



**HACETTEPE ÜNİVERSİTESİ**  
**EĞİTİM BİLİMLERİ ENSTİTÜSÜ**

Bilgisayar ve Öğretim Teknolojileri Eğitimi Ana Bilim Dalı

ORTAÖĞRETİM ÖĞRENCİLERİNİN DİJİTAL AYAK İZİ FARKINDALIKLARI VE BİLGİ  
GÜVENLİĞİ FARKINDALIKLARI ARASINDAKİ İLİŞKİNİN İNCELENMESİ

EDA SANİN

Yüksek Lisans Tezi

Ankara, 2022

Liderlik, arařtırma, inovasyon, kaliteli eđitim ve deđiřim ile

*Daha ileriye... En iyiye...*



Bilgisayar ve Öğretim Teknolojileri Eğitimi Ana Bilim Dalı

ORTAÖĞRETİM ÖĞRENCİLERİNİN DİJİTAL AYAK İZİ FARKINDALIKLARI VE BİLGİ  
GÜVENLİĞİ FARKINDALIKLARI ARASINDAKİ İLİŞKİNİN İNCELENMESİ

EXAMINING THE RELATIONSHIP BETWEEN HIGH SCHOOL STUDENTS' DIGITAL  
FOOTPRINT AWARENESS AND INFORMATION SECURITY AWARENESS

EDA SANİN

Yüksek Lisans Tezi

Ankara, 2022

## Kabul ve Onay

Eđitim Bilimleri Enstitüsü M¼d¼rl¼đ¼ne,

Eda SANİN'in hazırladıđı "Ortaöđretim Öđrencilerinin Dijital Ayak İzi Farkındalıkları ve Bilgi Güvenliđi Farkındalıkları Arasındaki İlişkinin İncelenmesi" başlıklı bu çalıřma j¼rimiz tarafından **Bilgisayar ve Öđretim Teknolojileri Eđitimi Ana Bilim Dalında Yüksek Lisans Tezi** olarak kabul edilmiřtir.

J¼ri Bařkanı

Doç. Dr. Yasemin DEMİRASLAN ÇEVİK

J¼ri Üyesi (Danıřman)

Doç. Dr. Gökhan DAĐHAN

J¼ri Üyesi

Doç. Dr. Çelebi ULUYOL

J¼ri Üyesi

Dr. Öđr. Üyesi Fatih ÖZDİNÇ

J¼ri Üyesi

Dr. Öđr. Üyesi Abdullah Yasin G¼ND¼Z

Bu tez Hacettepe Üniversitesi Lisansüstü Eđitim, Öđretim ve Sınav Yönetmeliđi'nin ilgili maddeleri uyarınca yukarıdaki j¼ri üyeleri tarafından 21 / 01 / 2022 tarihinde uygun gör¼lm¼ř ve Enstitü Yönetim Kurulunca ..... / ..... / ..... tarihi itibarıyla kabul edilmiřtir.

Prof. Dr. Selahattin GELBAL

Eđitim Bilimleri Enstitüsü M¼d¼r¼

## Öz

Bu çalışmanın amacı, ortaöğretim düzeyindeki öğrencilere yönelik olarak dijital ayak izi farkındalık ölçeği geliştirmek ve dijital ayak izi farkındalığı ile bilgi güvenliği farkındalığı arasındaki ilişkiyi incelemektir. Dijital ayak izi, bireyin çevrimiçi ortamlardaki davranışlarının tamamının kayıt altına alınması ile birey adına oluşan sanal bir kimliktir. Bilinçsiz internet kullanımı ile olumsuz bir sanal kimlik oluşmakta ve bireyin hayatını farklı dönemlerde olumsuz anlamda etkileyebilmektedir. Olumlu sanal kimlik oluşmasının da farkındalığın artmasının önemi büyüktür fakat bu farkındalık düzeyinin ne seviyede olduğunun da bilinmesi de önem arz etmektedir. Bu kapsamda ortaöğretim düzeyindeki öğrencilere yönelik bir DAFÖ (dijital ayak izi farkındalık ölçeği) geliştirilmiştir. Ölçek kişisel veri paylaşımı farkındalığı, kişisel veri paylaşımı uygulaması, sosyal medya kullanım farkındalığı ve sosyal medya kullanım uygulaması olmak üzere dört alt boyuttan oluşmaktadır. Araştırmanın ikinci boyutu olan dijital ayak izi farkındalığı ile bilgi güvenliği farkındalığı arasındaki ilişkinin incelenebilmesi için Güldüren, Çetinkaya ve Keser (2016) tarafından geliştirilen ve gerekli izinleri alınan Ortaöğretim Öğrencilerine Yönelik Bilgi Güvenliği Farkındalık Ölçeği ile araştırmacı tarafından geliştirilen Dijital Ayak İzi Farkındalık Ölçeği farklı bir gruba birlikte uygulanmıştır. Araştırmanın sonuçlarına bakıldığında dijital ayak izi farkındalığı ve bilgi güvenliği farkındalığı arasındaki ilişkinin yüksek olduğu görülmüştür. Sosyal medya kullanımı ve veri paylaşımı konularında farkındalığa sahip olan katılımcıların bunu uygulama oranları da yüksektir. Araştırma sonuçları arasında en düşük sayılabilecek ilişkinin saldırı ve tehditler ile mahremiyet arasında olduğu görülmüştür.

**Anahtar sözcükler:** dijital ayak izi, dijital ayak izi farkındalığı, ortaöğretim öğrencileri, bilgi güvenliği, bilgi güvenliği farkındalığı.

## Abstract

The purpose of this study is to develop a digital footprint awareness scale for high school students and to examine the relationship between digital footprint awareness and information security awareness. Digital footprint is a virtual identity formed on behalf of the individual by tracking all of the individual's behaviours in online environments. With irresponsible internet usage, virtual identity is formed with a negative infrastructure and this virtual identity can appear in different periods of the individual's life and affect the individual negatively. The prerequisite for a positive virtual identity is increased awareness. It is thought that the level of awareness should be known in order to increase awareness. In this context, a digital footprint awareness scale has been developed for high school students. The scale consists of four sub-dimensions. These are personal data sharing awareness, personal data sharing (implementation), social media usage awareness, and social media usage (implementation). In order to examine the relationship between digital footprint awareness and information security awareness, which is the second dimension of the study, the Information Security Awareness Scale for High School Students developed by Güldüren, Çetinkaya, and Keser (2016) was used. Based on result of research, it was seen that the relationship between information security awareness and digital footprint awareness was high. Participants who are aware of the social media usage and data sharing have a high rate of implementation. It has been seen that the lowest relation among the research results is between attacks, threats and privacy.

**Keywords:** digital footprint, digital footprint awareness, high school students, information security, information security awareness.

## Teşekkür

Tez hazırlık ve yazım süreci boyunca desteklerini hiç bir zaman esirgemeyen, her zaman en anlayışlı ve çözüm odaklı paylaşımlarıyla destek olan ve süreçte kendimi geliştirmemi sağlayan sayın danışmanım Doç. Dr. Gökhan DAĞHAN'a sonsuz teşekkürlerimi sunuyorum. Getirdiğiniz her öneri, yorum ve yaptığınız her yönlendirme attığım adımların sağlamlığı açısından bana daha çok güven verdi, verecek. Sabrınız, yönlendirmeleriniz sayesinde bu süreci mutlu bir şekilde tamamlayabilmek benim için çok anlamlı. Tüm emekleriniz için çok teşekkür ederim.

Tez savunmam sırasında yaptıkları dönüşler sayesinde tezime katkılarından dolayı sayın Doç. Dr. Yasemin DEMİRASLAN ÇEVİK'e, sayın Doç. Dr. Çelebi ULUYOL'a, sayın Dr. Öğr. Üyesi Fatih ÖZDİNÇ'e ve sayın Dr. Öğr. Üyesi Abdullah Yasin GÜNDÜZ'e sonsuz teşekkürler.

Süreç zaman zaman düşündürüp kimi zaman zorlasa da her aşamasında çokça öğrendiğim, yazdıkça kendimi geliştirdiğim, okumanın ve yazmanın sonunun olmadığını okudukça fark ettiğim ve tüm bu sebeplerle çokça zevk aldığım bir dönemdi. Bu süre zarfında desteklerini her zaman hissettiğim tüm arkadaşlarıma ve aileme de çok teşekkür ediyorum.

Yol uzun ve keyifli, öğrenmenin sonu yok. İyi ki başladı ve iyi ki devam ediyor. Öğrenmenin bitmeyeceği, öğrendikçe eksik hissedeceğim bu keyifli yolda yanımda olan ve olacak herkese sonsuz sevgiler.

## İçindekiler

Kabul ve Onay.....	ii
Öz.....	iii
Abstract.....	iv
Teşekkür.....	v
Tablolar Dizini.....	viii
Şekiller Dizini.....	ix
Simgeler ve Kısaltmalar Dizini.....	x
Bölüm 1 Giriş.....	1
Problem Durumu.....	1
Araştırmanın Amacı ve Önemi.....	4
Araştırma Problemleri.....	5
Sayıltılar.....	5
Tanımlar.....	5
Bölüm 2 Araştırmanın Kuramsal Temeli ve İlgili Araştırmalar.....	7
Dijital Ayak İzi ve Bilgi Güvenliği.....	7
Dijital Ayak İzi Farkındalığı.....	8
İlgili Araştırmalar.....	9
Bölüm 3 Yöntem.....	18
Araştırma Modeli.....	18
Araştırmanın Çalışma Grubu.....	18
Veri Toplama Aracının Geliştirilmesi.....	23
Kullanılan Veri Toplama Aracı.....	24
Veri Toplama Süreci.....	25
Verilerin Analizi.....	25
Bölüm 4 Bulgular ve Yorumlar.....	27
Dijital Ayak İzi Farkındalık Ölçeğinin Açıklayıcı Faktör Analizi (AFA) Bulguları.....	27



Dijital Ayak İzi Farkındalık Ölçeğinin Doğrulayıcı Faktör Analizi (DFA) Bulguları .....	35
Dijital Ayak İzi Farkındalık Ölçeği'nin İkinci Düzey Doğrulayıcı Faktör Analizi Sonuçları .....	40
Dijital Ayak İzi Farkındalık Ölçeğinin Güvenirlik Bulguları .....	44
Dijital Ayak İzi Farkındalığı ile Bilgi Güvenliği Farkındalığı İlişkisi .....	47
Bölüm 5 Sonuç, Tartışma ve Öneriler .....	51
Sonuçlar ve Tartışma .....	51
Öneriler .....	57
Kaynaklar .....	59
EK-A: Ortaöğretim Öğrencilerine Yönelik Dijital Ayak İzi Farkındalık Ölçeği .....	Ixiv
EK-B: Ortaöğretim Öğrencilerine Yönelik Bilgi Güvenliği Farkındalık Ölçeği Kullanım İzni.....	Ixvii
EK-C: Ortaöğretim Öğrencilerine Yönelik Bilgi Güvenliği Farkındalık Ölçeği .....	Ixviii
EK-Ç: Etik Komisyonu Onay Bildirimi .....	Ixx
EK-D: Etik Beyanı.....	Ixxi
EK-E: Yüksek Lisans Tez Çalışması Orijinallik Raporu.....	Ixxii
EK-F: Thesis Originality Report .....	Ixxiii
EK-G: Yayımlama ve Fikrî Mülkiyet Hakları Beyanı .....	Ixxiv

## Tablolar Dizini

<b>Tablo 1</b> Ölçek Geliştirme Aşamasındaki Araştırma Grubuna İlişkin Betimsel İstatistikler .....	18
<b>Tablo 2</b> Dijital Ayak İzi Farkındalığı ve Bilgi Güvenliği Farkındalığının Araştırıldığı Araştırma Grubuna İlişkin Betimsel İstatistikler .....	21
<b>Tablo 3</b> KMO ve Bartlett Testleri Sonuçları.....	27
<b>Tablo 4</b> Açıklanan Toplam Varyans Dağılımları.....	28
<b>Tablo 5</b> Bileşen Matrisi ve Faktör Yüklerinin Dağılımı.....	30
<b>Tablo 6</b> Varimax Döndürmesi Sonucu Oluşan Açıklanan Toplam Varyans Dağılımları.....	32
<b>Tablo 7</b> Döndürülmüş Bileşen Matrisi ve Faktör Yüklerinin Dağılımı .....	33
<b>Tablo 8</b> Birincil Düzey Doğrulayıcı Faktör Analizinde Uyum İyiliği İndekslerine İlişkin Bulgular.....	36
<b>Tablo 9</b> Birincil Düzey Doğrulayıcı Faktör Analizinde Modifikasyon Sonrası Uyum İyiliği İndekslerine İlişkin Bulgular.....	37
<b>Tablo 10</b> İkinci Düzey Doğrulayıcı Faktör Analizinde Modifikasyon Sonrası Uyum İyiliği İndekslerine İlişkin Bulgular.....	40
<b>Tablo 11</b> Dijital Ayak İzi Farkındalık Ölçeği Cronbach Alpha İç Tutarlılık Katsayıları .....	44
<b>Tablo 12</b> Dijital Ayak İzi Farkındalığı ile Bilgi Güvenliği Farkındalığı arasındaki ilişkileri gösterir Pearson Korelasyon Katsayıları.....	48

**Şekiller Dizini**

<b>Şekil 1</b> Öz Değer ve Bileşen Sayılarına Ait Yamaç Eğim Grafiği .....	30
<b>Şekil 2</b> Dijital Ayak İzi Farkındalık Ölçeğinin Birinci Düzey Doğrulayıcı Faktör Analizi Bağlantı Diyagramı (Standart Katsayılar) .....	38
<b>Şekil 3</b> Dijital Ayak İzi Farkındalık Ölçeğinin Birinci Düzey Doğrulayıcı Faktör Analizi Bağlantı Diyagramı (t Değerleri) .....	39
<b>Şekil 4</b> Dijital Ayak İzi Farkındalık Ölçeğinin İkinci Düzey Doğrulayıcı Faktör Analizi Bağlantı Diyagramı (Standart Katsayılar) .....	42
<b>Şekil 5</b> Dijital Ayak İzi Farkındalık Ölçeğinin İkinci Düzey Doğrulayıcı Faktör Analizi Bağlantı Diyagramı (t Değerleri) .....	43

## Simgeler ve Kısaltmalar Dizini

**BT:** Bilişim Teknolojileri

**DLEARN:** European Digital Learning Network

**RMSEA:** Root Mean Square Error of Approximation (Yaklaşık Hataların Ortalama Karekökü)

**CFI:** Comparative Fit Index (Karşılaştırmalı Uyum İndeksi)

**GFI:** Goodness of Fit Index (İyilik Uyum İndeksi)

**NFI:** Normed Fit Index (Normlaştırılmış Uyum İndeksi)

**NNFI:** Non-normed Fit Index (Normlaştırılmamış Uyum İndeksi)

**AGFI:** Adjusted Goodness of Fit Index (Düzenlenmiş İyilik Uyum İndeksi)

**S-RMR:** Standardized Root Mean Square Residuals (Standardize Edilmiş Artık Ortalamaların Karekökü)

**KMO:** Kaiser – Meyer – Olkin Örneklem Uygunluğu Değeri

$\chi^2$ : Ki Kare Değeri

## Bölüm 1

### Giriş

Bu bölümde problem durumu, araştırmanın amacı ve önemi, problem cümlesi, sayılılar, sınırlılıklar ve tanımlar yer almaktadır.

#### Problem Durumu

İnternet kullanımının giderek artması, bilgiye erişimin kolaylığı, olumlu gelişmelerin yanı sıra bazı olumsuz sonuçların doğmasına da neden olabilmektedir (Çelen, Seferoğlu ve Çelik, 2011). Londra merkezli bir sosyal medya kuruluşu olan We Are Social'ın Hootsuite ile işbirliği içerisinde hazırladığı "Digital 2020 Global Overview" raporuna göre dünya genelinde 4.5 milyar insanın internet kullandığı, bunların 3.8 milyarının ise sosyal medya kullanıcısı olduğu belirtilmiştir (We Are Social, 2020). Türkiye verilerine bakıldığında ise internet kullanımı %4,6 oranında artmıştır. Bu da var olan sayının 3 milyara yakın arttığı anlamına gelmektedir. İnternete erişen her bireyin dijital bir kimliğinin oluştuğu göz önüne alındığında yaygın internet kullanımı ile birlikte, dijital ayak izi konusu ve bu konuda geliştirilen farkındalık da gün geçtikçe önem kazanmaktadır. Dijital Ayak izi, dijital ortamda kullanıcıya ait kayıt altına alınan tüm işlemler olarak tanımlanabilir (Sürmeliöğlu ve Seferoğlu, 2019). Başka bir tanım ile kurumların veya bireylerin çevrimiçi etkileşimde buldukları zaman geride bıraktıkları iz şeklinde daha kapsayıcı bir hale gelmiştir (Bodhani, 2012). Bu tanımlardan hareketle bireylerin çevrimiçi ortamda her türlü etkileşimi sonucu bıraktığı iz dijital ayak izi olarak tanımlanabilir. Bu etkileşimlere, e-posta gönderimi, sosyal medya paylaşımları, çevrimiçi mesajlaşmalar örnek olarak verilebilir. Dijital ayak izi tanımlardan hareketle düşünüldüğünde günümüzde oldukça önemli ve dikkat edilmesi gereken bir kavramdır. Her çevrimiçi ortam kullanıcısının bilmesi, farkında olması ve bıraktığı dijital ayak izlerini kontrol altına alabiliyor olması gerekmektedir. Aksi takdirde düşünmeden ve deneyimsiz yapılan fare ve klavye tıklamaları gelecekteki iş hayatında ya da üniversite kabulünde gençlerin önüne bir engel olarak çıkabilmektedir (O'Keeffe, Clarke-Pearson, & Council on Communications and Media, 2011). Thompson

(2012) da benzer şekilde bireylerin internet ortamında ifade ettikleri, yaptıkları ve paylaştıklarının zamanla dijital ayak izine evrildiğini belirtmiştir. Aynı zamanda değiştirilmesi kolay olmayan dijital ayak izlerinin ekran ile etkileşimden, dijital ortamlardaki paylaşımlardan ve arama motorları sonuçlarından oluştuğunu da ifade etmiştir (Thompson, 2021). Yaygın çevrimiçi ortam kullanımı ile da oluşan dijital ayak izlerinin büyüklüğünde artmaktadır (Malhotra, Totti, Meira, Kumaraguru, & Almeida, 2012). Bu dijital ayak izleri bireyler hakkında oldukça önemli bilgiler içermektedir ve yeri geldiğinde bu bilgiler birey aleyhine kullanılması mümkün görünmektedir.

Bireyin dijital ayak izini doğru yönetebilmesi için iyi bir çevrimiçi ortam kullanıcısı olması gerekir. Çevrimiçi olarak zaman geçiren, bir ya da birden fazla cihazla bağlantı kuran, arkadaşları, ailesi ve meslektaşlarıyla dijital yoldan irtibat kuran herkes birer dijital vatandaşdır (eTwinning, 2016). Buradan hareketle çevrimiçi ortamlarda vakit geçiren her bireyin birer dijital vatandaş olduğu söylenebilir. Yaş dijital vatandaşlık açısından herhangi bir belirleyici olmasa da Ribble (2011) çocuklara çok erken yaşlardan itibaren dijital araçların doğru ve etkili kullanımının öğretilmesi gerektiğini ve ancak bu şekilde dijital vatandaşlık algısının oluşturulabileceğini belirtmiştir. Mossberger, Tolbert ve McNeal (2007) dijital vatandaşlığı teknoloji kullanımına ilişkin davranış normları olarak, başka bir deyişle, teknolojiyi kullanırken etik ve uygun davranışlarda bulunma ve bu konuda bilgilenme olarak tanımlamaktadırlar. Dijital vatandaş, dijital ortamda iletişim kurabilen, bilgi üretebilen, bilgiyi kullanabilen ve kullanırken eleştirebilen, dijital ortamda alışveriş yapabilen, dijital ortamdan eğitim alabilen ve bu davranışları yaparken etik kurallara uyan, hak ve sorumluluklarının bilincinde olan bireylerdir (Kuh Karyeli ve Dağhan, 2020).

Çevrimiçi ortamları doğru bir şekilde kullanmayı öğrenen her birey ileride yaşayabileceği sorunları en aza indirerek iyi birer dijital vatandaş olabilir. Çevrimiçi ortamların güvenli ve etkin bir şekilde kullanımında bu konudaki farkındalık önemlidir. Alanyazında bu farkındalık "dijital ayak izi farkındalığı" (digital footprint awareness) olarak anılmaktadır. Dijital ayak izi farkındalığı, medya okuryazarı olmanın ve modern topluma tam olarak katılabilmenin

öncüsü ve teknik becerilerin (genellikle dijital okuryazarlık olarak adlandırılır) ve bilişsel becerilerin (bilgi edinme ve çevrimiçi aktivitelerin etkilerini anlama kapasitesi) edinilmesi için gerekli bir ön koşuldur (EAVI, 20 2019). Ayrıca, bireylerin dijital ayak izleri üzerinde uyguladıkları mevcut ve istenen kontrol seviyeleri ve gelecekte uygulamak istedikleri koruma ve önlemleri de bu kapsamda düşünülebilir (EAVI, 2019). Kısaca, bireylerin dijital ayak izlerini yönetebilmeleri için dijital ayak izi farkındalığına sahip olmalıdır. Uluslararası alanyazında dijital ayak izi farkındalığı (digital footprint awareness) şeklinde adlandırılmakta ve henüz okul çağlarındayken öğrencilere kazandırılması gerektiği ileri sürülmektedir (EAVI, 2019). Ayrıca ülkemizde son dönemde ortaöğretim Bilişim Teknolojileri ve Yazılım dersinin müfredatına bakıldığında dijital kimlik, sosyal medya, dijital vatandaşlık, gizlilik, güvenlik gibi konuların da ele alındığı görülmektedir (MEB, 2020). TÜİK 2021 verileri incelendiğinde internet kullanımı, 6-15 yaş grubundaki çocuklar için 2013 yılında %50,8 iken 2021 yılında %82,7 olduğu görülmektedir. Bu oran oldukça yüksek olmakla beraber dijital ayak izi kavramının önemini de tekrar göz önüne getirmektedir. İnternet kullanımının çocuklar arasında bu kadar artması sonucu bırakılan dijital ayak izleri de artacak, bunun kontrol edilmesi zorlaşacaktır. Bu durum da bu yaş grubundaki bireylerin dijital ayak izini yönetebilmeleri, bir diğer ifade ile dijital ayak izi farkındalığına sahip olmaları önem arz etmektedir.

Bu kapsamda ortaöğretim çağındaki bireylerin dijital ayak izi farkındalıklarının belirlenmesi, bu sebeple de bu psikometrik yapıyı ölçecek bir ölçeğin geliştirilmesi bunun yanında bilgi güvenliği ile ilişkisinin incelenmesi önem arz etmektedir. Güldüren, Çetinkaya ve Keser (2016) yaptıkları çalışmada dijital ayak izi kavramına benzer şekilde öğrencilerin gezintileri sonucu dijital ortamda güvenliklerini ve gizliliklerini sağlamalarının önemini vurgulamışlardır. Dijital ortamlarda yapılan gezintilerde bırakılan her izin kişisel güvenliği de tehdit ettiği bilinmektedir. Buradan hareketle dijital ayak izi farkındalığı kavramının bilgi güvenliği farkındalığı kavramı ile ilişkisi olduğu düşünülmektedir. Bu ilişkinin saptanması öğrenciler açısından verilen farkındalık eğitimlerinde dikkat edilmesi, ön plana çıkarılması gereken konuların neler olduğu konusunda yardımcı olacağı düşünülmektedir.

