

T.C.
BALIKESİR ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
BİLGİSAYAR VE ÖĞRETİM TEKNOLOJİLERİ EĞİTİMİ
ANABİLİM DALI



ÖĞRETMENLERİN TEKNOLOJİ YETERLİĞİ ÖZ-
DEĞERLENDİRMELERİ VE DİJİTAL VERİ GÜVENLİĞİ
FARKINDALIKLARI

ÖZNUR UZUNOĞLU

YÜKSEK LİSANS TEZİ

Jüri Üyeleri : **Doç. Dr. Gülcan ÖZTÜRK (Tez Danışmanı)**

Doç. Dr. Ayşen KARAMETE

Dr. Öğr. Üyesi Hüseyin Can ŞENEL

BALIKESİR, TEMMUZ - 2026

ETİK BEYAN

Balıkesir Üniversitesi Fen Bilimleri Enstitüsü Tez Yazım Kurallarına uygun olarak tarafımda hazırlanan “**Öğretmenlerin Teknoloji Yeterliği Öz-Değerlendirmeleri ve Dijital Veri Güvenliği Farkındalıkları**” başlıklı tezde,

- Tüm bilgi ve belgeleri akademik kurallar çerçevesinde elde ettiğimi,
- Kullanılan veriler ve sonuçlarda herhangi bir değişiklik yapmadığımı,
- Tüm bilgi ve sonuçları bilimsel araştırma ve etik ilkelere uygun şekilde sunduğumu,
- Yararlandığım eserlere atıfta bulunarak kaynak gösterdiğimi,

beyan eder, aksinin ortaya çıkması durumunda her türlü yasal sonucu kabul ederim.

Öznur UZUNOĞLU

ÖZET

ÖĞRETMENLERİN TEKNOLOJİ YETERLİĞİ ÖZ-DEĞERLENDİRMELERİ VE DİJİTAL VERİ GÜVENLİĞİ FARKINDALIKLARI

YÜKSEK LİSANS TEZİ

ÖZNUR UZUNOĞLU

BALIKESİR ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ
BİLGİSAYAR VE ÖĞRETİM TEKNOLOJİLERİ EĞİTİMİ ANABİLİM DALI

(TEZ DANIŞMANI: DOÇ. DR. GÜLCAN ÖZTÜRK)

BALIKESİR, TEMMUZ - 2026

Bu araştırmanın amacı, öğretmenlerin teknoloji yeterliği öz-değerlendirmeleri ile dijital veri güvenliği farkındalıkları arasındaki ilişkiyi incelemektir. Keşfedici korelasyonel araştırma modelinde tasarlanan çalışmanın örneklemini devlet okullarında görev yapan 307 öğretmen oluşturmaktadır. Araştırma verileri, kişisel bilgi formu, “21. Yüzyıl Öğrenmeleri için Teknoloji Yeterliği Öz-Değerlendirme Ölçeği” ve “Dijital Veri Güvenliği Farkındalık Ölçeği” kullanılarak toplanmıştır. Verilerin analizinde betimsel istatistikler, bağımsız gruplar t-testi, tek yönlü varyans analizi ve Pearson korelasyon katsayısı kullanılmıştır. Araştırma sonucunda, öğretmenlerin teknoloji yeterliği öz-değerlendirmelerinin ve dijital veri güvenliği farkındalıklarının yüksek düzeyde olduğu bulunmuştur. Öğretmenlerin teknoloji yeterliği öz-değerlendirmeleri, cinsiyet, görev türü, eğitim düzeyi, bilgisayar sahipliği, dijital güvenlikle ilgili ders/kurs alma ve 21. yüzyıl becerileri kavramını bilme durumu değişkenlerine göre anlamlı farklılık gösterirken mesleki kıdem değişkenine göre anlamlı bir farklılık göstermemiştir. Öğretmenlerin dijital veri güvenliği farkındalıkları cinsiyet, dijital güvenlikle ilgili ders/kurs alma durumu ve 21. yüzyıl becerileri kavramını bilme durumu değişkenlerine göre anlamlı biçimde farklılaştığı; görev türü, eğitim düzeyi, mesleki kıdem ve bilgisayar sahipliği durumuna göre anlamlı bir farklılık göstermediği bulunmuştur. Öğretmenlerin teknoloji yeterliği öz-değerlendirmeleri ile dijital veri güvenliği farkındalıkları arasında pozitif yönde, güçlü düzeyde anlamlı bir ilişki olduğu belirlenmiştir. Elde edilen bulgular doğrultusunda, öğretmenlerin 21. yüzyıl becerilerini eğitim ortamlarına güvenli bir şekilde entegre edebilmeleri için siber güvenlik ve teknoloji odaklı hizmet içi eğitim programlarının yaygınlaştırılması önerilmektedir.

ANAHTAR KELİMELELER: Dijital veri güvenliği farkındalığı, teknoloji yeterliği öz-değerlendirmesi, 21. yüzyıl öğrenmesi

ABSTRACT

TEACHERS' TECHNOLOGY PROFICIENCY SELF-ASSESSMENTS AND DIGITAL DATA SECURITY AWARENESS

MSC THESIS

ÖZNUR UZUNOĞLU

**BALIKESİR UNIVERSITY INSTITUTE OF SCIENCE
COMPUTER EDUCATION AND INSTRUCTIONAL TECHNOLOGY**

(SUPERVISOR: ASSOC. PROF. DR. GÜLCAN ÖZTÜRK)

BALIKESİR, JULY - 2026

This study aimed to investigate relationship between teachers' technology proficiency self-assessments and digital data security awareness. Sample of the study, which was designed in exploratory correlational research model consisted of 307 teachers working in public schools. Research data were collected using a personal information form, the "Technology Competence Self-Assessment Scale for 21st-Century Learning" and the "Digital Data Security Awareness Scale". Descriptive statistics, independent groups t-test, one-way analysis of variance, and Pearson correlation coefficient were used for analysis of the data. As a result of research, it was found that teachers' technology proficiency self-assessments and digital data security awareness were at a high level. Teachers' technology proficiency self-assessments demonstrated significant differences based on gender, occupational position, educational level, computer ownership, participation in digital security related courses, and familiarity with concept of 21st-century skills; but, no significant difference was found based on professional work experience. It was found that teachers' digital data security awareness differed significantly according to gender, participation in digital security-related courses, and familiarity with concept of 21st-century skills; but there were no significant differences based on occupational position, educational level, professional work experience, and computer ownership. A strong, positive, and statistically significant relationship was identified between teachers' technology proficiency self-assessments and digital data security awareness. Based on these findings, it was recommended that cybersecurity and technology-focused in-service training programs be expanded to enable teachers to safely integrate 21st-century skills into their educational environments.

KEYWORDS: Digital data security awareness, technology proficiency self-assessments, 21st century learning

İÇİNDEKİLER

	<u>Sayfa</u>
ÖZET	i
ABSTRACT	ii
İÇİNDEKİLER.....	iii
ŞEKİL LİSTESİ	v
TABLO LİSTESİ.....	vi
KISALTMA VE SEMBOL LİSTESİ	vii
ÖNSÖZ VE TEŞEKKÜR	ix
1. GİRİŞ.....	1
1.1 Teknoloji ve Dijitalleşme	3
1.2 Dijital Teknolojilerin Eğitime Entegrasyonu	5
1.3 Teknoloji Yeterliği Öz-Değerlendirmesi	14
1.4 Dijital Veri ve Dijital Veri Güvenliği.....	16
1.5 Dijital Veri Güvenliği Farkındalığı	24
1.6 Problem Durumu	33
1.7 Araştırmanın Problemleri	35
1.8 Araştırmanın Amacı	35
1.9 Araştırmanın Önemi	35
1.10 Araştırmanın Sınırlılıkları	36
1.11 Araştırmanın Sayıtları	36
1.12 Tanımlar	37
2. ALANYAZIN İNCELEMESİ	38
2.1 Teknoloji Yeterliği Öz-Değerlendirmesi ile İlgili Alanyazın.....	38
2.2 Dijital Veri Güvenliği Farkındalığı ile İlgili Alanyazın	43
3. YÖNTEM	48
3.1 Araştırmanın Modeli	48
3.2 Örneklem	48
3.3 Veri Toplama Araçları.....	50
3.3.1 Kişisel bilgi formu	50
3.3.2 21. yüzyıl öğrenmeleri için teknoloji yeterliği öz-değerlendirme ölçeği (YYÖTYÖ).....	50
3.3.3 Dijital veri güvenliği farkındalığı ölçeği (DVGFO).....	51
3.4 Verilerin Analizi	51
3.5 Verilerin Geçerliliği ve Güvenirliği.....	53
3.6 Etik Hususlar	53
4. BULGULAR	55
4.1 Birinci Probleme Ait Bulgular	55
4.1.1 YYÖTYÖ'den elde edilen bulgular	55
4.1.2 DVGFO'den elde edilen bulgular.....	56
4.2 İkinci Probleme Ait Bulgular	58
4.2.1 YYÖTYÖ puanlarının çeşitli değişkenlere göre incelenmesi	58
4.2.2 DVGFO puanlarının çeşitli değişkenlere göre incelenmesi	62
4.3 Üçüncü Probleme Ait Bulgular	65
5. SONUÇ, TARTIŞMA VE ÖNERİLER.....	67
5.1 Araştırmanın Sonuçları.....	67
5.2 Tartışma	68
5.2.1 Birinci probleme ilişkin tartışma	68
5.2.2 İkinci probleme ilişkin tartışma	69
5.2.3. Üçüncü probleme ilişkin tartışma.....	72

İÇİNDEKİLER (devam)

5.3 Öneriler.....	73
5.3.1 Uygulamaya yönelik öneriler	73
5.3.2 İleride yapılacak araştırmalara yönelik öneriler	75
6. KAYNAKLAR.....	77
EKLER.....	95
ÖZGEÇMİŞ.....	103

ŞEKİL LİSTESİ

Sayfa

Şekil 1.1: Dijital teknolojilerin eğitime entegrasyonu	9
Şekil 1.2: Güvenlik üçgeni.....	23

TABLO LİSTESİ

Sayfa

Tablo 3.1: Katılımcıların kişisel özelliklerine göre dağılımı.....	49
Tablo 3.2: Grup bazında çarpıklık ve basıklık değerleri	51
Tablo 4.1: YYÖTYÖ'ye ilişkin betimsel istatistikler.....	55
Tablo 4.2: DVGFÖ'ye ilişkin betimsel istatistikler.....	56
Tablo 4.3: YYÖTYÖ puanlarının cinsiyete göre t-testi sonuçları.....	58
Tablo 4.4: YYÖTYÖ puanlarının görev türüne göre t-testi sonuçları	59
Tablo 4.5: YYÖTYÖ puanlarının eğitim düzeyine göre t-testi sonuçları	59
Tablo 4.6: YYÖTYÖ puanlarının mesleki kıdeme göre ANOVA sonuçları	60
Tablo 4.7: YYÖTYÖ puanlarının bilgisayar sahipliği durumuna göre t-testi sonuçları	60
Tablo 4.8: YYÖTYÖ puanlarının dijital güvenlikle ilgili ders/kurs alma durumuna göre t-testi sonuçları	61
Tablo 4.9: YYÖTYÖ puanlarının 21. yüzyıl becerileri kavramını bilme durumuna göre t-testi sonuçları	61
Tablo 4.10: DVGFÖ puanlarının cinsiyete göre t-testi sonuçları.....	62
Tablo 4.11: DVGFÖ puanlarının görev türüne göre t-testi sonuçları.....	62
Tablo 4.12: DVGFÖ puanlarının eğitim düzeyine göre t-testi sonuçları	63
Tablo 4.13: DVGFÖ puanlarının mesleki kıdeme göre ANOVA sonuçları	63
Tablo 4.14: DVGFÖ puanlarının bilgisayar sahipliği durumuna göre t-testi sonuçları	64
Tablo 4.15: DVGFÖ puanlarının dijital güvenlikle ilgili ders/kurs alma durumuna göre t-testi sonuçları	64
Tablo 4.16: DVGFÖ puanlarının 21. yüzyıl becerileri kavramını bilme durumuna göre t-testi sonuçları	65
Tablo 4.17: YYÖTYÖ ve boyutları ile DVGFÖ arasındaki pearson korelasyon analizi sonuçları.....	65

KISALTMA VE SEMBOL LİSTESİ

AECT	: Association for Educational Communications and Technology (Eğitim İletişim ve Teknoloji Derneği)
AB	: Avrupa Birliği
AR	: Augmented Reality (Artırılmış Gerçeklik)
BİT	: Bilgi ve İletişim Teknolojileri
BT	: Bilişim Teknolojileri
BTK	: Bilgi Teknolojileri ve İletişim Kurumu
DDoS	: Distibuted Denial of Service (Dağıtılmış Hizmet Reddi)
DVGfÖ	: Dijital Veri Güvenliği Farkındalık Ölçeği
EBA	: Eğitim Bilişim Ağı
FATİH	: Fırsatları Artırma ve Teknolojiyi İyileştirme Hareketi
GDPR	: General Data Protection Regulation (Genel Veri Koruma Yönetmeliği)
ICT CFT	: Information and Communication Technology Competency Framework for Teachers (Öğretmenlere Yönelik Bilgi İletişim Teknolojisi Yetkinlikleri Çerçevesi)
IoT	: Internet of Things (Nesnelerin İnterneti)
ISO	: International Organization for Standardization
ISTE	: International Society for Technology in Education (Uluslararası Eğitimde Teknoloji Topluluğu)
iTEC	: Innovative Technologies for an Engaging Classroom (Bağlayıcı Sınıf İçin Yenilikçi Teknolojiler)
KVKK	: Kişisel Verilerin Korunması Kanunu
LMS	: Learning Management System (Öğrenme Yönetim Sistemi)
MEB	: Millî Eğitim Bakanlığı
MEBBİS	: Millî Eğitim Bakanlığı Bilişim Sistemleri
MEGP	: Milli Eğitimi Geliştirme Projesi
MLO	: Müfredat Laboratuvar Okulu
NAEP	: National Assessment of Educational Progress (Ulusal Eğitim İlerleme Değerlendirmesi)
NARA	: National Archives and Records Administration (Ulusal Arşivler ve Kayıtlar İdaresi)
NCES	: National Center for Education Statistics (Ulusal Eğitim İstatistikleri Merkezi)
NETS	: National Educational Technology Standards (Ulusal Eğitim Teknolojisi Standartları)
NETS-A	: National Educational Technology Standards for Administrators (Yöneticiler için Ulusal Eğitim Teknolojisi Standartları)
NETS-S	: National Educational Technology Standards for Students (Öğrenciler için Ulusal Eğitim Teknolojisi Standartları)
NETS-T	: National Educational Technology Standards for Teachers (Öğretmenler için Ulusal Eğitim Teknolojisi Standartları)
NIST	: National Institute of Standards and Technology (Ulusal Standartlar ve Teknoloji Enstitüsü)
OECD	: Organisation for Economic Co-operation and Development (Ekonomik İşbirliği ve Kalkınma Örgütü)
ÖBA	: Öğretmen Bilişim Ağı
ÖYGGM	: Öğretmen Yetiştirme ve Geliştirme Genel Müdürlüğü

KISALTMA VE SEMBOL LİSTESİ (devam)

ÖSYM	: Ölçme, Seçme ve Yerleştirme Merkezi
P21	: Partnership for 21st Century Skills (21. Yüzyıl Becerileri Ortaklığı)
SPSS	: Statistical Package for the Social Sciences (Sosyal Bilimler için İstatistik Paketi)
STEM	: Science, Technology, Engineering and Mathematics (Fen, Teknoloji, Mühendislik ve Matematik)
STM ThinkTech	: Savunma Teknolojileri Mühendislik Teknolojik Düşünce Merkezi
TEDP	: Temel Eğitime Destek Programı
TPAB	: Teknolojik Pedagojik Alan Bilgisi
TPSA	: Technology Proficiency Self-Assessment (Teknoloji Yeterliği Öz-Değerlendirme Ölçeği)
TPSA C-21	: Technology Proficiency Self-Assessment for 21st Century Learning (21. Yüzyıl Öğrenmeleri için Teknoloji Yeterliği Öz-Değerlendirme Ölçeği)
TÜBİSAD	: Türkiye Bilişim Sanayicileri Derneği
TÜİK	: Türkiye İstatistik Kurumu
UNCTAD	: United Nations Conference on Trade and Development (Birleşmiş Milletler Ticaret ve Kalkınma Konferansı)
UNESCO	: United Nations Educational, Scientific and Cultural Organization (Birleşmiş Milletler Eğitim, Bilim ve Kültür Örgütü)
USOM	: Ulusal Siber Olaylara Müdahale Merkezi
VR	: Virtual Reality (Sanal Gerçeklik)
WWW	: World Wide Web (Küresel Ağ)
YÖK	: Yükseköğretim Kurulu
YEĞİTEK	: Yenilik ve Eğitim Teknolojileri Genel Müdürlüğü
YYÖTYÖ	: 21. Yüzyıl Öğrenmeleri için Teknoloji Yeterliği Öz-Değerlendirme Ölçeği
N	: Katılımcı sayısı
$\bar{x}$	: Ortalama
S	: Standart sapma
R	: Pearson korelasyon katsayısı
η^2	: Eta kare (Etki büyüklüğünü belirtmek amacıyla kullanılmıştır)
p	: Anlamlılık düzeyi

ÖNSÖZ VE TEŞEKKÜR

Bu çalışmada, öğretmenlerin teknoloji yeterliği öz-değerlendirmeleri ile dijital veri güvenliği farkındalıkları arasındaki ilişki araştırılmıştır.

Bu uzun ve emek gerektiren araştırma sürecinde; engin bilgi, birikim ve tecrübeleriyle bana yol gösteren, her aşamada sabırla beni yönlendiren ve kıymetli desteklerini hiçbir zaman esirgemeyen saygıdeğer tez danışmanım Doç. Dr. Gülcan ÖZTÜRK'e en derin şükranlarımı sunarım. Tez savunmamda jüri üyesi olarak çalışmama katkı sağlayan ve değerli zamanlarını ayıran Doç. Dr. Ayşen KARAMETE ve Dr. Öğr. Üyesi Hüseyin Can ŞENEL'e kıymetli değerlendirmeleri için teşekkür ederim. Eğitim hayatım boyunca değerli katkılarıyla ufkumu açan ve vizyon katan kıymetli hocalarıma teşekkürü bir borç bilirim. Araştırmamın veri toplama sürecinde değerli vakitlerini ayırarak ölçekleri içtenlikle yanıtlayan ve çalışmama gönüllü olarak katkı sağlayan tüm meslektaşlarıma teşekkür ederim.

Son olarak; hayatımın her döneminde olduğu gibi bu yoğun ve yorucu tez sürecinde de sonsuz sabır, sevgi ve anlayışlarıyla beni daima destekleyen, her an yanımda hissettiğim kıymetli aileme, özellikle de oğluma sonsuz sevgi ve teşekkürlerimi sunarım.

Balıkesir, 2026

Öznur UZUNOĞLU

1. GİRİŞ

21. yüzyıl bilgi ve iletişim teknolojilerinin tüm toplumsal alanlara hızla yayıldığı, bilginin üretim ve tüketim dinamiklerinin köklü biçimde dönüştüğü ve dijitalleşmenin kaçınılmaz bir gerçekliğe dönüştüğü bir çağı temsil etmektedir. Bu çağın en belirgin özelliklerinden biri, bireylerin yalnızca bilgiye erişim becerisine sahip olmasının artık yeterli görülmemesi, bilgiyi anlamlandırma, eleştirel bir süzgeçten geçirme, üretken biçimde kullanma ve paylaşma kapasitelerinin de vazgeçilmez yetkinlikler olarak öne çıkmasıdır. Nitekim 21. Yüzyıl Becerileri Ortaklığı (Partnership for 21st Century Skills [P21]) (2017), Ekonomik İşbirliği ve Kalkınma Örgütü (Organisation for Economic Co-operation and Development [OECD]) (2018) ve Uluslararası Eğitimde Teknoloji Topluluğu (International Society for Technology in Education [ISTE]) (2016) gibi uluslararası kuruluşların hazırladığı raporlar incelendiğinde, dijital okuryazarlık ve teknoloji yetkinliklerinin 21. yüzyıl bireyinin taşıması gereken temel beceriler arasında yer aldığı görülmektedir. Bu bağlamda eğitim sistemleri de köklü bir dönüşüm baskısıyla karşı karşıya kalmakta hem içerik hem de süreç boyutunda yeniden yapılanma kaçınılmaz bir zorunluluk haline gelmektedir.

Eğitim sistemlerinin bu dönüşümde en önemli rolü üstlenen paydaşı hiç kuşkusuz öğretmenlerdir. Teknolojinin eğitime entegrasyon sürecinde öğretmenlerin hem uygulayıcı hem de yönlendirici konumunda bulunması, onların teknoloji yeterliklerini belirleyici bir değişken olarak öne çıkarmaktadır. Seferoğlu (2009), eğitim sistemlerinin niteliğini doğrudan belirleyen en önemli unsurun öğretmenlerin mesleki yeterlikleri olduğunu vurgularken Ertmer and Ottenbreit-Leftwich (2010) öğretmenlerin teknolojiyi sınıf içinde etkin biçimde kullanabilmelerinin mesleki gelişimlerinin ayrılmaz bir boyutu haline geldiğini belirtmektedir. Bu doğrultuda Christensen and Knezek (2017) tarafından geliştirilen Teknoloji Yeterliği Öz-Değerlendirme Ölçeği (Technology Proficiency Self-Assessment for 21st Century Learning [TPSA C-21]) ve Türkiye koşullarına uyarlanan haliyle 21. Yüzyıl Öğrenmeleri için Teknoloji Yeterliği Öz-Değerlendirme Ölçeği (YYÖTYÖ), öğretmenlerin 21. yüzyıl öğrenmelerindeki teknoloji yeterlik düzeylerini kendi algıları üzerinden ortaya koymaya imkân tanıyan geçerli ve güvenilir bir araç olarak alanyazındaki yerini almıştır (Fidan vd., 2020).

Öte yandan dijitalleşmenin derinleşmesiyle birlikte bireylerin yalnızca teknolojiyi kullanmayı değil, onu güvenli, etik ve bilinçli biçimde kullanmayı da öğrenmesi zorunlu

hale gelmiştir. Dijital ortamlarda üretilen, saklanan ve paylaşılan veri miktarındaki çarpıcı artış kimlik hırsızlığı, kimlik avı saldırıları, zararlı yazılımlar ve veri sızıntısı gibi tehditlerin gündelik yaşamın ayrılmaz bir parçası haline gelmesine zemin hazırlamıştır (Canbek ve Sağıroğlu, 2007a, 2007b). Birleşmiş Milletler, OECD ve Avrupa Birliği (AB) başta olmak üzere pek çok uluslararası kuruluş, dijital veri güvenliği farkındalığını bireylerin 21. yüzyılda taşıması gereken temel yetkinlikler arasında saymaktadır. Bu bağlamda öğretmenlerin dijital veri güvenliği farkındalığı yalnızca bireysel bir mesele olarak değil kurumsal güvenlik, öğrenci mahremiyeti ve dijital vatandaşlık eğitimi açısından da stratejik bir öneme sahip bir konu olarak değerlendirilmelidir.

Alanyazın incelendiğinde, öğretmenlerin teknoloji yeterliklerini çeşitli değişkenler açısından ele alan çok sayıda çalışma bulunmaktadır (Dursun ve Saracaloğlu, 2017; Güney ve Mete, 2022; Hacıömeroğlu vd., 2014; Saykal ve Uluçınar-Sağır, 2021; Schmidt et al, 2009). Bununla birlikte teknoloji yeterliği öz-değerlendirmeleri ile dijital veri güvenliği farkındalığını bir arada inceleyen ve bu iki değişken arasındaki ilişkiyi ortaya koymayı hedefleyen araştırmaların son derece sınırlı olduğu dikkat çekmektedir. Bu eksiklik, özellikle eğitim ortamlarının giderek daha fazla dijitalleştiği günümüzde önemli bir araştırma boşluğuna işaret etmektedir. Öğretmenlerin teknoloji yeterliği öz-değerlendirmeleri ile dijital veri güvenliği farkındalıklarının birlikte değerlendirilmesi hem karar vericilere hem de hizmet içi eğitim programcılarına önemli veriler sunabilecektir. Tüm bu gerekçelerden hareketle bu araştırmanın yapılmasına karar verilmiştir.

Bu çalışmada, devlet okullarında görev yapan öğretmenlerin teknoloji yeterliği öz-değerlendirme düzeyleri ile dijital veri güvenliği farkındalık düzeylerinin incelenmesi amaçlanmaktadır. Araştırmada ayrıca öğretmenlerin söz konusu iki değişkene ilişkin düzeylerinin çeşitli demografik değişkenlere göre anlamlı farklılık gösterip göstermediği ve teknoloji yeterliği öz-değerlendirmeleri ile dijital veri güvenliği farkındalıkları arasında anlamlı bir ilişki bulunup bulunmadığı belirlenmiştir. Bu yönüyle araştırmanın, öğretmenlerin mesleki gelişim gereksinimlerinin belirlenmesine, hizmet içi eğitim programlarının yapılandırılmasına ve eğitimde güvenli teknoloji kullanımına ilişkin politika ve uygulamalara katkı sağlaması beklenmektedir.

1.1 Teknoloji ve Dijitalleşme

Teknoloji, insanlığın tarihsel gelişimiyle birlikte şekillenmiş; bilimsel bilginin insan yaşamının pratik amaçlarına uygulanması yoluyla araç, yöntem ve sistemler üretme süreci olarak gelişmiştir. Bu bağlamda teknoloji, insanın çevresini dönüştürmesine, yaşam koşullarını iyileştirmesine ve toplumsal yapıları yeniden düzenlemesine olanak sağlayan dinamik bir bilgi ve uygulama alanı olarak değerlendirilebilir (Encyclopaedia Britannica, 2026). Teknolojik değişimin insanlık tarihindeki büyük dönüşümler, devrimler ve toplumsal gelişmelerle yakından ilişkili olması, teknolojinin yalnızca teknik bir araç değil, aynı zamanda tarihsel ve toplumsal değişimin temel belirleyicilerinden biri olduğunu göstermektedir (Sætra, 2023). Teknoloji felsefesi, teknolojinin yalnızca araçsal yönünü değil, insan, toplum ve değerlerle ilişkisini de ele alan çok boyutlu bir çalışma alanıdır (Hansen, 2020). Hansen'e (2020) göre teknoloji felsefesi, teknolojinin insan yaşamı, toplumsal yapı ve düşünce sistemleri üzerindeki etkilerini anlamaya yönelik önemli bir kuramsal çerçeve sunmaktadır.

Bu tanımın, yalnızca teknoloji kullanıcıları için yeterli bir çerçeve sunduğunu, konuyu daha eleştirel bir gözle değerlendirenlerin bu yaklaşımı son derece yüzeysel bulacağını belirtmektedir. Modern toplumların dinamiklerini ve dönüşümlerini kavrayabilmek için filozoflar, tarihçiler, eğitimciler, siyasetçiler, sosyologlar, ekonomistler ve eleştirmenler bu konuya yoğun ilgi göstermiştir. Bu çok boyutlu inceleme süreci, teknoloji kavramının göstergebilimsel bir çerçevede ele alınmasına zemin hazırlamıştır. Schatzberg (2018)'e göre teknoloji sözcüğü günümüz kullanımında “endüstriyel sanat”, “uygulamalı bilim” ve “teknik” olmak üzere üç temel kategori altında sınıflandırılmaktadır.

Felsefi açıdan teknoloji kavramı, Yunan kültüründeki “techne” kavramıyla ilişkilendirilmekte ve “meydana getirme” ya da “açığa çıkarma” anlamlarıyla ele alınmaktadır. Günay (2017), “techne”, “aletheia” ve “discover” kavramları arasındaki ilişkiyi açıklayarak teknolojinin yalnızca araç üretme süreci değil, aynı zamanda var olanı görünür kılan bir “açığa çıkarma” biçimi olduğunu belirtmektedir. Bu yaklaşım, Heidegger'in teknolojiyi yalnızca araçsal bir etkinlik olarak değil, varlığın belirli bir biçimde açığa çıkmasıyla ilişkili felsefi bir sorun olarak ele alan görüşleriyle de ilişkilendirilmektedir (Günay, 2017). Günay'a (2017) göre teknolojik bir ürünün ortaya çıkışı, Aristoteles'in varlığın dört nedeni olarak ifade edilen maddi, formal, ereksel ve fail nedenleriyle açıklanabilir; çünkü bir ürün, tasarımın malzemeye birleşmesi ve insan etkinliği aracılığıyla

somut bir varlık hâline gelmesi sonucunda meydana gelir. Teknoloji kavramı, yalnızca teknik araçlarla sınırlı olmayıp bilim, insan yaşamı, eğitim ve toplumsal dönüşümle de yakından ilişkilidir. Bu bağlamda teknoloji, insanın yaşam koşullarını dönüştüren, düşünme biçimlerini etkileyen ve eğitim kurumlarının içinde bulunulan çağa uyum sağlamasında belirleyici rol oynayan dinamik bir kavram olarak değerlendirilebilir (Parmaksız, 2023).

Teknoloji, yalnızca araç ve makinelerden oluşan teknik bir alan değil; bilgi, beceri, emek, organizasyon ve toplumsal ilişkilerle birlikte işleyen çok katmanlı bir olgu olarak ele alınabilir. İnsanların bilgi ve becerilerini üretim süreçleriyle bütünleştiren teknoloji, hayatı kolaylaştırmanın yanı sıra yeni meslek alanlarının ortaya çıkmasına, değerlerin ve kültürel yapıların dönüşmesine de katkıda bulunmaktadır. Bu nedenle teknoloji, bilim, insan yaşamı, kültür ve toplumsal dönüşümle iç içe geçmiş dinamik bir yapı olarak ele alınabilir.

Dijital teknoloji, verilerin sayısal biçimde üretilmesi, işlenmesi, saklanması ve ağlar aracılığıyla aktarılmasına dayanan; bilgisayarlar, mobil cihazlar, yazılım uygulamaları, bulut bilişim, yapay zekâ, büyük veri analitiği, nesnelerin interneti ve yeni nesil bağlantı altyapıları gibi birbirini tamamlayan bileşenlerden oluşan dinamik bir ekosistem olarak değerlendirilmektedir. OECD'ye (2024) göre dijital teknoloji ekosistemi, bilgi ve iletişim teknolojileri sektörünün yanı sıra yapay zekâ, büyük veri, bulut bilişim, 5G ve sürükleyici teknolojiler gibi alanlar aracılığıyla ekonomik ve toplumsal dönüşümü hızlandırmaktadır. Benzer biçimde Birleşmiş Milletler Ticaret ve Kalkınma Konferansı (United Nations Conference on Trade and Development [UNCTAD]) (2024), dijitalleşmenin yalnızca ekonomik büyüme ve bilgiye erişim açısından değil; veri merkezleri, cihaz üretimi, enerji tüketimi, elektronik atık ve sürdürülebilirlik gibi çevresel etkiler bakımından da ele alınması gerektiğini vurgulamaktadır. Dijital teknolojilerin tarihsel temelleri Boole cebiri, Turing'in hesaplanabilirlik kuramı ve von Neumann'ın saklı program mimarisi gibi kurucu çalışmalara dayanmakta; günümüzde bu birikim yapay zekâ, veri analitiği, bulut sistemleri ve bağlantılı cihazlarla daha bütünleşik, akıllı ve ağ temelli bir yapıya dönüşmektedir (Boole, 1854/2005; Turing, 1937; Von-Neumann, 1945/1993). Bu nedenle dijital teknoloji, yalnızca donanım ve yazılım araçlarından oluşan teknik bir yapı değil; bireylerin iletişim, öğrenme, üretim ve toplumsal yaşama katılım biçimlerini dönüştüren çok boyutlu bir sistem olarak ele alınmalıdır (OECD, 2024; UNCTAD, 2024).

1.2 Dijital Teknolojilerin Eğitime Entegrasyonu

Dijital dönüşüm, kurumların dijital teknolojilerden yararlanarak iş süreçlerini, örgütsel yapılarını, değer üretme biçimlerini ve stratejik yönelimlerini yeniden düzenledikleri kapsamlı bir değişim sürecidir (Baslyman, 2022; Vial, 2019). Bu süreç, yalnızca teknolojik araçların kuruma dâhil edilmesiyle sınırlı olmayıp, aynı zamanda kurumsal strateji, operasyonel işleyiş, hizmet sunumu ve kullanıcı deneyimi üzerinde önemli dönüşümler meydana getirmektedir (Baslyman, 2022; Verhoef et al., 2021). Dijital bir yol haritası izlemek, organizasyonların geleneksel iş süreçlerini yeniden yapılandırmasına ve rekabetçi koşullara uyum sağlamasına katkı sunmaktadır (Bughin et al., 2017; Garcia-Ortega et al., 2021). Bununla birlikte dijital dönüşüm, her kurum ve sektör için aynı biçimde gerçekleşmeyen; kurumsal kapasite, sektör yapısı, liderlik anlayışı ve dijital olgunluk düzeyine göre farklılaşan çok boyutlu bir süreçtir (Verhoef et al., 2021; Vial, 2019). Bu süreçte başarılı sonuçlara ulaşılabilmesi için güçlü liderlik, açık bir vizyon, üst yönetim desteği ve değişime uyum sağlayabilecek bir örgüt kültürü gerekli görülmektedir (Garcia-Ortega et al., 2021; Kotter, 2012). Alanyazında dijital dönüşümün kamu, endüstri, sağlık, iletişim ve eğitim gibi birçok alanda giderek zorunlu hâle geldiği vurgulanmakta; bu dönüşümün, dijitalleştirme ve dijitalleşme aşamalarını kapsayan daha geniş bir kurumsal değişim süreci olduğu belirtilmektedir (Verhoef et al., 2021; Vial, 2019).

Dijital dönüşüm, eğitimde yalnızca basılı materyallerin dijital ortama aktarılması değil; öğretim, ölçme-değerlendirme ve iletişim süreçlerinin dijital teknolojilerle yeniden düzenlenmesi anlamına gelmektedir (OECD, 2023; Birleşmiş Milletler Eğitim, Bilim ve Kültür Örgütü [United Nations Educational, Scientific and Cultural Organization (UNESCO)], 2023). Bu süreçte dijital platformlar, öğrenci bilgi sistemleri ve çevrim içi öğrenme ortamları eğitim süreçlerini daha erişilebilir ve düzenli hâle getirmektedir (OECD, 2023). Ancak dijital dönüşümün etkili olabilmesi için teknolojinin pedagojik amaçlara uygun kullanılması ve öğrencilerin dijital ortamlarda bilinçli hareket etmeleri önemlidir (UNESCO, 2023). Öztürk (2021), öğrencilerin dijital araçları yoğun biçimde kullanmaları nedeniyle dijital vatandaşlık becerilerinin geliştirilmesi gerektiğini vurgulamaktadır.

Dijitalleştirme, analog formattaki bilgilerin, görsellerin ya da ses kayıtlarının elektronik sistemler tarafından depolanıp işlenebilir ve iletilebilir dijital formatlara aktarılması sürecini ifade etmektedir (Brennen and Kreiss, 2016; UNESCO, 2003). Bu dönüşüm, fiziksel ya da analog verilerin dijital temsillerinin oluşturulmasını kapsamakta; bilgiye erişimi, paylaşımı

ve düzenlenmesini kolaylaştırmaktadır (Ulusal Arşivler ve Kayıtlar İdaresi [National Archives and Records Administration (NARA)], 2023; UNESCO, 2003).

Dijitalleştirme, kurumların operasyonlarını modernize etmelerini, verimliliklerini artırmalarını ve bilgiye her platformdan erişilebilirliği iyileştirmelerini sağlayan kapsamlı dijital dönüşümün temel bir adımı olarak kabul edilmektedir (Garcia-Ortega et al., 2021). Bu süreçte geleneksel sistemler dijital sistemlere dönüştürülmekte, bilgi teknolojisi altyapısı güncellenmekte, veri tabanları standartlaştırılmakta ve kâğıt belgeler dijital ortamlara aktarılmaktadır. Brennen and Kreiss'e (2016) göre dijitalleştirme teknik bir süreç iken dijitalleşme, dijital teknolojilerin toplumsal ve kültürel bağlamda nasıl bütünleştiğini açıklayan sosyo-kültürel bir dönüşümü simgelemektedir. Yoo et al. (2010) dijitalleştirmeyi, dijital teknolojilerin iş süreçlerini dönüştürme ve veri temelli yeni iş modelleri oluşturma kapasitesi çerçevesinde ele almaktadır. Tilson et al. (2010) ise dijitalleştirme sürecini, iş süreçlerinin, organizasyonel yapının ve sektörel dinamiklerin dijital teknoloji aracılığıyla yeniden biçimlendirilmesi olarak tanımlamakta ve veri analitiğiyle dijital platformların artan rolünü vurgulamaktadır. Eğitim bağlamında dijitalleştirme, basılı ders materyallerinin, sınav kâğıtlarının veya not kayıtlarının dijital platformlara aktarılması biçiminde somutlaşmaktadır (OECD, 2023; Redecker, 2017; UNESCO Institute for Statistics, 2018). Bu süreç, öğretim materyallerinin dijital kaynaklara dönüştürülmesini, ölçme-değerlendirme uygulamalarının teknoloji destekli yürütülmesini ve eğitimsel verilerin daha erişilebilir, düzenlenebilir ve paylaşılabılır hâle getirilmesini kapsamaktadır (OECD, 2023; Redecker, 2023).

