



**SOSYAL BİLGİLER DERSİNDE DİJİTAL GÜVENLİK YETERLİĞİ
İÇİN GELİŞTİRİLEN ÇEVİRİM İÇİ DESTEKLEYİCİ ÖĞRENME
ARACININ ÖĞRENCİLERİN ÖZ YETERLİK ALGILARINA ETKİSİ**

FATMA AKCAN

DOKTORA TEZİ

TÜRKÇE VE SOSYAL BİLİMLER EĞİTİMİ ANABİLİM DALI

**GAZİ ÜNİVERSİTESİ
EĞİTİM BİLİMLERİ ENSTİTÜSÜ**

OCAK, 2023

TELİF HAKKI VE TEZ FOTOKOPİ İZİN FORMU

Bu tezin tüm hakları saklıdır. Kaynak göstermek koşuluyla tezin teslim tarihinden itibaren 12 (1 yıl) ay sonra tezden fotokopi çekilebilir.

YAZARIN

Adı: Fatma

Soyadı: Akcan

Bölümü: Sosyal Bilgiler Eğitimi Bölümü

İmza:

Teslim tarihi:

TEZİN

Türkçe Adı: Sosyal Bilgiler Dersinde Dijital Güvenlik Yeterliği İçin Geliştirilen Çevrim İçi Destekleyici Öğrenme Aracının Öğrencilerin Öz Yeterlik Algılarına Etkisi

İngilizce Adı: The Effect of the Online Supportive Learning Tool Developed for Digital Security Proficiency in Social Studies Course on Students' Self-Efficacy Perceptions

ETİK İLKELERE UYGUNLUK BEYANI

Tez yazım sürecinde bilimsel ve etik ilkelere uyduğumu, yararlandığım tüm kaynakları kaynak gösterme ilkelerine uygun olarak kaynakçada belirttiğimi ve bu bölümler dışındaki tüm ifadelerin şahsıma ait olduğunu beyan ederim.

Yazar Adı Soyadı: Fatma Akcan

İmza:

JÜRİ ONAY SAYFASI

Fatma Akcan tarafından hazırlanan “Sosyal Bilgiler Dersinde Dijital Güvenlik Yeterliği için Geliştirilen Çevrim İçi Destekleyici Öğrenme Aracının Öğrencilerin Öz Yeterlik Algılarına Etkisi” adlı tez çalışması aşağıdaki jüri tarafından oy birliği ile Gazi Üniversitesi Türkçe ve Sosyal Bilimler Eğitimi Anabilim Dalı’nda Doktora Tezi olarak kabul edilmiştir.

Danışman: Prof. Dr. Mehmet Ali ÇAKMAK
Sosyal Bilgiler Eğitimi, Gazi Üniversitesi

Başkan: Prof. Dr. Cemil Cahit YEŞİLBURSA
Sosyal Bilgiler Eğitimi, Gazi Üniversitesi

Üye: Doç. Dr. Mutlu Tahsin ÜSTÜNDAĞ
Bilgisayar ve Öğretim Teknolojileri Eğitimi, Gazi Üniversitesi

Üye: Doç. Dr. Hasan IŞIK
Tarih, Yıldırım Bayezid Üniversitesi

Üye: Dr. Öğretim Üyesi Sami PEKTAŞ
Eğitim Bilimleri Bölümü, Niğde Ömer Halisdemir Üniversitesi

Tez Savunma Tarihi: 11.01.2023

Bu tezin Türkçe ve Sosyal Bilimler Eğitimi Anabilim Dalı’nda “Doktora Tezi” olması için şartları yerine getirdiğini onaylıyorum.

Prof. Dr. Şaban ÇETİN

Eğitim Bilimleri Enstitüsü Müdürü

TEŞEKKÜR

Bu araştırmanın yürütülmesinde her konuda destekçi olan ve yardımlarını esirgemeyen saygıdeğer danışmanım Prof. Dr. Mehmet Ali Çakmak’a teşekkürü bir borç bilirim. Ayrıca tezimin her sürecine destek ve takipçi olan değerli hocam Doç. Dr. Mutlu Tahsin Üstündağ’a, görüşleriyle ve yardımlarıyla çalışmama destek olan değerli hocalarım Prof. Dr. Cemil Cahit Yeşilbursa, Doç. Dr. Hasan Işık, Dr. Öğr. Üyesi Sami Pektaş, Gazi Üniversitesi Uzaktan Eğitim Araştırma ve Uygulama Merkezi (GUZEM) akademisyenlerine ve Betül Çoban’a şükranlarımı sunarım.