## **Araştırmanın Amacı ve Önemi**

Çevrimiçi ortamların kullanımının son yıllarda bu kadar artması, çevrimiçi ortam kullanımının oldukça erken yaşlara inmesi, bilinçli veya bilinçsiz internet kullanımını da beraberinde getirmiştir. Özellikle küçük yaştaki çocukların bilinçsiz internet kullanımlarının birçok olumsuz sonucu olabilir. Bilinçsiz kullanımın, bireylerin hayatlarının farklı dönemlerinde eylemlerini etkileyecek şekilde karşılına çıkabileceği unutulmamalıdır. Canbek ve Sağıroğlu (2007) tarafından yapılan çalışmada İnternet'in yoğun ve denetimsiz bir şekilde kullanımının, internet kullanıcıları olarak sayıları hızlı bir şekilde artan çocuklar için ortaya koyduğu birtakım risk ve tehditler üzerinde durulması gerektiği vurgulanmıştır. Acele'nin (2020) araştırmasında, gençler ve çocukların kişisel mahremiyetlerini koruma konusunda dikkatsiz davranabildikleri, interneti güvenli bir şekilde kullanmaktan uzaklaşabildikleri ve farkında olmadan risk alabildikleri belirtilmiştir. Buradan hareketle bilinçsiz internet kullanımı sonucu kullanılan çevrimiçi ortamda bırakılan izler, diğer bir deyişle olumsuz dijital ayak izi, önemli bir konu haline gelmektedir.

Türkiye'de bu konu kapsamında alanyazına bakıldığında ortaöğretim, ortaokul ve ilkokul çağındaki çocukların dijital ayak izi farkındalığının belirlenmesi amacıyla az sayıda çalışma yapıldığı ve ortaöğretim düzeyinde ölçek olmadığı görülmüştür. Bireylerin, özellikle genç yetişkinlerin bu konudaki farkındalıklarının üzerine çalışılabilmesinin, farkındalığın geliştirilebilmesi açısından önem arz ettiği düşünülmektedir.

Bilişim Teknolojileri ve Yazılım dersi müfredatı içerisinde dijital kimlik, dijital ayak izi, etik, gizlilik ve güvenlik konularının da incelenmesinden hareketle öğrencilerin dijital ayak izi farkındalıkları ve bilgi güvenliği farkındalıkları arasında bir ilişki olduğu düşünülmektedir. İlişkinin saptanması durumunda bu çalışmanın alanyazına ve ilgili öğretim programındaki kazanımların kazandırılması sürecine katkı getirebileceği öngörülmektedir.



## **Araştırma Problemleri**

1. Öğrencilerin kişisel veri paylaşımı farkındalığı ve bunu uygulama düzeyleri ne durumdadır?
2. Öğrencilerin sosyal medya kullanımı farkındalığı ve bunu uygulama düzeyleri ne durumdadır?
3. Öğrencilerin bilgi güvenliği farkındalık durumları ne durumdadır?
4. Öğrencilerin dijital ayak izi farkındalıkları ve bilgi güvenliği farkındalıkları arasında bir ilişki var mıdır?

## **Sayıtlılar**

Geliştirilen Dijital Ayak İzi Farkındalık Ölçeği ile 2016 yılında Güldüren, Çetinkaya ve Keser tarafından geliştirilen ve kullanım için gerekli izinleri alınan Bilgi Güvenliği Farkındalık ölçeğinin uygulanması sonucunda elde edilen bulguların var olan durumu ortaya koyduğu varsayılmıştır. Öğrencilerin ölçek sorularına içtenlikle cevap verdikleri varsayılmıştır.

## **Sınırlılıklar**

Bu çalışmanın sonuçları 2020-2021 eğitim-öğretim yılında Ankara'da iki ortaöğretim kurumunda öğretim gören öğrencilerden oluşan örneklem grubunun yanıtları ile sınırlıdır.

## **Tanımlar**

**Kişisel Veri Paylaşımı:** Bireyler gerek kullandıkları sosyal ağlarla gerekse herhangi bir çevrimiçi ortamda fiziksel, ekonomik, kültürel, sosyal veya psikolojik özelliklerini ifade eden paylaşımlar yapabilmektedirler. Bu kapsamda bireylerin çevrimiçi ortamda kendileri hakkında bilgi sunabilecekleri her türlü paylaşımları, kişisel veri paylaşımı olarak tanımlanmaktadır.

**Sosyal Medya:** Kişilerin fotoğraf, video, metin v.b paylaşımlar yapabildiği, diyaloglarını sürdürebildiği çevrimiçi ortamlar.

**Dijital Ayak İzi:** Yaygınlaşan internet kullanımı ile bireylerin çevrimiçi ortamlarda etkileşimde bulunma oranı da artmaktadır. Buna bağlı olarak artan etkileşimler birey hakkında gerek sosyal ve kültürel gerekse psikolojik anlamda birçok ipucunu ortaya koymaktadır. Dijital ayak izi kurumların veya bireylerin çevrimiçi etkileşimde buldukları zaman geride bıraktıkları izdir (Bodhani, 2012).

**Dijital Vatandaşlık:** Bireyler dijital ortamları kullanırken birçok etkileşimde bulunmaktadır. Bu etkileşimler birey hakkında fikir vererek onun bir profilini çizmekle beraber bireylerin de bu dijital ortamları kullanırken birtakım sorumlulukları üstlenmesi gerektiğini ve bu sorumlulukları üstlenirken hangi haklara sahip olduğunu da bilmesini gerekli kılar. Dijital vatandaşlık en genel kapsamı itibariyle teknoloji kullanımına ilişkin hak ve sorumluluklar bütününde yer alan davranış normları olarak ifade edilmektedir (Çubukçu ve Bayzan, 2013).

**Dijital Ayak İzi Farkındalığı:** Bireyler dijital ortamları kullanırken etkileşimleri sonucu kendileri hakkında sosyal, kültürel ve psikolojik izler bırakmaktadır. Bu izlerin bireyler hakkında birçok bilgiyi barındırdığı ve bunun bireyin gelecek yaşamını etkileyebileceği bilinen bir gerçektir. Bireyin bıraktığı tüm bu izler konusunda bilgi sahibi olması ve bunun farkında olarak çevrimiçi ortamlardaki eylemlerini şekillendirmesi elzemdir. Dijital ayak izi farkındalığı, bireylerin internette bıraktıkları izler ve bu izlerin beraberinde getirdiklerine ilişkin bireylerin farkındalık düzeyleridir (Acele, 2020).

## Bölüm 2

### Araştırmanın Kuramsal Temeli ve İlgili Araştırmalar

Bu kısımda, tezin anahtar kavramları olarak dijital ayak izi ve dijital ayak izi farkındalığı kavramlarına yer verilmiş ve ilgili araştırmalar sunulmuştur.

#### Dijital Ayak İzi ve Bilgi Güvenliği

Dijital ayak izi genel anlamı ile bireylerin çevrimiçi ortamlarda bıraktıkları izlerdir. Bırakılan izler, paylaşılan gönderiler ve fotoğraflardan, e-postalardan, izlenen videolardan, paylaşılan kişisel bilgilerden v.b birçok farklı ortamdan olabilir. Bu izler kimi zaman bilinçli, kimi zaman bilinçsiz bir şekilde bırakılmaktadır. "Dijital ayak izi klavyeden, fareden ya da ekrandan, tuşlayarak, tıklayarak ya da dokunarak elektronik ortama aktarılan bireyle ilgili her türlü iz" şeklinde tanımlanmaktadır (Akkoyunlu, 2016). Avustralya Haberleşme ve Medya Kurumu (ACMA), "dijital ayak izleri" terimini, insanların çevrimiçi ortamda geride bıraktıkları iz veya "ayak izleri" şeklinde tanımlamıştır (ACMA, 2013).

Bireyin her türlü hareketinden, veri gönderip almasından, bir veri izlemesinden hareketle birey hakkında farklı bir veri toplanır. Toplanan veriler bütününde birey için bir dijital kimlik ortaya çıkar. Avustralya Haberleşme ve Medya Kurumu (ACMA), "dijital kimlik", gerçek bir kişinin özelliklerini yansıtabilecek veya yansıtmayacak bir dizi belirleyici özellik içeren bir dijital bilgi topluluğudur (ACMA, 2013). Bu kimlik içerisinde birey açısından önem arz eden pek çok veri bulunabilir. Bu veriler kimi zaman bir kurum, kimi zaman başka birey tarafından kullanıma açık olabilir. Bu verilerin pazarlama, reklam gibi farklı açılardan kullanılması günümüzde sık karşılaşılan bir durumdur. Bu durumun birey açısından mevcut ve ilerleyen dönemlerdeki eylemlerinde belirleyici sonuçlar doğmasına olanak sağlaması muhtemeldir. Birey hakkında bu kadar bilgi edinilmesi, sektör açısından oldukça kârlı görünse de bireyin hem özel hayatı hem sosyal hayatı hem de gelecek yaşantısı için risk oluşturabilir.

Bilginin korunması ve güvenli bir biçimde iletilmesi, kişisel verilerin güvenliğinin sağlanması, büyük verilerin depolanması vb. noktalarda güvenlik konusu ön plana çıkmaktadır

(Dönmez, 2019). Bilgi güvenliği, bir varlık türü olarak bilginin izinsiz veya yetkisiz bir biçimde erişimini, kullanımını, değiştirilmesini, ifşa edilmesini, ortadan kaldırılmasını, el değiştirmesini ve hasar verilmesini önlemek olarak tanımlanabilir (Keser ve Güldüren, 2015). Günümüzde, bilgi sistemlerinin küreselleşmesi sonucunda bu sistemlerle doğrudan veya dolaylı yönden ilişkili olan ve bu sistemleri kullanan tüm birey ve kurumların artık bilgi güvenliğine katkıda bulunması gerekmektedir (Özcan, 2009; Vardal, 2009; Vural ve Sağıroğlu, 2011). Bilgi güvenliği risklerinden korunmanın en iyi yolu bilgi teknolojilerine çok para harcamak ve korunma amaçlı teknolojileri daha çok kullanmaktan önce, insanların bilinçlenmesi ve ihtiyaç duyulan güvenlik teknolojisini doğru yer ve zamanda kullanmakla mümkün olabilir (Puhakainen, 2006; Siponen, 2001; Şahinaslan, Kantürk, Şahinaslan ve Borandağ, 2009).

Bilgi güvenliği ilerleyen teknolojik gelişmeler ile birlikte birçok kurum, kuruluş tarafından özenle çalışılan ve dikkat edilen bir nokta haline gelmiştir. Fakat burada bireylerin kendi kişisel bilgi güvenliklerini sağlaması özellikle sosyal ortamlarda geçirdikleri vakit düşünüldüğünde oldukça önemli bir konu haline gelmiştir. Dijital ayak izi tanımlanırken “bireylerin çevrimiçi ortamlarda bıraktıkları izler” ifadesi kullanılmıştır. Buradan hareketle bıraktıkları bu izlerin kişilerin güvenliklerini tehdit etmemesi, dijital ayak izlerinin kişilerin kontrolünde olması, farklı bir ifade ile davranışlarının farkında olmaları da önem arz etmektedir. Bu sebeple dijital ayak izi ve bilgi güvenliği kavramlarının birbirleri ile ilişkili olduğunu düşünülmektedir.

### **Dijital Ayak İzi Farkındalığı**

Dijital ayak izi genel anlamı ile bireylerin çevrimiçi ortamlarda bıraktıkları izlerden meydana gelmektedir. Dijital ayak izi farkındalığı ise bireyin bu izleri bırakırken, bıraktığı izleri fark etme ve davranışlarını buna göre yönlendirme düzeyi olarak düşünülebilir. Dijital ayak izi farkındalığı, medya okuryazarı olmanın ve modern topluma tam olarak katılabilmenin öncüsü ve teknik becerilerin (genellikle dijital okuryazarlık olarak adlandırılır) ve bilişsel becerilerin (bilgi edinme ve çevrimiçi aktivitelerin etkilerini anlama kapasitesi) edinilmesi için gerekli bir ön koşuldur (EAVI, 2019).

Bireylerin çevrimiçi ortamlardaki eylemleri üzerinde bilişsel olarak kontrol sağlayabilmeleri ve teknik olarak yeterli ve kontrollü olmaları dijital ayak izi farkındalığı açısından bilinçli olmalarının ön koşulu olarak düşünülmektedir. Bu kapsamda bireylerin çevrimiçi eylemlerinin sonuçlarının farkında olmaları o ortamda oluşacak kimlik açısından önemlidir. Birçok ülkenin hükümeti ve işverenleri internet kullanıcılarının kendilerini tanımlaması gerektiği yerde karşılaştıkları yanlış ve yanıltıcı bilgiler dolayısıyla yaşadıkları karmaşıklık ve zorluklardan bahsetmişlerdir (ACMA, 2013). Bu bağlamda güvenilir kimlikler, yaşanılacak sahtekârlıklar ve yetkisiz veri toplama gibi olumsuz faaliyetleri azaltmak için önemlidir (Acele, 2020). Ramachandran (2016), yaptığı bir çalışmaya katılanların %80'inin internet verilerinden tanımlanabileceği bulgusuna ulaşmıştır. Bu bulgu veri toplayan şirketlerin bireyler hakkında ulaşabildiği verilerin önemini vurgulamaktadır. Veri toplamanın önüne geçmek, bireylerin bu işletmeler ile çalışmalarını sürdürdükleri göz önüne alındığında oldukça güçtür. Bu sebeple, dijital ayak izi farkındalığı çevrimiçi ortamlardaki gizlilik tutumunun gelişmiş olması ile ilişkilidir.

### **İlgili Araştırmalar**

Buchanan, Scevak, Smith ve Southgate (2016) Avustralya'da çocukların ve gençlerin yaygın sosyal medya kullanımına rağmen dijital ayak izinden ne anladıklarına yönelik bilgi eksikliğini vurgulayarak, ilkökul öğrencilerinin ve yükseköğrenim öğrencilerinin dijital ayak izinden ne anladıklarını odak grup görüşmeleri ve Delphi anketinin bulgularını sunmuşlardır. Amaç öğrencilerin dijital ayak izi yönetimine yardımcı strateji geliştirmelerini desteklemektir.

53 uzman ile (akademik çalışanlar, araştırmacılar, politikacılar, öğretmenler, üniversite kariyer danışmanları) yapılan Delphi çalışması sonucu belirtilenler; verilen eğitimler, eğitimi alanların gelişimi ile aynı doğrultuda ve gelişimsel olmalıdır, çocukların çevrimiçi ortamlardaki paylaşımların uzun ömürlülüğü konusunda yeterli bilişsel gelişime sahip olmadıkları konusunda endişe duyulmaktadır, soruna bütüncül olarak yaklaşılarak eğitim aileden, okullardan, hükümetten ve üniversitelerden gelmelidir. İlkokul öğrencileri (10-12 yaş) ile

yapılan çevrimiçi anket sonucu ise; siber güvenliğin farkındadırlar, farklı düzeylerde ebeveyn desteği alınmaktadır, dijital ayak izlerinin ne olduğunun farkındadırlar ve bunun sonuçlarını açıklayabilmektedirler. 635 üniversite öğrencisinin doldurduğu çevrimiçi anketten elde edilen sonuçlar ise, yayınlanması tavsiye edilmeyen içerikleri yayınlama olasılıkları yüksektir, profesyonel sosyal ağları duyma, kullanma ve içerik oluşturma olasılıkları düşüktür, profesyonel sosyal medya ağlarını bilme olasılıkları yüksektir.

Odak grup görüşmeleri sonucu ise (1 üniversiteden 30 kişi), mahremiyet haklarının farkında oldukları fakat sahip olduklarını hissetmedikleri, dijital ayak izini sorumluluk olarak gördükleri fakat kendilerini çevrimiçi ortamda savunmasız olarak algıladıkları yönündedir. Ayrıca öğrenciler korunma amaçlı, gizlilik ayarlarını kullanma, anonim kalma, profilleri kilitli kullanma veya herkese açık olsa bile herhangi bir paylaşımında bulunmama konularında dikkatli oldukları araştırma sonuçlarındandır.

Buchanan, Southgate, Smith, Murray ve Noble, 2017 yılında yaptıkları bir araştırmada, Avustralya'daki 3 okuldan 33 çocuk ile (10-12 yaş aralığı) dijital ayak izi farkındalığını araştırdıkları bir odak grup çalışması yürütmüşlerdir. Çocuklara, dijital ayak izinin ne olduğu, Google'da arattıklarında karşılıklarına ne çıkacağını düşündükleri, çevrimiçi ortamlarda neler yaptıkları, internete hangi cihazlardan eriştikleri ve internet hakkında ne bilmek istedikleri sorulmuştur. Çalışmanın sonucunda çevrimiçi ortamlarda arkadaş ve aile ile iletişim için, okul araştırmaları için, Youtube'da video izlemek için, çevrimiçi oyunlar oynamak için ve ilgi alanlarını keşfetmek için kullandıklarını belirtmişlerdir. Öğrencilerin çoğu dijital ayak izini tanımlayabilmiş ve bunların davranışları üzerindeki etkileri belirtebilmiştir. Çocuklar siber güvenliğin farkındadırlar ve aynı zamanda çevrimiçi risklerin en aza nasıl indirilebileceğine dair açıklamalarda bulunmuşlardır. Buradan hareketle çocukların dijital ayak izi ve siber güvenlik açısından farkındalıklarının yüksek olduğu söylenebilir. Ayrıca çalışmanın bir başka bulgusu da ilköğretimin son iki yılının (10-12 yaş aralığı) dijital ayak izi hakkında eğitim vermenin en uygun yaş aralığı olduğudur.

Koidl, Reijers, Farrell ve Hoover (2018) yaptıkları arařtırmada 300 katılımcının sosyal medyada bıraktıkları dijital ayak izlerinin farkında olup olmadıklarını belirlemeye yönelik bir arařtırma tasarlamıřlardır. Toplam 289 kullanıcı ile gerekleřtirilen arařtırma kullanıcılara evrimii davranıřları ile ilgili doldurtulan bir anket ve bu davranıřları sergilemek durumunda kaldıkları bir uygulama zerinden yrtlmřtr. Facebook zerinden kullanıcıların aık izinleri ile 3 ay sreyle veri toplamıřtır. Bu veriler etiketlemeler, beğeniler ve fotoğraflara yönelik verilerdir. Ankette sorulan sorular ise, gnderi paylařma sıklığı, etiket kullanma sıklığı, makale baėlantıları paylařma sıklığı, arkadař gnderilerinin paylařılma sıklığı, arkadařları gnderilere etiketleme sıklığı, kendi kendini kendi gnderine etiketleme sıklığı ve arkadařların gnderine etiketlenme sıklığı gibi konular zereindedir. Sonular katılımcıların kendilerini gerekte olduėundan daha aktif olarak algıladıklarını gstermektedir. Anket sonuları, etiketleme sıklıklarının ok fazla olduėu ynndedir fakat uygulama verilerinde kendilerinden ziyade bařkalarını etiketleme davranıřları sergilediklerini gstermiřtir. Etkinlikler bazında “gidiyor” tarzında yapılan iřaretlemeleler yalnızca hatırlatma aracı olarak kullanılması sebebi ile farkındalığın bu ynde az olduėu, aık profil kullanma konusunda markaların, řirketlerin kullandıėı ynnde fikir belirterek kendilerinin kullanmadığını, bu sebeple bu konuda farkındalıklarının artan dzeyde olduėu ortaya konulmuřtur.

Temmuz 2018-Aėustos 2019 yılları arasında DLEARN tarafından Avrupa vatandařları ile yapılan bir arařtırmada, vatandařların dijital ayak izlerine karřı genel bilgi dzeylerini, farkındalıklarını ve tutumlarını belirlemek, bilinli olarak evrimii ortamlarda aıkladıkları bilgiler hakkında veri toplamak amalanmıřtır. Veri toplama srecini kolaylařtırmak ve Avrupa vatandařları arasında mmkn olduėunca ok cevap elde etmek iin anket sadece İngilizce deėil, diėer 12 Avrupa dilinde de mmkn olan tm iletiřim kanallarından daėıtılmıřtır. Bir yılda toplam 19.728 yanıt toplanmıřtır.

Katılımcıların lkelere yönelik katılımları, Belika %10,14, Fransa %9,81, İtalya %6,70, Yunanistan %4,5, İngiltere %12,35, Portekiz %7,97, Almanya %9,78, İrlanda %6,88, Romanya %3,5, Bulgaristan %3,7, İspanya %5,6 řeklindeedir. Ankette sonu olarak, dijital ayak izi ile ilgili

konularda hala yanlış anlaşılmalarda olduğu görülmektedir. Katılımcılar çoğunlukla yetişkinlerdir ve yüksek seviyede eğitilmiştirler. Çoğunun gizlilik politikalarını tam olarak okumadıkları görülebilir. Özellikle kişisel verilerin paylaşılması ile ilgili olarak kuralların uygulanmadığı söylenebilir. İnternetin güvenli ve dikkatli kullanımı konusunda hassas oldukları dile getirilse de dijital ayak izi konularında yanlış anlaşılma noktaları olduğu sonuçlarda görülmektedir. Açık bir şekilde paylaştıkları kişisel verilerinin korunduğuna emin olduklarını dile getirdikleri halde sahte haberlerin kurbanı olduklarını da belirtmeleri tartışılması gereken bir konudur. Bir diğer sonuç katılımcıların reklamlar, özel modda gezinme gibi bazı hileleri ve araçları kullanmak için doğru yetkinliğe sahip olmadıklarını yönündedir. Araştırmacılar bu sonuçlar ve katılımcıların daha fazla destek istemeleri sebebiyle sosyal medya aracılığıyla daha fazla destek verilebileceğini belirtmektedirler.

Sürmeliolu ve Seferoğlu (2019) yükseköğretim öğrencilerinin dijital ayak izi farkındalıkları ve dijital ayak izi bağlamında yaşantılarını belirlemek üzere bir araştırma yürütmüşlerdir. Çalışmada iki ayrı veri toplama aracı geliştirilmiştir. Bu ölçeklerden biri "Kişisel Bilgi Formu" dur. Kullanılan diğer veri toplama aracı ise "Yükseköğretim Öğrencilerinin Dijital Ortamları Kullanma Durumları Anketi"dir. Araştırmanın sonuçlarına bakıldığında Sürmeliolu ve Seferoğlu (2019), yükseköğretim öğrencilerinin dijital ayak izi farkındalıklarının yüksek düzeyde olduğunu, yükseköğretim öğrencilerinin dijital ayak izi farkındalıklarının cinsiyete göre farklılık göstermediğini, yaş değişkenine ilişkin yapılan değerlendirmelerde dijital ayak izi farkındalıklarının bu değişkenden etkilendiğini fakat dijital ayak izi yaşantılarının bu değişkenden etkilenmediğini tespit etmişlerdir. Diğer taraftan dijital ayak izi farkındalıkları en uzun süre yaşanan yerden etkilenirken, dijital ayak izi yaşantılarının etkilenmediğini tespit etmişlerdir. Araştırmacılar, çevrimiçi araçları kullanmada yeterli hissetme düzeyinin dijital ayak izi farkındalık durumunu etkilerken, dijital ayak izi yaşantılarının bu değişkenden etkilenmediğini, meslek yüksekokulu, fakülte ve enstitü öğrencilerinin dijital ayak izi farkındalıklarının eğitim düzeyi arttıkça farklılaştığını bulmuşlardır.