Dijitalleşme, dijitalleştirmeyi izleyen daha ileri bir aşama olarak değerlendirilmektedir. Ham ya da basılı dokümanların dijital platforma aktarılması “dijitalleştirme” olarak tanımlanırken, bu verilerin farklı platformlarda kullanılabilir, işlenebilir ve paylaşılabılır hâle gelmesi “dijitalleşme” kavramıyla ifade edilmektedir (Brennen and Kreiss, 2016; Verhoef et al., 2021). Brennen and Kreiss (2016), dijitalleştirmeyi analog bilgi akışlarının dijital bitlere dönüştürülmesi; dijitalleşmeyi ise toplumsal ve kurumsal süreçlerin dijital iletişim ve medya altyapıları etrafında yeniden yapılandırılması olarak açıklamaktadır. Dijital dönüşüm, dijital teknolojilerin sektörler ve toplumsal işlevler genelinde yaygın biçimde benimsenmesiyle; işletmelerin çalışma biçimlerini, bireyler arası etkileşimleri ve hizmet sunum süreçlerini köklü biçimde değiştiren stratejik ve örgütsel bir dönüşüm süreci olarak değerlendirilmektedir (Rogers, 2016; Vial, 2019). Bankacılık, perakende, sağlık,

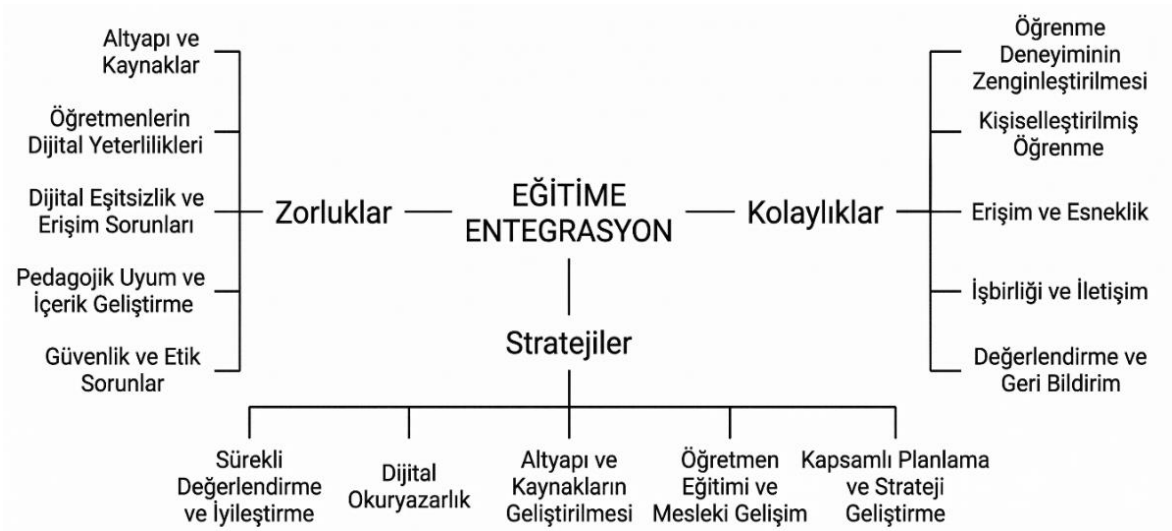
lojistik ve eğitim gibi alanlarda bulut bilişim, veri analitiği, yapay zekâ ve Nesnelerin İnterneti gibi teknolojilere dayalı yeni iş modelleri, dijital dönüşüm sürecinin somut örnekleri arasında yer almaktadır. (Le-Viet and Dang-Quoc, 2023; Rogers, 2016). Dijitalleşme aynı zamanda dijital ekonominin gelişimini desteklemekte; büyük veri ve veri analitiği aracılığıyla karar alma süreçlerini, iş modellerini ve kurumsal değer üretme biçimlerini dönüştürmektedir (Mayer-Schönberger and Cukier, 2013; McAfee and Brynjolfsson, 2017). Teknolojik değişimin ivmesi geleneksel iş döngülerini geride bıraktıkça, kurumların ve bireylerin dijital teknolojilere uyum sağlama kapasitesi daha önemli hâle gelmektedir (McAfee and Brynjolfsson, 2017; Verhoef et al., 2021).

Dijital dönüşüm ise dijitalleşmeden daha kapsamlı bir değişim sürecini ifade etmektedir. Bu süreç, dijital teknolojilerin yalnızca belirli iş süreçlerine uygulanmasıyla sınırlı olmayıp, kurumların stratejik yönelimlerini, örgütsel yapılarını, operasyonel süreçlerini ve değer üretme biçimlerini yeniden şekillendirmesini gerektirmektedir (Verhoef et al., 2021; Vial, 2019). Gartner'ın 2022 yılı stratejik teknoloji eğilimleri raporunda dijitalleşme; büyüme, verimlilik, veri odaklı yapılar, bulut yerel platformlar, karar zekâsı, hiperotomasyon ve siber güvenlik gibi alanlarla ilişkilendirilmektedir (Gartner, 2021). Dijital dönüşüm sayesinde kurumlar operasyonel verimliliklerini artırabilmekte, maliyetlerini azaltabilmekte, veri temelli karar alma mekanizmalarını güçlendirebilmekte ve rekabet avantajı elde edebilmektedir (Bughin et al., 2017; Le-Viet and Dang-Quoc, 2023). Bununla birlikte dijital dönüşümün başarısı yalnızca teknoloji yatırımlarına değil; liderlik, örgüt kültürü, insan kaynağı yetkinliği, değişime uyum kapasitesi ve uzun vadeli stratejik vizyon gibi unsurlara da bağlıdır (Verhoef et al., 2021; Vial, 2019).

Dijital dönüşüm; kurumların operasyonel verimliliklerini artırmalarına, müşteri deneyimini geliştirmelerine, yeni iş modelleri oluşturmalarına ve rekabet avantajı elde etmelerine katkı sağlayan stratejik bir süreçtir. Bunun yanında dijital dönüşüm, veri güvenliği, yasal uyumluluk ve çevresel sürdürülebilirlik gibi alanlarda da kurumlara önemli kazanımlar sunmaktadır (Katsamakas, 2022; Pascoe vd., 2024; Verhoef et al., 2021; Vial, 2019). Operasyonel verimliliği artırmak, manuel süreçlerin otomasyonu ve veri analitiğiyle sağlanan verimlilik artışları bu hedefin temelini oluşturmaktadır (Ross et al., 2016; Yıldız, 2018). Müşteri deneyimini iyileştirmek, dijital pazarlama stratejileri ve müşteri odaklı yaklaşımlarla kullanıcı beklentilerini daha iyi karşılamak hedeflenmektedir (Bulunmaz, 2016). Dijital dönüşümün önemli hedeflerinden biri, işletmelerin dijital teknolojiler

aracılığıyla yeni pazarlara girmesi, yenilikçi iş modelleri geliştirmesi ve yeni gelir kaynakları oluşturmaktır (Westerman et al., 2014). Rekabet avantajı sağlamak, dijital araçlar, işletmelerin pazar koşullarına hızlı uyum sağlamasını ve sürdürülebilir rekabet gücü elde etmesini desteklemektedir (Brynjolfsson and McAfee, 2014). Veri güvenliği ve uyumluluğu artırmak, dijital dönüşüm süreci veri güvenliği standartlarının güçlendirilmesini ve yasal gerekliliklere uyumu da kapsamaktadır (Davenport and Ronanki, 2018). Dijital dönüşüm verimlilik, inovasyon ve rekabet avantajı sağlamasına karşın çeşitli engellerle de karşı karşıyadır. Bjerke-Busch and Aspelund'e (2021) göre bu engeller sürecin her aşamasında ortaya çıkabilir ve başarılı bir dijital dönüşüm için stratejik bir yönetim anlayışının benimsenmesi kaçınılmazdır. Bu bağlamda dijital dönüşüm yalnızca işletmeler ve kurumsal yapılarla sınırlı kalmamakta; eğitim başta olmak üzere farklı toplumsal alanlarda da yapısal değişimleri beraberinde getirmektedir.

21. yüzyılın değişen ve hızla gelişen dinamikleri bağlamında dijital teknolojiler, diğer toplumsal alanlarda olduğu gibi eğitim alanında da kapsamlı ve yapısal dönüşümlere yol açmaktadır. Bu doğrultuda geleneksel öğretim yaklaşımları yeniden yapılandırılarak dijital araç ve ortamlarla bütünleştirilmiş; böylece öğrenme süreçlerinin daha etkileşimli, erişilebilir ve bireyselleştirilmiş bir nitelik kazandığı bir eğitim anlayışı ortaya çıkmıştır (Kocaman-Karoğlu vd., 2020; Yıldırım ve Keçeci, 2025). Dijital teknolojilerin yaygınlaşması, öğrenen profillerinde de önemli değişimlere neden olmuş ve yeni kuşakların bilgiye erişim, işleme ve öğrenme biçimlerini farklılaştırmıştır (Prensky, 2001). Bu durum, eğitim süreçlerinin yeniden düzenlenmesini gerektiren önemli bir dönüşüm alanı olarak değerlendirilmektedir. Dijital teknolojilerin eğitime entegrasyon süreci Şekil 1.1'de gösterilmiştir (Greenhow and Lewin, 2018, Hodges et al., 2020, Yuan and Powell, 2013).



Şekil 1.1: Dijital teknolojilerin eğitime entegrasyonu (Greenhow and Lewin, 2018; Hodges et al., 2020; Yuan and Powell, 2013)

Şekil 1.1, dijital teknolojilerin eğitime entegrasyon sürecini zorluklar, kolaylıklar ve stratejiler ekseninde bütüncül bir çerçevede ortaya koymaktadır. Bu süreç, öğrenme deneyimlerinin zenginleşmesi ve erişim olanaklarının artması gibi pedagojik kazanımlar sağlamakla birlikte (Greenhow and Lewin, 2018), altyapı ve dijital yeterliliklere bağlı sınırlılıkları da içermektedir (Hodges et al., 2020). Bununla birlikte çevrimiçi ve açık öğrenme uygulamalarının yaygınlaşması, erişim kapsamını genişletirken kurumsal dönüşüm gereksinimlerini de gündeme getirmektedir (Yuan and Powell, 2013). Bu bağlamda, entegrasyon sürecinin etkili bir şekilde yürütülebilmesi, stratejik planlama ve bütüncül bir yaklaşımın benimsenmesine bağlıdır.

Teknolojinin eğitim süreçleriyle bütünleşmesi yalnızca teknik donanımın sağlanmasıyla açıklanabilecek bir durum değildir. Bu sürecin başarıya ulaşabilmesi için örgütsel ve bireysel düzeyde çeşitli ön koşulların birlikte bulunması gerekmektedir. Mevcut uygulamalardan duyulan hoşnutsuzluk, sürece ayrılacak yeterli zaman, kaynaklara erişim, gerekli bilgi ve becerilere sahip olma, teşvik edici unsurların varlığı, paydaş katılımının sağlanması, güven veren bir destek yapısının oluşturulması ve etkili liderlik bu koşullar arasında sayılmaktadır (Ertmer and Ottenbreit-Leftwich, 2010). Söz konusu değişkenlerin bir araya gelmesi, BİT'in eğitim ortamlarına daha sağlam, etkili ve sürdürülebilir biçimde bütünleşmeyi mümkün kılmaktadır.

Dijital teknolojilerin eğitime entegrasyonu çeşitli çerçevelerden tanımlanmaktadır: Hew and Brush (2007), teknolojilerin eğitime entegrasyonunu eğitim teknolojisini, okul ortamlarında masaüstü, dizüstü ve el bilgisayarları başta olmak üzere yazılım ve internet gibi dijital araçların öğretimsel amaçlarla kullanılması olarak ele almaktadır. Usluel vd.'ne (2007) göre eğitime teknoloji entegrasyonu BİT'in öğretim hedeflerinin kazandırılmasında araç olarak işlev görmesidir. Ogle and Branch'a (2002) göre teknolojilerin eğitime entegrasyonu teknoloji kaynaklarının ve uygulamalarının günlük yaşama, iş hayatına ve okul yönetimine dahil edilmesidir. Kozloski'ye (2006) göre eğitime teknoloji entegrasyonu öğrenme sürecinde teknolojinin işlevsel bir araç olarak devreye sokulmasıdır. Griffin'e (2003) göre teknolojilerin eğitime entegrasyonu öğretim programının düzenlenmesi ve geliştirilmesinde eğitim teknolojisinin belirli hedeflere yönelik olarak kullanılmasıdır. Spazak'a (2013) göre eğitime teknoloji entegrasyonu öğrenme düzeyini artırmak, konuları daha etkin biçimde kavratmak ve üst düzey düşünme becerilerini güçlendirmek amacıyla teknolojinin araçsal biçimde kullanılmasıdır. Eğitime teknoloji entegrasyonu, öğretmenlerin teknolojik araçları derslerinde pedagojik amaçlara uygun biçimde kullanarak öğrenmeyi desteklemesi ve öğretim sürecinin etkililiğini artırması olarak tanımlanmaktadır (Kaya ve Yılayaz, 2013; Ulusal Eğitim İstatistikleri Merkezi [National Center for Education Statistics (NCES)], 2005). Bu nedenle öğretmenler teknolojik gelişmeleri yakından izlemeli ve öğretim süreçlerine uyarlamalıdır. BİT becerilerinin öğrencilere kazandırılmasında ve derslerde teknoloji entegrasyonunun sağlanmasında okullara ve öğretmenlere büyük sorumluluklar düşmektedir (Şad ve Nalçaçı, 2015).

Dijital gelişmelerin eğitim sistemlerine dahil edilmesinin yalnızca araçların öğrenme ortamlarına sokulmasından ibaret olmadığı görülmektedir, bu süreç aynı zamanda pedagojik yaklaşımların yeniden yapılandırılmasını ve eğitim paradigmasının köklü biçimde dönüştürülmesini de kapsamaktadır. Öğretmen ve öğrencilerin rollerini yeniden tanımlayan bu süreç, öğrenmeyi daha işbirlikçi, öğrenci odaklı ve deneyimsel bir düzleme taşımaktadır (Mishra and Koehler, 2006).

Dijital teknolojiler, öğrenme ortamlarının daha esnek, etkileşimli ve öğrenci merkezli biçimde yapılandırılmasına olanak sağlayan önemli araçlar arasında yer almaktadır. Özellikle üç boyutlu sanal öğrenme ortamları, simülasyonlar ve sanal gerçeklik uygulamaları, öğrencilerin soyut kavramları somut deneyimler yoluyla anlamlandırmalarına katkı sunmaktadır. Dalgarno and Lee'ye (2010) göre üç boyutlu sanal öğrenme ortamları;

deneyimsel öğrenmeyi destekleme, mekânsal bilgi edinimini güçlendirme, öğrenen motivasyonunu artırma ve iş birliğine dayalı öğrenme süreçlerini geliştirme açısından önemli pedagojik olanaklar sağlamaktadır. Bu bağlamda dijital teknolojiler, özellikle fen bilimleri, coğrafya ve teknoloji temelli derslerde öğrenme sürecinin görselleştirilmesine ve öğrencilerin kavramsal anlamalarının derinleştirilmesine katkıda bulunabilir (Dalgarno and Lee, 2010).

Türkiye bağlamında dijital teknolojilerin eğitim süreçlerine etkili biçimde entegre edilebilmesi, öğretmenlerin dijital yeterlik düzeyleriyle yakından ilişkilidir. Millî Eğitim Bakanlığı tarafından yayımlanan Dijital Öğretmen Yeterlikleri belgesinde öğretmen yeterlikleri; dijital okuryazarlık, öğrenme ve öğretmede dijital teknolojiler ile kapsayıcı, sürdürülebilir ve etik kullanım olmak üzere üç temel alan altında ele alınmaktadır (Millî Eğitim Bakanlığı [MEB], 2023). Bu çerçeve, öğretmenlerin yalnızca dijital araçları teknik olarak kullanabilmelerini değil, aynı zamanda bu araçları pedagojik amaçlara uygun, etik ve kapsayıcı biçimde öğrenme-öğretme süreçlerine dâhil edebilmelerini gerekli kılmaktadır (MEB, 2023).

Bununla birlikte, dijital teknolojilerin eğitimde yaygınlaşması her öğrenci açısından eşit öğrenme fırsatlarının kendiliğinden oluşacağı anlamına gelmemektedir. Dijital uçurum, yalnızca bilgisayar ve internet erişimine sahip olma durumu ile sınırlı değildir; bireylerin dijital teknolojileri kullanma becerileri, motivasyonları ve bu teknolojileri öğrenme amaçlı kullanabilme düzeyleri de dijital eşitsizliğin temel boyutları arasında yer almaktadır (Van Dijk, 2006). Türkiye’de yapılan çalışmalar da dijital eşitsizliklerin kent-kır ayrımı, bölgesel gelişmişlik farkları, gelir düzeyi ve toplumsal cinsiyet gibi değişkenlerle ilişkili olduğunu göstermektedir (Ay ve Kılıç, 2023).

Bu nedenle dijital teknoloji entegrasyonu yalnızca teknik altyapı yatırımı olarak değerlendirilmemeli; öğretmen yeterlikleri, dijital okuryazarlık, pedagojik uygunluk, erişim eşitliği ve etik kullanım boyutlarıyla birlikte ele alınmalıdır. Uluslararası alanyazın dijital uçurumun çok boyutlu yapısını ortaya koyarken, Türkiye merkezli çalışmalar bu sorunun yerel düzeyde bölgesel ve sosyoekonomik farklılıklarla daha da belirginleştiğini göstermektedir (Ay ve Kılıç, 2023; Van Dijk, 2006). Bu doğrultuda eğitim sistemlerinde dijital dönüşümün sürdürülebilir ve kapsayıcı biçimde yürütülebilmesi için hem kuramsal

çerçevelerden hem de Türkiye bağlamına özgü ampirik bulgulardan yararlanılması gerekmektedir (Dalgarno and Lee, 2010; MEB, 2023).

Dijital teknolojilerde yaşanan hızlı gelişmeler, eğitim sistemlerinin yapısını, öğrenme-öğretme süreçlerini ve bilgiye erişim biçimlerini önemli ölçüde dönüştürmektedir. Bilgi kaynaklarının çeşitlenmesi, öğrenme ortamlarının fiziksel sınıf sınırlarının dışına taşması ve bireyselleştirilmiş öğrenme gereksinimlerinin artması, teknolojiyi çağdaş eğitim anlayışının temel bileşenlerinden biri hâline getirmiştir. UNESCO'nun 2023 yılında yayımladığı Küresel Eğitim İzleme Raporu'nda da teknolojinin; eğitime erişimi artırma, öğrenme niteliğini geliştirme, eğitimde kapsayıcılığı destekleme ve fırsat eşitliğini güçlendirme açısından önemli bir araç olduğu vurgulanmaktadır (UNESCO, 2023).

Eğitimde teknoloji kullanımı, öğrenme-öğretme süreçlerinin daha etkileşimli, esnek ve öğrenci merkezli bir yapıya kavuşmasına katkı sağlamaktadır. Dijital materyaller, çevrim içi öğrenme platformları, çoklu ortam içerikleri ve etkileşimli uygulamalar, öğrencilerin derse yönelik ilgisini artırmakta ve öğrenme sürecine daha aktif biçimde katılmalarını desteklemektedir. Eğitim teknolojileri üzerine yapılan sistematik incelemeler, bilgi ve iletişim teknolojileriyle desteklenen öğrenme ortamlarının uygun pedagojik yaklaşımlarla birlikte kullanıldığında öğrencilerin akademik başarıları üzerinde olumlu etkiler oluşturabildiğini göstermektedir (Valverde-Berrocso et al., 2022). Bu bağlamda teknoloji, tek başına öğrenmeyi garanti eden bir unsur olmaktan çok, etkili öğretim tasarımıyla bütünleştğinde öğrenme çıktılarının niteliğini artıran bir araç olarak değerlendirilmelidir.

Teknoloji destekli öğrenme ortamları, öğrencilerin yalnızca akademik başarılarını değil, aynı zamanda motivasyonlarını, derse katılımlarını ve öğrenme sürecindeki etkileşim düzeylerini de etkileyebilmektedir. Özellikle etkileşimli içerikler, oyunlaştırma uygulamaları, sanal simülasyonlar ve dijital değerlendirme araçları, öğrencilerin öğrenme sürecinde daha aktif rol almalarına olanak tanımaktadır. Güncel araştırmalar, teknolojiyle zenginleştirilmiş öğrenme ortamlarının öğrenci motivasyonunu artırabildiğini ve daha derin öğrenme deneyimlerinin oluşmasına katkı sağlayabildiğini ortaya koymaktadır (Duterte, 2024). Bu yönüyle teknoloji, geleneksel öğretim yöntemlerini tamamlayan ve öğrenme süreçlerini çeşitlendiren önemli bir destek unsuru olarak öne çıkmaktadır.

Dijital teknolojilerin eğitimdeki önemli katkılarından biri de bireyselleştirilmiş öğrenme olanakları sunmasıdır. Uyarlanabilir öğrenme sistemleri, öğrenme analitiği ve yapay zekâ destekli uygulamalar, öğrencilerin öğrenme hızlarına, ilgi alanlarına ve gereksinimlerine uygun içeriklerle karşılaşmalarını mümkün kılmaktadır. Böylece öğrenme süreci daha esnek, izlenebilir ve öğrenci ihtiyaçlarına duyarlı bir hâle gelmektedir. Son yıllarda yapay zekânın eğitimde kullanımına yönelik çalışmaların artması da bu dönüşümün önemli göstergelerinden biridir. Türkiye’de 2020-2024 yılları arasında eğitimde yapay zekâ konulu çalışmaların incelendiği araştırmada, yapay zekâ temelli uygulamaların öğrenme süreçlerini iyileştirme, öğretmenlerin zaman yönetimini destekleme ve öğrenci başarısını geliştirme potansiyeline sahip olduğu belirtilmektedir (Oruç vd., 2024).

Eğitimde teknoloji kullanımı yalnızca sınıf içi uygulamalarla sınırlı değildir; aynı zamanda eğitim politikalarının, öğretim programlarının ve kurumsal stratejilerin de önemli bir parçası hâline gelmiştir. Birçok ülke, eğitimde dijital dönüşümü desteklemek amacıyla altyapı yatırımları yapmakta, öğretmenlerin dijital yeterliklerini geliştirmeye yönelik programlar yürütmekte ve eğitim teknolojilerine ilişkin stratejik planlar oluşturmaktadır. Türkiye’de de Millî Eğitim Bakanlığı tarafından yürütülen çalışmalar, eğitimde dijitalleşme ve yapay zekâ temelli dönüşümün sürdürülebilir, kapsayıcı, etik ve pedagojik temellere dayalı biçimde gerçekleştirilmesi gerektiğini ortaya koymaktadır (MEB, 2025). Bu doğrultuda teknolojinin eğitim sistemine entegrasyonu, yalnızca araç ve altyapı sağlama süreci olarak değil, öğretim süreçlerinin niteliğini artırmaya yönelik bütüncül bir dönüşüm olarak ele alınmalıdır.

Eğitimde teknolojinin etkili biçimde kullanılabilmesinde öğretmenlerin sahip olduğu yeterlikler belirleyici bir role sahiptir. Öğretmenlerin dijital araçları yalnızca teknik açıdan kullanabilmeleri yeterli değildir; bu araçları pedagojik amaçlara uygun biçimde seçmeleri, ders içeriğiyle bütünleştirmeleri ve öğrenci öğrenmesini destekleyecek şekilde kullanmaları gerekmektedir. Bu noktada teknolojik pedagojik alan bilgisi, öğretmenlerin teknoloji entegrasyonu sürecindeki temel yeterlik alanlarından biri olarak değerlendirilmektedir. Türkiye’de eğitimde teknoloji entegrasyonuna yönelik yapılan çalışmalar, öğretmen yeterliklerinin bu sürecin başarısında önemli bir unsur olduğunu ve teknoloji kullanımının pedagojik temellerle desteklenmesi gerektiğini göstermektedir (Arslan vd., 2022).

Sonuç olarak eğitimde teknoloji kullanımı; öğrenme ortamlarını zenginleştiren, öğrenci katılımını artıran, bireyselleştirilmiş öğrenmeyi destekleyen ve öğretim süreçlerinin

niteliğini geliştiren önemli bir unsur olarak değerlendirilmektedir. Bununla birlikte teknolojinin eğitimde etkili sonuçlar üretebilmesi, yalnızca teknolojik araçların varlığına bağlı değildir. Etkili teknoloji kullanımı; pedagojik amaçlarla uyumlu öğretim tasarımı, öğretmenlerin dijital yeterliklerinin geliştirilmesi, kurumsal destek mekanizmalarının oluşturulması ve eğitim politikalarının sürdürülebilir biçimde yapılandırılması ile mümkün olmaktadır. Bu nedenle eğitimde teknoloji entegrasyonu, teknik bir yenilikten çok pedagojik, kurumsal ve politik boyutları olan kapsamlı bir dönüşüm süreci olarak ele alınmalıdır.

Okullar ve öğretmenlerin teknolojik standartlarda bir altyapıya ve yetkinliğe sahip olması gerekmektedir (ISTE, 2017). Bu yeterlikler şu şekilde özetlenebilir: (1) Öğretmenler öğrencilerin öğrenmesine katkı sağlayan yeni teknolojileri gerektiğinde destek olarak içselleştirmelidir ve sürekli gelişime açık kalmayı sürdürmelidir. (2) Öğretmenler öğrencilerin başarısına katkı sağlayacak ve öğretim kalitesini yükseltecek mesleki liderlik sergilemelidir. (3) Öğretmenler öğrencilerin dijital vatandaşlık sorumluluklarını üstlenmelerine ve bu doğrultuda topluma katkıda bulunmalarına zemin hazırlamalıdır. (4) Öğretmenler öğrencilerin yeni kaynak ve yaklaşımları keşfetmek, sorunları çözmek ve bilgi paylaşımını gerçekleştirmek amacıyla meslektaşları ve öğrencileriyle iş birliğine girerek bunun için özel zaman ayırmalıdır. (5) Öğretmenler bireysel farklılıkları dikkate alarak öğrenci merkezli ve yaratıcı öğrenme ortamları tasarlamalıdır. (6) Öğretmenler öğrenci başarısını artırmak amacıyla teknolojiden etkin biçimde yararlanmalı ve öğrenmeyi kolaylaştıran ortamlar oluşturmalıdır. (7) Öğretmenler öğrencilerin hedeflerine ulaşmalarını desteklemek amacıyla teknoloji odaklı değerlendirmeler gerçekleştirmeli ve elde edilen verileri karar süreçlerine dâhil etmelidir (ISTE, 2017). Bunların yanı sıra nitelikli bir eğitim için tüm öğretmenlerin eğitime teknoloji entegrasyonu konusunda gerekli bilgiye sahip olmaları ve öğrencilerini bu araçları kullanmaya teşvik etmeleri büyük önem taşımaktadır.

1.3 Teknoloji Yeterliği Öz-Değerlendirmesi

Öz-değerlendirme, bireyin kendi bilgi, beceri, performans ve gelişim düzeyini belirli ölçütler doğrultusunda inceleyerek güçlü ve geliştirilmesi gereken yönlerini belirlemesi sürecidir (Andrade, 2019; McMillan and Hearn, 2008). Eğitim bağlamında öz-değerlendirme, bireyin yalnızca mevcut yeterlik düzeyini fark etmesine değil, aynı zamanda öğrenme sürecine ilişkin sorumluluk geliştirmesine de katkı sağlamaktadır. Bandura'nın (1986) öz-yeterlik kuramı açısından değerlendirildiğinde, bireyin belirli bir görevi başarıyla yerine

getirebileceğine ilişkin inancı, o göreve yönelik davranışlarını, çabasını ve sürekliliğini etkileyen temel değişkenlerden biridir. Bu bağlamda öğretmenlerin teknoloji kullanımına ilişkin öz-yeterlik ve yeterlik algıları, onların sınıf içi teknoloji entegrasyonuna yönelik tutum ve uygulamalarını doğrudan etkileyebilmektedir (Woolfolk-Hoy, 2003).

Öğretmenlerin teknoloji yeterliği, yalnızca temel bilgisayar kullanımı ya da dijital araçlara erişim becerisiyle sınırlı değildir. Bu yeterlik; teknolojiyi pedagojik amaçlarla kullanabilme, dijital içerik ve öğrenme ortamları tasarlayabilme, öğrencilerin teknoloji destekli öğrenme süreçlerine aktif katılımını sağlayabilme ve dijital araçları öğretim hedefleriyle uyumlu biçimde bütünleştirebilme becerilerini içermektedir. Teknolojik Pedagojik Alan Bilgisi (TPAB) yaklaşımı da öğretmenlerin etkili teknoloji kullanımı için teknoloji bilgisi, pedagojik bilgi ve alan bilgisini bütüncül biçimde yapılandırmaları gerektiğini ortaya koymaktadır (Koehler and Mishra, 2005; Mishra and Koehler, 2006).

Öğretmenlerin teknoloji yeterliklerini belirlemeye yönelik ilk kapsamlı araçlardan biri Ropp (1999) tarafından geliştirilen Technology Proficiency Self-Assessment (TPSA) ölçeğidir. Bu ölçekte teknoloji yeterliği e-posta kullanımı, WWW, entegre uygulamalar ve öğretimde teknoloji kullanımı boyutlarında ele alınmıştır. Christensen and Knezek (2017), söz konusu yapıyı 21. yüzyıl öğrenme gereksinimlerine uyarlayarak TPSA C-21 ölçeğini geliştirmiştir. Fidan vd. (2020) tarafından Türkçeye uyarlanan YYÖTYÖ (21. Yüzyıl Öğrenmeleri için Teknoloji Yeterliği Öz-Değerlendirme Ölçeği) ise 24 madde ve dört faktörlü yapısıyla öğretmenlerin teknoloji yeterliklerini öz-değerlendirme yoluyla belirlemeye olanak sağlamaktadır.

Alanyazında öğretmenlerin teknoloji yeterliklerini etkileyen değişkenlere ilişkin farklı bulgular bulunmaktadır. Bazı araştırmalarda cinsiyet, branş, mesleki kıdem, eğitim düzeyi, hizmet içi eğitim alma durumu ve teknoloji kullanım deneyimi gibi değişkenlerin öğretmenlerin teknoloji kullanım yeterliklerinde anlamlı farklılıklar oluşturabildiği görülmektedir. Durak ve Seferoğlu (2017), Fırsatları Artırma ve Teknolojiyi İyileştirme Hareketi (FATİH) Projesi kapsamında görev yapan öğretmenlerin bilişim teknolojileri kullanım yeterliklerini inceledikleri çalışmalarında öğretmenlerin bazı teknoloji kullanım alanlarında yüksek yeterlik gösterdiklerini, ancak çevrim içi iletişim ve bazı dijital uygulama alanlarında daha düşük yeterlik düzeylerine sahip olduklarını belirlemiştir. Karadeniz ve Vatanartıran (2015) ise sınıf öğretmenlerinin teknolojik pedagojik alan bilgilerini

inceledikleri çalışmalarında, öğretmenlerin kendilerini genel olarak yeterli gördüklerini; ancak bazı alt boyutlarda cinsiyet ve mesleki deneyime göre anlamlı farklılıklar bulunduğunu ortaya koymuştur.

Bu bulgular, öğretmenlerin teknoloji yeterliklerinin tek boyutlu bir beceri alanı olarak değil; pedagojik, mesleki, demografik ve bağlamsal değişkenlerle birlikte ele alınması gereken çok boyutlu bir yapı olduğunu göstermektedir. Bu nedenle öğretmenlerin teknoloji yeterliği öz-değerlendirme düzeylerinin belirlenmesi, hem öğretmenlerin mesleki gelişim gereksinimlerinin ortaya konulması hem de eğitimde teknoloji entegrasyonu politikalarının daha etkili biçimde yapılandırılması açısından önemlidir.

1.4 Dijital Veri ve Dijital Veri Güvenliği

Dijital veri güvenliği modern toplumda yaşamsal bir önem taşımakta; bu alandaki risklerin en aza indirilmesinde bilinçli ve donanımlı bireylerin rolü belirleyici olmaktadır. Bu nedenle bireylerin dijital veri koruma konusundaki farkındalıklarının artırılması ve bu alanda eğitim almaları vazgeçilmez bir gereklilik hâline gelmiştir (Canbek ve Sağıroğlu, 2007a). Medya kanalları, sosyal platformlar ve okul seminerlerinin yanı sıra ihtiyaca özgü eğitim programlarının geliştirilmesi, bireylerde dijital güvenlik kültürünün oluşturulmasına doğrudan katkı sağlamaktadır. Nitekim Birleşik Krallık'ta 2011 yılından itibaren ilköğretim düzeyinde güvenli internet kullanımına yönelik zorunlu derslerin öğretim programlarına eklenmesi planlanmıştır (Ulaşanoğlu vd., 2010).

Dijital veri güvenliğini sağlamaya yönelik çok sayıda teknik önlem bulunmakla birlikte insan faktörü göz ardı edilmemelidir. Yeterli güvenlik farkındalığına sahip olmayan bireyler, güvenlik önlemlerinin etkinliğini zayıflatabilmekte ve sürecin çeşitli aşamalarında ciddi aksaklıklara yol açabilmektedir (Şahinaslan vd., 2013). Bilgi paylaşımında yapılabilecek en küçük hatalar ya da bilinçsiz davranışlar, alınan teknik tedbirlerin tamamını işlevsiz kılabilir (Şahinaslan vd., 2009). Kablosuz bağlantılar, cep telefonları ve internet gibi kişisel kullanım araçları dikkate alındığında, güvenlik çözümlerinin bireysel düzeyde de benimsenmesinin hayati önem taşıdığı görülmektedir (Swaminatha ve Elden, 2003).

Dijital veri güvenliği; verilerin yetkisiz erişim, değiştirme, bozulma, ifşa ya da yok edilme gibi istenmeyen durumlardan korunmasını ifade etmekte ve kişisel veri güvenliği, kurumsal veri güvenliği ve ulusal siber güvenlik olmak üzere üç temel kategoride ele alınmaktadır

(Güngör, 2015). Kişisel veri güvenliği; kimlik, finansal ve sağlık verileri ile dijital izler gibi bireye ait verilerin korunmasını kapsarken kurumsal bilgi güvenliği, kurumların bilgi varlıklarını tehditlere karşı koruyacak politika, süreç ve altyapıları oluşturmasını içermektedir (Uluslararası Standartlaştırma Örgütü [International Organization for Standardization, ISO], 2022; 6698 sayılı Kişisel Verilerin Korunması Kanunu [KVKK], 2016; Özdemir ve Uluyol, 2021). Ulusal siber güvenlik ise uluslararası iş birliğini, siber suçlarla mücadeleyi ve kapsamlı ulusal güvenlik politikalarını bünyesinde barındıran geniş çaplı bir stratejik alanı ifade etmektedir (Güngör, 2015).

Dijital veri güvenliğinde öncelikle insan faktörüne odaklanmak gerekmektedir. Güvenlik farkındalığı, zararlı yazılımlar, sosyal mühendislik saldırıları ve kişisel verilerin korunması gibi konularda düzenlenen eğitimler, bireylerin güvenlik bilincinin gelişmesine katkı sağlamaktadır (Chmura, 2017; Frank and Ament, 2021). Bilgi güvenliği; bir kuruluşun verileri üzerinde denetim sağlamasının yanı sıra teknolojik kaynakların korunmasını, yasal yükümlülüklerin yerine getirilmesini ve bilişim teknolojileri sistemlerinin güvenli biçimde işletilmesini de kapsamaktadır (Whitman and Mattord, 2011).

Bilgi teknolojilerindeki tehditlerin çeşitlenmesi, kurumları hem dışarıdan hem de içeriden gelen saldırılara karşı daha dikkatli olmaya zorlamaktadır. İç tehditler çoğunlukla insan hataları, ihmal, farkındalık eksikliği ya da kötü niyetli davranışlar sonucunda ortaya çıkabilmektedir (Frank and Ament, 2021; Liginlal et al., 2009). Bu nedenle kurumların yalnızca teknik güvenlik önlemlerine değil; çalışan eğitimi, farkındalık çalışmaları, güvenlik politikaları ve süreç yönetimine de önem vermesi gerekmektedir (Chmura, 2017; Whitman and Mattord, 2011).

Thomas Reid'in 1786'da dile getirdiği "bir sistemin gücü en zayıf halkasına bağlıdır" ilkesi, bilgi güvenliği açısından da geçerliliğini korumaktadır (Reid, 1786; Chmura, 2017). İç tehditleri göz ardı ederek yalnızca dışsal saldırılara odaklanan bir organizasyon, sistem bütünlüğünü ciddi biçimde riske atabilir. Bu nedenle taşınabilir cihazlar, kullanıcı davranışları, erişim yetkileri ve güvenlik farkındalığı, kurumların genel güvenlik stratejisinin ayrılmaz bir parçası olarak ele alınmalıdır (Frank and Ament, 2021; Whitman and Mattord, 2011).

Dijital veri güvenliğini tehdit eden başlıca unsurlar şu şekilde sıralanabilir (Canbek ve Sağıroğlu, 2007a, 2007b):

- **Dağıtılmış Hizmet Reddi (Distributed Denial of Service [DDoS]):** Hedef sistemi işlevsiz kılarak hizmet erişimini engeller.
- **Truva Atı:** Kullanıcı bilgisi olmadan kötü amaçlı eylemler gerçekleştiren yazılımlardır.
- **Mantık Bombası:** Belirli bir koşul tetiklendiğinde devreye giren zararlı programlardır.
- **Arka Kapı:** Yetkisiz erişim sağlamak için kullanılan gizli erişim noktalarıdır.
- **Solucanlar:** Ağ üzerinde kendi kendine yayılan zararlı yazılımlardır.
- **Virüsler:** Programlara bulaşarak zararlı işlemler gerçekleştiren yazılımlardır.
- **Reklam Destekli ve Casus Yazılımlar:** Kullanıcı izni olmadan bilgi toplayan ya da istenmeyen içerikler sunan yazılımlardır.
- **Ortalama veya Sazan Avlama (Phishing):** Kullanıcıları kandırarak kişisel bilgileri ele geçiren sosyal mühendislik saldırılarıdır.
- **Zincir E-posta ve İnternet Adresi Aldatmacası:** Zararlı bağlantılar aracılığıyla kullanıcıları yanıltan saldırılardır.
- **Spam:** Zararlı ya da istenmeyen içerikler barındıran e-posta ve mesajlardır.

İnsan kaynaklı tehditler, kullanıcıların bilinçsiz davranışları ya da kötü niyetli eylemleri sonucunda ortaya çıkmakta ve sistemleri savunmasız bırakan açıkların en önemli kaynağını oluşturmaktadır (Tekerek, 2008). Symantec'in (2013) 18. İnternet Güvenlik Tehdit Raporu, 2012 yılında siber saldırıların belirgin biçimde arttığını ortaya koymaktadır: Web tabanlı saldırılar %30, zararlı mobil yazılımlar ise %58 oranında artış göstermiştir. Türkiye bu dönemde Avrupa ülkeleri arasında istem dışı e-posta saldırılarında beşinci, ortalama saldırılarında sekizinci, virüs saldırılarında ise beşinci sırada yer almıştır (Symantec, 2013).

Dijital veri güvenliğinin sağlanmasına yönelik bireysel ve kurumsal düzeyde alınabilecek başlıca önlemler şu şekilde sıralanabilir (Öztürk, 2022; Yavanoğlu vd., 2012):

- **Güçlü Şifreler Kullanmak:** Karmaşık ve düzenli olarak güncellenen şifreler hesap güvenliğini pekiştirir.
- **İki Faktörlü Kimlik Doğrulama:** Hassas hesaplar için ek bir güvenlik katmanı sağlar.

- **Güvenlik Yazılımları ve Güncellemeler:** Antivirüs ve güvenlik duvarı yazılımlarının düzenli güncellenmesi büyük önem taşımaktadır.
- **Bilinçli İnternet Kullanımı:** Şüpheli e-posta ve bağlantılardan kaçınmak ile güvenilmeyen kaynaklara karşı temkinli olmak, zararlı yazılımların sisteme sızmasını önler.
- **Veri Yedekleme:** Düzenli yedekleme, olası veri kayıplarına karşı etkin bir güvence oluşturur.
- **Eğitim ve Bilinçlendirme:** Sosyal mühendislik gibi tehditlere karşı dirençli olunabilmesi için kullanıcıların bilinçlendirilmesi büyük önem taşır.
- **Yasal Düzenlemeler ve Denetimler:** Devlet düzeyinde yapılan düzenlemeler, bireylerin ve kurumların güvenlik standartlarına uyumunu teşvik etmektedir.

