

DİJİTAL MAHREMİYET BAĞLAMINDA LİSE ÖĞRENCİLERİNİN SOSYAL MEDYA PRATİKLERİ ÜZERİNE KARMA BİR ARAŞTIRMA

Sevra Su TATLIOĞLU

Bağımsız Araştırmacı, Eskişehir/Türkiye
sstatlioglu@gmail.com, ORCID: 0000-0001-5236-0161

Cem GÜLCAN

Bağımsız Araştırmacı, Eskişehir/Türkiye,
cemgulcan26@gmail.com, ORCID: 0000-0003-0771-3030

Article Types / Makale Türü: Research Article / Araştırma Makalesi

Received / Makale Geliş Tarihi: 27/08/2024, Accepted / Kabul Tarihi: 07/01/2025

Doi: <https://doi.org/10.26791/sarkiat.1539595>

Bu çalışma Anadolu Üniversitesi Araştırma ve Yayın Kurulu'ndan alınan 03.06.2020 tarihli, 31269 kodlu Etik Kurul onayı ve Eskişehir İl Milli Eğitim Müdürlüğü'nden alınan "17.09.2020" tarihli, "88074293-605.01-E.12930413" sayılı onay ile Anadolu Üniversitesi'nde gerçekleştirilen "Dijital Toplumda Mahremiyet Algısının Dönüşümü: Eskişehir'de Öğrenci, Öğretmen ve Ebeveynlerin Mahremiyet Farkındalıklarının Geliştirilmesi" Bilimsel Araştırma Projesi'nden üretilmiştir.

Dijital Mahremiyet Bağlamında Lise Öğrencilerinin Sosyal Medya Pratikleri Üzerine Karma Bir Araştırma

Öz

Dijital teknolojilerin hızla gelişmesi, bireylerin bu teknolojileri güvenli kullanma yeteneklerini geride bırakmakta, bu da dijital mahremiyet kavramını önemli kılmaktadır. Lise öğrencileri, dijital dünyanın en aktif kullanıcıları olup aynı zamanda potansiyel risk gruplarını oluşturmaktadır. Bu çalışmanın amacı, lise öğrencilerinin dijital mahremiyet bilinci ve kaygı düzeylerini sosyal medya pratikleri üzerinden incelemektir. Araştırmada karma yöntem kullanılmıştır. Karma yöntemler, istatistiki verilerin yanında derinlemesine bilgiler de sunan yapıya sahiptir. Bu doğrultuda; Eskişehir’deki çeşitli liselerden 1371 öğrenciyle yapılan anket çalışmasıyla nicel veriler toplanmış, ANOVA analiziyle hipotezler test edilmiştir. Bulgulara göre, öğrencilerin dijital mahremiyet bilinci, sosyal medya kullanım sıklığına göre farklılaşmakta; kullanım arttıkça bilinç seviyesi düşmektedir. Dijital mahremiyet kaygısı ise cinsiyet ve sosyal medya kullanım sıklığına göre farklılık göstermektedir. Kız öğrenciler erkeklere göre daha fazla kaygı duymakta; kullanımları arttıkça ise kaygı seviyesi azalmaktadır. Nitel aşamada ise, 15 öğrenciyle yapılan yarı yapılandırılmış görüşmelerde dijital mahremiyet pratikleri altı ana kategoride incelenmiştir: güvenlik önlemleri, tanınmayan kişiler araştırma, kişisel paylaşımlara dikkat etme, kişisel bilgilere erişime karşı önlemler, gözetlenme endişesi, önleme dayalı endişesizlik ve kaygı duymama. Kız öğrencilerin dijital mahremiyet kaygılarının toplumsal cinsiyet normlarıyla şekillendiği tespit edilmiştir.

Anahtar Kelimeler: Mahremiyet, Dijital Mahremiyet, Mahremiyet Kaygısı, Mahremiyet Bilinci, Sosyal Medya.

A Mixed-Methods Study On High School Students’ Social Media Practices In The Context Of Digital Privacy

Abstract

The rapid development of digital technologies has outpaced individuals’ ability to use these technologies safely, making the concept of digital privacy increasingly important. High school students are among the most active users of the digital world and also constitute a vulnerable risk group. The aim of this study is to examine high school students’ awareness of and concerns about digital privacy through their social media practices. A mixed-methods approach was used, which combines statistical data with in-depth information. Accordingly, quantitative data was collected through a survey of 1,371 students from various high schools in Eskişehir, and hypotheses were tested using ANOVA analysis. The findings reveal that students’ awareness of digital privacy varies according to social media usage frequency, with awareness decreasing as usage increases. Digital privacy concerns also differ based on gender and social media usage frequency. Female students experience more concerns than male students, and their concern levels decrease as usage increases. In the qualitative phase, semi-structured interviews with 15 students explored digital privacy practices, categorized into six main themes: security measures, investigating unknown individuals, being cautious with personal shares, taking precautions against access to personal information, concerns about surveillance, and a lack of concern based on preventive measures. It was found that female students’ concerns about digital privacy are shaped by gender norms.

Keywords: Privacy, Digital Privacy, Privacy Concern, Privacy Awareness, Social Media.

GİRİŞ

Teknolojinin gelişimi, tarih boyunca insan hayatını sosyal, kültürel, ekonomik ve politik açıdan dönüştürmüştür. İnsanlığın bilgi havuzuna eklenen her bir bilgi tuğlası, yeni bir teknolojinin inşasına katkı sağlamıştır. Tarımdan ya-
pay zekaya kadar her teknoloji, insanlığın ilerlemesiyle ortaya çıkmıştır; teknoloji insanlığı, insanlık da teknolojiyi
şekillendirmiştir. Bugünün dijital çağında ise değişen gündelik yaşam pratikleriyle beraber gizlilik, güvenlik ve mah-
remiyet gibi kavramların önemi giderek artmaktadır.

Dijital teknolojilerin beraberinde getirdiği ve çözülmesi gereken düğümlerden belki de en önemlisi mahremiyet
problemidir. Yüzlerce yılda şekillenen sosyal, kültürel ve dini normlar, insanların mahremiyet algısını şekillendir-
mektedir. Mahremiyet kavramı geleneksel olarak gizlilik ve özel alanla ilişkilendirilmektedir. Özel ve kişisel olanla
ilgili belirli bir sınıra işaret eden bu kavram dijital alanda dönüşüme uğrayarak çizgileri daha belirsiz bir noktada
duran dijital mahremiyet kavramını ortaya çıkarmaktadır. Dijital teknolojiler, normların şekillenmesinden çok daha
hızlı değişim göstermektedir. Bu bağlamda dijital mahremiyet kavramı, kişisel verilerin toplanması, depolanması,
işlenmesi ve paylaşılması süreçlerinde algoritmalar ve gözetimi içeren çok katmanlı bir yapıya işaret etmekte ve
burada bireylerin kişisel bilgilerinin üzerindeki kontrol ve denetimini ifade etmektedir. Dolayısıyla dijital dünyanın,
mahremiyet kavramını dönüştürdüğü ve mahremiyete dair tartışmaları gündeme taşıdığı açık bir gerçektir.

Dijital mecralardaki mahremiyet problemlerinin en büyük odak noktasının da gelişim çağındaki çocuklar ve er-
genler olduğunu belirtmek gerekmektedir. Gerek hukuki gerekse psikolojik açıdan 18 yaşının altındaki bireylerin
“mahremiyet” problemleri, erişkin bireylerinkine nazaran çok daha travmatik sonuçlara yol açabilmektedir. Dolayı-
sıyla bu yaş grubunun dijital alanda yaşadığı mahremiyet kaygılarına ve farkındalıklarına odaklanmak, erken yaşta
önlem alabilmek adına oldukça önemlidir. Bu doğrultuda bu çalışmanın eksenini, lise öğrencilerinin dijital mahre-
miyet algıları ve pratikleri oluşturmaktadır. Özellikle lise öğrencileri, dijital dünyada aktif kullanıcılar olup, yüksek
risk grupları arasında yer almaktadır. Araştırma, öğrencilerin öncelikle dijital mahremiyet bilinç ve kaygı seviyelerini
tespit etmeyi, ardından bunlarla bağlantılı pratiklerini ortaya koymayı hedeflemektedir. Bu bağlamda çalışma, genç-
lerin dijital mahremiyet algılarını ve bu konudaki bilinç düzeylerini ortaya koyması, bu alanda farkındalığı artırmayı
hedeflemesi bakımından önem arz etmektedir. Ayrıca dijital mahremiyet konusunda büyük rol düşen aile ve eğitim
kurumlarına yönelik yol göstericiliği de araştırmayı önemli kılmaktadır.

Araştırma kapsamında açımlayıcı sıralı karma desen kullanılmıştır. Buna paralel olarak araştırmanın ilk aşaması
olan nicel aşamada lise öğrencileriyle anket çalışması gerçekleştirilmiştir. Bu anket çalışmasının ardından ortaya
çıkan verilerle ikinci aşama olan nitel çalışma gerçekleştirilmiştir. Bu aşamada ise öğrencilerle yarı yapılandırılmış
derinlemesine görüşmeler gerçekleştirilmiş ve bu görüşmelerden elde edilen veriler yorumlanmıştır. Bu çalışma kap-
samında, nicel araştırma yöntemi kullanılarak Eskişehir’ın çeşitli bölgelerinde bulunan ve farklı tiplerdeki 10 liseden
toplam 1371 öğrenci ile anket çalışması gerçekleştirilmiştir. Nitel aşamada ise 15 öğrenci ile yarı yapılandırılmış
görüşmeler gerçekleştirilmiştir. Elde edilen nicel ve nitel bulgular dijital mahremiyet kaygısı ve bilinci arasında be-
raberinde gelen çeşitli toplumsal dinamiklerle ilişki kurularak değerlendirilmiştir.

1. Dijital mahremiyet kavramı

Medya ve iletişim teknolojilerindeki hızlı ilerleme gündelik hayatın içerisindeki birçok kavramın yeniden ele
alınması gerekliliğini ortaya çıkarmaktadır. Bugün modern yaşamın bir simgesi haline gelen dijitalleşme, bireylerin
çeşitli uygulamalar ve sosyal ağlarla kişisel ve sosyal alanını paylaştığı, eğlendiği, sosyalleştiği, gündelik pratiklerini
gerçekleştirdiği geniş bir alan sunmaktadır. Bu doğrultuda kamusal ve özel alan ayrımının da silikleşmeye başlaması
mahrem ve mahrem olmayan arasındaki sınırların da yeniden şekillenmesine yol açmaktadır.