Wook, Mohammed, Noor, Muda ve Zairon (2019) Malezya'da gençler arasındaki dijital ayak izi farkındalık düzeyinin analizi amacıyla bir çalışma yürütmüşlerdir. Nicel araştırma yöntemi kullanılan bu çalışmada kentsel, kırsal ve kent yaşamından uzakta olan yerlerden (sub-urban) toplam 234 kişiden oluşan, 15-30 yaş arası bir örneklem grubu ile anket aracılığıyla veri toplanmıştır. Araştırma sonucunda, ankete yanıt verenlerin profillerden 70 kişi 15-20 yaş, 75 kişi 21-25 yaş, 89 kişi ise 26-30 yaş aralığındadır. 112 kişi kentsel alandan, 73 kişi kırsal alandan ve 49 kişi kent yaşamından uzak (sub-urban) alandan oluşmaktadır. Anket sonucuna göre az farkındalık düzeyine sahip ortalama 1.75, risklerin farkında olmadığını gösteren ikinci ortalama 3.89, riskin umursanmadığını gösteren bir diğer ortalama ise 3.45'dir. Son ortalama olan 3.92 de dijital ayak izine yönelik farkındalığın kabul edilmediğine yönelik perspektifi göstermektedir. Özetle farkındalık düzeyinin ortalama bir değerde, risklerin farkında olunmadığına yönelik sonuçların yüksek ve farkındalığın bulunduğu risklere yönelik umursamama düzeyinin yüksek olduğu belirtilebilir. Sonuçlar üzerinde sosyo-ekonomik düzey gibi faktörlerinde etkili olduğu belirtilmektedir.

Dönmez (2019) lise düzeyindeki öğrencilerin bilgi güvenliği farkındalığı ve dijital okuryazarlıkları arasındaki ilişkiyi incelediği bir araştırma yürütmüştür. Bu çalışmada araştırma grubu 2018-2019 eğitim öğretim yılında lise düzeyinde öğrenimi gören 187 öğrencidir. Araştırmada odaklanılan bilgi güvenliği farkındalık durumu, dijital okuryazarlık durumları, cinsiyet, internet kullanımı, sosyal medya kullanımı, çevrimiçi araç kullanmada kendini yeterli hissetme gibi değişkenlerdir. Bulgulara bakıldığında öğrencilerin dijital okuryazarlığının iyi durumda olduğu görülmüştür ve bunun cinsiyete göre farklılaşmadığı sonucuna ulaşılmıştır. Fakat bilgi güvenliği farkındalık durumu cinsiyete göre farklılaşmaktadır. Bilgi güvenliği farkındalığı ve dijital okuryazarlık arasında anlamlı ve pozitif yönde bir ilişki bulunduğu görülmektedir. Çeşitli değişkenlere göre incelendiğinde ise günlük internet kullanımının süresinin artmasının bilgi güvenliği farkındalığının artmasına yönelik bir etkisi olduğu görülmüştür. Bir diğer değişken ise çevrimiçi araçları kullanmada kendini yeterli hissetmedir. Bu değişkenin bilgi güvenliği farkındalığı ile pozitif yönde ve anlamlı bir ilişkisi olduğu görülmüştür. Son olarak

çevrimiçi araçları kullanma konusunda kendini yeterli görme açısından da erkekler lehine sonuç bulunmuştur.

Aslankara ve Seferoğlu (2019) Z kuşağının teknoloji ile oldukça iç içe olduğunu düşünülerek bu kişilere örnek olduklarını düşündükleri için öğretmenlerin dijital ayak izi farkındalıklarını incelemişlerdir. Sakarya'da ilkokul, ortaokul ve lisede görev yapan toplamda 40 öğretmenden oluşan bir örneklem üzerinden araştırma yürütülmüştür. Veriler "Öğretmenlerin Dijital Ortamları Kullanma / Farkındalık Durumları Anketi" ile çevrimiçi olarak toplanmıştır. Sonuç olarak öğretmenlerin dijital ayak izi farkındalıklarının yüksek olduğu, en çok dijital ayak izini sosyal ağlar, çevrimiçi sohbetler ve web sayfalarında (alışveriş vb.) en az ise öğrenme yönetim sistemleri, forum sayfaları ve akademik paylaşım sayfalarında bıraktıkları bulunmuştur. Cinsiyet açısından dijital ayak izi farkındalığına bakıldığında ise erkekler lehine bir durum saptanmıştır.

Kuh Karyeli ve Dağhan'ın (2020) yaptığı araştırmada, Bilişim Teknolojileri ve Yazılım dersi öğretim programlarına eklenen ve çevrimiçi ortamdaki faaliyetlerin tamamını kapsayan dijital ayak izi kavramını öğretmeyi amaçlayan bir ders tasarlamıştır. Araştırmada dijital ayak izini konu edinen ders tasarımının öğrencilerin dijital vatandaşlık konusunda akademik başarılarına etkisi incelenmiştir. Çalışma, 2016-2017 yılında 5. ve 6. sınıf öğrencilerinden oluşan toplam 141 öğrenciyle yürütülmüştür. 9 hafta süren bu çalışmada toplam 120 öğrencinin verileri değerlendirmeye alınmıştır. Süreç ön test, 7 hafta ders şeklinde uygulama ve son test olarak ilerlemiştir. Dersin içeriği olan dijital ayak izi ile ilgili temel kavramlar, dijital vatandaşlık, güvenli internet kuralları, güçlü şifreler, siber zorbalık, siber taciz, gizlilik ve veri koruma ile ilgili içerik sunulmuş, afişler hazırlanmış ve öğrencilere videolar izletilmiştir. Uygulama sonucunda, öğrencilerin ön test ve son test puanları arasında anlamlı bir fark ortaya çıkmıştır. Son test puanları ön test puanlarına göre oldukça etkili bir artış göstermiştir. İzletilen derslerin öğrencilerin dijital vatandaşlık konusunda akademik başarıları üzerinde anlamlı bir etkisi olduğu görülmüştür. Araştırma sonuçlarından bir diğeri de çevrimiçi olmanın ne anlama geldiği ve gelecekteki hayatı nasıl etkilediği konusunda yeterli bilgi sahibi olunmadığıdır.

Buradan hareketle araştırma sonuçlarının ve alanyazın bulgularının dijital vatandaşlık konusunun öğretim programındaki önemini artırılmasını da desteklediği belirtmektedir.

Buitrago-Ropero, Ramírez-Montoya ve Chiappe Laverde (2020) yürüttükleri bir araştırmada 2005-2019 yılları arasında dijital ayak izi ile ilgili yayınlanan araştırmalarını analiz etmişlerdir. Araştırmalarında Scopus ve Web of Science (WoS) veri tabanlarında, toplam 134 araştırma ile araştırmaya başlanıp çift olanlar ve erişilemeyen araştırmalar elendikten sonra toplamda 46 çalışma analiz edilmiştir. Araştırmalarının sonucunda ise eğitim araştırmalarının analitik öğrenme, dijital varlığın incelenmesi ve psikometrik modelleme başlıklarına odaklandığını saptamışlardır. Kitlese Açık Çevrimiçi Kurslarda (MOOCs) dijital ayak izi hakkında az araştırma yapılmasının sonuçlarını gösterdiğini belirterek dijital ayak izi kavramının genel olarak bir eylem ve hizmet anlamında kullanıldığını belirtmişlerdir. Öneri olarak, bilişsel değerlendirme, sayısal eşitlik, okul başarı ve başarısızlığının tahmini için dijital ayak izi yönetimi ile ilgili uygulamaya yönelik eğitim kurumlarının hazırlanmasını dile getirmişlerdir. Böylelikle öğrencilere ve eğitim topluluklarına sunulan yönetim ve politika eylemlerine de katkı sağlayacağını eklemiştir.

Acele (2020) yaptığı tez çalışmasında BT öğretmenlerinin (78 kişi) ve BT öğretmen adaylarının (266 kişi) dijital ayak izi farkındalık durumlarını incelemiştir. Sonuçlar incelendiğinde ilk olarak gizlilik sözleşmelerinin okunup okunmadığı durumu için hem BT öğretmenlerinin hem de BT öğretmen adayları %82'si oranında okuduğunu belirtmişlerdir. İkinci olarak verilere erişim için üçüncü şahıslara en az bir kere izin verdiğini belirten BT öğretmenleri ve BT öğretmen adaylarının oranı %46 olarak belirlenmiştir. Üçüncü olarak verilerin kişinin kendisine ait olduğunu ve kimsenin kullanmamasını belirten BT öğretmenlerinin oranı %84 iken BT öğretmen adaylarının %57'si buna olumlu cevap vermiştir. Verilerin paylaşılması konusunda BT öğretmenleri daha katı bir tutum sergilerken bu düşüncenin iş hayatında benimseyenlerin sayısının arttığı gibi bir sonuca varılabilir.

BT öğretmen ve öğretmen adaylarının Google'da kendilerini arayıp aramadıklarına iki grupta da %78 oranında aradıkları sonuca ulaşıldığı raporlanmıştır. Ayrıca dijital kimlikleri

yönetebilme konusunda “Yönetebiliyorum” cevabını veren sayısı her iki grupta da fazladır. Son olarak, BT öğretmenlerinin %96’sı ve BT öğretmen adaylarının %83’ü tarafından kişisel veriler içerisinde finansal bilgilerini korunmayı tercih etmişlerdir. Kullanıcılar için silme seçeneğini BT öğretmenlerinin %82’si onaylarken BT öğretmen adaylarında bu oran %75 olarak bulunmuştur. Bir diğer bulgu ulusal güvenliğe sunulması için verilerin toplanması konusunu BT öğretmenlerinin çoğu yanlış bulurken BT öğretmen adaylarının çoğu doğru bulmuştur. Medya okuryazarlığında çevrimiçi itibarın nerede öğretilmesi konusuna iki grup da okul sonrasında çevrimiçi kaynaklardan yanıtını vermiştir.

Yılmaz Soylu, Demiröz ve Akkoyunlu (2021) yürüttükleri çalışmada ortaokul öğrencilerinin dijital ayak izi farkındalıklarını sınıf düzeyi, cinsiyet, elektronik araç ve ortamlarda geçirilen süre değişkenleri açısından incelemeyi amaçlamışlardır. Bu doğrultuda öncesinde dijital ayak izi ölçeği geliştirerek ölçeği psikometrik açıdan değerlendirmişlerdir. Geliştirilen ölçek 23 maddeden oluşan Likert tipi bir ölçektir. Geliştirilen ölçek bu çalışma kapsamında geliştirilmiş olan ölçek ile dijital ayak izi farkındalığını ölçmek amacıyla tasarlanmış olması açısından benzerlik göstermektedir fakat Yılmaz Soylu, Demiröz ve Akkoyunlu (2021) tarafından geliştirilen ölçek ortaokul öğrencilerine yönelikken bu çalışma kapsamında geliştirilen ölçek ortaöğretim öğrencilerine yöneliktir. Ölçek maddeleri incelendiğinde maddelerin sosyal ağ ve internet kullanımına yönelik olduğu ve bu açıdan da bu çalışma kapsamında geliştirilen ölçek ile ortak özellikler taşıdığı düşünülse de çalışma kapsamında geliştirilen ölçeğin farkındalık ve uygulama alt boyutları ile toplanan veri açısından daha kapsamlı bilgi sunduğu söylenebilir.

Geliştirilen 17 maddelik DAFÖ üç alt boyuttan oluşmaktadır. Bunlar; kişisel bilgi paylaşımı ve online oyunlar, kişisel bilgi paylaşımından önce düşünme, dijital ayak izi farkındalığıdır. Her birinin Cronbach Alpha güvenirlik katsayıları sırasıyla .73, .73, .74 şeklindedir. Buradan hareketle ölçeğin güvenilir bir ölçek olduğu belirtilmiştir. Sonuçlar cinsiyet değişkeni açısından incelendiğinde kız öğrencilerin kişisel bilgi paylaşımı ve çevrimiçi oyunlar açısından dijital ayak izi farkındalığının erkeklerden daha yüksek olduğu bulunmuştur. Sınıf

değişkeni açısından bakıldığında 5. sınıf öğrencileri 6. ve 7. sınıf öğrencilerine göre kişisel bilgi paylaşımından önce düşünmeye daha yatkındırlar. Öğrencilere yöneltilen bir günde ortalama ne kadar telefon kullandıklarına yönelik sorunun cevabında ise çok az telefon kullananların biraz veya çok kullananlara göre kişisel bilgi paylaşımı ve çevrimiçi oyunlardaki dijital ayak izi farkındalığının daha yüksek olduğu bulunmuştur. Ayrıca günlük cep telefonu kullanımı süresinin çok olmayanların kişisel bilgilerini paylaşmadan önce düşünmeye daha yatkın oldukları saptanmıştır. Aynı şekilde çevrimiçi oyun oynama süreleri ile sosyal medya kullanım sürelerinin de azalmasıyla birlikte yukarıda bahsedilen sonuçlara benzer sonuçların elde edildiği görülmüştür. Araştırmanın sonunda ise araştırmacılar inceledikleri değişkenler açısından elde edilen sonuçların dijital ayak izi farkındalığı boyutunda istatistiksel açıdan anlamlı bir farkın oluşmadığını belirtmişlerdir. Ayrıca araştırmacılar ortaokul öğrencilerinin dijital ayak izi ile ilgili bilgiye sahip olduklarını fakat bu farkındalığın uygulamaya geçirildiği aşamada farklı değişkenler açısından etkilendiği sonucuna ulaşmışlardır.

İlgili araştırmalar ele alındığında dijital ayak izi ile ilgili alanyazında birçok çalışma yer almaktadır. Dijital ayak izi farkındalığı ile ilgili de araştırmalara rastlanmış olmasına rağmen, alanyazında psikometrik ölçümler yapabilecek ortaöğretim düzeyinde bir ölçeğe henüz rastlanmamıştır. Gerek DLEARN'in çalışması, gerekse de diğer ilgili alanyazında dijital ayak izi farkındalığı anketlerle veya nitel diğer araştırma yöntemleri ile belirlenmeye çalışılmıştır. Oysaki farkındalık psikolojik bir yapıdır ve ölçekle ölçülmesi gerekmektedir. Ölçek kavramı özünde ölçme sonuçlarının matematiksel niteliklerini göstermekle birlikte (Turgut ve Baykul, 1992) eğitim ve psikoloji gibi davranış bilimlerinin birçok alanında, hedeflenen kişi(ler), sistem, konu ya da içerik açısından veri/bilgi toplamak amacıyla kullanılır (Yurdugül, 2005). Bu nedenle bu araştırmada dijital ayak izi farkındalığının ölçülmesine yönelik bir ölçek geliştirilmiştir.

## Bölüm 3

### Yöntem

#### Araştırma Modeli

Bu araştırmada öncelikle bir ölçek geliştirilmiştir. Ölçek geliştirme aşamasını takiben, dijital ayak izi farkındalığı ve bilgi güvenliği farkındalığı arasındaki ilişki incelenmiştir. Bu bakımdan çalışma, keşfedici ilişkisel araştırma türündedir.

#### Araştırmanın Çalışma Grubu

Araştırmanın ölçek geliştirme aşamasındaki çalışma grubunu Ankara'daki bir Anadolu Lisesi'nin 9., 10., 11. ve 12. sınıflarında öğrenim gören toplam 699 ortaöğretim öğrencisi oluşturmaktadır. Anket 1017 öğrenciye ulaştırılmış, bunlardan %68,7'si yani 699 öğrenci anketi doldurmuştur. Bu öğrencilerin betimsel istatistikleri Tablo 1'de sunulmaktadır.

**Tablo 1**

*Ölçek Geliştirme Aşamasındaki Araştırma Grubuna İlişkin Betimsel İstatistikler*

Değişkenler	Seçenekler	(f)	(%)
Cinsiyet	Kadın	338	49,5
	Erkek	361	50,5
Sınıf	9. Sınıf	145	21,7
	10. Sınıf	169	25,2
	11. Sınıf	180	27
	12. Sınıf	175	26,1
Yaş	15	169	24,2
	16	165	23,7
	17	160	22,8
	18	148	21,2
	19	57	8,1

	Yok	50	7,1
Annenizin Eğitim Durumu	İlkokul	69	9,9
	Ortaokul	104	14,9
	Ortaöğretim	237	33,9
	Üniversite	193	27,6
	Lisansüstü	46	6,6
		Yok	36
Babanızın Eğitim Durumu	İlkokul	45	6,4
	Ortaokul	147	21
	Ortaöğretim	262	37,5
	Üniversite	170	24,3
	Lisansüstü	39	5,6
	Kullanabileceğiniz aktif bir internet bağlantınız var mı?	Evet	612
	Hayır	87	12,5
Sosyal Medya hesabına (Facebook, Instagram, Twitter) sahip misiniz?	Evet	699	100
	Hayır	0	0
Eğer var ise günde kaç saat aktif kullanıyorsunuz?	Kullanmıyorum	0	0
	1-3 saat	434	62,1
	4-6 saat	195	27,9
	7-9 saat	61	8,7
	10+ saat	9	1,3
İnterneti günlük ortalama kullanma süreniz nedir?	Kullanmıyorum	0	0
	1-3 saat	441	63,1
	4-6 saat	187	26,8
	7-9 saat	61	8,7
	10+ saat	10	1,4

	Sadece Bilgisayar	104	14,9
	Sadece Tablet	68	9,7
Aşağıdaki donanımlardan	Sadece Telefon	104	14,9
hangisine / hangilerine	Bilgisayar + Tablet	98	14
sahipsiniz?	Bilgisayar + Telefon	213	30,5
	Tablet + Telefon	105	15
	Diğer	7	1
	Hiçbiri	0	0
	TOPLAM	699	100

Tablo 1 incelendiğinde çalışmaya 338 kadın 361 erkek olmak üzere toplam 699 öğrencinin katıldığı görülmektedir. Bu öğrencilerden 145'i 9. sınıf, 169'u 10. sınıf, 180'i 11. sınıf ve 175'i 12. sınıftır. Öğrencilerden 169'u 15, 165'i 16, 160'ı 17, 148'i 18 ve 51'si 19 yaşındadır. Öğrencilerden 50'si annesinin eğitim almadığını, 69'u ilkokul eğitimi aldığını, 104'ü ortaokul eğitimi aldığını, 237'si ortaöğretim eğitimi aldığını, 193'ü üniversite ve 46'sı annesinin lisansüstü eğitimi aldığını belirtmiştir. Babalarının eğitim durumuna ise 36'sı yok, 45'i ilkokul, 147'si ortaokul, 262'si ortaöğretim, 170'si üniversite ve 39'u ise lisansüstü eğitim aldığı yanıtını vermiştir. "Kullanabileceğiniz aktif bir internet bağlantınız var mı?" sorusuna ise 612 öğrenci "evet" derken 87 si "hayır" cevabını vermiştir. "Sosyal medya hesabına sahip misiniz?" sorusuna ise tüm öğrenciler evet cevabını vermiştir.

Seçilen ortaöğretim kurumu, tez danışmanının "danışman akademisyeni" olduğu bir Anadolu Lisesidir. Millî Eğitim Bakanlığı 2023 Eğitim Vizyonu hedefleri çerçevesinde, yönetim süreçlerinin etkili yürütülmesi, öğretmen yetkinliklerinin geliştirilmesi, çevre-okul ilişkilerinin güçlendirilmesi ve öğrenci başarısının her alanda artırılarak okullarda nitelikli eğitimin sağlanması gibi amaçlarla okullar ve üniversiteler arasında bağ kurabilecek akademisyenlerin görevlendirilmesi uygulaması kapsamında, tez danışmanının akademik danışmanlığını yürüttüğü lisede veri toplanmıştır.

Araştırmanın dijital ayak izi farkındalığı ile bilgi güvenliği farkındalığı arasındaki ilişkinin incelendiği ikinci aşamasındaki çalışma grubunu ise, Ankara'daki başka bir Anadolu Lisesi'nin



9., 10., 11. ve 12. sınıflarında öğrenim gören toplam 214 ortaöğretim öğrencisi oluşturmaktadır. Bu öğrencilerin betimsel istatistikleri Tablo 2'de sunulmaktadır.

**Tablo 2**

*Dijital Ayak İzi Farkındalığı ve Bilgi Güvenliği Farkındalığının Araştırıldığı Araştırma Grubuna İlişkin Betimsel İstatistikler*

Değişkenler	Seçenekler	(f)	(%)
Cinsiyet	Kadın	101	47,2
	Erkek	113	52,8
Sınıf	9. Sınıf	58	27,1
	10. Sınıf	55	25,7
	11. Sınıf	52	24,3
	12. Sınıf	49	22,9
Yaş	15	60	28
	16	52	24,3
	17	55	25,7
	18	43	20
	19	4	2
Annenezin Eğitim Durumu	Yok	4	1,9
	İlkokul	17	7,9
	Ortaokul	35	16,3
	Ortaöğretim	71	33,2
	Üniversite	83	38,8
	Lisansüstü	4	1,9
Babanızın Eğitim Durumu	Yok	1	0,5
	İlkokul	21	9,8
	Ortaokul	35	16,4
	Ortaöğretim	119	55,6
	Üniversite	28	13

	Lisansüstü	10	4,7
Kullanabileceğiniz aktif bir internet bağlantınız var mı?	Evet	213	99,5
	Hayır	1	0,5
Sosyal Medya hesabına (Facebook, Instagram, Twitter) sahip misiniz?	Evet	214	100
	Hayır	0	0
	Kullanmıyorum	0	0
Eğer var ise günde kaç saat aktif kullanıyorsunuz?	1-3 saat	202	94,4
	4-6 saat	11	5,1
	7-9 saat	1	0,5
	10+ saat	0	0
	Kullanmıyorum	0	0
İnterneti günlük ortalama kullanma süreniz nedir?	1-3 saat	178	83,2
	4-6 saat	28	13,1
	7-9 saat	8	3,7
	10+ saat	0	0
Aşağıdaki donanımlardan hangisine/ hangilerine sahipsiniz?	Sadece Bilgisayar	19	8,9
	Sadece Tablet	2	0,9
	Sadece Telefon	21	9,8
	Bilgisayar + Tablet	55	25,7
	Bilgisayar + Telefon	104	48,6
	Tablet + Telefon	9	4,2
	Diğer	4	1,9
	Hiçbiri	0	0

Tablo 2 incelendiğinde araştırmanın ikinci boyutu olan iki ölçek arasındaki ilişkinin incelenmesi amacı ile veri toplanan ortaöğretim öğrencileri hakkındaki sayısal bilgiler görülmektedir. Öğrencilerden 101'i kadın 113'ü erkektir. Çalışmaya 58 9. sınıf öğrencisi, 55 10. sınıf öğrencisi, 52 11. sınıf öğrencisi, 49. 12. sınıf öğrencisi katılmıştır. Öğrencilerin yaşlarına bakıldığında, 60'ı 15, 52'si 16, 55'i 17, 43'ü 18 ve 4 tanesi de 19 yaşındadır.

Annelerinin eğitim durumuna 4 kişi yok derken, 17 tanesi kişi, 35 kişi ortaokul, 71 kişi ortaöğretim, 83 kişi üniversite ve 4 kişide lisansüstü eğitim aldı cevabını vermiştir. Babalarının eğitim durumu ise, 1 kişi yok, 21 kişi ilkokul, 35 kişi ortaokul, 119 kişi ortaöğretim, 28 kişi üniversite, 10 kişi ise lisansüstü yanıtını vermiştir. Kullanabilecekleri aktif internetleri olup olmadığı sorusuna ise 1 kişi hayır derken 213 kişi evet cevabını vermiştir. Öğrencilerden tamamı sosyal medya hesabına sahiptir. 202 kişi günde 1-3 saat arası kullanmaktadır, 11 kişi 4-6 saat ve 1 kişi ise 7-9 saat arası kullandığını belirtmiştir. İnterneti ise 178 kişi günde 1-3 saat, 28 kişi 4-6 saat, 8 kişi ise 7-9 saat arası kullanmaktadırlar. Öğrencilerden 19 kişi sadece bilgisayara sahip iken, 2 kişi sadece tablete sahip olduğunu belirtmiştir, 21 kişi ise sadece telefona sahiptir. Bilgisayar ve tablete sahip öğrenci sayı 55 iken bilgisayar ve telefona sahip öğrenci sayısı 104'dür. Tablet ve telefona sahip kullanıcı sayısı 9 ve sahip olduğu araçları diğer kategorisinde belirten öğrenci sayısı ise 4'dür. Buradan öğrencilerin hepsinin en an bir donanıma sahip olduğu çıkarılabilir.