Dijital ortamların yaygınlaşması beraberinde önemli güvenlik risklerini de getirmekte (Uluslararası Telekomünikasyon Birliği [International Telecommunications Union], 2008); verilerin yetkisiz kişilerin eline geçmesi ciddi sonuçlar doğurabilmektedir (Keleş ve Güneş, 2013). Bu nedenle hem bireylerin hem de kurumların güçlü güvenlik politikaları ve teknolojik çözümler benimseyerek verilerini koruması gerekmektedir (Korucu, 2021). Veri ihlallerinin tespiti zaman alıcı ve karmaşık bir süreçtir. İhlalin boyutları finansal, operasyonel ve itibar kayıpları açısından çok yönlü biçimde değerlendirilmeli; benzer olayların tekrarlanmasını önlemeye yönelik tedbirlerin belirlenmesi için kapsamlı bir inceleme yapılmalıdır (Yılmaz, 2015).

Bireysel veri güvenliği denetimi, kişisel verilerin bilinçli biçimde korunmasını ve dijital platformların güvenli kullanımını kapsamaktadır. Kişisel veriler bireyi doğrudan ya da dolaylı olarak tanımlayabilen bilgiler olduğundan, bu verilerin korunması mahremiyet hakkı ve özel hayatın gizliliği açısından önem taşımaktadır (Dülger, 2015, 2016). Bu süreçte insan faktörü belirleyici olmakla birlikte güvenlik ayarlarının doğru yapılandırılması, güçlü şifrelerin seçilmesi, güvenilir ve güncel yazılımların kullanılması, güvenlik yazılımlarının etkin biçimde işletilmesi ve kullanıcı farkındalığının artırılması da gereklidir (Öztürk, 2022). Gizlilik, bütünlük ve erişilebilirlik ilkelerinin bütüncül biçimde uygulanması ise güvenli bir dijital ortamın temel koşulunu oluşturmaktadır (Öztürk, 2022; Tokat Gaziosmanpaşa Üniversitesi, 2018).

Bilişim ve veri güvenliği alanında kullanılan pek çok terim, zaman içinde ya özgün anlamını yitirmiş ya da birbiriyle örtüşen kavramlar hâlinde kullanılmaya başlanmıştır. Veri ile enformasyon arasındaki sınırın kavranması, bu terimlerin doğru kullanımı açısından belirleyici bir rol üstlenmektedir. Veri, işlenmemiş ham sembol ve olguları; enformasyon, belirli bir bağlamda işlenerek anlamlandırılmış veriyi; bilgi ise enformasyonun deneyim, yorum ve amaç doğrultusunda yapılandırılmış biçimini ifade etmektedir (Ackoff, 1989; Rowley, 2007). Peter Drucker'ın da işaret ettiği üzere, çağdaş örgütlerde bilgi ve bilgi çalışanlarının üretkenliği, kurumsal verimlilik ve değer üretimi açısından temel belirleyicilerden biri hâline gelmiştir (Drucker, 1999).

Dijital dünyada hiçbir sistemin mutlak güvenli olmadığı bilinmekle birlikte, bu alandaki farkındalık eksikliği güvenlik açıklarının büyümesine zemin hazırlamaktadır (Yılmaz vd., 2016). Ergül ve Yıldız (2021), sosyal medya platformlarında mahremiyet sınırlarının dönüşüme uğradığını ve kullanıcı paylaşımlarının çeşitli mahremiyet riskleri doğurabildiğini ortaya koymaktadır.

Dijital veri; elektronik ortamda saklanan, işlenen, iletilen ve belirli bir düzen dâhilinde erişilebilir biçimde yönetilen içerikleri ifade etmekte olup bu verilerin güvenliği bilgi güvenliğinin temel hedefleri arasında yer almaktadır (Canbek ve Sağıroğlu, 2006). Dijital veri miktarının hızla artması; masaüstü bilgisayarlar, akıllı telefonlar, sunucular ve çeşitli dijital platformlar aracılığıyla işlenen, saklanan ve iletilen bilgi hacmiyle doğrudan ilişkilidir. Dijital veri, gündelik yaşamın ayrılmaz bir parçası hâline gelmiştir. Bu tür veriler pek çok farklı teknolojik araç üzerinde üretilebilmekte; elektronik belgeler, e-kitaplar, e-postalar, dijital videolar, müzik dosyaları ve fotoğraflar gibi içerikler dijital verinin kapsamına girmektedir (Yılmaz vd., 2016).

Dijital veri güvenliği; salt teknik altyapıyla sınırlı kalmayan, toplumsal, hukuki, ekonomik ve insani dinamiklerle yoğun etkileşim içinde olan karmaşık ve çok boyutlu bir kavramdır. Dijital sistemlerin tasarımcıları, kullanıcıları ve bu sistemlere yönelik ihlal girişiminde bulunan aktörler insan olduğundan, dijital veri güvenliği; insan faktörü, kullanıcı davranışları, farkındalık düzeyi ve kurumsal güvenlik kültürü gibi özgün iç dinamikler barındırmaktadır (Chmura, 2017; Öztürk, 2022). Yasal düzenlemelerin yetersiz kaldığı durumlarda dijital sistemlerin kötüye kullanımına yönelik riskler artmakta; bu nedenle veri güvenliğinin bireysel hakların korunması, dijital delillerin güvenliği ve hukuki denetim

mekanizmalarıyla birlikte ele alınması gerekmektedir (Sarsıkoğlu ve Ergün, 2025). Dijital sistemlerde güvenlik zafiyetleri yalnızca teknik kayıplara değil, aynı zamanda maddi zarar, itibar kaybı ve güven kaybı gibi kurumsal sonuçlara da yol açabileceğinden, veri güvenliği teknik, hukuki, ekonomik ve örgütsel boyutlarıyla birlikte değerlendirilmelidir (Makridis, 2021).

Türkiye’de siber güvenlik alanındaki kurumsal politika çerçevesi; kamu kurumları, kritik altyapılar, özel sektör ve bireylerin dijital güvenliğini artırmaya yönelik stratejik belgeler ve teknik rehberler aracılığıyla şekillenmektedir. Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020-2023), Ulaştırma ve Altyapı Bakanlığı tarafından kamu kurumları, özel sektör, sivil toplum kuruluşları ve üniversitelerle iş birliği içinde hazırlanmış; ulusal siber güvenlik kapasitesinin geliştirilmesi, siber tehditlere karşı dayanıklılığın artırılması ve güvenli bir dijital ekosistemin oluşturulması temel hedefler arasında gösterilmiştir (T.C. Ulaştırma ve Altyapı Bakanlığı, 2020).

Siber olaylara müdahale süreçlerine ilişkin yayımlanan kurumsal dokümanlar, kurumların yalnızca olay sonrasında değil olay gerçekleşmeden önce de hazırlıklı olmaları gerektiğini ortaya koymaktadır. Sistemlerin güncel tutulması, varlık envanterinin oluşturulması, güvenlik açıklarının belirlenmesi, çalışanların sosyal mühendislik ve oltalama saldırılarını ayırt edebilecek farkındalık düzeyine ulaştırılması, zararlı web sitelerine erişimin kısıtlanması, düzenli yedekleme yapılması ve siber olay müdahale planlarının hazırlanması bu kapsamdaki temel önlemler arasında yer almaktadır (Ulusal Siber Olaylara Müdahale Merkezi [USOM], t.y.).

Kişisel verilerin korunması açısından değerlendirildiğinde, KVKK’nın 2023 yılı faaliyet raporu; Türkiye’de veri güvenliği, ihbar ve şikâyet süreçleri ile veri ihlal bildirimlerinin kurumsal düzeyde izlendiğini göstermektedir. Raporda ihbar ve şikâyetlerin sektörel ve konu bazında dağılımına, veri ihlal bildirimlerine ve inceleme süreçlerine yer verilmesi, kişisel verilerin hukuka uygun işlenmesi ve veri güvenliği yükümlülüklerinin denetimi açısından kurumsal izleme mekanizmasının işlediğini ortaya koymaktadır (Kişisel Verileri Koruma Kurumu [KVKK], 2024).

Güncel siber tehdit raporları incelendiğinde, Türkiye’de oltalama saldırıları, zararlı yazılımlar, fidye yazılımları ve yazılım tedarik zinciri güvenliği gibi konuların önemli risk

alanları arasında yer aldığı görülmektedir. Savunma Teknolojileri Mühendislik Teknolojik Düşünce Merkezi (STM ThinkTech) tarafından yayımlanan 2023 yılı siber tehdit durum raporlarında; özellikle kriz ve afet dönemlerinde toplumsal duyarlılığı istismar eden ortalama kampanyalarına, zararlı yazılım örneklerine ve tedarik zinciri güvenliğine dikkat çekilmiştir (STM ThinkTech, 2023a, 2023b).

Genel olarak değerlendirildiğinde, Türkiye’de siber güvenlik riskleri yalnızca teknik açıklıklardan değil; insan faktörü, sosyal mühendislik yöntemleri, kurumsal farkındalık eksiklikleri ve yetersiz olay müdahale süreçlerinden de kaynaklanmaktadır. Bu nedenle fidye yazılımları, ortalama saldırıları ve zararlı yazılımlara karşı teknik güvenlik önlemlerinin yanında; düzenli personel eğitimi, farkındalık çalışmaları, güçlü veri koruma politikaları, güncel yedekleme stratejileri ve uygulanabilir olay müdahale planlarının geliştirilmesi gerekmektedir (STM ThinkTech, 2023a, 2023b; USOM, t.y.).

ABD’de yayımlanan *The National Strategy for Homeland Security* belgesinde, iç güvenlik politikalarının yürütülmesinde bilişim teknolojileri ve bilgi paylaşım sistemlerinin önemli rol oynadığı; bu kapsamda temel güvenlik alanlarının istihbarat ve erken uyarı, sınır ve ulaştırma güvenliği, yerel anti-terörizm, kritik altyapıların korunması, yıkıcı tehditlere karşı savunma ile acil durum hazırlığı ve müdahale başlıkları altında ele alındığı görülmektedir (İç Güvenlik Ofisi [Office of Homeland Security], 2002).

- **İstihbarat ve Erken Uyarı Sistemleri:** Teröristlerin iletişiminin analiz edilmesi ve sahte kimlik tespiti gibi faaliyetlerle önceden önlem alınmasına olanak tanımaktadır.
- **Sınır ve Ulaştırma Güvenliği:** Yolcu bilgileri, belge kontrolleri ve biyometrik veriler aracılığıyla “akıllı sınırlar” uygulamaları hayata geçirilmektedir.
- **Yerel Anti-Terörizm:** Gelişmiş bilişim sistemleri, yerel tehditlerin izlenmesi ve analiz edilmesinde önemli bir rol üstlenmektedir.
- **Önemli Altyapı ve Anahtar Bileşenlerin Korunması:** Su, elektrik ve ulaşım gibi hayati altyapıların hem fiziksel hem de siber tehditlere karşı korunması için teknolojik sistemlerin geliştirilmesi gerekmektedir.
- **Yıkıcı Terörizme Karşı Savunma:** Kimyasal, biyolojik veya radyolojik tehditlere karşı bilişim sistemleri; erken tespit, analiz ve alarm süreçlerini yönetmektedir.
- **Acil Yardım ve Yanıt Sistemi:** Teknoloji destekli acil durum yönetimi, olası saldırı durumlarında zararın en aza indirilmesi açısından hayati öneme sahiptir.

Sonuç olarak veri güvenliği, yalnızca teknolojik bir mesele olmanın ötesinde sosyal, hukuki ve etik boyutları bulunan çok katmanlı bir kavramdır. Bu dengenin gözetilmesi hem bireysel hem de toplumsal düzeyde önemli bir sorumluluk olarak öne çıkmaktadır.

Dijital veri güvenliği; gizlilik, bütünlük ve erişilebilirlik olmak üzere üç temel boyuttan oluşmaktadır. Alanyazında güvenlik üçgeni olarak adlandırılan bu üç boyut (Şekil 1.2) birbirinden bağımsız değildir; herhangi birindeki açık, diğerlerinin güvenilirliğini de tehlikeye atabilmektedir (Fussell, 2005).



Şekil 1.2: Güvenlik üçgeni (Dönmez, 2019)

Şekil 1.2’deki güvenlik üçgeninde yer alan unsurlardan herhangi birinde sorun yaşanması, sistemde güvenlik ihlaline yol açabilmektedir. Bu nedenle dijital veri güvenliğinde yalnızca verilerin gizli tutulması değil; aynı zamanda doğru ve eksiksiz biçimde korunması ve yetkili kullanıcılar tarafından ihtiyaç duyulduğunda erişilebilir olması da önemlidir (Öztürk, 2022).

Bu bütüncül yapının ilk unsuru olan gizlilik, bireylerin dijital veri güvenliğine ilişkin en temel kaygılarından biri olan kişisel bilgilere yetkisiz erişim sorunuyla doğrudan ilişkilidir. Gizlilik; bilginin yetkisiz kişiler, kuruluşlar ya da işlemler tarafından erişilememesi, kullanılamaması, değiştirilmemesi, depolanmaması veya ifşa edilmemesi olarak tanımlanmaktadır (Öztürk, 2022). Gizliliğin ihlal edilmesi durumunda veriler yok edilebilmekte, kötüye kullanılabilmekte, değiştirilebilmekte ya da ifşa edilebilmekte; böylece veri bütünlüğü de ciddi biçimde zarar görebilmektedir (Gülpınar-Demirci ve Buluz-Kömeçoğlu, 2022; Öztürk, 2022).

Kişisel verilerin hukuka aykırı biçimde işlenmesi, paylaşılması veya ifşa edilmesi; mahremiyetin ihlali, kişilik haklarının zedelenmesi, kişisel itibar kaybı ve maddi zarar gibi sonuçlar doğurabilmektedir (Dülger, 2016). Gizliliğin güvence altına alınmasında şifreleme, kullanıcı denetimleri, güçlü parola kullanımı, SMS ile doğrulama, iki adımlı doğrulama ve yetkilendirme mekanizmaları gibi önlemler büyük önem taşımaktadır (Henkoğlu ve Külcü, 2013; Öztürk, 2022).

Bütünlük boyutu, bilginin doğruluğunun ve tamlığının korunmasını ifade etmektedir (Öztürk, 2022). Verilerin kasıtlı ya da kazara bozulmasının, silinmesinin veya değiştirilmesinin önüne geçilebilmesi için bireylerin ve kurumların gerekli tedbirleri alması ve bu konuda bilinçlendirilmesi gerekmektedir (Erdoğan, 2024; Öztürk, 2022). Öztürk'e (2022) göre bilgi bütünlüğünün zarar görmesi durumunda, bilgi sistemlerindeki veriler yetkisiz kişiler tarafından değiştirilebilmekte, bozulabilmekte veya silinebilmektedir. Bu nedenle şifreleme sistemleri, kullanıcı denetimleri, erişim yetkilerinin sınırlandırılması ve kullanıcıların erişebileceği alanların belirlenmesi, bütünlüğün korunmasına yönelik başlıca güvenlik önlemleri arasında yer almaktadır (Öztürk, 2022).

Erişilebilirlik ise yetkili kişi ya da kurumlar tarafından istendiğinde bilginin erişilebilir ve işlenebilir durumda olması olarak tanımlanmaktadır (Öztürk, 2022). Verilerin yetkili kişilerce ihtiyaç duyulan her an erişilebilir ve işlenebilir durumda olması, bilgi güvenliği ve iş süreçlerinin sürekliliği açısından büyük önem taşımaktadır (Öztürk, 2022). Sistem kesintileri, siber saldırılar, virüs bulaşması, işletim sistemi sorunları ve olası teknik arızalar veri erişilebilirliğini ciddi ölçüde tehlikeye atabilmektedir (Öztürk, 2022). Erişilebilirliğin sağlanabilmesi için verileri tehdit eden unsurların kapsamlı biçimde analiz edilmesi şarttır; bu unsurlar arasında bilgi sızıntısı, sosyal mühendislik, zayıf kimlik doğrulama mekanizmaları, kötü amaçlı yazılımlar, fiziksel güvenlik açıkları, insan hataları, yetersiz güvenlik politikaları ve düzenleyici ihlaller sayılabilir (Çankır, 2024). Disk yedekleri, yedekli sunucular, hataya dayanıklı sistemler, düzenli sistem yedekleri, antivirüs yazılımları ve güvenlik duvarı gibi önlemler ise erişilebilirliğin korunmasında önemli rol oynamaktadır (Öztürk, 2022).

1.5 Dijital Veri Güvenliği Farkındalığı

Dijital veri güvenliği, elektronik ortamlarda üretilen, depolanan, işlenen ve paylaşılan verilerin yetkisiz erişim, değiştirme, bozulma, ifşa edilme ya da yok edilme gibi tehditlere

karşı korunmasını amaçlayan teknik, idari ve davranışsal önlemler bütünüdür (Canbek ve Sağıroğlu, 2006). Veri güvenliği genel olarak gizlilik, bütünlük ve erişilebilirlik ilkeleri üzerine temellendirilmektedir. Gizlilik veriye yalnızca yetkili kişilerin erişebilmesini, bütünlük verinin doğruluğunun ve değişmezliğinin korunmasını, erişilebilirlik ise yetkili kullanıcıların ihtiyaç duyduklarında veriye ulaşabilmesini ifade etmektedir (Fussell, 2005). Bu üç ilke birbirini tamamlayan temel boyutlar olduğundan, herhangi birindeki zayıflık dijital veri güvenliğinin bütününe olumsuz etkileyebilmektedir.

Dijital veri güvenliği farkındalığı ise bireylerin dijital ortamlarda karşılaşılabilecekleri riskleri tanıma, bu risklere karşı uygun önlemler geliştirme ve güvenli dijital davranışlar sergileme yeterliği olarak tanımlanabilir. Bu farkındalık; güçlü parola kullanımı, iki faktörlü kimlik doğrulama, zararlı yazılımlara karşı korunma, güvenilmeyen bağlantılardan kaçınma, verilerin düzenli olarak yedeklenmesi, kişisel verilerin korunması ve sosyal mühendislik saldırılarına karşı dikkatli olunması gibi davranışları kapsamaktadır (Yılmaz vd., 2016). Siber güvenlik tehditlerinde insan faktörünün önemli bir zayıflık noktası olduğu dikkate alındığında, dijital veri güvenliği farkındalığı teknik güvenlik önlemlerini tamamlayan kritik bir unsur olarak değerlendirilmektedir.

Eğitim kurumlarında dijital veri güvenliği farkındalığı ayrı bir önem taşımaktadır. Okullarda öğrencilere ait kişisel bilgiler, akademik kayıtlar, dijital materyaller, çevrim içi etkinlik verileri ve iletişim kayıtları gibi çok sayıda hassas veri işlenmektedir. Bu verilerin güvenli biçimde korunmaması; öğrenci mahremiyetinin ihlali, kişisel verilerin yetkisiz kişilerle paylaşılması, siber zorbalık, kimlik hırsızlığı ve kurumsal güvenlik zafiyetleri gibi risklere yol açabilir. Bu nedenle öğretmenlerin dijital veri güvenliği farkındalıkları yalnızca bireysel teknoloji kullanımı açısından değil; öğrenci haklarının korunması, okul güvenliği ve etik sorumluluklar açısından da önemlidir (Serin, 2019).

Türkiye’de kişisel verilerin korunmasına ilişkin yasal düzenlemeler de eğitimcilerin dijital veri güvenliği konusundaki sorumluluklarını güçlendirmektedir. Kişisel Verilerin Korunması Kanunu, kişisel verilerin hukuka uygun biçimde işlenmesi, saklanması ve paylaşılmasına ilişkin temel ilkeleri belirlemektedir (KVKK, 2016). Buna göre öğretmenlerin, öğrencilerle ilgili görsel, yazılı ya da dijital içerikleri paylaşırken mahremiyet ve veri güvenliği ilkelerine uygun davranmaları gerekmektedir. Millî Eğitim Bakanlığı tarafından yapılan düzenlemeler de öğretmenlerin sosyal medya ve dijital platformlarda

öğrenci bilgilerinin paylaşımı konusunda dikkatli olmaları gerektiğini ortaya koymaktadır (MEB, 2017).

Yılmaz (2015) tarafından geliştirilen Dijital Veri Güvenliği Farkındalık Ölçeği (DVGFÖ), öğretmenlerin dijital veri güvenliğine ilişkin farkındalık düzeylerini belirlemeye yönelik önemli bir ölçme aracıdır. Ölçek; zararlı yazılımlar, parola güvenliği, güvenli internet kullanımı, veri yedekleme ve sosyal mühendislik saldırılarına karşı bilinçlilik gibi alanları kapsamaktadır. Geçerlik ve güvenilirlik çalışmaları sonucunda tek faktörlü ve 32 maddelik bir yapı elde edilmiş; ölçeğin öğretmenlerin dijital veri güvenliği farkındalıklarını ölçmede kullanılabilecek güvenilir bir araç olduğu belirtilmiştir (Yılmaz, 2015).

Dijital veri güvenliği farkındalığının öğretmenler özelinde incelenmesi, eğitimde güvenli teknoloji kullanımının geliştirilmesi açısından önemlidir. Öğretmenler dijital araçları yalnızca kendi mesleki uygulamalarında kullanmakla kalmamakta; öğrenciler için rol model olmakta ve onların dijital vatandaşlık becerilerinin gelişimini de etkilemektedir. Bu nedenle öğretmenlerin dijital veri güvenliği farkındalık düzeylerinin belirlenmesi, hem mesleki gelişim programlarının planlanmasına hem de okullarda güvenli dijital kültürün oluşturulmasına katkı sağlayabilir.

Teknolojinin sunduğu olanaklar dikkate alındığında; yalnızca teknolojiye erişim sağlamak değil, onu bilinçli, güvenli ve etik bir çerçevede kullanmak da günümüzün en önemli meselelerinden biri hâline gelmiştir. Sosyal medya, yapay zekâ ve büyük veri gibi alanların yaygınlaşmasıyla birlikte etik kaygılar derinleşmiş ve veri güvenliği ön plana çıkmıştır. Dijital dünyada mutlak güvenlik söz edilememekte; bu konudaki farkındalık eksikliği, güvenlik açıklarını büyüten bir etken olmaya devam etmektedir (Yılmaz vd., 2016).

Dijital veri güvenliği farkındalığı; bireylerin ve kurumların dijital ortamdaki olası tehditleri önceden tanıyarak bu tehditlere karşı proaktif önlemler alabilmesini sağlayan önemli bir yetkinlik alanıdır. Dijital tehditler çoğunlukla zarar yaşandıktan sonra fark edilmekte, bu durum telafisi güç kayıplara zemin hazırlamaktadır. Oysa dijital veri güvenliği farkındalığı, oluşabilecek maddi ve manevi zararları önleyici bir unsur olarak bireylerin erken dönemde harekete geçmesini sağlamaktadır (Yılmaz vd., 2016).

Dijital güvenlik farkındalığı, yalnızca teknik güvenlik önlemlerinin uygulanmasıyla sınırlı olmayıp bireylerin siber tehditler, veri ihlalleri, çevrim içi mahremiyet ve güvenli dijital davranışlar konusunda bilinçlenmesini de kapsamaktadır. Dijital okuryazarlık düzeyi, çevrim içi mahremiyet kaygıları ve siber güvenlik davranışları arasında anlamlı ilişkiler bulunduğu; siber güvenlik farkındalığının ise bu ilişkileri güçlendiren önemli bir değişken olduğu belirtilmektedir (Elrayah and Jamil, 2023).

Bilgi güvenliğine yönelik risklerin azaltılmasında teknolojik çözümler önemli olmakla birlikte insan faktörünün göz ardı edilmemesi gerekmektedir. Özellikle bireylerin bilgi güvenliği farkındalık düzeylerinin erken yaşlardan itibaren belirlenmesi ve geliştirilmesi, insan kaynaklı güvenlik risklerinin azaltılması açısından kritik görülmektedir. Nitekim Çetinkaya ve Öktelik (2022), ortaokul öğrencilerine yönelik bilgi güvenliği farkındalık ölçeği geliştirdikleri çalışmalarında, bilgi güvenliği farkındalığının erken yaşlarda ölçülmesi ve desteklenmesi gerektiğini vurgulamaktadır.

Dijital veri güvenliği farkındalığı yüksek bireyler, dijital ortamlarda daha güvenli davranış örüntüleri geliştirebilmekte; kişisel verilerini, çevrim içi hesaplarını ve bağlı oldukları kurumların dijital varlıklarını koruma konusunda daha bilinçli hareket edebilmektedir. İnsan faktörünün bilgi güvenliği açısından kritik bir zayıf nokta olabileceği ve veri ihlallerinin önlenmesinde güvenli kullanıcı davranışlarının önemli rol oynadığı ilgili alanyazında da belirtilmektedir (Hughes-Lartey et al., 2021; McMahon, 2020).

Türkiye İstatistik Kurumunun 2025 yılı Hanehalkı Bilişim Teknolojileri Kullanım Araştırması'na göre, Türkiye'de 16-74 yaş grubundaki bireylerde internet kullanım oranı 2024 yılında %88.8 iken 2025 yılında %90.9'a yükselmiştir. Cinsiyete göre değerlendirildiğinde, internet kullanım oranının erkeklerde %93.6, kadınlarda ise %88.2 olduğu görülmektedir. Aynı çalışmada, son 12 ay içinde özel amaçla resmi makamların web sitelerini veya uygulamalarını kullanan ve internet üzerinden kamu hizmetlerinden yararlanan bireylerin oranı %76.1 olarak açıklanmıştır. Bu oran erkeklerde %82.8, kadınlarda ise %69.5 düzeyindedir. E-devlet hizmetlerinden yararlanma oranı yaş gruplarına göre incelendiğinde, en yüksek kullanımın %92.8 ile 25-34 yaş grubunda, en düşük kullanımın ise %29.6 ile 65-74 yaş grubunda gerçekleştiği görülmektedir (Türkiye İstatistik Kurumu [TÜİK], 2025).

TÜİK verilerine göre bireylerin e-devlet hizmetlerini kullanma amaçları arasında ilk sırada %68.5 ile resmi makamlar veya kamu hizmetleri tarafından kendileri hakkında saklanan kişisel bilgilere erişim yer almaktadır. Bunu %53.6 ile kamu kurumlarından veya kamu hizmetlerinden randevu alma ya da rezervasyon yaptırma ve %46.4 ile kamu kuruluşlarına ait web sitelerinden bilgi edinme izlemektedir. Bununla birlikte, internet üzerinden mal veya hizmet satın alma ya da sipariş verme oranı 2024 yılında %51.7 iken 2025 yılında %55.7'ye yükselmiştir. Cinsiyete göre değerlendirildiğinde, çevrim içi alışveriş yapma oranının erkeklerde %59.1, kadınlarda ise %52.3 olduğu belirlenmiştir (TÜİK, 2025).

Araştırmada sosyal medya ve mesajlaşma uygulamalarının kullanımına ilişkin bulgular da dijital teknolojilerin gündelik yaşam pratikleri içerisindeki yaygınlığını ortaya koymaktadır. Buna göre bireylerin en fazla kullandıkları sosyal medya ve mesajlaşma uygulamaları sırasıyla %88.6 ile WhatsApp, %72.9 ile YouTube ve %68.1 ile Instagram'dır. Ayrıca internet üzerinden eğitim, mesleki veya özel amaçlı öğrenme faaliyeti gerçekleştiren bireylerin oranı 2025 yılında %17.7'ye yükselmiş; bu oran erkeklerde %17.5, kadınlarda ise %18.0 olarak gerçekleşmiştir (TÜİK, 2025).

Bu veriler, Türkiye'de dijital teknolojilerin bireylerin gündelik yaşamında giderek daha merkezi bir konuma yerleştiğini göstermektedir. İnternet, e-devlet, e-ticaret, sosyal medya ve çevrim içi öğrenme faaliyetlerindeki artış; bireylerin kişisel verilerini dijital ortamlarda daha yoğun biçimde paylaşımlarına, çevrim içi kimlik doğrulama süreçlerine daha sık dâhil olmalarına ve dijital platformlarda daha fazla etkileşim kurmalarına neden olmaktadır. Bu durum, hesap güvenliği, mahremiyet, kişisel veri koruma, çevrim içi alışveriş güvenliği ve kimlik doğrulama gibi alanlarda dijital güvenlik risklerinin daha görünür hâle gelmesine yol açmaktadır. Bu nedenle dijital veri güvenliği farkındalığının geliştirilmesi; yalnızca bireysel kullanıcı güvenliği açısından değil, kamu hizmetlerinin etkin kullanımı, eğitim kurumlarının dijital dönüşümü ve dijital ekonominin sürdürülebilirliği açısından da önemli bir gereklilik olarak değerlendirilebilir (Elrayah and Jamil, 2023; TÜİK, 2025).

Dijital teknolojilerin eğitim süreçlerinde giderek daha fazla kullanılması, dijital veri güvenliği farkındalığını eğitim kurumları ve öğretmenler açısından ayrıca önemli hâle getirmektedir. Öğrenme yönetim sistemleri, çevrim içi iletişim araçları, dijital ölçme ve değerlendirme uygulamaları ile öğrenci bilgilerinin işlendiği dijital platformlar, eğitim ortamlarında veri güvenliği konusunu daha görünür ve gerekli bir alan hâline getirmektedir.

Bu noktada öğretmenler, yalnızca dijital teknolojileri kullanan bireyler değil, aynı zamanda öğrencilerin güvenli ve bilinçli teknoloji kullanımına rehberlik eden temel eğitim paydaşları olarak değerlendirilebilir. Öğretmenlerin eğitim-öğretim süreçlerinde dijital veriler üretmeleri, saklamaları ve paylaşımları, onların dijital veri güvenliği farkındalık düzeylerinin hem bireysel hem de kurumsal güvenlik açısından önemli olduğunu göstermektedir (Yılmaz vd., 2016).

Sonuç olarak dijital veri güvenliği farkındalığı; bireylerin dijital tehditlere karşı yalnızca olay sonrasında tepki vermelerini değil, aynı zamanda riskleri önceden fark ederek önleyici ve bilinçli bir tutum geliştirmelerini sağlamaktadır. Bu nedenle dijital güvenlik farkındalığının erken yaşlardan itibaren eğitim yoluyla kazandırılması, siber güvenlik risklerinin azaltılması açısından önem taşımaktadır. Öğretmenlerin dijital veri güvenliğine ilişkin farkındalık düzeyleri ise yalnızca kendi dijital güvenliklerini değil, görev yaptıkları kurumları ve öğrencilerini de etkileyen önemli bir unsur olarak değerlendirilebilir. Bu çerçevede öğretmenlerin dijital veri güvenliği farkındalıklarının incelenmesi, eğitim ortamlarında güvenli dijital kültürün geliştirilmesine ve öğrencilerin bilinçli teknoloji kullanımı konusunda desteklenmesine katkı sağlayabilir (Çetinkaya ve Öktelik, 2022; Elrayah and Jamil, 2023; Yılmaz vd., 2016).

Eğitim alanında dijital veri güvenliği; öğrenci ve öğretmenlere ait kişisel bilgilerin, sınav sonuçlarının, akademik kayıtların, görsel-işitsel materyallerin ve dijital içeriklerin yetkisiz erişim, kötüye kullanım, değiştirme veya izinsiz paylaşım gibi tehditlere karşı korunmasını kapsamaktadır. Eğitim kurumlarında öğrencilerin kimlik bilgileri, aile bilgileri, fotoğrafları, sınav, karne ve not bilgileri ile adres bilgileri gibi pek çok kişisel verinin işlendiği dikkate alındığında, okullar dijital veri güvenliği açısından özel önem taşıyan kurumlardır (Bayar ve Korkmaz, 2022; KVKK, 2016). Dijital teknolojilerin eğitim süreçlerinde yaygın olarak kullanılması, bilginin üretimini ve saklanmasını kolaylaştırmakla birlikte güvenlik, gizlilik ve mahremiyet risklerini de artırmaktadır. Bu nedenle eğitim ortamlarında dijital veri güvenliğinin sağlanması ve öğretmenlerin bu konuda bilinçlendirilmesi önemli bir gereklilik olarak değerlendirilmektedir (Yılmaz vd., 2016; Öztürk ve Çakır, 2022).

FATİH Projesi, Türkiye’de eğitim sistemine bilgi ve iletişim teknolojilerini entegre etmeyi hedefleyen geniş ölçekli bir girişimdir. Proje; etkileşimli tahtalar, dijital içerikler ve eğitim teknolojileri aracılığıyla öğretme-öğrenme süreçlerini desteklemeyi amaçlamaktadır (Ekici

ve Yılmaz, 2013). Benzer biçimde Türkiye Yüzyılı Maarif Modeli'nde teknoloji entegrasyonu; öğrenci merkezli öğrenme, eleştirel düşünme, problem çözme ve küresel rekabetçilikle ilişkilendirilmekte, dijital yeterliklerin eğitim sistemindeki önemi vurgulanmaktadır (Ülçay, 2024). MEB'in "Okullarda Sosyal Medyanın Kullanılması" konulu genelgesinde ise okul ortamında çekilen öğrenci görüntülerinin ve videolarının internet siteleri veya sosyal medya ortamlarında paylaşılması konusunda kişisel verilerin korunması, çocuk hakları ve mahremiyet ilkelerine dikkat edilmesi gerektiği belirtilmiştir (MEB, 2017). Dolayısıyla öğretmenlerden yalnızca teknolojiyi kullanmaları değil, dijital verileri etik, güvenli ve hukuka uygun biçimde yönetmeleri de beklenmektedir.

Dijital ortamların eğitime giderek daha fazla entegre edilmesiyle birlikte öğrencilerin kişisel verilerinin korunmasında öğretmenlerin sorumluluğu artmaktadır. Öğretmenler; dijital materyal üretme, çevrim içi platform kullanma, öğrenci bilgilerini kaydetme ve sınıf içi etkinlikleri dijital ortamda paylaşma süreçlerinde veri güvenliği ilkelerine uygun hareket etmelidir. Yılmaz vd. (2016), öğretmenlerin artık bilgiyi dijital ortamlarda ürettiklerini ve sakladıklarını belirterek öğretmenlere ait dijital verilerin güvenliğinin önemine dikkat çekmektedir. Ayrıca öğretmenlerin; öğrencilere ait fotoğraf, video, sınav ve not bilgileri gibi verileri paylaşırken kişisel verilerin korunması ve mahremiyet ilkelerini gözetmeleri gerektiği vurgulanmaktadır (Bayar ve Korkmaz, 2022; KVKK, 2021).

Alanyazındaki bazı çalışmalar, öğretmenlerin sosyal medya ve dijital ortam kullanımlarında öğrenci mahremiyeti açısından riskli uygulamaların ortaya çıkabildiğini göstermektedir. Örneğin özel eğitim öğretmenlerinin sosyal medya paylaşımlarını inceleyen bir araştırmada, öğrencilerin yüz ve bedensel özelliklerinin çoğunlukla gizlenmediği ve bazı paylaşımlarda öğrenci adlarının açık biçimde yer aldığı belirlenmiştir (Ak vd., 2022). Benzer biçimde Serin (2019), sosyal medya ortamlarında çocuklara ait kişisel verilerin hukuka aykırı biçimde paylaşılmasının çocuk hakları ve mahremiyet açısından sorunlar doğurabileceğini belirtmektedir. Bu nedenle veri güvenliğinin sağlanmasında teknik önlemler kadar insan faktörü de belirleyici olup öğretmenlerin dijital veri güvenliği farkındalıklarının artırılması hem bireysel hem de kurumsal güvenlik açısından önemlidir (Hughes-Lartey et al., 2021; McMahon, 2020).

Öğretmenlerin sosyal medyada öğrenci fotoğrafı, adı, okul bilgisi veya sınıf içi görüntüleri paylaşması; mahremiyet ihlali, kimlik bilgilerinin kötüye kullanılması, siber zorbalık ve çocuk güvenliği açısından risk oluşturabilmektedir. Bayar ve Korkmaz (2022); eğitimcilerin,

öğrencilerin korunması gereken kişisel verileri arasında kimlik bilgilerini, fotoğrafları, videoları, sınav, karne ve not bilgileri ile adres bilgilerini saydıklarını; bu verilerin korunamamasının öğrencilerde alay edilme, siber zorbalığa maruz kalma, aşağılanma, güvensizlik ve akran baskısı gibi olumsuz sonuçlara yol açabileceğini ortaya koymuştur. KVKK'ya göre kişisel veri, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi kapsamaktadır; kişisel verilerin işlenmesi ise ancak hukuka uygun koşullarda ve gerekli durumlarda açık rıza temelinde gerçekleştirilebilmektedir (KVKK, 2016). Benzer şekilde GDPR kapsamında da kişisel veri, kimliği belirli veya belirlenebilir kişiye ilişkin her türlü bilgi olarak tanımlanmakta; fotoğrafın internet ortamında paylaşılması kişisel veri işleme faaliyeti kapsamında değerlendirilmektedir (Avrupa Komisyonu [European Commission], t.y.).

Siber zorbalık, öğrencilerin akademik, sosyal ve duygusal gelişimleri üzerinde ciddi etkiler oluşturabilmektedir. Kestel ve Akbıyık (2016), siber zorbalığa maruz kalan öğrencilerin korku, öfke, tedirginlik, uyku sorunları, sosyal ilişkilerde bozulma ve akademik başarıda düşüş gibi sorunlar yaşayabildiklerini ortaya koymuştur. MEB tarafından hazırlanan Siber Zorbalık Rehber Öğretmen/Psikolojik Danışman Kitapçığı'nda da siber zorbalığın çocuklar ve gençler açısından önemli bir risk alanı olduğu ve eğitim ortamlarında farkındalık çalışmalarının gerekliliği vurgulanmaktadır (MEB, 2021). Öğrenci fotoğrafları, okul bilgileri ve kişisel verilerin çevrim içi ortamlarda paylaşılması, öğrencilerin dijital ayak izlerini de kalıcı hâle getirebilmektedir. Dijital ayak izi farkındalığı; bireylerin çevrim içi ortamlarda bıraktıkları verilerin uzun süreli etkilerini anlamaları ve bu izleri bilinçli biçimde yönetmeleri açısından önem taşımaktadır (Arslankara ve Seferoğlu, 2019; Koçyiğit ve Özkul, 2023).

Dijital materyallerin eğitimde giderek daha yaygın kullanılması; telif hakkı ihlalleri, içeriklerin izinsiz çoğaltılması, veri sızıntısı ve zararlı yazılım bulaşması gibi riskleri de beraberinde getirmektedir. Özellikle okullarda ders materyallerinin taşınabilir bellekler aracılığıyla farklı bilgisayarlar ve etkileşimli tahtalar arasında aktarılması, kötü amaçlı yazılımların yayılması açısından önemli bir güvenlik riski oluşturabilmektedir. USB belleklerin veri aktarımında pratik araçlar olmasına karşın veri sızıntısı ve zararlı yazılım bulaşması gibi riskler taşıdığı; bu nedenle güvenilir olmayan taşınabilir belleklerin kullanılmaması, belleklerin taranması ve kurumsal güvenlik politikalarının uygulanması gerektiği belirtilmektedir (Ulusal Standartlar ve Teknoloji Enstitüsü (National Institute of

Standards and Technology [NIST]), 2025; Ontario Institute for Studies in Education, t.y.). Bu bağlamda, eğitim sürecinin temel unsurlarından biri olan öğretmenlerin dijital materyalleri güvenli biçimde kullanmaları ve dijital veri güvenliği konusunda farkındalık sahibi olmaları, eğitimde dijitalleşme sürecinin sağlıklı ve sürdürülebilir biçimde yürütülmesi açısından önem taşımaktadır.