Mahremiyet geleneksel olarak; gizli, özel olanla ilişkilendirilirken dijital ortamda bu kavram daha esnek ve çok
katmanlı bir hal almaktadır. Mahremiyet kavramı TDK’da “gizlilik” olarak tanımlanmaktadır (<https://sozluk.gov.tr>,
2024). Ancak, daha kapsamlı bir yaklaşımla Altman (1977: 68), mahremiyetin kültürel ve bağlamsal olarak değişebi-
len bir kavram olduğunu ve bireylerin etkileşimlerini düzenleme becerileriyle doğrudan ilişkili olduğunu belirtmek-
tedir. Diğer yandan, Westin (1967) mahremiyeti, “bireylerin, grupların ve kurumların, kendileri hakkındaki bilgilerin
başkalarına ne zaman, nasıl ve ne ölçüde iletileceğini kendilerinin belirleme hakkı” olarak tanımlamaktadır. Türk ve
Demirci (2016, 519) çalışmasında mahrem alanı; bireyin kendi sınırlarını kendisinin belirlediği, neyi kiminle ne ka-
dar paylaşacağına karar verdiği, kendine has etik kodları olan özel bir alan olarak ifade etmektedir. Tüm bu tanımlara
bakıldığında mahremiyet kavramının yalnızca fiziksel alanı değil, aynı zamanda bireylerin kişisel bilgilerini, düşün-
celerini ve ilişkilerini de kapsadığı görülmektedir.

Mahremiyet hakkı, genel olarak üç ana türde incelenebilir: bölgesel mahremiyet, bireysel mahremiyet ve enformasyonel mahremiyet. Bölgesel mahremiyet, bir bireyin çevresindeki fiziksel alanın korunmasını ifade eder. Bireysel mahremiyet, kişinin duygusal ve/veya fiziksel açıdan rahatsız edici müdahalelerden korunmasını kapsar. Enformasyonel mahremiyet ise, kişisel verilerin toplanması, depolanması, işlenmesi ve paylaşılması süreçlerinde bireyin kontrol sağlayarak bilgilerin korunmasını hedefler (Fischer-Hübner, 1998, 422). Tam da bu noktada enformasyonel mahremiyetle ilişkili olan dijital mahremiyet kavramı karşımıza çıkmaktadır. Nispeten yeni bir kavram olan dijital mahremiyet, fiziksel sınırların ötesine geçerek sanal dünyaya uzanmaktadır. Bu kavram kısaca sosyal medya platformları, arama motorları ve çevrimiçi gerçekleştirilen tüm işlemler de dahil olmak üzere çevrimiçi alanlarda kişisel bilgilerin korunmasıyla ilişkilidir (Solove, 2021, 32). Geleneksel mahremiyet kavramı öncelikle özel alan, fiziksel gözetim ve kişisel sınırlar gibi somut yönlerle ilgilenirken, dijital mahremiyet; veri toplama, algoritmalar ve çevrimiçi gözetimle ilgili karmaşık sorunlara işaret etmektedir (Tüfekci, 2015, 210).

Günümüzde, mahremiyetin özel alan olarak tanımlanan sınırları dijital alanda daha belirsiz hale gelmiştir. Artık herkesin her türlü bilgisini paylaşmasının yanı sıra paylaşılan her datanın da depolandığı, işlendiği ve kullanıldığı geniş bir dijital ortamdır söz edilmektedir. Dolayısıyla dijital mahremiyet, kullanıcıların dijital ortamda hangi verilerinin korunacağı ve/veya kullanılacağına dair kontrolünü ifade eden bir kavramdır. Bu nedenle, dijital mahremiyet ihlalleri kişisel bilgilerin kötüye kullanımı, özel hayatın gizliliğinin ihlali, sosyal mühendislik, dolandırıcılık ve gözetim gibi çeşitli biçimlerde kendini göstermektedir (Aslanyürek, 2015, 22-23).

Dijital dünyada aktif katılım ve paylaşım, etkileşimlerin büyük ölçüde sosyal medya platformları üzerinden beğeniler ve takipler üzerinden gerçekleşmesi gibi durumlarla birleştiğinde, çevrimiçi dünyada birçok fotoğraf, video, metin ve kişisel bilginin mahremiyet gözetilmeden dolaşımına zemin hazırlamaktadır. Özellikle sosyal medyanın etkileşimli doğasında insanlar yalnızca özel hayatlarını paylaşmakla kalmamakta, aynı zamanda inşa ettikleri dijital kimliklerini de kamuya açmaktadır. Böylelikle, bireyler dijital alanda hayatlarının hangi yönlerini ifşa edeceklerini ve hangilerini gizleyeceklerini belirledikçe mahremiyetin sınırlarını da kendileri belirlemektedir. Bu nedenle, sosyal medyada kendini sunma süreci, kullanıcıların kamusal ve özel benliklerini sürekli müzakere etmesiyle mahremiyetin dönüşümünde önemli bir faktör haline gelmektedir (Bilbil ve Atalay, 2020, 180).

Bu bağlamda dijital mahremiyet kavramı, teknolojiyle birlikte gelişen ve fiziksel mahremiyetin ötesine geçen sanal ortamda kişisel bilgilere, veriye ve dijital kimliğe odaklanmaktadır (Solove, 2008, 33). Dijital mahremiyet, yalnızca kişinin çevrimiçi etkileşimlerinde değil, aynı zamanda kullanıcıların dijital ayak izlerini takip eden algoritmalar ve veri toplama uygulamaları gibi tehditlerle de doğrudan ilgilidir. Dolayısıyla bu durum dijital mahremiyetin geleneksel mahremiyet anlayışından farklı olarak daha fazla esneklik ve kontrol ihtiyacı doğurduğunu ortaya koymaktadır.

Öte yandan, Marwick ve boyd (2014) insanların tıpkı kamusal alanda olduğu gibi ağ tabanlı kamusal ağlarda da mahremiyet arayışının olduğunu ve bunu sağlamaya yönelik önlemler aldıklarını belirtmektedir. Dijital mahremiyet ihlalleri; büyük veri analizinin gelişimiyle birlikte bireylerin bilgilerinin depolanması, dijital ayak izlerinin takip edilmesi ve kullanıcıların profillerinin analiz edilmesi ile farklı biçimlerde de gerçekleşmektedir. Kişiyi özel sunulan reklamlar bunun en belirgin örneğidir (Eroğlu, 2018, 132). Bu gibi gündelik pratiklerle de mahremiyet ihlalleri fark edilmeyecek biçimde gerçekleşebilmekte, sıradanlaşmakta, hatta sosyal medyadaki paylaşım pratikleri ile zaman zaman gönüllü, karşılıklı bir mahremiyet ihlaline dönüşmektedir (Arık ve Arık, 2020, 454).

2. Dijital mahremiyet tehditleri ve kaygı

Dijital mahremiyet kavramının sınırlarının çizilmesinin oldukça zor olduğu günümüzde; hangi bilgilerin mahrem kategorisine girdiği, gündelik hayatın mahrem kabul edilen pratiklerinin nasıl kamusallaştığı, bu verilerin kimlerle paylaşıldığı, bu paylaşımların nasıl tehlikeler yarattığı gibi konular gündeme gelmektedir. Westin (1967) mahremiyeti tehdit eden unsurları “ifşa”, “merak” ve “gözetleme” olarak sıralamaktadır. Benzer şekilde Berkup (2015, 25) dijital mahremiyeti tehdit eden unsurları “kişisel bilgilere kolay erişim”, “ifşa” ve “gözetim” olarak sıralamaktadır.

Mahremiyet ihlallerine zemin hazırlayan gözetim/ gözetleme pratikleri; Foucault’un panoptikon kavramına dayanmakla birlikte bugünün dijital çağında Poster’in süper-panoptikon kavramı dijital gözetlemeye işaret etmektedir. Dijital araçlarla, dijital ortamda gerçekleştirilen; iletişim, alışveriş, bankacılık işlemleri, sosyalleşme, eğlenme gibi birçok etkinlik bireylerin bilgilerini kendi rızalarıyla vermelerini gerektirmektedir. Böylelikle insanların gönüllü olarak paylaştıkları kişisel bilgileri, konumları, adresleri vs. dijital dünyada depolanmakta ve rahatlıkla paylaşılabilir (Kalaman, 2019, 582). Dolayısıyla dijital gözetimde insanlar gönüllü olarak kendi bilgilerini paylaşmakta ve bunlar üzerinden etkileşim sağlayabilmektedir. Mahremiyet kaygısından ziyade gönüllü bir görünürlük söz konu-

sudur (Han, 2017, 12). Bireyler dijital ayak izlerinin nasıl işlendiğine dair derin bir bilgiye sahip olmamakla beraber sosyal ağlarda aktif paylaşım yapmaya devam etmektedir. Sosyal ağların sunduğu yeni kamusal alanlarda insanlar kendi sanal kimliklerini yaratırken, başkalarına da kendisini gözetleme iznini kendi rızasıyla vermektedir. Aynı zamanda kendisi de benzer şekilde bu gözetim ilişkisinde gözetleyen konumunda olabilmektedir (Özdemir, 2020, 85-86). Ancak bireylerin bu şekilde sınırsız bir gözetleme döngüsüne girebildiği dijital çağda, mahremiyetin kişisel kontrolü ve özerkliğin kaybı konusunda endişeler de giderek artmaktadır. Bireyler bu tehditlerin daha fazla farkına vardıkça, artan bir savunmasızlık ve güçsüzlük hissi ortaya çıkabilmektedir (Fuchs, 2018, 218).

Teşhir ise mahremiyet sınırlarını önemli ölçüde etkileyen, tıpkı siber zorbalık gibi psikolojik etkilere sebep olabilen ve bir yandan da sosyal medyada bir kültür haline dönüşen bir davranış biçimidir. “Gösterme, sergileme, herkese duyurma” gibi anlamlara sahip olan teşhirde, kişinin mahremiyetini sergilemesi söz konusudur. Sosyal medya da bu işleyişte bireyi teşhire teşvik eden bir manipülasyon aracı işlevi görmektedir. Bireyler, diğer sosyal medya kullanıcılarından ayrılmak için bu ortamı bir teşhir dünyası olarak kullanabilmektedir; öyle ki kullanıcılar burada gönüllü olarak kendi mahremiyetlerini ifşa etmektedirler ve bu davranışın da motivasyonlarından en güçlüleri popüler olma, şöhret olma, kendini kanıtlama arzusudur (Budak, 2018, 152). Teşhirin en belirgin özelliği, sergileme/gösterme davranışı gerçekleştirilirken görülmenin bilinçli olarak arzulanmasıdır. Dijital kimliğini; sosyal medyada sergilediği giysileri, bedeni, aksesuarları, evi, gittiği tatil yerleri, hobileri vb. ile yansıtmaya çalışan birey bunları bir gösteri nesnesine dönüştürmekte ve bir statü sembolü haline getirmektedir. Sıradan şeyleri devasa gösteriler olarak sunan bireyler, özellikle de Instagram, Youtube, TikTok gibi mecralarda yoğun biçimde fotoğraf ve video paylaşarak, kimlik ve imajlarını sergilemektedir (Çağlak, 2020, 16). Bu süreçte bireyler kişisel bilgilerini paylaşmanın sonuçlarını genellikle tam olarak kestirememekte ve dijital platformların sunduğu etkileşim ve pratikler nedeniyle mahremiyetlerini göz ardı edebilmektedir. Bu paradoks, yani görünürlük ve kişisel bilgilerin kontrolü arasındaki dengeyi sağlamada yaşanan zorluk, dijital mahremiyetin temelindeki sorunu yansıtmaktadır (Acquisti, Brandimarte ve Loewenstein, 2020, 741). Bu bağlamda, dijital dünyada kişisel verilerin toplanması ve izinsiz kullanımı da giderek artmakta ve mahremiyet endişeleri de büyük bir sorun haline gelmektedir. Bireylerin mahremiyet konusundaki endişelerinin temelinde, kişisel verilerinin nasıl kullanıldığına ilişkin belirsizlik ve bu konuda kontrol sağlamada karşılaştıkları zorluklar bulunmaktadır. Dijital platformlar büyük miktarda kullanıcı verisi toplamaya devam ettikçe, bireylerin özerklikleri ve kişisel sınırları sıklıkla tehlikeye girmekte ve bu da gözetim ve veri kullanımı konusunda artan endişelere yol açmaktadır (Connor ve Doan, 2019, 47).