### **Veri Toplama Aracının Geliştirilmesi**

Araştırmada ilk olarak Dijital Ayak İzi Farkındalık Ölçeği geliştirilmiştir. Geliştirilen ölçeğin maddeleri araştırmacılar tarafından alanyazından hareketle kendi oluşturdukları madde havuzu aracılığıyla hazırlanmıştır. Alanyazın desteği ile yazılan maddelerin yanı sıra, 2020-2021 Öğretim yılı Güz döneminde tez danışmanı tarafından Hacettepe Üniversitesi Eğitim Fakültesi Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümünde verilen BTE309 – Bilişim Öğretim Programları dersinde yapılan bir çalışmadan da yararlanılmıştır. Bu ders kapsamında öğretim programı incelemeleri yapılırken, 2018 yılından itibaren uygulanmakta olan Bilişim Teknolojileri ve Yazılım dersi öğretim programının ilgili kazanımları ele alınmıştır. Her bir kazanımın öğrencilere nasıl kazandırılabileceği üzerine tartışmalar yürütülmüştür. Öğrencilerin bu kazanımları elde ettikleri durumda ne tür bilgi, beceri ve tutumlara sahip olabilecekleri tartışılmıştır. Daha sonra 34 3. sınıf öğrencisine dijital ayak izi farkındalığına işaret edebileceğini düşündükleri ifadeleri yazma çalışması yaptırılmıştır. Bu öğrencilerden değişen sayılarda örnekler gelmiş, bunlar araştırmacılar tarafından okunmuş, filtrelenmiştir.

Ardından oluşturulan maddelere son şekli verilmiştir. Belirlenen maddeler ile oluşturulan taslak ölçek, alan uzmanlarından görüşler alınarak revize edilmiştir. İlk olarak Türk Dili ve Edebiyatı alanı uzmanı bir öğretim üyesinden dönütler alınmış ve alınan dönütler neticesinde ölçekte dil bilgisi açısından düzeltmeler yapılmıştır. Ardından ölçeğin revize edilmiş hali iki BÖTE alan uzmanı ile paylaşılmıştır. Öğretim üyesi olarak görev yapan alan uzmanları ile görüşmeler sonucunda ölçek son haline getirilmiştir. Elde edilecek olası ölçeğin, ortaöğretim düzeyindeki öğrencilerin dijital ayak izi farkındalıklarını ölçebilecek, geçerli ve güvenilir bir ölçme aracı olması hedeflenmektedir.

### **Kullanılan Veri Toplama Aracı**

Bu çalışmada araştırmacı tarafından geliştirilen “Dijital Ayak İzi Farkındalık Ölçeği” ve 2016 yılında Güldüren, Çetinkaya ve Keser tarafından geliştirilen “Ortaöğretim Öğrencilerine Yönelik Bilgi Güvenliği Farkındalık Ölçeği” (Ek C) kullanılmıştır. Öncelikle Dr. Can Güldüren, Prof. Dr. Hafize Keser ve Doç. Dr. Levent Çetinkaya’ya e-posta yoluyla ulaşıp ölçeğin kullanım izni alınmıştır. Ölçek maddelerine ilgili araştırmalarında ulaşamadığı için kendilerinden istenmiş, kendileri e-posta yoluyla ölçeğin orijinalini paylaşmışlar ve ölçeğin kullanımına izin vermişlerdir (EK B). İlgili ölçek 34 madde ve 3 alt boyuttan (saldırı ve tehditler, mahremiyet, kişisel verilerin korunması) oluşmaktadır. Araştırmalarında ölçeğin Cronbach Alpha güvenilirlik katsayısı .955; her alt boyut için sırasıyla .954, .890 ve .808 olarak bulunmuştur ve doğrulayıcı faktör analizi ile yapı geçerliği sınanmıştır. Buradan yola çıkarak ölçeğin geçerli ve güvenilir olduğu belirtilmiştir.

İkinci veri toplama aracı ise bu çalışma kapsamında geliştirilen Dijital Ayak İzi Farkındalık Ölçeği’dir. Bu ölçeğin taslak maddelerinin iki ana kavram etrafında toplandığı bilinmektedir. Bunlar kişisel veri paylaşımı ile sosyal medya kullanımınıdır. Bu ana kavramlar belirlenirken araştırmacının yapılacağı yaş grubundaki bireyler arasında sıklıkla kullanılan ve ayak izi oluşmasına sebep olabilecek ortamlar göz önüne alınmıştır. Dil alanı uzmanı ve iki BÖTE alan uzmanının getirdikleri öneriler doğrultusunda ölçek taslağına son şekli verilmiş ve

ölçeğe eklenen demografik özellikler ile ilgili soruların ardından Veli Onam Formu, Çocuk/Ergen Formu, Gönüllü Katılım Formları da geliştirilerek etik bağlamında gerekli izinler alınmıştır.

### **Veri Toplama Süreci**

Veri toplama sürecinin ilk aşaması olarak, “Ortaöğretim Öğrencilerine Yönelik Bilgi Güvenliği Farkındalık Ölçeği”nin kullanım izni sonrasında ise, Hacettepe Üniversitesi Etik Komisyonundan etik izin alınmıştır (Ek Ç). Araştırmanın ölçek geliştirme aşamasındaki verileri, Aralık 2020 – Ocak 2021 döneminde Ankara’da bulunan bir Anadolu Lisesinde çevrimiçi ortamda paylaşarak toplanmıştır. Verinin toplanma sürecinde okul yönetiminden destek alınmış, öğrencilere e-posta adresleri ve kullandıkları öğrenme yönetim sistemi aracılığıyla anketin bağlantısı birer hafta aralıklarla tekrar tekrar ulaştırılmıştır. Veli onam formu basılı olarak okul yönetimince derlenmiş, çocuk / ergen formu ve gönüllü katılım formları ise elektronik olarak onaylanmıştır. Araştırmanın ölçek geliştirme aşamasındaki veri toplama sürecinin sonunda toplam 699 ortaöğretim öğrencisine ulaşılmıştır. Bu öğrencilerden elde edilen verinin tek sıralarında yer alan 350 öğrencinin verisiyle açımlayıcı faktör analizi, çift sıralarında yer alan 349 öğrencinin verisiyle doğrulayıcı faktör analizi gerçekleştirilmiştir. Başka bir Anadolu Lisesinin 214 öğrencisinden elde edilen Dijital Ayak İzi Farkındalık Ölçeği ve Bilgi Güvenliği Farkındalık Ölçeği verileriyle gerçekleştirilen ilişkisel araştırma verileri ise Mart 2021’de, yine çevrimiçi ortamda toplanmıştır.

### **Verilerin Analizi**

Toplanan verilerin analizine geçilmeden önce ilk olarak ters maddeler çevrilmiştir. Toplamda beş ölçek maddesi ters madde olarak belirlenmiştir. Bunlardan üç tanesi Kişisel Veri Paylaşımı - Uygulama alt boyutundan, iki tanesi ise Sosyal Medya Kullanımı - Uygulama alt boyutundandır. Ters maddelere örnek olarak;

- “İnternet ortamında fotoğraflarımı paylaşmaktan çekinmem.”

- “Sosyal medya hesaplarımda profil resmi kullanırım”, maddeleri verilebilir.

Araştırma verisinde boş soru bırakılmayacağı için, kayıp veri bulunmamaktadır. Aykırı değer veya uç değer özelliği sergileyen ölçek maddesine de rastlanmamıştır.

Araştırma verilerinin analizinde, ölçek geliştirme boyutunda geçerlik ve güvenilirlik ölçümleri için açımlayıcı ve doğrulayıcı faktör analizleri ile güvenilirlik analizlerinden, ilişki araştırma boyutunda ise Pearson momentler çarpımı korelasyon katsayısından yararlanılmıştır.

## Bölüm 4

### Bulgular ve Yorumlar

Bu kısımda, öncelikle Dijital Ayak İzi Farkındalık Ölçeğinin geliştirilmesi sürecine yönelik olarak açımlayıcı faktör analizi ve doğrulayıcı faktör analizi sonuçları sunulmuştur. Geçerlik kanıtlarının raporlanmasının ardından güvenilirlik bulguları verilmiştir. Daha sonra ortaöğretim öğrencilerine yönelik geliştirilen Dijital Ayak İzi Farkındalık Ölçeğinden elde edilen puanlar ile yine ortaöğretim öğrencilerine yönelik olarak geliştirilen Bilgi Güvenliği Farkındalık Ölçeği puanları arasındaki ilişki araştırılmıştır.

#### Dijital Ayak İzi Farkındalık Ölçeğinin Açımlayıcı Faktör Analizi (AFA) Bulguları

Faktör analizine başlamadan önce, Dijital Ayak İzi Farkındalık Ölçeğinin uygulanmasından elde edilen verilerin, faktör analizi için uygun olup olmadığının belirlenebilmesi adına, Kaiser-Meyer-Olkin (KMO) örneklem uygunluğu testi ile Bartlett'in küresellik testi yapılmıştır. KMO örneklem uygunluğu testi ve Bartlett'in küresellik testi sonuçları Tablo 3'de gösterilmiştir.

**Tablo 3**

#### *KMO ve Bartlett Testleri Sonuçları*

Kaiser-Meyer-Olkin (KMO)	Örneklem Uygunluğu Değeri	,913
	Yaklaşık Ki-Kare Değeri ( $\chi^2$ )	9449,491
Bartlett'in Küresellik Testi	Serbestlik Derecesi (df)	496
	Anlamlılık Seviyesi (Sig.)	,000

KMO örneklem uygunluğu değerinin 0,913 ve Bartlett'in küresellik testinin anlamlılık seviyesinin .000 çıkması ( $p \leq 0.05$ ), verilerin faktör analizine uygun olduğunu göstermektedir. KMO değerinin 0.50'den büyük olması, veri kümesinin faktörleşebilmesine olanak sağladığı anlamına gelmektedir (Field, 2000). KMO örneklem uygunluğu değerinin 1'e yakın çıkması, veri kümesinin faktör analizine mükemmel uyum sağladığını ve homojen bir dağılıma sahip

olduğunu ifade etmektedir. Bartlett'in küresellik testinin istatistiksel olarak anlamlı olması da, faktör analizinin bir ön koşuludur (Tatlıldil, 2002).

Faktör analizine uygun olduğuna karar verilen veriler için temel bileşenler analiz metoduyla faktör analizi yapılmıştır. Tablo 4'de, açıklanan toplam varyans dağılımları gösterilmektedir.

**Tablo 4**

*Açıklanan Toplam Varyans Dağılımları*

Bileşen	Başlangıç Öz Değerleri			Kareli Yük Toplamlarının İlk Hali		
	Toplam	Varyans (%)	Kümülatif (%)	Toplam	Varyans (%)	Kümülatif (%)
1	10,915	34,110	34,110	10,915	34,110	34,110
2	5,185	16,203	50,313	5,185	16,203	50,313
3	1,925	6,015	56,328	1,925	6,015	56,328
4	1,436	4,489	60,817	1,436	4,489	60,817
5	,977	3,053	63,870			
6	,910	2,844	66,714			
7	,831	2,598	69,312			
8	,743	2,322	71,634			
9	,737	2,302	73,936			
10	,666	2,081	76,017			
11	,657	2,054	78,071			
12	,592	1,849	79,919			
13	,569	1,777	81,697			
14	,559	1,748	83,445			
15	,526	1,643	85,088			
16	,480	1,499	86,588			
17	,451	1,408	87,996			
18	,409	1,279	89,275			
19	,381	1,191	90,466			



20	,350	1,093	91,559
21	,347	1,084	92,643
22	,329	1,027	93,670
23	,300	,938	94,608
24	,297	,929	95,537
25	,262	,819	96,356
26	,256	,801	97,157
27	,254	,795	97,952
28	,239	,748	98,700
29	,216	,676	99,376
30	,193	,602	99,978
31	,004	,013	99,990
32	,003	,010	100,000

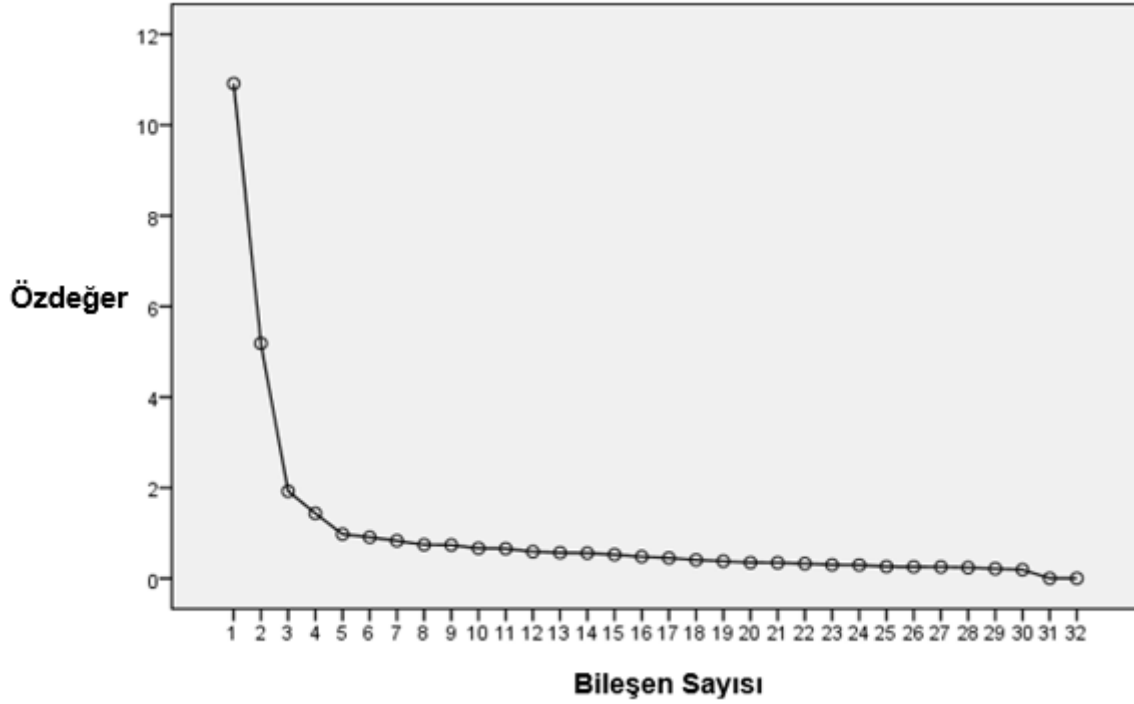
Tablo 4 incelendiği zaman, veri kümesinin öz değerleri 1 ve üzerinde olan 4 faktörle incelenebileceği görülmektedir. 1. faktör, toplam varyansın % 34,11'ini, 2. faktör toplam varyansın %16,203'ünü, 3. faktör toplam varyansın %6,015'ini ve 4. faktör toplam varyansın %4,489'unu açıklamaktadır. Dört faktör birlikte göz önüne alındığında, toplam varyanstaki değişimin %60,817'sini açıklamaktadırlar. Bu oran da, sosyal bilimlerde gerçekleştirilen çalışmalarında beklenen açıklama yüzdesi oranları dâhilinde kabul edilebilir bir değerdir.

Veri kümesinden seçilecek olan faktör sayısının belirlenebilmesinin diğer bir yöntemi de, yamaç eğim testi (scree plot) sonucuna bakmaktır. Yamaç eğim testi, öz değerler bulunduktan sonra, bulunan bu öz değerlerin büyüklük sırasına göre dizilim değerlerinin bir çizgi grafiği ile gösterilmesini ifade etmektedir (Özdamar, 2004). Öz değerlerin azalarak gösterildiği yamaç eğim grafiğinde, eğim çizgisinin azalarak doğrusal bir hareket kazandığı ya da değişimin çok küçük azalan değerlere ulaştığı noktalar dikkate alınarak yorum yapılmaktadır. Bu noktalara kadar olan öz değer sayısı kadar temel bileşen seçilmektedir. Şekil 1 incelendiğinde, 5. bileşenden sonra eğim çizgisinin yatay bir seyir izlediği görülmektedir.

Dolayısıyla, 5. bileşenden önceki bileşen sayısı kadar faktör seçmek uygundur ve veri kümesi 4 faktörle açıklanabilmektedir.

### Şekil 1

Öz Değer ve Bileşen Sayılarına Ait Yamaç Eğim Grafiği



Tablo 4'de sunulan açıklanan toplam varyans dağılımları ve Şekil 1'de gösterilen yamaç eğim grafiğinden hareketle Dijital Ayak İzi Farkındalık Ölçeğinin 4 faktörlü bir yapısı olduğu sonucuna ulaşılmıştır. Tablo 5'de bileşen matrisi gösterilmiştir.

### Tablo 5

Bileşen Matrisi ve Faktör Yüklerinin Dağılımı

	Bileşen			
	1	2	3	4
ku6	,733	,230	,051	,326
ku8	,730	,242	-,030	,244
kf7	-,715	,522	-,095	,178
kf9	-,709	,535	-,096	,176

ku7	,698	,181	,082	,212
kf6	-,669	,475	-,093	,096
ku9	,668	,224	-,038	,161
ku1	,665	,315	,049	,255
ku11	,663	,322	-,007	,120
ku5	,651	,091	,201	,307
kf8	-,644	,481	-,212	,055
kf10	-,643	,480	-,213	,060
ku10	,641	,244	,020	,183
kf5	-,628	,551	-,163	,119
ku12	,614	,406	-,039	,074
ku3	,589	,341	-,010	,090
ku4	,575	,357	-,072	,047
ku2	,574	,368	-,005	,278
kf2	-,559	,471	-,141	,147
sf4	,549	,470	,133	-,338
sf5	,497	,415	,044	-,212
sf1	,479	,440	,061	-,324
sf3	,431	,405	-,073	-,271
kf4	-,553	,573	-,121	,036
sf2	,435	,554	-,019	-,462
sf6	,447	,550	,053	-,416
kf3	-,493	,501	-,187	,072
kf1	-,362	,443	-,097	-,193
su1	-,344	,223	,684	,088
su4	-,452	,143	,676	,091
su3	-,476	,287	,619	-,022
su2	-,480	,344	,549	-,042

Faktör Çıkarma Yöntemi: Temel Bileşenler Analizi.

4 bileşen çıkartılmıştır.

Tablo 5 incelendiğinde, bazı maddelerin belirli bir faktöre işaret etmediği ve belirli bir faktöre yük verme noktasında kararsız kaldıkları görülmektedir. Bu nedenle dik döndürme yöntemlerinden Varimax rotasyonu uygulanmış ve döndürme sonrası açıklanan toplam varyans dağılımları Tablo 6'de sunulmuştur.

**Tablo 6**

*Varimax Döndürmesi Sonucu Oluşan Açıklanan Toplam Varyans Dağılımları*

Bileşen	Başlangıç Öz Değerleri			Kareli Yük Toplamlarının İlk Hali			Kareli Yük Toplamlarının Rotasyonlu Hali		
	Toplam	Varyans (%)	Kümülatif (%)	Toplam	Varyans (%)	Kümülatif (%)	Toplam	Varyans (%)	Kümülatif (%)
	1	10,915	34,110	34,110	10,915	34,110	34,110	6,711	20,971
2	5,185	16,203	50,313	5,185	16,203	50,313	6,338	19,807	40,778
3	1,925	6,015	56,328	1,925	6,015	56,328	3,729	11,654	52,432
4	1,436	4,489	60,817	1,436	4,489	60,817	2,683	8,385	60,817
5	,977	3,053	63,870						
6	,910	2,844	66,714						
7	,831	2,598	69,312						
8	,743	2,322	71,634						
9	,737	2,302	73,936						
10	,666	2,081	76,017						
11	,657	2,054	78,071						
12	,592	1,849	79,919						
13	,569	1,777	81,697						
14	,559	1,748	83,445						
15	,526	1,643	85,088						
16	,480	1,499	86,588						
17	,451	1,408	87,996						
18	,409	1,279	89,275						
19	,381	1,191	90,466						

20	,350	1,093	91,559
21	,347	1,084	92,643
22	,329	1,027	93,670
23	,300	,938	94,608
24	,297	,929	95,537
25	,262	,819	96,356
26	,256	,801	97,157
27	,254	,795	97,952
28	,239	,748	98,700
29	,216	,676	99,376
30	,193	,602	99,978
31	,004	,013	99,990
32	,003	,010	100,000

Tablo 6 incelendiğinde, ölçeğin yine 4 faktörlü yapısının korunduğu ve toplam varyansın %60,817'sinin açıklanabildiği görülmektedir. Varimax rotasyonu sonucunda döndürülmüş bileşen matrisi ve faktör yüklerinin dağılımı Tablo 7'de sunulmuştur.

**Tablo 7**

*Döndürülmüş Bileşen Matrisi ve Faktör Yüklerinin Dağılımı*

	Bileşen			
	1	2	3	4
kf9	,865	-,145	-,119	,215
kf7	,859	-,154	-,129	,215
kf5	,839	-,123	-,040	,130
kf10	,804	-,202	-,039	,069
kf8	,803	-,205	-,035	,070
kf6	,782	-,192	-,074	,190
kf4	,782	-,112	,064	,150
kf2	,740	-,092	-,078	,118
kf3	,723	-,084	,019	,059

kf1	,526	-,177	,244	,082
ku6	-,227	,788	,139	-,080
ku8	-,205	,737	,205	-,158
ku1	-,139	,736	,214	-,051
ku2	-,025	,708	,189	-,066
ku7	-,273	,677	,190	-,058
ku5	-,330	,671	,058	,054
ku11	-,139	,652	,318	-,110
ku10	-,179	,644	,222	-,091
ku9	-,194	,637	,236	-,158
ku12	-,048	,626	,378	-,113
ku3	-,086	,593	,324	-,091
ku4	-,054	,560	,358	-,146
sf2	,058	,243	,803	-,050
sf6	,032	,282	,773	,017
sf4	-,097	,368	,712	,054
sf1	-,051	,312	,657	-,001
sf3	,007	,290	,575	-,118
sf5	-,052	,382	,564	-,020
su4	,163	-,147	-,133	,790
su1	,153	-,042	-,049	,785
su3	,277	-,174	,018	,764
su2	,340	-,168	,059	,710

Faktör Çıkarma Yöntemi: Temel Bileşenler Analizi.

4 bileşen çıkartılmıştır.

Tablo 7 incelendiğinde, Varimax rotasyonu sonrasında elde edilen faktörler ve faktör yüklerinin dağılımı görülmektedir. 1. faktör altında 10 ölçek maddesi, 2. faktör altında 12 ölçek maddesi, 3. faktör altında 6 ölçek maddesi ve 4. faktör altında 4 ölçek maddesi toplanmıştır. Dijital Ayak İzi Farkındalığının aynı faktör altında toplanan maddeleri ve söz ettikleri işlevler incelendiğinde, 1. faktörün kişisel veri paylaşımı farkındalığı, 2. faktörün kişisel veri paylaşımı

uygulama, 3. faktörün sosyal medya kullanımı farkındalığı ve 4. faktör sosyal medya kullanımı uygulama olarak adlandırılmasına karar verilmiştir. Kişisel veri paylaşımı uygulama ve sosyal medya kullanımı uygulama faktör isimleri daha net ifade edilecek olursa bu konularda ki farkındalığın ne düzeyde uygulamaya döküldüğünü ifade etmek amaçlanmıştır. Ek A'da ölçeğin boyutları ve maddeleri bütüncül olarak sunulmuştur. Açıklayıcı faktör analizi sonrasında faktör yapısına karar verilen Dijital Ayak İzi Farkındalık Ölçeğinin ortaya konan faktör yapısının doğrulanabilmesi için Doğrulayıcı Faktör Analizi (DFA) yapılmıştır. Aşağıda DFA'ya ilişkin bulgulara yer verilmiştir.

