.3
SA6. Flört uygulamaları aracılığıyla iletişim kurmak (Tinder, Match vb.)	182	31.9	389	68.1
Diğer	6	1.05	565	98.95

f: Frekans

Tabloda ayrıca az sayıda katılımcının (%1.05, $n = 6$) diğer kullanım amaçlarını belirttiği görülmektedir. Bu kullanım biçimleri arasında Sahibinden platformunda emekli öğretmenlerle araçlar üzerine sohbet başlatmak, Reels ve YouTube içeriklerinden iletişim sağlamak, oyunlar üzerinden sosyal etkileşimde bulunmak, yayıncılık yapmak ya da araştırma ve film izlemek yer almaktadır. Bu sonuçlar, üniversite öğrencilerinin sosyal medya platformlarını yalnızca sohbet ve etkileşim için değil, aynı zamanda çok çeşitli ilgi alanlarına yönelik paylaşımları takip etme, içerik üretme ve bu içerikler aracılığıyla başkalarıyla bağlantı kurma amacıyla kullandığını göstermektedir.

3.3.2. Araştırma Sorusu 1: Üniversite Öğrencilerinin Siber Zorbalık/Mağduriyet ve Çevrim İçi Mahremiyet Farkındalık Düzeyleri

Bu bölümde, araştırmada kullanılan veri toplama araçlarından “Üniversite Öğrencileri için Siber Zorbalık/Mağduriyet Envanteri” ve “Çevrim içi Mahremiyet Farkındalık Ölçeği” ne ilişkin bulgulara yer verilmektedir. Öncelikle katılımcıların bu iki ölçekten elde ettikleri puanlara ilişkin betimleyici istatistikler sunulmuştur. Aritmetik ortalama ($\bar{X}$) ve standart sapma (SS) değerleri hesaplanmıştır.

3.3.2.1. Üniversite Öğrencilerinin Siber Zorbalık ve Siber Mağduriyet Seviyeleri

Tablo 3.9’da öğrencilerin kendi gerçekleştirdikleri siber zorbalık davranışları ile bu davranışlara maruz kalma düzeylerine ilişkin betimleyici istatistik sonuçları sunulmuştur. Bulgular incelendiğinde, uygulanan siber zorbalık düzeylerinin genel aritmetik ortalamasının ($\bar{X} = 1.16$, $SS = 0.32$), mağduriyet düzeylerinin genel aritmetik ortalamasına göre ($\bar{X} = 1.30$, $SS = 0.46$) daha düşük olduğu görülmektedir. Maddeler bazında değerlendirildiğinde, hem uygulanan hem de maruz kalınan zorbalık düzeylerinin en yüksek olduğu madde “Sanal ortamda birilerine küfür etmek”tir (zorbalık: $\bar{X} = 1.48$, $SS = 0.96$; mağduriyet: $\bar{X} = 1.60$, $SS = 1.05$). Bunu, “İnternette tehdit içeren, utandırıcı ya da kırııcı mesajlar göndermek” (zorbalık: $\bar{X} = 1.13$, $SS = 0.50$; mağduriyet: $\bar{X} = 1.42$, $SS = 0.85$) ve “İzin almadan kişisel bilgileri (dosya, fotoğraf, mesaj vb.) ele geçirmek” (zorbalık: $\bar{X} = 1.12$, $SS = 0.43$; mağduriyet: $\bar{X} = 1.36$, $SS = 0.76$) maddeleri izlemektedir.

Diğer maddelere bakıldığında, uygulanan ve maruz kalınan zorbalık düzeylerinin görece daha düşük olduğu anlaşılmaktadır. Örneğin, “İnternette başkasının kimliğiyle izinsiz paylaşım yapmak” (zorbalık: $\bar{X} = 1.08$, $SS = 0.35$; mağduriyet: $\bar{X} = 1.18$, $SS = 0.53$) ve “SMS aracılığıyla tehdit edici, utandırıcı ya da kırııcı mesajlar göndermek” (zorbalık: $\bar{X} = 1.08$, $SS = 0.36$; mağduriyet: $\bar{X} = 1.32$, $SS = 0.75$) maddeleri, en düşük ortalamalara sahip maddelerdir.

Tablo 3.9 Siber Zorbalık ve Siber Mağduriyet Envanterinin Maddelerinin Tanımlayıcı İstatistik Değerleri

Maddeler	Sanal Zorbalık (Ben yaptım)		Sanal Mağduriyet (Bana yapıldı)	
	X	SS	X	SS
M1.İzin almadan, kişisel bilgisayar veya akıllı telefondaki bilgileri (dosya, fotoğraf, yazılı mesaj kayıtları vb.) almak	1,12	,43	1,36	,76
M2. İnternet ortamında başkasının kimliğiyle izinsiz paylaşımında bulunmak	1,08	,35	1,18	,53
M3. Görüntülü yapılan özel bir görüşmeyi, karşı tarafın haberi olmadan başkasına izlettirmek	1,11	,42	1,20	,59
M4. İnternet ortamında yapılan paylaşımlara (yorum, fotoğraf, video, bilgi) utandırıcı, kırıcı yorumlar yapmak	1,21	,63	1,26	,69
M5. İnternette tehdit içeren, utandırıcı, kırıcı mesajlar göndermek	1,13	,50	1,42	,85
M6. İnternet şifrelerini ele geçirerek erişimi engellemek	1,10	,42	1,28	,63
M7. SMS aracılığıyla tehdit edici, utandırıcı, kırıcı mesajlar göndermek	1,08	,36	1,32	,75
M8. İnternette, cinsiyetini farklı göstererek karşı tarafı kandırmak	1,12	,46	1,23	,60
M9. Sanal ortamda dedikodu veya söylenti yaymak	1,23	,70	1,36	,82
M10. Sanal ortamda birilerine küfür etmek	1,48	,96	1,60	1,05
M11. Küçük düşürücü bir mesajı, fotoğrafı veya video görüntüsünü sanal ortamda izinsiz paylaşmak	1,08	,39	1,13	,48
Toplam	1.16	0.32	1.30	.46

$\bar{X}$: Aritmetik ortalama; SS: Standart sapma

Sonuç olarak, öğrencilerin kendi uyguladıkları zorbalık davranışlarının düzeyi genel olarak düşük olmakla birlikte, aynı davranışların mağduriyet boyutunun daha yaygın olduğu söylenebilir. Bu bulgular, öğrencilerin dijital ortamda karşılaştıkları siber zorbalık deneyimlerinin azaltılmasına yönelik farkındalık çalışmaları ve önleyici uygulamaların geliştirilmesine ihtiyaç olduğunu göstermektedir.

3.3.2.2. Üniversite Öğrencilerinin Çevrim İçi Mahremiyet Farkındalık Seviyeleri

Tablo 3.10 incelendiğinde, öğrencilerin çevrim içi mahremiyet farkındalığı düzeylerinin toplam aritmetik ortalamasının orta-yüksek seviyede olduğu görülmektedir ($\bar{X} = 3.82$, $SS = 0.61$). Üç alt boyut arasında en yüksek ortalamanın İletişim & Paylaşım boyutunda yer aldığı saptanmıştır ($\bar{X} = 4.08$, $SS = 0.77$). Bu boyut kapsamında yer alan maddelerden en yüksek ortalama sahip olan ifade, “Çevrim içi ortamlarda tanımadığım kişilerle kişisel bilgilerimi (adres, doğum tarihi, yaş, iş, telefon vb.) paylaşırım” ($\bar{X} = 4.39$, $SS = 0.98$) maddesidir. Bunu

sırasıyla, “Başkalarına ait bilgi, resim, video vb. içerikleri çevrim içi ortamlarda izin almaya gerek duymadan paylaşırım” ($\bar{X} = 4.34$, $SS = 0.96$) ve “Arkadaşlarımla veya yakınlarımla yaptığım yazışmaların ekran görüntülerini izin almaya gerek duymadan paylaşırım” ($\bar{X} = 3.95$, $SS = 1.17$) maddeleri izlemiştir. Bu bulgular, öğrencilerin başkalarının mahremiyetine yönelik daha az hassasiyet gösterdiklerine işaret etmektedir.

İkinci sırada yer alan Dikkat boyutunun ortalaması $\bar{X} = 3.89$ ($SS = 0.82$) olarak hesaplanmış olup, bu boyutta en yüksek ortalamaya sahip madde, “Çevrim içi ortamlarda paylaştığım bilgilerin şirketler, devlet kurumları veya bilgisayar korsanları tarafından kullanılabileceğinin farkındayım” ($\bar{X} = 4.10$, $SS = 1.07$) ifadesidir. Bu boyutta en düşük ortalama ise “E-posta veya sosyal ağlardan aldığım mesajların içeriğinin güvenilir olup olmadığını anlarım” ($\bar{X} = 3.66$, $SS = 0.99$) maddesinde görülmüştür.

Son olarak, Güvenlik boyutunun ortalaması $\bar{X} = 3.45$ ($SS = 0.89$) olup diğer boyutlara kıyasla daha düşük düzeydedir. Bu boyutta en yüksek ortalamaya sahip madde, “Mobil cihazıma uygulama yüklerken uygulamanın hangi izinleri talep ettiğine dikkat ederim” ($\bar{X} = 3.69$, $SS = 1.13$) iken, en düşük ortalamaya sahip madde, “İnternet sitelerinin kullandığı çerez (cookies) dosyaları hakkında bilgim vardır” ($\bar{X} = 3.09$, $SS = 1.10$) maddesidir. Güvenlik boyutundaki bu sonuçlar, öğrencilerin çevrim içi güvenlik araçlarını tanıma ve kullanma konusundaki bilinç düzeylerinin daha sınırlı olduğuna işaret etmektedir.

Tablo 3.10 Çevrim İçi Mahremiyet Farkındalık Ölçeği Maddelerinin Tanımlayıcı İstatistik Değerleri

Maddeler	$\bar{X}$	SS
Dikkat	3,89	0,82
M3. Çevrim içi ortamlarda kullandığım parolaların güçlü olmasına (büyük-küçük harf, rakam, özel karakterler ve en az 8 karakter kullanımıyla) dikkat ederim.	3,99	1,12
M4. Çevrim içi ortamlarda paylaştığım bilgilerin şirketler, devlet kurumları veya bilgisayar korsanları tarafından kullanılabileceğinin farkındayım.	3,98	1,03
M5. Çevrim içi ortamlarda tanımadığım kişilerden gelen mesaj veya e-postaların güvenlik riski oluşturup oluşturmadığını anlarım.	3,77	0,99
M9. Çevrim içi platformlarda paylaştığım bilgilerin kötü niyetli kişiler tarafından kullanılabileceğinin farkındayım.	4,10	1,07
M10. E-posta veya sosyal ağlardan aldığım mesajların içeriğinin güvenilir olup olmadığını anlarım.	3,66	0,99
M13. Kullandığım çevrim içi ortamlarda (sosyal ağlar, alışveriş siteleri, oyunlar vb.) hesabımın gizlilik ayarlarını yaparım.	3,88	1,05
M14. Kullandığım çevrim içi platformların gizlilik ayarlarını ve bildirimlerini kontrol ederim.	3,83	1,05
Güvenlik	3,45	0,89
M11. İnternet sitelerinin kullandığı çerez (cookies) dosyaları hakkında bilgim vardır.	3,09	1,10

M12. İnternet sitelerinin ve mobil uygulamaların güvenlik sertifikalarını ve veri şifreleme yöntemlerini kontrol ederim.	3,17	1,14
M15. Mobil cihazıma uygulama yüklerken uygulamanın hangi izinleri talep ettiğine dikkat ederim.	3,69	1,13
M16. Web tarayıcımdaki eklentilerin hangi bilgilere erişeceğine dikkat ederim.	3,59	1,11
M17. Ziyaret ettiğim web sitelerinin güvenliğini kontrol ederim.	3,69	1,06
İletişim & Paylaşım	4,08	0,77
t-M1. Arkadaşlarımla veya yakınlarımla yaptığım yazışmaların ekran görüntülerini izin almaya gerek duymadan paylaşıyorum.	3,95	1,17
t-M2. Başkalarına ait bilgi, resim, video vb. içerikleri çevrim içi ortamlarda izin almaya gerek duymadan paylaşıyorum.	4,34	0,96
t-M6. Çevrim içi ortamlarda tanımadığım kişilerin beni takip etmesine veya arkadaş olmasına izin veririm.	3,90	1,12
t-M7. Çevrim içi ortamlarda tanımadığım kişilerle iletişim kurarım.	3,83	1,17
t-M8. Çevrim içi ortamlarda tanımadığım kişilerle kişisel bilgilerimi (adres, doğum tarihi, yaş, iş, telefon vb.) paylaşıyorum.	4,39	0,98
Toplam ÇMF	3,82	0,61

$\bar{X}$: Aritmetik ortalama; SS: Standart sapma

Sonuç olarak, bu bulgular, öğrencilerin çevrim içi ortamlarda dikkat ve güvenlik konularında görece daha yüksek farkındalık düzeyine sahip olduklarını, ancak iletişim ve paylaşım boyutunda gizlilik ve veri güvenliği konularında daha düşük düzeyde farkındalık gösterdiklerini ortaya koymaktadır. Ayrıca, güvenlik boyutunun diğer alt boyutlara kıyasla daha düşük ortalamaya sahip olması, öğrencilerin çevrim içi güvenlik uygulamalarıyla ilgili bilgi düzeylerinin sınırlı olduğuna işaret etmektedir.

3.3.3. Araştırma Sorusu 2: Üniversite Öğrencilerinin Siber Zorbalık ve Mağduriyet ile Çevrim İçi Mahremiyet Genel ve Alt Boyut Puanları Arasında İlişki

Üniversite öğrencilerinin siber zorbalık ve mağduriyet düzeyleri ile çevrim içi mahremiyet farkındalığı (genel ve alt boyutlar) arasındaki ilişkiler bu bölümde incelenmiştir. Ölçme araçlarının normallik varsayımı karşılanmadığı için analizlerde Spearman sıra korelasyonu kullanılmıştır.

İlk olarak, siber zorbalık ile siber mağduriyet toplam puanı arasında pozitif yönlü, yüksek düzeyde ve istatistiksel olarak anlamlı bir ilişki bulunmuştur ($r = .62, p < .01$). Pallant'a (2017) göre, .40'ın üzerindeki korelasyon katsayıları orta düzeyde bir ilişkinin varlığına işaret etmektedir. Bu sonuç, sanal ortamda zorbalık yapan öğrencilerin aynı zamanda mağduriyet yaşama risklerinin de yüksek olduğunu göstermektedir.

Çevrim içi mahremiyet toplam puanı, siber zorbalık ($r = -.20, p < .01$) ve siber mağduriyet ($r = -.12, p < .01$) puanlarıyla anlamlı ve negatif yönde ilişki göstermiştir. Bu durum, mahremiyet farkındalık düzeyi yüksek olan öğrencilerin, siber zorbalık yapma ve mağduriyet yaşama olasılıklarının daha düşük olduğuna işaret etmektedir.

Alt boyutlar incelendiğinde, “Dikkat” boyutunun siber zorbalık ($r = -.07, p = .102$) ve siber mağduriyet ($r = -.02, p = .691$) ile anlamlı bir ilişki göstermediği; “Güvenlik” boyutunun ise siber zorbalık ($r = -.11, p < .01$) düzeyiyle düşük ancak anlamlı bir negatif ilişki sergilediği görülmüştür. Bunun yanı sıra, “İletişim & Paylaşım” boyutunun hem siber zorbalık ($r = -.35, p < .01$) hem de siber mağduriyet ($r = -.30, p < .01$) düzeyleriyle anlamlı, negatif ve düşük düzeyde bir ilişki gösterdiği tespit edilmiştir.

Elde edilen bulgular, öğrencilerin çevrim içi mahremiyet farkındalıklarının bazı boyutlarının, özellikle iletişim ve paylaşım davranışlarının, siber zorbalık ve mağduriyet deneyimleriyle önemli ölçüde ilişkili olduğuna işaret etmektedir. Bulguların detayları Tablo 3.11’de sunulmuştur.

Tablo 3.11 Üniversite Öğrencilerinin Siber Zorbalık ve Mağduriyet ile Çevrim İçi Mahremiyet Genel ve Alt Boyut Puanları Arasında İlişki Tablosu

Ölçek	Siber Zorbalık		Siber Mağduriyet	
	<i>r</i>	<i>p</i>	<i>r</i>	<i>p</i>
Siber Zorbalık	-	-	.62**	.000
Çevrim İçi Mahremiyet	-.20**	.000	-.12**	.003
Dikkat	-.07	.102	-.02	.691
Güvenlik	-.11**	.008	-.05**	.211
İletişim & Paylaşım	-.35**	.000	-.30**	.000

* $p < .05$, ** $p < .01$, *r*: Spearman korelasyon katsayısı

3.3.4. Araştırma Sorusu 3: Üniversite Öğrencilerinin Sanal Zorbalık/Mağduriyet ve Çevrim İçi Mahremiyet Farkındalık Genel ve Alt Boyut Puanlarının Cinsiyete Göre Farklılaşması

Bu bölümde, üniversite öğrencilerinin sanal zorbalık ve sanal mağduriyet düzeylerinin cinsiyete göre anlamlı bir farklılık gösterip göstermediği incelenmiştir. Verilerin normallik varsayımını karşılamaması nedeniyle, bu analiz için parametrik olmayan bir teknik olan Mann-Whitney *U* testi kullanılmıştır. Ardından, öğrencilerin çevrim içi mahremiyet farkındalık toplam puanı ve alt boyutlarının cinsiyete göre değişip değişmediği araştırılmıştır. Bu değişkenlere ait verilerin normal dağılım gösterdiği belirlendiğinden, analiz için bağımsız gruplar *t*-testi uygulanmıştır.

3.3.4.1.1. Üniversite Öğrencilerinin Sanal Zorbalık ve Sanal Mağduriyet Puanlarının Cinsiyete Göre Farklılaşması

Elde edilen bulgular Tablo 3.12’de sunulmuştur. Katılımcıların sanal zorbalık (SZ) puanlarının cinsiyete göre anlamlı şekilde farklılaştığı görülmüştür ($U = 21650.50$, $p = .000$, $p < .05$). Erkek katılımcıların sanal zorbalık sıra ortalaması ($\bar{X}_{sıra} = 327.36$), kadın katılımcıların sanal zorbalık sıra ortalamasından ($\bar{X}_{sıra} = 266.62$) daha yüksektir. Bu bulgu, erkek öğrencilerin sanal zorbalık düzeylerinin kadın öğrencilere kıyasla anlamlı biçimde daha yüksek olduğunu göstermektedir. Buna karşılık, sanal mağduriyet (SM) puanlarının cinsiyete göre anlamlı bir farklılık göstermediği bulunmuştur ($U = 27337.00$, $p = .841$, $p > .05$). Kadın katılımcıların sanal mağduriyet sıra ortalaması ($\bar{X}_{sıra} = 279.78$) ile erkek katılımcıların sanal mağduriyet sıra ortalaması ($\bar{X}_{sıra} = 282.93$) birbirine oldukça yakındır. Bu sonuç, üniversite öğrencilerinin sanal mağduriyet deneyimlerinin cinsiyete göre değişmediğini göstermektedir.