Tüm bu çerçevede dijital mahremiyetin, hızla gelişen dijital teknolojilerin beraberinde getirdiği önemli bir sorun olduğunu gözler önüne sermektedir. Dijital çağda kişisel verilerin korunması konusunda geleneksel yöntemler yetersiz kalmaktadır. Dijital teknolojilerin kullanımının artmasıyla birlikte, kişisel verilerin toplanması ve işlenmesi daha karmaşık bir hal almış, bu da mahremiyetin korunmasını güçleştirmiştir. Kişisel verilerin çevrimiçi ortamda toplanması kullanıcıların rızası dışında gerçekleşebilmekte ve bu durum ciddi mahremiyet ihallerine yol açabilmektedir. Özellikle sosyal medya ve büyük veri analizlerinin mahremiyet üzerindeki etkileri giderek artmaktadır. Bu nedenle dijital dünyada mahremiyetin korunması için teknolojik yeniliklerin hızına paralel olarak gelişen yasal ve etik standartların ortaya koyulması ve sürekli güncellenmesi önemli bir gerekliliktir (Romansky & Noninska, 2020, 5290- 5292).

Bugün dijital mahremiyet ihlalleri toplumun temel bir sorunu olmakla beraber, çalışmanın da örneklemini oluşturan çocukların ve ergenlerin dijital ortamda geçirdikleri vakit göz önünde bulundurulduğunda mahremiyet ihlallerine maruz kalmaları kaçınılmaz olmaktadır. Özellikle bu çağa doğmuş, dijital dünyanın doğal öznesi olan çocukların/ergenlerin maruz kalabileceği dijital tehlikeler endişe verici bir tartışma konusudur. İnternetin halihazırdaki tehlikeleri, çocukların maruz kalmaları durumunda kalıcı hasarlar verebilmektedir. Bu bağlamda, dijital dünyada çocukların karşılaşabileceği tehlikelere; kişisel bilgilerin ifşası, taciz ve pedofili tehlikesi, siber zorbalık, rencide edici yorumlar ve paylaşımlar, uygunsuz içeriklere maruz kalma gibi çeşitli örnekler verilebilir (Akça ve Çilekçiler, 2019, 404). Öte yandan, çocuklar ve ergenlerin sosyal ağları kullanış biçimleri ve kendi paylaşımları da mahremiyetleri açısından riskler barındırabilmektedir. Yaşadığımız dönemin sunduğu dijital dünyada beğenilme, merak etme, şöhret olma gibi arzular gelişim çağındaki çocukların mahremiyet algısını biçimlendirmekte ya da esnetmektedir.

Çocuk ve ergenlerde farklılaşan mahremiyet algısı kendini, dijital dünyaya doğan neslin kişisel bilgilerini ve görüntülerini paylaşırken daha az kaygılı hareket etmesinde göstermektedir. Birçok çalışma sosyal paylaşım ağlarında teknolojiyle büyüyen bireylerin paylaşımları konusunda mahremiyet çekincelerinin düşük düzeyde olduğunu, kimisinin de zaten güvenlik ve gizlilik ayarlarının bilincinde olarak paylaşımlarında bir kısıtlama hissetmediğine işaret etmektedir (Barkuş ve Koç, 2019, 38). Yıldız da (2012, 530); teknolojinin içine doğan dijital yerlilerin genel veya özel herhangi bir bilgi ve görüntü paylaşımında neredeyse hiçbir çekince yaşamadığını öne sürmekte ve bu ne-

denle dijital yerlilerin mahremiyet algısının sorgulanması gerektiğini ifade etmektedir. Prensky (2001, 3) tarafından kavramsallaştırılan “dijital yerliler”; dijital teknolojilerin içine doğan, internet, sosyal medya ve mobil cihazlar gibi dijital araçları ve alanları yaşamlarının doğal bir parçası olarak gören ve bunları ustaca kullanan kişilerdir. Dolayısıyla dijital becerileri dijital yerlilerin çalışma, öğrenme ve sosyalleşme şekillerini de etkilemektedir. Bu bağlamda bu çalışmada; dijital dünyaya doğan, dijital araçlara hâkim, bilgiye hızlı erişim, çoklu görev yapabilme ve dijital iletişimde yetkinlik gibi özelliklere sahip olan, dijital yerli kategorisine giren lise öğrencilerinin dijital mahremiyet kaygısı ve bilinçlerine ilişkin bir araştırma yapılmıştır. Çalışmada, dijital mahremiyet bilinci ve kaygısının sosyal medya kullanım sıklığı, kullanım pratikleri ve cinsiyete göre belirgin bir biçimde farklılaştığı ortaya konulmuştur.

3. Yöntem

Bu başlık altında gerçekleştirilen araştırma hakkında bilgiler yer almaktadır. Araştırmanın amacı, sınırlılıkları, yöntem ve veri toplama ile ilgili adımlar paylaşılmıştır.

3.1. Araştırmanın amacı

Bu çalışmanın gerçekleştirilmesindeki temel amaç lise seviyesindeki öğrencilerin, dijital yaşantılarında mahremiyetlerinden ne ölçüde kaygı duydukları ve bununla ilgili ne tür tutumlar sergilediklerini keşfetmektir. Bu kapsamda, dijital mahremiyet ve lise seviyesindeki öğrencilerin dijital mecralardaki mahremiyet bilinçleri ve kaygı seviyelerinin, cinsiyet, sosyal medya kullanım sıklığı ve kullanım pratiklerine göre farklılaşıp farklılaşmadığını ortaya koymak amaçlanmaktadır.

3.2. Araştırmanın sınırlılıkları

Araştırma, Eskişehir’deki lise öğrencileri ile sınırlandırılmıştır. Mevcut çalışma mahremiyet algısını dijital boyutta ele almış ve bu kapsamla sınırlandırılmıştır.

3.3. Araştırma evreni ve örnekleme

Araştırmanın evrenini Eskişehir’de eğitimini sürdüren lise öğrencileri oluşturmaktadır. Bu evren toplam 42853 kişiden oluşmaktadır. Bu kapsamda nicel araştırma gerçekleştirilen örneklem grubu ise Eskişehir’in farklı bölgelerinde bulunan ve farklı türden 10 lisede öğrenim gören toplam 1371 öğrenciden meydana gelmiştir. Bu bilgiler ışığında, örneklemin evrene oranı %3,2 olarak ortaya çıkmıştır. Bu oran da örneklemin evreni temsil yeteneğinin yüksek olduğunu ortaya koymaktadır.

Araştırmanın planlanması, yazılması ve uygulanması gibi tüm adımlarda etik gereklilikler göz önünde bulundurulmuş ve bu gerekliliklere sadık kalınmıştır. Özellikle projenin hedef kitlesinin 18 yaş altında olan lise öğrencileri olması bu projeyi etik bağlamda hassas bir noktaya koymaktadır.

Çalışma kapsamında öncelikle, Anadolu Üniversitesi araştırma ve yayın kurulundan 03.06.2020 tarihinde etik onay alınmıştır. Bunun yanında veri toplama işleminin Eskişehir İl Milli Eğitim Müdürlüğü’ne bağlı liselerde gerçekleştirilebilmesi için gerekli başvurularda bulunulmuştur. İl Milli Eğitim Müdürlüğü, veri toplama çalışmasına “17.09.2020” tarihli ve “88074293–605.01-E.12930413” sayılı araştırma iznini vermiştir. Bu sayede hem yasal hem etik süreçler yerine getirilmiştir.

3.4. Araştırmanın yöntemi

Bu çalışmada açımlayıcı sıralı karma yöntem kullanılmıştır. Açımlayıcı sıralı karma yöntem, ilk aşamada güçlü bir nicel araştırmanın gerçekleştirilip elde verilerin analiz edildiği ve bu analizler ışında sonraki adım olan nitel araştırmanın yürütüldüğü tasarımlardır (Creswell, 2017, s. 224). Evren ve örneklem başlığı altında belirtilen hedef kitleye anket çalışması gerçekleştirilmiştir. Bu anket çalışması anket formlarıyla öğrencilere yüz yüze uygulanmış ve elde edilen veriler IBM SPSS 23 programına aktarılmıştır. Araştırmanın amacı, modeli ve hipotezleri doğrultusunda ANOVA uygulanmıştır. Bu analiz ile belirtilen değişkenler arasındaki farklılıklar ortaya konmuştur. Nitel kısımda ise yüz yüze yarı yapılandırılmış görüşme tekniği uygulanmıştır. Görüşmeler gerçekleştirildikten ve deşifre edildikten sonra kategorisel olarak analiz edilmiştir. Katılımcılar ve veliler her iki aşamada da araştırma ile ilgili bilgilendiril-

miştir. Ayrıca katılımcı-gönüllü onam formu imzalatılmıştır.

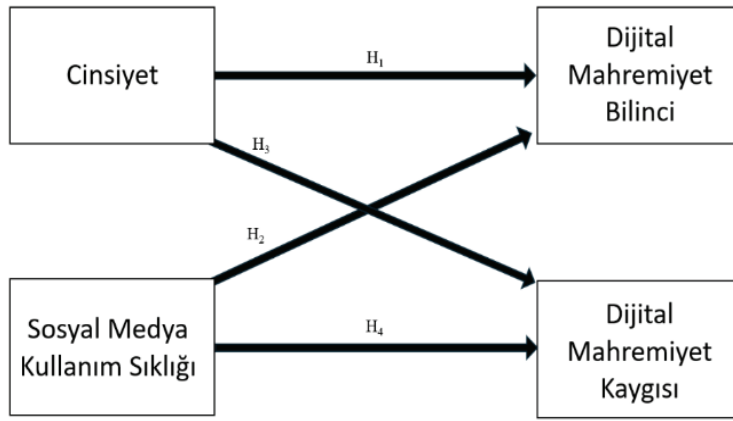
Tablo 1

Araştırmanın Hipotezleri

Hipotez kodu	Hipotez
H1	Çocukların dijital mahremiyet bilinci seviyesi, cinsiyete göre farklılaşmaktadır.
H2	Çocukların dijital mahremiyet bilinci seviyesi, sosyal medya kullanım sıklığına göre farklılaşmaktadır.
H3	Çocukların dijital mahremiyet kaygı seviyesi, cinsiyete göre farklılaşmaktadır.
H4	Çocukların dijital mahremiyet kaygı seviyesi, sosyal medya kullanım sıklığına göre farklılaşmaktadır.