### **Dijital Ayak İzi Farkındalık Ölçeğinin Doğrulayıcı Faktör Analizi (DFA) Bulguları**

Verilerin faktör analizi için uygunluğu belirlendikten sonra, ölçek maddelerinin yapı geçerliği doğrulayıcı faktör analizi ile sınanmıştır. Öncelikle araştırmada ele alınan yapılara ait maddelerin, belirlenen alt faktörlerde toplanıp toplanmadığının belirlenebilmesi için birincil düzey doğrulayıcı faktör analizi yapılmıştır. Yapılan ilk incelemede tüm maddelerin öngörülen yapıya yöneldiği ve ilişkilerin anlamlı olduğu görülmüştür. Bu nedenle ölçekten çıkarılması gereken bir madde olmadığına karar verilmiştir. Daha sonra veri - model uyumları incelenmiştir.  $\chi^2/sd$  oranı 1,895 olarak bulunmuştur ( $p < .05$ ). Bu değer 3'den küçük olması uyumun mükemmel olduğu anlamına gelmektedir ancak,  $\chi^2$  değeri örneklem genişliğinden kolaylıkla etkilenebilmekte ve büyük örneklerde .05 düzeyinde genellikle manidar değerler almaktadır (Schumacker & Lomax, 2004). Bu nedenle yalnızca  $\chi^2/sd$  oranına bakılarak yapılan yorumlar güvenilir olmayabilir. Bu oranla birlikte rapor edilen diğer uyum iyiliği indekslerinin sonuçları Tablo 8'de görülmektedir. Uyum iyiliği indekslerinin iyi uyum ve kabul edilebilir uyum değerleri, Schermelleh-Engel, Moosbrugger ve Müller'in (2003) çalışmasında rapor edilen değerlerden alınmış ve bu değerler üzerinden yorumlarda bulunulmuştur.

**Tablo 8***Birincil Düzey Doğrulayıcı Faktör Analizinde Uyum İyiliği İndekslerine İlişkin Bulgular*

Uyum İyiliği İndeksleri	Model Değeri	İyi Uyum Değeri	Kabul Edilebilir Uyum Değeri
RMSEA	0,062	$0 \leq \text{RMSEA} \leq ,05$	$,05 < \text{RMSEA} \leq ,08$
NFI	0,88	$,95 \leq \text{NFI} \leq 1,00$	$,90 \leq \text{NFI} < ,95$
NNFI	0,92	$,97 \leq \text{NNFI} \leq 1,00$	$,95 \leq \text{NNFI} < ,97$
CFI	0,92	$,97 \leq \text{CFI} \leq 1,00$	$,95 \leq \text{CFI} < ,97$
S-RMR	0,075	$0 \leq \text{S-RMR} \leq ,05$	$,05 < \text{S-RMR} \leq ,10$
GFI	0,84	$,95 \leq \text{GFI} \leq 1,00$	$,90 \leq \text{GFI} < ,95$
AGFI	0,82	$,90 \leq \text{AGFI} \leq 1,00$	$,85 \leq \text{AGFI} < ,90$

Tablo 8 incelendiğinde bazı model değerlerinin yeterli uyum göstermediği görülmektedir. Modele ilişkin olarak,  $\chi^2$  değeri üzerinde manidar değişiklik yapabilecek olan modifikasyon önerilerinden, aynı yapı içerisindeki maddeleri bağlamayı önerenler ve  $\chi^2$  değerinde önemli görülebilecek derecede düşüşe neden olanlar benimsenmiştir. Aynı yapı içerisindeki maddeler arasında bile olsa, bazı modifikasyon önerilerinin gerçekleştirilmesine gereksinim duyulmamıştır. Zira söz konusu modifikasyon önerilerinin  $\chi^2$  değerinde kayda değer bir düşüş yaratmayacağı, bu nedenle de uyum iyiliği indekslerinde ciddi bir değişikliğin olmayacağı söylenebilir. Bu noktada sf2-sf7 modifikasyonu, su1-su4 modifikasyonu, kf5-kf9 modifikasyonu, ku4-ku12 modifikasyonu ve ku1-ku8 modifikasyonu yapılmış ve nihai uyum iyiliği indeksleri Tablo 9'da gösterilmiştir. Gerçekleştirilen modifikasyon işlemleri sonrasında  $\chi^2/\text{sd}$  oranının 1,438 olduğu ve mükemmel uyuma karşılık geldiği görülmüştür ( $p < .05$ ).



**Tablo 9**

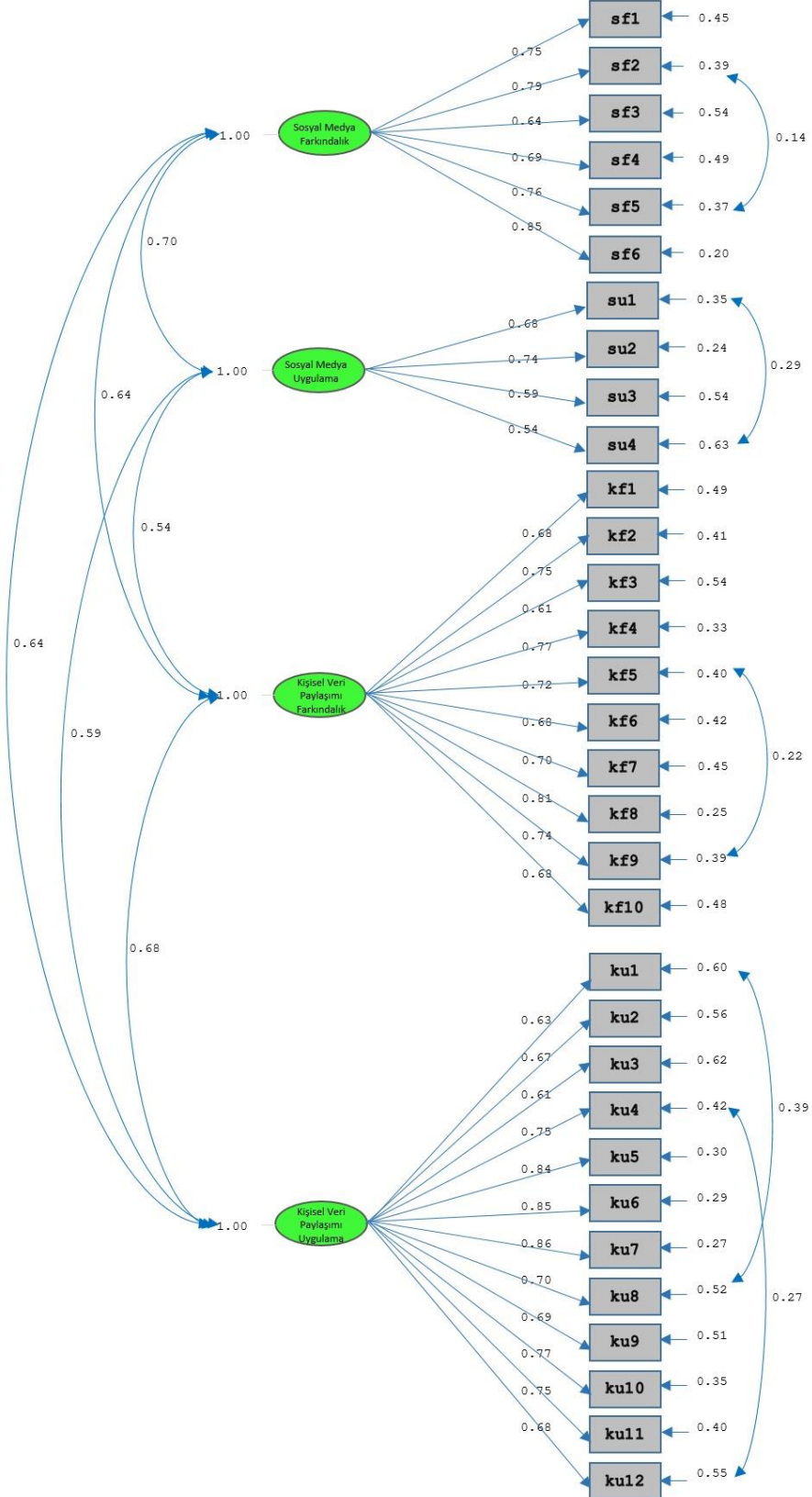
*Birincil Düzey Doğrulayıcı Faktör Analizinde Modifikasyon Sonrası Uyum İyiliği İndekslerine İlişkin Bulgular*

Uyum İyiliği İndeksleri	Model Değeri	İyi Uyum Değeri	Kabul Edilebilir Uyum Değeri
RMSEA	0,044	$0 \leq \text{RMSEA} \leq ,05$	$,05 < \text{RMSEA} \leq ,08$
NFI	0,93	$,95 \leq \text{NFI} \leq 1,00$	$,90 \leq \text{NFI} < ,95$
NNFI	0,97	$,97 \leq \text{NNFI} \leq 1,00$	$,95 \leq \text{NNFI} < ,97$
CFI	0,96	$,97 \leq \text{CFI} \leq 1,00$	$,95 \leq \text{CFI} < ,97$
S-RMR	0,048	$0 \leq \text{S-RMR} \leq ,05$	$,05 < \text{S-RMR} \leq ,10$
GFI	0,92	$,95 \leq \text{GFI} \leq 1,00$	$,90 \leq \text{GFI} < ,95$
AGFI	0,90	$,90 \leq \text{AGFI} \leq 1,00$	$,85 \leq \text{AGFI} < ,90$

Tablo 9 incelendiğinde uyum iyiliği indekslerinin büyük oranda iyi uyuma karşılık geldiği görülmektedir. Ölçek maddeleri ve birincil düzey doğrulayıcı faktör analizi sonucunda ortaya konan yapılar dikkatle incelenerek, ölçek boyutlarının “sosyal medya farkındalık”, “sosyal medya uygulama”, “kişisel veri paylaşımı farkındalık” ve “kişisel veri paylaşımı uygulama” şeklinde adlandırılmasına karar verilmiştir. Bu aşamaya ilişkin olarak, kurulan ölçme modelinin standart katsayıları Şekil 2’de, t testi bulguları ise Şekil 3’de gösterilmektedir.

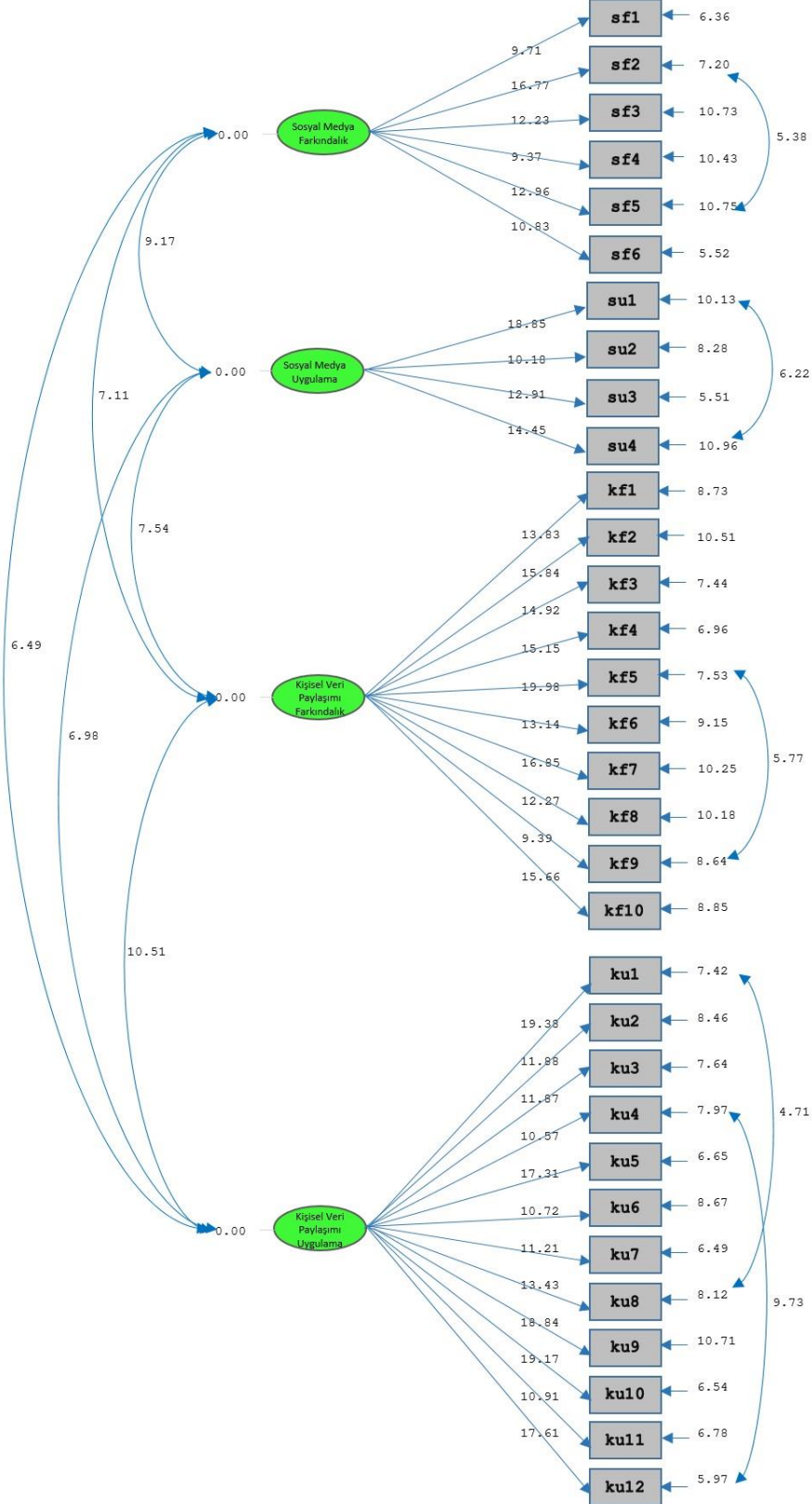
## Şekil 2

*Dijital Ayak İzi Farkındalık Ölçeğinin Birinci Düzey Doğrulayıcı Faktör Analizi Bağlantı Diyagramı (Standart Katsayılar)*



### Şekil 3

*Dijital Ayak İzi Farkındalık Ölçeğinin Birinci Düzey Doğrulayıcı Faktör Analizi Bağlantı Diyagramı (t Değerleri)*



## Dijital Ayak İzi Farkındalık Ölçeği'nin İkinci Düzey Doğrulayıcı Faktör Analizi Sonuçları

DAFÖ'nün birinci düzey doğrulayıcı faktör analizi ile elde edilen "sosyal medya farkındalık", "sosyal medya uygulama", "kişisel veri paylaşımı farkındalık" ve "kişisel veri paylaşımı uygulama" boyutlarının kuramsal olarak ileri sürülen dijital ayak izi farkındalığı faktörünü temsil edip etmediğini göstermek amacıyla bu dört boyutun bir üst boyutu olan dijital ayak izi farkındalığı ikinci düzey değişkeni ile olan yapısal ilişkilerini veren ikinci düzey doğrulayıcı faktör modeli oluşturulmuştur. 4 gizil ve 32 gösterge değişken ile test edilen birinci düzey doğrulayıcı faktöriyel yapıya, ikinci düzeyde dijital ayak izi farkındalığı gizil değişkeni de eklenerek ve birinci düzey doğrulayıcı faktör analizinde eklenen modifikasyon indeksleri de göz önünde bulundurularak ikinci düzey faktör modeli test edilmiştir. Gerçekleştirilen modifikasyon işlemleri sonrasında  $\chi^2/sd$  oranınının 1.264 olduğu ve mükemmel uyuma karşılık geldiği görülmüştür ( $p < .05$ ). Nihai uyum iyiliği indeksleri ise Tablo 10'da gösterilmiştir.

**Tablo 10**

*İkinci Düzey Doğrulayıcı Faktör Analizinde Modifikasyon Sonrası Uyum İyiliği İndekslerine İlişkin Bulgular*

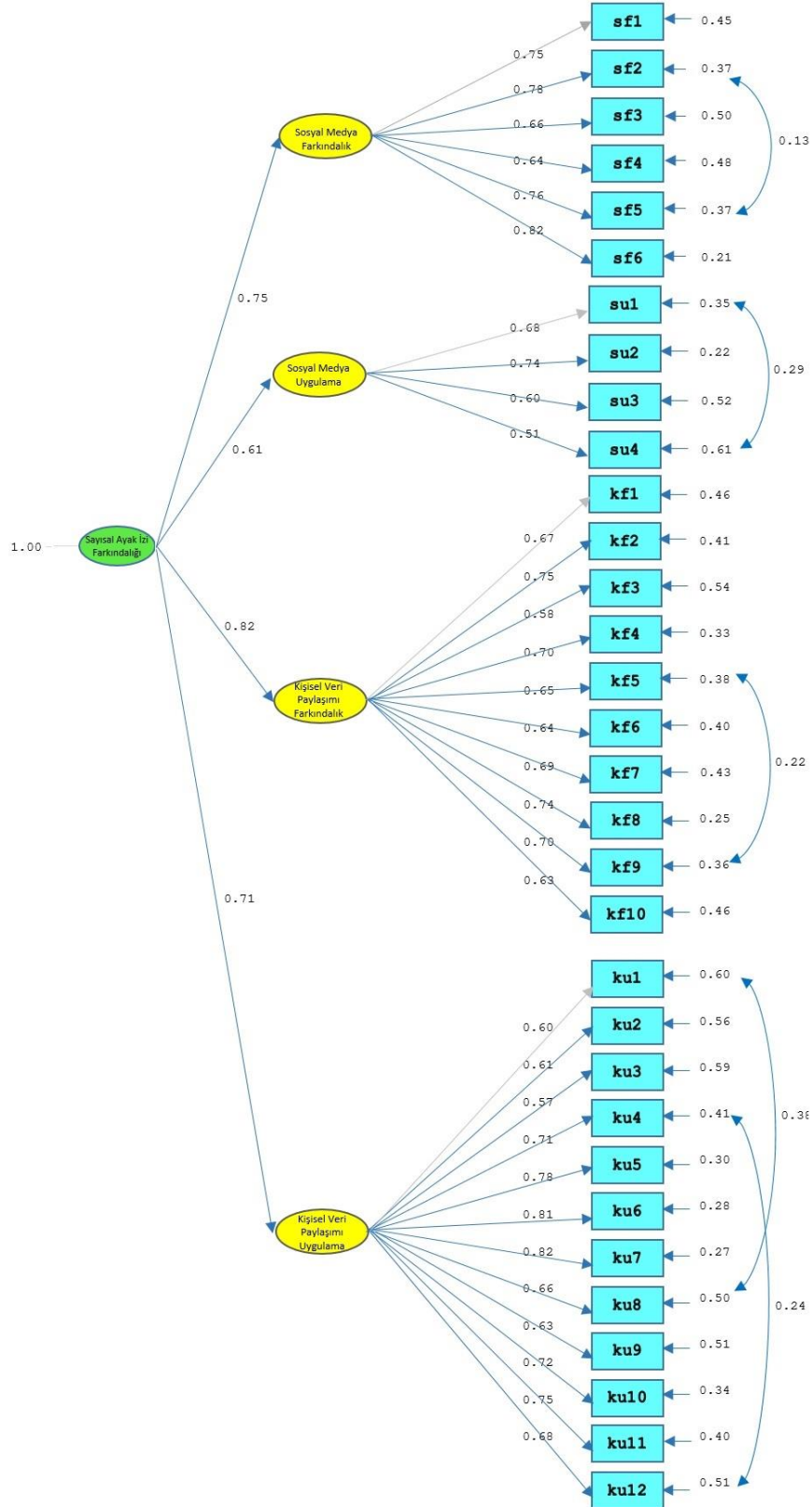
Uyum İyiliği İndeksleri	Model Değeri	İyi Uyum Değeri	Kabul Edilebilir Uyum Değeri
RMSEA	0,040	$0 \leq RMSEA \leq ,05$	$,05 < RMSEA \leq ,08$
NFI	0,94	$,95 \leq NFI \leq 1,00$	$,90 \leq NFI < ,95$
NNFI	0,98	$,97 \leq NNFI \leq 1,00$	$,95 \leq NNFI < ,97$
CFI	0,96	$,97 \leq CFI \leq 1,00$	$,95 \leq CFI < ,97$
S-RMR	0,042	$0 \leq S-RMR \leq ,05$	$,05 < S-RMR \leq ,10$
GFI	0,92	$,95 \leq GFI \leq 1,00$	$,90 \leq GFI < ,95$
AGFI	0,91	$,90 \leq AGFI \leq 1,00$	$,85 \leq AGFI < ,90$

Tablo 10 incelendiğinde uyum iyiliği indekslerinin büyük oranda iyi uyuma karşılık geldiği görülmektedir. Modelin nihai t değerleri Şekil 3.11'de görülmektedir. Nihai modele ilişkin standart katsayılar Şekil 4'de, t testi bulguları ise Şekil 5'de gösterilmektedir. Elde edilen bu

bulgular dođrultusunda ölçeđin çok faktörlü yapısının dođrulandıđı ve yapı geçerliđinin sađlandıđı söylenebilir.

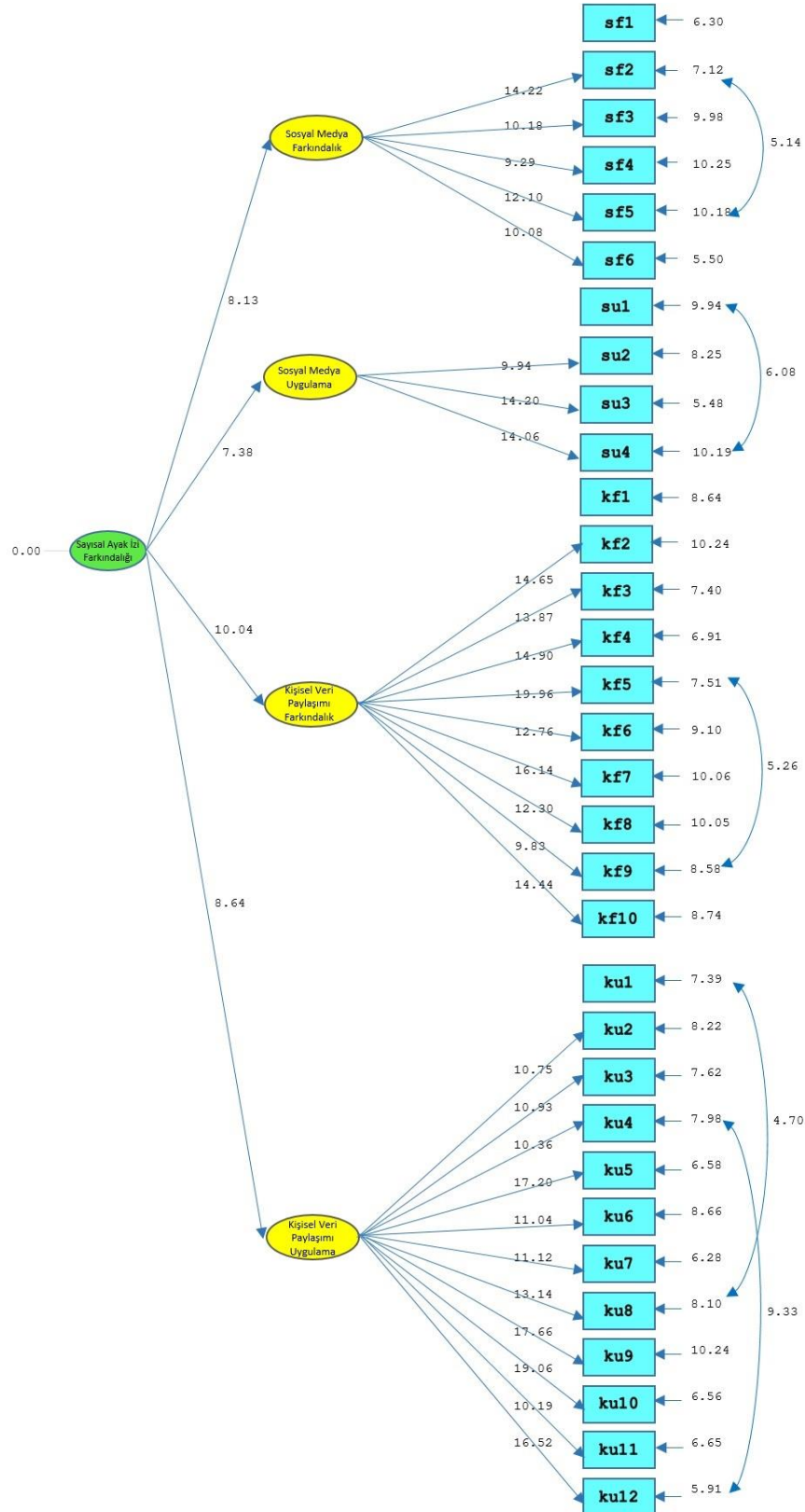
## Şekil 4

Dijital Ayak İzi Farkındalık Ölçeğinin İkinci Düzey Doğrulayıcı Faktör Analizi Bağlantı Diyagramı (Standart Katsayılar)



## Şekil 5

Dijital Ayak İzi Farkındalık Ölçeğinin İkinci Düzey Doğrulayıcı Faktör Analizi Bağlantı Diyagramı (t Değerleri)



## Dijital Ayak İzi Farkındalık Ölçeğinin Güvenirlik Bulguları

Dijital Ayak İzi Farkındalık Ölçeği'nin Cronbach Alpha iç tutarlılık katsayılarına ilişkin sonuçlar Tablo 11'de gösterilmektedir.