MEB'in köklü girişimlerinden biri olan Milli Eğitimi Geliştirme Projesi (MEGP), OECD üyesi ülkelerin iş birliğiyle yürütülen kapsamlı bir reform ve yeniden yapılanma sürecini ifade etmekte olup 10 Temmuz 1990 tarih ve 20570 sayılı Resmî Gazete'de yayımlanarak yürürlüğe girmiştir. Proje kapsamında 208 Müfredat Laboratuvar Okulu (MLO); bilgisayar, yazıcı, tarayıcı, televizyon, video kamera ve tepegöz gibi eğitim araçlarıyla donatılmış; müzik, resim, bilgisayar ve fen laboratuvarları ile kütüphaneler ve öğretmen çalışma odaları oluşturulmuştur. MLO'lar, geliştirilen öğretim programlarının ve yeni eğitim yaklaşımlarının sisteme geçirilmeden önce denendiği ve teknolojik yeniliklerin eğitime kazandırıldığı pilot kurumlardır. Bu okullar, pilot uygulama deneyimleriyle sisteme liderlik yapma işlevi üstlenmiştir (Sönmez, 2005).

MEB'in eğitimde teknoloji entegrasyonuna yönelik bir diğer kapsamlı projesi FATİH Projesi'dir. Projenin temel amacı; bilişim teknolojisi araçlarının öğrenme-öğretme sürecinde daha fazla duyu organına hitap edecek biçimde etkin kullanımını sağlayarak eğitimde fırsat eşitliğini güvence altına almaktır. FATİH Projesi beş ana bileşenden oluşmaktadır (FATİH Projesi, 2012). Projenin “bilinçli, güvenli ve yönetilebilir BT kullanımının sağlanması” bileşeni kapsamında eğitim yöneticileri ve öğretmenler “Bilişim Teknolojilerinin ve İnternetin Bilinçli, Güvenli Kullanımı Seminerleri”ne katılmaktadır. Dijital veri üzerine kurgulanan FATİH Projesi için dijital veri güvenliği bu nedenle büyük bir öneme sahiptir. Öğretmenlerin dijital ortamları etkin kullanabilmelerinin yanı sıra bu ortamlarda güvenlik ve gizlilik konularında da yeterli bilgiye sahip olmaları gerekmektedir; aksi durumda hem kendi verileri hem de öğrencilerin verileri risk altına girebilmektedir (Öztürk, 2022).

Öğretmen Yetiştirme ve Geliştirme Genel Müdürlüğü (ÖYGGM) tarafından hazırlanan ilgili hizmet içi eğitim programının amaçları arasında “İnterneti bilinçli ve güvenli kullanır” ve “İnternet üzerinde yayımlanan ders etkinliklerinde kullanabileceği materyalleri arar, bulur ve telif haklarına uygun olarak seçer” ifadeleri yer almaktadır (ÖYGGM, 2013a). ÖYGGM tarafından hazırlanan örnek hizmet içi eğitim programlarında, ikinci seviye modül

programları içinde yer alan “Eğitimde Bilişim Teknolojilerinin Kullanımı Kursu” üniteleri şunlardır (ÖYGGM, 2013b):

- Bilgi teknolojisi bileşenleri
- İnterneti etkin kullanma
- Etkili sunum teknikleri
- Bilişim teknolojilerini kullanarak ders işleme

MEB kapsamında öğretmenlere yönelik dijital yetkinlik, kişisel verilerin korunması ve yazılım güvenliği gibi eğitimler bulunmakla birlikte; dijital veri güvenliği farkındalığının öğretmenler açısından ayrı ve güçlendirilmesi gereken bir alan olduğu görülmektedir. Öğretmenlerin dijital ortamlarda bilgi üretme ve saklama süreçleri dikkate alındığında, dijital veri güvenliği farkındalığının mesleki gelişim eğitimlerinde daha etkili ve uygulamaya dönük biçimde ele alınması önem taşımaktadır (Avcı ve Arslan, 2019; Yılmaz vd., 2016).

1.6 Problem Durumu

Eğitimde dijital teknolojilerin yaygınlaşması, öğretmenlerin mesleki yeterliklerinin yalnızca alan bilgisi ve pedagojik bilgiyle sınırlı olmadığını; teknolojiyi öğretim süreçlerine uygun, etkili ve bilinçli biçimde bütünleştirme yeterliğini de kapsadığını göstermektedir. Öğretmenlerin teknoloji yeterlikleri, dijital araçları kullanma becerisinin ötesinde; bu araçları pedagojik amaçlarla kullanma, dijital öğrenme ortamları tasarlama ve öğrencilerin teknoloji destekli öğrenme süreçlerine rehberlik etme becerilerini içermektedir (Ertmer and Ottenbreit-Leftwich, 2010; Koehler and Mishra, 2005; Mishra and Koehler, 2006). Bu nedenle öğretmenlerin teknoloji yeterliği öz-değerlendirme düzeylerinin belirlenmesi, eğitimde teknoloji entegrasyonunun niteliğini ortaya koymak açısından önemli görülmektedir (Christensen and Knezek, 2017; Fidan vd., 2020).

Bununla birlikte dijital teknolojilerin eğitim ortamlarında yoğun biçimde kullanılması, veri güvenliği konusunu öğretmenlik mesleği açısından önemli bir sorumluluk alanı hâline getirmiştir. Öğretmenler, görevleri gereği öğrencilere ait kişisel bilgiler, akademik kayıtlar, dijital materyaller, çevrim içi öğrenme platformları ve okul yönetim sistemleriyle sürekli etkileşim içerisinde. Bu durum, öğretmenlerin yalnızca teknolojiyi kullanabilmelerini değil, aynı zamanda dijital verileri güvenli, etik ve bilinçli biçimde yönetebilmelerini de gerekli kılmaktadır. Dijital ortamlarda ortaya çıkan zararlı yazılımlar, veri güvenliği ihlalleri,

sosyal mühendislik saldırıları ve çeşitli güvenlik riskleri, dijital veri güvenliği farkındalığının öğretmenler açısından kritik bir yeterlik alanı olduğunu göstermektedir (Canbek ve Sağıroğlu, 2006, 2007a, 2007b; Tekerek, 2008; Yılmaz vd., 2016).

Alanyazında öğretmenlerin teknoloji yeterliklerini ya da dijital veri güvenliği farkındalıklarını ayrı ayrı ele alan çalışmalar bulunmakla birlikte, bu iki değişkeni aynı araştırma kapsamında birlikte inceleyen çalışmaların sınırlı olduğu görülmektedir. Öğretmenlerin teknoloji kullanımına ilişkin yeterlikleri çeşitli demografik ve mesleki değişkenler açısından incelenmiş; bazı çalışmalarda cinsiyet, eğitim düzeyi, branş, mesleki deneyim ve hizmet içi eğitim alma durumu gibi değişkenlerin teknoloji yeterlikleriyle ilişkili olabildiği belirlenmiştir (Durak ve Seferoğlu, 2017; Karadeniz ve Vatanartıran, 2015). Benzer biçimde, öğretmenlerin dijital veri güvenliği farkındalıklarının da çeşitli değişkenlere göre farklılaşabildiği ortaya konulmuştur (Yılmaz vd., 2016). Ancak teknoloji yeterliği öz-değerlendirmesi ile dijital veri güvenliği farkındalığı arasındaki ilişkinin yeterince açıklığa kavuşmamış olması, bu araştırmanın temel çıkış noktasını oluşturmaktadır.

Teknolojiyi etkili kullandığını düşünen bir öğretmenin dijital veri güvenliği konusunda da yeterli farkındalığa sahip olup olmadığı ayrıca incelenmesi gereken bir durumdur. Bu nedenle öğretmenlerin 21. Yüzyıl Öğrenmeleri İçin Teknoloji Yeterliği Öz-Değerlendirme Ölçeği (YYÖTYÖ) puanları ile Dijital Veri Güvenliği Farkındalık Ölçeği (DVGFO) puanları arasındaki ilişkinin belirlenmesi, öğretmenlerin dijital çağdaki mesleki yeterliklerinin daha bütüncül biçimde değerlendirilmesine katkı sağlayacaktır. Ayrıca cinsiyet, görev türü, eğitim düzeyi, mesleki kıdem, bilgisayar sahipliği, dijital güvenlikle ilgili ders/kurs alma durumu ve 21. yüzyıl becerileri kavramını bilme durumu gibi değişkenlerin bu iki yeterlik alanı üzerindeki etkisinin incelenmesi, öğretmenlerin mesleki gelişim gereksinimlerinin daha somut biçimde ortaya konulmasına yardımcı olabilir.

Bu bağlamda araştırmanın problem durumunu; öğretmenlerin teknoloji yeterliği öz-değerlendirme ve dijital veri güvenliği farkındalık düzeylerinin belirlenmesi, bu düzeylerin belirlenen değişkenlere göre anlamlı biçimde farklılaşıp farklılaşmadığının incelenmesi ve öğretmenlerin YYÖTYÖ puanları ile DVGFO puanları arasında istatistiksel olarak anlamlı bir ilişki bulunup bulunmadığının ortaya konulması oluşturmaktadır. Araştırmadan elde edilecek bulguların, öğretmenlerin teknoloji kullanımı ve dijital veri güvenliği alanındaki

mesleki gelişim ihtiyaçlarının belirlenmesine ve hizmet içi eğitim programlarının daha hedefli biçimde planlanmasına katkı sağlayacağı düşünülmektedir.

1.7 Araştırmanın Problemleri

Bu araştırmanın problemleri aşağıda verilmiştir:

1. Öğretmenlerin teknoloji yeterliği öz-değerlendirme ve dijital veri güvenliği farkındalık düzeyleri nedir?
2. Öğretmenlerin teknoloji yeterliği öz-değerlendirmeleri ile dijital veri güvenliği farkındalıkları cinsiyet, görev türü, eğitim düzeyi, mesleki kıdem, bilgisayar sahipliği, dijital güvenlikle ilgili ders/kurs alma ve 21. yüzyıl becerileri kavramını bilme durumu değişkenlerine göre anlamlı olarak farklılaşmakta mıdır?
3. Öğretmenlerin teknoloji yeterliği öz-değerlendirmeleri ile dijital veri güvenliği farkındalıkları arasında istatistiksel olarak anlamlı bir ilişki var mıdır?

1.8 Araştırmanın Amacı

Bu araştırmanın amacı MEB'e bağlı devlet okullarında görev yapan öğretmenlerin teknoloji yeterliği öz-değerlendirme düzeylerini ve dijital veri güvenliği farkındalık düzeylerini belirlemek ve bu iki değişken arasındaki ilişkiyi ortaya koymaktır. Araştırmanın bu temel amacı çerçevesinde öğretmenlerin söz konusu düzeylerinin cinsiyet, görev türü, eğitim düzeyi, mesleki kıdem, bilgisayar sahipliği, dijital güvenlikle ilgili ders/kurs alma ve 21. yüzyıl becerileri kavramını bilme durumu değişkenleri açısından anlamlı biçimde farklılaşıp farklılaşmadığının incelenmesi de amaçlanmaktadır.

1.9 Araştırmanın Önemi

21. yüzyılda eğitim sistemlerinin karşı karşıya kaldığı en büyük güçlüklerden biri hızla değişen teknolojik gerçekliğe uyum sağlayabilen, öğrencilerine dijital yetkinlikler kazandırabilen ve aynı zamanda dijital ortamdaki tehditlere karşı bilinçli bir profil sergileyen öğretmenler yetiştirmektir. Bu bağlamda öğretmenlerin teknoloji yeterliği öz-değerlendirmeleri ile dijital veri güvenliği farkındalıklarının birlikte incelenmesi eğitim alanındaki karar vericiler, hizmet içi eğitim programcıları ve alan araştırmacıları için önemli veriler sunma imkanı sunmaktadır.

Teorik açıdan bu araştırma teknoloji yeterliği öz-değerlendirmesi ile dijital veri güvenliği farkındalığı arasındaki ilişkiyi ilk kez veriye dayalı olarak sistematik biçimde inceleyen

alışmalardan biri olma özelliđi taşımaktadır. YYÖTYÖ ve DVGFÖ'nün aynı örneklem üzerinde birlikte kullanılması, alanyazındaki bu boşluđın doldurulmasına katkı sağlayacağı düşünülmektedir. Nitekim teknoloji yeterliđi yüksek bireylerin dijital güvenlik farkındalıklarının da yüksek olabileceđine dair teorik çıkarımlar, bu araştırmanın bulgularıyla deneysel bir zemine kavuşturulabilir.

Pratik açıdan ise araştırmanın bulguları MEB'in öğretmen eğitimi politikalarına, hizmet içi eğitim program içeriklerine ve dijital güvenlik farkındalıđı kampanyalarına yön verebilir. Özellikle hangi demografik gruplardaki öğretmenlerin daha düşük teknoloji yeterliđi öz-değerlendirmesi ve dijital veri güvenliđi farkındalıđı sergilediđinin belirlenmesi müdahale programlarının öncelikli hedef kitlelerinin dođru biçimde tanımlanmasına katkı sağlayabilir. Bunun yanı sıra araştırma bulguları FATİH Projesi, Eğitim Bilişim Ađı (EBA) ve Öğretmen Bilişim Ađı (ÖBA) gibi eğitim teknolojisi girişimlerinin etkinliđini değerlendirmeye yönelik tartışmalara da katkı sunabilir.

Son olarak öğretmenlerin teknoloji yeterliđi öz-değerlendirmelerinin ve dijital veri güvenliđi farkındalıklarının artırılması yalnızca bireysel düzeyde deđil kurumsal ve ulusal düzeyde de dijital güvenlik kültürünün oluşmasına katkı sağlayabilir. Öğretmenlerin bu konudaki yetkinliklerini geliştirmeleri öğrencilerine de güvenli dijital davranış örüntüleri kazandırmaları açısından önemli bir rol üstlenmelerini mümkün kılabilir.

1.10 Araştırmanın Sınırlılıkları

Araştırma, aşağıda yer verilen sınırlılıklar kapsamında gerçekleştirilmiştir:

- Araştırma, 2025-2026 eğitim-öğretim yılında MEB'e bađlı devlet okullarında görev yapan ve araştırmaya gönüllü olarak katılan 307 öğretmenin verileriyle sınırlıdır.
- Araştırmanın verileri, kullanılan veri toplama araçları olan YYÖTYÖ ve DVGFÖ'nün ölçmeyi hedeflediđi deđişkenlerle sınırlıdır.
- Katılımcıların ölçeklere verdikleri yanıtların kendi gerçek görüş ve değerlendirmelerini yansıttıđı varsayılmaktadır ve bu durum öznel yanlılık riskini beraberinde taşımaktadır.

1.11 Araştırmanın Sayıtları

Bu araştırma aşağıdaki temel sayıtlar üzerine kurgulanmıştır:

- Katılımcıların veri toplama araçlarındaki sorulara içtenlikle yanıt verdikleri ve gerçek duygu ile düşüncelerini yansıttıkları varsayılmaktadır.
- Araştırmada kullanılan ölçme araçlarının (YYÖTYÖ ve DVGFÖ) geçerlik ve güvenilirlik çalışmaları tamamlanmış olup bu araçların araştırmanın örnekleminde de geçerli ve güvenilir ölçümler sağladığı kabul edilmektedir.
- Veri toplama sürecinde katılımcıların birbirlerinden bağımsız biçimde yanıt verdikleri varsayılmaktadır.

1.12 Tanımlar

- **Teknoloji Yeterliği Öz-Değerlendirmesi:** Öğretmenlerin e-posta kullanımı, WWW, entegre uygulamalar ve teknolojiyle öğretim boyutlarındaki teknoloji yeterliklerini kendi algıları aracılığıyla değerlendirmeleri (Fidan vd., 2020).
- **Dijital Veri Güvenliği Farkındalığı:** Bireylerin dijital ortamdaki tehditleri (zararlı yazılımlar, kimlik avı saldırıları, zayıf parola kullanımı vb.) önceden tanıyarak bu tehditlere karşı proaktif önlemler alabilme düzeyi (Yılmaz, 2015).
- **Teknoloji Yeterliği:** Öğretmenlerin teknolojiyi pedagojik hedeflerle bütünleştirme, dijital öğrenme ortamları tasarlama ve teknolojiyi işlevsel biçimde kullanma kapasitesi (Mishra and Koehler, 2006).
- **Dijital Veri Güvenliği:** Elektronik ortamlarda üretilen, depolanan ve iletilen verileri yetkisiz erişim, değiştirme, bozulma ve yok etme gibi tehditlere karşı koruma altına almayı amaçlayan teknik ve idari önlemlerin bütünü (Canbek ve Sağiroğlu, 2006).
- **21. Yüzyıl Becerileri:** Bireylerin 21. yüzyılda eğitim ve iş hayatında başarılı olabilmeleri için sahip olmaları gereken iletişim, iş birliği, eleştirel düşünme, yaratıcılık, teknoloji okuryazarlığı ve dijital güvenlik gibi yetkinliklerin bütünü (P21, 2017).
- **YYÖTYÖ:** Fidan vd. (2020) tarafından Türkçeye uyarlanan, dört faktörlü (E-posta, WWW, Entegre Uygulamalar, Teknolojiyle Öğretim) ve 24 maddeden oluşan, beşli likert tipinde 21. yüzyıl öğrenmelerinde teknoloji yeterliği öz-değerlendirmesi ölçeğidir.
- **DVGFÖ:** Yılmaz (2015) tarafından geliştirilen, tek faktörlü ve 32 maddeden oluşan, beşli likert tipinde dijital veri güvenliği farkındalık ölçeğidir.

2. ALANYAZIN İNCELEMESİ

2.1 Teknoloji Yeterliği Öz-Değerlendirmesi ile İlgili Alanyazın

Bu bölümde bireylerin teknoloji yeterliği öz-değerlendirmeleriyle ilgili ulusal ve uluslararası araştırmalar kronolojik bir sıra izlenerek ele alınmıştır. İlgili alanyazın incelendiğinde, çalışmaların ilköğretim öğrencilerinden öğretmen adaylarına ve görevdeki öğretmenlere kadar farklı örneklem gruplarıyla yürütüldüğü görülmektedir. Araştırmalarda teknoloji yeterliği; dijital okuryazarlık, yaşam boyu öğrenme, akademik başarı, öğrenci bağlılığı ve 21. yüzyıl becerileri gibi değişkenlerle birlikte değerlendirilmiştir. Ayrıca teknoloji yeterliğinin belirlenmesinde TPSA C-21 gibi ölçme araçlarının kullanıldığı; Fen, Teknoloji, Mühendislik ve Matematik (Science, Technology, Engineering and Mathematics [STEM]), artırılmış gerçeklik, ters yüz öğrenme ve bağlantılı öğrenme gibi çağdaş yaklaşımların da bu becerilerin geliştirilmesinde ele alındığı görülmektedir. Bu doğrultuda incelenen çalışmaların amaçları, örneklem grupları, yöntemleri ve ulaşılan temel bulgular aşağıda özetlenmiştir.

Gülen (2013), Ankara ilinde altı farklı okulda öğrenim gören 612 ortaokul öğrencisiyle yürüttüğü çalışmada, öğrencilerin 21. yüzyıl öğrenme becerilerine sahip olma düzeyleri ile bu becerileri BT (Bilişim Teknolojileri) aracılığıyla destekleme düzeyleri arasındaki ilişkiyi araştırmıştır. Bulgular, öğrencilerin 21. yüzyıl becerileri olan aktif öğrenme, problem çözme, öğrenmeyi öğrenme, iş birliği ve iletişime iyi düzeyde sahip olduğunu; ancak bu becerileri BT ile destekleme düzeylerinin orta seviyede kaldığını ortaya koymuştur. İki değişken arasında pozitif yönlü anlamlı bir ilişki saptanmış, sınıf düzeyi yükseldikçe teknoloji kullanım yeterliklerinin arttığı belirlenmiştir.

Christensen and Knezek (2017), TPSA C-21 ölçeğinin geçerlik ve güvenirlik çalışmasını gerçekleştirmiştir. Çalışmada ölçeğin hizmet öncesi ve hizmet içi öğretmenlerin teknoloji entegrasyonuna yönelik öz-yeterliklerini belirlemede kullanılabilecek geçerli ve güvenilir bir ölçme aracı olduğu ortaya konmuştur. Ölçek; e-posta, WWW, bütünsel uygulamalar, teknolojiyle öğretim, gelişen teknolojilerle öğretim ve gelişen teknoloji becerileri olmak üzere alt boyutlardan oluşmaktadır (Christensen and Knezek, 2017).

Kozikoğlu ve Altunova (2018), Van Yüzüncü Yıl Üniversitesi Eğitim Fakültesi'nde öğrenim gören 400 öğretmen adayının 21. yüzyıl becerilerine ilişkin öz-yeterlik algılarının yaşam

boyu öğrenme eğilimlerini yordayıp yordamadığını araştırmıştır. Katılımcıların yaşam boyu öğrenme eğilimlerinin çok yüksek, 21. yüzyıl becerilerine ilişkin öz-yeterlikleri ile yaşam boyu öğrenme eğilimleri arasındaki ilişkinin ise pozitif yönlü ve anlamlı olduğu saptanmıştır. Öğrenme ve yenilenme becerileri ile yaşam ve kariyer becerilerinin yaşam boyu öğrenme eğilimlerini anlamlı düzeyde açıkladığı belirlenmiş; cinsiyet değişkeninin 21. yüzyıl becerilerine ilişkin öz-yeterlikte anlamlı farklılık yaratmadığı ancak yaşam boyu öğrenme eğilimini etkilediği ortaya konmuştur.

Önür (2018), Van ilindeki 920 ortaokul öğrencisiyle gerçekleştirdiği çalışmada öğrencilerin 21. yüzyıl öğrenme becerileri ile eğitim teknolojisi yeterliklerini incelemiştir. Öğrencilerin her iki alanda da yüksek düzeyde yeterliğe sahip olduğu; dijital vatandaşlık ve katılım yeterliğinin orta düzeyde kaldığı tespit edilmiştir. Bilgisayar, tablet ve akıllı telefon gibi dijital araçlara erişim olanağı olan öğrencilerin her iki alanda da anlamlı düzeyde daha yüksek puan aldığı belirlenmiş; 21. yüzyıl öğrenme becerileri ile eğitim teknolojisi yeterlikleri arasında orta düzeyde pozitif yönlü ve anlamlı bir ilişki saptanmıştır. Ayrıca eğitim teknolojisi yeterliklerinin 21. yüzyıl öğrenme becerilerinin yaklaşık dörtte birini (%25.1) yordayabildiği bulunmuştur.

Arslan (2020), İngilizce ve Sosyal Bilgiler öğretmen adaylarının pandemi öncesi ve pandemi sonrası dönemde öğrencilere kazandırılması gereken 21. yüzyıl becerilerine ilişkin görüşlerinin değişimini mobil teknolojiler aracılığıyla boylamsal bir yaklaşımla incelemiştir. Pandemi sonrası süreçte bilgiye erişim farkındalığının arttığı, eleştirel düşünme ve adaptasyon becerilerine yönelik vurgunun güçlendiği saptanmıştır.

Aydemir vd. (2020), İnönü Üniversitesi Eğitim Fakültesi Sosyal Bilgiler Öğretmenliği öğrencilerinden oluşan örnekleme öğretmen adaylarının 21. yüzyıl öğrenen ve öğretme becerilerine sahip olma düzeylerini incelemiştir. Çalışmada Mann Whitney U ve Kruskal-Wallis testleri kullanılmış; öğrenen becerilerinden otonom ve öğretme becerilerinden esnek öğretme becerilerinin sınıf düzeyine göre anlamlı biçimde farklılaştığı belirlenmiştir.

Erten (2020), Bingöl Üniversitesi'nde pedagojik formasyon eğitimi alan öğretmen adaylarının 21. yüzyıl becerilerine ilişkin yeterlik algılarını ve bu becerilerin demografik değişkenlere göre farklılaşıp farklılaşmadığını araştırmıştır. Öğretmen adaylarının 21. yüzyıl becerilerine yeterli düzeyde sahip olduğu; cinsiyet ve öğrenim alanına göre anlamlı farklılık

bulunmadığı ancak BİT (Bilgi ve İletişim Teknolojileri) yeterliliğinin 21. yüzyıl becerilerinin kazanımında belirleyici olduğu sonucuna ulaşılmıştır.

Woods (2020), Amerika Birleşik Devletleri'nde lise öğretmenleriyle gerçekleştirdiği doktora tezinde, öğretmenlerin teknoloji yeterlikleri ile kuşak, cinsiyet ve branş değişkenleri arasındaki ilişkiyi incelemiştir. Araştırmada öğretmenlerin 21. yüzyıl teknoloji araçlarını kullanma yeterlikleri 34 maddelik TPSA C-21 ölçeği ile ölçülmüştür. Bulgular, cinsiyet ve kuşak değişkenlerinin TPSA C-21'in bazı alt boyutlarında öğretmenlerin teknoloji yeterliklerini anlamlı biçimde yordadığını; branş değişkeninin ise anlamlı bir yordayıcı olmadığını göstermiştir.

Woods et al. (2021), Amerika Birleşik Devletleri'nde ortaöğretim öğretmenlerinin teknoloji yeterliklerini TPSA C-21 ölçeğiyle incelemiştir. Çalışmada cinsiyet ve kuşak değişkenlerinin ölçeğin toplam puanı ile WWW, bütünsel uygulamalar ve gelişen teknoloji becerileri alt boyutlarında anlamlı yordayıcılar olduğu; branş değişkeninin ise teknoloji yeterliği puanlarını anlamlı biçimde yordamadığı belirlenmiştir.

Sharma and Nazir (2021), Avrupa ve Birleşik Krallık'taki denizcilik eğitimi veren öğretim elemanlarının teknoloji öz-yeterliklerini TPSA C-21 ölçeğiyle incelemiştir. Araştırmada katılımcıların e-posta, web kullanımı, bütünsel uygulamalar, teknolojiyle öğretim ve gelişen teknolojilerle öğretim boyutlarındaki yeterlik algıları değerlendirilmiş; özellikle gelişen teknolojilerle öğretim boyutunda gelişime ihtiyaç olduğu sonucuna ulaşılmıştır (Sharma and Nazir, 2021).

Yıldırım (2021), Anadolu Üniversitesi Açıköğretim Fakültesi'nde öğrenim gören 2784 öğrencinin 21. yüzyıl öğrenme becerileri ile açık ve uzaktan eğitim ortamlarındaki bağıllık düzeyleri arasındaki ilişkiyi incelemiştir. 21. yüzyıl öğrenme becerileri arttıkça öğrenci bağıllığının da arttığı tespit edilmiştir. 21. yüzyıl öğrenme becerileri ile açık ve uzaktan eğitim ortamlarındaki bağıllık düzeylerinin yaş, cinsiyet, öğrenim kademesi ve medeni durum değişkenlerine göre anlamlı farklılık olduğu belirlenmiştir.

Uzun (2022), Karaman ilinde bir ilkokulun üçüncü sınıf öğrencileriyle yürüttüğü karma yöntem araştırmasında bağlantılı öğrenme yaklaşımı ile STEM etkinliklerinin 21. yüzyıl becerileri, dijital medya okuryazarlığı ve sosyal girişimcilik niyeti üzerindeki etkisini

incelemiştir. Bağlantılı öğrenme ve STEM uygulamalarının öğrencilerin 21. yüzyıl becerilerini ve dijital okuryazarlıklarını anlamlı düzeyde olumlu etkilediği belirlenmiştir.

Eken (2023), bir devlet üniversitesinin eğitim fakültesinde ters yüz öğrenme modeline dayalı öğretim sürecinin öğretmen adaylarının akademik başarı, eleştirel düşünme, iletişim becerileri ve dijital okuryazarlık üzerindeki etkisini karma araştırma yöntemiyle incelemiştir. Deney grubundaki öğretmen adaylarının söz konusu becerilerin tamamında istatistiksel olarak anlamlı artış gösterdiği, dijital okuryazarlık düzeylerinin de kontrol grubuna kıyasla anlamlı biçimde yükseldiği saptanmıştır.

Esteban et al. (2023), Filipinler’de öğretmen adaylarının teknoloji yeterlik düzeyleri ile akademik stres düzeyleri arasındaki ilişkiyi incelemiştir. Araştırmada öğretmen adaylarının teknoloji yeterlikleri TPSA C-21 ölçeği ile, akademik stres düzeyleri ise Akademik Stres Algıları ölçeği ile ölçülmüştür. Bulgular, öğretmen adaylarının teknoloji yeterliklerinin yüksek düzeyde olduğunu ve teknoloji yeterliği ile akademik beklentilere bağlı stres ve iş/sınav stresi arasında anlamlı ilişkiler bulunduğunu göstermiştir.

Oruçoğlu (2023), proje temelli bir ders ortamında çevik yaklaşım süreçlerinden yararlanan 41 Bilgisayar ve Öğretim Teknolojileri Eğitimi son sınıf öğrencisinin 21. yüzyıl becerileri öz-yeterlik algılarını karma yöntem durum çalışması deseniyle incelemiştir. Tasarlanan öğrenme ortamının öğretmen adaylarının 21. yüzyıl becerileri öz-yeterlik algılarını geliştirdiği ve grup çalışmasına olumlu katkı sağladığı bulunmuştur.

Okur-Türk (2024), Erzurum’daki 400 öğretmenle yürüttüğü araştırmasında YYÖTYÖ kullanarak öğretmenlerin 21. yüzyıl öğrenmeleri için teknoloji yeterliği öz-değerlendirmeleri ile yapılandırmacı yaklaşımı uygulamaya yönelik öz-yeterlikleri arasındaki ilişkiyi incelemiştir. Öğretmenlerin 21. yüzyıl teknoloji yeterliği öz-değerlendirme düzeylerinin çok yüksek olduğu; yaş ve görev yılının 21. yüzyıl teknoloji yeterliği öz-değerlendirmeleri üzerinde anlamlı farklılık yaratan değişkenler olduğu ortaya konmuştur. 21. yüzyıl öğrenmeleri için teknoloji yeterliği öz-değerlendirmeleri ile yapılandırmacı yaklaşımı uygulamaya yönelik öz-yeterlikleri arasında pozitif yönlü orta düzeyde anlamlı bir ilişki saptanmış; YYÖTYÖ puanlarının yapılandırmacı yaklaşımı uygulamaya yönelik öz-yeterliğin yaklaşık %9.4’ünü yordayabildiği belirlenmiştir.

Polat (2024), sosyal bilgiler öğretmen adaylarıyla gerçekleştirdiği yarı deneysel çalışmada AR uygulamalarının 21. yüzyıl öğrenme becerilerine etkisini incelemiştir. AR uygulamalarının öğrenci başarısını ve 21. yüzyıl yeterliklerini anlamlı ölçüde geliştirdiği; AR başarıları ile 21. yüzyıl yeterlikleri arasında orta düzeyde pozitif yönlü bir ilişki bulunduğu saptanmıştır.

Yu and Lwin (2024), Myanmar’da eğitim kolejlerinde görev yapan öğretmen eğitimcilerinin teknolojik bilgileri ile teknoloji öz-yeterlikleri arasındaki ilişkiyi incelemiştir. Araştırmada öğretmen eğitimcilerinin teknoloji öz-yeterliklerini belirlemek amacıyla TPSA C-21 ölçeği kullanılmıştır. Çalışma sonucunda teknolojik bilgi ile teknoloji öz-yeterliği arasında yüksek düzeyde pozitif ve anlamlı bir ilişki olduğu; teknolojik bilginin teknoloji öz-yeterliğini önemli ölçüde yordadığı belirlenmiştir.

Şahin (2025), Afyonkarahisar ilindeki 711 ilkokul öğrencisiyle yürüttüğü çalışmasında dijital okuryazarlık becerileri ile 21. yüzyıl öğrenme deneyimi algıları arasındaki ilişkiyi incelemiştir. Her iki değişkenin de orta düzeyde olduğu; dijital okuryazarlık ile 21. yüzyıl öğrenme deneyimi algısının alt boyutları arasında pozitif yönlü düşük ile orta düzeyde ilişkiler bulunduğu saptanmıştır. Bilgisayara sahip olan öğrencilerin teknik bilgi ve 21. yüzyıl öğrenme deneyimi algılarının bilgisayarı olmayanlara kıyasla anlamlı düzeyde daha yüksek olduğu belirlenmiştir.

İlgili araştırmalar birlikte değerlendirildiğinde, öğrenciler ve öğretmen adaylarının 21. yüzyıl becerilerine genel olarak orta ve yüksek düzeyde sahip oldukları; ancak bu becerilerin bilgi ve iletişim teknolojileriyle desteklenme düzeyinin çoğunlukla daha sınırlı kaldığı görülmektedir (Gülen, 2013; Önür, 2018). Çalışmalar, 21. yüzyıl becerileri ile teknoloji yeterliği, dijital okuryazarlık, yaşam boyu öğrenme eğilimi ve öğrenci bağlılığı gibi değişkenler arasında pozitif ve anlamlı ilişkiler bulunduğunu ortaya koyarken (Kozikoğlu ve Altunova, 2018; Şahin, 2025; Yıldırım, 2021), teknoloji öz-yeterliğinin bu becerilerin geliştirilmesinde önemli bir yordayıcı olduğunu vurgulamaktadır (Erten, 2020; Yu and Lwin, 2024). Ayrıca TPSA C-21 gibi ölçme araçlarının bu yeterliklerin belirlenmesinde geçerli ve güvenilir olduğu, demografik değişkenlerin ise bazı alt boyutlarda etkili olduğu belirlenmiştir (Christensen and Knezek, 2017; Woods et al., 2021). Bununla birlikte STEM, ters yüz öğrenme, artırılmış gerçeklik ve bağlantılı öğrenme gibi yenilikçi yaklaşımların 21. yüzyıl becerilerinin gelişimini anlamlı biçimde desteklediği ifade edilmektedir (Eken, 2023;

Polat, 2024; Uzun, 2022). Genel olarak bulgular, teknoloji entegrasyonunun ve çağdaş öğretim uygulamalarının 21. yüzyıl becerilerinin geliştirilmesinde önemli bir rol oynadığını göstermektedir.

2.2 Dijital Veri Güvenliği Farkındalığı ile İlgili Alanyazın

Bu bölümde dijital veri güvenliği ve siber güvenlik farkındalığına ilişkin ulusal ve uluslararası araştırmalar kronolojik bir sıra izlenerek sunulmuştur. İlgili alanyazın incelendiğinde, bu konunun ilkökul öğrencilerinden öğretmen adaylarına, öğretmenlerden akademisyenlere kadar farklı katılımcı grupları üzerinde ele alındığı görülmektedir. Çalışmalarda dijital veri güvenliği ve siber güvenlik farkındalığı; yalnızca teknik bilgi ve becerilerle sınırlı olmayan, dijital okuryazarlık, dijital vatandaşlık ve teknolojik pedagojik alan bilgisi gibi kavramlarla ilişkili çok boyutlu bir yeterlik alanı olarak değerlendirilmektedir. Bu doğrultuda incelenen çalışmaların temel amaçları, odaklandıkları değişkenler ve ulaştıkları başlıca bulgular aşağıda özetlenmiştir.

Yılmaz (2015), MEB'e bağlı okullarda görev yapan öğretmenlerin dijital veri güvenliği farkındalık düzeylerini belirlemek amacıyla bir ölçek geliştirmeyi ve bu ölçeği kullanarak mevcut durumu ortaya koymayı amaçlamıştır. Alanyazın taraması ve odak grup görüşmeleri sonucunda oluşturulan madde havuzundan geçerlik ve güvenilirlik süreçleri aşamasından geçirilerek tek faktörlü 32 maddelik bir ölçek geliştirilmiştir ($\alpha=.945$). Ölçeğin 1446 öğretmene uygulanması sonucunda öğretmenlerin dijital veri güvenliği farkındalık düzeylerinin oldukça yüksek olduğu ($\bar{x}=4.16$) belirlenmiştir. Parola güvenliği ve kimlik doğrulama konularındaki farkındalığın güçlü, güvenlik duvarı yazılımları ve çevrimiçi depolama hizmetleri konusundaki farkındalığın ise daha düşük olduğu saptanmıştır. Cinsiyet, günlük bilgisayar ve internet kullanım süresi ile çeşitli teknolojik araçlara sahip olmanın farkındalık düzeyinde anlamlı farklılığa yol açtığı tespit edilmiştir.

Yılmaz vd. (2016), Türkiye'nin batısında bulunan bir ilde 29 farklı okulda görev yapan 870 öğretmenle yürüttükleri araştırmada öğretmenlerin dijital veri güvenliği farkındalığı düzeylerinin oldukça yüksek olduğunu belirlemiştir. Cinsiyet, günlük bilgisayar kullanım süresi, günlük internet kullanım süresi ve teknolojik araç sahipliğinin farkındalık düzeyini etkileyen değişkenler olduğu; branş, öğrenim kademesi, eğitim düzeyi ve mesleki kıdemin ise anlamlı bir belirleyici olmadığı saptanmıştır.

Bhatnagar and Pry (2020), Amerika Birleşik Devletleri'nde bir üniversitede öğrenim gören 107 öğrencinin sosyal medya kullanımında kişisel gizlilik ve siber güvenlik farkındalıklarını incelemiştir. Araştırmada öğrencilerin sosyal medya ortamlarındaki gizlilik ve güvenlik risklerinin farkında oldukları, ancak bu konuda daha fazla eğitime ihtiyaç duydukları belirlenmiştir. Çalışmada ayrıca sosyal medya güvenliği eğitiminin yalnızca hesap ayarlarıyla sınırlı kalmaması; kişisel veri koruma, çevrim içi itibar yönetimi ve risk farkındalığını da kapsamı gerektiği vurgulanmıştır.

Göldağ (2021), İnönü Üniversitesi'nde öğrenim gören 265 öğrencinin dijital okuryazarlık ile dijital veri güvenliği farkındalıkları arasındaki ilişkiyi ilişkisel tarama modeliyle incelemiştir. Öğrencilerin dijital okuryazarlık düzeyinin orta, dijital veri güvenliği farkındalığının ise yüksek düzeyde olduğu saptanmıştır. Erkek öğrencilerin, bilgisayar sahibi olanların ve günlük cihaz kullanım süresi daha uzun olanların her iki alanda da anlamlı düzeyde daha yüksek puan aldığı belirlenmiştir. İki değişken arasında yüksek düzeyde pozitif yönlü anlamlı bir ilişki bulunmuştur.