Şekil 1

Araştırmanın Modeli



4. Bulgular ve Tartışma

Bu başlık altında araştırmanın nicel ve nitel aşamalarından elde edilen bulgular paylaşılmıştır.

4.1. Dijital mahremiyete yönelik nicel bulgular

Araştırmanın nicel kısmında yer alan 4 adet hipotezi test etmek amacıyla ANOVA analizi uygulanmıştır.

İlk hipotez olan “Çocukların dijital mahremiyet bilinci seviyesi, cinsiyete göre farklılaşmaktadır” hipotezine yönelik veriler Tablo 2’de yer almaktadır. Tablo 2, cinsiyet açısından sosyal medya bilinç düzeyinin anlamlı bir biçimde farklılaşmadığını göstermektedir ($p>0,05$). Dolayısıyla H1 kodlu hipotez reddedilmiştir.

Tablo 2. Dijital Mahremiyet Bilincinin Cinsiyet Açısından İncelenmesi

	Grup	<i>n</i>	$\bar{x}$	<i>s</i>	<i>t</i>	df	<i>p</i>
Dijital Mahremiyet Bilinç Düzeyi	Kız Öğrenci	640	2,04	0,66	-1,243	1234	0,214
	Erkek Öğrenci	596	1,99	0,79			

Bu kapsamda ikinci hipotez olan “Çocukların dijital mahremiyet bilinci seviyesi, sosyal medya kullanım sıklığına göre farklılaşmaktadır” hipotezine yönelik veriler aşağıdaki Tablo 3’te yer almaktadır. Tablo 3’e bakıldığında, $p<0,05$ olduğundan anlamlı bir farklılık söz konusudur. Dolayısıyla, H2 kodlu hipotez kabul edilmiştir.

Tablo 3. Dijital Mahremiyet Bilincinin Sosyal Medya Kullanım Sıklığı Açısından İncelenmesi

	Sosyal Medya Kullanım Sıklığı	<i>n</i>	$\bar{x}$	<i>s</i>	<i>t</i>	<i>df</i>	<i>p</i>
Dijital Mahremiyet Bilinci	1 saatten az	230	1.72	0.73	16,115	4	0,001*
	1-2 saat	505	2.01	0.70			
	3-4 saat	336	2.12	0.68			
	5-6 saat	117	2.16	0.66			
	7 saat ve üzeri	57	2.37	0.96			

Farkın hangi kullanım sıklıkları arasında olduğunu görmek için Post-Hoc testlerinden Tukey testi uygulanmıştır. Test sonuçlarına göre; *Dijital Mahremiyet Bilinç Düzeyi için* günlük 1 saatten az kullananlarla, 1-2 saat arasında kullananlar arasında (Ortalama farkı=-0,29; $p<0,001$); 3-4 saat kullananlar arasında (ortalama farkı=-0,39; $p<0,001$); 5-6 saat kullananlar arasında (Ortalama farkı=-0,43; $p<0,001$); ve 7 saat üzeri kullananlar arasında (Ortalama farkı=-0,65; $p<0,001$) anlamlı fark bulunmaktadır. Dolayısıyla, sosyal medyayı günlük 1 saatten az kullananlardaki sosyal medya bilinç düzeyinin, sosyal medyayı 1 saat ve üzerinden kullananlardan daha fazla olduğu anlaşılmaktadır. Ayrıca, günlük 1-2 saat kullananlarla, 7 saat üzeri kullananlar arasında (Ortalama farkı=-0,35; $p<0,05$) yine anlamlı fark bulunduğu görülmektedir.

Üçüncü hipotez olan “Çocukların dijital mahremiyet kaygı seviyesi, cinsiyete göre farklılaşmaktadır” hipotezine yönelik veriler, Tablo 4’te yer almaktadır. Cinsiyet açısından Dijital Mahremiyet kaygı düzeyinin anlamlı bir biçimde farklılaştığı görülmektedir ($p>0,05$). Dolayısıyla H3 kodlu hipotez kabul edilmiştir. Kız öğrencilerin kaygı düzeyi erkek öğrencilerin kaygı düzeyinden yüksektir (Ortalama farkı= 0,17; $p<0,05$).

Tablo 4. Cinsiyet Açısından Sosyal Medya Mahremiyet Kaygı Düzeyinin İncelenmesi

	Grup	<i>n</i>	$\bar{x}$	<i>s</i>	<i>t</i>	<i>df</i>	<i>p</i>
Dijital Mahremiyet Kaygısı	Kız Öğrenci	631	2,69	0,92	-2,956	1225	0,003*
	Erkek Öğrenci	596	2,52	1,06			

Dördüncü ve son hipotez olan “Çocukların dijital mahremiyet kaygı seviyesi, sosyal medya kullanım sıklığına göre farklılaşmaktadır” hipotezine yönelik bulgular aşağıda yer alan Tablo 5’te yer almaktadır. ANOVA sonuçlarına göre, Dijital mahremiyet kaygı düzeyi, sosyal medya kullanım sıklığına göre anlamlı fark göstermektedir. Sonuç olarak H4 kodlu hipotez kabul edilmiştir. Farkın hangi kullanım sıklıkları arasında olduğunu görmek için Post-Hoc testlerinden Tukey testi uygulanmıştır. Test sonuçlarına göre;

Sosyal medya mahremiyet kaygı düzeyi için günlük 1 saatten az kullananlarla, 1-2 saat arasında kullananlar arasında (Ortalama farkı=0,25; $p<0,05$) ve 7 saat üzeri kullananlar arasında (Ortalama farkı=0, 49; $p<0,05$) anlamlı fark bulunmaktadır. Özetle denilebilir ki sosyal medya kullanım süresi arttıkça, dijital mahremiyet kaygı seviyesi azalmaktadır.

Tablo 5. Sosyal medya kullanım sıklığının sosyal medya mahremiyet kaygı düzeyinin incelenmesi

	Sosyal medya kullanım sıklığı	<i>n</i>	$\bar{x}$	<i>s</i>	<i>t</i>	<i>df</i>	<i>p</i>
Dijital Mahremiyet Kaygısı	1 saatten az	225	2.79	1.07	4,202	4	0,002*
	1-2 saat	506	2.54	1.00			
	3-4 saat	329	2.66	0.92			
	5-6 saat	119	2.57	0.97			
	7 saat ve üzeri	58	2.31	0.98			

4.2. Dijital mahremiyet kaygısına yönelik nitel bulgular

Önceki bölümlerde de ifade edildiği üzere 15 lise öğrencisiyle derinlemesine görüşmeler gerçekleştirilmiştir. Bu öğrencilerin kodları, cinsiyetleri, yaşları ve sınıfları Tablo 6’da yer almaktadır.

Tablo 6. Nitel Katılımcılara yönelik bilgiler

İsim	Cinsiyet	Yaş	Sınıf
K1	Erkek	16	10.sınıf
K2	Kız	14	9.sınıf
K3	Erkek	16	10.sınıf
K4	Erkek	16	10.sınıf
K5	Kız	16	10.sınıf
K6	Kız	15	10.sınıf
K7	Erkek	16	10.sınıf
K8	Kız	15	9.sınıf
K9	Kız	15	10.sınıf
K10	Erkek	15	10.sınıf
K11	Kız	15	10.sınıf
K12	Kız	15	9.sınıf
K13	Erkek	16	9.sınıf
K14	Kız	15	10.sınıf
K15	Erkek	17	11.sınıf

4.2.1. Güvenlik Önlemleri Alma

Katılımcıların mahremiyet ihlaliyle ilgili kaygılarından ilki güvenliklerinin tehdit edilmesiyle ilgilidir. Bu nedenle aldıkları ilk önlemin kişisel hesaplarında ve dijital ortamdaki etkinliklerinde güvenliklerini korumaya çalışmak olduğu görülmektedir. Bu doğrultuda katılımcıların; güçlü şifreler koyma, kimlik doğrulamaları, doğru bilgiler vermeme ve sosyal medya hesaplarını gizleme gibi önlemler aldıkları görülmektedir:

K8: *En büyük kaygım bir yerden kamerada ya da mikrofondan ulaşım ulaşamayacakları oluyor. (...) Kendimi korumak için siber güvenlik tedbirlerini zaten ailemle birlikte alıyorum ama eğer böyle bir şey başıma gelirse sosyal medya, bilgisayar, genel olarak dijital kullanımım çok daha aza ineceğini düşünüyorum bu yaratılan travma yüzünden. Bunu önlemek amacıyla da kesinlikle önlemlerimi alıyorum; siber güvenlik anlamındaki yazıları okuyorum, güvenlik sözleşmelerini okuyorum, ondan sonra izinlerimi, bütün bilgilerimi, özel bilgilerimi paylaşmıyorum, bu konuda bence yeteri kadar önlem alıyorum.*

K12: *Mesela Instagram'da şifremi koyarken tabii ki birazcık daha zor koyuyorum, sonuçta artık birini tanıyacağın zaman direkt Instagram'ına, sosyal medyasına falan baktığın için...ve insanlar mesela bazen hesap kırmak istiyor. (...) Yani bu artık gerçekten çevremizde var; bir iki tane arkadaşım var, ona söylüyorum onlar bazen insanların hesaplarını falan bakıyorlar.*

K6: *Ben şifrelerimi çok imkânsız şifreler koyuyorum yani. Böyle Da Vinci şifresi gibi bir şey. Bazen böyle içime vesvese düşüyor ve değiştiresim geliyor. Koyduğum şifreler de böyle saçma sapan şeyler, kimse bulamaz yani hacker bile der ki bu ne yani. Bir de hesaplarımı gizliyorum.*

İfadelerde de görüldüğü üzere katılımcıların güçlü ve benzersiz şifreler kullanmaları, hesaplarını yetkisiz erişime karşı korumak adına önemli bir önlemdir. Bu şekilde kendi dijital varlıklarını korumaya alan öğrenciler iki faktörlü doğrulama gibi daha ileri düzey önlemler de alabilmektedir:

K10: *(...) Yani kişisel bilgilerimden tabii ki endişe ediyorum bazen de işte o 2 aşamalı kimlik doğrulama falan oluyor onları etkinleştirdiğimde kendimi en azından daha güvende hissediyorum. Yani atıyorum biri hesabıma girmek istiyor, direkt bana telefon numarası üzerinden sms geliyor böyle böyle bir kod geliyor. Adam kodu görmediği sürece hesaba giremiyor.*

İki faktörlü doğrulama hesaba yetkisiz erişim konusunda kritik bir rol oynamaktadır. Öte yandan dijital ortamda gerçek kişisel bilgilerini kullanmama, hesaplarını gizli tutma gibi önlemler de şifrelere ulaşılması durumunda bile hesabın çalınmasının önlenmesi ve paylaşımların belli bir kitleye ulaşmasını sağlama konusunda etkili olabilmektedir:

K4: *Ya hani doğum tarihime dair doğru bilgi vermem ben kimseye. Hani en basiti, eskiden HES kodundan mesela karantinaya alabiliyorlardı. İsteseler benim doğum tarihim girerek beni temaslı bile gösterebilirler. Fakat kimse*

benim doğum tarihim doğru bir şekilde bilmiyor. Mesela şifrelerdeyken de başka bir gizli bilgimle alakalı bir şey yapıyorum ki başka kimse bulamasın diye.