SOSYAL BİLGİLER DERSİNDE DİJİTAL GÜVENLİK YETERLİĞİ İÇİN GELİŞTİRİLEN ÇEVİRİM İÇİ DESTEKLEYİCİ ÖĞRENME ARACININ ÖĞRENCİLERİN ÖZ YETERLİK ALGILARINA ETKİSİ

(Doktora Tezi)

Fatma Akcan

GAZİ ÜNİVERSİTESİ

EĞİTİM BİLİMLERİ ENSTİTÜSÜ

Ocak 2023

ÖZ

Bu araştırmanın amacı, sosyal bilgiler dersinde dijital güvenlik yeterliği için geliştirilen çevrim içi destekleyici öğrenme aracının öğrencilerin öz yeterlik algılarına etkisini belirlemektir. Araştırmada deneysel desen modellerinden öntest sontest eşleştirilmiş kontrol gruplu yarı deneysel desen kullanılmıştır. Araştırmanın deneysel kısmı 2021-2022 eğitim öğretim yılının bahar döneminde yürütülmüştür. Araştırmanın çalışma grubunu devlet ortaokulundaki 7. sınıf öğrencileri oluşturmuştur. Deney grubunda 35, kontrol grubunda 32 öğrenci olmak üzere toplamda 67 öğrenci çalışma grubunda yer almıştır. Araştırmada veri toplama aracı olarak “Dijital Güvenlik Öz Yeterlik Envanteri” kullanılmıştır. Dijital güvenlik öz yeterlik envanteri, teknik alt ölçeği, psikososyal alt ölçeği, çevrim içi alışveriş alt ölçeği, hak ve sorumluluk alt ölçeği ve sağlık alt ölçeği olmak üzere 5 alt ölçekten oluşmaktadır. Araştırmadan elde edilen verilerin analizinde SPSS-24.0 ve AMOS-21 paket programı kullanılmıştır. Verilerin çözümlenmesinde ise “Mann-Whitney U Testi” ve “Wilcoxon İşaretli Sıralar Testi” kullanılmıştır. Araştırma bulgularından elde edilen sonuçlara göre sosyal bilgiler dersinde dijital güvenlik yeterliği için geliştirilen çevrim içi

destekleyici öğrenme aracının öğrencilerin dijital güvenlik öz yeterlik algısını olumlu yönde etkilediği tespit edilmiştir. Deney ve kontrol grupları son testler açısından karşılaştırıldığında dijital güvenlik öz yeterlik algısında teknik alt ölçeğinde, psikososyal alt ölçeğinde, çevrim içi alışveriş alt ölçeğinde ve sağlık alt ölçeğinde deney grubunun lehine anlamlı bir farklılık olduğu tespit edilmiştir. Hak ve sorumluluk alt ölçeğinde ise deney grubu lehine puanlar yüksek olsa da anlamlı farklılık olmadığı tespit edilmiştir. Araştırma kapsamında ise çevrim içi ortamda, çevrim içi destekleyici öğrenme araçları ile yapılacak olan deneysel araştırmalar öncesinde oryantasyon sürecinin iyi planlanması amacıyla öğrencilerin bilgisayar kullanma becerilerinin tespit edilmesi önerilmektedir. Bununla birlikte uygulama yapılacak olan grup için dijital eşitsizlik konusuna önem verilmesi ve bu probleme ilişkin çözüm üretilmesi önerilmektedir.



Anahtar Kelimeler: Dijital güvenlik, öz yeterlik, çevrim içi öğrenme, sosyal bilgiler

Sayfa adedi : xvi+221

Danışman : Prof. Dr. Mehmet Ali ÇAKMAK

**THE EFFECT OF THE ONLINE SUPPORTIVE LEARNING TOOL
DEVELOPED FOR DIGITAL SECURITY PROFICIENCY IN SOCIAL
STUDIES COURSE ON STUDENTS' SELF-EFFICACY
PERCEPTIONS**

(Ph.D. Thesis)

Fatma Akcan

GAZI UNIVERSITY

GRADUATE SCHOOL OF EDUCATION SCIENCES

January 2023

ABSTRACT

The aim of this research is to determine the effect of the online supportive learning tool developed for digital security proficiency in social studies course on students' self-efficacy perceptions. In the research, one of the experimental pattern models, pretest posttest paired control group semi-experimental pattern was used. The experimental part of the research was conducted in the spring semester of the 2021-2022 academic year. The study group of the research was conducted at the 7th state secondary school. the class is composed of students. A total of 67 students, including 35 students in the experimental group and 32 students in the control group, took part in the study group. The “Digital Security Self-Efficacy Inventory” was used as a data collection tool in the research. The digital security self-efficacy inventory consists of 5 sub-scales: technical sub-scale, psychosocial sub-scale, online shopping sub-scale, rights and responsibilities sub-scale and health sub-scale. SPSS-24.0 and AMOS-21 package program were used in the analysis of the data obtained from the research. In the analysis of the data, the “Mann-Whitney U Test” and the “Wilcoxon

Signed Ranks Test” were used. Research findings according to the results, the adequacy of a supportive learning tool developed for students in social studies online digital security digital security, self-sufficiency, it has been determined that has a positive impact on perception. The experimental and control groups-test compared in terms of digital security, self-sufficiency in the perception of technical sub-scale on the psychosocial sub-scale, online shopping and health on a lower scale sub-scale in favor of the experimental group it has been found that there is a significant difference. On the rights and responsibilities sub-scale, although the scores were high in favor of the experimental group, it was found that there was no significant difference. Within the scope of the research, it is proposed to determine the computer usage skills of the students in order to plan the orientation process well before the experimental researches to be carried out with the online supportive learning tools in the online environment. In addition, it is suggested to give importance to the issue of digital inequality for the group to be implemented and to produce a solution to this problem.