Hızmalı (2022), Trakya Üniversitesi'nin farklı kademelerinde öğrenim gören 2500 öğrencinin dijital veri güvenliği farkındalıkları ile dijital vatandaşlık düzeylerini karşılaştırmalı biçimde incelemiştir. Öğrencilerin her iki alanda da yüksek düzeyde sergilediği; iki değişken arasında yüksek düzeyde pozitif yönlü anlamlı bir ilişki bulunduğu belirlenmiştir. Erkek öğrencilerin her iki ölçekte de kadın öğrencilerden anlamlı düzeyde daha yüksek puan aldığı, lisans ve lisansüstü öğrencilerin ön lisans öğrencilerine kıyasla daha yüksek DVGFO puanına sahip olduğu saptanmıştır.

Öztürk ve Çakır (2022), 253 öğretmenin katıldığı ilişkisel tarama çalışmasında dijital oyunlardan yararlanma ile dijital veri güvenliği farkındalığı arasındaki ilişkiyi incelemiştir. Her iki değişkenin de yüksek düzeyde olduğu ve aralarında pozitif yönlü anlamlı bir ilişki bulunduğu saptanmıştır. Cinsiyet ve kurumun dijital oyun kullanımında farklılık yaratmazken yaş, çalışma yılı ve günlük internet kullanım süresinin anlamlı farklılık oluşturduğu belirlenmiştir. Dijital veri güvenliği farkındalığı açısından ise cinsiyet ve yaşın belirleyici olmadığı, çalışılan kurum, hizmet yılı ve günlük internet süresinin ise anlamlı fark yarattığı tespit edilmiştir.

Raju et al. (2022), Malezya’da yükseköğretim kurumunda öğrenim gören 110 öğrencinin dijital platform kullanımı bağlamında siber güvenlik farkındalıklarını incelemiştir. Araştırma, COVID-19 sonrası çevrim içi öğrenme platformlarının yaygınlaşmasıyla öğrencilerin siber tehditlere daha açık hâle geldiği varsayımından hareketle yürütülmüştür. Betimsel analiz sonuçları, öğrencilerin siber güvenlik, siber saldırı ve siber zorbalık konularında genel olarak bilgi ve farkındalık sahibi olduklarını göstermiştir. Çalışmada dijital öğrenme ortamlarında veri güvenliği ve mahremiyet farkındalığının güçlendirilmesi gerektiği vurgulanmıştır.

Alqahtani (2022), Suudi Arabistan’da bir üniversitedeki öğrencilerinin siber güvenlik farkındalık düzeylerini etkileyen faktörleri incelemiştir. 450 öğrenciden elde edilen veriler üzerinde geçerlik, güvenirlik, korelasyon, çoklu regresyon ve tek yönlü varyans analizi (ANOVA) gerçekleştirilmiştir. Araştırmada parola güvenliği, tarayıcı güvenliği ve sosyal medya kullanımının öğrencilerin siber güvenlik farkındalığını anlamlı biçimde etkilediği belirlenmiştir. Bulgular, özellikle sosyal medya etkinliklerinin siber güvenlik farkındalığı üzerinde önemli bir belirleyici olduğunu göstermiştir.

Aksoğan ve Atıcı (2023), Malatya’daki iki devlet üniversitesinde görev yapan akademisyenlerin dijital veri güvenliği farkındalık düzeylerini incelemiştir. Katılımcıların farkındalık düzeyinin yeterli olduğu; erkek akademisyenlerin kadın meslektaşlarına kıyasla anlamlı düzeyde daha yüksek dijital veri güvenliği farkındalık puanı aldığı belirlenmiştir. Mesleki deneyimi 1-5 yıl arasında olan akademisyenlerin en yüksek farkındalığa sahip olduğu, ortalama internet kullanım süresi arttıkça dijital veri güvenliği farkındalık düzeyinin de yükseldiği saptanmıştır.

Singh (2024), Hindistan’da öğretmen adaylarının siber güvenlik ve siber güvenlik uygulamalarına ilişkin farkındalık düzeylerini incelemiştir. Araştırma, D.El.Ed. programında öğrenim gören 97 öğretmen adayıyla nicel yöntem kullanılarak yürütülmüştür. Bulgular, katılımcıların büyük çoğunluğunun siber güvenlik hakkında ön bilgiye sahip olduğunu; ancak oltalama (phishing) gibi belirli tehditlere ilişkin bilgilerinin orta düzeyde kaldığını göstermiştir. Öğretmen adaylarının çevrim içi gizlilik konusunda yüksek düzeyde kaygı taşımasına karşın siber riskleri yönetme konusunda öz güvenlerinin düşük olduğu, parola paylaşımı ve zayıf parola yönetimi gibi davranışların önemli güvenlik açıkları

oluşturduğu belirlenmiştir. Çalışmada öğretmen yetiştirme programlarında dijital güvenlik eğitimlerinin güçlendirilmesi gerektiği vurgulanmıştır.

İbekçi (2025), Atatürk Üniversitesi Bilgi ve Belge Yönetimi Bölümü'ndeki 194 lisans öğrencisinin dijital okuryazarlık ve dijital veri güvenliği farkındalık düzeyleri arasındaki ilişkiyi incelemiştir. Öğrencilerin dijital okuryazarlık düzeyinin orta, dijital veri güvenliği farkındalık düzeyinin ise iyi olduğu saptanmıştır. Cinsiyet ve sınıf düzeyi her iki değişken üzerinde anlamlı farklılık yaratmazken, uzun süreli BİT kullanımının dijital okuryazarlık üzerinde anlamlı etki yarattığı belirlenmiştir. İki değişken arasında pozitif yönlü orta düzeyde anlamlı bir ilişki saptanmıştır.

Ravichandran et al. (2025), Hindistan'da öğretmenlerin siber güvenlik farkındalıklarını, deneyimlerini ve dijital ortamdaki güvenlik uygulamalarını incelemiştir. Yapılandırılmış anket aracılığıyla yürütülen çalışmada öğretmenlerin siber tehditler, çevrim içi davranışlar, siber suç deneyimleri ve siber olaylara müdahale mekanizmalarına ilişkin bilgi düzeyleri değerlendirilmiştir. Bulgular, öğretmenlerin siber güvenlik farkındalık düzeylerinin değişkenlik gösterdiğini; birçok öğretmenin oltalama (phishing) ve kimlik hırsızlığı gibi yaygın tehditler konusunda sınırlı bilgiye sahip olduğunu ortaya koymuştur. Ayrıca dijital araçların öğretimde giderek daha fazla kullanılmasına rağmen öğretmenlerin önemli bir bölümünün formal siber güvenlik eğitimi almadığı belirlenmiş ve öğretmenlere yönelik hedeflenmiş farkındalık programlarının gerekli olduğu vurgulanmıştır.

Gökkaya-Babacan (2025), liselerde görev yapan öğretmenlerin TPAB (Teknolojik Pedagojik Alan Bilgisi) yeterlik düzeyleri ile dijital veri güvenliği farkındalık düzeyleri arasındaki ilişkiyi incelemiştir. TPAB yeterliği yüksek olan öğretmenlerin dijital veri güvenliği farkındalık düzeylerinin de anlamlı biçimde yüksek olduğu belirlenmiştir. Bilişim teknolojileri öğretmenlerinin her iki alanda da diğer branşlara kıyasla daha yüksek düzey sergilediği, erkek öğretmenlerin kadın meslektaşlarından anlamlı düzeyde daha yüksek TPAB ve dijital veri güvenliği farkındalık puanı aldığı ve günde dört saat ve üzeri bilgisayar kullanan öğretmenlerin her iki alanda da üstünlük sağladığı tespit edilmiştir. Mesleki kıdemin ise her iki değişken üzerinde anlamlı bir belirleyici olmadığı saptanmıştır.

Leung et al. (2026), Hong Kong'da erken çocukluk, ilköğretim ve yükseköğretim kademelerinde görev yapan 120 öğretmenle yürüttükleri nicel araştırmada öğretmenlerin

siber güvenlik farkındalıklarını mesleki gelişim ve medya okuryazarlığı bağlamında incelemiştir. Çalışmada sosyal medya, e-posta ve bulut depolama ortamlarında kişisel ve öğrenci verilerinin korunmasına odaklanılmıştır. Araştırma sonucunda veri koruma farkındalığı, algılanan ciddiyet, algılanan savunmasızlık, öz-yeterlik ve veri koruma stratejileri arasında pozitif ilişkiler bulunduğu belirlenmiştir. Bununla birlikte öğretmenlerin siber saldırılara ilişkin farkındalıklarında ve medya okuryazarlığı kavramlarını anlamalarında eksiklikler olduğu saptanmış; hizmet öncesi öğretmen eğitimi programlarına kapsamlı medya okuryazarlığı ve siber güvenlik eğitiminin eklenmesi, görevdeki öğretmenlere ise zorunlu ve uygulamalı eğitimler verilmesi önerilmiştir.

İlgili çalışmalar genel olarak dijital veri güvenliği ve siber güvenlik farkındalığının öğretmenler, öğretmen adayları, akademisyenler ve öğrenciler açısından önemli bir yeterlik alanı olduğunu göstermektedir (Aksoğan ve Atıcı, 2023; Singh, 2024; Yılmaz, 2015; Yılmaz vd., 2016). Araştırmalarda farkındalık düzeyinin çoğunlukla yüksek olduğu, ancak parola güvenliği, oltalama, çevrim içi depolama, sosyal medya kullanımı ve veri mahremiyeti gibi konularda çeşitli eksikliklerin sürdüğü görülmektedir (Alqahtani, 2022; Bhatnagar and Pry, 2020; Leung et al., 2026; Raju et al., 2022; Ravichandran et al., 2025). Ayrıca cinsiyet, teknoloji kullanım süresi, dijital okuryazarlık, dijital vatandaşlık, TPAB (Teknolojik Pedagojik Alan Bilgisi) yeterliği ve teknolojik araç sahipliği gibi değişkenlerin dijital veri güvenliği farkındalık düzeyiyle ilişkili olduğu belirlenmiştir (Gökkaya-Babacan, 2025; Göldağ, 2021; Hızmalı, 2022; İbekçi, 2025; Öztürk ve Çakır, 2022). Çalışmalardan elde edilen bulgular, dijital güvenlik farkındalığının yalnızca bireysel teknoloji kullanımıyla sınırlı olmadığını; dijital okuryazarlık, mesleki yeterlik ve uygulamalı eğitim süreçleriyle birlikte ele alınması gereken çok boyutlu bir yapı olduğunu ortaya koymaktadır (Göldağ, 2021; Leung et al., 2026).

3. YÖNTEM

Bu bölümde araştırmanın modeli, örnekleme, veri toplama araçları, verilerin analizi ve verilerin geçerlik-güvenirliğine ilişkin bilgilere yer verilmiştir.

3.1 Araştırmanın Modeli

Bu araştırmada, öğretmenlerin teknoloji yeterliği öz-değerlendirmeleri ile dijital veri güvenliği farkındalıkları arasındaki ilişkiyi incelemek ve söz konusu değişkenlerin çeşitli demografik özellikler açısından farklılaşıp farklılaşmadığını belirlemek amacıyla keşfedici korelasyonel araştırma modeli benimsenmiştir. Korelasyonel araştırmalar, iki ya da daha fazla değişken arasındaki ilişkinin varlığını ve derecesini belirlemeye yönelik araştırmalardır (Büyüköztürk vd., 2016; Fraenkel et al., 2012). Bu kapsamda araştırmada bağımsız değişkenler olarak cinsiyet, görev türü, eğitim düzeyi, mesleki kıdem, bilgisayar sahipliği, dijital güvenlikle ilgili ders/kurs alma durumu ve 21. yüzyıl becerileri kavramını bilme durumu gibi demografik değişkenler ele alınmıştır. Araştırmanın bağımlı değişkenleri ise YYÖTYÖ ve DVGFO puanlarıdır.

3.2 Örneklem

Araştırmanın çalışma grubu, devlet okullarında görev yapan 307 öğretmenden elde edilen veriler incelenmiş; uç değer analizleri sonucunda 24 katılımcı veri setinden çıkarılmış ve analizler 283 öğretmenden oluşan örneklem üzerinde gerçekleştirilmiştir. Çalışmada, seçkisiz olmayan örnekleme yöntemlerinden uygun örnekleme yöntemi kullanılmıştır. Uygun örnekleme, araştırmacının zaman, maliyet, erişilebilirlik ve uygulama kolaylığı gibi koşulları dikkate alarak ulaşabildiği ve araştırmaya katılmaya gönüllü bireylerden veri toplamasına dayanan bir örnekleme yöntemidir (Büyüköztürk vd., 2016; Fraenkel et al., 2012). Bu araştırmada da çalışma grubunun belirlenmesinde öğretmenlere erişim olanakları, veri toplama sürecinin uygulanabilirliği ve gönüllü katılım esas alındığından uygun örnekleme yöntemi tercih edilmiştir. Örneklemde yer alan öğretmenlerin kişisel özelliklerine dağılımı Tablo 3.1’de verilmiştir.

Tablo 3.1: Katılımcıların kişisel özelliklerine göre dağılımı

Değişken	Gruplar	N	%
Cinsiyet	Kadın	176	62.2
	Erkek	107	37.8
	Toplam	283	100.0
Görev türü	Yönetici	80	28.3
	Öğretmen	203	71.7
	Toplam	283	100.0
Eğitim düzeyi	Ön lisans-Lisans	194	68.6
	Yüksek Lisans-Doktora	89	31.4
	Toplam	283	100.0
Mesleki kıdem	10 yıl ve altı	39	13.8
	11-20 yıl	111	39.2
	21-30 yıl	109	38.5
	31 yıl ve üstü	24	8.5
	Toplam	283	100.0
Bilgisayar sahipliği durumu	Evet	267	94.3
	Hayır	16	5.7
	Toplam	283	100.0
Dijital güvenlikle ilgili ders/kurs alma durumu	Evet	135	47.7
	Hayır	148	52.3
	Toplam	283	100.0
21. yüzyıl becerileri kavramını bilme durumu	Evet	249	88.0
	Hayır	34	12.0
	Toplam	283	100.0

Tablo 3.1 incelendiğinde araştırmaya katılan öğretmenlerin 176'sının (%62.2) kadın, 107'sinin (%37.8) erkek olduğu görülmektedir. Görev türü açısından bakıldığında katılımcıların büyük çoğunluğunun öğretmenlerden (n=203, %71.7) oluştuğu, 80'inin (%28.3) ise yönetici (okul müdürü veya müdür yardımcısı) olduğu anlaşılmaktadır. Eğitim düzeyi bakımından katılımcıların %68.6'sı (n=194) ön lisans-lisans, %31.4'ü (n=89) yüksek lisans-doktora mezunudur. Mesleki kıdem açısından 11-20 yıl aralığı (n=111, %39.2) ve 21-

30 yıl aralığı (n=109, %38.5) en kalabalık grupları oluşturmaktadır. Katılımcıların büyük çoğunluğunun (n=267, %94.3) kişisel bilgisayara sahip olduğu; 135'inin (%47.7) daha önce dijital güvenlikle ilgili ders/kurs aldığı belirlenmiştir. 21. yüzyıl becerileri kavramını bilenlerin oranı %88.0 (n=249) iken bu kavramı bilmeyenlerin oranı %12.0'dir (n=34).

3.3 Veri Toplama Araçları

Araştırmada veriler iki bölümden oluşan bir çevrim içi form aracılığıyla toplanmıştır. Birinci bölümde katılımcıların demografik özelliklerini belirlemek amacıyla araştırmacı tarafından hazırlanan kişisel bilgi formu EK A'da yer almaktadır. İkinci bölüm ise iki ölçek içermektedir: EK B'deki 21. Yüzyıl Öğrenmeleri için Teknoloji Yeterliği Öz-Değerlendirme Ölçeği (YYÖTYÖ) ve EK C'deki Dijital Veri Güvenliği Farkındalık Ölçeği (DVGfÖ).

3.3.1 Kişisel bilgi formu

Araştırmada katılımcıların bireysel özelliklerini belirlemek amacıyla araştırmacı tarafından geliştirilen bir “Kişisel Bilgi Formu” kullanılmıştır. EK A'da bulunan bu form, katılımcıların çeşitli özelliklerini ortaya koymaya yönelik maddelerden oluşmaktadır. Kişisel bilgi formunda; cinsiyet, görev türü, eğitim düzeyi, mesleki kıdem, bilgisayar sahipliği ile ilgili sorular bulunmaktadır. Ayrıca katılımcıların dijital yeterliklerine ilişkin durumlarını belirlemek amacıyla dijital güvenlikle ilgili ders/kurs alıp almadıkları ve 21. yüzyıl becerileri kavramını bilip bilmediklerine ilişkin soruları içeren maddelere de yer verilmiştir. Kişisel bilgi formu, araştırmanın amacına uygun olarak hazırlanmış ve katılımcıların araştırma kapsamındaki profillerinin belirlenmesine katkı sağlamıştır.

3.3.2 21. yüzyıl öğrenmeleri için teknoloji yeterliği öz-değerlendirme ölçeği (YYÖTYÖ)

Christensen and Knezek (2017) tarafından geliştirip Fidan vd. (2020) tarafından Türkçe'ye uyarlaması yapılan YYÖTYÖ, toplam 24 maddeden oluşan beşli likert tipinde bir ölçektir. Katılımcılar, EK B'deki ölçekte yer alan maddelere katılma düzeylerini 1-hiç katılmıyorum ile 5-tamamen katılıyorum arasında değişen beş seçenekten birini işaretleyerek belirtmektedirler. Ölçekten alınabilecek toplam puanlar 24 ile 120 arasında değişmektedir. Toplam puanların ölçekte yer alan madde sayısına bölünmesiyle elde edilen YYÖTYÖ puanlarının yorumlanmasında 1.00-1.80 aralığı “hiç katılmıyorum”, 1.81-2.60 aralığı “katılmıyorum”, 2.61-3.40 aralığı “kararsızım”, 3.41-4.20 aralığı “katılıyorum” ve 4.21-5.00 aralığı “tamamen katılıyorum” olarak değerlendirilmektedir. Ölçekte ters madde bulunmamaktadır. YYÖTYÖ E-posta (1-5. maddeler), WWW (6-10. maddeler), Entegre

Uygulamalar (11-15. maddeler) ve Teknolojiyle Öğretim (16-24. maddeler) olmak üzere dört faktörlü bir yapıya sahiptir. Ölçeğin tümüne ilişkin Cronbach'ın alfa katsayısı .89 olarak, ölçek boyutlarına ilişkin Cronbach'ın alfa katsayıları .80 ile .91 arasında bulunmuştur (Fidan vd., 2020).

3.3.3 Dijital veri güvenliği farkındalığı ölçeği (DVGFÖ)

Yılmaz (2015) tarafından geliştirilen DVGFÖ, toplam 32 maddeden oluşan beşli likert tipinde bir ölçektir. Katılımcılar, EK C'deki ölçekte yer alan maddelere katılma düzeylerini 1-hiç katılmıyorum ile 5-tamamen katılıyorum arasında değişen beş seçenekten birini işaretleyerek belirtmektedirler. Ölçekten alınabilecek toplam puanlar 32 ile 160 arasında değişmektedir. Toplam puanların ölçekte yer alan madde sayısına bölünmesiyle elde edilen DVGFÖ puanlarının yorumlanmasında 1.00-1.80 aralığı “hiç katılmıyorum”, 1.81-2.60 aralığı “katılmıyorum”, 2.61-3.40 aralığı “kararsızım”, 3.41-4.20 aralığı “katılıyorum” ve 4.21-5.00 aralığı “tamamen katılıyorum” olarak değerlendirilmektedir. Tek faktörlü yapıya sahip olan ölçekte ters madde bulunmamaktadır. DVGFÖ puanı arttıkça dijital veri güvenliği farkındalığı da artmaktadır. Ölçek için Cronbach'ın alfa katsayısı .95 olarak hesaplanmıştır (Yılmaz, 2015).

3.4 Verilerin Analizi

Araştırmada toplanan verilerin çözümlenmesinde IBM SPSS Statistics 27 istatistik paket programı kullanılmıştır. Verilerin analizine geçilmeden önce normallik varsayımının karşılanıp karşılanmadığı incelenmiştir. Normallik değerlendirmesinde her bir bağımsız değişkene ait grupların çarpıklık ve basıklık katsayıları incelenmiştir. Bu katsayıların ± 1.5 aralığında kalması normal dağılım için kabul edilebilir ölçüt olarak benimsenmiştir (Tabachnick and Fidell, 2013). Elde edilen çarpıklık ve basıklık değerleri Tablo 3.2'de sunulmuştur.

Tablo 3.2: Grup bazında çarpıklık ve basıklık değerleri

Ölçekler		YYÖTYÖ			DVGFÖ	
Değişkenler	Gruplar	N	Çarpıklık	Basıklık	Çarpıklık	Basıklık
Cinsiyet	Kadın	176	-0.911	+0.396	-1.028	+0.283
	Erkek	107	-1.010	+0.599	-1.245	+0.713
Görev türü	Yönetici	80	-0.729	-0.131	-0.937	-0.377
	Öğretmen	203	-0.920	+0.321	-1.224	+0.922

Tablo 3.2 (devam)

Eğitim düzeyi	Ön lisans-Lisans	194	-0.795	+0.160	-1.126	+0.637
	Yüksek Lisans-Doktora	89	-1.176	+1.315	-1.178	+0.325
Mesleki kıdem	10 yıl ve altı	39	-0.758	+0.159	-0.817	-0.396
	11-20 yıl	111	-0.783	-0.219	-1.067	+0.075
	21-30 yıl	109	-1.128	+0.772	-1.254	+1.152
	31 yıl ve üstü	24	-0.735	+0.054	-0.895	-0.346
Bilgisayar sahipliği durumu	Evet	267	-1.063	+0.920	-1.198	+0.826
	Hayır	16	-0.353	-1.123	-0.733	-0.583
Dijital güvenlikle ilgili ders/kurs alma durumu	Evet	135	-1.171	+1.299	-1.373	+1.156
	Hayır	148	-0.840	+0.241	-0.908	+0.056
21. yüzyıl becerileri kavramını bilme durumu	Evet	249	-1.159	+1.288	-1.323	+1.175
	Hayır	34	-0.239	-0.806	-0.424	-0.516

Not. YYÖTYÖ: 21. Yüzyıl Öğrenmeleri için Teknoloji Yeterliği Öz-Değerlendirme Ölçeği, DVGFÖ: Dijital Veri Güvenliği Farkındalık Ölçeği

Tablo 3.2’de yer alan çarpıklık ve basıklık değerleri incelendiğinde, YYÖTYÖ ve DVGFÖ ölçeklerinden elde edilen puanların tüm alt gruplarda çarpıklık ve basıklık değerlerinin ± 1.5 aralığında kaldığı normal dağılım gösterdiği görülmektedir. Çarpıklık değerleri -1.373 ile -0.239, basıklık değerleri ise -1.123 ile +1.315 arasında değişmektedir. Bu değerlerin kabul edilebilir normal dağılım sınırları içerisinde yer alması nedeniyle araştırmada parametrik testlerin kullanılmasının uygun olduğu sonucuna ulaşılmıştır. Bu sonuç, söz konusu değişkenler için normallik varsayımının karşılandığını göstermekte ve parametrik testlerin kullanımına imkân tanımaktadır (Tabachnick and Fidell, 2013).

Bu doğrultuda iki kategoriye sahip bağımsız değişkenler için bağımsız örneklem t-testi, ikiden fazla kategoriye sahip değişkenler için tek yönlü varyans analizi (ANOVA) kullanılmasına karar verilmiştir. ANOVA testinin anlamlı çıktığı durumlarda, farklılığın hangi gruplar arasında olduğunu belirlemek amacıyla Tukey HSD post-hoc testi kullanılmıştır. Tukey HSD testi, üç ve daha fazla grup ortalamasının karşılaştırıldığı durumlarda ANOVA sonrasında tüm olası ikili karşılaştırmaları yapmaya olanak sağlaması ve çoklu karşılaştırmalardan kaynaklanabilecek Tip I hata olasılığını kontrol etmesi nedeniyle tercih edilmektedir (Büyüköztürk, 2023; Field, 2018). İki ölçek arasındaki

ilişkinin incelenmesinde Pearson korelasyon katsayısı hesaplanmıştır. Tüm istatistiksel analizlerde anlamlılık düzeyi .05 olarak belirlenmiştir.

3.5 Verilerin Geçerliği ve Güvenirliği

Araştırmada katılımcıların demografik özelliklerini, mesleki durumlarını ve teknoloji kullanım alışkanlıklarını belirlemek amacıyla araştırmacılar tarafından kişisel bilgi formu hazırlanmıştır. Formdaki sorular belirlenirken dijital veri güvenliği farkındalığı, teknoloji yeterliği ve 21. yüzyıl becerileri alanındaki çalışmalar incelenmiştir. Bu doğrultuda alanyazında sıklıkla ele alınan cinsiyet, görev türü, eğitim düzeyi ve mesleki kıdem gibi demografik değişkenlerin yanı sıra bilgisayar sahipliği durumu, dijital güvenlikle ilgili ders/kurs alma durumu ve 21. yüzyıl becerileri kavramını bilme durumu değişkenlerine yer verilmiştir (Avcı ve Arslan, 2019; Fidan ve Cura-Yeleğen, 2022; Woods et al., 2021; Yılmaz vd., 2016). Bu değişkenlerin katılımcıların teknoloji yeterliği öz-değerlendirmeleri ile dijital veri güvenliği farkındalıkları farklılaştırıcı etkiye sahip olabileceği öngörülmüştür. Hazırlanan formun kapsam, anlaşılabilirlik ve araştırmanın amacıyla uyum açısından değerlendirilmesi amacıyla öğretim teknolojileri alanında uzman iki akademisyenin görüşüne başvurulmuş, alınan geri bildirimler doğrultusunda gerekli düzenlemeler yapılarak forma son şekli verilmiştir.

Bu araştırmada kullanılan ölçeklerin her ikisi de geçerlik ve güvenirlik çalışmaları tamamlanmış ölçme araçlarıdır. YYÖTYÖ'nün Türkçeye uyarlaması Fidan vd. (2020) tarafından gerçekleştirilmiş; açıklayıcı ve doğrulayıcı faktör analizleri ile yapı geçerliğinin sağlandığı gösterilmiştir. Ölçeğin bu araştırma örneklemini üzerinde hesaplanan Cronbach'ın alfa katsayısı (.91), Fidan vd. (2020) tarafından hesaplanan Cronbach'ın Alfa katsayısı (.89) değeri ile yakınlık göstermekte olup yüksek düzeyde iç tutarlılığa işaret etmektedir. DVGFO ise Yılmaz (2015) tarafından geliştirilmiş; açıklayıcı ve doğrulayıcı faktör analizleri gerçekleştirilmiş, tek faktörlü yapısının geçerliliği kanıtlanmıştır. Ölçeğin bu araştırma örneklemini üzerindeki Cronbach Alfa katsayısı (.94) Yılmaz (2015) tarafından hesaplanan Cronbach'ın alfa katsayısı (.95) değeri ile yakınlık göstermekte olup yüksek düzeyde iç tutarlılığa işaret etmektedir (Büyüköztürk, 2023).

3.6 Etik Hususlar

Veri toplama aşamasından önce Balıkesir Üniversitesi Fen ve Mühendislik Bilimleri Etik Komisyonuna başvurularak araştırmanın etik açıdan uygun olduğuna dair 17.01.2025 tarihli

ve E-16031472-108.01-472837 sayılı etik kurul onayı alınmıştır. Bu onay belgesi EK D’de sunulmuştur. Bunun yanı sıra, devlet okullarında görev yapan öğretmenlerden veri toplanabilmesi için Millî Eğitim Bakanlıđından araştırma uygulama izni alınmış ve ilgili belge EK E’de verilmiştir. Etik kurul onayı ve uygulama izinlerinin ardından veri toplama araçları öğretmenlere uygulanmıştır.

Bu çalışmanın yazım aşamasında, metnin dilsel açıdan düzenlenmesi, ifadelerin daha anlaşılır biçimde yeniden yapılandırılması ve akademik anlatımın güçlendirilmesi amacıyla Microsoft M365 Copilot, Gemini ve NotebookLM araçlarından yararlanılmıştır. Söz konusu araçlar; araştırma probleminin oluşturulması, verilerin analiz edilmesi, bulguların yorumlanması veya çalışmanın bilimsel içeriğine katkı sağlanması amacıyla kullanılmamıştır. Araştırmaya ilişkin tüm bilimsel değerlendirmeler, içerik tercihleri ve nihai düzenlemeler yazarlar tarafından gerçekleştirilmiştir.

4. BULGULAR

Bu bölümde araştırmanın problemlerine göre elde edilen bulgulara yer verilmiştir.

4.1 Birinci Probleme Ait Bulgular

Araştırmanın birinci problemi “Öğretmenlerin teknoloji yeterliği öz-değerlendirme ve dijital veri güvenliği farkındalık düzeyleri nedir?” şeklinde belirlenmiştir. Bu probleme yanıt vermek amacıyla her iki ölçekten elde edilen puanların betimsel istatistikleri hesaplanmıştır.

4.1.1 YYÖTYÖ’den elde edilen bulgular

283 öğretmenden elde edilen YYÖTYÖ verilerine ilişkin betimsel istatistikler Tablo 4.1’de sunulmuştur.

Tablo 4.1: YYÖTYÖ’ye ilişkin betimsel istatistikler

Ölçek/Boyut	N	$\bar{x}$	S	Minimum	Maksimum
YYÖTYÖ Puanı	283	4.35	0.55	2.25	5.00
E-Posta Boyutu Puanı	283	4.80	0.53	1.00	5.00
WWW Boyutu Puanı	283	4.89	0.29	2.40	5.00
Entegre Uygulamalar Boyutu Puanı	283	3.73	1.03	1.00	5.00
Teknolojiyle Öğretim Boyutu Puanı	283	4.10	0.80	1.00	5.00

Not. YYÖTYÖ: 21. Yüzyıl Öğrenmeleri için Teknoloji Yeterliği Öz-Değerlendirme Ölçeği, N: katılımcı sayısı, $\bar{x}$: ortalama, S: standart sapma

Tablo 4.1 incelendiğinde öğretmenlerin YYÖTYÖ puanlarının ortalamasının 4.35 (S=0.55) olduğu görülmektedir. Bu değer yöntem bölümünde yer alan ölçeklemeye göre “tamamen katılıyorum” düzeyine karşılık gelmekte ve öğretmenlerin teknoloji yeterliği öz-değerlendirmelerinin yüksek düzeyde olduğuna işaret etmektedir. Boyutlar incelendiğinde en yüksek ortalamayı WWW boyutunun ($\bar{x}$ =4.89, S=0.29) aldığı ve bunu E-posta boyutunun ($\bar{x}$ =4.80, S=0.53) izlediği görülmektedir. Teknolojiyle Öğretim boyutunda ortalama 4.10 (S=0.80) iken en düşük ortalamanın Entegre Uygulamalar boyutuna ait olduğu ($\bar{x}$ =3.73, S=1.03) dikkat çekmektedir. Bu bulgunun, öğretmenlerin temel teknoloji kullanım becerilerinin ileri düzey teknoloji entegrasyon becerilerine kıyasla daha yüksek olduğunu ortaya koyduğu yorumu yapılabilir.

Araştırmada kullanılan ölçek maddelerine ilişkin tanılayıcı istatistikler incelendiğinde, katılımcıların 21. Yüzyıl Öğrenmeleri İçin Teknoloji Yeterliği Öz-Değerlendirme Ölçeği

maddelerine verdikleri yanıtların genel olarak yüksek düzeyde olduğu görülmektedir. Ölçekte yer alan maddeler arasında en yüksek ortalamanın “Üniversitemin veya Millî Eğitim Bakanlığı’nın internet sitelerini arayıp bulabilirim” maddesine ait olduğu belirlenmiştir ($\bar{x}=4.96$). Bu maddeyi “Bir arama motoru kullanarak ilgilendiğim konulara ilişkin web sayfalarını bulabilirim” maddesi izlemektedir ($\bar{x}=4.95$). Her iki maddenin de “tamamen katılıyorum” düzeyinde olduğu görülmektedir. Bu bulgu, katılımcıların internet ortamında bilgiye erişme, arama motorlarını kullanma ve resmî kurumlara ait web sitelerine ulaşma konusunda kendilerini oldukça yeterli gördüklerini göstermektedir. Özellikle web ortamında bilgi arama ve ilgili kaynaklara ulaşma becerilerinin katılımcılar açısından güçlü bir yeterlik alanı olduğu söylenebilir.

Ölçekte en düşük ortalamaya sahip maddenin “Başkalarının dokümanları farklı kelime işlemci programlarında okuyabilecekleri formatta kaydedebilirim” maddesi olduğu belirlenmiştir ($\bar{x}=3.17$). Bunu “Öğrencilerimle uzaktan öğretim yapmak için çevrimiçi araçları kullanabilirim” maddesi izlemektedir ($\bar{x}=3.31$). Bu maddelerin “kısmen katılıyorum” düzeyinde yer aldığı görülmektedir.

Katılımcıların temel internet kullanımı ve bilgiye erişim becerilerinde yüksek yeterlik algısına sahip olmalarına karşın, farklı dosya formatlarında belge kaydetme ve çevrim içi araçları öğretim sürecinde kullanma gibi daha teknik ve pedagojik teknoloji yeterliği gerektiren alanlara göre daha düşük düzeyde yeterlik algısına sahip olduklarını göstermektedir. Bu bağlamda, katılımcıların teknoloji kullanımına ilişkin temel becerilerinin güçlü olduğu; ancak öğretim sürecine teknoloji entegrasyonu ve dijital içeriklerin teknik olarak düzenlenmesi konularında desteklenmeye ihtiyaç duyabilecekleri söylenebilir.

4.1.2 DVGFÖ’den elde edilen bulgular

Araştırmaya katılan 283 öğretmene uygulanan DVGFÖ’den elde edilen betimsel istatistik değerleri Tablo 4.2’de verilmiştir.

Tablo 4.2: DVGFÖ’ye ilişkin betimsel istatistikler

Ölçek	N	$\bar{x}$.	S	Minimum	Maksimum
DVGFÖ	283	4.57	0.45	2.91	5.00

Not. DVGFÖ: Dijital Veri Güvenliği Farkındalık Ölçeği, N: katılımcı sayısı, $\bar{x}$: ortalama, S: standart sapma

Tablo 4.2 incelendiğinde öğretmenlerin DVGFÖ puan ortalamasının 4.57 ($S=0.45$) olduğu görülmektedir. Bu değer yöntem bölümünde yer alan ölçeklemeye göre “tamamen katılıyorum” düzeyine karşılık gelmekte ve öğretmenlerin dijital veri güvenliği farkındalıklarının yüksek düzeyde olduğuna işaret etmektedir.

Araştırmada kullanılan Dijital Veri Güvenliği Farkındalığı Ölçeği maddelerine ilişkin ortalama puanlar incelendiğinde ise katılımcıların dijital veri güvenliğine yönelik farkındalık düzeylerinin genel olarak yüksek olduğu görülmektedir. Ölçekte en yüksek ortalamaya sahip maddenin “Cep telefonuna gelen tek kullanımlık parola ile yapılan giriş işlemlerinin, güvenliği arttırdığını bilirim” maddesi olduğu belirlenmiştir ($\bar{x}=4.86$). Bu maddeyi “Parola oluştururken harf, sayı ve özel karakter kullanmanın önemini bilirim” Ve “Parola oluştururken karakter sayısının fazla olmasının önemini bilirim” maddeleri izlemektedir ($\bar{x}=4.82$). Bu maddelerin “tamamen katılıyorum” düzeyinde olduğu görülmektedir. Bu bulgu, katılımcıların özellikle güçlü parola oluşturma, parola güvenliği ve tek kullanımlık parola gibi bireysel hesap güvenliğine ilişkin konularda yüksek düzeyde farkındalığa sahip olduklarını göstermektedir. Başka bir ifadeyle, katılımcıların dijital ortamlarda kişisel hesap güvenliğini sağlamaya yönelik temel güvenlik önlemlerinin önemini farkında oldukları söylenebilir.

Ölçekte en düşük ortalamaya sahip maddenin “Güvenlik duvarı yazılımları konusunda bilgi sahibiyim” maddesi olduğu belirlenmiştir ($\bar{x}=3.59$). Bu maddeyi “Zararlı yazılımlar konusunda bilgi sahibiyim” maddesi izlemektedir ($\bar{x}=3.92$). Bu maddelerin ortalamaları diğer maddelere kıyasla daha düşük olmakla birlikte, katılımcıların bu maddelere yönelik yanıtlarının genel olarak olumlu düzeyde olduğu görülmektedir.

Katılımcıların parola güvenliği gibi bireysel ve günlük dijital güvenlik uygulamalarında daha yüksek farkındalığa sahip olduklarını; buna karşın güvenlik duvarı yazılımları ve zararlı yazılımlar gibi daha teknik bilgi gerektiren konularda farkındalık düzeylerinin daha düşük olduğunu göstermektedir. Dolayısıyla katılımcıların dijital veri güvenliğine ilişkin temel farkındalıklarının yüksek olduğu, ancak sistem güvenliği ve güvenlik yazılımlarına yönelik teknik bilgi gerektiren alanlarda daha fazla bilgilendirme ve uygulamalı desteğe ihtiyaç duyabilecekleri ifade edilebilir.

4.2 İkinci Probleme Ait Bulgular

Araştırmanın ikinci problemi “Öğretmenlerin teknoloji yeterliği öz-değerlendirmeleri ile dijital veri güvenliği farkındalıkları cinsiyet, görev türü, eğitim düzeyi, mesleki kıdem, bilgisayar sahipliği, dijital güvenlikle ilgili ders/kurs alma durumu ve 21. yüzyıl becerileri kavramını bilme durumuna göre anlamlı düzeyde farklılık göstermekte midir?” şeklinde belirlenmiştir.

4.2.1 YYÖTYÖ puanlarının çeşitli değişkenlere göre incelenmesi

Öğretmenlerin YYÖTYÖ puanlarının cinsiyete göre farklılık gösterip göstermediğini belirlemek amacıyla gerçekleştirilen bağımsız örneklem t-testi sonuçları Tablo 4.3’te verilmiştir.

Tablo 4.3: YYÖTYÖ puanlarının cinsiyete göre t-testi sonuçları

Cinsiyet	N	$\bar{x}$	S	Levene F	Levene p	t	sd	p	Cohen d
Kadın	176	4.264	0.586	3.865	.050	3.291	281	.001	.403
Erkek	107	4.483	0.466						

Not. YYÖTYÖ: 21. Yüzyıl Öğrenmeleri için Teknoloji Yeterliği Öz-Değerlendirme Ölçeği, N: katılımcı sayısı, $\bar{x}$: ortalama, S: standart sapma

Tablo 4.3 incelendiğinde erkek öğretmenlerin YYÖTYÖ puan ortalamasının ($\bar{x}$ =4.483, S=0.466) kadın öğretmenlerin puan ortalamasından ($\bar{x}$ =4.264, S=0.586) yüksek olduğu görülmektedir. Levene testi sonucuna göre grup varyansları homojendir (F=3.865, p=.050). Bağımsız örneklem t-testi sonucuna göre öğretmenlerin YYÖTYÖ puanları cinsiyete göre istatistiksel olarak anlamlı biçimde farklılaşmaktadır, $t(281)=3.291$, $p=.001$. Etki büyüklüğü Cohen d=0.403 olarak hesaplanmış olup bu orta düzey bir etkiye karşılık gelmektedir.