Lise öğrencilerinin dijital mahremiyet kaygıları doğrultusunda aldıkları bu önlemler, bu yaş grubunun dijital güvenlik konusunda bilinçlendiğinin ve proaktif adımlar attığının bir göstergesi olarak değerlendirilebilir. Bu durum aynı zamanda lise öğrencilerinin farkındalık düzeyine işaret etmektedir. Dijital güvenliğin ilk adımları olan güvenlik önlemleri kendi dijital mahremiyetlerini korumaya dair bilinçli davranışlar sergilediklerini göstermektedir.

4.2.2. Tanınmayan Kişileri Araştırma-Kontrol Etme

Dijital ortamda mahremiyet kaygısı ile bağlantılı pratiklerden bir diğeri de öğrencilerin tanımadıkları kişilerden, bilinmeyen hesaplardan aldıkları eklem talebi, mesajlar gibi durumlarda kişileri araştırma davranışlarıdır. Kendi ifadeleri ile “stalk” yapan katılımcılar, bu yöntemi karşılarındaki hesabın güvenilirliğini kontrol etmek amacıyla kullanmaktadır:

K7: *Tabii ki kendimi korumak istiyorum. Bunun için birini hesabıma almadan önce, isteğini kabul etmeden önce onu başka bir hesabımdan “stalkluyorum veya ortak arkadaşlarınıza bakıyorum. Ortak arkadaşım yoksa onu genellikle zaten almıyorum.*

K12: *Zaten çok tanımadığım insanları veya profili hoşuma gitmeyen insanları almıyorum veya zaten bio denen bir şey var, işte böyle hesabına girdiğinde orada gözüküyor, bazen oraya yazdıkları cümleler falan filan oluyor, mesela onlar itici geliyor, diyorum “Bunu eklemeyeyim”. Direkt bazı insanlar hesabını kapatmıyor, böyle herkese açık oluyor. Mesela oradan stalkluyorum, birazcık bakıyorum, “Kimmiş neymiş? Kimler ortak arkadaşlarım?” veya ortak arkadaşım olmayanları genellikle almıyorum.*

Kendi bilgilerine erişilmesi konusunda kaygı duyan öğrenciler, önlem almak adına başkalarının bilgilerini araştırma eğiliminde olabilmektedir. Bu doğrultuda bazı katılımcılar tanımadıkları kişilerden gelen taleplerde kişileri kontrol etmek için sahte hesaplarından araştırmayı tercih etmektedir:

K12: (...) İnsanlara böyle girip bakıyorum. Diyelim ki biri bana bir şey yazdı, işte ben de buna bir şeyler yazmadan önce önlem almak için, kim olduğunu tanımak için başka, tanınmayan hesabımdan girip ilk önce onu stalkluyorum, “Ortak arkadaşımız var mı? Kimdir, nedir, hangi okula gidiyor veya hangi şehirde?” gibi şeylere bakıyorum, ondan sonra ona cevap veriyorum veya iletişim kuruyorum her yönden veya takipçim olarak alıyorum onu hesabıma.

4.2.3. Kişisel Paylaşımlara Dikkat Etme

Dijital mahremiyet ihlaline dair en sık karşılaşılan sorunlardan biri sosyal medya hesaplarından çalınarak kullanılan kişisel bilgiler, konum, fotoğraflar ve videolardır. Bu verilerin kötü amaçlar için kullanımı oldukça yaygındır ve katılımcılar da bu doğrultuda bir endişe taşımakta, dolayısıyla çeşitli önlemler almaktadırlar:

K12: *Mesela çok açık giyindiğim vesaire bir şey olduğunda onu herkesin görmesini istemem, gidip de Instagram’ıma atmam öyle şeyi ama gidip de arkadaşlarımı, Yakın Arkadaşlara ekleyip... Mesela diyelim ki yazın sahilde işte arkadaşlarımla bikinili bir fotoğraf çekilmişimdir, onu gidip yakın olduğum insanlara atarım ama gidip de Instagram’a koymam yani.*

K13: *Konumumun belli olması ve bir de ondan da önemlisi yani simanın sosyal medyaya gitmesi mesela bazı özel görüntülerin, tatil fotoğraflarınızın mesela. Çünkü kişiliğinizi çalabilirler o fotoğrafları alarak.*

K8: *Attığım storylerde kendi yüzümü çok paylaşıyorum ama 8 kere düşünerek atıyorum yani ve gerçekten çok etkiliyor. (...) O aslında sosyal medya değil de ya orta okulda mutlaka zorbalığa uğramıştır insanlar. Yani günlük hayatta yüz yüze yediğim ufak zorbalıklar sebebi böyle oldu ama sosyal medyanın da illaki bilinçaltıma işlediği birkaç şeydir bu konuda.*

Bu katılımcıların ifadelerinde sosyal medyada da bedensel mahremiyet endişesinin yoğun yaşandığı görülmektedir. Özellikle kız öğrencilerin kişisel hesaplarında “açık” ya da “yüzünün görüldüğü” fotoğraflar paylaşmamaya özen gösterdiği dikkat çekmektedir. Nicel verilerin de işaret ettiği üzere sosyal medyada mahremiyet ihlali kaygısı kız öğrencilerde daha yaygındır. Bu da toplumsal cinsiyet normlarının sosyal medya pratiklerinde de ne kadar etkili olduğunu ortaya koymaktadır. Toplumda yaşanan olumsuz örneklerin kadınlar üzerinden gerçekleştiği göz önünde bulundurulduğunda özellikle ergenlik çağında kız öğrencilerin kendilerini daha büyük baskı ve risk altında hissetmeleri dolayısıyla paylaşımlarını kısıtlamaları normal görülmektedir. Paylaşımlarını yakınlarıyla sınırlı tutmaları da bunun en belirgin örneği olarak karşımıza çıkmaktadır:

K12: *Açıkçası daha önceden tartıştığım insanlara sosyal medya hesaplarında falan, böyle yine ekliyoruz birbiri-mizi, ben hikâye attığımda falan onun görmesini istemiyorum veya işte diyelim ki bir akrabam var, onun görmesini istemiyorum. O zaman, direkt mesela Instagram'a bir hikâye atacağım, onu yakın arkadaşlara alıp atıyorum. Orada yakın arkadaşlardan atmak istediklerimi seçiyorum, kimlerin görmesini istiyorsam o şekilde atıyorum.*

K3: *Paylaşılacak şeyler bence kişisel bilgiler olmalı yani ne bileyim şöyle, birçok kişinin şu anda kullandığı gizli hesapları var kendilerine ait. Onlarda daha kendilerine yakın gördüğü kişilerle paylaşılabilir ama onun dışında herkese açık olan hesaplarda mesela kendisinin kimden hoşlandığı veya ne tür aktiviteler yaptığı bence paylaşması birazcık absürt kaçıyor. Bunları kötüye kullanan insan çok fazla olabiliyor.*

Katılımcıların ifadelerinde dijital mahremiyet ihlallerinin konum paylaşımı üzerinden gerçekleşebileceğine karşı endişeler de dikkat çekmektedir. Konum verilerinin paylaşılması, bireylerin fiziksel güvenliğini tehdit edebilmektedir. Özellikle gençler, kötü niyetli kişilerin kendilerini takip etmesinden endişe duyabilmekte, hatta günlük aktivitelerinin ortaya çıkması dolayısıyla mahremiyetlerinin ihlal edilebileceği kaygısını duyabilmektedir:

K9: *Özellikle mesela konum açısından çok bir şey paylaşmayı sevmiyorum hani çünkü ne bileyim hani mesela önceki hesabımda çok konum paylaşmazdım çünkü hani insanlar benim orada olduğumu görüyor. Tanımadığım insanlar gelip orada beni bulabilir açısından.*

K7: *Hiçbir şey paylaşmıyorum. Çünkü zaten bu haberlerde de çıkıyor, ne kadar doğru bilmiyorum ama, hırsızlar falan insanların tatilde olduğunu öğreniyor mesela sosyal medyadan sonra kişinin evini soyuyor falan. Tabii ki de tatil fotoğraflarını paylaşmayacaksın diye bir şey yok da hani her şey her an paylaşılırsa sıkıntı çıkabilir.*

4.2.4. Kişisel Bilgilere Erişime Karşı Alınan Önlemler

Bir diğer mahremiyet ihlali kaygısı da kişisel bilgilere erişim konusunda ortaya çıkmaktadır. Fazla detay kişisel bilgi istenmesi kişisel bilgilerin kötüye kullanımı ve kimlik hırsızlığı gibi endişeleri beraberinde getirmektedir. Bu doğrultuda katılımcılar bu endişeleriyle ilgili de çeşitli pratikler sergilemektedir:

K11: *Yani aslında işte doğum tarihi falan sorarsa o zaman sıkıntı değil ama mesela hani kimliği falan soruyorlar ya hani öyle bir durum olduğunda önce şey yapıyorum hani işte uygulamanın yorumlarını okuyorum, internetten araştırıyorum falan öyle. (...) Mesela okuyorum hani işte bu açıdan hiç şikâyet olmamış, kişisel mahremiyet falan hiç şikâyet olmamışsa hani güveniyorum buna.*

K12: *Mesela insanlarla, sosyal medyadan iletişim kuruyorum arada ve bunlarla hani böyle konuşmalarımın başka insanların eline geçip tehdit amaçlı kullanılabilmelerinden korkuyorum veya telefon numaramın veya kimliğimde yazan herhangi bir özel bilginin başkasının eline geçmesinden korkuyorum.*

K11: *Yani aslında mesela hani bunlar çalındıktan sonra şeyden en çok korktum, mesela bunlar çalınıyor diyelim benim üstüme bir suç işleniyor sonra bu benim üstüme kalırsa diye korkuyorum. (...) Yani işte, beni işte dediğim gibi en çok korkutan hani kişiler bilgilerimin bulunup benim üzerime suç işlenmesi. Çünkü hani kimse bunda araştırmaz bence Direkt benim üstüme kalırmış gibi geliyor. Sonra hani mesela şey korkutuyor hani hesabımın çalınıp hani benim gibi başkalarına mesaj atmam, o.*

K13: *Bir makale okumuştum kişilik hırsızlığı hakkında. Bazı dolandırıcılar sizin sosyal medyaya atığınız fotoğrafları başkalarının aleyhine kullanarak, başkalarını kazıklayarak kullanabiliyor. Mesela o attığınız fotoğrafları mesela o hacker hesabınızdan alıp kendisininmiş gibi kullanarak başkalarıyla sizmiş gibi konuşabiliyor. O yüzden ben çok kendi yüzümün gözüktüğü videoları veya başkalarının yüzünün gözüktüğü videoları veya resimleri asla sosyal medyaya yüklememeye dikkat ediyorum.*

K15: *Yani, nerede kullanacağı belli olmaz, şirket açar batırır. (...) Manevi şeyleri zaten paylaşmadığım için hiçbir yerde, maddi şeylerimi çalmalarından korkarım.*

Kişisel bilgilerin paylaşımına dair alınan önlemler de dijital mahremiyet konusunda bilinç düzeyinin bir işareti olarak değerlendirilebilir. Yaşanan ya da yaşanma ihtimali olan olumsuz deneyimler öğrencileri kişisel bilgilerini paylaşma konusunda daha tedbirli davranmaya sevk edebilmektedir. Bu da aslında mahremiyetlerini korumak adına anlamlı önlemler aldıklarını göstermektedir.