**Tablo 11**

*Dijital Ayak İzi Farkındalık Ölçeği Cronbach Alpha İç Tutarlılık Katsayıları*

Faktör	Madde	Madde		
		Toplam Korelasyonu (r)	$\alpha$	$\omega$
Kişisel Veri Paylaşımı Farkındalık	1. İnternet ortamındaki paylaştığım kişisel bilgilerimin kontrolüm dışında yabancı kişiler ile paylaşılabilceğini bilirim.	0,541	,937	,881
	2. İnternet ortamdaki her hareketimin dijital kimliğimin bir parçasını oluşturduğunu bilirim.	0,587		
	3. İnternet ortamındaki her hareketimin kayıt altına alındığını bilirim.	0,612		
	4. İnternet ortamında bıraktığım izlerin farklı sektörlerde veri olarak kullanılabileceğinin farkındayım.	0,628		
	5. İnternet ortamında yaptığım her paylaşımın gelecekte karşıma çıkabileceğinin farkındayım.	0,493		
	6. Ziyaret ettiğim web sitelerinin, yaklaşık konumumu tanımlayan IP adresimi kaydettiğinin farkındayım.	0,543		
	7. İnternet kafe, ortak kullanımlı bilgisayar laboratuvarları vb. ortamlarda bilgilerimin/ paylaşımlarımın başkalarının eline geçme ihtimali olduğunu düşünürüm.	0,596		



	8. İnternet ortamında ücretsiz hizmet veren sitelerin bir amacının da kullanıcı deneyimleri kapsamında kişisel verileri toplamak olduğunun farkındayım.	0,621	
	9. İnternet ortamda gezinirken karşıma çıkan reklamlara tıklamamam gerektiğinin farkındayım.	0,610	
	10. İnternet ortamlarında oynadığım oyunların, izlediğim video, film ve dizilerin, okuduğum haberlerin reklam algoritmaları için veri kaynağı olduğunu bilirim.	0,588	
	1. İnternet ortamında fotoğraflarımı paylaşmaktan çekinmem.	0,550	
	2. İnternet ortamında kullandığım şifrelerim için "Beni Hatırla" özelliğini kullanırım.	0,452	
	3. İnternet üzerinde karşıma çıkan ve onaylamak zorunda olduğum kullanıcı sözleşmelerini okurum.	0,592	
	4. İnternette kimlik bilgilerimi paylaşmamaya dikkat ederim.	0,646	
	5. Arama motorlarına adımları yazıp hakkımda çıkan bilgileri kontrol ederim.	0,608	
Kişisel Veri Paylaşımı	6. Ortak kullanım alanlarında kullanıcı adı ve şifre bilgisiyle giriş yaptığım uygulamalardan, bilgisayardan kalkmadan önce çıkış yaparım.	0,544	,922 ,842
Uygulama	7. Ortak kullanım alanlarında (kafeler, kütüphaneler gibi) şifresiz kablosuz ağ (Wi-Fi) bağlantılarına katılmam.	0,512	
	8. İnternet ortamında kullandığım şifrelerin güçlü (büyük/küçük harf, özel karakter, rakam içermesi gibi) olmasına özen gösteririm.	0,496	
	9. Mail adresime gelen mailerin içerisindeki linklerin güvenliğinden emin olmadan tıklamam.	0,564	

	10. İnternet ortamında kullanmak zorunda olduğum uygulamalara yeterli düzeyde bilgi veririm.	0,398		
	11. İnternet ortamında yaptığım herkese açık paylaşımlar, gerçek düşüncelerimi yansıtmaktadır.	0,474		
	12. İnternet sitelerinde, mikrofon kullanımına izin ver, kamera kullanımına izin ver, konum paylaşmaya izin ver gibi izin taleplerine dikkat eder, yalnızca gerekli gördüklerimi onaylarım.	0,516		
	1. Sosyal medya ortamlarında paylaştığım, yorum yaptığım veya beğendiğim paylaşımları silsem bile tamamen yok olmadığını bilirim.	0,488		
	2. Sosyal medya ortamlarında paylaştığım fotoğrafların, yaptığım beğenilerin karakterim, özel yaşantım, kültürel ve sosyal hayatım hakkında fikir oluşturduğunun farkındayım.	0,546		
Sosyal Medya Farkındalık	3. Paylaştığım gönderilerin yalnızca benim izin verdiğim kimseler tarafından görüntülenmediğinin farkındayım.	0,538	,854	,810
	4. Sosyal medyada paylaştığım fotoğraf, video ve yorumların kontrolüm dışında kullanılabileceğinin farkındayım.	0,640		
	5. Sosyal medyada yaptığım her türlü işlemin kayıt altına alındığını bilirim.	0,618		
	6. Sosyal medyada kişiler arası sohbetlerin gizli kalmayabileceğinin farkındayım.	0,592		
Sosyal Medya Uygulama	1. Kullandığım sosyal medya araçlarının gizlilik ayarlarını sürekli gözden geçirip düzenlerim.	0,482		
	2. Sosyal medya platformlarında profilimde paylaştığım her gönderiyi herkese açık bir şekilde paylaşırım.	0,526	,829	,794

3. Sosyal medyada yazdıklarımı üslup ve içerik açısından kontrol ederek paylaşırım.	0,608
4. Sosyal medya hesaplarımda profil resmi kullanırım.	0,590

32 maddelik Dijital Ayak İzi Farkındalık Ölçeği'nin tamamının Cronbach Alpha iç tutarlılık katsayısı ,828 ve Standartlaştırılmış Cronbach Alpha iç tutarlılık katsayısı ise ,827 olarak bulunmuştur. Her iki iç tutarlılık değerinin 1'e yakın olduğu görülmektedir. 1'e yakın değerler alan iç tutarlılık katsayıları, ölçeğin güvenilir olduğunu belirtmektedir. Aynı şekilde ölçeğin tamamına ilişkin McDonald's Omega ( $\omega$ ) katsayısı ise ,832'dir.

Her bir maddenin kendisi ve toplam puan ile arasındaki korelasyonu gösteren madde toplam korelasyonları incelendiğinde 0,398 ve 0,646 arasında değiştiği sonucuna ulaşılmıştır. Tüm değerler 0,3 üzerinde olduğu için bu değerler kabul edilebilir seviyededir (Field, 2005).

### **Dijital Ayak İzi Farkındalığı ile Bilgi Güvenliği Farkındalığı İlişkisi**

Dijital Ayak İzi Farkındalığı ile Bilgi Güvenliği Farkındalığı ölçeklerinin her bir alt boyutu ile ölçeklerin bütünü aralarındaki korelasyonlar Pearson korelasyon katsayısı ile incelenmiştir. Sonuçlar Tablo 12'de sunulmuştur.

**Tablo 12**

*Dijital Ayak İzi Farkındalığı ile Bilgi Güvenliği Farkındalığı arasındaki ilişkileri gösterir*

*Pearson Korelasyon Katsayıları*

	1	2	3	4	5	6	7	Sayısal Ayak İzi Farkındalığı	Bilgi Güvenliği Farkındalığı
1- Saldırı ve Tehditler	1								
2- Mahremiyet	,326*	1							
3- Kişisel Verilerin Korunması	,458*	,860*	1						
4- Kişisel Veri Paylaşımı	,568*	,712*	,806*	1					
5- Kişisel Veri Paylaşımı	,602*	,740*	,740*	,882*	1				
6- Sosyal Medya	,580*	,625*	,579*	,758*	,587*	1			
7- Sosyal Medya	,456*	,618*	,568*	,684*	,648*	,827*	1		
Sayısal Ayak İzi Farkındalığı	,618*	,705*	,774*	,785*	,705*	,782*	,793*	1	
Bilgi Güvenliği Farkındalığı	,694*	,732*	,693*	,764*	,678*	,666*	,588*	,794*	1

\*: p<,05

Tablo 12 incelendiğinde en önemli bulgunun ilişkisi araştırılan dijital ayak izi farkındalığı ve bilgi güvenliği farkındalığı arasında ve yüksek düzeyde olduğu görülmektedir. Bu bulgu bize bilgi güvenliği farkındalığına sahip öğrencilerin dijital ayak izi konusunda da farkındalık sahibi oldukları ve bunu uygulamaya döktükleri sonucuna ulaştırabilir. Bunun aksi de geçerlidir. Düşük düzeyde bilgi güvenliği farkındalığına sahip öğrencilerin benzer şekilde düşük düzeyde dijital ayak izi farkındalığına sahip oldukları söylenebilir.

Tablodaki en yüksek ilişki ,882 ile DAFÖ alt boyutlarından kişisel veri paylaşımı uygulama ve kişisel veri paylaşımı farkındalık arasındadır. Bu yüksek ilişki bize kişisel veri paylaşımı farkındalık düzeyi yüksek olan kullanıcıların bunu uygulamaya da döktüklerini söylemektedir. Kişisel veri paylaşımı konusunda özenli davranan, mahremiyetine önem veren kullanıcıların bu bilgileri paylaşırken de özenli ve dikkatli davrandıkları söylenebilir.

Tablodaki ikinci yüksek ilişki ise BGFÖ alt boyutlarından kişisel verilerin korunması ve mahremiyet arasındadır. Mahremiyet kişilerin bireysel alanları ile ilgilidir. Kişisel verilerin korunması benzer şekilde mahremiyete dikkat etmeyi de beraberinde getirir.

Tabloda bilgi güvenliği farkındalığı ile sosyal medya uygulama arasında orta düzeyde bir ilişki olduğu görülmüştür. Bu bize bilgi güvenliği farkındalığına sahip kullanıcıların sosyal medya kullanımında aynı farkındalıkla davranmadıklarını, bilgiye sahip olsalar da yeterli düzeyde dikkatli davranmadıklarını söylemektedir.

Bir diğer orta düzeyde ilişki ise sosyal medya farkındalık ve saldırı ve tehditler arasındadır. Bu sonuç sosyal medyanın verimli ve sağlıklı kullanımı konusunda farkındalık sahibi kullanıcıların saldırı ve tehditlere karşı yeterince bilgi sahibi olmadığı veya yeterince önlem almadığını söylemektedir. Kullanıcıların sosyal medya kullanımı hakkında farkındalıklı olsalar dahi saldırı ve tehditlere karşı aynı oranda farkındalık sahibi olmadıkları, savunmasız kaldıkları söylenebilir.

Tablodaki en düşük düzeyde ilişki ise BGFÖ alt boyutlarından mahremiyet ve saldırı ve tehditler arasındadır. Saldırı ve tehditler ile tüm bireylerin karşılaşabileceği, bunun kişinin

farkındalığına ve kişisel mahremiyetine dikkat etmesi ile ilgisi olmadığı, mahremiyetine dikkat eden kullanıcıların da saldırı ve tehditler ile karşı karşıya kaldığı yorumu yapılabilir. Saldırı ve tehditlerin dışardan geldiği düşünülduğünde bu ilişki beklenen sonuçlardan biridir.

Tablo geneline bakıldığında çoğu ilişkinin yüksek düzeyde olduğu görülmektedir. Kısaca dijital ayak izi farkındalığı ile bilgi güvenliği farkındalığı arasında yüksek bir ilişki olduğu söylenebilir. Bunun yanında dijital ayak izi farkındalığı ölçeği alt boyutlarından sosyal medya kullanımı ve kişisel veri paylaşımı arasında da yüksek düzeyde ilişki görülmüştür. BGFÖ ölçeği alt boyutları arasında ise DAFÖ kıyasla daha düşük ilişkiler göze çarpmaktadır.

## Bölüm 5

### Sonuç, Tartışma ve Öneriler

#### Sonuçlar ve Tartışma

Bu araştırma kapsamında Acele'nin (2020) bu alandaki psikolojik yapıyı ölçmeye yarayan bir ölçek gereksinimi olduğu noktasından ve alanyazından hareketle ortaöğretim öğrencilerinin dijital ayak izi farkındalığını ölçebilecek bir ölçme aracı geliştirilmiş, geçerliliği ve güvenilirliği sınanmıştır. Ardından "Ortaöğretim Öğrencilerine Yönelik Bilgi Güvenliği Farkındalık Ölçeği" aracılığı ile öğrencilerin bilgi güvenliği farkındalığı araştırılmış ve dijital ayak izi farkındalıkları ile arasındaki ilişki incelenmiştir.

Araştırmanın en önemli bulgusu dijital ayak izi farkındalığı ve bilgi güvenliği farkındalığı arasındaki yüksek ilişkidir. Katılımcıların bilgi güvenliği konusundaki farkındalıkları ve dijital ayak izi farkındalıkları arasındaki ilişki oldukça yüksek bulunmuştur. Buradan hareketle katılımcıların bilgi güvenliği farkındalığı arttıkça dijital ayak izi konusundaki farkındalık ve uygulama düzeylerinin de benzer oranda artacağı söylenebilir. Bilgi güvenliği konusunda özenli davranan kullanıcıların çevrimiçi ortamlarda bıraktıkları dijital ayak izleri konusunda da özenli oldukları ve bunu uygulama düzeyinde de gösterdikleri çalışmanın sonuçları arasındadır. Dönmez'in 2019 yılında lise öğrencileri ile yaptıkları çalışmada bilgi güvenliği farkındalığı ve dijital okuryazarlık arasında anlamlı ve pozitif yönde bir ilişki bulunmuştur. Bu bulgu, yapılan bu araştırmanın bulguları ile örtüşmektedir. Ayrıca Yılmaz Soylu, Demiröz ve Akkoyunlu'nun 2021 yılında ortaokul öğrencileri ile yaptıkları çalışmada, ortaokul öğrencilerinin dijital ayak izi ile ilgili bilgiye sahip olduklarını fakat uygulama boyutuna bakıldığında farklı değişkenlerden etkilendiği yönünde bulguları bulunmaktadır.

Bu çalışmada DAFÖ boyutlarından sosyal medya ve kişisel veri paylaşımının farkındalık boyutu ile sosyal medya - kişisel veri paylaşımı uygulama boyutu arasında yüksek düzeyde bir ilişki bulunmuştur. Yani örneklem grubunun sosyal medya ve kişisel veri paylaşımı konusunda farkındalığı arttıkça bunu uygulamaya dökme durumları da aynı oranda artacaktır.

Araştırma, Yılmaz Soylu, Demiröz ve Akkoyunlu'nun (2021) yaptıkları çalışma ile bu noktada birbirinden ayrılmaktadır. Farklılığın, bu çalışmada farkındalığın uygulama boyutunun farklı değişkenler açısından incelenmemiş olmasından veya araştırmanın yürütüldüğü sınıf düzeyinin farklı olmasından kaynaklandığı düşünülmektedir.

Araştırmada en yüksek ilişki, DAFÖ boyutlarından kişisel bilgi paylaşımının uygulama düzeyi ile kişisel bilgi paylaşımı farkındalığı arasında görülmüştür. Bu durum katılımcıların kişisel bilgi paylaşımı farkındalık düzeyleri arttıkça bu farkındalığı uygulamaya dökme, kişisel bilgilerini paylaşırken özenli davranma konusundaki davranışlarının da benzer oranda arttığını ortaya koymaktadır. Vervier vd. (2017) dijital ayak izi algısı ve gizliliğin değeri üzerine yaptıkları çalışmada kişilerin çevrimiçi ortamda geride bıraktıkları kişisel bilgilerin, özellikle hassas verilerin öneminin farkındalığına ne ölçüde sahip oldukları araştırmışlardır. Sonuçlar, gençlerin bilinçli olarak dijital ayak izlerini yönetemediğini ortaya koymaktadır. Araştırmacıların, farkındalık düzeyi düşük öğrencilerin bilgi paylaşımı konusunda yeterince özenli olamadığı sonucuna ulaşması bu çalışma sonuçlarını da destekler niteliktedir.

İkinci bir benzer sonuç ise DAFÖ boyutlarından sosyal medyayı etkin kullanma ve sosyal medyaya ilişkin farkındalık düzeyleri arasında görülmüştür. Sosyal medyanın verimli ve güvenli kullanımı hakkında farkındalığı yüksek olan öğrencilerin sosyal medyayı etkin ve düzenli kullandıkları da araştırmanın sonuçları arasındadır. Sürmelioğlu ve Seferoğlu'nun (2019) yaptıkları çalışmadan hareketle en fazla dijital ayak izi bırakılan ortamlar arasında sosyal ağların ikinci sırada gelmesi çalışmanın bulguları açısından önem taşımaktadır. Bu önemli bulgudan sonra en çok dijital izi bırakılan alanlardan biri olan sosyal ağlar konusunda farkındalığın, uygulama düzeyini de yüksek oranda etkilediği göz önünde bulundurulmalıdır.

Camacho vd. (2012) lisans düzeyinde öğrenim görmekte olan 18- 45 yaş aralığındaki 135 öğrenciden dijital kimlik algıları, sosyal ağ kullanımı hakkındaki tutumları ve öğrencilerin gizlilik tercihleri konusunda veri toplamışlardır. Katılımcıların kimlik oluşturma süreçleri hakkında yüksek seviyede bir farkındalık gösterdiği, gizlilik ayarlarını kullandıkları, yükledikleri içeriğe önem verdikleri ve gerçek kimlikleriyle yakından ilişkili bir kimlik sundukları araştırma



bulgularındandır. Katılımcıların çoğu kişisel ve mesleki hayatlarını korumak açısından dijital ayak izlerinin etkisi konusunda endişe duysalar da “çevrimiçi olma” arzusunu ve gerçekte kim olduklarını, kişilik özelliklerini yansıtmak istediklerini belirtmişlerdir.

BGFÖ boyutlarından kişisel verilerin korunması ve mahremiyet arasında da oldukça yüksek bir ilişki olduğu görülmüştür. Katılımcıların mahremiyetlerine dikkat ettikleri ölçüde kişisel verilerinin korunması konusundaki hassasiyetlerinin arttığı söylenebilir.

Katılımcıların DAFÖ boyutlarından kişisel veri paylaşımı konusundaki farkındalıkları ile kişisel verilerin korunması konusundaki davranışları arasında da yüksek bir ilişki olduğu söylenebilir. Kişisel veri paylaşımına dikkat eden katılımcıların kişisel verilerinin korunması konusunda oldukça duyarlı davrandıkları bu araştırmanın sonuçlarındandır.

Yukarıdaki sonuçlara benzer şekilde katılımcıların DAFÖ boyutlarından sosyal medya konusunda ki farkındalıkları ve kişisel veri paylaşımı farkındalık düzeyleri arasında da yüksek bir korelasyon olduğu görülmüştür. Buradan hareketle sosyal medya kullanımında farkındalığı olan katılımcılar kişisel veri paylaşımı konusunda da dikkatli davranmaktadır. Sosyal medyanın bir açıdan çok fazla kişisel veri paylaşımına sebebiyet verdiği düşünülürse bu sonucun beklenen bir sonuç olduğu söylenebilir.

DLEARN (2019) tarafından Avrupa vatandaşları ile yapılan araştırmada yükseköğretim mezunu katılımcıların bıraktıkları dijital ayak izleri konusunda yeterince bilgi sahibi olmadıkları ve araştırmada %39,49 oranında Facebook, Instagram gibi özel şirketlerin bırakılan bu izlere sahip olduğunu belirtmişlerdir. Bu araştırmanın sonuçlarından hareketle dijital ayak izi ve sosyal medya kullanımında bırakılan izlerin farkında olmayan örneklem grubunun kişisel veri paylaşımı konusundaki farkındalık ve uygulama düzeylerinin de düşük olabileceği ve benzer şekilde bilgi güvenliği farkındalıklarının düşük olabileceği yorumu yapılabilir.

Katılımcıların DAFÖ boyutlarından kişisel verileri paylaşma konusundaki davranış düzeyleri ile BGFÖ boyutu olan kişisel verilerin korunması arasında yüksek bir korelasyon olduğu görülmüştür. Kişisel verilerini paylaşma konusunda etkin davranan katılımcıların kişisel

verilerin korunması konusunda da etkin olduğu söylenebilir. Benzer şekilde kişisel veri paylaşımı konusunda dikkatli davranan katılımcıların BGFÖ boyutu olan mahremiyet konusuna da dikkat ettikleri çalışma sonuçları arasında yer almaktadır. DLEARN (2019) tarafından yapılan araştırma da katılımcıların %70,91'inin çevrimiçi kişisel verilerinin ihlale maruz kalabileceğinin farkında olduklarını belirtmişlerdir.

DAFÖ boyutu olan kişisel veri paylaşımı farkındalığı ile BGFÖ boyutu olan mahremiyet arasında da yüksek bir ilişki olduğu görülmüştür. Kişisel veri paylaşımı konusunda farkındalığı sahip katılımcıların mahremiyetlerine de aynı oranda dikkat ettikleri söylenebilir. Yine bir diğer yüksek korelasyon DAFÖ boyutlarından dijital ayak izi konusundaki farkındalık ile sosyal medya kullanımı arasında görülmektedir. Dijital ayak izi farkındalığı yüksek olan katılımcıların sosyal medya kullanımında dikkatli ve daha bilinçli davrandıkları söylenebilir. Buradan hareketle benzer şekilde dijital ayak izi farkındalığı ile sosyal medya kullanımı konusundaki farkındalık düzeyi de yüksek oranda ilişkilidir. Aynı zamanda yine DAFÖ boyutlarından dijital ayak izi farkındalığı ile kişisel veri paylaşımı farkındalığı arasında da yüksek düzeyli bir ilişki görülmüştür. Dijital ayak izi konusunda farkındalığı yüksek katılımcıların kişisel verilerini paylaşma konusundaki farkındalıkları da yüksektir denilebilir. Dijital ayak izi farkındalığı yüksek kullanıcıların kişisel verilerinin korunması konusunda da dikkatli davrandıkları bu çalışmanın sonuçları arasındadır.

Yukarıdaki sonuçlara benzer şekilde dijital ayak izi farkındalığı yüksek kullanıcılarında BAFÖ boyutlarından mahremiyet konusuna dikkat etme düzeyleri de yüksektir. Sosyal medyayı etkin ve özenli kullanan kullanıcılarında dijital ayak izi farkındalıklarının yüksek olduğu yine çalışma sonuçları arasında yer almaktadır.