Öğretmenlerin YYÖTYÖ puanlarının görev türüne göre farklılık gösterip göstermediğini belirlemek amacıyla gerçekleştirilen bağımsız örneklem t-testi sonuçları Tablo 4.4’te verilmiştir.

Tablo 4.4: YYÖTYÖ puanlarının görev türüne göre t-testi sonuçları

Görev türü	N	$\bar{x}$	S	Levene F	Levene p	t	sd	p	Cohen d
Yönetici	80	4.469	0.411	7.382	.007	2.741	208	.007	.310
Öğretmen	203	4.299	0.595						

Not. YYÖTYÖ: 21. Yüzyıl Öğrenmeleri için Teknoloji Yeterliği Öz-Değerlendirme Ölçeği, N: katılımcı sayısı, $\bar{x}$: ortalama, S: standart sapma. Levene testi anlamlı olduğundan ($p=.007$)

Tablo 4.4 incelendiğinde yöneticilerin YYÖTYÖ puan ortalamasının ($\bar{x}=4.469$, $S=0.411$) yönetici olmayan öğretmenlere ($\bar{x}=4.299$, $S=0.595$) kıyasla daha yüksek olduğu görülmektedir. t-testi sonucuna göre YYÖTYÖ puanları görev türüne göre istatistiksel olarak anlamlı biçimde farklılaşmaktadır, $t(208)=2.741$, $p=.007$. Etki büyüklüğünü belirlemek amacıyla hesaplanan Cohen d katsayısı 0.310 olup, bu değer görev türünün YYÖTYÖ puanları üzerindeki etkisinin küçük düzeyde olduğunu göstermektedir.

Öğretmenlerin YYÖTYÖ puanlarının eğitim düzeyine göre farklılık gösterip göstermediğini belirlemek amacıyla gerçekleştirilen bağımsız örneklem t-testi sonuçları Tablo 4.5'te verilmiştir.

Tablo 4.5: YYÖTYÖ puanlarının eğitim düzeyine göre t-testi sonuçları

Eğitim düzeyi	N	$\bar{x}$	S	Levene F	Levene p	t	sd	p	Cohen d
Ön lisans-Lisans	194	4.256	0.594	13.991	.000	4.884	248	.000	.538
Yüksek Lisans-Doktora	89	4.545	0.387						

Not. YYÖTYÖ: 21. Yüzyıl Öğrenmeleri için Teknoloji Yeterliği Öz-Değerlendirme Ölçeği, N: katılımcı sayısı, $\bar{x}$: ortalama, S: standart sapma.

Tablo 4.5 incelendiğinde yüksek lisans veya doktora mezunu öğretmenlerin YYÖTYÖ puan ortalamasının ($\bar{x}=4.545$, $S=0.387$) ön lisans-lisans mezunlarına ($\bar{x}=4.256$, $S=0.594$) kıyasla belirgin biçimde yüksek olduğu görülmektedir. T-testi sonucuna göre bu fark istatistiksel olarak anlamlıdır, $t(248)=4.884$, $p<.001$, Cohen d=0.538.

Öğretmenlerin YYÖTYÖ puanlarının mesleki kıdemlerine göre istatistiksel olarak anlamlı bir farklılık gösterip göstermediğini belirlemek amacıyla gerçekleştirilen ANOVA sonuçları Tablo 4.6'da verilmiştir.

Tablo 4.6: YYÖTYÖ puanlarının mesleki kıdeme göre ANOVA sonuçları

Mesleki kıdem	N	$\bar{x}$	S	F	sd1	sd2	p	η^2
10 yıl ve altı	39	4.323	0.450	0.436	3	279	.728	0.005
11-20 yıl	111	4.377	0.521					
21-30 yıl	109	4.309	0.627					
31 yıl ve üstü	24	4.418	0.508					

Not. YYÖTYÖ: 21. Yüzyıl Öğrenmeleri için Teknoloji Yeterliği Öz-Değerlendirme Ölçeği, N: katılımcı sayısı, $\bar{x}$: ortalama, S: standart sapma

Tablo 4.6'ya göre mesleki kıdem grupları arasında YYÖTYÖ puanları bakımından istatistiksel olarak anlamlı bir farklılık bulunmamaktadır, $F(3,279)=0.436$, $p=.728$. Mesleki kıdam değişkeni, öğretmenlerin teknoloji yeterliği öz-değerlendirme düzeylerinde belirleyici bir değişken olarak öne çıkmamaktadır.

Öğretmenlerin YYÖTYÖ puanlarının bilgisayar sahipliğine göre farklılık gösterip göstermediğini belirlemek amacıyla gerçekleştirilen bağımsız örneklem t-testi sonuçları Tablo 4.7'de verilmiştir.

Tablo 4.7: YYÖTYÖ puanlarının bilgisayar sahipliği durumuna göre t-testi sonuçları

Bilgisayar Sahipliği	N	$\bar{x}$	S	Levene F	Levene p	t	sd	p	Cohen d
Evet	267	4.363	0.548	0.296	.587	2.068	281	.040	.532
Hayır	16	4.070	0.598						

Not. YYÖTYÖ: 21. Yüzyıl Öğrenmeleri için Teknoloji Yeterliği Öz-Değerlendirme Ölçeği, N: katılımcı sayısı, $\bar{x}$: ortalama, S: standart sapma

Tablo 4.7'ye göre bilgisayara sahip olan öğretmenlerin YYÖTYÖ puan ortalamasının ($\bar{x}=4.363$, $S=0.548$) bilgisayar sahip olmayan öğretmenlere ($\bar{x}=4.070$, $S=0.598$) kıyasla anlamlı düzeyde daha yüksek olduğu görülmektedir, $t(281)=2.068$, $p=.040$, Cohen $d=0.532$. Bilgisayarı olmayan grubun örneklem büyüklüğünün küçüklüğü ($n=16$) bu bulgunun yorumlanmasında göz önünde bulundurulmalıdır.

Öğretmenlerin YYÖTYÖ puanlarının dijital güvenlikle ilgili ders/kurs alma durumuna göre farklılık gösterip göstermediğini belirlemek amacıyla gerçekleştirilen bağımsız örneklem t-testi sonuçları Tablo 4.8’de verilmiştir.

Tablo 4.8: YYÖTYÖ puanlarının dijital güvenlikle ilgili ders/kurs alma durumuna göre t-testi sonuçları

Dijital güvenlikle ilgili ders/kurs alma	N	$\bar{x}$	S	Levene F	Levene p	t	sd	p	Cohen d
Evet	135	4.487	0.481	3.583	.059	4.190	281	.000	.499
Hayır	148	4.219	0.585						

Not. YYÖTYÖ: 21. Yüzyıl Öğrenmeleri için Teknoloji Yeterliği Öz-Değerlendirme Ölçeği, N: katılımcı sayısı, $\bar{x}$: ortalama, S: standart sapma

Tablo 4.8 incelendiğinde dijital güvenlikle ilgili ders/kurs almış öğretmenlerin YYÖTYÖ puan ortalamasının ($\bar{x}$ =4.487, S=0.481) almamış olanlara ($\bar{x}$ =4.219, S=0.585) kıyasla anlamlı düzeyde daha yüksek olduğu görülmektedir, $t(281)=4.190$, $p<.001$, Cohen d=0.499.

Öğretmenlerin YYÖTYÖ puanlarının 21. yüzyıl becerileri kavramını bilme durumuna göre farklılık gösterip göstermediğini belirlemek amacıyla gerçekleştirilen bağımsız örneklem t-testi sonuçları Tablo 4.9’da verilmiştir.

Tablo 4.9: YYÖTYÖ puanlarının 21. yüzyıl becerileri kavramını bilme durumuna göre t-testi sonuçları

21. yüzyıl becerileri kavramını bilme	N	$\bar{x}$	S	Levene F	Levene p	t	sd	p	Cohen d
Evet	249	4.392	0.534	1.961	.163	3.817	281	.000	.698
Hayır	34	4.015	0.588						

Not. YYÖTYÖ: 21. Yüzyıl Öğrenmeleri için Teknoloji Yeterliği Öz-Değerlendirme Ölçeği, N: katılımcı sayısı, $\bar{x}$: ortalama, S: standart sapma

Tablo 4.9’a göre 21. yüzyıl becerileri kavramını daha bildiklerini ifade eden öğretmenlerin YYÖTYÖ puan ortalaması ($\bar{x}$ =4.392, S=0.534), kavramı bilmediklerini belirtenlere ($\bar{x}$ =4.015, S=0.588) kıyasla istatistiksel olarak anlamlı biçimde daha yüksektir,

$t(281)=3.817$, $p<.001$, Cohen $d=0.698$. Bu değişken YYÖTYÖ puanları üzerinde en güçlü etki büyüklüğünü (Cohen $d=0.698$) üreten demografik olarak öne çıkmaktadır.

4.2.2 DVGFÖ puanlarının çeşitli değişkenlere göre incelenmesi

Öğretmenlerin DVGFÖ puanlarının cinsiyete göre farklılık gösterip göstermediğini belirlemek amacıyla gerçekleştirilen bağımsız örneklem t-testi sonuçları Tablo 4.10'da verilmiştir.

Tablo 4.10: DVGFÖ puanlarının cinsiyete göre t-testi sonuçları

Cinsiyet	N	$\bar{x}$	S	Levene F	Levene p	t	sd	p	Cohen d
Kadın	176	4.499	0.483	5.934	.015	3.676	267	.000	.422
Erkek	107	4.686	0.368						

Not. DVGFÖ: Dijital Veri Güvenliği Farkındalık Ölçeği, N: katılımcı sayısı, $\bar{x}$: ortalama, S: standart sapma.

Tablo 4.10 incelendiğinde erkek öğretmenlerin DVGFÖ puan ortalamasının ($\bar{x}=4.686$, $S=0.368$) kadın öğretmenlere ($\bar{x}=4.499$, $S=0.483$) kıyasla anlamlı düzeyde yüksek olduğu görülmektedir. T-testi sonucuna göre bu fark istatistiksel olarak anlamlıdır, $t(267)=3.676$, $p<.001$, Cohen $d=0.422$.

Öğretmenlerin DVGFÖ puanlarının görev türüne göre farklılık gösterip göstermediğini belirlemek amacıyla gerçekleştirilen bağımsız örneklem t-testi sonuçları Tablo 4.11'de verilmiştir.

Tablo 4.11: DVGFÖ puanlarının görev türüne göre t-testi sonuçları

Görev türü	N	$\bar{x}$	S	Levene F	Levene p	t	sd	p	Cohen d
Yönetici	80	4.593	0.422	0.281	.597	0.537	281	.592	.071
Öğretmen	203	4.560	0.464						

Not. DVGFÖ: Dijital Veri Güvenliği Farkındalık Ölçeği, N: katılımcı sayısı, $\bar{x}$: ortalama, S: standart sapma

Tablo 4.11'e göre yönetici ve öğretmen grupları arasında DVGFÖ puanları bakımından istatistiksel olarak anlamlı bir farklılık bulunmamaktadır, $t(281)=0.537$, $p=.592$.

Öğretmenlerin DVGFÖ puanlarının eğitim düzeyine göre farklılık gösterip göstermediğini belirlemek amacıyla gerçekleştirilen bağımsız örneklem t-testi sonuçları Tablo 4.12’de verilmiştir.

Tablo 4.12: DVGFÖ puanlarının eğitim düzeyine göre t-testi sonuçları

Eğitim düzeyi	N	$\bar{x}$	S	Levene F	Levene p	t	sd	p	Cohen d
Ön lisans-Lisans	194	4.539	0.471	2.358	.126	1.677	281	.095	.215
Yüksek Lisans-Doktora	89	4.636	0.403						

Not. DVGFÖ: Dijital Veri Güvenliği Farkındalık Ölçeği, N: katılımcı sayısı, $\bar{x}$: ortalama, S: standart sapma

Tablo 4.12 incelendiğinde ön lisans-lisans grubu ile yüksek lisans-doktora grubu öğretmenlerin DVGFÖ puan ortalamaları arasında gözlenen farkın yüksek lisans-doktora grubu lehine olduğu görülmektedir. Ancak yapılan bağımsız örneklem t-testi sonucunda bu farkın istatistiksel olarak anlamlı olmadığı belirlenmiştir, $t(281)=1.677$, $p=.095$. Etki büyüklüğünü belirlemek amacıyla hesaplanan Cohen d değeri 0.215 olup, bu değer eğitim düzeyinin dijital veri güvenliği farkındalığı üzerindeki etkisinin küçük düzeyde olduğunu göstermektedir. Buna göre öğretmenlerin dijital veri güvenliği farkındalıkları eğitim düzeyine göre anlamlı biçimde farklılaşmamaktadır.

Öğretmenlerin DVGFÖ puanlarının mesleki kıdeme göre farklılık gösterip göstermediğini belirlemek amacıyla gerçekleştirilen ANOVA sonuçları Tablo 4.13’te verilmiştir.

Tablo 4.13: DVGFÖ puanlarının mesleki kıdeme göre ANOVA sonuçları

Mesleki kıdem	N	$\bar{x}$	S	F	sd1	sd2	p	η^2
10 yıl ve altı	39	4.459	0.474	2.261	3	279	.082	0.024
11-20 yıl	111	4.582	0.441					
21-30 yıl	109	4.555	0.477					
31 yıl ve üstü	24	4.758	0.272					

Not. DVGFÖ: Dijital Veri Güvenliği Farkındalık Ölçeği, N: katılımcı sayısı, $\bar{x}$: ortalama, S: standart sapma

Tablo 4.13 incelendiğinde 31 yıl ve üstü kıdeme sahip öğretmenlerin DVGFÖ puan ortalamasının ($\bar{x}=4.758$, $S=0.272$) diğer kıdem gruplarına göre daha yüksek olduğu görülmektedir. Bununla birlikte tek yönlü varyans analizi (ANOVA) sonucunda

öğretmenlerin DVGFÖ puanlarının mesleki kıdemlerine göre istatistiksel olarak anlamlı düzeyde farklılaşmadığı belirlenmiştir, $F(3,279)=2.261$, $p=.082$. Etki büyüklüğünü belirlemek amacıyla hesaplanan eta kare (η^2) değeri .024 olup, bu değer mesleki kıdem in dijital veri güvenliği farkındalığı üzerindeki etkisinin küçük düzeyde olduğunu göstermektedir. Buna göre öğretmenlerin dijital veri güvenliği farkındalıklarının mesleki kıdem değişkenine göre anlamlı bir farklılık göstermediği söylenebilir.

Öğretmenlerin DVGFÖ puanlarının bilgisayar sahipliği durumuna göre farklılık gösterip göstermediğini belirlemek amacıyla gerçekleştirilen bağımsız örneklem t-testi sonuçları Tablo 4.14’te verilmiştir.

Tablo 4.14: DVGFÖ puanlarının bilgisayar sahipliği durumuna göre t-testi sonuçları

Bilgisayar sahipliği	N	$\bar{x}$	S	Levene F	Levene p	t	sd	p	Cohen d
Evet	267	4.576	0.448	0.533	.466	1.043	281	.298	.269
Hayır	16	4.455	0.519						

Not. DVGFÖ: Dijital Veri Güvenliği Farkındalık Ölçeği, N: katılımcı sayısı, $\bar{x}$: ortalama, S: standart sapma

Tablo 4.14’e göre, Cohen d değerinin 0.269 olması, grup ortalamaları arasındaki farkın küçük düzeyde bir etkiye sahip olduğunu göstermektedir. Bu sonuç, bilgisayar sahipliği durumunun dijital veri güvenliği farkındalığı açısından sınırlı bir farklılaşmaya yol açtığı şeklinde yorumlanabilir.

Öğretmenlerin DVGFÖ puanlarının dijital güvenlikle ilgili ders/kurs alma durumuna göre farklılık gösterip göstermediğini belirlemek amacıyla gerçekleştirilen bağımsız örneklem t-testi sonuçları Tablo 4.15’te verilmiştir.

Tablo 4.15: DVGFÖ puanlarının dijital güvenlikle ilgili ders/kurs alma durumuna göre t-testi sonuçları

Dijital güvenlikle ilgili ders/kurs alma	N	$\bar{x}$	S	Levene F	Levene p	t	sd	p	Cohen d
Evet	135	4.686	0.367	11.676	.001	4.306	270	.000	.506
Hayır	148	4.464	0.495						

Not. DVGFÖ: Dijital Veri Güvenliği Farkındalık Ölçeği, N: katılımcı sayısı, $\bar{x}$: ortalama, S: standart sapma.

Tablo 4.15 incelendiğinde dijital güvenlikle ilgili ders/kurs almış öğretmenlerin DVGFÖ puan ortalamasının ($\bar{x}$ =4.686, S=0.367) almamış olanlara ($\bar{x}$ =4.464, S=0.495) kıyasla anlamlı düzeyde yüksek olduğu görülmektedir, $t(270)=4.306$, $p<.001$, Cohen $d=0.506$.

Öğretmenlerin DVGFÖ puanlarının 21. yüzyıl becerileri kavramını bilme durumuna göre farklılık gösterip göstermediğini belirlemek amacıyla gerçekleştirilen bağımsız örneklem t-testi sonuçları Tablo 4.16’da verilmiştir.

Tablo 4.16: DVGFÖ puanlarının 21. yüzyıl becerileri kavramını bilme durumuna göre t-testi sonuçları

21. yüzyıl becerileri kavramını bilme	N	$\bar{x}$	S	Levene F	Levene p	t	sd	p	Cohen d
Evet	249	4.600	0.444	0.504	.478	3.128	281	.002	.572
Hayır	34	4.346	0.450						

Not. DVGFÖ: Dijital Veri Güvenliği Farkındalık Ölçeği, N: katılımcı sayısı, $\bar{x}$: ortalama, S: standart sapma

Tablo 4.16’ya göre 21. yüzyıl becerileri kavramını bildiğini ifade eden öğretmenler, bu kavramı bilmediğini belirtenlere kıyasla DVGFÖ puanları bakımından istatistiksel olarak anlamlı düzeyde daha yüksek puan almıştır, $t(281)=3.128$, $p=.002$, Cohen $d=0.572$.

4.3 Üçüncü Probleme Ait Bulgular

Araştırmanın üçüncü problemi “Öğretmenlerin teknoloji yeterliği öz-değerlendirmeleri ile dijital veri güvenliği farkındalıkları arasında anlamlı bir ilişki var mıdır?” şeklinde belirlenmiştir. Bu probleme yanıt vermek amacıyla YYÖTYÖ puanı, YYÖTYÖ boyutları ve DVGFÖ puanı arasındaki ilişkiyi incelemek için Pearson çarpım momentler korelasyon katsayısı hesaplanmıştır. Analiz sonuçları Tablo 4.17’de verilmiştir.

Tablo 4.17: YYÖTYÖ ve boyutları ile DVGFÖ arasındaki pearson korelasyon analizi sonuçları

Değişken	1. YYÖTY Puanı	2. E-Posta Boyutu Puanı	3. WWW Boyutu Puanı	4. Entegre Uygulamalar Boyutu Puanı	5. Teknolojiyle Öğrenme Boyutu Puanı	6. DVGFÖ Puanı
1. YYÖTY Puanı	—					
2. E-Posta Boyutu Puanı	.567***	—				

Tablo 4.17 (devam)

3. WWW Boyutu Puanı	.505***	.455***	—			
4. Entegre Uygulamalar Boyutu Puanı	.872***	.392***	.322***	—		
5. Teknolojiyle Öğrenme Boyutu Puanı	.936***	.330***	.344***	.749***	—	
6. DVGFÖ Puanı	.605***	.291***	.434***	.427***	.612***	—

Not. YYÖTYÖ: 21. Yüzyıl Öğrenmeleri için Teknoloji Yeterliği Öz-Değerlendirme Ölçeği, DVGFÖ: Dijital Veri Güvenliği Farkındalık Ölçeği, N: katılımcı sayısı, $\bar{x}$: ortalama, S: standart sapma. *** $p < .001$. r : Pearson korelasyon katsayısı.

Tablo 4.17 incelendiğinde YYÖTYÖ puanı ile DVGFÖ puanı arasında pozitif yönlü, güçlü ve istatistiksel olarak anlamlı bir ilişki olduğu görülmektedir, $r=.605$, $p<.001$. Bu bulgu, öğretmenlerin teknoloji yeterliği öz-değerlendirmeleri arttıkça dijital veri güvenliği farkındalıklarının da anlamlı biçimde arttığına işaret etmektedir. Determinasyon katsayısı ($r^2=.366$) göz önüne alındığında DVGFÖ puanlarındaki varyansın yaklaşık %36.6'sının YYÖTYÖ puanlarıyla açıklanabildiği veya YYÖTYÖ puanlarındaki varyansın yaklaşık %36.6'sının DVGFÖ puanlarıyla açıklanabildiği söylenebilir.

YYÖTYÖ boyutları ile DVGFÖ puanı arasındaki ilişkiler incelendiğinde en güçlü ilişkinin Teknolojiyle Öğretim boyutu puanı ile DVGFÖ puanı arasında olduğu görülmektedir ($r=.612$, $p<.001$). Bunu sırasıyla Entegre Uygulamalar boyutu ($r=.427$, $p<.001$), WWW boyutu ($r=.434$, $p<.001$) ve E-posta boyutu ($r=.291$, $p<.001$) puanları DVGFÖ puanı arasındaki korelasyon değerleri izlemektedir. Tüm boyutlar ile DVGFÖ arasındaki korelasyonlar istatistiksel olarak anlamlı olup pozitif yönlüdür.

5. SONUÇ, TARTIŞMA VE ÖNERİLER

Bu bölümde araştırmadan elde edilen bulgular, ilgili alanyazınla karşılaştırmalı biçimde tartışılmış; araştırmanın temel sonuçları sistematik olarak özetlenmiş ve bu sonuçlar doğrultusunda uygulamaya ile ileriki araştırmalara yönelik öneriler geliştirilmiştir.

5.1 Araştırmanın Sonuçları

Araştırmadan elde edilen sonuçlar, problemler çerçevesinde aşağıda özetlenmiştir. Birinci probleme ilişkin sonuçlar:

- Öğretmenlerin YYÖTYÖ puan ortalaması $\bar{x}=4.35$ ($S=0.55$) olup beşli Likert ölçeğinde “tamamen katılıyorum” düzeyine karşılık gelmektedir. Bu sonuç, öğretmenlerin teknoloji yeterliği öz-değerlendirmelerinin yüksek düzeyde olduğunu ortaya koymaktadır.
- YYÖTYÖ boyutlarına ait puanlar incelendiğinde en yüksek ortalamanın WWW boyutuna ($\bar{x}=4.89$), en düşük ortalamanın ise Entegre Uygulamalar boyutuna ($\bar{x}=3.73$) ait olduğu görülmektedir. E-posta ($\bar{x}=4.80$) ve Teknolojiyle Öğretim ($\bar{x}=4.10$) boyutları ara değerlerde yer almaktadır.
- Öğretmenlerin DVGFÖ puan ortalaması $\bar{x}=4.57$ ($S=0.45$) olup “tamamen katılıyorum” düzeyine karşılık gelmektedir. Bu sonuç, öğretmenlerin dijital veri güvenliği farkındalıklarının yüksek düzeyde olduğuna işaret etmektedir.

İkinci probleme ilişkin sonuçlar:

- Cinsiyet değişkeni açısından erkek öğretmenler, kadın öğretmenlere kıyasla hem YYÖTYÖ [$t(281)=3.291$, $p=.001$, Cohen $d=.403$] hem de DVGFÖ [$t(267)=3.676$, $p<.001$, Cohen $d=.422$] puanlarında istatistiksel olarak anlamlı biçimde daha yüksek puan almıştır.
- Görev türü değişkeni açısından yöneticiler, öğretmenlere kıyasla YYÖTYÖ puanlarında anlamlı düzeyde daha yüksek puan almıştır [$t(208)=2.741$, $p=.007$, Cohen $d=.310$]. DVGFÖ puanlarında ise görev türüne göre anlamlı farklılık saptanmamıştır [$t(281)=0.537$, $p=.592$].
- Eğitim düzeyi değişkeni açısından yüksek lisans-doktora mezunu öğretmenler, ön lisans-lisans mezunlarına kıyasla YYÖTYÖ puanlarında anlamlı düzeyde daha yüksek puan almıştır [$t(248)=4.884$, $p<.001$, Cohen $d=.538$]. DVGFÖ puanlarında ise eğitim düzeyine göre anlamlı farklılık bulunmamaktadır [$t(281)=1.677$, $p=.095$].

- Mesleki kıdem değişkeni açısından ne YYÖTYÖ [F(3,279)=0.436, p=.728] ne de DVGFÖ [F(3,279)=2.261, p=.082] gruplar arasında puanlar bakımından istatistiksel olarak anlamlı bir farklılık olmadığı saptanmıştır.
- Bilgisayar sahipliği değişkeni açısından kişisel bilgisayara sahip öğretmenler, sahip olmayanlara kıyasla YYÖTYÖ puanlarında anlamlı düzeyde daha yüksek puan almıştır [t(281)=2.068, p=.040, Cohen d=.532]. DVGFÖ puanlarında ise anlamlı farklılık bulunmamaktadır [t(281)=1.043, p=.298].
- Ders/kurs alma değişkeni açısından dijital güvenlikle ilgili ders/kurs almış öğretmenler, almamış olanlara kıyasla hem YYÖTYÖ [t(281)=4.190, p<.001, Cohen d=.499] hem de DVGFÖ [t(270)=4.306, p<.001, Cohen d=.506] puanlarında anlamlı düzeyde daha yüksek puan almıştır.
- 21. yüzyıl becerileri kavramını bilme değişkeni açısından kavramı bildiğini ifade eden öğretmenler, bu kavramı bilmediğini belirtenlere kıyasla hem YYÖTYÖ [t(281)=3.817, p<.001, Cohen d=.698] hem de DVGFÖ [t(281)=3.128, p=.002, Cohen d=.572] puanlarında anlamlı düzeyde daha yüksek puan almıştır. YYÖTYÖ için en güçlü etki büyüklüğü bu değişkende gözlemlenmiştir (Cohen d=.698).

Üçüncü probleme ilişkin sonuçlar:

- YYÖTYÖ puanı ile DVGFÖ puanı arasında pozitif yönlü, güçlü ve istatistiksel olarak anlamlı bir ilişki saptanmıştır ($r=.605$, $p<.001$). Determinasyon katsayısına göre DVGFÖ puanlarındaki varyansın %36.6'sı YYÖTYÖ puanlarıyla açıklanabilmektedir.
- YYÖTYÖ boyutları ile DVGFÖ puanları arasındaki ilişkiler incelendiğinde en güçlü ilişkinin Teknolojiyle Öğretim boyutu ile DVGFÖ puanları arasında olduğu görülmektedir ($r=.612$, $p<.001$). Tüm boyutlar ile DVGFÖ puanları arasındaki korelasyonlar pozitif yönlü ve istatistiksel olarak anlamlıdır.

5.2 Tartışma

Bu bölümde araştırmadan elde edilen bulgular ilgili alanyazınla karşılaştırmalı biçimde ele alınmıştır. Tartışma, araştırmanın problemleri temel alınarak düzenlenmiştir.

5.2.1 Birinci probleme ilişkin tartışma

Bu araştırmada öğretmenlerin YYÖTYÖ puan ortalamasının yüksek düzeyde ($\bar{x}=4.35$) olduğu belirlenmiştir. Bu sonuç, araştırmanın yürütüldüğü ilin dışında ve farklı kurum

türlerinde yürütülen çalışmalarla büyük ölçüde örtüşmektedir. Okur-Türk (2024), Erzurum ilinde 400 öğretmenle yürüttüğü araştırmasında teknoloji yeterliği öz-değerlendirmelerinin yüksek düzeyde olduğunu ortaya koymuştur. Söz konusu bulguların tutarlılığı, Türkiye’deki öğretmenlerin genel olarak teknoloji yeterliği konusunda kendilerini yetkin algıladıklarına işaret ettiği şeklinde yorumlanabilir.

Bununla birlikte bu çalışmada YYÖTYÖ boyutları arasında dikkat çekici bir örüntü göze çarpmaktadır: WWW ($\bar{x}=4.89$) ve E-posta ($\bar{x}=4.80$) boyutları yüksek ortalamalara ulaşırken Entegre Uygulamalar boyutu ($\bar{x}=3.73$) belirgin biçimde daha düşük kalmıştır. Bu bulgu, Gülen’in (2013) 612 ortaokul öğrencisiyle yürüttüğü çalışmasında öğrencilerin temel 21. yüzyıl becerilerine iyi düzeyde sahip olmalarına karşın bu becerileri BT ile destekleme düzeylerinin orta seviyede kaldığı sonucu ile kavramsal bir paralellik taşımaktadır. Her iki çalışma da temel teknoloji kullanım becerilerinin güçlü, ileri düzey teknoloji entegrasyon becerilerinin ise sınırlı olduğuna işaret etmektedir. Öğretmenlerin grafik oluşturma, veri tabanı hazırlama ve uygulama yazılımlarını dersleriyle bütünleştirme gibi karmaşık teknoloji becerilerinde kendilerini daha az yetkin hissetmeleri, bu alanlarda hizmet içi eğitimlere olan ihtiyacı gündeme taşımaktadır.

Öğretmenlerin DVGFÖ puan ortalamasının yüksek düzeyde ($\bar{x}=4.57$) olduğu belirlenmiştir. Bu bulgu, Yılmaz (2015) tarafından gerçekleştirilen ölçek geliştirme çalışmasının bulgularıyla ($\bar{x}=4.16$) ve Yılmaz vd., (2016) aynı ölçeği 870 öğretmene uyguladığı çalışmasının sonuçlarıyla tutarlılık göstermektedir. Bu çalışmada elde edilen ortalamanın söz konusu çalışmalara kıyasla daha yüksek çıkması; geçen süre içinde öğretmenlerin dijital veri güvenliği konusundaki bilinç düzeyinin arttığına ya da örneklem özelliklerindeki farklılıklara bağlanabilir. Nitekim bu çalışmada elde edilen sonuçlara benzer olarak Aksoğan ve Atıcı (2023) ve Gökkaya-Babacan (2025) da farklı örneklemelerle yürüttükleri araştırmalarda katılımcıların dijital veri güvenliği farkındalık düzeylerini yüksek ya da yeterli olarak nitelendirmiştir.

5.2.2 İkinci probleme ilişkin tartışma

Bu çalışmada erkek öğretmenlerin hem YYÖTYÖ hem de DVGFÖ puanlarında kadın öğretmenlerden anlamlı düzeyde daha yüksek puan aldığı saptanmıştır. 21. yüzyıl öğrenmelerinde teknoloji yeterliği öz-değerlendirmeleri açısından alanyazında çelişkili

sonular bulunmaktadır. Kozikoęlu ve Altunova (2018) ile Erten (2020), cinsiyet deęiřkeninin 21. yzyıl yeterlik z-deęerlendirme dzeyleri zerinde anlamlı bir farklılık oluřturmadıęını belirlemiřtir. Buna karřın bu arařtırmada erkek ęretmenler lehine anlamlı bir farklılık elde edilmiřtir.

Dijital veri gvenlięi farkındalıęı aısından elde edilen bulgular ise alanyazınla byk lde rtřmektedir. Yılmaz (2015), Yılmaz vd. (2016), Hızmal (2022), Gldaę (2021), Aksoęan ve Atıcı (2023) ile Gkkaya-Babacan'ın (2025) arařtırmalarında erkeklerin dijital veri gvenlięi farkındalıęı bakımından kadınlara kıyasla anlamlı dzeyde daha yksek puanlara sahip olduęu belirlenmiřtir. Bu arařtırmada elde edilen bulgu da sz konusu alıřmaların sonularını destekler niteliktedir. Alanyazında farklı rneklemeler zerinde gerekleřtirilen arařtırmalarda benzer sonuların elde edilmesi, dijital veri gvenlięi farkındalıęı aısından erkeklerin kadınlara gre daha yksek puan alma eęiliminin tekrarlanan bir bulgu olduęunu gstermektedir. Bu durum, cinsiyet deęiřkeninin dijital veri gvenlięi farkındalıęı ile iliřkili olabilecek nemli deęiřkenlerden biri olarak deęerlendirilebileceęini dřndrmektedir.

Grev tr deęiřkeni aısından yneticilerin ęretmenlere kıyasla YYTY puanlarında anlamlı dzeyde daha yksek puan aldıęı belirlenmiřtir. Bu bulgunun doęrudan karřılařtırılabileceęi bir alıřma alanyazında sınırlı olmakla birlikte yneticilerin teknolojiyi kurumsal dzeyde planlama, koordinasyon ve denetim gibi iřlevler iin kullandıkları dřnldęnde daha yksek teknoloji yeterlięi sergilemelerinin beklenen bir sonu olduęu sylenebilir. DVGf puanlarında grev trne gre anlamlı farklılık saptanmaması ise dijital veri gvenlięi farkındalıęının rol kaynaklı deęil, bireysel eęitim ve deneyimle řekillenen bir yetkinlik olduęuna iřaret ettięi yorumu yapılabilir.

Eęitim dzeyi deęiřkeni aısından yksek lisans ya da doktora mezunu ęretmenlerin YYTY puanlarında anlamlı dzeyde daha yksek puan aldıęı bulunmuřtur. Bu bulgunun doęrudan karřılařtırılabileceęi bir alıřma alanyazında sınırlı olmakla birlikte, lisansst eęitimin arařtırma becerilerini, teknoloji aralarına ynelik farkındalıęı ve z-ynetimli ęrenme eęilimini geliřtirdięi dřnldęnde bu sonucun anlařılır olduęu yorumu yapılabilir.

DVGfÖ puanları açısından eğitim düzeyine göre istatistiksel olarak anlamlı bir farklılık saptanmamıştır. Bu bulgu, Yılmaz (2015) ve Yılmaz vd. (2016) tarafından yapılan çalışmalarda eğitim düzeyi değişkenine göre dijital veri güvenliği farkındalığında anlamlı bir farklılık bulunmamasıyla benzerlik göstermektedir. Bu durum, dijital veri güvenliği farkındalığının yalnızca formal eğitim düzeyiyle değil; bireylerin teknoloji kullanım deneyimleri, dijital güvenlik konusunda aldıkları özel eğitimler ve günlük dijital pratikleriyle de ilişkili olabileceği yorumu yapılabilir.

Mesleki kıdem değişkeni açısından ne YYÖTYÖ ne de DVGfÖ puanlarında gruplar arasında anlamlı farklılık saptanmıştır. YYÖTYÖ açısından Okur-Türk (2024), yaş ve görev yılının 21. yüzyıl teknoloji yeterliği öz-değerlendirmeleri üzerinde anlamlı farklılık yaratan değişkenler olduğunu ortaya koymuştur; bu çalışmada ise mesleki kıdeme göre anlamlı farklılık saptanmamıştır. Bu durum, mesleki kıdem değişkenine ilişkin bulguların alanyazında her zaman aynı yönde olmadığı söylenebilir. DVGfÖ için elde edilen sonuç ise Yılmaz (2015), Yılmaz vd. (2016) ile Gökkaya-Babacan'ın (2025) çalışmalarında mesleki kıdem değişkenine ilişkin elde edilen bulgularla benzerlik göstermektedir. Bu çalışmada mesleki kıdeme göre anlamlı farklılık bulunmaması, öğretmenlerin teknoloji yeterliği öz-değerlendirmeleri ve dijital veri güvenliği farkındalıklarının yalnızca mesleki deneyim süresiyle açıklanamayabileceğini düşündürmektedir. Bu bağlamda, teknoloji kullanımı, dijital güvenlik konusunda alınan eğitimler ve bireysel teknoloji deneyimleri gibi farklı değişkenlerin de etkili olabileceği söylenebilir.

Bilgisayar sahipliği değişkeni açısından kişisel bilgisayara sahip öğretmenlerin YYÖTYÖ puanlarında anlamlı düzeyde daha yüksek puan aldığı belirlenmiştir. Bu sonuç, Önür'ün (2018) bilgisayar, tablet ve akıllı telefon gibi dijital araçlara erişim olanağı olan öğrencilerin 21. yüzyıl öğrenme becerileri ile eğitim teknolojisi yeterliklerinde anlamlı düzeyde daha yüksek puan aldığını ortaya koyan bulgularıyla örtüşmektedir. Şahin (2025) de bilgisayara sahip ilköğrencilerinin teknik bilgi ve 21. yüzyıl öğrenme deneyimi algılarının bilgisayarı olmayanlara kıyasla anlamlı düzeyde daha yüksek olduğunu bümüştür. DVGfÖ puanlarında ise bilgisayar sahipliğine göre anlamlı farklılık saptanmamıştır. Bu sonuç, dijital güvenlik farkındalığının yalnızca cihaz sahipliğiyle değil, bu cihazları güvenli biçimde kullanmaya ilişkin bilgi ve tutumlarla da yakından ilişkili olduğuna işaret ettiği şeklinde yorumlanabilir. Ayrıca bilgisayarı olmayan grubun örneklem büyüklüğünün oldukça küçük

olduğu (n=16) göz önünde bulundurulduğunda bu bulgunun dikkatli yorumlanması gerektiği ifade edilebilir.

Bu araştırmada en güçlü etkiyi üreten değişkenlerden birinin dijital güvenlikle ilgili ders/kurs alma durumu olduğu görülmüştür. Dijital güvenlikle ilgili ders/kurs almış öğretmenler her iki ölçekte de anlamlı düzeyde daha yüksek puan almış; etki büyüklükleri hem YYÖTYÖ (Cohen d=.499) hem de DVGFÖ (Cohen d=.506) için orta düzeye ulaşmıştır. Bu bulgu, Erten'in (2020) BİT yeterliliğinin 21. yüzyıl becerilerine sahip olmada belirleyici bir etken olduğunu vurguladığı sonuçlarıyla örtüşmektedir. Yılmaz (2015) de araştırmasında MEB tarafından hayata geçirilen projelerde dijital veri güvenliğine yeterince yer verilmediğini ve bu eksikliğin giderilmesi gerektiğini vurgulayarak dijital güvenlikle ilgili eğitim almış öğretmenlerin daha yüksek farkındalık düzeyine sahip olacağını öngörmüştür. Söz konusu bulgular birlikte değerlendirildiğinde, nitelikli hizmet içi eğitim programlarının öğretmenlerin hem teknoloji yeterliği hem de dijital güvenlik farkındalığı üzerinde güçlü ve olumlu etkiler doğurduğu yorumu yapılabilir.