4.2.5. Gözetlenme Endişesiyle İlgili Pratikler

Sosyal medyadaki gözetim pratikleri aslında karşılıklı bir gözetlemeyi, gözetişimi, teşvik eden bir yapıya sahiptir. Bu bir yanıyla birbirini takip etme gibi rızaya dayalı karşılıklı gözetim ilişkisini beslerken, bir yandan merkezsiz yapısı nedeniyle gözetlenme endişesini de beraberinde getirebilmektedir. Özellikle teknolojinin hızlı gelişimi yaş grubu fark etmeksizin toplumsal olarak gözetlenme endişesini perçinlemektedir. Bu doğrultuda katılımcıların gözetlenme endişesi taşıdıklarına dair ifadeler dikkat çekmektedir:

K5: *Gözetlendiğimi düşünüyorum. Beni sevmeyen insanlar tarafından. Yani aslında hiç güvenilir bir ortam değil açıkçası. Çünkü engelledikçe bir şey değişmiyor yani. Güvenilir olduğunu düşünmüyorum. Ama çok tehlikeli olduğunu da zannetmiyorum. Orta karar.*

K10: *Valla yakın arkadaşlarım bakıyor olabilir. (...) Şimdi şöyle diyeyim, dışarıda çok görüştüğüm ama çok samimi olmadığım insanlar benim hakkımda daha çok şey öğrenmek için falan giriyor olabilirler, bakıyor olabilirler. Onun dışında yakın arkadaşlarım falan niye baksın bilmiyorum girip ne yapmış falan diye bakıyor olabilirler.*

K12: *Yani şöyle, benim de birkaç tane tanıdığım insan var, bunlar böyle artık hesapların şifresi falan kırılabilir ve hesaplara giriş yapılabilir. Ben bunu sık sık aktif olduğum Instagram hesabında kontrol ediyorum ama fake hesabımda falan çok fazla kontrol etmiyordum ve geçen gün girip baktığımda böyle konumda başka şehirlerin şeyleri vardı, yani birkaç kişi şifremi kırıp girmiş. Tabii ki böyle korktum çünkü senin hesabından giriş yapmışlar, orada ne olup bittiğini, kiminle konuştuğunu, her şeyi görebiliyorlar. Bu yüzden izlendiğimi falan düşünüyorum arada, o yüzden ha bire kontrol ediyorum. (..) mesela, tanınmayan sitelere girdiğimde böyle sanki izleniyormuşum gibi hissediyorum, o yüzden kameraya falan bir şeyler yapıştırdığım oluyor bazen.*

K2: *Yani bazen gözetlendiğimi düşünüyorum. Mesela herhangi bir bilgisayar oyunu oynamayı severim ben. Bilgisayar oyunu indireceğim zaman genel de mesela sitelerde bir tedirgin falan olurum. Bağlantı indirdiğimiz için hani belki bilgisayarıma erişim olabilir tarzı bir tereddüt.*

K4: *Ben bunu böyle merak ettim, bir araştırma yapacağım dedim hatta annelere. Sadece 5 dakika boyunca işte futbol konuştum işte futbolcu ismi söyledim futbolla ilgili sonra futbol topu çıktı, Nike'ın formaları çıkmaya başladı. (...) Sonra deterjanlarla ilgili bir konu açtım annemle. Yine böyle konuştum konuştum ondan sonra şampuan reklamı çıktı. (...) Fiziksel olarak da hayalet ekran kullanıyorum mesela ben kendi telefonumu, kimse benimkini görmesin diye.*

Gözetlenme, bireysel özgürlük ve mahremiyet konusunda ciddi endişeler yaratabilmektedir. Sosyal medya platformları kişisel bilgilerin dolaşımında olduğu ve izlenebilir olduğu ortamlardır. Ancak bunun yanı sıra kurumsal veri toplama ve depolama faaliyetleri de kaygı uyandırabilmektedir. Kişiye özel reklamlar, depolanmış verilerden yola çıkılarak oluşturulan öneriler gibi deneyimler gençleri şimdi ve geleceğe dair de kaygılandırabilmektedir:

K6: *Evet çok duyuyorum açıkçası ama birinin beni gözetlemesi değil daha çok o hesabın, atıyorum Instagram şirketi mesela, benim her türlü bilgim, hikayelerim, konuşmalarım, o tür şeyler insanı biraz tedirgin ediyor. Yani gözetleniyor gibi hissediyorum kendimi.*

K8: *Kesinlikle gözetlendiğimi hissediyorum. Siber güvenlik için gözetliyor olabilirler ama onun dışında bir makalede okumuştum, Apple harici ürünlerde, androidlerde çok kolay bir şekilde ulaşılabilir olmuş kameralara ve bu beni bir tık korkuttu bir de makale gibi bir yerde okuyunca. Çünkü ben Android kullanıyorum, Iphone kullanmayı tercih etmiyorum ve yani gerçekten kameradan insan izleniyormuş gibi hissediyor ama bu tamamen psikolojik.*

K15: *Sinir bozucu oluyor, bir şey konuşuyorum ardından geliyor. “Bisiklet, bisiklet, bisiklet” diyorum ardından bisiklet reklamları çıkıyor. “Araba, araba” diyorum Sahibinden ilanları çıkıyor. Sinir bozucu şeyler.*

K6: *Bir ara şey vardı, WhatsApp'ın bir haberi çıktı herkes böyle ses çıkardı, mesajlarımız kaydedilecek gibi mi öyle bir şey olmuştu. Ondan sonra işte güncelleyecekmişiz WhatsApp'ı hatta ondan sonra olacakmış. Ben güncellemeyecektim. Ben, Elon Musk hatta bir tane Messenger gibi bir şey önermişti onu kullanacaktım ama, he Signal, ama bundan sonra düşünmeye başladım daha çok yani şimdi ben bunu hep konuşuyorum arkadaşlarımla, hocalarımla da bunların hepsi acaba kaydediliyor mu? Şimdi kaç adım attığımızı bile gösteren telefonda, böyle bir teknolojiye, bu tür medya hesapları neden bizi takip etmesin diye düşünüyorum.*

Katılımcıların ifadelerinde de dikkat çektiği üzere gözetlenme endişesi, öğrencilerin çevrimiçi davranışlarını değiştirmelerine yol açabilmektedir. Bunu kişisel mahremiyetlerine ve özgürlüklerine müdahale olarak algılayan öğrenciler daha dikkatli ve kısıtlı paylaşım yapma, gizlilik ayarlarını sıkılaştırma gibi önlemler alabilmektedirler.

4.2.6. Önleme Dayalı Endişesizlik

Dijital mahremiyet kaygısıyla alınan önlemler bu kaygıyı önleme konusunda da etkili olabilmektedir. Bu noktada; alınan önlemlerin ne kadar etkili olduğu şüpheli bir noktada durmaktadır, ancak dijital becerilerine ve tedbirlerine güvenmeleri nedeniyle bazı katılımcıların mahremiyet kaygısı duymadıklarına dair ifadeleri mevcuttur:

K11: *Yani aslında şöyle, nasıl desem hani o kadar da özel şeyler paylaşmadığım için mesela hesabım kapansa çok umurumda olmuyor benim. Hani çünkü zaten altı üstü bir hesap yani ne olabilir ki diye düşünüyorum. O yüzden çok... mesela güvenlik için de şey var iki faktörlü doğrulama var. Biri benim hesabıma giremiyor onla. Bana mesaj geliyor, benim onaylamam gerekiyor girmesi için. O açık.*

K7: *Beni kim neden gözetlesin yani. Çok zaten farklı bir şey yapmıyorum. Yani farklı bir şey yapmıyorum dediğim hani internetten falan indirmiyorum, virüs olsun ya da herhangi bir şey. Steam'den indiriyorum hani arada oynuyorum yani o yüzden herhangi bir güvenlik tehdidi yok, stresim yok. Oyunlarda da herhangi bir bilgi paylaşmıyorum bitiyor yani. Ulaşamazlar sonuç olarak.*

K13: *Bende öyle bir korku yok çünkü biri beni takip etse, gözetlese bile bende bulabileceği pek bir şey yok ki. Onun için benim ileri düzey bir hacker tarafından sanal saldırıya uğramam lazım. O da niye beni seçsin yani? O yüzden çok öyle bir korkum yok.*

K14: *Konuştuklarımın dinlendiğini, başkası görüyor mu duyuyor mu diye endişelenirdim. Ama kullanmadığım için endişem yok. WhatsApp da fazla kullanmıyorum. En çok Snapchat'teyim. Onda da kötü bir şey yapmadığım için kafam rahat.*

Bu noktada, tedbirlerin alınmasıyla azalan mahremiyet kaygısı konusunda bazı çıkarımlar yapmak mümkündür:

Öğrenciler, dijital mahremiyet konusunda bilinçlendikçe ve farkındalıkları arttıkça, aldıkları önlemlerin etkisini görebilmektedir. Bu bilinç, güven duygusunu artırırken, endişeleri de azaltabilmektedir.

Kullandıkları güçlü ve benzersiz şifreler, iki faktörlü kimlik doğrulamaları gibi temel önlemler, hesapları ve kendi güvenlikleri hakkında endişelerini yok edebilmektedir.

Gizlilik ayarlarına hâkim olma ve paylaşım pratiklerinde dikkatli davranma endişelerini azaltabilmektedir.

Kendi dijital mahremiyetlerini önemseyen ve kontrol edebildiklerini bilen öğrencilerin kontrol hissi kendilerine güvenlerini artırabilmekte ve kaygılarını da azaltabilmektedir.