BDFÖ boyutlarından bilgi güvenliği farkındalığı ile DAFÖ boyutlarından kişisel veri paylaşımı farkındalığına bakıldığında aralarında yüksek oranda bir ilişki olduğu görülebilir. Bilgi güvenliği konusunda farkındalığı olan katılımcıların kişisel veri paylaşımı konusunda da farkındalıklı oldukları söylenebilir. Ayrıca bilgi güvenliği farkındalığı yüksek kullanıcıların kişisel verileri paylaşma konusunda da özenli davrandıkları bu çalışmanın sonuçlarındandır.

Bir diğ er sonuç BGFÖ boyutlarından bilgi güvenliđ i farkındalıđ ı ile mahremiyet arasındaki yüksek iliřkidir. Bilgi güvenliđ i farkındalıđ ı yüksek kullanıcıların mahremiyet konusunda da duyarlı oldukları görölmüřtür. Mahremiyetine dikkat eden katılımcıların bilgi güvenliđ i farkındalıđ ı da yüksektir denilebilir.

BGFÖ boyutlarından bilgi güvenliđ i farkındalıđ ı ile saldırı ve tehditler arasında da yüksek düzeyli bir korelasyon görölmüřtür. Buradan hareketle bilgi güvenliđ i farkındalıđ ı yüksek olan katılımcıların saldırı ve tehditler konusunda duyarlı ve farkında oldukları söylenebilir. Tehditler, özellikle gençlere özgü olmamakla birlikte, gençlerin yeni bir teknolojiyi benimsemekteki tutkuları, karşılaşılabilecekleri tehditler konusundaki saflıkları ile birleşince onları bu tehditlere karşı onları daha açık kılmaktadır (Atkinson vd., 2009). Burada farkındalıđ ın önemi bir kez daha ortaya çıkmaktadır. Teknoloji geliřtikçe bilgi güvenliđ ine yönelik tehdit ve saldırı yöntemleri de çeşitlenmektedir (Güldüren vd., 2016). Bu noktada insanları doğru olmayan bilgiler ile kandırmaya dayanan sosyal mühendislik, çevrimiçi ortamlarda saldırganların çok sık kullandıđ ı bir taktik haline gelmiřtir (Mitnick, 2002).

DAFÖ boyutlarından dijital ayak izi farkındalıđ ı ile BGFÖ boyutlarından saldırı ve tehditler arasında da yüksek oranda bir iliřki söz konusudur. Dijital ortamda bırakılan izler konusunda farkındalıđ ı yüksek olan katılımcıların saldırı ve tehditler konusunda aynı oranda dikkatli ve farkında davrandıkları söylenebilir.

DAFÖ boyutlarından kişisel verilerini paylaşma konusunda özenli davranıř sergileyen ve bu konuda dikkatli davranan kullanıcıların BGFÖ boyutlarından saldırı ve tehditler konusunda da aynı oradan bilgi sahibi oldukları ve temkinli davrandıkları söylenebilir. Sosyal medyayı etkin kullanma ile kişisel veri paylaşımı konusunda dikkatli davranıř sergileme arasında yüksek bir iliřki vardır. Buradan hareketle kişisel veri paylaşımı konusunda özenli davranan katılımcıların sosyal medyada da özenli davrandıkları görölmüřtür.

BGFÖ boyutlarından mahremiyete bakıldıđ ında bu konuda dikkatli katılımcıların saldırı ve tehditlerden kaçınmaları açısından tablo incelendiđ inde zayıf bir iliřki olduđu görölmüřtür. Mahremiyet daha kişisel bir alan iken saldırı ve tehditlerin dışardan geldiđ i ve engellenemez

olduğu düşünülürken beklenen bir sonuç olduğu söylenebilir. Kişisel verilerin korunması ile saldırı ve tehditler arasındaki ilişkiye bakıldığında ise orta düzeyde bir korelasyon olduğu görülmüştür. Bu bilgi kişisel verilerin korunması konusunda farkındalığı yüksek olan katılımcıların saldırı ve tehditler konusunda orta düzeyde farkında oldukları ve bunun orta düzeyde önlenebilir olduğu sonucuna götürebilir.

Araştırma kapsamında geliştirilen ölçeğin boyutlarından biri olan kişisel veri paylaşımı konusundaki katılımcıların farkındalıkları ile saldırı ve tehditler konusundaki farkındalık düzeyleri arasındaki ilişki orta düzeyde bulunmuştur. Buradan hareketle kişisel verilerin korunması konusunda farkındalığı olan katılımcıların saldırı ve tehditler konusunda da farkındalıklı oldukları orta düzeyde de olsa beklenebilir bir sonuçtur. Benzer şekilde sosyal medyayı etkin kullanma konusunda farkındalıklı katılımcıların saldırı ve tehditler konusundaki farkındalıkları arasında da orta düzeyde bir ilişki bulunmuştur.

Yüksek düzeyde bulunan bir diğer ilişki ise bilgi güvenliği farkındalığı ve katılımcıların kişisel verilerin korunması konusundaki bilgileri arasındadır. Kişisel verilerin korunması konusunda bilgi sahibi olan katılımcıların bilgi güvenliği farkındalıklarının da yüksek olması beklenen sonuçlar arasındadır. Benzer şekilde sosyal medya kullanımı konusunda farkındalık sahibi kullanıcıların bilgi güvenliği konusunda farkındalıklarının yüksek olduğu araştırma sonuçlarındandır.

Bir diğer sonuç kişisel mahremiyetlerine dikkat eden katılımcıların sosyal medya kullanımı konusunda daha farkında davrandıkları ve bunu uygulamaya döktükleri, sosyal medyayı daha özenli ve dikkatli kullandıkları görülmüştür. Etik kurallara uymak, amacına uygun hareket etmek ve bunu mahremiyet bilinci ile gerçekleştirmek dijital ayak izini oluşturan temel bileşenlerdir (Acele, 2019). Dijital ayak izlerine dikkat eden, internet ortamında doğru gezinen bireylerin daha iyi birer dijital vatandaş olabilecekleri açıktır (Acele, 2019). Bu durumun da henüz okul çağlarındayken öğrencilere kazandırılması gerektiği ileri sürülmektedir (EAVI, 2019). Kişisel veri paylaşımı konusunda dikkatli davranış sergileyen kullanıcıların sosyal medyayı kullanma konusunda da dikkatli ve özenli davrandıkları, aralarında yüksek düzeyde

ilişki ile açıklanabilir. Fakat kişisel veri paylaşımı konusunda dikkatli olan katılımcıların orta düzeyde sosyal medya kullanımı farkındalığına sahip olduğu araştırma sonuçları arasındadır.

Orta düzeyde bir diğer ilişki ise BGFÖ boyutlarından sosyal medyanın etkin kullanımı ile katılımcıların kişisel verilerin korunması konusundaki bilgi düzeyleri arasındadır. Benzer şekilde sosyal medyanın etkin kullanımı konusunda farkında olan katılımcıların da kişisel verilerin korunması konusundaki farkındalıkları arasında orta düzeyde bir ilişki bulunmuştur. DAFÖ boyutlarından sosyal medyanın etkin kullanımı ile BGFÖ boyutlarından saldırı ve tehditler konusundaki farkındalık arasında orta düzeyde bir ilişki görülürken, bilgi güvenliği ve farkındalığı ile sosyal medyayı etkin kullanım arasında da benzer şekilde orta düzeyde bir ilişki bulunduğu yine araştırma sonuçları arasındadır.

## Öneriler

- Araştırma sonucunda elde edilen sonuçlardan aşağıdaki öneriler sunulabilir:
- Ortaöğretim öğrencileri için geliştirilmiş olan Dijital Ayak İzi Farkındalığı Ölçeğinin ilerleyen yıllarda aynı geçerlilik ve güvenilirliği sergileyip sergilemediği belirli bir süre sonra yeniden araştırılabilir.
- Bu çalışma kapsamında geliştirilen ölçek ile ortaöğretim öğrencileri üzerinde dijital ayak izi farkındalığı ve başka değişkenler arasındaki ilişki araştırılabilir.
- Çalışma sonucunda ortaya çıkan ölçek, ortaöğretim öğrencilerinin dijital ayak izi farkındalıklarını ölçmek için kullanılabilir.
- Öğrencilerin dijital ayak izi farkındalık seviyelerinin bir takım demografik değişkenlere göre değişip değişmediği araştırılabilir.
- Bu araştırma bulguları öğrencilerin kendi öz beyanlarına dayalı verilerden elde edildiği için bu ölçümlerin gerçek hayattaki davranışlara ne kadar yansıdığı araştırılabilir. Buradan hareketle dijital ayak izi farkındalığı ve bilgi güvenliği farkındalığının gerçek

bir davranışa evrilip evrilmediđi, daha farklı bir ifadeyle benimsenerek sosyal medyanın veya diđer dijital mecraların dikkatli kullanılıp kullanılmadıđı araştırılabilir.

## Kaynaklar

- Acele, B. (2020). *Bilişim teknolojileri öğretmenlerinin ve öğretmen adaylarının sayısal ayak izi farkındalık düzeylerinin incelenmesi*. Yayınlanmamış yüksek lisans tezi, Hacettepe Üniversitesi Eğitim Bilimleri Enstitüsü, Ankara.
- Akkoyunlu, B. (2016). *Sayısal ayak izim*. <http://www.bilimiletisimi.com/show.php?id=2832>
- Australian Communications and Media Authority. (2013). *Digital footprints and identities: Community attitudinal research*. <https://www.acma.gov.au/-/media/Regulatory-Frameworks-and-InternationalEngagement/Information/pdf/Digital-footprints-and-identities-communityattitudinal-research-pdf.pdf>
- Aslankara, V. B., & Seferoğlu, S. S. (2019). Öğretmenlerin dijital ayak izi farkındalık durumlarıyla ilgili bir inceleme. *13. Bilgisayar ve Öğretim Teknolojileri Sempozyumu*, Kırşehir.
- Atkinson, S., Furnell, S., & Phippen, A. (2009). Securing the next generation: enhancing e-safety awareness among young people. *Computer Fraud & Security*, 7, 13-19. [https://doi.org/10.1016/S1361-3723\(09\)70088-0](https://doi.org/10.1016/S1361-3723(09)70088-0)
- Bodhani, A. (2012). Shops offer the e-tail experience. *Engineering & Technology*, 7(5), 46-49. <http://dx.doi.org/10.1049/et.2012.0512>
- Buchanan, R., Scevak, J., Smith, S. P., & Southgate, E. (2016). What do students understand about dijital footprint management? Examining social media education for career guidance. *AARE Conference*, November 27- December 1, Melbourne.
- Buchanan R., Southgate, E., Smith, S. P., Murray, T., & Noble, B. (2017). Post no photos, leave no trace: Children's digital footprint management strategies. *E-Learning and Digital Media*, 14(5), 275–290. <https://doi.org/10.1177/2042753017751711>
- Buitrago-Roperro, M. E., Ramírez-Montoya, M. S., & Laverde, A. C. (2020). Digital footprints (2005–2019): A systematic mapping of studies in education. *Interactive Learning*

*Environments*. Advance online publication.

<https://doi.org/10.1080/10494820.2020.1814821>

- Camacho, M., Minelli, J., & Grosseck, G. (2012). Self and identity: Raising undergraduate students' awareness on their digital footprints. *Procedia - Social and Behavioral Sciences*, 46, 3176-3181. <https://doi.org/10.1016/j.sbspro.2012.06.032>
- Canberk, G., & Sađırođlu, Ő. (2007). Çocukların ve gençlerin bilgisayar ve internet güvenliđi. *Politeknik Dergisi*, 10(1), 33-39.
- Çelen, K., Seferođlu, S. S., & Çelik, A. (2011). Yükseköđretimde çevrim-içi öğrenme: Sistemde yaşanan sorunlar ve çözüm önerileri. *Journal of European Education*, 1(1), 25-34.
- Çubukçu, A., & Bayzan, Ő. (2013). Türkiye'de dijital vatandaşlık algısı ve bu algıyı internetin bilinçli, güvenli ve etkin kullanımı ile artırma yöntemleri. *Middle Eastern & African Journal of Educational Research*, 5, 148-174.
- Dönmez, G. (2019). *Lise öğrencilerinin bilgi güvenliđi farkındalıđı ile dijital okuryazarlıđı arasındaki iliŐkinin incelenmesi*. YayınlanmamıŐ yüksek lisans tezi, Hacettepe Üniversitesi Eğitim Bilimleri Enstitüsü, Ankara.
- EAVI (2019). *Digital footprint awareness*. <https://www.surveymonkey.com/r/CFXJHK3>
- eTwinning (2016). Dijital vatandaşlık. eTwinning yoluyla aktif vatandaşlıđın geliŐtirilmesi. [https://www.etwinning.net/eun-files/book2016/TR\\_eTwinningBook.pdf](https://www.etwinning.net/eun-files/book2016/TR_eTwinningBook.pdf)
- Field, A. (2000). *Discovering statistics using SPSS for Windows*. London – Thousand Oaks – New Delhi: Sage Publications.
- Keser, H., & Güldüren, C. (2015). Bilgi güvenliđi farkındalık ölçeđi (BGFÖ) geliŐtirme çalışması. *Kastamonu Eğitim Dergisi*, 23(3), 1167-1184.
- Koidl, K., Reijers, W., Farrell, M., & Hoover, M. (2018). The BigFoot Initiative: An investigation of digital footprint awareness in social media. *SMSociety '18: Proceedings of the 9th*



*International Conference on Social Media and Society*, pp. 120-127.

<https://doi.org/10.1145/3217804.3217904>

Kuh Karyeli, G., & Dağhan, G. (2020). Sayısal ayak izi ders tasarımının öğrencilerin sayısal vatandaşlık konusundaki akademik başarılarına etkisi. *Erzincan Üniversitesi Eğitim Fakültesi Dergisi*, 22(1), 256-275. <https://doi.org/10.17556/erziefd.622919>

Malhotra, A., Totti, L., Meira, W., Kumaraguru, P., & Almeida, V. (2012). Studying user footprints in different online social networks. *Proceedings of the 2012 International Conference on Advances in Social Networks Analysis and Mining (ASONAM 2012)*, pp. 1065-1070. <https://doi.org/10.1109/ASONAM.2012.184>

MEB (2020). *Bilişim Teknolojileri ve Yazılım dersi öğretim programı*. <http://mufredat.meb.gov.tr/Dosyalar/2018124103559587-Bili%C5%9Fim%20Teknolojileri%20ve%20Yaz%C4%B1%C4%B1m%205-6.%20S%C4%B1n%C4%B1flar.pdf>

Mitnick, K. (2002). *The art of deception*. Hoboken, NJ: John Wiley & Sons.

O'Keeffe, G. S., Clarke-Pearson, K., & Council on Communications and Media. (2011). The impact of social media on children, adolescents, and families. *Pediatrics*, 127(4), 800-804. <https://doi.org/10.1542/peds.2011-0054>

Özcan, B. (2009). *Kurumsal bilgi güvenliği ve COBIT*. Yayımlanmamış yüksek lisans tezi, Haliç Üniversitesi Fen Bilimleri Enstitüsü, İstanbul.

Özdamar, K. (2004). *Paket programlar ile istatistiksel veri analizi - 2 (Çok değişkenli analizler)*. Kaan Kitabevi.

Puhakainen, P. (2006). *A design theory for information security awareness*. Master's thesis, Acta University of Oulu, Faculty of Science Department of Information Processing Science, Oulu. <http://jultika.oulu.fi/files/isbn9514281144.pdf>

- Ramachandran, V. (2016). *You are less anonymous on the web than you think - much less*.  
<https://engineering.stanford.edu/magazine/article/you-are-lessanonymous-web-you-think-much-less>
- Ribble, M. (2011). *Digital citizenship in schools* (2<sup>nd</sup> Ed.). International Society for Technology in Education (ISTE).
- Siponen, M. T. (2001). Five dimensions of information security awareness. *ACM SIGCAS Computers and Society*, 31(2), 24-29. <https://doi.org/10.1145/503345.503348>
- Sürmelioglu, Y., & Seferoglu, S. S. (2019). An examination of digital footprint awareness and digital experiences of higher education students. *World Journal on Educational Technology*, 11(1), 48-64.
- Şahinaslan, E., Kantürk, A., Şahinaslan, Ö., & Borandağ, E. (2009). Kurumlarda bilgi güvenliği farkındalığı, önemi ve oluşturma yöntemleri. *Akademik Bilişim 2009 - XI. Akademik Bilişim Konferansı Bildirileri*, (ss. 597-602), Şanlıurfa.
- Şeker, H., & Gençdoğan, B. (2006). *Psikolojide ve eğitimde ölçme aracı geliştirme*. Ankara: Nobel Yayın Dağıtım.
- Tatlidil, H. (2002). *Uygulamalı çok değişkenli istatistiksel analiz*. Ankara: Ziraat Matbaacılık.
- Thompson, T. L. (2012). I'm deleting as fast as I can: Negotiating learning practices in cyberspace. *Pedagogy, Culture & Society*, 20(1), 93-112.  
<https://doi.org/10.1080/14681366.2012.649417>
- Turgut, M. F., & Baykul, Y. (1992). *Ölçekleme teknikleri*. ÖSYM Yayınları: Ankara.
- TÜİK (2021). *Çocuklarda Bilişim Teknolojileri Kullanım Araştırması, 2021*.  
<https://data.tuik.gov.tr/Bulten/Index?p=Cocuklarda-Bilisim-Teknolojileri-Kullanim-Arastirmasi-2021-41132>
- Tozzi, A., & Coppola G. (2020). A European survey to analyse EU citizens' understanding of digital footprint. *European Digital Learning Network*.

- Vardal, N. (2009). *Yükseköğretimde bilgi güvenliği: Bilgi güvenlik yönetim sistemi için bir model önerisi ve uygulaması*. Yayımlanmamış doktora tezi, Gazi Üniversitesi Eğitim Bilimleri Enstitüsü, Ankara.
- Vervier, L., Zeissig, E. M., Lidynia, C., & Ziefle, M. (2017). Perceptions of digital footprints and the value of privacy. *In Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security - IoTBDS*, pp. 80-91. <https://doi.org/10.5220/0006301000800091>
- Vural, Y., & Sağıroğlu, Ş. (2011). Kurumsal bilgi güvenliğinde güvenlik testleri ve öneriler. *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi*, 26(1), 89-103.
- We Are Social. (2020). *Digital 2020: 3.8 billion people use social media*. <https://wearesocial.com/uk/blog/2020/01/digital-2020-3-8-billion-people-use-social-media/>
- Wook, T. S. M. T., Mohammed, H., Noor, S. F. M., Muda, Z., & Zairon, I. Y. (2019). Awareness of digital footprint management in the new media amongst youth. *Malaysian Journal of Communication*, 35(3), 407-421. <https://doi.org/10.17576/JKMJC-2019-3503-24>
- Yurdugül, H. (2005). Ölçek geliştirme çalışmalarında kapsam geçerliği için kapsam geçerlik indekslerinin kullanılması. *XIV. Ulusal Eğitim Bilimleri Kongresi, Pamukkale Üniversitesi Eğitim Fakültesi, 28–30 Eylül 2005, Denizli*.
- Yılmaz Soylu, M., Demiröz, S., & Akkoyunlu, B. (2021). Ortaokul öğrencilerinin dijital ayak izi farkındalıkları ve yaşantılarının incelenmesi. *Journal of Computer and Education Research*, 9(17), 177-198. <https://doi.org/10.18009/jcer.838856>
- Yang, H., & Chen, P. (2010). Exploring teachers' beliefs about digital citizenship and responsibility. In K. Elleithy, T. Sobh, M. Iskander, V. Kapila, M. A. Karim, & A. Mahmood (Eds.). *Technological Developments in Networking, Education and Automation*, 49-54. [https://doi.org/10.1007/978-90-481-9151-2\\_9](https://doi.org/10.1007/978-90-481-9151-2_9)

## EK-A: Ortaöğretim Öğrencilerine Yönelik Dijital Ayak İzi Farkındalık Ölçeği

Sevgili Öğrenciler, Bu ölçek Hacettepe Üniversitesi'nde yürütülen yüksek lisans tez çalışması için veri toplamak amacıyla hazırlanmıştır. Ölçeğin amacı, Dijital Ayak izi Farkındalık Ölçeğinin Geliştirilmesi ve Bilgi Güvenliği Farkındalığı ile İlişkisinin İncelenmesidir. Ölçekteki sorulara vereceğiniz yanıtlar bu çalışmanın başarılı sonuçlara ulaşmasında önemlidir. Vereceğiniz yanıtlar yalnızca araştırma amacıyla kullanılacak ve başkalarıyla paylaşılmayacaktır. Ölçeğin doldurulmasında gönüllülük esas alınmaktadır.

Yardıminız ve katılımınız için şimdiden teşekkür ederiz.