Tablo 3.12 Üniversite Öğrencilerinin Cinsiyetlerine Göre Sanal Zorbalık ve Sanal Mağduriyet Puanları Arasında Karşılaştırma Tablosu

Ölçek	Cinsiyet	N	$\bar{X}_{sıra}$	$\Sigma_{sıra}$	U	Z	p
SZ	Kadın	432	266.62	115178.50	21650.50	-4.266	.000**
	Erkek	128	327.36	41901.50			
SM	Kadın	432	279.78	120865.50	27337.00	-.201	.841
	Erkek	128	282.93	36215.50			

* $p < .05$; ** $p < .01$; $\bar{X}_{sıra}$: sıra ortalaması; $\Sigma_{sıra}$: sıra toplamı; U: Mann-Whitney test değeri Z: Standartlaştırılmış U değeri

3.3.4.1.2. Üniversite Öğrencilerinin Çevrim İçi Mahremiyet Farkındalık Genel ve Alt Boyut Puanlarının Cinsiyete Göre Farklılaşması

Elde edilen sonuçlar Tablo 3.13’te sunulmuştur. Bulgulara göre, öğrencilerin toplam çevrim içi mahremiyet puanlarında kadın ($\bar{X} = 3.85$, $ss = .58$) ve erkek ($\bar{X} = 3.69$, $ss = .69$) öğrenciler arasında anlamlı bir farklılık saptanmıştır ($t(558) = 2.637$, $p = .009$, $p < .01$). Bu sonuç, kadın öğrencilerin toplam çevrim içi mahremiyet farkındalıklarının erkek öğrencilere kıyasla anlamlı düzeyde daha yüksek olduğunu göstermektedir. Alt boyutlar incelendiğinde, dikkat boyutunda da anlamlı bir farklılık görülmektedir ($t(558) = 2.207$, $p = .028$, $p < .05$), kadın öğrencilerin ($\bar{X} = 3.93$, $ss = .76$) erkek öğrencilerden ($\bar{X} = 3.75$, $ss = .99$) daha yüksek puan aldığı tespit edilmiştir. Güvenlik boyutunda ise kadın ($\bar{X} = 3.44$, $ss = .86$) ve erkek ($\bar{X} = 3.45$, $ss = 1.00$) öğrencilerin puanları arasında anlamlı bir farklılık bulunmamıştır ($t(558) = -.107$, $p = .915$, $p > .05$). Son olarak, iletişim ve paylaşım alt boyutunda kadın öğrencilerin ($\bar{X} =$

4.15, $ss = .74$), erkek öğrencilerden ($\bar{X} = 3.85$, $ss = .81$) anlamlı şekilde daha yüksek puan aldığı görülmüştür ($t(558) = 4.031$, $p = .000$, $p < .01$).

Tablo 3.13 Üniversite Öğrencilerinin Cinsiyetlerine Göre Çevrim İçi Mahremiyet Genel ve Alt Boyutları Puanları Arasında Karşılaştırma Tablosu

Ölçekler	Grup	N	Ortalama	ss	$t_{(558)}$	p
Çevrim İçi Mahremiyet	Kadın	432	3.85	.58	2.637	.009**
	Erkek	128	3.69	.69		
Dikkat	Kadın	432	3.93	.76	2.207	.028*
	Erkek	128	3.75	.99		
Güvenlik	Kadın	432	3.44	.86	-.107	.915
	Erkek	128	3.45	1.00		
İletişim & Paylaşım	Kadın	432	4.15	.74	4.031	.000**
	Erkek	128	3.85	.81		

* $p < .05$; ** $p < .01$; $\bar{x}$: aritmetik ortalama; ss: standart sapma; t: bağımsız gruplar t testi istatistik değeri

Bu bulgular, özellikle toplam çevrim içi mahremiyet, dikkat ve iletişim & paylaşım boyutlarında kadın öğrencilerin erkek öğrencilere göre daha yüksek farkındalık seviyelerine sahip olduğunu göstermektedir.

3.3.5. Araştırma Sorusu 4: Üniversite Öğrencilerinin Sanal Zorbalık/Mağduriyet ve Çevrim İçi Mahremiyet Farkındalık Genel ve Alt Boyut Puanlarının Sınıf Düzeylerine Göre Farklılaşması

Bu bölümde, üniversite öğrencilerinin sanal zorbalık ve sanal mağduriyet düzeylerinin sınıf düzeylerine göre anlamlı bir farklılık gösterip göstermediği incelenmiştir. Sanal zorbalık ve sanal mağduriyet değişkenlerine ilişkin verilerin normallik varsayımını karşılamaması nedeniyle, analiz için parametrik olmayan bir teknik olan Kruskal-Wallis H testi kullanılmıştır. Ayrıca, öğrencilerin çevrim içi mahremiyet farkındalık toplam puanı ve alt boyutlarının sınıf düzeylerine göre değişip değişmediği araştırılmıştır. Bu değişkenlere ait verilerin normal dağılım gösterdiği belirlendiğinden, analiz için tek yönlü varyans analizi (one-way ANOVA) uygulanmıştır. Her iki analizde de gruplar arası farkların hangi gruplar arasında oluştuğunu belirlemek amacıyla ikili karşılaştırmalar (pairwise comparisons) yapılmıştır.

3.3.5.1. Üniversite Öğrencilerinin Sanal Zorbalık ve Sanal Mağduriyet Puanlarının Sınıf Düzeyine Göre Farklılaşması

Tablo 3.14'te sunulan bulgulara göre, üniversite öğrencilerinin sanal zorbalık (SZ) ve sanal mağduriyet (SM) puanlarının sınıf düzeylerine göre anlamlı şekilde farklılaştığı görülmüştür. SZ için yapılan Kruskal-Wallis testi sonuçlarına göre sınıf düzeyleri arasında

istatistiksel olarak anlamlı bir fark olduğu saptanmıştır ($H(3) = 11.044$, $p = .011$). Benzer şekilde, SM için de anlamlı bir farklılık elde edilmiştir ($H(3) = 13.568$, $p = .004$). İkili karşılaştırmalar incelendiğinde, SZ için 1. sınıf ($\bar{X}_{\text{sıra}} = 268.12$) ve 4. sınıf ($\bar{X}_{\text{sıra}} = 314.56$) öğrencileri arasında ($p < .05$), ayrıca 3. sınıf ($\bar{X}_{\text{sıra}} = 257.09$) ve 4. sınıf ($\bar{X}_{\text{sıra}} = 314.56$) öğrencileri arasında ($p < .05$) anlamlı farklılık bulunmuştur. Sıra ortalaması daha büyük olan 4. sınıf öğrencilerinin SZ puanlarının, 1. ve 3. sınıflara kıyasla daha yüksek olduğu söylenebilir. Diğer sınıflar arasındaki karşılaştırmalarda anlamlı fark elde edilmemiştir. Benzer şekilde, SM için yapılan pairwise karşılaştırmalar, 1. sınıf ($\bar{X}_{\text{sıra}} = 259.22$) ve 4. sınıf ($\bar{X}_{\text{sıra}} = 312.41$) öğrencileri arasında ($p < .05$), ayrıca 3. sınıf ($\bar{X}_{\text{sıra}} = 246.57$) ve 4. sınıf ($\bar{X}_{\text{sıra}} = 312.41$) öğrencileri arasında ($p < .05$) anlamlı farklar olduğunu göstermektedir. Bu durumda da sıra ortalaması daha yüksek olan 4. sınıf öğrencilerinin SM düzeylerinin, 1. ve 3. sınıftaki öğrencilere kıyasla daha yüksek olduğu görülmektedir. Diğer grup karşılaştırmalarında anlamlı bir fark bulunmamıştır. Diğer karşılaştırmalarda ise istatistiksel açıdan anlamlı bir fark bulunmamıştır. Sonuç olarak, hem sanal zorbalık hem de sanal mağduriyet düzeylerinin 4. sınıf öğrencilerinde diğer sınıflara kıyasla daha yüksek olduğu görülmüştür.

Tablo 3.14 Üniversite Öğrencilerinin Sınıf Düzeylerine göre Çevrim İçi Mahremiyet Genel ve Alt Boyutları Puanları Arasında Karşılaştırma Tablosu

Ölçek	Sınıf Düzeyi	N	$\bar{X}_{\text{sıra}}$	H	df	p
SZ	1. Sınıf	143	268.12	11.044	3	.011
	2. Sınıf	195	279.09			
	3. Sınıf	96	257.09			
	4. Sınıf	126	314,56			
SM	1. Sınıf	143	259.22	13.568	3	.004
	2. Sınıf	195	292.19			
	3. Sınıf	96	246.571			
	4. Sınıf	126	312.41			

* $p < .05$; ** $p < .01$; H : Kruskal-Wallis test değeri

3.3.5.2. Üniversite Öğrencilerinin Çevrim İçi Mahremiyet Farkındalık Genel ve Alt Boyut Puanlarının Sınıf Düzeyine Göre Farklılaşması

Üniversite öğrencilerinin çevrim içi mahremiyet farkındalığı genel ve alt boyut puanlarının sınıf düzeyine göre farklılaşıp farklılaşmadığını incelemek amacıyla tek yönlü varyans analizi (one-way ANOVA) gerçekleştirilmiş; elde edilen sonuçlar Tablo 3.15'te

sunulmuştur. Katılımcıların sınıf düzeylerine göre çevrim içi mahremiyet farkındalık genel ölçek puanlarında anlamlı bir farklılık saptanmamıştır ($F(3,556) = 2.186, p = .089, p > .05$). Benzer şekilde, dikkat ($F(3,556) = .606, p = .611, p > .05$) ve güvenlik ($F(3,556) = 1.444, p = .229, p > .05$) alt boyutlarında da anlamlı farklılık bulunmamıştır. Ancak iletişim ve paylaşım alt boyutunda sınıf düzeylerine göre anlamlı bir fark olduğu belirlenmiştir ($F(3,556) = 4.352, p = .005, p < .01$). LSD karşılaştırma sonuçlarına göre birinci sınıf öğrencilerinin iletişim ve paylaşım puanlarının ($\bar{X} = 4.25, ss = 0.76$), ikinci sınıf ($\bar{X} = 4.05, ss = 0.80$), üçüncü sınıf ($\bar{X} = 4.11, ss = 0.62$) ve dördüncü sınıf öğrencilerinden ($\bar{X} = 3.92, ss = 0.80$) anlamlı düzeyde daha yüksek olduğu bulunmuştur. Bu sonuç, birinci sınıf öğrencilerinin iletişim ve paylaşım boyutunda diğer sınıflara kıyasla daha yüksek ortalamaya sahip olduklarını göstermektedir.

Tablo 3.15 Üniversite Öğrencilerinin Sınıf Düzeylerine göre Çevrim İçi Mahremiyet Genel ve Alt Boyutları Puanları Arasında Karşılaştırma Tablosu

Ölçekler	Grup	N	Ortalama	ss	$F(3,556)$	p	Fark
Çevrim İçi mahremiyet	1. Sınıf	143	3.90	.63	2.186	.089	
	2. Sınıf	195	3.83	.63			
	3. Sınıf	96	3.79	.60			
	4. Sınıf	126	3.71	.56			
Dikkat	1. Sınıf	143	3.90	.85	.606	.611	
	2. Sınıf	195	3.94	.83			
	3. Sınıf	96	3.83	.83			
	4. Sınıf	126	3.84	.75			
Güvenlik	1. Sınıf	143	3.55	0.91	1.444	.229	
	2. Sınıf	195	3.46	0.91			
	3. Sınıf	96	3.42	0.90			
	4. Sınıf	126	3.32	0.84			
İletişim&Paylaşım	1. Sınıf	143	4.25	0.76	4.352	.005	1>2,3,4
	2. Sınıf	195	4.05	0.80			
	3. Sınıf	96	4.11	0.62			
	4. Sınıf	126	3.92	0.80			

* $p < .05$; ** $p < .01$; ss: standart sapma; F: ANOVA yöntemi istatistik değeri; Fark: Anlamlı ANOVA sonucu için farkın hangi grup lehine olduğunu gösteren LSD karşılaştırma sonucu

3.3.6. Araştırma Sorusu 5: Üniversite Öğrencilerinin Çeşitli Değişkenler (Demografik Özellikler ve İnternet Kullanım Alışkanlıkları) ile Sanal Zorbalık/Mağduriyet ve Çevrim İçi Mahremiyet Farkındalık Puanları Arasındaki İlişki

Bu bölümde, üniversite öğrencilerinin demografik özellikleri ve internet kullanım alışkanlıklarının sanal zorbalık, sanal mağduriyet ve çevrim içi mahremiyet farkındalık puanlarıyla arasındaki ilişki incelenmiştir. Sanal zorbalık ve sanal mağduriyet değişkenlerinde normallik varsayımı karşılanmadığı için, bu değişkenlerle ilgili analizlerde non-parametrik

tekniklerden Spearman korelasyon katsayısı kullanılmıştır. Buna karşılık, çevrim içi mahremiyet farkındalığı toplam puanı ve alt boyutlarının normal dağılım göstermesi nedeniyle, bu değişkenlerle yapılan analizlerde parametrik bir teknik olan Pearson korelasyon katsayısından yararlanılmıştır.

3.3.6.1. Üniversite Öğrencilerinin Yaşları ile Sanal Zorbalık, Sanal Mağduriyet, Çevrim İçi Mahremiyet Farkındalık Genel ve Alt Boyut Puanları Arasındaki İlişki

Üniversite öğrencilerinin yaşları ile sanal zorbalık, sanal mağduriyet ve çevrim içi mahremiyet farkındalık toplam ve alt boyut puanları arasındaki ilişkiyi incelemek amacıyla yapılan analiz sonuçları Tablo 3.16’da sunulmuştur. Öğrencilerin yaşı ile sanal zorbalık ($r = .000, p = .995$), sanal mağduriyet ($r = -.005, p = .901$), çevrim içi mahremiyet toplam puanı ($r = .057, p = .175$), dikkat alt boyutu ($r = .042, p = .323$), güvenlik alt boyutu ($r = .029, p = .493$) ve iletişim & paylaşım alt boyutu ($r = .060, p = .157$) arasında anlamlı bir ilişki bulunmamıştır ($p > .05$). Bu bulgular, üniversite öğrencilerinin sanal zorbalık, sanal mağduriyet ve çevrim içi mahremiyet farkındalık düzeylerinin yaş değişkeniyle bağlantılı olmadığını göstermektedir.

Tablo 3.16 Üniversite Öğrencilerinin Yaşları ile Sanal Zorbalık, Sanal Mağduriyet, Çevrim İçi Mahremiyet Farkındalık Genel ve Alt Boyut Puanları Arasındaki İlişki

Ölçek	Yaş	
	r	p
Siber Zorbalık	.000	.995
Siber Mağduriyet	-.005	.901
Çevrim İçi Mahremiyet	.057	.175
Dikkat	.042	.323
Güvenlik	.029	.493
İletişim & Paylaşım	.060	.157

* $p < .05$; ** $p < .01$; r : Spearman ve Pearson korelasyon katsayısı

3.3.6.2. Üniversite Öğrencilerinin Günlük İnternet Kullanım Süreleri ile Sanal Zorbalık, Sanal Mağduriyet, Çevrim İçi Mahremiyet Farkındalık Genel ve Alt Boyut Puanları Arasındaki İlişki

Tablo 3.17’de üniversite öğrencilerinin günlük internet kullanım süresi ile sanal zorbalık, sanal mağduriyet ve çevrim içi mahremiyet farkındalık toplam ve alt boyut puanları arasındaki ilişkiler verilmiştir. Analiz sonuçlarına göre, öğrencilerin günlük internet kullanım süresiyle sanal zorbalık arasında pozitif ve düşük düzeyde anlamlı bir ilişki bulunmuştur ($r = .092, p = .029$). Ayrıca, günlük internet kullanım süresiyle sanal mağduriyet arasında pozitif yönde düşük düzeyde ve anlamlı bir ilişki elde edilmiştir ($r = .163, p < .01$). Bu bulgular, günlük

internet kullanım süresi arttıkça öğrencilerin sanal zorbalık yapma ve sanal mağduriyet yaşama düzeylerinin de hafif düzeyde arttığını göstermektedir.

Buna karşılık, günlük internet kullanım süresiyle çevrim içi mahremiyet toplam puanı ($r = -.031, p = .466$), dikkat alt boyutu ($r = .016, p = .713$) ve iletişim & paylaşım alt boyutu ($r = -.010, p = .809$) arasında anlamlı bir ilişki bulunmamıştır ($p > .05$). Bununla birlikte, güvenlik alt boyutuyla günlük internet kullanım süresi arasındaki ilişkinin negatif yönde ve düşük düzeyde anlamlı olduğu görülmüştür ($r = -.083, p = .048$). Bu sonuç, günlük internet kullanım süresi arttıkça öğrencilerin güvenlik boyutuna ilişkin farkındalıklarının çok düşük düzeyde azaldığına işaret etmektedir.

Tablo 3.17 Üniversite Öğrencilerinin Günlük İnternet Kullanım Süreleri ile Sanal Zorbalık, Sanal Mağduriyet, Çevrim İçi Mahremiyet Farkındalık Genel ve Alt Boyut Puanları Arasındaki İlişki

Ölçek	Günlük İnternet Kullanım Süresi	
	r	p
Siber Zorbalık	.092*	.029
Siber Mağduriyet	.163**	.000
Çevrim İçi Mahremiyet	-.031	.466
Dikkat	.016	.713
Güvenlik	-.083	.048
İletişim & Paylaşım	-.010	.809

* $p < .05$; ** $p < .01$; r : Spearman ve Pearson korelasyon katsayısı

Pallant (2017)'ye göre r değerlerinin .10'un altında olması çok zayıf ilişki düzeyine karşılık gelmektedir. Bu bağlamda elde edilen anlamlı ilişkilerin yönü pozitif ya da negatif olmakla birlikte, güç düzeyi düşük bulunmuştur.