4.2.7. Kaygı Duymama

Dijital mahremiyet kaygısı duyanların yanı sıra çeşitli nedenlerden dolayı böyle bir kaygı duymayan katılımcılar da bulunmaktadır. Sosyal medya kullanımı ve paylaşım pratikleri günlük yaşamın bir parçası olarak değerlendirilmektedir. Bu nedenle bazı öğrencilerin sosyal medyada bilgi paylaşımının kabul edilebilir ve yaygın olmasından dolayı endişelenmenin gereksiz olduğunu düşündükleri görülmektedir.:

K1: *Ya sorun olacağını düşünmüştüm evet ama herkes paylaştığı için yani... Bir şey olmaz. Kim niye benim bilgilerimle bir şeyler yapsın? Ünlü olsam mesela aktör falan olsam o zaman sakınabilirdim ama yok yani şu an. Zaten çok bilgi vermiyorum.*

K11: *Yani şey diyorum aslında hani zaten hani benim gibi birçok paylaşım yapan insan var hani önemli değil diyorum. Yani şey, hani onca insanın hayatı var benim hayatım bu kadar önemli değildir herhalde diyorum.*

İfadelerde de dikkat çektiği üzere bazı öğrenciler, sosyal medyayı kullanan kişilerin çok fazla olmasından dolayı kendi bilgilerinin kötüye kullanılma ihtimalinin düşük olduğunu düşünmektedir. Öte yandan, bir önceki başlıkta da değinildiği gibi bazı öğrencilerin de dijital mahremiyetlerini korumak için aldıkları tedbirlerin yeterli olduğunu düşünmesi dolayısıyla endişe duymadıkları görülmektedir:

K5: *Yani fotoğrafın içeriğine göre değişiyor açıkçası. Ama sonuçta herkes yaptığı için de çok da takmıyor gibi bir şeyim. (...) Şifre olarak çok bir şey yapamıyorum çünkü genelde lazım olan şeyler oluyor mesela uygulamaya girmek için şifreyi artık mecbur, el mecbur yani. Biraz da risk almak gerekiyor galiba.*

K9: *Yani bence endişeleneceksen, çok bir şey varsa kullanma. Bunu kullanmama gibi bir seçeneğimiz de olmadığı için endişelenmeyelim ki hayatımızı daha güzel yaşayalım yani. Sürekli endişelenerek bir yere varamayız.*

SONUÇ

Dijital iletişim, günlük yaşamın ortasında yer almasına karşın henüz başta etik ve hukuk gibi pek çok alanda zeminini oturtamamış bir yapıdır. Ticaretten eğlenceye, eğitimden sağlığa kadar hemen her alanda kullanılan dijital iletişim araçları her yaştan birey için büyük avantaj olduğu kadar çeşitli riskler de barındırmaktadır. Bu risk ve sorunlarla erişkin bireyler dahi sıklıkla yüz yüze kalırken, erişkin olmayan bireyler için durum çok daha karmaşıktır. Özellikle, dijital iletişim araçlarının sebep olduğu mahremiyet problemleri henüz yetişkin olmamış bireyler için büyük tehditler barındırabilmektedir.

Bu çalışmayla da henüz yetişkin olmamış bireylerin mahremiyet algıları ve kaygıları üzerine hem nicel hem de nitel araştırmalar gerçekleştirilmiştir. İlk aşama olan nicel aşama kapsamında ortaya konan hipotezleri test etmek amacıyla ANOVA analizi uygulanmıştır. Bu kapsamda hipotezlerin sonuçları Tablo 6’da yer almaktadır. Analiz sonuçlarına göre “Çocukların dijital bilinci seviyesi, cinsiyete göre farklılaşmaktadır” hipotezi reddedilmiştir. Öte yandan “Çocukların dijital mahremiyet seviyesi, sosyal medya kullanım sıklığına göre farklılaşmaktadır” hipotezi kabul edilmiştir. Yapılan Post-hoc (TUKEY) testine göre; sosyal medya kullanım sıklığının artışıyla birlikte bilinç seviyesinin düştüğü gözlemlenmiştir.

Diğer bir hipotez olan “Çocukların dijital mahremiyet kaygı seviyesi, cinsiyete göre farklılaşmaktadır” hipotezi kabul edilmiştir. Buna göre kız öğrencilerin kaygı seviyesi erkeklerinkinden fazla bulunmuştur.

Son hipotez olan “Çocukların dijital mahremiyet kaygı seviyesi, sosyal medya kullanım sıklığına göre farklılaşmaktadır” hipotezi de kabul edilmiştir. Buna göre; sosyal medya kullanım seviyesi arttıkça kaygı seviyesi tam tersi şekilde azalmaktadır.

Tablo 7. Hipotezlerin Değerlendirilmesi

Hipotez Kodu	Hipotez	Sonuç
H1	Çocukların dijital mahremiyet bilinci seviyesi, cinsiyete göre farklılaşmaktadır.	Reddedildi
H2	Çocukların dijital mahremiyet bilinci seviyesi, sosyal medya kullanım sıklığına göre farklılaşmaktadır.	Kabul Edildi
H3	Çocukların dijital mahremiyet kaygı seviyesi, cinsiyete göre farklılaşmaktadır.	Kabul Edildi
H4	Çocukların dijital mahremiyet kaygı seviyesi, sosyal medya kullanım sıklığına göre farklılaşmaktadır.	Kabul Edildi

Nicel aşamayla hipotezlerin test edilmesinin ardından daha derinlikli veri elde edebilmek için nitel aşamaya geçilmiştir. Bu kapsamda “Yöntem” bölümünde daha detaylı bahsedilmekle beraber 15 öğrenciyle derinlemesine görüşmeler gerçekleştirilmiştir. Bu görüşmeler deşifre edildikten sonra bulgular kısmında detaylıca analiz edilmiştir. Bu nitel analiz aşamasında kategorisel analiz yapılmıştır. Katılımcılarla yapılan görüşmelerde dijital mahremiyet kaygıları doğrultusunda öğrencilerin sergiledikleri pratikler altı kategori üzerinden sıralanmıştır. Bunlar;

- » Güvenlik önlemleri alma,
- » Tanınmayan kişileri araştırma-kontrol etme,
- » Kişisel paylaşımlara dikkat etme,
- » Kişisel bilgilere erişime karşı alınan önlemler,
- » Gözetlenme endişesiyle ilgili pratikler,
- » Önleme dayalı endişesizlik ve
- » Kaygı duymama kategorileridir.

Görüşmelerdeki ifadeler göstermektedir ki lise öğrencilerinin çoğunluğu dijital mahremiyetlerine dair endişe hissetmekte ve bu nedenle çeşitli önlemler almaktadır. Bu önlemlerin dijital mahremiyet bilinciyle ve dijital becerilerle ilişkisi kuvvetli görünmektedir. Genel olarak her öğrencinin güvenlik önlemleri almaktaki temel kaygısı hesaplarına yetkisiz erişim, kişisel bilgilerin çalınması ve bilgilerin kötüye kullanılması üzerinden şekillenmektedir. Dolayısıyla aldıkları önemli temel tedbirler de güçlü şifreler kullanma, hesaplarını gizli tutma, paylaşımlarını sınırlamadır. Tanınmadıkları kişilerin ekleme ve mesaj taleplerine karşı tedbirli yaklaşma, onları araştırma, güvenilirliklerini kontrol etme davranışı da belli bir dijital bilinç düzeyine işaret etmesi açısından önemlidir.

Kişisel bilgilere erişimin olumsuz sonuçlarını deneyimlediğimiz veya gözlemleyebildiğimiz günümüzde kimlik

hırsızlığı, dolandırıcılık gibi çeşitli risklerin katılımcılarda da büyük bir kaygı yarattığı görülmektedir. Bu risklerin farkındalığı ve tedbirli kullanım pratikleri de önemli bir bulgudur. Öte yandan katılımcıların mahremiyet kaygılarının en net hissedildiği bulgunun yaptıkları paylaşımlara dikkat etme ve bu paylaşımları yakın çevreleriyle sınırlama pratiği olduğunu söylemek mümkündür. Buradaki önemli bir detay kız öğrencilerin bu konudaki endişelerinin daha yoğun olmasıdır. Özellikle bedensel mahremiyetlerine dair endişe duyduklarını belirten katılımcılar, bedensel açıklık ve yüzünü gösterme konusunda daha dikkatli davrandığını ifade etmektedir. Bu noktada toplumsal cinsiyet normlarının kadınların bedensel sınırlarını koruma konusunda daha dikkatli davranmalarına neden olan yapısını vurgulamak gerekmektedir.

Kız öğrencilerin dijital platformlarda yüzlerini veya bedenlerini gösterme konusunda daha temkinli davranmaları, bu toplumsal normlara ve cinsiyetle ilgili endişelere işaret etmektedir. Özellikle toplumsal cinsiyet nedeniyle yaşanabilecek olumsuz sonuçlar kadınlar üzerinde nispeten daha travmatik etkilere neden olmakta, sosyal medyada, haberlerde ya da televizyonda karşılaşılan olumsuz örnekler kaygı düzeyini artırabilmektedir. Özellikle dijital kültürün toplumsal normları pekiştirici olabilme özelliği genç kullanıcılar üzerinde algıları şekillendirici bir potansiyel taşıyabilmektedir. Dolayısıyla kız öğrencilerin dijital paylaşımlarında daha dikkatli olmaları, toplumsal cinsiyet rollerine ve bu rollerin getirdiği baskılara karşı bir korunma tedbiri olarak değerlendirilebilmektedir. Bir diğer önemli bulgu gözetlenme kaygısıyla ilgilidir. Gözetlenme kaygısı, bireylerin özgürlüklerine yönelik algı ve toplumun dijital çağdaki mahremiyet anlayışıyla doğrudan ilişkilidir. Katılımcıların ifadeleri doğrultusunda dijital çağda kişisel verilerin toplanması ve izlenmesi, toplumsal kontrol mekanizmalarının bir uzantısı olarak görülebilmektedir. Özellikle gençlerin, dijital platformlarda sürekli izlendiklerini ve reklamlar aracılığıyla kişisel verilerinin kullanıldığını düşünmeleri özgürlüklerine yönelik bir tehdit olarak algılanabilmektedir. Kullanıcıların çevrimiçi etkinliklerinin izlenmesi ve analiz edilmesi yoluyla sunulan reklamlar mahremiyetin ihlaline ilişkin bir kaygı ortaya çıkarmaktadır. Bu kaygı da bireylerin kendilerini daha temkinli ve sınırlayıcı bir şekilde ifade etmelerine yol açabilmektedir. Tüm bunların yanı sıra katılımcıların bazılarının kendi dijital becerilerine ve aldıkları önlemlere olan güvenlerinden kaynaklı ve sosyal medyanın yaygın kullanımı ve kalabalık yapısı nedeniyle dijital mahremiyetlerine dair kaygı duymadıkları görülmektedir. Bu da dijital kültürün bir başka sonucu olarak değerlendirilebilir.

Bu çalışmadan elde edilen veriler doğrultusunda gelecek çalışmalarda öncelikli olarak kız öğrencilerin dijital platformlarda bedensel mahremiyetleriyle ilgili kaygılarının, toplumsal cinsiyet normları ve dijital mahremiyet riskleri ile doğrudan bağlantılı olduğu göz önünde bulundurulmalıdır. Bu bulgu, toplumsal cinsiyet normlarının ve dijital kültürün genç bireyler üzerindeki etkilerini anlamak için bir temel oluşturmaktadır. Gelecekte yapılacak araştırmalar, bu endişelerin nasıl azaltılabileceği ve toplumsal cinsiyet eşitliğinin dijital ortamda nasıl teşvik edilebileceği üzerine odaklanabilir.