### Kişisel Bilgiler (Siz ve Aileniz):

1-Cinsiyetiniz	Kadın	Erkek				
2-Sınıfınız	9.sınıf	10.sınıf	11.sınıf	12.sınıf		
3-Yaşınız	13-20 arası açılır liste					
4-Anninizin eğitim durumu	Yok	İlkokul	Ortaokul	Ortaöğretim	Üniversite	Lisansüstü
5-Babanızın eğitim durumu	Yok	İlkokul	Ortaokul	Ortaöğretim	Üniversite	Lisansüstü

### Sosyal Medya, İnternete Erişim ve Kullanma Durumu:

1-Kullanabileceğiniz aktif bir internet bağlantınız var mı?	Evet	Hayır			
2-Sosya Medya hesabına (Facebook, Instagram, Twitter) sahip misiniz?	Evet	Hayır			
3-Eğer var ise günde kaç saat aktif kullanıyorsunuz?	Kullanmıyorum	1-3 saat	4-6 saat	7-9 saat	10+ saat
4-İnterneti günlük ortalama kullanma süreniz nedir?	Kullanmıyorum	1-3 saat	4-6 saat	7-9 saat	10+ saat
5-Aşağıdaki donanımlardan hangisine / hangilerine sahipsiniz?	Bilgisayar	Tablet	Telefon	Diğer	

Maddeler	1: Kesinlikle Katılmıyorum 5: Kesinlikle Katılıyorum				
<b>Kişisel Veri Paylaşımı</b>					
<b>Farkındalık</b>					
1. İnternet ortamındaki paylaştığım kişisel bilgilerimin kontrolüm dışında yabancı kişiler ile paylaşılabilceğini bilirim.	1	2	3	4	5
2. İnternet ortamdaki her hareketimin sayısal kimliğimin bir parçasını oluşturduğunu bilirim.	1	2	3	4	5
3. İnternet ortamındaki her hareketimin kayıt altına alındığını bilirim.	1	2	3	4	5
4. İnternet ortamında bıraktığım izlerin farklı sektörlerde veri olarak kullanılabilceğinin farkındayım.	1	2	3	4	5
5. İnternet ortamında yaptığım her paylaşımın gelecekte karşıma çıkabileceğinin farkındayım.	1	2	3	4	5
6. Ziyaret ettiğim web sitelerinin, yaklaşık konumumu tanımlayan IP adresimi kaydettiğinin farkındayım.	1	2	3	4	5
7. İnternet kafe, ortak kullanımlı bilgisayar laboratuvarları vb. ortamlarda bilgilerimin/ paylaşımlarımın başkalarının eline geçme ihtimali olduğunu düşünürüm.	1	2	3	4	5
8. İnternet ortamında ücretsiz hizmet veren sitelerin bir amacının da kullanıcı deneyimleri kapsamında kişisel verileri toplamak olduğunu farkındayım.	1	2	3	4	5
9. İnternet ortamda gezinirken karşıma çıkan reklamlara tıklamamam gerektiğinin farkındayım.	1	2	3	4	5
10. İnternet ortamlarında oynadığım oyunların, izlediğim video, film ve dizilerin, okuduğum haberlerin reklam algoritmaları için veri kaynağı olduğunu bilirim.	1	2	3	4	5
<b>Uygulama</b>					
1. İnternet ortamında fotoğraflarımı paylaşmaktan çekinmem.	1	2	3	4	5
2. İnternet ortamında kullandığım şifrelerim için "Beni Hatırla" özelliğini kullanırım.	1	2	3	4	5
3. İnternet üzerinde karşıma çıkan ve onaylamak zorunda olduğum kullanıcı sözleşmelerini okurum.	1	2	3	4	5
4. İnternette kimlik bilgilerimi paylaşmamaya dikkat ederim.	1	2	3	4	5
5. Arama motorlarına adımları yazıp hakkımda çıkan bilgileri kontrol ederim.	1	2	3	4	5
6. Ortak kullanım alanlarında kullanıcı adı ve şifre bilgisiyle giriş yaptığım uygulamalardan, bilgisayardan kalkmadan önce çıkış yaparım.	1	2	3	4	5

7. Ortak kullanım alanlarında (kafeler, kütüphaneler gibi) şifresiz kablosuz ağ (Wi-Fi) bağlantılarına katılmam.	1	2	3	4	5
8. İnternet ortamında kullandığım şifrelerin güçlü (büyük/küçük harf, özel karakter, rakam içermesi gibi) olmasına özen gösteririm.	1	2	3	4	5
9. Mail adresime gelen mailerin içerisindeki linklerin güvenliğinden emin olmadan tıklamam.	1	2	3	4	5
10. İnternet ortamında kullanmak zorunda olduğum uygulamalara yeterli düzeyde bilgi veririm.	1	2	3	4	5
11. İnternet ortamında yaptığım herkese açık paylaşımlar, gerçek düşüncelerimi yansıtmaktadır.	1	2	3	4	5
12. İnternet sitelerinde, mikrofon kullanımına izin ver, kamera kullanımına izin ver, konum paylaşmaya izin ver gibi izin taleplerine dikkat eder, yalnızca gerekli gördüklerimi onaylarım.	1	2	3	4	5
<b>Sosyal Medya Kullanımı</b>					
<b>Farkındalık</b>					
1. Sosyal medya ortamlarında paylaştığım, yorum yaptığım veya beğendiğim paylaşımları silsem bile tamamen yok olmadığını bilirim.	1	2	3	4	5
2. Sosyal medya ortamlarında paylaştığım fotoğrafların, yaptığım beğenilerin karakterim, özel yaşantım, kültürel ve sosyal hayatım hakkında fikir oluşturduğunun farkındayım.	1	2	3	4	5
3. Paylaştığım gönderilerin yalnızca benim izin verdiğim kişiler tarafından görüntülenmediğinin farkındayım.	1	2	3	4	5
4. Sosyal medyada paylaştığım fotoğraf, video ve yorumların kontrolüm dışında kullanılabileceğinin farkındayım.	1	2	3	4	5
5. Sosyal medyada yaptığım her türlü işlemin kayıt altına alındığını bilirim.	1	2	3	4	5
6. Sosyal medyada kişiler arası sohbetlerin gizli kalmayabileceğinin farkındayım.	1	2	3	4	5
<b>Uygulama</b>					
1. Kullandığım sosyal medya araçlarının gizlilik ayarlarını sürekli gözden geçirip düzenlerim.	1	2	3	4	5
2. Sosyal medya platformlarında profilimde paylaştığım her gönderiyi herkese açık bir şekilde paylaşıyorum.	1	2	3	4	5
3. Sosyal medyada yazdıklarımı üslup ve içerik açısından kontrol ederek paylaşıyorum.	1	2	3	4	5
4. Sosyal medya hesaplarımda profil resmi kullanırım.	1	2	3	4	5

## EK-B: Ortaöğretim Öğrencilerine Yönelik Bilgi Güvenliği Farkındalık Ölçeği Kullanım İzni

BGFÖ Kullanım İzni ve Ölçek Maddeleri H.k. Gelen Kutusu X



**Eda Sanin**

Alıcı:

24 Eyl 2020 Per 21:41



Sayın hocalarım,

Ankara Üniversitesi Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü mezunuyum ve Hacettepe Üniversitesi Eğitim Bilimleri Enstitüsü Bilgisayar ve Öğretim Teknolojileri Eğitimi A.B.D. yüksek lisans öğrencisiyim. Tezimi Gökhan DAĞHAN hocamla çalışıyorum. Tezim kapsamında, ortaöğretim öğrencilerine yönelik geliştirmiş olduğunuz "Bilgi Güvenliği Farkındalık Ölçeği"ni (BGFÖ)" kullanmak istiyoruz. Bu nedenle hem kullanım izninize, hem de ölçek maddelerine ihtiyaç duyuyoruz.

Eğer sizler için de bir mahsuru yoksa kullanım izninizi alabilir miyim? Ölçek maddelerini makalede göremediğim için maddeleri de gönderebilirseniz çok sevinirim hocalarım.

En derin saygılarımla.

Eda SANİN



**Hafize Keser**

Alıcı: ben

30 Eyl 2020 15:42



Edacığım,

Ortaöğretim öğrencileri için geliştirdiğimiz Bilgi Güvenliği Farkındalık Ölçeğini tez çalışmada tabii ki kullanabilirsin. Ölçeği ve puanlamaya ilişkin ayrıntılı bilgiyi size Can GÜLDÜREN hoca gönderecektir. Araştırmanın sonuçlarını bizimle paylaşmanızı bekleriz. Başarılar dilerim.

Prof. Dr. Hafize Keser



**CAN GULDÜREN**

Alıcı: ben

25 Eyl 2020 Cum 11:21



Eda merhaba,

İstemiş olduğun ölçek maddelerini ekteki dosyada bulabilirsin.

Tasarladığınız çalışmada ilgili ölçeği kullanabilirsiniz. Çalışma sonuçlarınızı paylaşırsanız sevinirim.

**Ölçek Açıklamaları:**

Ölçek 14-18 yaş arası Lise (K12) öğrencileri üzerinde geliştirilmiştir. Ölçekte ters kodlanmış madde yoktur. Ölçek toplam puanı ve alt faktörlere ilişkin puanlar attıkça, katılımcıların Bilgi Güvenliği Farkındalığı artmaktadır.

**Bilgi Güvenliği Ölçek Faktör Yapısı:** Kişisel Verilerin Korunması: 1-6, Saldırı ve Tehditler: 7- 25, Mahremiyet: 26-36

Kolay gelsin.

İyi çalışmalar.

Can GÜLDÜREN

Dr. Öğr. Üyesi

Bilgisayar Teknolojileri Bölümü

Ufuk Üniversitesi

### EK-C: Ortaöğretim Öğrencilerine Yönelik Bilgi Güvenliği Farkındalık Ölçeği

	Kesinlikle katılmıyorum	Katılmıyorum	Kısmen katılmıyorum	Katılıyorum	Kesinlikle katılıyorum
Aşağıda bilgi güvenliği farkındalığına yönelik görüşlerinizi tanımlayan 36 madde bulunmaktadır. Aşağıdaki ifadelere ne derece katılıp-katılmadığınızı seçeneğin altındaki kutuya (X) işareti koyarak belirtiniz. Lütfen her soruyu dikkatli okuyunuz ve boş madde bırakmayınız.					
1. Bilgi güvenliğinin ne anlama geldiğini biliyorum.	1	2	3	4	5
2. Bilgi güvenliği ile ilgili sorumluluklarımın ne olduğunu biliyorum.	1	2	3	4	5
3. Kullandığım bilgi sistemlerinde tanımlanmış olan kuralları nasıl uygulayacağımı biliyorum.	1	2	3	4	5
4. Yönetim tarafından bilgi güvenliği gereksinimleri ile ilgili yeterince bilgilendirildiğimi düşünüyorum.	1	2	3	4	5
5. Çocukların bilgisayar güvenli kullanmaları için yapılması gerekenleri biliyorum.	1	2	3	4	5
6. Kişisel verilerimi nasıl korumam gerektiğini biliyorum	1	2	3	4	5
7. Aldatmaca (hoax) nedir biliyorum.	1	2	3	4	5
8. Zincir e-postalara (chain e-mail) karşı nasıl hareket etmem gerektiğini biliyorum.	1	2	3	4	5
9. Casus yazılım (spyware) nedir biliyorum.	1	2	3	4	5
10. Bilgisayarımda casus yazılım olup olmadığını anlayabilirim.	1	2	3	4	5
11. Bilgisayarıma casus yazılım yüklenmesinin engelleme yöntemlerini biliyorum.	1	2	3	4	5
12. Kimlik hırsızlığı (identity theft) nedir biliyorum.	1	2	3	4	5
13. Kimlik hırsızlığına karşı alınması gereken güvenlik tedbirlerini biliyorum.	1	2	3	4	5
14. Sahte virüs koruma yazılımının ne olduğunu biliyorum.	1	2	3	4	5
15. Hizmet aksatma (Denial of Service - DoS) saldırısı nedir biliyorum.	1	2	3	4	5
16. Kimlik avı (phishing) saldırısı nedir biliyorum.	1	2	3	4	5
17. Sosyal mühendislik (social engineering) saldırısı nedir biliyorum.	1	2	3	4	5
18. Sosyal mühendislik saldırısına uğramamak için nasıl hareket etmem gerektiğini biliyorum.	1	2	3	4	5
19. Siber zorbalık (cyberbullying) nedir biliyorum.	1	2	3	4	5
20. Siber zorbalığa karşı kendimi nasıl koruyacağımı biliyorum.	1	2	3	4	5
21. Siber zorbalığa karşı çocukları nasıl koruyacağımı biliyorum.	1	2	3	4	5
22. Dijital imza (digital signature) nedir biliyorum.	1	2	3	4	5
23. Web sayfalarında kullanılan çerezlerin (cookies) ne işe yaradığını biliyorum.	1	2	3	4	5
24. Web Sitesi sertifikasının (web site certificate) ne işe yaradığını biliyorum.	1	2	3	4	5
25. Son kullanıcı lisans sözleşmesi (end-user license agreement) nedir biliyorum.	1	2	3	4	5
26. Şüpheli veya bilinmeyen kaynaklardan gelen özellikle eklentisi olan e-postaları açmanın taşıdığı riski biliyorum.	1	2	3	4	5



27.	Sosyal ağ sitelerini (social networking sites) güvenli olarak nasıl kullanacağımı biliyorum.	1	2	3	4	5
28.	USB sürücülerini (USB drives) kullanırken dikkat edilmesi gereken hususları biliyorum.	1	2	3	4	5
29.	Taşınabilir cihazlara (portable devices) yönelik fiziksel güvenliği sağlamak ile ilgili dikkat edilmesi gereken konuları biliyorum.	1	2	3	4	5
30.	Taşınabilir cihazlara yönelik veri güvenliği ile ilgili dikkat edilmesi gereken konuları biliyorum.	1	2	3	4	5
31.	Kişisel mahremiyet nedir biliyorum.	1	2	3	4	5
32.	Bilgi güvenliği konusunda yasal sorumluluklarımı biliyorum.	1	2	3	4	5
33.	İnternette gezinirken mahremiyetimi korumak için alınması gereken tedbirleri biliyorum.	1	2	3	4	5
34.	İnternette gezinirken hakkımda toplanan bilgi miktarının nasıl sınırlandırılacağını biliyorum.	1	2	3	4	5
35.	Şifre kullanımına ilave olarak alınması gereken tedbirlerin neler olduğunu biliyorum.	1	2	3	4	5
36.	Çevrimiçi güvenli alışveriş yapmak için gerekli olan güvenlik tedbirlerini biliyorum.	1	2	3	4	5

#### Ölçek Açıklamaları:

Ölçek 14-18 yaş arası Lise (K12) öğrencileri üzerinde geliştirilmiştir. Ölçekte ters kodlanmış madde yoktur. Ölçek toplam puanı ve alt faktörlere ilişkin puanlar attıkça, katılımcıların Bilgi Güvenliği Farkındalığı artmaktadır.

**Bilgi Güvenliği Ölçek Faktör Yapısı:** Kişisel Verilerin Korunması: 1-6, Saldırı ve Tehditler: 7- 25, Mahremiyet: 26-36

#### İletişim:

Prof. Dr. Hafize KESER

Dr. Can GÜLDÜREN

Dr. Levent ÇETİNKAYA

**EK-Ç: Etik Komisyonu Onay Bildirimi\***

T.C.  
HACETTEPE ÜNİVERSİTESİ REKTÖRLÜĞÜ  
Rektörlük

Tarih: 18/01/2021  
Sayı: E-35853172-300-00001402950  
  
0001402950

Sayı : E-35853172-300-00001402950  
Konu : Eda SANİN Hk. (Etik Komisyon İzni)

18.01.2021

**EĞİTİM BİLİMLERİ ENSTİTÜSÜ MÜDÜRLÜĞÜNE**

İlgi : 24.12.2020 tarihli ve E-51944218-300-00001374021 sayılı yazı.

Enstitünüz Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı yüksek lisans programı öğrencilerinden Eda SANİN'in Doç. Dr. Gökhan DAĞHAN danışmanlığında yürüttüğü "Dijital Ayakizi Farkındalık Ölçeğinin Geliştirilmesi ve Bilgi Güvenliği Farkındalığı ile İlişkisinin İncelenmesi" başlıklı tez çalışması, Üniversitemiz Senatosu Etik Komisyonunun 12 Ocak 2021 tarihinde yapmış olduğu toplantıda incelenmiş olup, etik açıdan uygun bulunmuştur.

Bilgilerinizi ve gereğini saygılarımla rica ederim.

Prof. Dr. Vural GÖKMEN  
Rektör Yardımcısı

**Bu belge güvenli elektronik imza ile imzalanmıştır.**

Belge Doğrulama Kodu: 881CFEAE-9788-437B-84D4-59E80382D0D9

Belge Doğrulama Adresi: <https://www.turkiye.gov.tr/hu-ebys>

Adres: Hacettepe Üniversitesi Rektörlük 06100 Sıhhiye-Ankara

Bilgi için: Duygu Didem İLERİ

E-posta: yazim@hacettepe.edu.tr İnternet Adresi: [www.hacettepe.edu.tr](http://www.hacettepe.edu.tr) Elektronik

Memur

Ağ: [www.hacettepe.edu.tr](http://www.hacettepe.edu.tr)

Telefon: 0 (312) 305 3001-3002 Faks: 0 (312) 311 9992

Telefon: .

Kep: [hacettepeuniversitesi@hs01.kep.tr](mailto:hacettepeuniversitesi@hs01.kep.tr)



\* Tez başlığı ile alınan etik kurul onayındaki başlığın farklılığı, 21.01.2022 tarihinde yapılan Yüksek Lisans Tez Savunma Sınavı jürisinin önerisi ve Eğitim Bilimleri Enstitüsü Yönetim Kurulu'nun 01.02.2022 tarih ve 05 sayılı oturumunda almış olduğu 2022-05/68 sayılı tez başlığı değişikliği onayından kaynaklanmaktadır.

**EK-D: Etik Beyanı**

Hacettepe Üniversitesi Eğitim Bilimleri Enstitüsü, tez yazım kurallarına uygun olarak hazırladığım bu tez çalışmasında,

- \* tez içindeki bütün bilgi ve belgeleri akademik kurallar çerçevesinde elde ettiğimi,
- \* görsel, işitsel ve yazılı bütün bilgi ve sonuçları bilimsel ahlak kurallarına uygun olarak sunduğumu,
- \* başkalarının eserlerinden yararlanılması durumunda ilgili eserlere bilimsel normlara uygun olarak atıfta bulunduğumu,
- \* atıfta bulunduğum eserlerin bütününe kaynak olarak gösterdiğimi,
- \* kullanılan verilerde herhangi bir tahrifat yapmadığımı,
- \* bu tezin herhangi bir bölümünü bu üniversitede veya başka bir üniversitede başka bir tez çalışması olarak sunmadığımı

beyan ederim.

14/03/2022

Eda SANİN

**EK-E: Yüksek Lisans Tez Çalışması Orijinallik Raporu**

14/03/2022

HACETTEPE ÜNİVERSİTESİ

Eğitim Bilimleri Enstitüsü

Bilgisayar ve Öğretim Teknolojileri Eğitimi Ana Bilim Dalı Başkanlığına,

Tez Başlığı: Ortaöğretim Öğrencilerinin Dijital Ayak İzi Farkındalıkları Ve Bilgi Güvenliği Farkındalıkları Arasındaki İlişkinin İncelenmesi

Yukarıda başlığı verilen tez çalışmamın tamamı (kapak sayfası, özetler, ana bölümler, kaynakça) aşağıdaki filtreler kullanılarak **Turnitin** adlı intihal programı aracılığı ile kontrol edilmiştir. Kontrol sonucunda aşağıdaki veriler elde edilmiştir:

Rapor Tarihi	Sayfa Sayısı	Karakter Sayısı	Savunma Tarihi	Benzerlik Oranı	Gönderim Numarası
14/03/2022	74	110097	21/01/2022	%25	1783912441

Uygulanan filtreler:

1. Kaynaklar hariç
2. Alıntılar dâhil
3. 5 kelimedenden daha az örtüşme içeren metin kısımları hariç

Hacettepe Üniversitesi Eğitim Bilimleri Enstitüsü Tez Çalışması Orijinallik Raporu Alınması ve Kullanılması Uygulama Esasları'nı inceledim ve çalışmamın herhangi bir intihal içermediğini; aksinin tespit edileceği muhtemel durumda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi ve yukarıda vermiş olduğum bilgilerin doğru olduğunu beyan eder, gereğini saygılarımla arz ederim.

**Ad Soyadı:** Eda SANİN

**Öğrenci No.:** N18139549

**Ana Bilim Dalı:** Bilgisayar ve Öğretim Teknolojileri Eğitimi

**Programı:** Bilgisayar ve Öğretim Teknolojileri Eğitimi

**Statüsü:**  Y.Lisans  Doktora  Bütünleşik Dr.

**DANIŞMAN ONAYI**

UYGUNDUR.

Doç. Dr. Gökhan DAĞHAN

## EK-F: Thesis Originality Report

14/03/2022

HACETTEPE UNIVERSITY  
Graduate School of Educational Sciences  
To The Department of Computer Education and Instructional Technology

Thesis Title: Examining the Relationship Between High School Students' Digital Footprint Awareness and Information Security Awareness

The whole thesis that includes the *title page, introduction, main chapters, conclusions and bibliography section* is checked by using **Turnitin** plagiarism detection software take into the consideration requested filtering options. According to the originality report obtained data are as below.

Time Submitted	Page Count	Character Count	Date of Thesis Defense	Similarity Index	Submission ID
14/03/2022	74	110097	21/01/2022	%25	1783912441

Filtering options applied:

1. Bibliography excluded
2. Quotes included
3. Match size up to 5 words excluded

I declare that I have carefully read Hacettepe University Graduate School of Educational Sciences Guidelines for Obtaining and Using Thesis Originality Reports; that according to the maximum similarity index values specified in the Guidelines, my thesis does not include any form of plagiarism; that in any future detection of possible infringement of the regulations I accept all legal responsibility; and that all the information I have provided is correct to the best of my knowledge.

I respectfully submit this for approval.

**Name Lastname:** Eda SANIN  
**Student No.:** N18139549  
**Department:** Computer Education and Instructional Technology  
**Program:** Computer Education and Instructional Technology  
**Status:**  Masters     Ph.D.     Integrated Ph.D.

### ADVISOR APPROVAL

APPROVED  
Assoc. Prof. Dr. Gökhan DAĞHAN

## EK-G: Yayınlama ve Fikrî Mülkiyet Hakları Beyanı

Enstitü tarafından onaylanan lisansüstü tezimin/raporumun tamamını veya herhangi bir kısmını, basılı (kâğıt) ve elektronik formatta arşivleme ve aşağıda verilen koşullarla kullanıma açma iznini Hacettepe Üniversitesine verdiğimi bildiririm. Bu izinle Üniversiteye verilen kullanım hakları dışındaki tüm fikri mülkiyet haklarım bende kalacak, tezimin tamamının ya da bir bölümünün gelecekteki çalışmalarda (makale, kitap, lisans ve patent vb.) kullanım hakları bana ait olacaktır.

Tezin kendi orijinal çalışmam olduğunu, başkalarının haklarını ihlal etmediğimi ve tezimin tek yetkili sahibi olduğumu beyan ve taahhüt ederim. Tezimde yer alan telif hakkı bulunan ve sahiplerinden yazılı izin alınarak kullanılması zorunlu metinlerin yazılı izin alınarak kullandığımı ve istenildiğinde suretlerini Üniversiteye teslim etmeyi taahhüt ederim.

Yükseköğretim Kurulu tarafından yayınlanan "**Lisansüstü Tezlerin Elektronik Ortamda Toplanması, Düzenlenmesi ve Erişime Açılmasına İlişkin Yönerge**" kapsamında tezim aşağıda belirtilen koşullar haricince YÖK Ulusal Tez Merkezi / H.Ü. Kütüphaneleri Açık Erişim Sisteminde erişime açılır.

- Enstitü/Fakülte yönetim kurulu kararı ile tezimin erişime açılması mezuniyet tarihinden itibaren 2 yıl ertelenmiştir. <sup>(1)</sup>
- Enstitü/Fakülte yönetim kurulunun gerekçeli kararı ile tezimin erişime açılması mezuniyet tarihinden itibaren ... ay ertelenmiştir. <sup>(2)</sup>
- Tezimle ilgili gizlilik kararı verilmiştir. <sup>(3)</sup>

14/03/2022

Eda SANİN

---

"Lisansüstü Tezlerin Elektronik Ortamda Toplanması, Düzenlenmesi ve Erişime Açılmasına İlişkin Yönerge"

- (1) Madde 6. 1. Lisansüstü teze ilgili patent başvurusu yapılması veya patent alma sürecinin devam etmesi durumunda, tez danışmanının önerisi ve enstitü anabilim dalının uygun görüşü üzerine enstitü veya fakülte yönetim kurulu iki yıl süre ile tezinerişime açılmasının ertelenmesine karar verebilir.
- (2) Madde 6.2. Yeni teknik, materyal ve metotların kullanıldığı, henüz makaleye dönüşmemiş veya patent gibi yöntemlerle korunmamış ve internette paylaşılması durumunda 3 şahıslara veya kurumlara haksız kazanç; imkânı oluşturabilecek bilgi ve bulguları içeren tezler hakkında tez danışmanının önerisi ve enstitü anabilim dalının uygun görüşü üzerine enstitü veya fakülte yönetim kurulunun gerekçeli kararı ile altı ayı aşmamak üzere tezin erişime açılması engellenebilir.
- (3) Madde 7. 1. Ulusal çıkarları veya güvenliği ilgilendiren, emniyet, istihbarat, savunma ve güvenlik, sağlık vb. konulara ilişkin lisansüstü tezlerle ilgili gizlilik kararı, tezin yapıldığı kurum tarafından verilir\*. Kurum ve kuruluşlarla yapılan işbirliği protokolü çerçevesinde hazırlanan lisansüstü tezlere ilişkin gizlilik kararı ise, ilgili kurum ve kuruluşun önerisi ile enstitü veya fakültenin uygun görüşü üzerine üniversite yönetim kurulu tarafından verilir. Gizlilik kararı verilen tezler Yükseköğretim Kuruluna bildirilir.  
Madde 7.2. Gizlilik kararı verilen tezler gizlilik süresince enstitü veya fakülte tarafından gizlilik kuralları çerçevesinde muhafaza edilir, gizlilik kararının kaldırılması halinde Tez Otomasyon Sistemine yüklenir  
\*Tez danışmanının önerisi ve enstitü anabilim dalının uygun görüşü üzerine enstitü veya fakülte yönetim kurulu tarafından karar verilir.