3.3.6.3. Üniversite Öğrencilerinin Akademik İnternet Kullanım ile Sanal Zorbalık, Sanal Mağduriyet, Çevrim İçi Mahremiyet Farkındalık Genel ve Alt Boyut Puanları Arasındaki İlişki

Tablo 3.18 incelendiğinde, üniversite öğrencilerinin akademik internet kullanım süreleri ile sanal zorbalık, sanal mağduriyet ve çevrim içi mahremiyet farkındalık toplam ve alt boyut puanları arasındaki ilişkiler sunulmuştur. Bulgulara göre, öğrencilerin akademik internet kullanımı süresiyle sanal mağduriyet puanları arasında pozitif yönlü, düşük düzeyde ve anlamlı bir ilişki saptanmıştır ($r = .110, p = .009, p < .01$). Bu sonuç, akademik internet kullanımı arttıkça öğrencilerin sanal mağduriyet deneyimlerinin hafif düzeyde artabileceğini göstermektedir.

Buna karşılık, akademik internet kullanımı süresiyle sanal zorbalık toplam puanı ($r = -.049, p = .246$), çevrim içi mahremiyet toplam puanı ($r = .036, p = .389$), dikkat alt boyutu ($r = .013, p = .762$), güvenlik alt boyutu ($r = .005, p = .910$) ve iletişim & paylaşım alt boyutu ($r =$

.074, $p = .078$) arasında anlamlı bir ilişki bulunmamıştır ($p > .05$). Dolayısıyla, akademik internet kullanımı değişkeninin bu boyutlarla istatistiksel açıdan önemli bir bağlantısının olmadığı görülmektedir

Tablo 3.18 Üniversite Öğrencilerinin Akademik İnternet Kullanım Süreleri ile Sanal Zorbalık, Sanal Mağduriyet, Çevrim İçi Mahremiyet Farkındalık Genel ve Alt Boyut Puanları Arasındaki İlişki

Ölçek	Akademik İnternet Kullanım Süresi	
	r	p
Siber Zorbalık	-.049	.246
Siber Mağduriyet	.110**	.009
Çevrim İçi Mahremiyet	.036	.389
Dikkat	.013	.762
Güvenlik	.005	.910
İletişim & Paylaşım	.074	.078

* $p < .05$; ** $p < .01$; r: Spearman ve Pearson korelasyon katsayısı

3.3.6.4. Üniversite Öğrencilerinin Sosyal Medya Kullanım Süreleri ile Sanal Zorbalık, Sanal mağduriyet, Çevrim İçi Mahremiyet Farkındalık Genel ve Alt Boyut Puanları Arasındaki İlişki

Tablo 3.19 incelendiğinde, üniversite öğrencilerinin sosyal medya kullanım süreleriyle sanal zorbalık, sanal mağduriyet ve çevrim içi mahremiyet farkındalık toplam ve alt boyut puanları arasındaki ilişkilere yer verilmiştir. Bulgulara göre, öğrencilerin sosyal medya kullanım süresiyle sanal zorbalık ($r = .113$, $p = .007$, $p < .01$) ve sanal mağduriyet ($r = .115$, $p = .006$, $p < .01$) toplam puanları arasında pozitif yönlü, düşük düzeyde ve anlamlı ilişkiler saptanmıştır. Bu sonuç, sosyal medya kullanımı arttıkça öğrencilerin sanal zorbalık ve sanal mağduriyet deneyimlerinin de hafif düzeyde artabileceğini göstermektedir.

Çevrim içi mahremiyet toplam puanı ile sosyal medya kullanım süresi arasında ise negatif yönlü, düşük düzeyde ve anlamlı bir ilişki bulunmuştur ($r = -.104$, $p = .014$, $p < .05$). Bu bulgu, sosyal medya kullanımı arttıkça öğrencilerin çevrim içi mahremiyet farkındalıklarının hafif düzeyde azalabileceğini ortaya koymaktadır. Alt boyutlar incelendiğinde, güvenlik alt boyutu ($r = -.122$, $p = .004$, $p < .01$) ile sosyal medya kullanımı arasında negatif yönlü, düşük düzeyde anlamlı bir ilişki bulunurken, dikkat ($r = -.064$, $p = .128$) ve iletişim & paylaşım ($r = -.045$, $p = .289$) alt boyutlarında anlamlı bir ilişkiye rastlanmamıştır ($p > .05$).

Tablo 3.19 Üniversite Öğrencilerinin Akademik İnternet Kullanım Süreleri ile Sanal Zorbalık, Sanal Mağduriyet, Çevrim İçi Mahremiyet Farkındalık Genel ve Alt Boyut Puanları Arasındaki İlişki

Ölçek	Sosyal Medya Kullanım Süresi	
	<i>r</i>	<i>p</i>
Siber Zorbalık	.113**	.007
Siber Mağduriyet	.115**	.006
Çevrim İçi Mahremiyet	-.104*	.014
Dikkat	-.064	.128
Güvenlik	-.122**	.004
İletişim & Paylaşım	-.045	.289

p* < .05; *p* < .01; *r*: Spearman ve Pearson korelasyon katsayısı

Pallant'a (2017) göre, .40'ın altındaki korelasyon katsayıları düşük düzeyde ilişkiyi gösterdiğinden, bu analizde elde edilen tüm anlamlı ilişkilerin yönlerinin pozitif ya da negatif olmasıyla birlikte düşük düzeyde olduğu söylenebilir.

3.4. Tartışma

Araştırma bulgularına göre, katılımcı üniversite öğrencilerinin çevrim içi mahremiyet farkındalıkları genel olarak orta düzeydedir. Ölçeğin alt boyutları dikkat, güvenlik, iletişim ve paylaşım düzeyleri de ortalamada seyretmektedir. Bu bulgu, öğrencilerin mahremiyet farkındalıklarının kendilerini çevrim içi mağduriyetten korumaya yetecek ölçüde olmadığını göstermektedir. Orta düzeydeki mahremiyet farkındalığı öğrencilerin çevrim içi riskler karşısında kısmen temkinli olsalar da bu risklere tam anlamıyla dikkat etmediklerini yansıtmaktadır. Benzer bulgular Gültekin'in (2024) gerçekleştirdiği çalışmada da görülmektedir. Bulgu, öğrencilerin kişisel verilerinin gizliliği konusunda belirli bir bilinç düzeyine sahip olduklarını ama bilincin mahremiyeti koruyabilecek tutarlı davranışlara tam yansımadığını göstermektedir. Özellikle dikkat ve güvenlik düzeyi ile iletişim ve paylaşım tercihlerinin ortalamada kalması; öğrencilerin hangi bilgileri, bilginin ne kadarını, kimlerle ve hangi amaç uğruna paylaşacakları konusunda tam anlamıyla farkındalık sahibi ya da kendini koruyabilir yetkinlikte olmadıklarını yansıtmaktadır.

Araştırmanın bu bulgusu Güçlendirme Kuramı açısından ele alındığında, öğrencilerin eleştirel bilinç, bilişsel güçlenme ve öz yeterlik konularında henüz tam anlamıyla güçlenemedikleri, bununla birlikte güçlenme potansiyellerinin olduğu ifade edilebilmektedir. Kuram bireylerin bilgi sahibi olmakla kalmayıp sahip oldukları bilgiyi eyleme dönüştürecek öz yeterlik- eleştirel güç ve çevresel desteklere de sahip olmalarını savunmaktadır (Kırlioğlu, 2019). Katılımcı üniversite öğrencilerinin mahremiyet farkındalıklarının davranışa dönüşmemesi; bu öğrencilerin çevrim içi ortamlarda kendi hak ve sınırlarını korumalarını sağlayacak öz-yeterliğe; gizlilik ihlalleri, kişisel verilerin kullanımı gibi yapısal tehditleri

sorgulayacak eleştirel bilince henüz tam anlamıyla ulaşamadıklarını göstermektedir. Bunlara ek olarak, orta düzey farkındalık, çevrim içi ortamlardaki davranışları konusunda öğrencilerin kendileri dışındaki unsurların etkisinde kaldığını göstermektedir. Okumuş ve Atılğan'ın (2021) araştırmalarına göre öğrencilerin çevrim içi ortamlarda karar alma otonomilerinin sınırlılığı; bu ortamlarda arkadaş baskıları, dijital çevrenin normları, platform ayarları ve oradaki çeşitli faktörlerin, sözelimi yorum yapabilmek için aktif paylaşım yapma şartı gibi zorlayıcı unsurların mahremiyet ihlaline yol açacak davranışlarına sebep olabildiği görülmektedir.

Güçlendirme Kuramı bağlamında bu bulgu ışığında, dijital alanlarda hala mahremiyet ihlallerine karşı riskli bir konumda olan üniversite öğrencilerinin güvende olabilmeleri, yani mahremiyetlerini riske atmayan dijital davranışlar sergileyebilmeleri için güçlenme sürecinin tamamlanmasının gerekli olduğu ifade edilebilir. Güçlenme ise ancak öğrencinin dijital ortamlarda haklarının bilincinde olup onlara sahip çıkabildiği, çevrim içi ortamlardaki risklerin doğasını, işleyiş biçimini anlayabildiği ve dijital ortamlardaki davranışlarının kendi kontrolünde olduğu durumlarda mümkün olabilmektedir (Öngören & Yılmaz, 2023).

Çalışmanın bulguları, sosyo-demografik değişkenlerin mahremiyet farkındalığı üzerinde etkili olduğunu açığa çıkarmaktadır.

Cinsiyet, öğrencilerin mahremiyet bilincine etki eden değişkenlerden biridir. Çalışma, cinsiyetin çevrim içi ortamlarda mahremiyet bilincini etkileyen bir değişken olup kadın öğrencilerin mahremiyet farkındalıklarının, özellikle de iletişim ve paylaşım süreçlerine dair farkındalıklarının erkek öğrencilerden daha yüksek olduğunu ortaya koymaktadır. Bir başka anlatımla kadınlar, dijital ortamlardaki ilişkilerinde mahremiyet sınırlarına daha çok özen göstermekte, paylaşımlarının ne kadarının kimlerce görülebileceği ve sonuçlarının ne olacağını daha çok sorgulamaktadır.

Çalışmanın bu bulgusu, kadın öğrencilerin dijital farkındalıklarının çevrim içi ortamlarda dijital mahremiyetlerini korumaya yönelik davranışlara yansıdığını ortaya koyan (De Wolf, 2019; Topbaş & Gazi, 2016; Töngel, 2020) çalışma bulgularıyla paralellik göstermektedir. Kadınların erkeklere göre daha yüksek mahremiyet bilincine sahip oldukları bulgusu, ilk bakışta kadınların dijital alanlarda daha güçlü, daha özgür olduklarını düşündürülebilir. Ne var ki Stevens ve arkadaşlarının (2024) gerçekleştirdiği çalışmada ulaşılan bulgulara göre cinsiyetler arasındaki bu farklılık, kadınların güçlenmelerinin bir göstergesinden ziyade dijital alanlarda erkeklerden daha çok korunmalarını gerektiren toplumsal cinsiyet normlarından kaynaklandığını gözler önüne sermektedir. Toplumsal cinsiyet normları, tıpkı çevrim dışı alanlarda olduğu gibi çevrim içi alanlarda da erkekleri egemen olarak konumlandırırken (Tutgun Ünal & Tarhan, 2022) kadınları ise denetlenebilir, sınırlandırılabilir

ve teşhir edilebilir bedenler olarak (Atalay, 2020) mahremiyet ihlallerine açık hale getirebilmektedir. Bu bakımdan da kadın öğrenciler erkek egemen çevrim içi alanlarda mahremiyet ihlallerini sıklıkla deneyimleyebilmektedirler. Bu olumsuz deneyimler, literatürde de vurgulanmış olduğu gibi, örneğin Topbaş ve Gazi'nin (2016) yaptığı araştırmada olduğu gibi, bu deneyimden “ders” çıkaran kadın öğrencilerin mahremiyete daha fazla önem verme yönünde bir korunma stratejisi geliştirmeleri eğilimde olmaları ihtimalinden söz edilebilmektedir. Bu bağlamda bu bulgunun, kadın öğrencilerin dijital alanlarda daha güçlü değil bilakis güçlenemediği bir durumu yansıttığı ifade edilebilmektedir.

Yaş pek çok çalışmada mahremiyet farkındalığına etki eden önemli bir değişken olmakla birlikte bu çalışmada üniversite öğrencilerinin yaşı ile çevrim içi mahremiyet farkındalıkları arasında anlamlı bir ilişki bulunmamıştır. Bu bulgu, mevcut literatürü desteklememektedir. Zira alan yazında yaş ve çevrim içi mahremiyet arasında anlamlı bir ilişki olduğunu ortaya koyan çalışmalar yoğunluktadır (Karadaş & Kara, 2021; Yüksel & Kaplan, 2021). Literatürde dijital mahremiyet farkındalığına ilişkin çalışmalar genellikle belli yaş gruplarıyla (ortaokul öğrencileri, lise öğrencileri, ergenler) yürütülmektedir. Bu durum söz konusu çalışmalarda yaş etkisinin sınırlı olmasına sebep olabilmektedir. Zira Özer, Çelik ve Özatl'nın (2021) araştırmasında görüldüğü üzere homojen yaş dağılımı, yaşa bağlı deneyim farklılıklarının ortaya konulmasını engelleyebilmektedir. Nitekim bu çalışmanın örneklemini oluşturan üniversite öğrencilerinin yaş aralığı geniş görünmekle birlikte (17-55) dağılım 20'li yaşlarda yoğunlaşmaktadır. Oysa 17 yaşındaki birey ile 55 yaşındaki bireyin dijital ortamlardaki deneyimlerinin birbirlerinden oldukça farklı olması beklenmektedir.

Örneklemin yaş bakımından homojen olması dışında katılımcılarının üniversite öğrencileri olması da alan yazındaki bulgularla çelişen sonuçların ortaya çıkmasında etkili görünmektedir. Bu çalışmada yaş ile dijital mahremiyet arasında ilişki saptanamaması, örneklemin kimlik oluşumu, sosyal beceriler ve bilişsel gelişim bakımından görece daha istikrarlı bir evre olan genç yetişkinlik döneminde (Senemoğlu, 2020) olmalarıyla ilişkilendirilebilir. Hızlı gelişimsel değişimler yaşayan lise veya ortaokul çağındaki öğrenciler (Senemoğlu, 2020) arasındaki birkaç yıllık yaş farkı, bilişsel ve sosyal gelişim açısından büyük değişimler yaratacağından bu yaşlardaki öğrencilerin mahremiyet bilinci üzerinde anlamlı bir fark yaratabilmektedir. Diğer taraftan bu yaş farkı, gelişimsel dönemlerini görece tamamlamış olan üniversite öğrencilerinin dijital davranışları üzerinde anlamlı bir fark yaratmayacaktır. Bu bakımdan da bu çalışmanın yaşı mahremiyet farkındalığına etkisi bağlamındaki bulgularının hızlı gelişimsel özelliklerin sergilendiği dönemlerinde olan öğrencilerle yürütülen çalışmalarla çatışan sonuçlar ortaya koyması beklenebilir.

Alan yazında eğitim düzeyi, mahremiyet farkındalığına etki eden bir değişken olarak değerlendirilmektedir. Bununla birlikte bu çalışmanın genel bulgularında üniversite öğrencilerinin sınıf düzeyi ile mahremiyet farkındalıkları arasında anlamlı bir ilişki bulunmamıştır. Sadece mahremiyetin alt boyutu olan iletişim ve paylaşım konusunda 1. Sınıf öğrencilerinin diğer öğrencilere kıyasla daha yüksek bir farkındalık seviyesine sahip olduğu anlaşılmıştır. Bu bulgu, üniversiteye gitmek için belki de ilk kez aile ortamından ayrılan öğrencilerin bireysel yaşam kurdukları bir dönemde (Doğru Çabuker & Balcı Çelik, 2019) çevrim dışı alanda olduğu gibi çevrim içi alanda da mahremiyetlerini korumaya yönelik daha kontrollü davrandıkları şeklinde yorumlanabilmektedir. Öğrencilerin bireysel sorumluluklarının arttığı yeni bir hayata geçiş evresinde, çevrim içi alanlardaki paylaşım ve iletişim süreçlerinde daha dikkatli olmaları, bu alt boyutlardaki farkındalık düzeyinin yüksek olmasına katkı sağlamış olabilmektedir.

1. sınıf düzeyinde iletişim ve paylaşım boyutlarında daha yüksek bir farkındalık sergilenmesinin bir diğer olası nedeni, bu öğrencilerin hala ebeveynlerinin denetiminin etkisinde kalmaları olabilmektedir. Zira ailelerinden yeni ayrılmış olan 1. sınıf öğrencileri hala aile ortamındaki içselleştirilmiş ebeveyn alışkanlıklarını sürdürüyor ve dijital ortamlarda ebeveynlerinin dolaylı kontrolüne uygun davranıyor olabilmektedirler. Aile denetiminden uzaklaştıkça, içselleştirilmiş denetimin etkisini yitirmesiyle mahremiyet davranışlarında esnemeler ortaya çıkabilmektedir.

Eğitim düzeyine ilişkin genel tablo, sınıf düzeyi arttıkça mahremiyet bilincinin beklenir bir şekilde artmadığını yansıtmaktadır. Bu durum, üniversitelerde öğrencilerin mahremiyet bilincini sınıf bazında etkileyecek bir eğitim içeriğinin mevcut olmadığını, mevcut eğitimin öğrencilerin dijital ortamlarda güvenlik- öz yeterlik ve kontrol davranışlarına etki edecek çıktılar sağlamadığını düşündürmektedir. Daha yalın bir anlatımla, öğrenciler eğitim hayatları boyunca benzer dijital bilgelere erişebildiklerinden sınıf düzeyinin bu çalışmada tek başına belirleyici bir değişken olmadığı anlaşılmaktadır.

Sınıf düzeyi bazında dijital mahremiyet bilincinin farklılaşmadığına ilişkin bulgu, bireyleri güçlendirme potansiyeline sahip olan eğitimin mevcut haliyle üniversite öğrencilerinin dijital mahremiyet konusunda güçlendirmede yansıtmaktadır. Bilgiyi edinmek kadar bu bilgiyi eyleme dönüştürmenin de güçlenmenin koşulu olduğunu savunan Güçlendirme Kuramı (Cankurtaran, Akoğlu & Sakarya, 2020) bağlamında ele alındığında sınıf düzeyleri yükseldikçe öğrencilerin artan farkındalıklarını davranışa dönüştürme kapasitelerinin artması ve böylelikle dijital alanlarda daha güçlü hale gelmeleri beklenmektedir. Ancak bu türden bir ilişkinin

bulunmadığını yansıtan bu bulgu, öğrencilerin aldıkları eğitimin dijital alanlarda daha güçlü konumlanmalarına işlevsel katkısını sorgulamayı gerektirmektedir.