Dijital dünyada güvenliğin sağlanması, kişisel bilgilerin korunması ve bu konularda bilinçli davranışların geliştirilmesi açısından öğrencilerin dijital mahremiyet farkındalığını artırmak adına okullar ve eğitimciler, öğrencilere dijital dünyada nasıl daha güvenli bir şekilde hareket edebileceklerini öğreten programlar ve dersler tasarlayabilir. Ayrıca ebeveynlerin, çocuklarının dijital gizlilik konusundaki bilinç düzeyini artırmada kritik bir role sahip olması dolayısıyla ebeveynlere yönelik eğitim ve bilgilendirme programlarının geliştirilmesi büyük önem taşımaktadır. Öte yandan gözetlenme kaygısı, bireylerin dijital platformlarda kişisel özgürlüklerini ve mahremiyetlerini koruma arayışını yansıtmaktadır. Toplumsal normlar, dijital gözetim uygulamaları ve kişisel verilerin kullanımı, bireylerin özgürlük algısını etkilemektedir. Bu kaygının ele alınması, toplumsal bilinçlenme, yasal düzenlemeler, teknolojik çözümler ve sosyal destek mekanizmaları yoluyla gerçekleştirilebilir. Böylece, bireylerin dijital ortamda daha güvende hissetmeleri ve özgürlüklerinin korunması sağlanabilir.

KAYNAKÇA

- Acquisti, Alessandro - Brandimarte, Laura - Loewenstein, George. Secrets and likes: The drive for privacy and the difficulty of achieving it in the digital age. *Journal of Consumer Psychology*, 30/4 (2020). 736-758.
- Akça, Figen. - Çilekçiler, Nuray Koç. Okul öncesi dönemdeki çocukların en çok etkilendiği çizgi film karakterleri ve bu karakterlerle özdeşleşmelerinin yol açabileceği dijital tehlikeler. *Addicta: The Turkish Journal on Addictions*, 6/2, (2019). 403-433.
- Arik, Bilal. - Arik, Emel. Facebook'un dönüşen mahremiyet yaklaşımı: "Gelecek mahremiyettir". *Intermedia International e-journal*, 7/13, (2020). 447-461.
- Aslanyürek, Malik. İnternet Güvenliği ve Çevrim İçi Gizlilik Alanlarında Yaşanan Sorunlar: İnternet ve Sosyal Medya Kullanıcılarının İnternet Güvenliği Ve Çevrimiçi Gizlilik İle İlgili Kanaatleri Ve Farkındalıkları Üzerine Bir Araştırma. *Gazi Üniversitesi Sosyal Bilimler Enstitüsü*. 3/1, (2015). 80-106.
- Barkuş, Fatma. - Koç, Mustafa. Dijital mahremiyet kavramı ve ilgili çalışmalar üzerine bir derleme. *Bilim Eğitim Sanat ve Teknoloji Dergisi*, 3/1, (2019). 35-44.
- Berkup, Sezin Baysal. Sosyal ağlarda bireysel mahremiyet paylaşımı: X ve Y kuşakları arasında karşılaştırmalı bir analiz. (Yayımlanmamış Doktora Tezi). *Sosyal Bilimler Enstitüsü, Ege Üniversitesi*. (2015).
- Bilbil, Emel Karayel - Atalay, Didem. Sosyal medya ekseninde mahremiyetin dönüşümü ve benlik inşası. *Global Media Journal TR Edition*, 10/20 (2020). 176-195.
- Budak, Hatice. Sosyal medya iletişiminde mahremiyetin serüveni. *Itobiad: Journal of the Human & Social Science Researches*, 7/1, (2018). 146-170.
- Çağlak, Uğur. Teşhir toplumu ve yeni medya: Teşhir toplumunun oluşmasında önemli bir araç olan yeni medya üzerine bir değerlendirme. *Kritik İletişim Çalışmaları Dergisi*, 2/2, (2020). 12-20.
- Connor, Brian - Doan, Long. Privacy Concerns in the Digital World. *The Dialectic of Digital Culture*, (2019). 47.
- Creswell. John Ward. Araştırma Deseni: Nitel, Nicel ve Karma Yöntem Yaklaşımları, 3. Baskı, Ankara: Eğiten Kitap. (2017).
- Eroğlu, Şahika. 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, (2018). 130-153.
- Fischer-Hübner, Simone. Privacy and security at risk in the global information society. *Information Communication & Society*, 1/4 (1998). 420-441.
- Fuchs, Christian. Sosyal medya: Eleştirel bir giriş. *Notabene Yayınları*. (2018).
- Han, Byung Chul. Şeffaflık Toplumu. *İstanbul: Metis Yayınları*. (2017).
- Kalaman, Sefer. Yeni medya ve dijital gözetim: Türkiye'deki sosyal medya kullanıcıları üzerine bir araştırma. *Yönetim ve Ekonomi Dergisi*, 26/2, (2019). 575-594.
- Marwick, Alice - boyd, Danah. Networked privacy: How teenagers negotiate context in social media. *New media & society*, 16/7, (2014). 1051-1067.
- Özdemir, Şebnem. Post-panoptikon çağı: Gözetimin dijitalleşmesi ve çevrimiçi kimliğin gizliliği üzerine bir analiz. *Anadolu Üniversitesi Sosyal Bilimler Dergisi* 20/3, (2020). 81-108.
- Prensky, Marc. Digital Natives, Digital Immigrants. *On The Horizon, Mcb University Press*, 9/5, (2001). 1-6.
- Romansky, Radi P. - Noninska, Irina S. Challenges of the digital age for privacy and personal data protection. *Mathematical Biosciences and Engineering*, 17/5, (2020). 5288-5303.
- Solove, Daniel J. Understanding privacy. *Harvard University Press*. (2021).
- Tufekci, Zeynep. Algorithmic harms beyond Facebook and Google: Emergent challenges of computational agency. *Colo. Tech. LJ*, 13, 203. (2015).
- Türk, Gül Dilek. - Demirci, Esra. Sanal dünyada dönüşen mahremiyet algısı; Instagram örneği. In *1st International Academic Research Congress*, (2016). 518-525.
- Westin, Alan. F. Privacy and Freedom. *Atheneum*. (1967).
- Yıldız Kakırman, Asiye Sosyal paylaşım sitelerinin dijital yerlilerin bilgi edinme ve mahremiyet anlayışına etkisi. *Bilgi Dünyası*, 13/2, (2012). 529-542.

EXTENDED ABSTRACT

Purpose

The purpose of this study is to explore the perceptions and practices related to digital privacy among high school students, who are among the most active users of digital technologies. Given the rapid development of digital technologies and the evolving nature of privacy, this research aims to assess the level of concern and awareness regarding digital privacy within this demographic group. Individuals who are not legally recognized as adults are often considered to be at a higher risk when it comes to privacy issues. The dual factors of growing up with digital technologies and facing significant privacy threats place high school students at the center of this study. Therefore, the research aims to gather both quantitative and qualitative data. This mixed-method study seeks to understand how high school students perceive, manage, and cope with digital privacy issues within the context of social media applications. Data were collected from students at 10 different high schools in Eskişehir within the scope of the concept of digital privacy.

Design and Methodology

This research was conducted using a mixed-method approach to achieve a comprehensive understanding of digital privacy among high school students. The mixed-method approach combines both quantitative and qualitative data collection and analysis techniques to offer a richer and more in-depth understanding. The methodology of the study consists of two main phases:

Quantitative Phase: In the first phase, a comprehensive survey was administered to a total of 1,371 students from various high schools in Eskişehir to assess their awareness and concerns regarding digital privacy. This survey aimed to evaluate students' levels of knowledge about digital privacy, their social media usage, and gender differences. The survey data were analyzed using IBM SPSS 23 software. During the analysis process, an ANOVA test was conducted to examine the relationship between students' awareness of digital privacy and their social media usage habits. Additionally, the analysis explored whether there were gender-based differences in students' attitudes towards digital privacy.

Qualitative Phase: In the second phase, semi-structured in-depth interviews were conducted with 15 high school students to support the quantitative findings. These interviews aimed to gain a more detailed understanding of students' personal experiences, concerns, and attitudes regarding digital privacy. The data obtained from the interviews were transcribed and analyzed using thematic analysis. Thematic analysis allows for the categorization of data into specific themes and categories, providing a broader understanding of the issues at hand. The qualitative data obtained during this phase revealed students' levels of awareness regarding digital privacy and their approaches to managing these concerns.

In both phases, necessary information was provided to the participating students and their parents, and an ethical research process was followed by obtaining signed consent forms from the participants.

Limitations

The research was limited to high school students in Eskişehir. This regional limitation may impose some restrictions on the generalizability of the study's findings. However, focusing on high school students in Eskişehir provides valuable insights into the specific dynamics of digital privacy concerns within this group. The study examined the perception and practices of digital privacy within the specific context of the level of access to digital technologies, socio-economic profiles, and local cultural factors in Eskişehir's educational institutions.

The current research addressed the concept of privacy within the digital domain and was confined to this scope. This means that the study focused solely on privacy issues occurring in digital environments. Traditional concepts of privacy, such as physical or social privacy, were excluded from the study's scope. Therefore, the findings should be evaluated only within the context of digital platforms and social media usage. These limitations allowed the study to develop a specific perspective on understanding privacy dynamics in the digital world, but they did not permit direct inferences regarding general privacy perceptions.

Implications

The findings of this study offer significant and noteworthy insights into digital privacy awareness and social media practices among high school students. The research has established a solid foundation for the steps that need to be taken and strategies that need to be developed by determining the level of awareness among high school students regarding digital privacy. The data obtained highlighted a potential lack of knowledge and insufficient awareness among young people concerning digital privacy, allowing for the development of various recommendations to improve this situation.

Educational Interventions: The results of the study clearly indicate the need for more targeted, comprehensive, and effective educational programs on the risks of digital privacy. To ensure security in the digital world, protect personal information, and develop conscious behaviors in this regard, educational modules that increase students' awareness of digital privacy are of great importance. Schools and educators should review their curricula and design programs and courses that teach students how to navigate the digital world more safely. Such education would not only help students better protect their personal information but also prepare them to face digital threats more effectively.

Parental Guidance: The study emphasizes the crucial role that parents play in monitoring and guiding their children's behavior in the digital world. It is evident that parents play a critical role in raising their children's awareness of digital privacy. Therefore, the development of educational and informative programs aimed at parents is of great importance. When parents are made more aware of the dangers in the digital world, they can provide more informed guidance to their children about the risks they may encounter online. In this way, they can play a more active role in protecting their children's digital privacy.

Policy Development: The findings of the study offer significant contributions toward the development of policies and regulations related to digital privacy. Particularly in the context of young people and social media use, the need for legal regulations that protect digital privacy is emphasized by this research. Policymakers can develop legal regulations that ensure students use digital technologies safely. Such regulations would not only protect young people's privacy rights in the digital world but also allow them to develop their digital skills.

Originality/Value

This study is original in its evaluation of digital privacy awareness among high school students in Eskişehir. No similar studies have been identified in this region before. By combining quantitative data with qualitative findings, it offers a detailed understanding of how students perceive digital privacy issues and how they cope with these issues. The study contributes to the existing literature by focusing on a specific demographic group (high school students) and provides actionable recommendations for educators, parents, and policymakers. The originality of this research lies in its comprehensive examination of concerns and practices related to digital privacy from both statistical and personal perspectives, filling a gap in current academic discussions on the digital privacy of young people. Additionally, due to the timeliness of the topic, there are few studies in this area. Of the studies available, very few employ mixed methods to produce findings, which is another unique value of this research.