21. yüzyıl becerileri kavramını bilme durumu ise bu araştırmada teknoloji yeterliği öz-değerlendirmeleri üzerinde en güçlü etki büyüklüğünü üreten demografik değişken olarak öne çıkmıştır (Cohen d=.698). Kavramı bildiğini ifade eden öğretmenler, bilmediğini belirtenlere kıyasla hem YYÖTYÖ hem de DVGFÖ puanlarında anlamlı düzeyde üstünlük sağlamıştır. Erten (2020), BİT alanındaki yeterliliğin 21. yüzyıl becerilerini kazanmada etkili olduğunu ortaya koymuş; Kozikoğlu ve Altunova (2018) öğretmen adaylarının 21. yüzyıl becerilerine ilişkin öz-yeterlik algıları ile yaşam boyu öğrenme eğilimleri arasındaki olumlu ilişkiyi belgelemiştir. Bu araştırmanın bulgusu söz konusu çalışmalarla kavramsal açıdan örtüşmekte; kavramsal farkındalığın pratik yetkinliklerle güçlü biçimde ilişkili olduğunu gözler önüne sermekte olduğu yorumu yapılabilir. Bir kavramın adını bilmek ve içeriğini özümsemek, öğretmenlerin eğitim gündemlerinde bu alana daha fazla yer ayırmalarını ve kendilerini geliştirme motivasyonlarını artırmalarını kolaylaştırabilir.

5.2.3. Üçüncü probleme ilişkin tartışma

Bu araştırmada YYÖTYÖ ile DVGFÖ puanları arasında pozitif yönlü, güçlü ve istatistiksel olarak anlamlı bir ilişki saptanmıştır ($r=.605$, $p<.001$). Bu bulgu; teknoloji yeterliği öz-değerlendirmesinin ve dijital veri güvenliği farkındalığının birbirleriyle ilişkili yetkinlik alanları olduğunu ortaya koymakta ve öğretmenlerin teknoloji yeterliği öz-değerlendirmeleri

arttıkça dijital güvenlik farkındalıklarının da paralel biçimde yükseldiğine gösterdiği şekilde yorumlanabilir.

Alanyazında doğrudan bu iki değişkeni birlikte ele alan çalışmalar bulunmamakla birlikte konuya dolaylı biçimde ışık tutan pek çok araştırma mevcuttur. Gökkaya-Babacan (2025), lise öğretmenlerinin TPAB yeterlikleri ile dijital veri güvenliği farkındalık düzeyleri arasında pozitif yönlü anlamlı bir ilişki bulmuş; TPAB düzeyleri yüksek öğretmenlerin dijital veri güvenliği farkındalığı açısından da daha yetkin olduğunu belirlemiştir. Göldağ (2021) üniversite öğrencilerinde dijital okuryazarlık ile dijital veri güvenliği farkındalığı arasında yüksek düzeyde pozitif yönlü anlamlı bir ilişki saptamış; İbekçi (2025) ise aynı değişkenler arasında orta düzeyde pozitif yönlü anlamlı bir ilişki tespit etmiştir. Öztürk ve Çakır (2022) da öğretmenlerde dijital oyunlardan yararlanma ile dijital veri güvenliği farkındalıkları arasında pozitif yönlü anlamlı bir bağ bulmuştur. Bu çalışmalar bir arada değerlendirildiğinde, dijital yetkinliğin farklı boyutlarının birbirini besleyen ve pekiştiren bir bütünlük oluşturduğu şeklinde yorum yapılabilir.

Bu çalışmada YYÖTYÖ boyutları arasında DVGFÖ ile en güçlü ilişkinin Teknolojiyle Öğretim boyutunda gözlemlenmesi ($r=.612$) anlamlı bir bulgudur. Pedagojik süreçlerde teknolojiyi işlevsel biçimde kullanan öğretmenler, dijital araçların güvenli kullanımı konusunda da daha yüksek farkındalık geliştirmiş olduğu ifade edilebilir. Bu sonuç, Okur-Türk'ün (2024) YYÖTYÖ puanlarının yapılandırmacı yaklaşımı uygulamaya yönelik öz-yeterliği anlamlı biçimde yordadığını ortaya koyduğu bulgusuyla da uyum içindedir. Tüm bu sonuçları; teknoloji yeterliği ile dijital güvenlik farkındalığının bütünlük bir perspektifle ele alınması gerektiğini güçlü biçimde desteklediği yorumlanabilir.

5.3 Öneriler

Bu çalışmadan elde edilen bulgular ve yürütülen tartışmalar doğrultusunda, uygulamaya ve gelecekte gerçekleştirilecek araştırmalara yönelik öneriler aşağıda sunulmuştur.

5.3.1 Uygulamaya yönelik öneriler

Bu çalışmada, YYÖTYÖ'nün entegre uygulamalar boyutundan elde edilen puanların diğer boyutlara kıyasla daha düşük düzeyde kalması dikkat çekici bir bulgu olarak değerlendirilebilir. Bu doğrultuda, Millî Eğitim Bakanlığı ve üniversiteler tarafından öğretmenlerin ileri düzey teknoloji entegrasyon becerilerini geliştirmeye yönelik uygulamalı

hizmet içi eğitim modülleri hazırlanabilir. Bu eğitimlerde grafik oluşturma, veri tabanı hazırlama, dijital içerik üretme ve uygulama yazılımlarını öğretim süreçleriyle bütünleştirme gibi becerilere ağırlık verilmesi, öğretmenlerin teknolojiyi pedagojik amaçlarla daha etkili kullanmalarına katkı sağlayabilir.

Dijital güvenlikle ilgili ders ya da kurs alma değişkeninin her iki ölçekten elde edilen puanlar üzerinde anlamlı ve güçlü bir etkiye sahip olması, teknoloji yeterliği ile dijital veri güvenliği farkındalığının birlikte ele alınmasının önemini ortaya koyabilir. Bu kapsamda, MEB tarafından yürütülen hizmet içi eğitimlerde teknoloji yeterliği ile dijital veri güvenliği farkındalığı konuları bütüncül bir anlayışla ele alınabilir. Söz konusu eğitimler yalnızca teknik bilgi aktarımıyla sınırlı kalmayıp, güvenli dijital davranış örüntülerinin kazandırılmasına da odaklanabilir.

21. yüzyıl becerileri kavramını bilme değişkeninin YYÖTYÖ ve DVGFÖ puanları üzerinde güçlü bir etki büyüklüğü oluşturduğunu göstermektedir. Bu sonuç doğrultusunda, okul yöneticileri ve öğretmenlerin 21. yüzyıl becerilerine ilişkin kavramsal farkındalıklarını artırmaya yönelik seminer, atölye çalışması ve mesleki gelişim programları çeşitlendirilebilir. Böylece öğretmenlerin dijital yeterlik, eleştirel düşünme, problem çözme, iş birliği, iletişim ve dijital güvenlik gibi çağdaş eğitim süreçlerinde öne çıkan becerilere yönelik farkındalıkları desteklenebilir.

Cinsiyet değişkeni açısından erkek öğretmenlerin hem YYÖTYÖ hem de DVGFÖ puanlarında kadın öğretmenlerden anlamlı düzeyde daha yüksek puan aldığı belirlenmiştir. Bu bulgu doğrultusunda, kadın öğretmenlerin teknoloji kullanımı ve dijital veri güvenliği alanındaki mesleki gelişim gereksinimlerini desteklemeye yönelik uygulamalı hizmet içi eğitimler düzenlenebilir. Bu eğitimlerde kişisel ve öğrenci verilerinin korunması, güvenli dosya paylaşımı, güçlü parola oluşturma, iki aşamalı doğrulama ve sosyal medya gizlilik ayarları gibi konulara yer verilerek öğretmenlerin teknoloji öz yeterlikleri ve dijital güvenlik farkındalıkları desteklenebilir.

Araştırmada, okul yöneticilerinin YYÖTYÖ puanlarının öğretmenlere kıyasla anlamlı düzeyde yüksek olduğu sonucuna ulaşılmıştır. Bu bulgu, okul yöneticilerinin teknoloji kullanımına ilişkin yeterliklerinin okul geneline yaygınlaştırılmasını sağlayacak liderlik mekanizmalarının işletilmesi gerektiğini düşündürülebilir. Bu doğrultuda, okul yöneticileri

teknoloji entegrasyonu ve dijital güvenlik kültürünün okul ikliminin bir parçası hâline getirilmesi sürecinde aktif roller üstlenebilir. Ayrıca yöneticiler, öğretmenleri dijital araçların etkili ve güvenli kullanımı konusunda destekleyerek okul düzeyinde sürdürülebilir bir dijital güvenlik kültürünün oluşmasına katkı sağlayabilir.

EBA ve ÖBA gibi eğitim platformlarının içeriklerinde siber güvenlik, kişisel verilerin korunması, dijital etik, güvenli internet kullanımı ve dijital veri güvenliği konularına daha kapsamlı biçimde yer verilebilir. Bu platformlarda yer alacak modüller, erişilebilir ve uygulama temelli içerikler, öğretmenlerin dijital güvenlik farkındalıklarını sürdürülebilir biçimde geliştirmelerine katkı sağlayabilir. Ayrıca bu içeriklerin belirli aralıklarla güncellenmesi, öğretmenlerin dijital güvenlik alanındaki güncel riskler ve yeni uygulamalar konusunda bilinçli kalmasını destekleyebilir.

Araştırma bulguları YYÖTYÖ ile DVGFO puanları arasındaki güçlü pozitif ilişkiyi ortaya koymaktadır. Bu ilişkinin güçlü çıkması, teknoloji yeterliği ile dijital veri güvenliği farkındalığının benzer dijital yeterlik alanlarıyla ilişkili olmasından kaynaklanmış olabilir. Alanyazında dijital okuryazarlık, teknoloji yeterliği ve siber güvenlik farkındalığı arasında anlamlı ilişkiler bulunduğunu gösteren çalışmalar bu yorumu desteklemektedir (Elrayah and Jamil, 2023; Göldağ, 2021; Leung et al., 2026). Bu nedenle teknolojiyi pedagojik amaçlarla etkili kullanabilen öğretmenlerin, dijital ortamlardaki güvenlik risklerini tanıma ve verileri koruma konusunda da daha bilinçli olmaları beklenebilir.

5.3.2 İleride yapılacak araştırmalara yönelik öneriler

Bu araştırma, devlet okullarında görev yapan okul yöneticileri ve öğretmenlerle sınırlı tutulmuştur. Bulguların genellenebilirliğini artırmak amacıyla, ileride yapılacak araştırmalar farklı il, bölge ve okul türlerinden seçilecek daha geniş örneklemeler üzerinde gerçekleştirilebilir. Bu tür çalışmalar, farklı sosyo-kültürel ve kurumsal bağlamlarda elde edilecek bulguların karşılaştırılmasına olanak sağlayabilir.

Bu çalışmada, 21. yüzyıl öğrenmelerinde teknoloji yeterliği öz-değerlendirme düzeyi ile dijital veri güvenliği farkındalığı arasındaki ilişki korelasyonel düzeyde incelenmiştir. İleride gerçekleştirilecek çalışmalarda, söz konusu değişkenler arasındaki doğrudan ve dolaylı ilişkileri daha kapsamlı biçimde ortaya koymak amacıyla yapısal eşitlik modellemesi kullanılabilir. Ayrıca teknoloji yeterliği öz-değerlendirme puanlarının ve çeşitli demografik

değişkenlerin dijital veri güvenliği farkındalığı üzerindeki yordayıcı etkileri çoklu regresyon analizi ile daha ayrıntılı biçimde incelenebilir.

Dijital güvenlikle ilgili ders ya da kurs alma durumu ile 21. yüzyıl becerileri kavramını bilme değişkenlerinin, YYÖTYÖ ve DVGFÖ puanları üzerinde güçlü etkiler oluşturduğu görülmektedir. Bu doğrultuda, ileride yapılacak araştırmalarda bu değişkenlere yönelik geliştirilecek eğitim, seminer, atölye ya da müdahale programlarının etkililiğini inceleyen deneysel veya yarı deneysel çalışmalar tasarlanabilir. Böylece öğretmenlerin teknoloji yeterliği öz-değerlendirmeleri ve dijital veri güvenliği farkındalık düzeyleri üzerinde söz konusu programların etkisi daha somut biçimde değerlendirilebilir.

Bu araştırma yalnızca okul yöneticileri ve öğretmenleri kapsamaktadır. Gelecekte yapılacak çalışmalarda öğrenciler, öğretmen adayları ve farklı eğitim paydaşları da araştırma sürecine dâhil edilebilir. Bu kapsamda yürütülecek karşılaştırmalı çalışmalar, eğitim sisteminin farklı paydaşlarının teknoloji yeterliği öz-değerlendirme düzeyleri ile dijital veri güvenliği farkındalık profillerinin bütüncül biçimde ortaya konulmasına katkı sağlayabilir.

Araştırmada nicel araştırma yöntemi kullanılmıştır. İlerleyen çalışmalarda, nicel bulgulara nitel bir derinlik kazandırmak amacıyla karma yöntem araştırmaları tasarlanabilir. Görüşme, odak grup görüşmesi ve gözlem gibi nitel veri toplama teknikleri aracılığıyla öğretmenlerin teknoloji yeterliği öz-değerlendirmelerine ve dijital veri güvenliği farkındalıklarına ilişkin deneyimleri, algıları, tutumları ve uygulamaları daha ayrıntılı biçimde incelenebilir.

Bu araştırmanın sonuçları, devlet okullarında görev yapan katılımcılardan elde edilen verilerle sınırlıdır. Bu nedenle ileride özel öğretim kurumlarında görev yapan öğretmenlerle benzer araştırmalar yürütülebilir. Böylece farklı kurumsal koşulların öğretmenlerin 21. yüzyıl öğrenmelerinde teknoloji yeterliği öz-değerlendirme düzeyleri ve dijital veri güvenliği farkındalıklarıyla ilişkisi incelenebilir. Özel ve devlet okullarının teknolojik altyapıları, hizmet içi eğitim olanakları, dijital güvenlik politikaları ve teknoloji kullanım kültürleri farklılık gösterebileceğinden, farklı örneklemeler üzerinde gerçekleştirilecek çalışmalar mevcut bulguların karşılaştırılmasına ve genellenebilirliğinin değerlendirilmesine katkı sağlayabilir.

6. KAYNAKLAR

- Ackoff, R. L.** (1989). From data to wisdom. *Journal of Applied Systems Analysis*, 16, 3-9.
<https://faculty.ung.edu/kmelton/documents/datawisdom.pdf>
- Ak, G., Kılınç, Ş., Yazçayır, G. ve Kıyak, Ü. E.** (2022). Özel eğitim öğretmenlerinin öğrencileriyle ilgili sosyal medya paylaşımlarının incelenmesi. *Ankara Üniversitesi Eğitim Bilimleri Fakültesi Özel Eğitim Dergisi*, 23(3), 263-280.
<https://doi.org/10.12984/egeefd.1090493>
- Aksoğan, M. ve Atıcı, B.** (2023). Akademisyenlerin dijital veri güvenliği farkındalıkları üzerine bir araştırma: Malatya örneği. *Gümüşhane Üniversitesi Sosyal Bilimler Dergisi*, 14(2), 429-439. <https://doi.org/10.36362/gumus.1139840>
- Alqahtani, M. A.** (2022). Factors affecting cybersecurity awareness among university students. *Applied Sciences*, 12(5), 2589. <https://doi.org/10.3390/app12052589>
- Andrade, H. L.** (2019). A critical review of research on student self-assessment. *Frontiers in Education*, 4, 87. <https://doi.org/10.3389/educ.2019.00087>
- Arslan, A.** (2020). Öğretmen adayları perspektifinden pandemi öncesi ve sonrası öğrencilere kazandırılması gereken 21. yüzyıl becerilerinin belirlenmesi. *Milli Eğitim Dergisi*, 49(Özel Sayı), 553-571. <https://doi.org/10.37669/milliegitim.779446>
- Arslan, G. B., Kızılay, E. ve Hamalosmanoğlu, M.** (2022). Eğitimde teknoloji entegrasyonu ile ilgili Türkiye’de yapılan çalışmaların incelenmesi. *Anadolu Üniversitesi Eğitim Fakültesi Dergisi*, 6(1), 39-55.
<https://doi.org/10.34056/aujef.976627>
- Arslankara, V. B. ve Seferoğlu, S. S.** (2019, 2-4 Mayıs). Öğretmenlerin dijital ayak izi farkındalık durumlarıyla ilgili bir inceleme. *13th International Computer and Instructional Technologies Symposium*. Kırşehir Üniversitesi, Kırşehir, Türkiye.
- Avcı, Ü. ve Arslan, E.** (2019). Dijital veri güvenliği farkındalığı ve bilgi okuryazarlığı ile alınan hizmetiçi eğitimin etkisi. *Ankara Üniversitesi Eğitim Bilimleri Fakültesi Dergisi*, 52(3), 891-914. <https://doi.org/10.30964/auebfd.493124>
- Avrupa Komisyonu [European Commission]** (t.y.). *Data protection explained*. https://commission.europa.eu/law/law-topic/data-protection/data-protection-explained_en

KAYNAKLAR DİZİNİ (devamı)

- Ay, S. ve Kılıç, T.** (2023). Coğrafi dijital uçurum: Türkiye’de dijital dönüşümün kentsel-kırsal, bölgesel ve cinsiyet eşitsizlikleri. *Coğrafya Dergisi*, 46, 111-122. <https://doi.org/10.26650/JGEOG2023-1169477>
- Aydemir, H., Karalı, Y. ve Coşanay, G.** (2020). Sosyal bilgiler öğretmen adaylarının 21. yüzyıl öğretme ve öğrenen becerilerinin incelenmesi. *Uluslararası Sosyal Bilimler Akademi Dergisi*, 2(4), 1199-1214. <https://doi.org/10.47994/usbad.824081>
- Bandura, A.** (1986). *Social foundations of thought and action: A social cognitive theory*. Prentice Hall. <https://archive.org/details/socialfoundation0000band>
- Baslyman, M.** (2022). Digital transformation from the industry perspective: Definitions, goals, conceptual model, and processes. *IEEE Access*, 10, 42961-42970. <https://doi.org/10.1109/ACCESS.2022.3166937>
- Bayar, A. ve Korkmaz, B.** (2022). Eğitimcilerin öğrencilerin kişisel verilerinin korunması konusundaki görüşleri. *Trakya Eğitim Dergisi*, 12(1), 133-147. <https://doi.org/10.24315/tred.880005>
- Bhatnagar, N. and Pry, M.** (2020). Student attitudes, awareness, and perceptions of personal privacy and cybersecurity in the use of social media: An initial study. *Information Systems Education Journal*, 18(1), 48-58. <https://files.eric.ed.gov/fulltext/EJ1246231.pdf>
- Birleşmiş Milletler Eğitim, Bilim ve Kültür Örgütü (United Nations Educational, Scientific and Cultural Organization [UNESCO])** (2003). *Charter on the preservation of the digital heritage*. UNESCO. <https://www.unesco.org/en/legal-affairs/charter-preservation-digital-heritage>
- Birleşmiş Milletler Eğitim, Bilim ve Kültür Örgütü (United Nations Educational, Scientific and Cultural Organization [UNESCO])** (2023). *Global education monitoring report 2023: Technology in education—A tool on whose terms?* UNESCO. <https://doi.org/10.54676/UZQV8501>
- Birleşmiş Milletler Ticaret ve Kalkınma Konferansı (United Nations Conference on Trade and Development [UNCTAD])** (2024). *Digital economy report 2024: Shaping an environmentally sustainable and inclusive digital future*. United Nations. <https://digitallibrary.un.org/record/4053817>

KAYNAKLAR DİZİNİ (devamı)

- Bjerke-Busch, L. S. and Aspelund, A.** (2021). Identifying barriers for digital transformation in the public sector. In D. R. A. Schallmo & J. Tidd (Eds.), *Digitalization: Approaches, case studies, and tools for strategy, transformation and implementation* (pp. 277-290). Springer. https://doi.org/10.1007/978-3-030-69380-0_15
- Boole, G.** (1854/2005). *An investigation of the laws of thought*. Project Gutenberg. <https://www.gutenberg.org/files/15114/15114-pdf.pdf>
- Brennen, J. S. and Kreiss, D.** (2016). Digitalization. In K. B. Jensen, R. T. Craig, J. D. Pooley, and E. W. Rothenbuhler (Eds.), *The International Encyclopedia of Communication Theory and Philosophy* (pp. 1-11). Wiley. <https://doi.org/10.1002/9781118766804.wbiect111>
- Bughin, J., LaBerge, L. and Mellbye, A.** (2017). *The case for digital reinvention*. McKinsey Quarterly.
- Bulunmaz, B.** (2016). Gelişen teknolojiyle birlikte değişen pazarlama yöntemleri ve dijital pazarlama. *TRT Akademi*, 1(2), 348-365. <https://izlik.org/JA63LK88NL>
- Büyüköztürk, Ş.** (2023). *Sosyal bilimler için veri analizi el kitabı: İstatistik, araştırma deseni, SPSS uygulamaları ve yorum*. Pegem Akademi.
- Büyüköztürk, Ş., Kılıç Çakmak, E., Erkan Akgün, Ö., Karadeniz, Ş. ve Demirel, F.** (2016). *Bilimsel araştırma yöntemleri*. Pegem Akademi.
- Canbek, G. ve Sağıroğlu, Ş.** (2006). Bilgi, bilgi güvenliği ve süreçleri üzerine bir inceleme. *Politeknik Dergisi*, 9(3), 165-174. <https://izlik.org/JA25AP56JY>
- Canbek, G. ve Sağıroğlu, Ş.** (2007a). Bilgisayar sistemlerine yapılan saldırılar ve türleri: Bir inceleme. *Erciyes Üniversitesi Fen Bilimleri Enstitüsü Dergisi*, 23(1-2), 1-12. <https://izlik.org/JA29EH89AK>
- Canbek, G. ve Sağıroğlu, Ş.** (2007b). Kötücül ve casus yazılımlar: Kapsamlı bir araştırma. *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi*, 22(1), 121-136. <https://izlik.org/JA46RM92RC>
- Chmura, J.** (2017). Forming the awareness of employees in the field of information security. *Journal of Positive Management*, 8(1), 78-85. <https://doi.org/10.12775/JPM.2017.006>

KAYNAKLAR DİZİNİ (devamı)

- Christensen, R. and Knezek, G.** (2017). Validating the technology proficiency self-assessment questionnaire for 21st century learning (TPSA C-21). *Journal of Digital Learning in Teacher Education*, 33(1), 20-31. <https://doi.org/10.1080/21532974.2016.1242391>
- Çetinkaya, L. ve Öktelik, B.** (2022). Ortaokul düzeyi öğrencilerine yönelik bilgi güvenliği farkındalık ölçeği geliştirme çalışması. *Cumhuriyet Uluslararası Eğitim Dergisi*, 11(4), 696-708. <https://doi.org/10.30703/cije.1131545>
- Dalgarno, B. and Lee, M. J. W.** (2010). What are the learning affordances of 3-D virtual environments? *British Journal of Educational Technology*, 41(1), 10-32. <https://doi.org/10.1111/j.1467-8535.2009.01038.x>
- Davenport, T. H. and Ronanki, R.** (2018). Artificial intelligence for the real world. *Harvard Business Review*, 96(1), 108-116.
- Dönmez, O.** (2019). Bilgi güvenliği. H. F. Odabaşı ve Ş. O. Leymun (eds.). *Bilişim etiği ve güvenliği içinde* (ss. 199-220). Nobel Akademik Yayıncılık.
- Drucker, P. F.** (1999). Knowledge-worker productivity: The biggest challenge. *California Management Review*, 41(2), 79-94. <https://doi.org/10.2307/411659>
- Durak, H. Y. ve Seferoğlu, S. S.** (2017). Öğretmenlerin teknoloji kullanım yeterliklerinde etkili olan faktörlerle ilgili bir inceleme. H. F. Odabaşı, B. Akkoyunlu ve A. İşman (Ed.), *Eğitim teknolojileri okumaları 2017 içinde* (ss. 537-556). TOJET.
- Dursun, F. ve Saracaloğlu, A. S.** (2017). Bilişim teknolojileri öğretmen yeterliklerinin değerlendirilmesi. *Turkish Studies*, 12(23), 89120. <https://doi.org/10.7827/TurkishStudies.1218>
- Duterte, J. P.** (2024). Technology-enhanced learning environments: Improving engagement and learning. *International Journal of Research and Innovation in Social Science*, 8(10). <https://doi.org/10.47772/IJRISS.2024.8100111>
- Dülger, M. V.** (2015). Sağlık hukukunda kişisel verilerin korunması ve hasta mahremiyeti. *İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi*, 1(2), 43-80. <http://dx.doi.org/10.2139/ssrn.2564595>
- Dülger, M. V.** (2016). Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu bağlamında kişisel verilerin ceza normlarıyla korunması. *İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi*, 3(2), 101-167. <https://izlik.org/JA57JF79WN>

KAYNAKLAR DİZİNİ (devamı)

- Eken, M.** (2023). *Ters yüz öğrenmeye dayalı öğretim programının öğretmen adaylarının akademik başarısına ve 21. yüzyıl öğrenme becerilerine etkisi* [Yayımlanmamış doktora tezi]. Aydın Adnan Menderes Üniversitesi.
- Ekici, S. ve Yılmaz, B.** (2013). FATİH Projesi üzerine bir değerlendirme. *Türk Kütüphaneciliği*, 27(2), 317-339. <https://izlik.org/JA48LF85GF>
- Ekonomik İşbirliği ve Kalkınma Örgütü (Organisation for Economic Co-operation and Development [OECD])** (2018). *The future of education and skills: Education 2030—The future we want*. OECD Publishing. https://www.oecd.org/content/dam/oecd/en/publications/reports/2018/06/the-future-of-education-and-skills_5424dd26/54ac7020-en.pdf
- Ekonomik İşbirliği ve Kalkınma Örgütü (Organisation for Economic Co-operation and Development [OECD])** (2023). *OECD digital education outlook 2023: Towards an effective digital education ecosystem*. OECD Publishing. <https://doi.org/10.1787/c74f03de-en>
- Ekonomik İşbirliği ve Kalkınma Örgütü (Organisation for Economic Co-operation and Development [OECD])** (2024). *OECD digital economy outlook 2024, volume 1: Embracing the technology frontier*. OECD Publishing. <https://doi.org/10.1787/a1689dc5-en>
- Elrayah, M. and Jamil, S.** (2023). *Impact of digital literacy and online privacy concerns on cybersecurity behaviour: The moderating role of cybersecurity awareness*. *International Journal of Cyber Criminology*, 17(2), 166-187. <https://eurekamag.com/research/097/504/097504848.php>
- Encyclopaedia Britannica** (2026). *Technology*. Encyclopaedia Britannica. <https://www.britannica.com/technology/technology>
- Ergül, G. ve Yıldız, S.** (2021). Sosyal medyada sosyal annelik: Instagram anneliği. *Kırıkkale Üniversitesi Sosyal Bilimler Dergisi*, 11(2), 611-627. <https://izlik.org/JA85LX63HB>
- Erten, P.** (2020). Öğretmen adaylarının 21. yüzyıl becerileri yeterlik algıları ve bu becerilerin kazandırılmasına yönelik görüşleri. *Milli Eğitim Dergisi*, 49(227), 33-64. <https://izlik.org/JA89BM96TW>

KAYNAKLAR DİZİNİ (devamı)

- Ertmer, P. A. and Ottenbreit-Leftwich, A. T. (2010).** *Teacher technology change: How knowledge, confidence, beliefs, and culture intersect. Journal of Research on Technology in Education*, 42(3), 255-284. <https://doi.org/10.1080/15391523.2010.10782551>
- Esteban, A. M., Vergara, C. R. and Tanghal, A. B. (2023).** Technology proficiency and academic stress level of pre-service teachers under the new normal. In *Proceedings of the 3rd International Conference on Education and Technology (ICETECH 2022)* (pp.501-512). https://doi.org/10.2991/978-2-38476-056-5_52
- Fidan, M. ve Cura-Yeleğen, H. (2022).** Öğretmenlerin dijital yeterliklerinin çeşitli değişkenler açısından incelenmesi ve dijital yeterlik gereksinimleri. *Ege Eğitim Dergisi*, 23(2), 150-170. <https://doi.org/10.12984/eggeefd.1075367>
- Fidan, M., Debbağ, M. ve Çukurbaşı, B. (2020).** *Technology proficiency self-assessments of teachers becoming professional in the 21st century: A scale adaptation study. Pegem Eğitim ve Öğretim Dergisi*, 10(2), 465-492. <https://doi.org/10.14527/pegegog.2020.016>
- Field, A. (2018).** *Discovering statistics using IBM SPSS statistics* (5th ed.) Sage.
- Fraenkel, J. R., Wallen, N. E. and Hyun, H. H. (2012).** *How to design and evaluate research in education* (8th ed.). McGraw-Hill.
- Frank, M. and Ament, C. (2021).** How motivation shapes the sharing of information security incident experience. *Proceedings of the 54th Hawaii International Conference on System Sciences*. <https://hdl.handle.net/10125/71166>
- Fussell, R. S. (2005).** Protecting information security availability via self-adapting intelligent agents. *Military Communications Conference*. IEEE. <https://ieeexplore.ieee.org/document/1606116>
- Garcia-Ortega, B., Lopez-Navarro, M. A. and Galan-Cubillo, J. (2021).** Top management support in the implementation of Industry 4.0 and business digitization: The case of companies in the main European stock indices. *IEEE Access*, 9, 139994-140009. <https://doi.org/10.1109/ACCESS.2021.3118988>
- Gartner (2021, October 18).** *Top strategic technology trends for 2022*. Gartner. <https://www.gartner.com/en/information-technology/insights/top-technology-trends>
- Gökkaya-Babacan, N. (2025).** *Lise öğretmenlerinin teknolojik pedagojik alan bilgileri ile dijital veri güvenliği farkındalığı arasındaki ilişki* [Yayımlanmamış yüksek lisans tezi]. Çukurova Üniversitesi.

KAYNAKLAR DİZİNİ (devamı)

- Göldağ, B.** (2021). *Üniversite öğrencilerinin dijital okuryazarlık düzeyleri ile dijital veri güvenliği farkındalık düzeyleri arasındaki ilişkinin incelenmesi*. *e-International Journal of Educational Research*, 12(3), 82-100. <https://doi.org/10.19160/e-ijer.950635>
- Greenhow, C. and Lewin, C.,** (2018). Social media and education: Reconceptualizing the boundaries of formal and informal learning. In N.Selwyn and E. Stirling (Eds.), *social media and education*. Routledge. <https://doi.org/10.4324/9781315121697>
- Griffin, D. A.** (2003). *Educators technology level of use and methods for learning technology integrations* [Unpublished doctoral dissertation]. University of North Texas.
- Gülen, Ş. B.** (2013). *Ortaokul öğrencilerinin 21. yüzyıl öğrenme becerileri ve bilişim teknolojileri ile destekleme düzeylerinin cinsiyet ve sınıf seviyesine göre incelenmesi* [Yayımlanmamış yüksek lisans tezi]. Gazi Üniversitesi.
- Gülpınar-Demirci, V. ve Buluz-Kömeçoğlu, B.** (2022). Sosyal ağlarda veri gizliliği: Türkiye’de WhatsApp gizlilik sözleşmesine gösterilen tepkilerinin duygu analizi. *Kafkas Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 13(26), 710-742. <https://doi.org/10.36543/kauibfd.2022.030>
- Günay, D.** (2017). Teknoloji Nedir? Felsefi Bir Yaklaşım. *Yükseköğretim ve Bilim Dergisi*, 1, 163-166. <https://doi.org/10.5961/jhes.2017.194>
- Güney, İ. ve Mete, P.** (2022). Öğretmenlerin bilişim teknolojileri öz yeterlik algıları ile uzaktan eğitime yönelik tutumları arasındaki ilişki. *Trakya Eğitim Dergisi*, 12(3), 1289-1309. <https://doi.org/10.24315/tred.976005>
- Güngör, M.** (2015). *Ulusal bilgi güvenliği: Strateji ve kurumsal yapılanma*. T.C. Kalkınma Bakanlığı. <https://www.sbb.gov.tr/wp-content/uploads/2022/08/Ulusal-Bilgi-Guvenligi-Strateji-ve-Kurumsal-Yapilanma-Murat-Gungor.pdf>
- Hacıömeroğlu, G., Şahin, Ç. ve Arcagök, S.** (2014). Öğretmen adaylarının teknolojik pedagojik alan bilgisini değerlendirme ölçeği’in Türkçe’ye uyarlama çalışması. *Eğitimde Kuram ve Uygulama*, 10(2), 297-315. <https://doi.org/10.17244/eku.24200>
- Hansen, S. B.** (2020). *Philosophers of technology*. De Gruyter. <https://doi.org/10.1515/9783110622072>
- Henkoğlu, T. ve Külcü, Ö.** (2013). Bilgi erişim platformu olarak bulut bilişim: Riskler ve hukuksal koşullar üzerine bir inceleme. *Bilgi Dünyası*, 14(1), 62-86. <https://doi.org/10.15612/BD.2013.135>

KAYNAKLAR DİZİNİ (devamı)

- Hew, K. F. and Brush, T.** (2007). Integrating technology into K-12 teaching and learning: Current knowledge gaps and recommendations for future research. *Educational Technology Research and Development*, 55(3), 223-252. <https://doi.org/10.1007/s11423-006-9022-5>
- Hızmalı, M.** (2022). *Üniversite öğrencilerinin dijital veri güvenliği farkındalıklarının dijital vatandaşlık bağlamında incelenmesi* [Yayımlanmamış yüksek lisans tezi]. Trakya Üniversitesi.
- Hodges, C., Moore, S., Lockee, B., Trust, T. and Bond, A.,** (2020). The difference between emergency remote teaching and online learning. *EDUCAUSE Review*. <https://er.educause.edu/articles/2020/3/the-difference-between-emergency-remote-teaching-and-online-learning>
- Hughes-Lartey, K., Li, M., Botchey, F. E. and Qin, Z.** (2021). Human factor, a critical weak point in the information security of an organization's Internet of Things. *Heliyon*, 7(3), e06522. <https://doi.org/10.1016/j.heliyon.2021.e06522>
- İbekçi, R.** (2025). *Bilgi ve belge yönetimi bölümü lisans öğrencilerinin dijital okuryazarlık düzeyleri ile dijital veri güvenliği farkındalık düzeyleri arasındaki ilişkinin incelenmesi* [Yayımlanmamış yüksek lisans tezi]. Atatürk Üniversitesi.
- İç Güvenlik Ofisi (Office of Homeland Security)** (2002). *The national strategy for homeland security*. The White House. <https://www.dhs.gov/sites/default/files/publications/nat-strat-hls-2002.pdf>
- Karadeniz, Ş. ve Vatanartıran, S.** (2015). *Sınıf öğretmenlerinin teknolojik pedagojik alan bilgilerinin incelenmesi*. *İlköğretim Online*, 14(3), 1017-1028. <https://doi.org/10.17051/io.2015.12578>
- Katsamakas, E.** (2022). Digital transformation and sustainable business models. *Sustainability*, 14(11), 6414. <https://doi.org/10.3390/su14116414>
- Kaya, Z. ve Yılayaz, Ö.** (2013). Öğretmen eğitimine teknoloji entegrasyonu modelleri ve teknolojik pedagojik alan bilgisi. *Batı Anadolu Eğitim Bilimleri Dergisi*, 4(8), 57-83. <https://izlik.org/JA33BK63AM>
- Keleş, M. K. ve Güneş, A.** (2013, 20-21 Eylül). 24 bit renkli dokümanların farklı biyometri teknoloji kullanılarak güvenliğinin sağlanması. *VI. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı*. Ankara, Türkiye.