Çalışmanın bulguları, öğrencilerin internet kullanım alışkanlıklarının da mahremiyet farkındalığı üzerinde etkili olduğunu yansıtmaktadır. Sosyal medya kullanım süresi, öğrencilerin mahremiyet bilinçlerine etki eden önemli bir değişkendir. Çalışma, öğrencilerin sosyal medyada geçirdikleri süredeki artışın mahremiyet bilincine zarar verdiğini ya da korunmaya yönelik davranışlarda esnekliğe sebep olduğunu ortaya koymuştur. Yani sosyal medya kullanım süresinin artması, öğrencilerin mahremiyet sınırlarını bulanıklaştırabilmekte, mahremiyet bilincini davranışa dönüştürme kapasitelerine zarar verebilmektedir. Sosyal medya kullanım süresinin artması, dijital mahremiyeti tüm boyutlarıyla (güvenlik, dikkat, paylaşım ve iletişim) etkilemekte ve öğrencilerin mahremiyet sınırlarını koruma konusundaki özenli tutumlarının değişmesine sebep olabilmektedir.

İnternette ve sosyal medyada geçirilen süre, özellikle düzenli şifre değişimi, tarayıcı geçmişlerinin düzenli temizliği, uygulama izinlerini kontrol etme gibi güvenlik odaklı mahremiyet davranışlarını olumsuz etkilemektedir. İnternet kullanımı süresi ile mahremiyet farkındalığı arasındaki negatif ilişkiye dair mevcut literatürü (Öz, 2014; Korucu & Gürkez, 2019; Tatlıoğlu & Gülcan, 2025) destekleyen bu bulgular, Güçlendirme Kuramı bağlamında ele alındığında, dijital alanların yoğun ve aktif kullanımının bilinçli kullanım avantajı sağlamadığı, hatta bu ortamlardaki tehditlere açık konumu güçlendirebildiği dile getirilebilmektedir. Zira bireyin dijital ortamdaki gücü, o ortama aktif katılımıyla ilişkili değildir; o ortamdaki öz yeterlik, sorgulama ve kontrol kapasitesiyle ilişkilidir (Akkoyunlu & Yılmaz, 2011; Çevik Tekin, Erdoğan & Şanlı, 2021). Daha yalın bir anlatımla, bireyin dijital alanlarda güçlü olması, içinde yer aldığı dijital ortamı sorgulayabilen, kendini koruyabilen, kendisinin ve kendisi dışındakilerin davranışlarını denetleyebilen bir bilinçle hareket etmesine bağlıdır. Aksine, bu bulgu, uzun süreli kullanımın öğrencilerin ihmalkâr davranışlarını artırdığını ortaya koymaktadır. Bu bakımdan çevrim içi alanlarda daha fazla yer alan üniversite öğrencileri için yoğun dijital varlığın güçlenmeden ziyade kırılganlık ile ilişkili olduğu ifade edilebilmektedir.

Araştırmada öğrencilerin siber zorbalık ve siber mağduriyet düzeylerine ilişkin dikkat çekici bulgular elde edilmiştir. Bu bulgulardan biri, üniversite öğrencileri arasındaki düşük siber zorbalık ve siber mağduriyet düzeyidir. Bu durumun olası birkaç nedeni vardır; üniversite öğrencileri çevrim içi alanlarda daha güvenli deneyimlere sahip olabilmektedirler. Yani öğrenciler çevrim içi alanlarda az şiddet içeren, karşılıklı haklara saygılı bir iletişim ortamında yer alıyor olabilmektedirler. Ayrıca öğrencilerin yaşadığı zorbalığı normalleştirmiş, fark

etmemiş ya da ifadeden kaçınıyor olmasından da başka bir neden olarak söz edilebilmektedir. Zorbalık davranışlarının “şaka” olarak kabul edildiği, mağduriyetin küçümsendiği, hatta mağdurun mızızlık yapıyor olmakla suçlanabildiği bir kültürel bağlamda öğrenciler mağduriyeti normalleştirme ya da dile getirmeme yönünde bir eğilim sergiliyor olabilmektedirler. Yaman ve Peker’in (2012) yaptığı çalışma incelendiğinde de bunun literatür ile paralel olduğu görülmektedir. Bu çalışmaya göre öğrenciler zorbalığı bir eğlence ve şaka aracı olarak görebilmekte ve bunu normalleştirebilmektedirler.

Öğrencilerin düşük düzeyde görünür olan siber zorbalık ve siber mağduriyet deneyimlerinin cinsiyet, internette geçirilen süre, mahremiyet farkındalığı gibi değişkenlerden etkilendiği anlaşılmıştır. Alan yazındaki Karakuş ve Turan’ın (2022) yaptıkları araştırma, bu çalışmadaki sonuçları destekler biçimdedir. Bu çalışmada da cinsiyetin siber zorbalık davranışlarına etki eden bir değişken olduğu ve erkeklerin dijital ortamlarda kadınlara kıyasla daha fazla dijital zorbalık davranışları sergileme eğiliminde olduğu ortaya konulmuştur. Bu durum, sertlik, öfke ve saldırganlık gibi davranış modellerini erkek cinsiyetine atfeden toplumsal cinsiyet rollerine dair evrensel normlarla açıklanabilmektedir (Sallan Gül & Altındal, 2015; Weaver vd., 2010). Erkek öğrencileri arasındaki nispeten yüksek siber zorbalık eğilimi, bu öğrencilerin çevrim içi ortamlarda etkileşim içinde oldukları bireylerin haklarını ihlal etme potansiyeline sahip olduğunu göstermektedir. Tam güçlenmenin salt savunma becerileri geliştirmekle kalmayıp başkalarına karşı da sorumlu davranışlar sergilemekle mümkün olduğu (Erbay, 2019) dikkate alındığında, özellikle erkek öğrenciler için başkalarına zarar verecek davranışlardan kaçınmalarını sağlayacak bilincin geliştirilmesi gerekliliği ortaya çıkmaktadır.

Bulgular, siber zorbalığın günlük ve sosyal amaçlı internet kullanımı ile pozitif ilişkili olduğunu ortaya koymaktadır. Bu bulgu Yenilmez ve Seferoğlu (2013) ile Koçak ve meslektaşlarının (2024) yapmış olduğu çalışmaların sonuçlarıyla örtüşmektedir. Siber mağduriyet ise sosyal, akademik ve de genel kullanım süreleriyle ilişkilidir. Başka bir anlatımla internette geçirilen süre ister akademik ister sosyal nedenlerle uzun olsun fark etmeksizin sürenin uzaması, siber mağduriyet düzeyini artırmaktadır. Bu bulgu, siber zorbalık davranışlarının yoğunluklu olarak sosyal medya gibi etkileşimli ortamlarda ortaya çıktığını (Tan & Şenkal, 2024); siber mağduriyetin ise sosyal platformlarla sınırlı kalmayarak akademik dijital ortamlarda dahi yaşanabildiğini göstermektedir. Akademik amaçlı kullanımın dahi mağduriyetle ilişkili olması, öğrencilerin çevrim içi alanlardaki görünürlüklerinin ve iletişim sıklıklarının artmasının, başlı başına bir risk faktörü haline gelebildiğine işaret etmektedir. Bu bulgudan hareketle üniversite öğrencilerinin güçlenme süreçlerinin tam anlamıyla işleyebilmesi için yalnızca sosyal medya platformlarında değil etkileşimin olduğu tüm çevrim içi

platformlarda potansiyel riskleri öngörüp bunlardan kendilerini koruyabilmeleri gerektiği belirtilebilmektedir.

Mahremiyet farkındalığı, öğrencilerin siber mağduriyet-zorbalık deneyimleri üzerinde etkili olan bir diğer değişkendir. Öğrencilerin özellikle iletişim ve paylaşım boyutlarında artan çevrim içi mahremiyet farkındalıklarının siber mağduriyet yaşama olasılıklarını düşürdüğü anlaşılmıştır. Bu bulgu, dijital ortamlarda etkileşim içinde oldukları bireylerden hangileriyle, neyi, ne oranda paylaşacakları hususunda kontrolleri yüksek olan öğrencilerin mahremiyet bilincinin de yüksek olduğunu ve bu sayede de çevrim içi alanlarda daha güvenli konumlandıklarını yansıtmaktadır. Mahremiyet konusunda bilinç kazanan öğrencilerin haklarını koruyabilme, riskleri öngörüp eyleme geçebilme eğilimlerini artırdığını yansıtan bu bulgu, Güçlendirme Kuramı'nın temel varsayımıyla örtüşmektedir: Güçlenme, haklarının bilincinde olmak değil; bu bilinci davranışa yansıtmaktır (Yıldırım, 2014). Bu bağlamda öğrencilerin dijital alanlarda güçlenmeleri ve güvenli bir konumda olmaları için, mahremiyeti bilincinin gelişmesi, temel bir adımdır. Dijital sınırlarını tanınmasını, koruyucu davranışlar geliştirilip mağduriyet riskine karşı önleyici tutumların sergilemesini bu bilinç mümkün kılmaktadır.

Mahremiyet farkındalığı, siber zorbalık davranışlarında da etkili bir değişkendir. Mahremiyet farkındalığı yüksek olanların siber mağduriyet yaşama olasılıkları düştüğü gibi, siber zorbalık davranışları sergileme eğilimleri de düşmektedir. Çalışma, güvenlik ile iletişim ve paylaşım konularında mahremiyet bilincine sahip olan öğrencilerin siber zorbalık oranlarının daha düşük olduğunu ortaya koymaktadır. Öte yandan mahremiyetin bir alt boyutu olan dikkat, siber zorbalık davranışlarına etki eden bir değişken değildir. Yani çevrim içi ortamlardaki dikkatli internet kullanımları, öğrencilerin zorbalık davranışlarına etki etmemektedir. Mahremiyet farkındalığının dikkat alt boyutu, daha çok bireysel güvenlik önlemleriyle ilişkilidir. Şüphe duyulan linke tıklamamaya, yabancı kişilerle kişisel bilgileri paylaşmamaya özen göstermek türünden davranışlar öğrencilerin kendi güvenlikleriyle ilişkilidir. Siber zorbalık ise öğrencilerin çevrim içi alanlarda kendi mahremiyetleri konusundaki dikkatleri ile ilişkili olmayıp, diğerlerine nasıl davrandığıyla alakalıdır (Kaygısız, 2020). Yani, öğrencilerin kendi mahremiyetine özen gösteriyor olması, başkalarının haklarını da gözeten sorumluluk sahibi dijital vatandaşlar gibi davranacakları anlamına gelmeyebilmektedir.

Diğer taraftan iletişim ve paylaşım ile güvenlik alt boyutlarındaki mahremiyet farkındalığı, siber zorbalık davranışlarının ortaya çıkmasını etkilemektedir. Yani güvenlik bilinci olan ve hangi dijital sınırlar içinde etkileşim kuracağını bilen öğrencilerin, kendi sınırları kadar diğerlerinin de sınırlarına saygı gösterdikleri için zorbalık davranışları

sergilememektedir. Öztürk ve meslektaşlarının (Öztürk, Eyüboğlu & Göçmen Baykara, 2022) yaptığı çalışmada da buna benzer bulgulara rastlanmaktadır, ancak bu çalışmaya göre gençlerin başkalarının mahremiyetini koruma konusunda biraz daha geliştirilmeleri gerektiği vurgulanmaktadır. Ayrıca bu araştırma sonucunda elde edilen bulgular, Çubukcu ve Bayzan'ın (2013) gerçekleştirdiği çalışma, güvenlik ve iletişim bilincinin öğrencinin çevrim içi alanlardaki davranışlarını etik sınırlar içinde biçimlendirdiğini göstermektedir.

Mahremiyet farkındalığının alt boyutlarının siber zorbalıkla ilişkisini ortaya koyan çalışmanın bu bulguları Güçlenme Kuramı bağlamında ele alındığında dikkat çekici bir gerçek ortaya çıkmaktadır. Öğrencilerin sadece kendi güvenlikleri konusunda dikkatli davranışlar sergilemeleri, kişisel güçlenmenin önemli bileşenlerinden biridir (Kırlıoğlu, 2019). Ancak bu tek başına yeterli değildir. Çünkü tam bir güçlenmeden bahsedebilmek için kendisi için hak talep ettiği gibi başkalarının haklarının da savunucusu olmak, onların sınırlarına duyarlı yurttaşlar olmak gerekmektedir (Erbay, 2019).

Siber zorbalık ve mağduriyet düşük seviyede görünmüş olsa da siber zorbalık ve siber mağduriyet arasındaki güçlü pozitif ilişki, dikkat çekicidir. Bu bulgu, bir üniversite öğrencisinin siber zorbalık davranışlarını sergilediği oranda siber mağduriyet yaşama olasılığının da arttığını yansıtmaktadır. Veya tam tersi, siber mağduriyet yaşayan bir üniversite öğrencisinin zorbalık davranışı sergileme riskinin de arttığına işaret etmektedir. Diğer çalışmalarda da (Uçar, 2015; Bakan, 2019; Kalafat Çat & Aydın Aydoğan, 2023) görüldüğü gibi bu bulgu çevrim içi ortamlardaki rol geçişkenliğinin varlığını ortaya koymaktadır. Çevrim içi ortamlarda öğrencilerin rolleri sabit kalmamakta; aynı öğrenci yaptığı bir paylaşım nedeniyle mağdur konumunda bulunurken, başka bir içerikte başkalarına zorbalık davranışları sergileyebilmektedir. Üniversite öğrencilerinin dijital ortamlarda fail/mağdur rollerinin geçişken bir yapıda olduğuna dair bu bulgu, Güçlendirme Kuramı bağlamında değerlendirildiğinde, öğrencilerin yalnızca mağduriyete ilişkin deneyimlerine odaklanmanın sakıncalarını gözler önüne sermektedir. Zira Güçlendirme Kuramı yalnızca bireyin kendi haklarını bilip korumasını değil, başkalarının haklarına da aynı ölçüde duyarlı olmasını savunmaktadır (Cankurtaran, Akoğlu & Sakarya, 2020). Kuramın temel varsayımlarından hareketle, öğrencilerin çevrim içi alanlarda tam anlamıyla güçlenmeleri için bu alanlarda kendilerini mağdur konuma düşürmekten kaçınmaya dikkat ettikleri kadar, sorumluluk sahibi dijital vatandaşlar gibi davranmaları gerektiği belirtilebilmektedir.

SONUÇ

Bu araştırma, üniversite öğrencilerinin dijital mahremiyet farkındalık düzeyleri ile siber mağduriyet deneyimleri arasındaki ilişkiyi sosyal hizmet perspektifinden incelemeyi amaçlamıştır. Türkiye genelinde farklı coğrafi bölgelerdeki üniversitelerden toplam 560 lisans öğrencisinin katılımıyla gerçekleştirilen araştırmada, veri toplama aracı olarak Demografik Bilgi Formu, Çevrim İçi Mahremiyet Farkındalık Ölçeği (ÇMFÖ) ve Siber Zorbalık/Siber Mağduriyet Envanteri kullanılmıştır.

Araştırma bulguları, üniversite öğrencilerinin dijital ortamlarda karşılaştıkları risklerin özellikle mahremiyet farkındalığı ve mağduriyet düzeyi açısından dikkat çekici olduğunu ortaya koymuştur. Katılımcıların genel dijital mahremiyet farkındalık düzeyi orta düzeyde belirlenmiş; özellikle iletişim ve paylaşım alt boyutlarında farkındalığın daha düşük olduğu saptanmıştır. Bu durum, öğrencilerin çevrim içi ortamlarda kişisel bilgilerini koruma ve bilinçli etkileşim kurma konularında yeterince donanımlı olmadıklarını göstermektedir.

Çalışmada siber zorbalık düzeyleri düşük bulunmuş olsa da öğrencilerin önemli bir kısmının siber mağduriyet deneyimi yaşadığı tespit edilmiştir. Bu durum, öğrencilerin dijital ortamda daha çok mağdur konumunda yer aldıklarını ve bu alanda savunmasız kaldıklarını ortaya koymaktadır. Demografik değişkenler doğrultusunda elde edilen bulgular ise, dijital mahremiyet farkındalığının cinsiyet ve sınıf düzeyine göre anlamlı farklılıklar gösterdiğini ortaya koymuştur. Kadın öğrenciler, erkek öğrencilere kıyasla özellikle dikkat ve paylaşım boyutlarında daha yüksek farkındalık düzeyine sahiptir. Ancak bu durum, kadın öğrencilerin dijital ortamlarda daha bilinçli olduklarından değil; çevrim dışı ortamlarda olduğu gibi çevrim içi mecralarda da daha sık taciz ve zorbalık tehdidiyle karşılaşmaları nedeniyle, daha temkinli davranmak zorunda kaldıklarını düşündürmektedir.

Sınıf düzeyi açısından yapılan değerlendirmelerde, dördüncü sınıf öğrencilerinin siber zorbalık ve mağduriyet düzeylerinin daha yüksek olduğu belirlenmiştir. Bu bulgu, üniversite eğitimi ilerledikçe öğrencilerin dijital ortamlardaki etkileşimlerinin arttığını ve bunun beraberinde riskleri de artırdığını düşündürmektedir. Buna karşılık, birinci sınıf öğrencilerinin iletişim ve paylaşım boyutlarında daha yüksek mahremiyet farkındalığına sahip olması, üniversiteye yeni başlayan bireylerin daha temkinli bir dijital davranış örüntüsüne sahip olabileceğini göstermektedir.

Ayrıca, internet kullanım süresi arttıkça özellikle güvenlik boyutundaki farkındalık düzeyinde düşüş yaşandığı tespit edilmiştir. Bu durum, dijital araçların yoğun kullanımının

farkındalığı otomatik olarak artırmadığını, aksine bazı güvenlik alışkanlıklarında zayıflamalara neden olabileceğini ortaya koymaktadır.

Elde edilen bulgular, öğrencilerin dijital ortamlarda karşılaştıkları siber risklerle başa çıkmada yalnızca bireysel farkındalıklarının yeterli olmadığını göstermektedir. Özellikle iletişim ve paylaşım alanlarında düşük farkındalık düzeyleri, öğrencilerin kendilerini çevrim içi tehditlere karşı koruma konusunda yetersiz kaldığını göstermektedir. Bu bağlamda, dijital mahremiyetin yalnızca bireysel bir sorumluluk alanı değil; aynı zamanda toplumsal ve yapısal desteklerle güçlendirilmesi gereken çok katmanlı bir alan olduğu ortaya çıkmaktadır.

Bu noktada, çalışmanın kuramsal dayanağını oluşturan Güçlendirme Kuramı önem kazanmaktadır. Güçlendirme yaklaşımı, bireyin yalnızca bilgi sahibi olmasıyla yetinmeyip, bu bilgiyi etkin biçimde kullanabilmesi, çevresel desteklerden yararlanabilmesi ve haklarını talep edebilecek sosyal koşullara erişebilmesi gerektiğini vurgular. Dolayısıyla bireyin dijital ortamda kendini koruyabilmesi için çok boyutlu bir destek sistemiyle donatılması gerekmektedir.

Bu doğrultuda hem uygulamaya hem de gelecekteki akademik çalışmalara yönelik öneriler şu şekilde sıralanabilir:

Dijital mahremiyet farkındalığı konusu, literatürde sınırlı sayıda çalışmaya konu olmuştur. Ancak dijitalleşen toplum bağlamında bu kavramın bireysel güvenlik, psikolojik iyi oluş ve toplumsal bilinç açısından taşıdığı önem dikkate alınarak, bu alanda daha fazla bilimsel çalışma yapılmalıdır.

Farklı yaş ve meslek gruplarındaki bireylerin dijital mahremiyet farkındalıklarının karşılaştırmalı biçimde incelendiği disiplinlerarası araştırmalar teşvik edilmelidir.

Sosyal hizmet eğitimi kapsamında dijital mahremiyet, siber zorbalık ve siber mağduriyet konularına yer verilmeli; bu alanlara ilişkin özgün ders içerikleri ve uygulama modülleri geliştirilmelidir.

İlköğretimden üniversiteye kadar tüm eğitim kademelerinde dijital mahremiyet ve güvenlik konularında farkındalık artırıcı müfredat düzenlemeleri yapılmalıdır.

Dijital mahremiyet yalnızca bireysel değil; toplumsal düzeyde korunması gereken bir hak olarak ele alınmalı; bu çerçevede yasa yapıcılar ve politika geliştiriciler için yol gösterici ulusal stratejiler oluşturulmalıdır.

Toplumsal farklı kesimlerine yönelik olarak çeşitli iletişim araçları (video, broşür, sosyal medya kampanyaları vb.) aracılığıyla dijital mahremiyet, siber zorbalık ve siber mağduriyet konularında yaygın bilinçlendirme çalışmaları yürütülmelidir.

Rehber öğretmenler, sosyal hizmet uzmanları ve gençlik çalışanları, dijital riskler konusunda gençleri güçlendirecek programlarla desteklenmelidir.

Güçlendirme kuramı doğrultusunda, çevrim içi ortamlarda bireyin kendini koruyabilme kapasitesini artırmaya yönelik yeni sosyal hizmet modelleri geliştirilmelidir.

Gelecek çalışmalarda, nitel yöntemlerle bireylerin dijital deneyimlerine ve mahremiyet algılarına daha derinlemesine bakılması önerilmektedir. Ayrıca sınıf düzeyi, fakülte türü, sosyoekonomik durum gibi değişkenlerin daha ayrıntılı biçimde incelenmesi, çalışmanın genellenebilirliğini artıracaktır.



KAYNAKÇA

- Abaido, G. M. (2020). Cyberbullying On Social Media Platforms Among University Students in the United Arab Emirates. *International Journal Of Adolescence and Youth*, 25(1), s. 407-420. doi:<https://doi.org/10.1080/02673843.2019.1669059>
- Agosto, D. E., & Abbas, J. (2017). “Don’t Be Dumb-That’s the Rule I Try to Live by”: A Closer Look at Older Teens’ Online Privacy and Safety Attitudes. *New Media & Society*, 19(3), s. 347-365.
- Agustina, J. R. (2015). Understanding Cyber Victimization: Digital Architectures and the Disinhibition Effect. *International Journal of Cyber Criminology*, 9(1), s. 35-54. doi:<https://doi.org/10.5281/zenodo.22239>
- Ahmedi, E. Ş. (2023). Mahremiyet, Dindarlık ve Sosyal Medya Bağımlılığı Üzerine Sosyolojik Bir Araştırma. *Medya ve Din Çalışmaları Dergisi*, 6(1), s. 25-46.
- Akkoyunlu, B., & Yılmaz, A. (2011). Prospective Teachers' Digital Empowerment and Their Information Literacy Self-Efficacy. *Eurasian Journal of Educational Research*, 11(44), s. 33-50.
- Al Qudah, M. F., Al-Barashdi, H. S., Hassan, E. M., Albursan, I. S., Heilat, M. Q., Bakhiet, S. F., & Al-Khadher, M. A. (2020). Psychological Security, Psychological Loneliness, and Age as the Predictors of Cyber-Bullying Among University Students. *Community Mental Health Journal*, 56(3), s. 393-403. doi:<https://doi.org/10.1007/s10597-019-00455-z>
- Al-Garadi, M. A., Hussain, M. R., Khan, N., Murtaza, G., Nweke, H. F., Ali, I., . . . Gani, A. (2019). Predicting Cyberbullying on Social Media in the Big Data Era Using Machine Learning Algorithms: Review of Literature and Open Challenges. *IEEE Access*, 7, s. 70701-70718. doi:<https://doi.org/10.1109/ACCESS.2019.2918354>
- Altıntaş Var, S. (2022). Sosyal Medyada Mahremiyet Farkındalığı: Hitit Üniversitesi Örneği. *Yayınlanmış Yüksek Lisans Tezi*. Hitit Üniversitesi.
- Alvarez-Garcia, D., Nunez, J. C., Gozalez-Castro, P., Rodriguez, C., & Cerezo, R. (2019). The Effect of Parental Control on Cyber-Victimization in Adolescence: The Mediating Role of Impulsivity and High-Risk Behaviors. *10*, s. 1-7. doi:Frontiers in Psychology
- Aly, H., Liu, Y., Anaraky, R. G., Khan, S., Moses, N., Byrne, K. A., & Knijnenburg, B. (2024). Tailoring Digital Privacy Education Interventions for Older Adults: A Comparative Study on Modality Preferences and Effectiveness. *Proceedings on Privacy Enhancing Technologies*, 2024(1), s. 635-656. doi:<https://doi.org/10.56553/popets-2024-0036>

- Anuradha, K. (2004). Empowering Families with Mentally Ill Members: A Strengths Perspective. *International Journal for the Advancement of Counselling*, 26(4), s. 383-391.
- Arıca, O. T., Tanrikulu, T., & Kınay, H. (2012). Siber Mağduriyet Ölçeği'nin İlk Psikometrik Bulguları. *Akdeniz Eğitim Araştırmaları Dergisi*(11), s. 1-6.
- Aries, P., & Duby, G. (2007). *Özel Hayatın Tarihi 3: Rönesans'tan Aydınlanma'ya*. (D. Çetinkasap, Çev.) İstanbul: Yapı Kredi Yayınları.
- Askheim, O. P. (2003). Empowerment as Guidance For Professional Social Work: An Act of Balancing on a Slack Rope. *European Journal of Social Work*, 6(3), s. 229-240.
- Aslanyürek, M. (2016). İnternet ve Sosyal Medya Kullanıcılarının İnternet Güvenliği ve Çevrimiçi Gizlilik ile İlgili Kanaatleri ve Farkındalıkları. *Maltepe Üniversitesi İletişim Fakültesi Dergisi*, 3(1), s. 80-106.
- Atalay, G. E. (2020). Toplumsal Cinsiyet Rollerine Dair Toplumsal Baskının Sosyal Medya Mecralarındaki Tezahürü: Siber Zorbalık. B. Muratoğlu Pehlivan (Dü.) içinde, *Medya ve Toplumsal Cinsiyet Üzerine Tartışmalar*. İstanbul: HiperYayın.
- Avcı, A., & Kayıran, D. (2023). Çocuk Gelişimi Ön Lisans Öğrencilerinin Ekran Bağımlılığı ve Çevrimiçi Mahremiyet Farkındalıklarının İncelenmesi. *İnönü Üniversitesi Sağlık Hizmetleri Meslek Yüksekokulu Dergisi*, 11(3), s. 1802-1815. doi:10.33715/inonusaglik.1288292
- Bağlı, M. (2011). *Modern Bilinç ve Mahremiyet*. İstanbul: Yarı Yayınılık.
- Bakan, U. (2019). Sosyal Medya'da Kimliklerin Sunumu: Facebook Kullanıcıları Üzerine Karşılaştırmalı Bir Analiz. *Intermedia International E-journal*, 6(11), s. 83-99.
- Bandura, A. (1997). *Self-Efficacy: The Exercise of Control*. New York: Freeman.
- Baritçi, F. (2023). Üniversite Öğrencilerinin Instagram'da Mahremiyet Algıları Üzerine Bir Saha Araştırması. *Gümüşhane Üniversitesi İletişim Fakültesi Elektronik Dergisi*, 11(1), s. 280-304.
- Barker, R. L. (2014). *The Social Work Dictionary*. Washington, DC: NASW Press. Mayıs 2025 tarihinde <https://archive.org/details/socialworkdictio0006bark/page/n531/mode/2up> adresinden alındı
- Barlett, C., DeWitt, C., Maronna, B., & Johnson, K. (2018). Social Media Use as a Tool to Facilitate or Reduce Cyberbullying Perpetration: A Review Focusing on Anonymous and Nonanonymous Social Media Platforms. *Violence and Gender*, 5(3), s. 147-152. doi:https://doi.org/10.1089/vio.2017.0057

- Bayram, N., & Saylı, M. (2013). Üniversite Öğrencileri Arasında Siber Zorbalık Davranışı. *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*, 71(1), s. 107-116.
- Baysal Berkup, S. (2015). Sosyal Ağlarda Bireysel Mahremiyet Paylaşımı: X ve Y Kuşakları Arasında Karşılaştırmalı Bir Analiz . *Yayınlanmış Doktora Tezi*. Ege Üniversitesi.
- Beran, T. N., & Li, Q. (2005). Cyber-Harassment: A Study of a New Method for an Old Behavior. *Journal of Educational Computing Research*, 32(3), s. 265-277. doi:<https://doi.org/10.2190/8YQM-B04H-PG4D-BLLH>
- Beran, T. N., & Li, Q. (2007). The Relationship between Cyberbullying and School Bullying. *The Journal of Student Wellbeing*, 1(2), s. 15-33. doi:<https://doi.org/10.21913/jsw.v1i2.172>
- Bernstein, J. Y., & Watson, M. W. (1997). Children Who Are Targets of Bullying: A Victim Pattern. *Journal of Interpersonal Violence*, 12(4), s. 483-498. doi:<https://doi.org/10.1177/088626097012004001>
- Bietz, M. J., Cheung, C., Rubanovich, C. K., Schairer, C., & Bloss, C. S. (2019). Privacy Perceptions and Norms in Youth and Adults. *Clinical Practice in Pediatric Psychology*, 7(1), s. 93-103. doi:<https://doi.org/10.1037/cpp0000270>
- Bishop, S. R., Lau, M., Shapiro, S., Carlson, L., Anderson, N. D., Carmody, J., . . . Devins, G. (2004). Mindfulness: A Proposed Operational Definition. *Clinical Psychology: Science and Practice*, 11(3), s. 230-241. doi:<https://doi.org/10.1093/clipsy.bph077>
- Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2018). Exploring Motivations for Online Privacy Protection Behavior: Insights From Panel Data. *Communication Research*, 48(7), s. 953-977. doi:<https://doi.org/10.1177/0093650218800915>
- Brown, C. F., Demaray, M. K., & Secord, S. M. (2014). Cyber Victimization in Middle School and Relations to Social Emotional Outcomes. *Computers in Human Behavior*, 35(6), s. 12-21. doi:<https://doi.org/10.1016/j.chb.2014.02.014>
- Bruin, E. I., Meppelink, R., & Bögels, S. (2015). Mindfulness in Higher Education: Awareness and Attention in University Students Increase During and After Participation in a Mindfulness Curriculum Course. *Mindfulness*, 6(5), s. 1137-1142. doi:<https://doi.org/10.1007/s12671-014-0364-5>
- Burger, C., & Bachmann, L. (2021). Perpetration and Victimization in Offline and Cyber Contexts: A Variable- and Person-Oriented Examination of Associations and Differences Regarding Domain-Specific Self-Esteem and School Adjustment. *International Journal of Environmental Research and Public Health*, 18(19), s. 1-21. doi:<https://doi.org/10.3390/ijerph181910429>

- Burke, C. A. (2010). Mindfulness-based Approaches with Children and Adolescents: A Preliminary Review of Current Redearch in an Emergent Field. *Journal of Child and Family Studies*, 19(2), s. 133-144. doi:<https://doi.org/10.1007/s10826-009-9282-x>
- Burnukara, P., & Uçanok, Z. (2012). İlk ve Orta Ergenlikte Akran Zorbalığı: Gerçekleştiği Yerler ve Baş Etme Yolları. *Türk Psikoloji Yazılar*, 15(29), s. 68-82.
- Büyüköztürk, Ş., Kılıç Çakmak, E., Akgün, Ö. E., Karadeniz, Ş., & Demirel, F. (2019). *Bilimsel Araştırma Yöntemleri*. Ankara: Pegem Akademi.
- Canbay, Y., & Sağiroğlu, Ş. (2020). Derin Öğrenmede Diferansiyel Mahremiyet. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, 6(1), s. 1-16.
- Cankurtaran, Ö., Akoğlu, G., & Sakarya, H. (2020). Güçlenmeyi Güç Güçsüzlük Baskı ve Güç İlişkileri Temelinde Anlamak. *Toplum Ve Sosyal Hizmet*, 31(4), s. 1913-1939. doi:<https://doi.org/10.33417/tsh.782159>
- Cho, H., Rivera-Sánchez, M., & Lim, S. S. (2009). A Multinational Study on Online Privacy: Global Concerns and Local Responses. *New Media and Society*, 11(3), s. 395-416. doi:<https://doi.org/10.1177/1461444808101618>
- Choi, H., Park, J., & Jung, Y. (2018). The Role of Privacy Fatigue in Online Privacy Behavior. *Computers In Human Behavior*, 81(3), s. 42-51.
- Creswell, J. W. (2012). *Educational Research: Planning, Conducting, and Evaluating Quantitative and Qualitative Research (4th edition.)*. New Jersey: Pearson.
- Çakır, H., Özüdoğru, G., Bozkurt, Ş. B., & Hava, K. (2015). Öğretmen Adaylarının Sosyal Ağ Sitelerinde Gizlilik Farkındalıklarının İncelenmesi. *Ahi Evran Üniversitesi Kırşehir Eğitim Fakültesi Dergisi*, 16(2), s. 235-249.
- Çalık, N. S. (2018). Beden, Mesken ve Bilgi Mahremiyeti Açısından Sosyal Medyadaki Tasarrufların Fikhî Açidan Değerlendirilmesi. *Turkish Academic Research Review*, 3(1), s. 25-44.
- Çatak, P. D., & Ögel, K. (2010). Farkındalık Temelli Terapiler ve Terapötik Süreçler. *Klinik Psikiyatri*, 13(1), s. 85-91.
- Çaycı, B., & Karagülle, A. E. (2014). X kuşağından Z Kuşağına Değişen Mahremiyet Algısı. *In International Trends and Issues in Communication and Media Conference*, (s. 190-196).
- Çevik Tekin, İ., Erdoğan, P., & Şanlı, Y. (2021). Sosyal Medya Tutumunu Öz-yeterlilik Etkiler mi?: Bir Alan Araştırması. *Turkish Studies-Economics, Finance, Politics*, 16(1), s. 537-551. doi:<http://dx.doi.org/10.47644/TurkishStudies.49132>

- Çubukcu, A., & Bayzan, Ş. (2013). Türkiye’de Dijital Vatandaşlık Algısı ve Bu Algıyı İnternetin Bilinçli, Güvenli ve Etkin Kullanımı İle Artırma Yöntemleri. *Middle Eastern & African Journal of Educational Research*(5), s. 148-174.
- Dağlı, G. N. (2024). Üniversite Öğrencilerinin Bilinçli Farkındalık, Siber Zorbalık ve Siber Mağduriyet Düzeylerinin Sosyal Medya Bağımlılığı ile İlişkisi. *Yayınlanmış Yüksek Lisans Tezi*. Kırşehir Ahi Evran Üniversitesi.
- Davis, K., & James, C. (2012). Tweens' Conceptions of Privacy Online: Implications for Educators. *Learning, Media and Technology*, 38(1), s. 4-25. doi:<https://doi.org/10.1080/17439884.2012.658404>
- Day, S., Bussey, K., Trompeter, N., & Mitchison, D. (2022). The Impact of Teasing and Bullying Victimization on Disordered Eating and Body Image Disturbance Among Adolescents: A Systematic Review. *Trauma, Violence, and Abuse*, 23(3), s. 985-1006. doi:<https://doi.org/10.1177/1524838020985534>
- De Wolf, R. (2019). Contextualizing How Teens Manage Personal and Interpersonal Privacy on Social Media. *New Media AND Society*, 22(6), s. 1058-1075. doi:<https://doi.org/10.1177/1461444819876570>
- Debatin, B., Lovejoy, J., Horn, A.-K., & Hughes, B. N. (2009). Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences. *Journal of Computer-Mediated Communication*, 15(1), s. 83-108. doi:<https://doi.org/10.1111/j.1083-6101.2009.01494.x>
- DePaolis, K., & Williford, A. (2015). The Nature and Prevalence of Cyber Victimization Among Elementary School Children. *Child and Youth Care Forum*, 44(3), s. 377-393. doi:<https://doi.org/10.1007/s10566-014-9292-8>
- Diaz, F. M. (2022). Mindfulness. G. E. McPherson (Dü.) içinde, *The Oxford Handbook of Music Performance, Volume 2*. Oxford University Press.
- Diler, R. (2014). Mahremiyet Eğitimi ve Önemi. *Gaziosmanpaşa Üniversitesi İlahiyat Fakültesi Dergisi*, 2(1), s. 69-98.
- Dilmaç, B. (2009). Psychological Needs as a Predictor of Cyber Bullying: A Preliminary Report on College Students. *Educational Sciences: Theory and Practice*, 9(3), s. 1307-1325.
- Doğan , T., & Eryılmaz, A. (2013). İki Boyutlu Benlik Saygısı ve Öznel İyi Oluş Arasındaki İlişkilerin İncelenmesi. *Pamukkale Üniversitesi Eğitim Fakültesi Dergisi*, 33(33), s. 107-117. doi:<https://doi.org/10.9779/PUJE434>
- Doğru Çabuker, N., & Balcı Çelik, S. (2019). Üniversite Öğrencilerinin Ayrışma Bireyleşme ve Kimlik Algılarının Bazı Demografik Özelliklerine Göre İncelenmesi. *Ondokuz*

- Mayıs Üniversitesi Eğitim Fakültesi Dergisi*, 38(1), s. 53-72.
doi:<https://doi.org/10.7822/omuefd.461862>
- Dowd, M. (2011). Contextualised Concerns: The Online Privacy Attitudes of Young Adults. *Privacy and Identity Management for Life*, 352, s. 78-89.
doi:https://doi.org/10.1007/978-3-642-20769-3_7
- Duyan, V., Özgür Sayar, Ö., & Özbulut, M. (2008). *Sosyal Hizmet Tanımak ve Anlamak: Sosyal Hizmet Uzmanları ve Sosyal Hizmet Alanında Çalışanlar İçin Bir Rehber*. Ankara: Sosyal Hizmet Uzmanları Derneği Yayını.
- Erbay, E. (2019). Güç ve Güçlendirme Kavramları Bağlamında Sosyal Hizmet Uygulaması. *Sosyal Politika Çalışmaları Dergisi*, 19(42), s. 41-64.
- Erikson, E. H. (1976). Reflections on Dr. Borg's Life Cycle. *Daedalus*, 105(2), s. 1-28.
- Eroğlu, Ş. (2018). Dijital Yaşamda Mahremiyet (Gizlilik) Kavramı ve Kişisel Veriler: Hacettepe Üniversitesi Bilgi ve Belge Yönetimi Bölümü Öğrencilerinin Mahremiyet ve Kişisel Veri Algılarının Analizi. *Hacettepe Üniversitesi Edebiyat Fakültesi Dergisi*, 35(2), s. 130-153. doi:10.32600/huefd.439007
- Eroğlu, Y., & Peker, A. (2011). Aileden ve Arkadaştan Algılanan Sosyal Destek ve Siber Mağduriyet: Yapısal Eşitlik Modeliyle Bir İnceleme. *Akademik Bakış Dergisi*, 1(27), s. 1-20.
- Fay, B. (1987). *Critical Social Science: Liberation and Its Limits*. New York: Cornell University Press.
- Fekih-Romdhane, F., Stambouli, M., Malaeb, D., Farah, N., Cheour, M., Obeid, S., & Hallit, S. (2023). Insomnia And Distress As Mediators On The Relationship From Cyber-Victimization To Self-Reported Positive Psychotic Experiences: A Binational Study From Tunisia And Lebanon. *BMC Psychiatry*, 23(1), s. 1-11.
doi:<https://doi.org/10.1186/s12888-023-05019-w>
- Fey, M. (2019). Components of Mindfulness Training: Impacts on Attention and Affect. University of Arkansas.
- Field, A. (2009). *Discovering Statistics Using SPSS (3rd edition)*. London: Sage Publications Ltd.
- Fischer-Hübner, S. (1998). Privacy and Security at Risk in the Global Information Society. *Information, Communication and Society*, 1(4), s. 420-441.
- Frankel, J. R., Wallen, N. E., & Hyun, H. H. (2012). *How to Design and Evaluate Research in Education (8th edition)*. New York: The McGraw-Hill Companies Inc.
- Freire, P. (1972). *Ezilenlerin Pedagojisi*. (D. Hattatoğlu, & E. Özbek, Çev.) Ayrıntı Yayınevi.