KAYNAKLAR DİZİNİ (devamı)

- Kestel, M. ve Akbıyık, C.** (2016). Siber zorbalığın öğrencilerin akademik, sosyal ve duygusal durumları üzerindeki etkisinin incelenmesi. *Mersin Üniversitesi Eğitim Fakültesi Dergisi*, 12(3), 844-859. <https://doi.org/10.17860/mersinefd.282384>
- Kişisel Verilerin Korunması Kanunu (KVKK)** (2016). *Resmî Gazete (Sayı: 29677)*. <https://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf>
- Kişisel Verileri Koruma Kurumu (KVKK)**. (2021). *İlgili kişinin fotoğrafının öğrencisi olduğu okul tarafından kullanılması hakkında Kişisel Verileri Koruma Kurulunun 09/06/2021 tarihli ve 2021/572 sayılı karar özeti*. <https://www.kvkk.gov.tr/Icerik/7118/2021-572>
- Kişisel Verileri Koruma Kurumu (KVKK)** (2024). *2023 yılı faaliyet raporu*. <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/1ee4f609-711f-4a85-aefc-69181bbcdf3a.pdf>
- Kocaman-Karoğlu, A., Bal-Çetinkaya, K. ve Çimşir, E.**, (2020). Toplum 5.0 sürecinde Türkiye’de eğitimde dijital dönüşüm. *Üniversite Araştırmaları Dergisi*, 3(3), 147-158. <https://doi.org/10.32329/uad.815428>
- Koçyiğit, İ. ve Özkul, A. S.** (2023). Bireylerin dijital ayakizi farkındalık ve yönetim düzeylerine yönelik bir araştırma. *Süleyman Demirel Üniversitesi Vizyoner Dergisi*, 14(40) , 1290-1310. <https://doi.org/10.21076/vizyoner.1219704>
- Koehler, M. J. and Mishra, P.** (2005). *What happens when teachers design educational technology? The development of technological pedagogical content knowledge. Journal of Educational Computing Research*, 32(2), 131-152. <https://doi.org/10.2190/0EW7-01WB-BKHL-QDYV>
- Korucu, O.** (2021). *Veri güvenliğinin iyileştirilmesi sürecinde risk tabanlı küresel standart, çerçeve ve en iyi uygulama yaklaşımları* [Yayımlanmamış yüksek lisans tezi]. İstanbul Bilgi Üniversitesi.
- Kotter, J. P.** (2012). *Leading change*. Harvard Business Review Press.
- Kozikoğlu, İ. ve Altunova, N.** (2018). Öğretmen adaylarının 21. yüzyıl becerilerine ilişkin öz-yeterlik algılarının yaşam boyu öğrenme eğilimlerini yordama gücü. *Yükseköğretim ve Bilim Dergisi*, 8(3), 522-531. <https://doi.org/10.5961/jhes.2018.293>
- Kozloski, K. C.** *Principal leadership for technology integration: A study of principal technology leadership* [Unpublished doctoral dissertation]. Drexel University. <https://doi.org/10.17918/etd-886>

KAYNAKLAR DİZİNİ (devamı)

- Leung, S. L. T., Ho, W. and Tam, W. K. C.** (2026). *Professional development in enhancing teachers' cybersecurity awareness: Current status and future directions of media literacy training.* *Education Sciences*, 16(2), 196. <https://doi.org/10.3390/educsci16020196>
- Le-Viet, H. and Dang-Quoc, H.** (2023). The factors affecting digital transformation in Vietnam logistics enterprises. *Electronics*, 12(8), 1825. <https://doi.org/10.3390/electronics12081825>
- Liginlal, D., Sim, I. and Khansa, L.** (2009). How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management. *Computers & Security*, 28(3-4), 215-228. <https://doi.org/10.1016/j.cose.2008.11.003>
- Makridis, C. A.** (2021). Do data breaches damage reputation? Evidence from 45 companies between 2002 and 2018. *Journal of Cybersecurity*, 7(1), tyab021. <https://doi.org/10.1093/cybsec/tyab021>
- Mayer-Schönberger, V. and Cukier, K.** (2013). *Big data: A revolution that will transform how we live, work, and think.* Houghton Mifflin Harcourt
- McAfee, A. and Brynjolfsson, E.** (2017). *Machine, platform, crowd: Harnessing our digital future.* W. W. Norton & Company.
- McMahon, C.** (2020). In defence of the human factor. *Frontiers in Psychology*, 11, 13-90. <https://doi.org/10.3389/fpsyg.2020.01390>
- McMillan, J. H. and Hearn, J.** (2008). *Student self-assessment: The key to stronger student motivation and higher achievement.* *Educational Horizons*, 87(1), 40-49. <https://files.eric.ed.gov/fulltext/EJ815370.pdf>
- Millî Eğitim Bakanlığı (MEB)** (2017). *Okullarda sosyal medyanın kullanılması* (Genelge 2017/12). <https://mevzuat.meb.gov.tr/dosyalar/1833.pdf>
- Millî Eğitim Bakanlığı (MEB)** (2021). *Siber zorbalık rehber öğretmen/psikolojik danışman kitapçığı.* MEB. https://orgm.meb.gov.tr/meb_iys_dosyalar/2025_05/09175900_siberzorbalik_rehberogretmen220322.pdf
- Millî Eğitim Bakanlığı (MEB)** (2023). *Dijital öğretmen yeterlikleri.* MEB. <https://ogedep.eba.gov.tr/wp-content/uploads/2025/08/dijitalyeterlikler.pdf>

KAYNAKLAR DİZİNİ (devamı)

- Millî Eğitim Bakanlığı (MEB)** (2025). *Eğitimde yapay zekâ politika belgesi ve eylem planı (2025-2029)*. MEB.
https://yegitek.meb.gov.tr/meb_iys_dosyalar/2025_06/17092340_egitimdeyapayze_kapolitikabelgesiveylemplani202520291.pdf
- Mishra, P. and Koehler, M. J.** (2006). Technological pedagogical content knowledge: A framework for teacher knowledge. *Teachers College Record*, 108(6), 1017-1054.
<https://doi.org/10.1111/j.1467-9620.2006.00684.x>
- National Archives and Records Administration (NARA)** (2023). *Subpart E-Digitizing permanent federal records (36 C.F.R. Part 1236)*. <https://www.ecfr.gov/current/title-36/chapter-XII/subchapter-B/part-1236/subpart-E>
- Ogle, T. and Branch, M.** (2002). *Technology in schools: Suggestions, tools, and guidelines for assessing technology in elementary and secondary education* (NCES 2003313). U.S. Department of Education, National Center for Education Statistics.
<https://nces.ed.gov/use-work/resource-library/report/forum-guide/technology-schools-suggestions-tools-and-guidelines-assessing-technology-elementary-and-secondary>
- Okur-Türk, M.** (2024). *Öğretmenlerin 21. yüzyıl öğrenmeleri için teknoloji öz yeterlikleri ile yapılandırmacı yaklaşımı uygulamaya yönelik öz yeterlikleri arasındaki ilişki* [Yayımlanmamış yüksek lisans tezi]. Atatürk Üniversitesi.
- Ontario Institute for Studies in Education (t.y.)**. *USB flash drive security*. University of Toronto. <https://www.oise.utoronto.ca/educationcommons/cybersecurity/usb-security>
- Oruç, T., Yeşilyurt, M. ve Kurt, M.** (2024). Eğitimde yapay zekâ konulu çalışmaların betimsel analizi. *Temel Eğitim*, 6(24), 44-60. <https://izlik.org/JA37CX58TW>
- Oruçoğlu, İ. B.** (2023). *Proje-temelli ders ortamında öğretmen adaylarının çevik yaklaşım ve 21. yüzyıl becerileri ile ilgili deneyimlerinin incelenmesi* [Yayımlanmamış doktora tezi]. Marmara Üniversitesi].
- Öğretmen Yetiştirme ve Geliştirme Genel Müdürlüğü (ÖYGGM)** (2013a). *Hizmet içi eğitim etkinlik programı*. http://hedb.meb.gov.tr/net/_Duyuru_dosyalar/fatih/EK-1.pdf
- Öğretmen Yetiştirme ve Geliştirme Genel Müdürlüğü (ÖYGGM)** (2013b). *Geliştirilen ve güncellenen standart kriterlere uygun olarak hazırlanan örnek hizmet içi eğitim programları*. http://hedb.meb.gov.tr/net/_standart_program/

KAYNAKLAR DİZİNİ (devamı)

- Önür, Z.** (2018). *Ortaokul öğrencilerinin 21. yüzyıl öğrenme becerileri ile eğitim teknolojisi yeterlikleri arasındaki ilişki* [Yayımlanmamış yüksek lisans tezi]. Van Yüzüncü Yıl Üniversitesi.
- Özdemir, A. ve Uluyol, Ç.** (2021). Kamu kurum ve kuruluşlarında bilgi güvenliği farkındalığı. *Türkiye Sosyal Araştırmalar Dergisi*, 25(3), 649-666. <https://doi.org/10.20296/tsadergisi.815635>
- Öztürk, G.** (2022). Uzaktan eğitim yazılımlarında/sistemlerinde güvenlik ve gizlilik. Ö. Aydın (Ed.), *Bilgisayar sistemlerinde güvenlik ve gizlilik* içinde (ss. 373-390). Efe Akademik Yayıncılık.
- Öztürk, İ. ve Çakır, R.** (2022). Öğretmenlerin sınıf ortamında dijital oyunlardan yararlanmaları ve dijital veri güvenliği farkındalıkları. *Türkiye Bilimsel Araştırmalar Dergisi*, 7(1), 123-146. <https://izlik.org/JA67AB63EA>
- Öztürk, M.** (2021). Dijital vatandaşlık araştırmalarının incelenmesi: Kavramsal ve yöntemsel eğilimler. *Yükseköğretim ve Bilim Dergisi*, 11(2). <https://doi.org/10.5961/jhes.2021.457>
- Parmaksız, A.** (2023). Türk düşüncesinde teknoloji kavramı ve eğitimle ilişkisi. *YENİSEY Dil ve Edebiyat Dergisi*, 4(2), 126-137. <https://doi.org/10.29228/yenisey.73317>
- Partnership for 21st Century Skills [P21]** (2017). *Framework for 21st century learning*. <http://www.p21.org/our-work/p21-framework>
- Pascoe, C., Quinn, S., and Scarfone, K.** (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST CSWP 29). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.CSWP.29>
- Polat, G.** (2024). *Artırılmış gerçeklik uygulamalarının sosyal bilgiler öğretmen adayları ders başarısına ve 21. yüzyıl becerilerine etkisi* [Yayımlanmamış yüksek lisans tezi]. Sinop Üniversitesi.
- Prensky, M.** (2001). Digital natives, digital immigrants part 1. *On the Horizon*, 9(5), 1-6. <https://doi.org/10.1108/10748120110424816>
- Raju, R., Abd Rahman, N. H. and Ahmad, A.** (2022). Cyber security awareness in using digital platforms among students in a higher learning institution. *Asian Journal of University Education*, 18(3), 756-766. <https://doi.org/10.24191/ajue.v18i3.18967>

KAYNAKLAR DİZİNİ (devamı)

- Ravichandran, R., Singh, S. and Sasikala, P.** (2025). Exploring school teachers' cyber security awareness, experiences, and practices in the digital age. *Journal of Cybersecurity Education, Research and Practice*, 2025(1), Article 1. <https://doi.org/10.62915/2472-2707.1214>
- Redecker, C.** (2017). *European framework for the digital competence of educators: DigCompEdu*, Y. Punie (Ed.). Publications Office of the European Union. <https://doi.org/10.2760/159770>
- Reid, T.** (1786). *Essays on the intellectual powers of man*. John Bell.
- Rogers, D. L.** (2016). *The digital transformation playbook: Rethink your business for the digital age*. Columbia University Press. <https://doi.org/10.7312/roge17544>
- Ropp, M. M.** (1999). Exploring individual characteristics associated with learning to use computers in preservice teacher preparation. *Journal of Research on Computing in Education*, 31(4), 402-424. <https://doi.org/10.1080/08886504.1999.10782262>
- Ross, J. W., Sebastian, I. M., Beath, C. M., Scantlebury, S., Mocker, M., Fonstad, N. O., Kagan, M., Moloney, K. G. and Krusell, D.** (2016). *Designing digital organizations* (MIT CISR Working Paper No. 406). MIT Sloan Center for Information Systems Research. https://cisl.mit.edu/publication/MIT_CISRwp406_DesigningDigitalOrganizations_RossSebastianBeathScantleburyMockerFonstadKaganMoloneyKrusellBCG
- Rowley, J.** (2007). The wisdom hierarchy: Representations of the DIKW hierarchy. *Journal of Information Science*, 33(2), 163-180. <https://doi.org/10.1177/0165551506070706>
- Sætra, H. S. (Ed.).** (2023). *Technology and sustainable development: The promise and pitfalls of techno-solutionism* (1st ed.). Routledge. <https://doi.org/10.1201/9781003325086>
- Sarsıkoğlu, Ş. ve Ergün, K. K.** (2025). Dijital çağda Türk ceza muhakemesi: Siber suçlar özelinde koruma tedbirlerinin genel teorisi. *Hacettepe Üniversitesi Hukuk Fakültesi Dergisi*, 15(2), 576-618. <https://doi.org/10.32957/hacettepehdf.1706831>
- Savunma Teknolojileri Mühendislik Teknolojik Düşünce Merkezi (STM ThinkTech)** (2023a). *Siber tehdit durum raporu: Ocak-Mart 2023*. STM ThinkTech. https://thinktech.stm.com.tr/uploads//docs/2023-yili-pdf-leri/1682506490_stmsibertehditdurumraporuocakmart2023.pdf

KAYNAKLAR DİZİNİ (devamı)

- Savunma Teknolojileri Mühendislik Teknolojik Düşünce Merkezi (STM ThinkTech)** (2023b). *Siber tehdit durum raporu: Ekim-Aralık 2023*. STM ThinkTech. <https://thinktech.stm.com.tr/tr/siber-tehdit-durum-raporu-ekim-aralik-2023>
- Saykal, A. ve Uluçınar-Sağır, Ş.** (2021). *Türkiye’de öğretmen yeterlikleri ve teknolojik pedagojik alan bilgisi araştırmaları*. *Gazi Eğitim Bilimleri Dergisi*, 7(2), 115-137. <https://doi.org/10.30855/GJES.2021.07.02.001>
- Schatzberg, E.** (2018). *Technology: Critical history of a concept*. University of Chicago Press. <https://doi.org/10.7208/chicago/9780226584027.001.0001>
- Schmidt, D. A., Baran, E., Thompson, A. D., Mishra, P., Koehler, M. J. and Shin, T. S.** (2009). Technological pedagogical content knowledge (TPACK): The development and validation of an assessment instrument for preservice teachers. *Journal of Research on Technology in Education*, 42(2), 123-149. <https://files.eric.ed.gov/fulltext/EJ868626.pdf>
- Seferoğlu, S. S.** (2009, 12-13 Kasım). Yeterlikler, standartlar ve bilişim teknolojilerindeki gelişmeler ışığında öğretmenlerin sürekli mesleki eğitimi. *Eğitimde Yansımalar IX: Türkiye’nin Öğretmen Yetiştirme Çıkmazı Ulusal Sempozyumu*. Başkent Üniversitesi, Ankara, Türkiye.
- Serin, H.** (2019). *Sosyal medyada çocuk hakları ihlalleri: Ebeveynler ve öğretmenler farkında mı? Eskişehir Osmangazi Üniversitesi Sosyal Bilimler Dergisi*, 20(Özel Sayı), 1005-1031. <https://doi.org/10.17494/ogusbd.555107>
- Sharma, A. and Nazir, S.** (2021). *Assessing the technology self-efficacy of maritime instructors: An explorative study*. *Education Sciences*, 11(7), 342. <https://doi.org/10.3390/educsci11070342>
- Singh, V.** (2024). *A study of awareness about cyber safety and security practices among pre-service teacher trainees*. *International Journal of Novel Research and Development*, 9(9), a720-a728. <https://www.ijnrd.org/papers/IJNRD2409081.pdf>
- Sönmez, S.** (2005). *İşbirliğine dayalı öğrenme yöntemi, birleştirme tekniği ile bilgisayar okur-yazarlığı öğretiminin akademik başarıya ve kalıcılığa etkisi* [Yayımlanmamış yüksek lisans tezi]. Çukurova Üniversitesi
- Spazak, L.** (2013). *Secondary preservice teachers’ perception of preparedness to integrate technology* [Unpublished doctoral dissertation]. Indiana University of Pennsylvania.

KAYNAKLAR DİZİNİ (devamı)

- Symantec** (2013). *Internet security threat report*.
http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf
- Şad, S. N. ve Nalçacı, Ö. İ.** (2015). Öğretmen adaylarının eğitimde bilgi ve iletişim teknolojilerini kullanmaya ilişkin yeterlilik algıları. *Mersin Üniversitesi Eğitim Fakültesi Dergisi*, 11(1), 177-197. <https://doi.org/10.17860/efd.16986>
- Şahin, Z.** (2025). *İlkokul öğrencilerinin dijital okuryazarlık becerileri ile 21. yüzyıl öğrenme deneyimi algıları arasındaki ilişkinin incelenmesi (Afyonkarahisar örnekleme)* [Yayımlanmamış yüksek lisans tezi]. Afyon Kocatepe Üniversitesi.
- Şahinaslan, E., Kantürk, A., Şahinaslan, Ö. ve Borandağ, E.** (2009, 11-13 Şubat). Kurumlarda bilgi güvenliği farkındalığı, önemi ve oluşturma yöntemleri. *Akademik Bilişim 2009*. Harran Üniversitesi, Şanlıurfa, Türkiye. <https://www.guvenliweb.org.tr/dosya/cCvJ7.pdf>
- Şahinaslan, Ö., Şahinaslan, E., Borandağ, E. ve Şahinaslan, A. M.** (2013, 23-25 Ocak). Güvenli bir toplum için son kullanıcı siber güvenliği. *XV. Akademik Bilişim Konferansı*. Akdeniz Üniversitesi, Antalya, Türkiye. https://www.ab.org.tr/inetd.org.tr/ab13/kitap/sahinaslan_sahinaslan_siber_AB13.pdf
- T.C. Ulaştırma ve Altyapı Bakanlığı** (2020). *Ulusal siber güvenlik stratejisi ve eylem planı (2020-2023)*. <https://www.sp.gov.tr/upload/xSPTemelBelge/files/HwolM+ulusal-siber-guvenlik-stratejisi-ep-2020-2023.pdf>
- Tabachnick, B. G. and Fidell, L. S.** (2013). *Using multivariate statistics* (6th ed.). Pearson.
- Tekerek, M.** (2008). Bilgi güvenliği yönetimi. *KSÜ Doğa Bilimleri Dergisi*, 11(1), 132-137. <https://izlik.org/JA58EM92BU>
- Tilson, D., Lyytinen, K. and Sørensen, C.** (2010). *Digital infrastructures: The missing IS research agenda*. *Information Systems Research*, 21(4), 748-759. <https://doi.org/10.1287/isre.1100.0318>
- Tokat Gaziosmanpaşa Üniversitesi** (2018). *Bilgi güvenliği yönetim sistemi politika belgesi*. Tokat Gaziosmanpaşa Üniversitesi. https://kalite.gop.edu.tr/depo/menuler/birim_11412/kalite_politikasi_441/html_icerik/files/TOG%C3%9C.POL.004%20Bilgi%20G%C3%BCvenli%C4%9Fi%20Y%C3%B6netim%20Sistemi%20Politikas%C4%B1.pdf

KAYNAKLAR DİZİNİ (devamı)

- Turing, A. M.** (1937). On computable numbers, with an application to the Entscheidungsproblem. *Proceedings of the London Mathematical Society* (Volume s2-42) (pp. 230-265). <https://doi.org/10.1112/plms/s2-42.1.230>
- Türkiye İstatistik Kurumu (TÜİK)** (2025). *Hanehalkı bilişim teknolojileri (BT) kullanım araştırması*, 2025 (Haber Bülteni No. 53925). <https://veriportali.tuik.gov.tr/tr/press/53925>
- Ulaşanoğlu, M. E., Yılmaz, R. ve Tekin, M. A.** (2010). *Bilgi güvenliği: Riskler ve öneriler*. Bilgi Teknolojileri ve İletişim Kurumu.
- Ulusal Eğitim İstatistikleri Merkezi (National Center for Education Statistics [NCES])** (2005). *Forum unified education technology suite: Part 8: Integrating your technology*. U.S. Department of Education. https://nces.ed.gov/pubs2005/tech_suite/part_8.asp
- Ulusal Siber Olaylara Müdahale Merkezi [USOM]** (t.y.). *Ulusal siber olaylara müdahale merkezi*. <https://www.usom.gov.tr/adres>
- Ulusal Standartlar ve Teknoloji Enstitüsü (National Institute of Standards and Technology [NIST])** (2025). *Reducing the cybersecurity risks of portable storage media in OT environments* (NIST SP 1334). <https://doi.org/10.6028/NIST.SP.1334>
- Uluslararası Eğitimde Teknoloji Topluluğu (International Society for Technology in Education [ISTE])** (2017). *ISTE standards for educators*. <https://www.iste.org/standards/for-educators>
- Uluslararası Eğitimde Teknoloji Topluluğu (International Society for Technology in Education [ISTE])** (2016). *ISTE standards for students*. <https://www.iste.org/standards>
- Uluslararası Telekomünikasyon Birliği (International Telecommunications Union)** (2008). *Regional cyber security forum meeting report*. <http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/sofia-cybersecurity-forumreport-oct-08.pdf>
- UNESCO Institute for Statistics** (2018). *A global framework of reference on digital literacy skills for indicator 4.4.2*. UNESCO Institute for Statistics. <https://unesdoc.unesco.org/ark:/48223/pf0000265403.locale=en>.
- Usluel, Y. K., Mumcu, F. K. ve Demiraslan, Y.** (2007). Öğrenme-öğretme sürecinde bilgi ve iletişim teknolojileri: Öğretmenlerin entegrasyon süreci ve engelleriyle ilgili görüşleri. *Hacettepe Üniversitesi Eğitim Fakültesi Dergisi*, 32, 164-178. <https://izlik.org/JA23AP39XG>

KAYNAKLAR DİZİNİ (devamı)

- Uzun, Y.** (2022). *Bağlantılı öğrenme ile STEM yaklaşımının ilkökul 3. sınıf öğrencilerinin 21. yüzyıl öğrenme ve yenilenme becerilerine, dijital medya okuryazarlıklarına ve sosyal girişimcilik niyetlerine etkisinin incelenmesi* [Yayımlanmamış yüksek lisans tezi]. Karamanoğlu Mehmetbey Üniversitesi.
- Ülçay, O.** (2024). Türkiye Yüzyılı Maarif Modeli değerlendirmesi. *Ulusal Eğitim Toplum ve Dünya Dergisi*, 1(2), 70-75. <https://doi.org/10.5281/zenodo.11097248>
- Valverde-Berrocso, J., Acevedo-Borrega, J. and Cerezo-Pizarro, M.** (2022). Educational technology and student performance: A systematic review. *Frontiers in Education*, 7, Article 916502. <https://doi.org/10.3389/feduc.2022.916502>
- Verhoef, P. C., Broekhuizen, T., Bart, Y., Bhattacharya, A., Dong, J. Q., Fabian, N. and Haenlein, M.** (2021). Digital transformation: A multidisciplinary reflection and research agenda. *Journal of Business Research*, 122, 889-901. <https://doi.org/10.1016/j.jbusres.2019.09.022>
- Vial, G.** (2019). Understanding digital transformation: A review and a research agenda. *The Journal of Strategic Information Systems*, 28(2), 118-144. <https://doi.org/10.1016/j.jsis.2019.01.003>
- Von-Neumann, J.** (1945/1993). First draft of a report on the EDVAC. *IEEE Annals of the History of Computing*, 15(4), 27-75. <https://doi.org/10.1109/85.238389>
- Westerman, G., Bonnet, D. and McAfee, A.** (2014). *Leading digital: Turning technology into business transformation*. Harvard Business Review Press.
- Whitman, M. E. and Mattord, H. J.** (2011). *Principles of information security* (4th ed.). Cengage Learning.
- Woods, K. D.** (2020). *Teacher technology efficacy: The relationship among generation, gender, and subject area of secondary teachers* [Unpublished doctoral dissertation]. Liberty University.
- Woods, K., Wendt, J. L., Barrios, A. and Lunde, R.** (2021). An examination of the relationship between generation, gender, subject area, and technology efficacy among secondary teachers in the United States. *International Journal of Technology in Education*, 4(4), 589-604. <https://doi.org/10.46328/ijte.126>
- Woolfolk-Hoy, A.** (2003). Self-efficacy in college teaching. *Essays on Teaching Excellence: Toward the Best in the Academy*, 15(7), 2003-2004. https://cft.vanderbilt.edu/wp-content/uploads/sites/59/vol15no7_self_efficacy.htm

KAYNAKLAR DİZİNİ (devamı)

- Yavanoğlu, U., Sağiroğlu, Ş. ve Çolak, İ.** (2012). Sosyal ağlarda bilgi güvenliği tehditleri ve alınması gereken önlemler. *Politeknik Dergisi*, 15(1), 15-27. <https://izlik.org/JA88WT43BD>
- Yıldırım, P. ve Keçeci, G.**, (2025). *Eğitimde dijital metamorfoz: Yapay zekâ, nesnelerin interneti, artırılmış gerçeklik ve sanal gerçeklik ile yeni öğrenme dünyası*. İksad Yayınevi.
- Yıldırım, Y.** (2021). *Açık ve uzaktan öğrenenlerin 21. yüzyıl öğrenme becerileri düzeyleri ile açık ve uzaktan eğitim ortamlarındaki bağlılık düzeyleri arasındaki ilişkinin incelenmesi* [Yayımlanmamış yüksek lisans tezi]. Anadolu Üniversitesi.
- Yıldız, A.** (2018). Endüstri 4.0 ve akıllı fabrikalar. *Sakarya Üniversitesi Fen Bilimleri Enstitüsü Dergisi*, 22(2), 546-556. <https://doi.org/10.16984/saufenbilder.321957>
- Yılmaz, E.** (2015). *Öğretmenlerin dijital veri güvenliği farkındalığı* [Yayımlanmamış doktora tezi], Anadolu Üniversitesi.
- Yılmaz, E., Şahin, Y. L. ve Akbulut, Y.** (2016). Öğretmenlerin dijital veri güvenliği farkındalığı. *Sakarya University Journal of Education*, 6(2), 26-45. <https://doi.org/10.19126/suje.29650>
- Yoo, Y., Henfridsson, O. and Lyytinen, K.** (2010). The new organizing logic of digital innovation: An agenda for information systems research. *Information Systems Research*, 21(4), 724-735. <https://doi.org/10.1287/isre.1100.0322>
- Yu, H. H. and Lwin, K. K.** (2024). *The relationship between teacher educators' technological knowledge and their self-efficacy in education degree colleges*. Myanmar Academy of Arts and Science. <https://www.maas.edu.mm/Research/Admin/pdf/21.%20Daw%20Htay%20Hnin%20Yu%20%28291-302%29.pdf>
- Yuan, L. and Powell, S.**, (2013). *MOOCs and open education: Implications for higher education*. JISC CETIS. <http://publications.cetis.org.uk/2013/667>

EKLER

EKLER

EK A: Kişisel bilgi formu.

Bu bölümde; cinsiyetiniz, eğitim düzeyiniz, öğretmenlik mesleğinde çalışma süreniz vb. ile ilgili sorular yer almaktadır.

1. Cinsiyetiniz nedir?
2. Görev yaptığınız okul türü nedir?
3. Eğitim düzeyiniz nedir?
4. Öğretmenlik mesleğinde kaç yıldır çalışıyorsunuz?
5. Kendinize ait bir bilgisayarınız var mı?
6. Dijital güvenlikle ilgili bir derse veya kursa katıldınız mı?
7. 21. yüzyıl becerileri kavramını duydunuz mu?

EK B: 21. yüzyıl öğrenmeleri için teknoloji yeterliği öz-değerlendirme ölçeği

1-Hiç Katılmıyorum, 2-Katılmıyorum, 3-Kısmen Katılıyorum, 4-Katılıyorum, 5-Tamamen Katılıyorum

	1	2	3	4	5
1. Bir arkadaşına e-posta gönderebilirim.	1	2	3	4	5
2. Bir tartışma forumuna (facebook grubu gibi) abone olabilirim.	1	2	3	4	5
3. Bir alıcı listesi oluşturarak, aynı anda birçok kişiye e-posta gönderebilirim.	1	2	3	4	5
4. E-posta mesajına bir doküman ekleyip gönderebilirim.	1	2	3	4	5
5. Başkalarına gönderdiğim mesajların kopyasını saklayabilirim.	1	2	3	4	5
6. Bir arama motoru (Google, Yandex vs.) kullanarak ilgilendiğim konulara ilişkin web sayfalarını bulabilirim.	1	2	3	4	5
7. Üniversitemin veya Milli Eğitim Bakanlığı'nın internet sitelerini arayıp bulabilirim.	1	2	3	4	5
8. Daha sonra tekrar dönebilmek için önceden ziyaret ettiğim internet sitesini saklayabilirim (Örneğin, sık kullanılanlara ekleyerek).	1	2	3	4	5
9. Öğretim sürecinde kullanabileceğim birincil bilgi kaynaklarını internetten bulabilirim.	1	2	3	4	5
10. Hesap tablosunu (Excel gibi) kullanarak bir paket içerisinde yer alan renkli şekerlerin oranını gösteren bir grafik (çubuk, daire gibi) oluşturabilirim.	1	2	3	4	5
11. Grafiklerle gazete oluştururum	1	2	3	4	5
12. Başkalarının dokümanları farklı kelime işlemci programlarında okuyabilecekleri formatta (word, pdf, rtf, txt kaydetmek gibi) kaydedebilirim.	1	2	3	4	5
13. Bir konu ile ilgili önemli yazarların bilgileri ile ilgili bir veri tabanı oluşturabilirim.	1	2	3	4	5
14. Söz konusu yazılımı konu ile bir bütün oluşturacak şekilde birleştiren bir ders ya da ünite hazırlayabilirim.	1	2	3	4	5
15. Sınıfta olmayan öğretmenler ve öğrenciler ile iş birliği yapmak için teknolojiyi kullanırım.	1	2	3	4	5
16. Sınıfım için satın alınacak olan teknolojiler için bütçe içeren bir plan yazabilirim.	1	2	3	4	5
17. Kendi öğretim programıma/ders planıma mobil teknolojileri entegre edebilirim.	1	2	3	4	5
18. Öğrencilerimin iş birliği yapması için bir blog ya da wiki oluşturabilirim.	1	2	3	4	5
19. Öğrencilerimle uzaktan öğretim yapmak için çevrimiçi araçları kullanabilirim.	1	2	3	4	5
20. Öğrencilerin kendi cihazlarına sahip oldukları ortamlarda bire bir öğretim yapabilirim.	1	2	3	4	5
21. Sınıfta öğrenci yanıtları için akıllı telefon ya da tablet bilgisayar kullanmalarının bir yolunu bulabilirim.	1	2	3	4	5
22. Öğrencilerimin öğrenme aktivitelerine erişimi için mobil cihazları kullanabilirim.	1	2	3	4	5
23. Film/video klip indirebilir ve izleyebilirim.	1	2	3	4	5
24. Bulut tabanlı bir ortamda (Google Drive, Dropbox gibi) dosyaları kaydedebilir ve geri alabilirim.	1	2	3	4	5

EK C: Dijital veri güvenliği farkındalığı ölçeği

1-Hiç Katılmıyorum, 2-Katılmıyorum, 3-Kararsızım, 4-Katılıyorum, 5-Tamamen Katılıyorum

	1	2	3	4	5
1. Zararlı yazılımlar (virüs, solucan, truva atı vb.) konusunda bilgi sahibiyim.					
2. Parola oluştururken harf, sayı ve özel karakter kullanmanın önemini bilirim.					
3. Farklı işlemler için farklı parola kullanmanın önemini bilirim.					
4. İzinsiz kullanılmaması için dosyalara parola konulabileceğinin farkındayım.					
5. Güvenlik duvarı yazılımları konusunda bilgi sahibiyim.					
6. Flash bellekleri, veri saklamak yerine sadece veri taşımak için kullanmanın farkını bilirim.					
7. İşletim sisteminin (Windows, Android vb.) güncel olmasına dikkat ederim.					
8. E-posta ile gelen kimlik bilgilerini doğrulama mesajlarına (parola, kredi kartı vb.) itibar edilmemesi gerektiğini bilirim.					
9. Taşınabilir depolama birimlerini (Flash bellek, taşınabilir sabit disk) kullanmadan önce virüs taraması yapılması gerektiğini bilirim.					
10. Güvenli olmadığını düşündüğüm e-postaları açmadan silmeye dikkat ederim.					
11. Programların, üreticinin kendi sitesinden indirilmesinin önemini bilirim.					
12. Antivirüs yazılımı kullanmanın önemini bilirim.					
13. Parola hatırlatmak için kullanılan güvenlik sorularına başkalarının tahmin edemeyeceği cevaplar verilmesi gerektiğini bilirim.					
14. Parola oluştururken karakter sayısının fazla olmasının önemini bilirim.					
15. Parolaların herhangi bir ortamda saklanması güvenlik riski oluşturacağının farkındayım.					
16. Verilerin, çeşitli uygulamalar (dropbox, google drive vb.) kullanılarak internet ortamında saklanabileceğini bilirim.					
17. Üzerinde çalışma yapılan dosyaların birden fazla ortamda yedeklenmesi gerektiğini bilirim.					
18. Başkalarının tahmin edemeyeceği parolalar oluşturmaya dikkat ederim.					
19. İnternet adres çubuğunda yanlış yönlendirme olup olmadığına dikkat ederim.					
20. Taşınabilir depolama birimlerini (Flash bellek, taşınabilir sabit disk) "Donanımı Güvenle Kaldır" seçeneğini kullanarak çıkartmaya dikkat ederim.					
21. Karmaşık yapıdaki parolaların kurulabileceğini bilirim.					
22. Parolaların belirli aralıklarla değiştirilmesi gerektiğinin farkındayım.					
23. Almak istemediğim çöp e-postaları "spam/gereksiz/önemsiz" olarak işaretlemeye dikkat ederim.					
24. İzinsiz kullanılmaması için cihazlara (akıllı telefon, tablet, bilgisayar vb.) parola konulabileceğinin farkındayım.					
25. Kendime ait olmayan cihazlarda, parola gerektiren işlemler yapmamaya dikkat ederim.					
26. İşletim sisteminin (Windows, Android vb.) güvenlikle ilgili uyarılarını dikkate alırım.					
27. Elektrik kesintisine karşı dizüstü bilgisayarları bataryası ile kullanmanın önemini bilirim.					
28. Cep telefonuna gelen tek kullanımlık parola ile yapılan giriş işlemlerinin, güvenliği artırdığını bilirim.					
29. Sanal klavye kullanmanın önemini bilirim.					
30. İnternet sitelerinde kullanıcı oturumunu kapatırken "güvenli çıkış" bağlantısını kullanmanın önemini bilirim.					
31. İnternet sitelerinde kullanılan güvenlik sertifikaları hakkında bilgi sahibiyim.					
32. Lisanslı olmayan yazılımların güvenlik açıkları oluşturabileceğinin farkındayım.					

EK D: Etik kurul onay belgeleri.

Evrak Tarih ve Sayısı: 17.01.2025-E.472837



T.C.
BALIKESİR UNIVERSİTESİ REKTÖRLÜĞÜ
Fen Bilimleri Enstitüsü Müdürlüğü

Sayı : E-16031472-108.01-472837
Konu : Etik Kurul Onayı (Özmer UZUNOĞLU)

17.01.2025

DAĞITIM YERLERİNE

İlgi : 16.01.2025 tarihli ve 19928322/108.01/472511 sayılı yazı.

Öğretim Üyesi Doç. Dr. Gülcan ÖZTÜRK'ün danışmanlığını yürüttüğü Anabilim Dalımız Yüksek Lisans Programı Öğrencisi Özmer UZUNOĞLU'nun "Öğretmenlerin 21. yüzyıl öğrenmelerinde teknoloji yeterliği öz-değerlendirmeleri ve dijital veri güvenliği farkındalıkları" isimli tez çalışmasının değerlendirilmesi ve bilimsel hakemli dergilerde yayınlanabilmesi için Fen ve Mühendislik Bilimleri Etik Komisyonu'nun 13.01.2025 tarih ve 2025/01 sayılı toplantısında alınan karar gereği düzenlenen onay belgesi ilişikte sunulmuştur.

Bilgilerini ve gereğini rica ederim.

Doç. Dr. Taner OZCAN
Müdür Yardımcısı

Ek:Yazı ve Eki (2 Sayfa)

Dağıtım:

Gereği:

Bilgisayar ve Öğretim Teknolojileri Eğitimi
Anabilim Dalı Başkanı

Bilgi:

Doç. Dr. Gülcan ÖZTÜRK

Bu belge, güvenli elektronik imza ile imzalanmıştır.

Belge Doğrulama Kodu :DSC69K3611, Pin Kodu :80942

Belge Takip Adresi : <https://www.tatbiya.gov.tr/balikesir-universitesi-etik-oby>

Adres:Fen Bilimleri Enstitüsü Çalışma Yerleşkesi 10145 Balıkesir

Tel:0266/121077 Faks:0266/121078

e-Posta:baufb@balikesir.edu.tr Web: <http://fbs.balikesir.edu.tr/>

Kapı Adresi:balikesirunivertesi@bal01.kap.tr

Bilgi için: Cihad Deyoğlu

Unvanı: Bilgisayar İşletmeni

Tel No: 0-266-6121400-101414





T.C.
BALIKESİR ÜNİVERSİTESİ REKTÖRLÜĞÜ
Rektörlük

Sayı :E-19928322-108.01-472511
Konu : Etik Kurul Onayı (Öznur UZUNOĞLU)

16.01.2025

FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRLÜĞÜNE

İlgi : 20.12.2024 tarihli ve 16031472/108.01/459924 sayılı yazı.

Fen Bilimleri Enstitüsü, Öğretim Üyesi Doç. Dr. Gülcan ÖZTÜRK'ün danışmanlığını yürütmüş olduğu; 202312643006 numaralı Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı Yüksek Lisans programı öğrencisi Öznur UZUNOĞLU'nun "Öğretmenlerin 21. yüzyıl öğrenmelerinde teknoloji yeterliği özdeğerlendirmeleri ve dijital veri güvenliği farkındalıkları" başlıklı tez çalışmasının araştırmaları için etik kurul onayı isteği ile ilgili Fen ve Mühendislik Bilimleri Etik Komisyonu'nun 13.01.2025 tarih ve 2025/1 sayılı toplantısında alınan karar gereği düzenlenen onay belgesi ekte gönderilmiştir.

Bilgilerinizi rica ederim.

Prof. Dr. Fatih SATIL
Rektör Yardımcısı

Bu belge, güvenli elektronik imza ile imzalanmıştır.

Belge Doğrulama Kodu :BİLİ0925166Y Pın Kodu :03472
Adres:Balıkesir Üniversitesi Rektörlüğü Çarşı Yarıyolu 10145 Balıkesir
Telefon:2666121400 Faks:2666121412
Web:http://www.balikesir.edu.tr
E-posta:balikesir@univnet.tr

Belge Takiy Adresi : <https://www.takiya.gov.tr/balikesir-universitesi-alyi>

Bilgi İçin: Seda Çelbay
Ünvanı: Bilgisayar İşletmeni
Tel No: 2666121418



T.C.
BALIKESİR ÜNİVERSİTESİ
FEN VE MÜHENDİSLİK BİLİMLERİ ETİK KOMİSYONU
ONAY BELGESİ

Balıkesir Üniversitesi Fen Bilimleri Enstitüsü, Öğretim Üyesi Doç. Dr. Gülcan ÖZTÜRK'ün danışmanlığını yürütmüş olduğu; 202312643006 numaralı Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı Yüksek Lisans programı öğrencisi Öznur UZUNOĞLU'nun "Öğretmenlerin 21. yüzyıl öğrenmelerinde teknoloji yeterliği özdeğerlendirmeleri ve dijital veri güvenliği farkındalıkları" başlıklı tez çalışmasının araştırmaları için etik kurul onay belgesi isteği komisyonumuzca değerlendirilmiş ve etik açıdan uygun bulunmuştur.13.01.2025

Komisyon Başkanı }
Prof. Dr. Zafer ASLAN

Prof. Dr. Baki ÇİÇEK
Üye

Prof. Dr. Ruhan BÉNLİKAYA
Üye

Prof. Dr. Nursen AZİZÖĞLÜ
Üye

EK E: Millî eğitim bakanlığı araştırma uygulama izni belgesi.



**T.C.
MİLLÎ EĞİTİM BAKANLIĞI
ARAŞTIRMA UYGULAMA İZİNİ BELGESİ**



Başvuru No: MEB.TT.2025.020250.01

T.C. Kimlik No:

Adı Soyadı: ÖZNUR UZUNOĞLU

Araştırmanın Adı: Öğretmenlerin 21. Yüzyıl Öğrenmelerinde Teknoloji Yeterliği Öz-Değerlendirmeleri Ve Dijital Veri Güvenliği Farkındalıkları

Araştırmanın Niteliği: Yüksek Lisans Tezi

Araştırmanın Örneklem / Çalışma Grubu: Öğretmen

Veri Toplama Aracının Başlığı: 21.Yüzyıl Öğrenimleri İçin TYÖD Ölçeği ve DVGF Ölçeği

Araştırma Uygulama İzninin Kabul Tarihi: 09.04.2025

Araştırma Uygulama İzninin Bitiş Tarihi: 09.04.2026

Yukarıda kimliği yazılı araştırmacı “Araştırma Uygulama İzinleri Yönergesine” göre belirtilen kapsamda araştırmasını yapmayı taahhüt etmiştir. Araştırmacının bilgi ve belgelerinin uygunluğu kontrol edilmiş olup aşağıda ifade edilen bilgiler kapsamında araştırma uygulama izni Millî Eğitim Bakanlığı ilgili birimleri tarafından onaylanmıştır.

ÖZGEÇMİŞ

Kişisel Bilgiler

Adı Soyadı : Öznur UZUNOĞLU

Doğum tarihi ve yeri :

e-posta :

Öğrenim Bilgileri

Derece	Okul/Program	Yıl
Lisans	Balıkesir Üniversitesi/Mühendislik Fakültesi/Bilgisayar Mühendisliği	2023
Ön lisans	Ataürk Üniversitesi/Açık Öğretim Fakültesi/Acil Durum ve Afet Yönetimi	2018
Lisans	Selçuk Üniversitesi/Teknik Eğitim Fakültesi/Bilgisayar Sistemleri Öğretmenliği	2007
Ön lisans	Ege Üniversitesi/Bilgisayar Programcılığı	2003
Lise	Balıkesir Anadolu Ticaret Meslek Lisesi/Bilgi İşlem	2001