- Fujita, J. S., & Ruffa, V. (2019). Cyberbullying: Família, Escola e Tecnologia Como Stakeholders. *Estudos Avançados*, 33(97), s. 401-412. doi:<https://doi.org/10.1590/s0103-4014.2019.3397.022>
- Fung, A. L. (2012). Intervention for Aggressive Victims of School Bullying in Hong Kong: A Longitudinal Mixed-methods Study. *Scandinavian Journal of Psychology*, 53(4), s. 360-367. doi:<https://doi.org/10.1111/j.1467-9450.2012.00953.x>
- Gavison, R. (1980). Privacy and the Limits of Law. *The Yale Law Journal*, 89(3), s. 421-471.
- George, D., & Mallery, M. (2010). *SPSS for Windows Step by Step: A Simple Guide and Reference (10th edition)*. Boston: Pearson.
- Gini, G., Card, N. A., & Pozzoli, T. (2018). A Meta-Analysis of the Differential Relations of Traditional and Cyber-Victimization with Internalizing Problems. *Aggressive Behavior*, 44(2), s. 185-198. doi:<https://doi.org/10.1002/ab.21742>
- Goethals, S., Matz, S., Provost, F., Martens, D., & Ramon, Y. (2025). The Impact of Cloaking Digital Footprints on User Privacy and Personalization. *Big Data*, s. 1-19. doi:<https://doi.org/10.1089/big.2024.0036>
- Goldfarb, A., & Que, V. F. (2023). The Economics of Digital Privacy. *Annual Review of Economics*, 15, s. 267-286. doi:<https://doi.org/10.1146/annurev-economics-082322-014346>
- Görmen Şen, H. (2024). Sosyal Bilgiler Öğretmenlerini Dijital Mahremiyete İlişkin Metafor Algıları Üzerine Bir İnceleme. *Yayınlanmış Yüksek Lisans Tezi*. Van Yüzüncü Yıl Üniversitesi.
- Greenbaum, J., Crawford-Jakubiak, J. E., Christian, C. W., Flaherty, E. G., Leventhal, J. M., Lukefahr, J. L., . . . Hurley, T. P. (2015). Child Sex Trafficking and Commercial Sexual Exploitation: Health Care Needs of Victims. *The American Academy of Pediatrics*, 135(3), s. 566-574. doi:<https://doi.org/10.1542/peds.2014-4138>
- Greene, G. J., & Lee, M. Y. (2002). The Social Construction of Empowerment. M. O'Melia, & K. K. Miley (Dü) içinde, *Pathways to Power: Readings in Contextual Social Work Practice*. Boston: Allyn and Bacon.
- Greene, G., Lee, M. Y., & Hoffpauir, S. (2005). The Language of Empowerment and Strengths in Clinical Social Work: A Constructivist Perspective. *Families in Society The Journal of Contemporary Social Services*, 86(2), s. 267-277.
- Gutierrez, L. M. (1990). Working with Women of Color: An Empowerment Perspective. *Social Work*, 35(2), s. 149-153.

- Gülderen, C., Çetinkaya, L., & Keser, H. (2016). Ortaöğretim Öğrencilerine Yönelik Bilgi Güvenliği Farkındalık Ölçeği (BGFÖ) Geliştirme Çalışması. *İlköğretim Online*, 15(2), s. 682-695.
- Güllük, İ. (2014). Avret Mahremiyeti Prensipleri Açısından Görüntü, Gerçeklik, Sanal Âlem ve Cinsellik Üzerine Fıkîhî Bir Analiz. *İslam Hukuku Araştırmaları Dergisi*(23), s. 105-128.
- Gültekin, V. (2024). Bilgi ve Belge Yönetimi Bölümü Öğrencilerinin Çevrimiçi Mahremiyet Farkındalığı. *Bilgi Dünyası*, 25(2), s. 185-215. doi:10.15612/BD.2024.768
- Gürkan, M. F. (2013). Düzenleyici ve Denetleyici Kurum Olarak Bilgi Teknolojileri ve İletişim Kurumu BTK. *İnönü Üniversitesi Hukuk Fakültesi Dergisi*, 4(2), s. 333-356. doi:https://doi.org/10.21492/inuhfd.239846
- Heiman, T., & Olenik Shemesh, D. (2019). Predictors of Cyber-Victimization of Higher-Education Students With and Without Learning Disabilities. *Journal of Youth Studies*, 22(2), s. 205-222. doi:https://doi.org/10.1080/13676261.2018.1492103
- Heiman, T., & Olenik-Shemesh, D. (2022). Cyber-Victimization Experience among Higher Education Students: Effects of Social Support, Loneliness, and Self-Efficacy. *Journal of Environmental Research and Public Health*, 19(12), s. 1-13. doi:https://doi.org/10.3390/ijerph19127395
- Herry, E., & Mulvey, K. L. (2022). Gender-Based Cyberbullying: Understanding Expected Bystander Behavior Online. *Journal of Social Issues*, 79(4), s. 1212-1230.
- Hinduja, S., & Patchin, J. W. (2010). Bullying, Cyberbullying, and Suicide. *Archives of Suicide Research*, 14(3), s. 206-221. doi:https://doi.org/10.1080/13811118.2010.494133
- Hou, Y., Xiong, D., Jiang, T., Song, L., & Wang, Q. (2019). Social Media addiction: Its Impact, Mediation, and Intervention. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 13(1), s. 1-17. doi:https://doi.org/10.5817/CP2019-1-4
- Jackson, C. L., & Cohen, R. (2012). Childhood Victimization: Modeling the Relation Between Classroom Victimization, Cyber Victimization, and Psychosocial Functioning. *Psychology of Popular Media Culture*, 1(4), s. 254-269. doi:https://doi.org/10.1037/a0029482
- Kabat-Zinn, J. (2013). *Full Catastrophe Living: Using the Wisdom of Your Body and Mind to Face Stress, Pain and Illness*. New York: Bantam.
- Kalafat Çat, A., & Aydın Aydoğan, B. (2023). Sosyal Medyada Dijital Kimlik İnşası: Instagram Kullanıcılarının Biyografi Yazılarının Cinsiyet ve Kuşak Kategorisine Göre Analizi. *Academic Knowledge*, 6(2), s. 219-233. doi:https://10.5281/zenodo.10443241

- Kalaman, S. (2017). Yeni Medya ve Mahremiyetin Dönüşümü: Facebook Türkiye Örneği. *Uluslararası Hakemli İletişim Ve Edebiyat Araştırmaları Dergisi*(14), s. 1-31.
- Kantar Özkes, D. (2023). Sosyal Medya Uygulamalarında Dijital Mahremiyet Farkındalığının Ölçülmesi. *Yayınlanmış Yüksek Lisans Tezi*. Hitit Üniversitesi.
- Karaca, M., Mutlu, T., & Gencer, G. (2021). Siber Mağduriyet: Kavramsal Bir Çalışma. *Anadolu Akademi Sosyal Bilimler Dergisi*, 3(1), s. 177-191.
- Karadaş, E., & Kara, M. (2021). Üniversite Öğrencilerinin Çevrimiçi Mahremiyet Farkındalıklarının Belirli Etkenler Açısından İncelenmesi. *Türkiye Sosyal Araştırmalar Dergisi*, 25(1), s. 147-162.
- Karakuş Yılmaz, T. (2020). Dijital Haklar ve Sorumluluklar. Ş. Sağiroğlu, H. İ. Bülbül, A. Kılıç, & M. Küçükali içinde, *Dijital Okuryazarlık: Araçlar, Metodolojiler, Uygulamalar ve Öneriler* (s. 127-180). Ankara: Nobel Yayınları.
- Karakuş, S., & Turan, S. G. (2022). Yetişkinlerin Siber Zorbalık Davranımları ile Dijital Vatandaşlık Becerileri Arasındaki İlişkinin İncelenmesi. *Pamukkale Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*(48), s. 409-427.
- Kaygısız, E. G. (2020). Şiddetin E-Hali: Siber Zorbalık. *Türkiye İnsan Hakları ve Eşitlik Kurumu Akademik Dergisi*(4-5), s. 161-174.
- Kırlioğlu, M. (2019). Güçler Temelli Yaklaşım ve Güçlendirme: Kolektif Kimlik, Bilgi-Beceri, Benlik Kavramı, Eleştirel Farkındalık, Harekete Geçme. *OPUS Uluslararası Toplum Araştırmaları Dergisi*, 14(20), s. 2248-2277. doi:<https://doi.org/10.26466/opus.597190>
- Koçak, S., Kınalı, A., Yazıcı, F., & Özen Üzel, A. (2024). Siber Zorbalık Davranışlarının Lise Öğrencilerinin Demografik Faktörlerine Göre İncelenmesi. *Ulusal Eğitim Dergisi*, 4(2), s. 906–922.
- Komisyon. (2019). *Dini terimler sözlüğü*. Ankara: Milli Eğitim Bakanlığı Yayınları.
- Korkmaz, Ö., Vergili, M., & Karadaş, E. (2021). Çevrimiçi Mahremiyet Farkındalık Ölçeğinin Geliştirilmesi: Güvenirlik ve Geçerlilik Çalışması. *Türkiye Bilimsel Araştırmalar Dergisi*, 6(2), s. 297-311.
- Korucu , A. T., & Gürkez, Ş. (2019). An Analysis of Online Privacy Concerns of Teacher Candidates. *Participatory Educational Research*, 6(2), s. 15-25. doi:<https://doi.org/10.17275/per.19.9.6.2>
- Kowalski, R., Giumetti, G., Schroeder, A., & Lattanner, M. (2014). Bullying in the Digital Age: A Critical Review and Meta-Analysis of Cyberbullying Research Among Youth. *Psychological Bulletin*, 140(4), s. 1073-1137.

- Kropczynski, J., Aljallad, Z., Elrod, N. J., Lipford, H., & Wisniewski, P. J. (2021). Towards Building Community Collective Efficacy for Managing Digital Privacy and Security within Older Adult Communities. *Association for Computing Machinery*, 4, s. 1-27. doi:<https://doi.org/10.1145/3432954>
- Lai, C. S., Mohamad, M. M., Lee, M. F., Salleh, K. M., Sulaiman, N., Rosli, D. I., & Chang, W. V. (2017). Prevalence of Cyberbullying among Students in Malaysian Higher Learning Institutions. *Advanced Science Letters*, 23(2), s. 781-784.
- Landoll, R., La Greca, A. M., Lai, B. S., Chan, S. F., & Herge, W. M. (2015). Cyber Victimization by Peers: Prospective Associations with Adolescent Social anxiety and Depressive Symptoms. *Journal of Adolescence*, 42(1), s. 77-86. doi:<https://doi.org/10.1016/j.adolescence.2015.04.002>
- Lee, J. A. (2001). *The Empowerment Approach to Social Work Practice: Building the Beloved Community*. New York: Columbia University Press.
- Levent, L. (2015). Mahremiyet ve Aile. *Diyanet Dergisi*, 1, s. 4-9.
- Lin, L., Liu, J., Cao, X., Wen, S., Xu, J., Xue, Z., & Lu, J. (2020). The Association Between Suicidality and Internet Addiction and Activities in Taiwanese Adolescents. *BMC Psychiatry*, 20(1), s. 1-8. doi:<https://doi.org/10.1186/s12888-020-02548-6>
- Liu, C., Liu, Z., & Yuan, G. (2021). Longitudinal Associations Between Cyberbullying Victimization, Mindfulness, Depression, and Anxiety: A Mediation Analysis. *Journal of Aggression, Maltreatment & Trauma*, 31(1), s. 121-132. doi:<https://doi.org/10.1080/10926771.2021.1876197>
- Livingstone, S., & Haddon, L. (2009). *EU Kids Online: Final Report*. London: EU Kids Online The London School of Economics.
- Lokke, E. (2018). *Mahremiyet: Dijital Toplumda Özel Hayat*. (D. Başak, Çev.) İstanbul: Koç Üniversitesi Yayınları.
- Lustgarten, S., Garrison, Y. L., Sinnard, M. T., & Flynn, A. W. (2020). Digital Privacy in Mental Healthcare: Current Issues and Recommendations for Technology Use. *Current Opinion in Psychoogy*, 36, s. 25-31. doi:<https://doi.org/10.1016/j.copsyc.2020.03.012>
- Mahadik, S., Pawar, P. M., Muthalagu, R., Prasad, N. R., Hawkins, S.-K., & Strielis, D. (2024). Digital Privacy in Healthcare: State-of-the-Art and Future Vision. *IEEE Access*, 12, s. 84273-84291. doi:10.1109/ACCESS.2024.3410035
- Malesky, L. A. (2007). Predatory Online Behavior: Modus Operandi of Convicted Sex Offenders in Identifying Potential Victims and Contacting Minors Over the Internet.

- Journal of Child Sexual Abuse*, 16(2), s. 23-32.
doi:https://doi.org/10.1300/J070v16n02_02
- Marco, J. H., Tormo-Irun, M. P., Galan-Escalante, A., & Gonzalez-Garcia, C. (2018). Is Cybervictimization Associated with Body Dissatisfaction, Depression, and Eating Disorder Psychopathology? *Cyberpsychology, Behavior, and Social Networking*, 21(10), s. 611-617. doi:<https://doi.org/10.1089/cyber.2018.0217>
- Martinez-Martinez, A. M., Lopez-Liria, R., Aguilar-Parra, J. M., Trigueros, R., Morales-Gazquez, M., & Rocamora-Perez, P. (2020). Relationship between Emotional Intelligence, Cybervictimization, and Academic Performance in Secondary School Students. *International Journal of Environmental Research and Public Health*, 17(21), s. 1-12. doi:<https://doi.org/https://doi.org/10.3390/ijerph17217717>
- Martínez-Monteağudo, M. C., Delgado, B., Ingles, C. J., & Escortell, R. (2020). Cyberbullying and Social Anxiety: A Latent Class Analysis Among Spanish Adolescents. *International Journal of Environmental Research and Public Health*, 17(2), s. 1-13.
- Mason, K. L. (2008). Cyberbullying: A Preliminary Assessment for School Personnel. *Psychology in the Schools*, 45(4), s. 323-348. doi:<https://doi.org/10.1002/pits.20301>
- Matthews, T., Caspi, A., Danese, A., Fisher, H. L., Moffitt, T. E., & Arseneault, L. (2022). A Longitudinal Twin Study of Victimization and Loneliness From Childhood to Young Adulthood. *Development and Psychopathology*, 34(1), s. 367-377. doi:<https://doi.org/10.1017/S0954579420001005>
- McLuhan, M., & Powers, B. R. (2020). *Global Köy: 21. Yüzyılda Yeryüzü Yaşamında ve Medyada Meydana Gelecek Dönüşümler*. (B. Ö. Düzgören, Çev.) İstanbul: Scala Yayıncılık.
- Medrano, J. L., Lopez, R. F., & Gamez-Guadix, M. (2018). Assessing the Links of Sexting, Cybervictimization, Depression, and Suicidal Ideation Among University Students. *Archives of Suicide Research*, 22(1), s. 153-164. doi:<https://doi.org/10.1080/13811118.2017.1304304>
- Mishna, F., Schwan, K. J., Birze, A., Van Wert, M., Lacombe-Duncan, A., McInroy, L., & Attar-Schwartz, S. (2020). Gendered and Sexualized Bullying and Cyber Bullying: Spotlighting Girls and Making Boys Invisible. *Youth and Society*, 52(3), s. 403-426.
- Mitchell, K. J., Finkelhor, D., & Wolak, J. (2003). Victimization of Youths on the Internet. *Journal of Aggression, Maltreatment and Trauma*, 8(1-2), s. 1-39. doi:https://doi.org/10.1300/J146v08n01_01

- Mitchell, K. J., Finkelhor, D., Wolak, J., Ybarra, M. L., & Turner, H. (2011). Youth Internet Victimization in a Broader Victimization Context. *Journal of Adolescent Health, 48*(2), s. 128-134. doi:<https://doi.org/10.1016/j.jadohealth.2010.06.009>
- Naslund, J. A., Bondre, A., Torous, J., & Aschbrenner, K. A. (2020). Social Media and Mental Health: Benefits, Risks and Opportunities for Research and Practice. *Journal of Technology in Behavioral Science, 5*(3), s. 245-257. doi:<https://doi.org/10.1007/s41347-020-00134-X>
- Neelakandan, S., Annamalai, R., Rayen, S. J., & Arunajsmine, J. (2020). Social Media Networks Owing to Disruptions for Effective Learning. *Procedia Computer Science, 172*, s. 145-151.
- Okumuş, M., & Atılgan, S. S. (2021). Üniversite Öğrencilerinin Dijital Okuryazarlık Becerileri ile Dijital Mahremiyet Kaygısı Arasındaki İlişki. *TRT Akademi, 6*(12), s. 342-363.
- Orlofsky, J. L., Marcia, J. E., & Lesser, I. M. (1973). Ego Identity Status and Theintimacy Versus Isolation Crisis of Young Adulthood. *Journal of Personality and Social, 27*(2), s. 211-219.
- Öngören, H., & Yılmaz, A. (2023). Ortaokuldaki Öğrencilerin Dijital Hak ve Sorumluluk Bilinci ile Sosyal ve Duygusal Öğrenme Becerileri Arasındaki İlişki. *Değerler Eğitimi Dergisi, 21*(46), s. 399-423. doi:<https://doi.org/10.34234/ded.1331264>
- Öz, M. (2014). Sosyal Medya Kullanımı ve Mahremiyet Algısı: Facebook Kullanıcılarının Mahremiyet Endişeleri ve Farkındalıkları. *Yaşar Üniversitesi E-Dergisi, 9*(35), s. 6245-6254. doi:<https://doi.org/10.19168/jyu.96978>
- Öz, M., & Kılıç, D. (2020). Kişisel Verilerin Çevrimiçi Mahremiyet İle İlişkisinin İçerik Analizi Yöntemiyle İncelenmesi. *Karamanoğlu Mehmetbey Üniversitesi Sosyal Ve Ekonomik Araştırmalar Dergisi, 22*(39), s. 206-224.
- Özbudun, E. (2025). *Türk Anayasa Hukuku*. Ankara: Yetkin Yayınları.
- Özdemir, H. (2020). *Dijital Mahremiyet*. İstanbul: İnsan ve Hayat Kitaplığı.
- Özen, Y. (2017). Farkında mıyız? Bilişsel Farkındalık ile Psikolojik İyi Oluşun İçerelleşmesi. *Kesit Akademi Dergisi, 3*(7), s. 167-189.
- Özer, N., Çelik, S., & Özatlı, N. S. (2021). Dijital Çağda X, Y, Z Kuşaklarının Medya Okuryazarlık Düzeylerinin Farklı Değişkenlere Göre İncelenmesi: Balıkesir Örneği. *Kırıkkale Üniversitesi Sosyal Bilimler Dergisi, 11*(1), s. 217-232.
- Özkaya, P. (2023). Dijital Dünyada Çevrimiçi Riskler, Bilişim Suçları ve Mağdur Çocuk. *Türkiye Adalet Akademisi Dergisi*(53), s. 13-42. doi:<https://doi.org/10.54049/taad.1231771>

- Öztürk, D., Eyüboğlu, G., & Göçmen Baykara, Z. (2022). Üniversite Öğrencilerinin Mahremiyet Bilinci. *Gazi Sağlık Bilimleri Dergisi*, 7(4), s. 68-77. doi:<https://doi.org/10.52881/gsbdergi.1014500>
- 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), s. 526-536.
- Pallant, J. (2017). *SPSS Kullanma Klavuzu SPSS ile Adım Adım Veri Analizi*. (S. Balcı, & B. Ahi, Çev.) Ankara: Anı Yayıncılık.
- Park, Y. J. (2013). Digital Literacy and Privacy Behavior Online. *Communication Research*, 40(2), s. 215-236. doi:<https://doi.org/10.1177/0093650211418338>
- Patchin, J. W., & Hinduja, S. (2006). Bullies Move Beyond the Schoolyard: A Preliminary Look at Cyberbullying. *Youth Violence and Juvenile Justice*, 4(2), s. 148-169. doi:<https://doi.org/10.1177/1541204006286288>
- Pellegrini, A. D. (1998). Bullies and Victims in School: A Review and Call for Research. *Journal of Applied Developmental Psychology*, 19(2), s. 165-176. doi:[https://doi.org/10.1016/S0193-3973\(99\)80034-3](https://doi.org/10.1016/S0193-3973(99)80034-3)
- Pyzalski, J. (2012). From Cyberbullying to Electronic Aggression: Typology of The Phenomenon. *Emotional and Behavioural Difficultie*, 17(3), s. 305-317.
- Rachels, J. (1975). Why Privacy is Important. *Philosophy and Public Affairs*, 4(4), s. 323-333.
- Ramsey, J. L., DiLalla, L. F., & McCrary, M. K. (2016). Cyber Victimization and Depressive Symptoms in Sexual Minority College Students. *Journal of School Violence*, 15(4), s. 483-502. doi:<https://doi.org/10.1080/15388220.2015.1100116>
- Rapp, C. A., & Goscha, R. J. (2004). The Principles of Effective Case Management of Mental Health Services. *Psychiatric Rehabilitation Journal*, 27(4), s. 319-333.
- Raskauskas, J., & Stoltz, A. D. (2007). Involvement in Traditional and Electronic Bullying Among Adolescents. *Developmental Psychology*, 43(3), s. 564-575. doi:<https://doi.org/10.1037/0012-1649.43.3.564>
- Reed, K. P., Cooper, R. L., Nugent, W. R., & Russell, K. (2015). Cyberbullying: A Literature Review of Its Relationship to Adolescent Depression and Current Intervention Strategies. *Journal of Human Behavior in the Social Environment*, 26(1), s. 37-45. doi:<https://doi.org/10.1080/10911359.2015.1059165>
- Reid, D., & Weigle, P. (2014). Social Media Use Among Adolescents: Benefits and Risks. *Adolescent Psychiatry*, 4(2), s. 73-80. doi:<https://doi.org/10.2174/221067660402140709115810>

- Robalo, T.L.A.S.; Abdul Rahim, R.B.B. (2023). Cyber Victimization, Restorative Justice and Victim-Offender Panels. *Asian Journal of Criminology*, 18(1), s. 61-74. doi:https://doi.org/10.1007/s11417-023-09396-9
- Robertson, L., & Muirhead, B. (2022). Digital Privacy in the Mainstream of Education. *The Open Cybernetics & Systemics Journal*, 18(7), s. 118-125.
- Ryan, K. N., & Curwen, T. (2013). Cyber-Victimized Students: Incidence, Impact, and Intervention. *Sage Open*, 3(4), s. 1-7. doi:https://doi.org/10.1177/2158244013516772
- Safaria, T., Tentama, F., & Suyono, H. (2016). Cyberbully, Cybervictim, and Forgiveness Among Indonesian High School Students. *The Turkish Online Journal of Educational Technology*, 15(3), s. 40-48.
- Saliebey, D. (2013). *The Strengths Perspective in Social Work*. Boston: Pearson.
- Sallan Gül, S., & Altındal, Y. (2015). Medyada Kadın Cinayeti Haberlerindeki Cinsiyetçi İzler: Radikal Gazetesi. *Akdeniz Üniversitesi İletişim Fakültesi Dergisi*(24), s. 168-188.
- Salmon, S., Turner, S., Taillieu, T. L., Fortier, J., & Afifi, T. O. (2018). Bullying Victimization Experiences Among Middle and High School Adolescents: Traditional Bullying, Discriminatory Harassment, and Cybervictimization. 63(1), s. 29-40. doi:https://doi.org/10.1016/j.adolescence.2017.12.005
- Schwartz, D., Dodge, K. A., Pettit, G. S., & Bates, J. E. (1997). The Early Socialization of Aggressive Victims of Bullying. *Child Development*, 68(4), s. 665-675. doi:https://doi.org/10.1111/j.1467-8624.1997.tb04228.x
- Seligman, M. E. (1975). *Helplessness: On Depression, Development, and Death*. San Francisco: CA: W.H. Freeman.
- Semiz Türkoğlu, H. (2018). Sosyal Medya Üzerinden Mahremiyet Farkındalığı ve Değişimin Ölçümlenmesine Yönelik Bir Araştırma. *Istanbul University Journal of Communication Sciences*, 54, s. 163-189.
- Senemoğlu, N. (2020). *Gelişim, Öğrenme ve Öğretim: Kuramdan Uygulamaya*. Ankara: Anı Yayıncılık.
- Sepetci, N. (2017). Sosyal Medyada Mahremiyet Algısının Çöküşü: Instagram Örneği. *Yayınlanmış Yüksek Lisans Tezi*. Marmara Üniversitesi.
- Serin, H. (2012). Ergenlerde Siber Zorbalık/Siber Mağduriyet Yaşantıları ve Bu Davranışlara İlişkin Öğretmen ve Eğitim Yöneticilerinin Görüşleri. *Yayınlanmamış Doktora Tezi*. İstanbul Üniversitesi.

- Shapiro, S. L., Carlson, L. E., Astin, J. A., & Freedman, B. (2006). Mechanisms of Mindfulness. *Journal of Clinical Psychology*, 62(3), s. 373-386. doi:https://doi.org/10.1002/jclp.20237
- Sine Nazlı, R., & Akcaoğlu Erdem, Ö. (2023). Instagram'da Mahremiyet Algısının Benlik İnşasına Etkisi: BAİBÜ Öğrencileri Örneği. *Abant Kültürel Araştırmalar Dergisi*, 8(16), s. 64-80.
- Slonje, R., Smith, P. K., & Frisen, A. (2013). The Nature of Cyberbullying, and Strategies for Prevention. *Computers in Human Behavior*, 29(1), s. 26-32. doi:https://doi.org/10.1016/j.chb.2012.05.024
- Solove, D. J. (2008). *Understanding Privacy*. Cambridge: Harvard University Press.
- Song, H., Lynch, M. J., & Cochran, J. K. (2015). A Macro-Social Exploratory Analysis of the Rate of Interstate Cyber-Victimization. *American Journal of Criminal Justice*, 41(3), s. 583-601. doi:https://doi.org/10.1007/s12103-015-9308-4
- Sontag, L. M., Clemans, K. H., Graber, J. A., & Lyndon, S. T. (2011). Traditional and Cyber Aggressors and Victims: A Comparison of Psychosocial Characteristics. *Journal of Youth and Adolescence*, 40(4), s. 392-404. doi:https://doi.org/10.1007/s10964-010-9575-9
- Stevens, F., Enock, F. E., Sippy, T., Bright, J., Cross, M., Johansson, P., . . . Margetts, H. Z. (2024). Women Are Less Comfortable Expressing Opinions Online Than Men and Report Heightened Fears for Safety: Surveying Gender Differences in Experiences of Online Harms. s. 1-18. doi:https://doi.org/10.48550/arXiv.2403.19037
- Strohmeier, D., Karna, A., & Salmivalli, C. (2010). Intrapersonal and Interpersonal Risk Factors for Peer Victimization in Immigrant Youth in Finland. *Developmental Psychology*, 47(1), s. 248-258. doi:https://doi.org/10.1037/a0020785
- Şahin, M., Sarı, S. V., Özer, Ö., & Er, S. H. (2010). Lise Öğrencilerinin Siber Zorba Davranışlarda Bulunma Ve Maruz Kalma Durumlarına İlişkin Görüşleri. *Süleyman Demirel Üniversitesi Fen-Edebiyat Fakültesi Sosyal Bilimler Dergisi*(21), s. 257-270.
- Şişman, N. (2020). Sunuş. N. Şişman (Dü.) içinde, *Mahremiyet: Hayatın Sırları ve Sınırları*. İstanbul: İnsan Yayınları.
- Tabachnick, B. G., & Fidell, L. S. (2013). *Using Multivariate Statistics*. Boston: Pearson.
- Talan, T., & Aktürk, C. (2021). Orta Öğretim Öğrencilerinin Dijital Okuryazarlık ve Bilgi Güvenliği Farkındalığı Seviyelerinin İncelenmesi. *Kahramanmaraş Sütçü İmam Üniversitesi Sosyal Bilimler Dergisi*, 18(1), s. 158-180. doi:https://doi.org/10.33437/ksusbd.668255

- Tan, H., & Şenkal, Y. (2024). Siber Zorbalık Olgusunun Psikolojik ve Davranışsal Etkileri ile Siber Zorbalığa Karşı Geliştirilen Savunma Mekanizmalarını Dijital Yerliler Üzerinden İncelemek. *Uluslararası Sosyal Bilimler Akademi Dergisi*, 6(16), s. 410-441. doi:<https://doi.org/10.47994/usbad.1510397>
- Tan, Q., & Pivot, F. (2015). Big Data Privacy: Changing Perception of Privacy. *2015 IEEE International Conference on Smart City/SocialCom/SustainCom (SmartCity)*, (s. 860-865). Chengdu, China. doi:<https://doi.org/10.1109/SmartCity.2015.176>
- Tanışık, S., & Bal, S. (2024). Dijital Mahremiyet ve Kurumsal Sorumluluk: Kişisel Verilerin Korunmasında İletişim Teknolojilerinin Kamusal Rolü. *Yeni Medya*(16), s. 268-285. doi:<https://doi.org/10.55609/yenimedya.1424182>
- Tanrıkulu, İ., & Erdur-Baker, Ö. (2020). Psychometric Properties of a Cyberbullying Inventory for University Students. *British Journal of Guidance and Counselling*, 49(3), s. 494-507. doi:<https://doi.org/10.1080/03069885.2020.1775174>
- Tapley, J., & Davies, P. (Dü). (2020). *Victimology: Research, Policy and Activism*. London: Palgrave Macmillan.
- Tathloğlu, S. S., & Gülcan, C. (2025). Dijital Mahremiyet Bağlamında Lise Öğrencilerinin Sosyal Medya Pratikleri Üzerine Karma Bir Araştırma. *Şarkiyat: İlmi Araştırmalar Dergisi*, 17(1), s. 204-221.
- Teater, B. (2015). *Sosyal Hizmet Kuram ve Yöntemleri: Uygulama İçin Bir Giriş*. (A. Karatay, Çev.) Nika Yayınevi.
- Thompson, N. (2007). *Güç ve Güçlendirme*. (Ö. Cankurtaran, Çev.) Ankara: Nika Yayınevi.
- Toblin, R. L., Schwartz, D., Hopmeyer, A., & Abou-ezzeddine, T. (2005). Social-Cognitive and Behavioral Attributes of Aggressive Victims of Bullying. *Journal of Applied Developmental Psychology*, 26(3), s. 329-346. doi:<https://doi.org/10.1016/j.appdev.2005.02.004>
- Tokunaga, R. S. (2010). Following You Home From School: A Critical Review and Synthesis of Research on Cyberbullying Victimization. *Computers in Human Behavior*, 26(3), s. 277-287. doi:<https://doi.org/10.1016/j.chb.2009.11.014>
- Topbaş, H., & Gazi, M. A. (2016). Sosyal Ağlarda Gizlilik Kaygısının Ölçülmesi: İnönü Üniversitesi Öğrencilerine Yönelik Bir Araştırma. *İnönü Üniversitesi Uluslararası Sosyal Bilimler Dergisi*, 5(1), s. 143-160.
- Töngel, E. (2020). Üniversite Öğrencilerinin Çevrimiçi Mahremiyet Farkındalıklarının Çeşitli Değişkenler Açısından İncelenmesi. *Yayınlanmış Yüksek Lisans Tezi*. Amasya Üniversitesi.

- Tran, H. G., Thai, T. T., Dang, N. T., Vo, D. K., & Duong, M. H. (2023). Cyber-Victimization and Its Effect on Depression in Adolescents: A Systematic Review and Meta-Analysis. *Trauma, Violence, and Abuse*, 24(2), s. 1124-1139. doi:<https://doi.org/10.1177/15248380211050597>
- Trompeter, N., Bussey, K., & Fitzpatrick, S. (2018). Cyber Victimization and Internalizing Difficulties: The Mediating Roles of Coping Self-Efficacy and Emotion Dysregulation. *Journal of Abnormal Child Psychology*, 46(5), s. 1129-1139. doi:<https://doi.org/10.1007/s10802-017-0378-2>
- Tuncay, T. (2009). Genç Kanser Hastalarının Hastalık Anlatılarının Güçlendirme Yaklaşımı Temelinde Analizi. *Toplum ve Sosyal Hizmet*, 20(2), s. 69-88.
- Turner, F. J. (2017). *Social Work Treatment: Interlocking Theoretical Approaches*. New York: Oxford University Press.
- Tutgun Ünal, A., & Tarhan, N. (2022). *Toplumsal Cinsiyet ve Medya Algısı*. İstanbul: Der Yayınları.
- Türk Dil Kurumu. (2025). *Türkçe Sözlük*. <https://sozluk.gov.tr/> adresinden alındı
- Türkileri, N. (2012). Ergenlerde Sanal Zorbalık: Nedenlerine İlişkin Algılar, Duygusal Tepkiler ve Baş Etme Yöntemleri İle Siber Zorbalık Statüleri Arasındaki İlişkiler . *Yayınlanmış Yüksek Lisans Tezi*. Hacettepe Üniversitesi.
- Türten, E. (2018). Yüksek Lisans Öğrencilerinin Sosyal Medyada Mahremiyet Algısı: Gümüşhane Üniversitesi İletişim Fakültesi Örneği. *Akdeniz Üniversitesi İletişim Fakültesi Dergisi*(29. Özel Sayısı), s. 143-162. doi:<https://doi.org/10.31123/akil.460160>
- Uçar, F. (2015). Facebook'ta Benlik Sunumu ve Toplumsal Cinsiyet Roller. *Selçuk İletişim*, 9(1), s. 312-338.
- UNİCEF. (2025). *Siber Zorbalık: Nedir ve Nasıl Önlenir*. Mayıs 2025 tarihinde <https://www.unicef.org/turkiye/siber-zorbal%C4%B1k-nedir-ve-nas%C4%B1l-%C3%B6nlenir> adresinden alındı
- Vale, A., Pereira, F., Gonçalves, M., & Matos, M. (2018). Cyber-Aggression in Adolescence and Internet Parenting Styles: A Study with Victims, Perpetrators and Victim-Perpetrators. *Children and Youth Services Review*, 93(1), s. 88-99.
- Varghese, M. E., & Pistole, M. C. (2017). College Student Cyberbullying: Self-Esteem, Depression, Loneliness, and Attachment. *Journal of College Counseling*, 20(1), s. 7-21. doi:<https://doi.org/10.1002/jocc.12055>

- Vatandaş, S. (2020). Mahremiyetin Dönüşümü ve İletişim Araçları. *HUMANITAS-Uluslararası Sosyal Bilimler Dergisi*, 8(16), s. 437-458.
- Vincent, D. (2022). *Mahremiyet: Kısa Bir Tarih*. (O. Düz, Çev.) Ankara: Fol Kitap.
- Von Marees, N., & Petermann, F. (2012). Cyberbullying: An Increasing Challenge for Schools. *School Psychology International*, 33(5), s. 467-476.
- Wang, J., Iannotti, R. J., Luk, J. W., & Nansel, T. (2010). Co-occurrence of Victimization from Five Subtypes of Bullying: Physical, Verbal, Social Exclusion, Spreading Rumors, and Cyber. *Journal of Pediatric Psychology*, 35(10), s. 1103-1112. doi:<https://doi.org/10.1093/jpepsy/jsq048>
- Wang, W., Vaillancourt, T., Brittain, H. L., McDougall, P., Krygsman, A., Smith, J. D., . . . Hymel, S. (2014). School Climate, Peer Victimization, and Academic Achievement: Results From a Multi-informant Study. *School Psychology Quarterly*, 29(3), s. 360-377. doi:<https://doi.org/10.1037/spq0000084>
- Weaver, J. R., Vandello, J. A., Bosson, J. K., & Burnaford, R. M. (2010). The Proof Is in the Punch: Gender Differences in Perceptions of Action and Aggression as Components of Manhood. *Sex Roles*, 62(3), s. 241-251. doi:<https://doi.org/10.1007/s11199-009-9713-6>
- West, D. (2015). An Investigation Into The Prevalence of Cyberbullying Among Students Aged 16–19 in Post-Compulsory Education. *Research in Post-Compulsory Education*, 20(1), s. 96-112.
- Westin, A. F. (1967). *Privacy and Freedom*. New York: Atheneum.
- Whitmore, E. (1988). Participation, Empowerment and Welfare. *Canadian Review of Social Policy*, 22, s. 51-60.
- Whittaker, E., & Kowalski, R. M. (2015). Cyberbullying Via Social Media. *Journal of School Violence*, 14(1), s. 11-29. doi:<https://doi.org/10.1080/15388220.2014.949377>
- Wigderson, S., & Lynch, M. (2013). Cyber and traditional Peer Victimization: Unique Relationships with Adolescent Well-being. *Psychology of Violence*, 3(4), s. 297-309. doi:<https://doi.org/10.1037/a0033657>
- Willard, N. E. (2007). *Cyberbullying and Cyberthreats: Responding to the Challenge of Online Social Aggression, Threats, and Distress*. Research Press.
- Wolke, D., Lee, K., & Guy, A. (2017). Cyberbullying: A Storm in A Teacup? *European Child & Adolescent Psychiatry*, 26(8), s. 899-908. doi:[https://doi.org/10.1007/s00787-017-0954-](https://doi.org/10.1007/s00787-017-0954-0)

- Wong, R. (2020). When No One Can Go To School: Does Online Learning Meet Students' Basic Learning Needs? . *Interactive Learning Environments*, 31(1), s. 434-450. doi:<https://doi.org/10.1080/10494820.2020.1789672>
- Wright , M. F., & Wachs, S. (2019). Adolescents' Psychological Consequences and Cyber Victimization: The Moderation of School-Belongingness and Ethnicity. *International Journal of Environmental Research and Public Health*, 16(14), s. 1-11. doi:<https://doi.org/10.3390/ijerph16142493>
- Wright, M. F., & Li, Y. (2013). The Association Between Cyber Victimization and Subsequent Cyber Aggression: The Moderating Effect of Peer Rejection. *Journal of Youth and Adolescence*, 42(5), s. 662-674. doi:<https://doi.org/10.1007/s10964-012-9903-3>
- Wright, M. F., & Wachs, S. (2020). Adolescents' Cyber Victimization: The Influence of Technologies, Gender, and Gender Stereotype Traits. *International Journal of Environmental Research and Public Health*, 17(4).
- Wu, Y., Lau, T., Atkin, D. J., & Lin, C. A. (2011). A Comparative Study of Online Privacy Regulations in the U.S. and China. *Telecommunications Policy*, 35(7), s. 603-616. doi:<https://doi.org/10.1016/j.telpol.2011.05.002>
- Yaman, E., & Peker, A. (2012). Ergenlerin Siber Zorbalık ve Siber Mağduriyete İlişkin Algıları. *Gaziantep Üniversitesi Sosyal Bilimler Dergisi*, 11(3), s. 819-833.
- Ybarra, M. L., & Mitchell, K. J. (2004). Online Aggressor/Targets, Aggressors, and Targets: A Comparison of Associated Youth Characteristics. *Journal of Child Psychology and Psychiatry*, 45(7), s. 1308-1316.
- Yenilmez, Y., & Seferoğlu, S. S. (2013). Sanal Zorbalık ve Öğretmenlerin Farkındalık Durumlarına Bir Bakış. *Eğitim ve Bilim*, 38(169), s. 420-432.
- Yıldırım, B. (2014). Bir Yaklaşımın Anatomisi: Güçlendirme. V. Işıkhani (Dü.) içinde, *Prof. Dr. Gönül Erkan'a Armağan: Sosyal Hizmet ve Mülakat*. Ankara.
- Youn, S. (2009). Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviors Among Young Adolescents. *Journal of Consumer Affairs*, 43(3), s. 389-418. doi:<https://doi.org/10.1111/j.1745-6606.2009.01146.x>
- Yörükan, T. (2024). *Sosyolojik ve Sosyal Psikolojik Görüş Açısıyla: Şehir, Konut ve Mahremiyet*. Ankara: Nobel Akademik Yayıncılık.
- Yusuf, S., Al-Majdoub, F. M., Mubin, N. N., Chaniago, R. H., & Khan, F. R. (2021). Cyber Aggression-Victimization Among Malaysians Youth. *Asian Journal of University Education*, 17(1), s. 240-260. doi:<https://doi.org/10.24191/ajue.v17i1.12616>

- Yüksel, A. H., & Kaplan, İ. (2021). Üniversite Öğrencisi Sosyal Medya Kullanıcılarının Mahremiyet Algısı. *Kurgu*, 29(1), s. 59-80.
- Yüksel, M. (2003). Mahremiyet Hakkı ve Sosyo-Tarihsel Gelişimi. *Ankara Üniversitesi SBF Dergisi*, 58(1), s. 181-213.
- Zhang, W., Yin, J., Chan, K. I., Sun, T., Jin, T., Jeung, J., & Gong, J. (2024). Beyond Digital Privacy: Uncovering Deeper Attitudes Toward Privacy in Cameras Among Older Adults. *International Journal of Human-Computer Studies*, 192. doi:<https://doi.org/10.1016/j.ijhcs.2024.103345>
- Zhu, J., Chen, Y., Su, B., & Zhang, W. (2021). Anxiety Symptoms Mediates the Influence of Cybervictimization on Adolescent Non-suicidal Self-injury: The Moderating Effect of Self-control. *Journal of Affective Disorders*, 285, s. 144-151. doi:<https://doi.org/10.1016/j.jad.2021.01.004>
- Zivnuska, S., Carlson, J. R., Carlson, D. S., Harris, R. B., & Harris, K. J. (2019). Social Media Addiction and Social Media Reactions: The Implications for Job Performance. *The Journal of Social Psychology*, 159(6), s. 746-760. doi:<https://doi.org/10.1080/00224545.2019.1578725>
- Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs.

EK 1 KİŞİSEL BİLGİ FORMU

Değerli Katılımcı,

Yukarıda adı geçen bu araştırma bilimsel bir makale çalışması olarak yürütülmektedir. Araştırma için Akdeniz Üniversitesi Etik Komisyonu'ndan gerekli onay alınmıştır.

Araştırmaya katılım kriterleri;

Akdeniz Üniversitesinde öğrenci olmak

Verilerin güvenilirliğini ve geçerliliğini artırmak amacıyla, görüşmeler yalnızca araştırmacı ve katılımcı arasında gerçekleştirilecek, kayıt altına alınacak ve üçüncü kişilerle paylaşılmayacaktır. Elde edilen bilimsel çıktılarda katılımcıların kimlik bilgileri kullanılmayacak, tüm veriler anonimleştirilerek analiz edilecektir. Araştırma kapsamında toplanan veriler yalnızca bilimsel amaçlarla kullanılacaktır.

Araştırmaya katılım tamamen gönüllülük esasına dayanmaktadır. Katılımcılar, araştırmanın herhangi bir aşamasında araştırmadan çekilme hakkına sahiptir. Çekilme talebi durumunda, ilgili katılımcıya ait veriler analiz sürecine dahil edilmeyecektir.

Sorulara vereceğiniz samimi ve dikkatli yanıtlar, doğru çıkarımlar yapılmasına ve sağlıklı sonuçlar elde edilmesine katkı sağlayacaktır. Bu bağlamda, soruları dikkatle okuyarak tüm soruları eksiksiz yanıtlamanızı önemle rica ederiz. Katkılarınız için şimdiden teşekkür eder, saygılarımızı sunarız.

Gizem ERMUMCU,

– Akdeniz Üniversitesi, Sosyal Bilimler Enstitüsü, Sosyal Hizmet Yüksek Lisans Programı

Lütfen, aşağıda yer alan her bir soruyu ilgili boşluğu doldurarak veya size en uygun olan seçeneği “X” ile işaretleyerek cevaplayınız.

1. Cinsiyetiniz : ☐ Kadın ☐ Erkek
2. Yaşınız :
3. Sınıf Düzeyiniz : ☐ Hazırlık ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ Diğer
4. Okuduğunuz Bölüm:
5. Günlük Akademik İnternet Kullanım Süreniz (saat):
6. Günlük Sosyal Medya (Whatsapp, Instagram, Facebook vb.) Kullanım Süreniz (saat):
7. Her gün İnternet kullanıyor musunuz? :☐ Evet ☐ Hayır
8. Her gün İnternet kullanıyorsanız günde yaklaşık kaç saat kullanıyorsunuz?
9. İnternete erişmek için en çok hangi cihazı ya da cihazları kullanıyorsunuz? (Birden çok seçenek işaretleyebilirsiniz.)
 - ☐ Masaüstü bilgisayar
 - ☐ Laptop/ notebook
 - ☐ Akıllı Telefon
 - ☐ Tablet
 - ☐ İnternet bağlantılı TV
 - ☐ Diğer belirtiniz...
10. İnterneti spesifik olarak hangi vakit geçirme amaçları için kullanıyorsunuz? (birden fazla seçenek işaretleyebilirsiniz.)
 - ☐ E hizmetler (internet bankacılığı, hastane işleri...)
 - ☐ İnternet'te haberler, gazeteler, sağlık, moda vb. ile ilgili bilgi arama/okuma
 - ☐ Çevrim içi alışveriş / satış yapmak (eBay, Gittigidiyor, Hepsiburada, Trendyol vb.)
 - ☐ Oyun oynama (Candycrush vb.)
 - ☐ Eğlence (Müzik dinleme, Video/film izleme, (Youtube, Netflix, Fızy, Spotify, Puhutv, Çevrim içi dizi/film siteleri vb.)
 - ☐ Instagram, Facebook gibi sosyal platformlarda fotoğraflara bakma / video izleme / paylaşım yapma
 - ☐ Öğrenme amaçlı, eğitimle ilgili bir şeyler paylaşma/ erişme
 - ☐ Kindle vb. üzerinden kitap okumak.
 - ☐ İlgi alanlarınıza yönelik web sitelerinden bilgi okuma (Onedio, Listelist, Bilimfili, Düşünbil vb.)
11. İnterneti sosyal amaçlarla kullanıyorsanız, spesifik olarak hangi sosyal amaçlar için kullanıyorsunuz? (birden fazla seçenek işaretleyebilirsiniz.)
 - ☐ Sosyal medya platformlarında doğrudan mesaj (DM) aracılığıyla etkileşime geçmek (Facebook, Twitter, Instagram vb. üzerinden)
 - ☐ WhatsApp aracılığıyla sosyalleşme/ muhabbet etme amaçlı iletişim kurmak
 - ☐ Sosyal medya üzerinden, yapılan paylaşımlara diğer insanlarla etkileşim kurmak için yorum yapmak. (Facebook, Twitter, Instagram vb.)
 - ☐ İlgi alanınıza yönelik İnternet forumlarında diğer insanlarla iletişim kurmak için mesaj (post) paylaşmak (Eksisözlük vb.)
 - ☐ Diğer insanlarla iletişim kurabilmek için ilgi alanlarınıza yönelik web sitelerinde yapılan paylaşımlara yorum yapmak (Onedio vb.)
 - ☐ Flört uygulamaları aracılığıyla iletişim kurmak (Tinder, Match vb.)
12. En sık kullandığınız sosyal medya platformunu işaretleyiniz. (birden fazla seçenek işaretleyebilirsiniz.)
 - ☐ Instagram
 - ☐ WhatsApp
 - ☐ YouTube
 - ☐ Twitter
 - ☐ TikTok
 - ☐ Facebook
 - ☐ Telegram
 - ☐ Snapchat
 - ☐ Diğer: _____

EK 2 ÜNİVERSİTE ÖĞRENCİLERİ İÇİN SİBER ZORBALIK/MAĞDURİYET ÖLÇEĞİ

Aşağıda sıralanan davranışları **SON 6 AY** içerisinde ne sıklıkla yaptığınızı **BEN YAPTIM** bölümüne işaretleyiniz.

Bu durumlara ne sıklıkla maruz kaldığınızı ise **BANA YAPILDI** bölümüne işaretleyiniz.

Lütfen cevabınızı **HER İKİ BÖLÜM** (BEN YAPTIM ve BANA YAPILDI) için AYRI AYRI işaretlemeyi **unutmayınız.**

0 ☐ Hiç

1 ☐ Bir Kez

2 ☐ İki-üç Kez

3 ☐ Üçten Çok

	BEN YAPTIM ↓				BANA YAPILDI ↓			
	Hiç	Bir Kez	İki-üç Kez	Üçten Çok	Hiç	Bir Kez	İki-üç Kez	Üçten Çok
1. İzin almadan, kişisel bilgisayar veya akıllı telefondaki bilgileri (dosya, fotoğraf, yazılı mesaj kayıtları vb.) almak	0	1	2	3	0	1	2	3
2. İnternet ortamında başkasının kimliğiyle izinsiz paylaşımda bulunmak	0	1	2	3	0	1	2	3
3. Görüntülü yapılan özel bir görüşmeyi, karşı tarafın haberi olmadan başkasına izlettirmek	0	1	2	3	0	1	2	3
4. İnternet ortamında yapılan paylaşımlara (yorum, fotoğraf, video, bilgi) utandırıcı, kırıcı yorumlar yapmak	0	1	2	3	0	1	2	3
5. İnternette tehdit içeren, utandırıcı, kırıcı mesajlar göndermek	0	1	2	3	0	1	2	3
6. İnternet şifrelerini ele geçirerek erişimi engellemek	0	1	2	3	0	1	2	3
7. SMS aracılığıyla tehdit edici, utandırıcı, kırıcı mesajlar göndermek	0	1	2	3	0	1	2	3
8. İnternette, cinsiyetini farklı göstererek karşı tarafı kandırmak	0	1	2	3	0	1	2	3
9. Sanal ortamda dedikodu veya söylenti yaymak	0	1	2	3	0	1	2	3
10. Sanal ortamda birilerine küfretmek	0	1	2	3	0	1	2	3
11. Küçük düşürücü bir mesajı, fotoğrafı veya video görüntüsünü sanal ortamda izinsiz paylaşmak	0	1	2	3	0	1	2	3

EK 3 ÇEVİRİMİÇİ MAHREMİYET FARKINDALIK ÖLÇEĞİ

Aşağıdaki ifadeleri okuyarak **son iki ay** boyunca çevrim içi ortamda başkalarıyla etkileşime girerken, bu ifadelerin sizde **ne sıklıkla** gerçekleştiğini derecelendiriniz.

(0 = Hiçbir zaman, 1 = Nadiren, 2 = Bazen, 3 = Sık sık, 4 = Çok sık)

1. Arkadaşlarımla veya yakınlarımla yaptığım yazışmaların ekran görüntülerini izin almaya gerek duymadan paylaşıyorum.
2. Başkalarına ait bilgi, resim, video vb. içerikleri çevrim içi ortamlarda izin almaya gerek duymadan paylaşıyorum.
3. Çevrim içi ortamlarda kullandığım parolaların güçlü olmasına (büyük-küçük harf, rakam, özel karakterler ve en az 8 karakter kullanımıyla) dikkat ederim.
4. Çevrim içi ortamlarda paylaştığım bilgilerin şirketler, devlet kurumları veya bilgisayar korsanları tarafından kullanılabileceğinin farkındayım.
5. Çevrim içi ortamlarda tanımadığım kişilerden gelen mesaj veya e-postaların güvenlik riski oluşturup oluşturmadığını anlarım.
6. Çevrim içi ortamlarda tanımadığım kişilerin beni takip etmesine veya arkadaş olmasına izin veririm.
7. Çevrim içi ortamlarda tanımadığım kişilerle iletişim kurarım.
8. Çevrim içi ortamlarda tanımadığım kişilerle kişisel bilgilerimi (adres, doğum tarihi, yaş, iş, telefon vb.) paylaşıyorum.
9. Çevrim içi platformlarda paylaştığım bilgilerin kötü niyetli kişiler tarafından kullanılabileceğinin farkındayım.
10. E-posta veya sosyal ağlardan aldığım mesajların içeriğinin güvenilir olup olmadığını anlarım.
11. İnternet sitelerinin kullandığı çerez (cookies) dosyaları hakkında bilgim vardır.
12. İnternet sitelerinin ve mobil uygulamaların güvenlik sertifikalarını ve veri şifreleme yöntemlerini kontrol ederim.
13. Kullandığım çevrim içi ortamlarda (sosyal ağlar, alışveriş siteleri, oyunlar vb.) hesabımın gizlilik ayarlarını yaparım.
14. Kullandığım çevrim içi platformların gizlilik ayarlarını ve bildirimlerini kontrol ederim.
15. Mobil cihazıma uygulama yüklerken uygulamanın hangi izinleri talep ettiğine dikkat ederim.
16. Web tarayıcısındaki eklentilerin hangi bilgilere erişeceğine dikkat ederim.
17. Ziyaret ettiğim web sitelerinin güvenliğini kontrol ederim.

ÖZGEÇMİŞ

Adı ve SOYADI	Gizem ERMUMCU
EĞİTİM DURUMU	
Lisans	Gazi Üniversitesi, Sağlık Bilimleri Fakültesi, Sosyal Hizmet (2018-2022)
Yüksek Lisans	Akdeniz Üniversitesi, Sosyal Bilimler Enstitüsü Sosyal Hizmet Bölümü (2022-)
Tez Konusu	Üniversite Öğrencilerinde Dijital Mahremiyet Farkındalığı ve Siber Mağduriyet Arasındaki İlişkinin İncelenmesi
Yabancı Dil/Diller	İngilizce