Keywords : Digital security, self-efficacy, online learning, social studies

Page number : xvi+221

Supervisor : Prof. Dr. Mehmet Ali AKMAK

İÇİNDEKİLER

TELİF HAKKI VE TEZ FOTOKOPİ İZİN FORMU	i
ETİK İLKELERE UYGUNLUK BEYANI.....	ii
JÜRİ ONAY SAYFASI.....	iii
TEŞEKKÜR.....	iv
ÖZ.....	v
ABSTRACT	vii
İÇİNDEKİLER.....	ix
TABLolar LİSTESİ.....	xiii
ŞEKİLLER LİSTESİ	xiv
SİMGE VE KISALTMALAR LİSTESİ.....	xv
BÖLÜM I.....	1
GİRİŞ	1
1.1. Problem Durumu	1
1.2.Araştırmanın Amacı	9
1.3.Araştırmanın Önemi.....	10
1.4. Varsayımlar	11
1.5. Sınırlılıklar.....	11
1.6. Tanımlar	12
BÖLÜM II.....	13
KURAMSAL ÇERÇEVE	13

2.1. Vatandaşlık Kavramı ve Tarihsel Gelişimi	13
2.2. Dijital Vatandaşlık	16
2.2.1. Dijital Vatandaşlığın Alt Boyutları	19
2.2.1.1. <i>Dijital Erişim</i>	19
2.2.1.2. <i>Dijital İletişim</i>	20
2.2.1.3. <i>Dijital Ticaret</i>	21
2.2.1.4. <i>Dijital Etik</i>	22
2.2.1.5. <i>Dijital Hukuk</i>	23
2.2.1.6. <i>Dijital Sağlık</i>	24
2.2.1.7. <i>Dijital Hak ve Sorumluluklar</i>	25
2.2.1.8. <i>Dijital Okuryazarlık</i>	26
2.2.1.9. <i>Dijital Güvenlik</i>	27
2.3. Dijital Teknolojiler, Dijital Dönüşüm ve Dijital Güvenlik.....	28
2.4. Yeterlik, Dijital Yeterlik ve Dijital Güvenlik Yeterliği	34
2.4.1. Yeterlik.....	34
2.4.2. Dijital Yeterlik.....	36
2.4.3. Dijital Güvenlik Yeterliği	38
2.4.3.1. <i>Teknik Boyutta Dijital Güvenlik Yeterliği</i>	40
2.4.3.2. <i>Psikososyal Boyutta Dijital Güvenlik Yeterliği</i>	43
2.4.3.3. <i>Çevrim İçi Alışveriş Boyutunda Dijital Güvenlik Yeterliği</i>	45
2.4.3.4. <i>Hak ve Sorumluluk Boyutunda Dijital Güvenlik Yeterliği</i>	47
2.4.3.5. <i>Sağlık Boyutunda Dijital Güvenlik Yeterliği</i>	48
2.5. Öz Yeterlik ve Dijital Güvenlik Öz Yeterliği	50
2.6. Çevrim İçi Öğrenme	53
2.7. Çevrim İçi Destekleyici Öğrenme Aracı	57
2.8. Öğrenme Yönetim Sistemleri.....	61
2.9. Dijital Güvenliğin Sosyal Bilgiler Dersi Öğretim Programı (SBDÖP) ile İlişkisi .	61
2.10. İlgili Araştırmalar	65
2.10.1. Yurt İçinde Yapılmış Araştırmalar	66
2.10.2. Yurt Dışında Yapılmış Araştırmalar	80

BÖLÜM III	90
YÖNTEM.....	90
3.1. Araştırmanın Modeli	90
3.2. Çalışma Grubu	93
3.3. Veri Toplama Aracı	95
3.3.1. Dijital Güvenlik Öz Yeterlik Envanteri	95
3.3.1.1. Teknik Alt Ölçeği.....	96
3.3.1.2. Psikososyal Alt Ölçeği	97
3.3.1.3. Çevrim İçi Alışveriş Alt Ölçeği.....	98
3.3.1.4. Hak ve Sorumluluk Alt Ölçeği.....	99
3.3.1.5. Sağlık Alt Ölçeği.....	100
3.4. Öğretim Materyali	100
3.4.1. Araç İçeriğinin Oluşturulması	102
3.4.1.1. Animasyon Video Bölümü	102
3.4.1.2. Önemli Kavramlar Bölümü.....	103
3.4.1.3. Özet Bölümü	104
3.4.1.4. Test Bölümü.....	105
3.4.2. SCORM Paketlerin Oluşturulması	107
3.4.3. SCORM Paketlerinin Öğrenci Erişimine Sunulması	108
3.5. Araştırmanın Deneysel Süreci	108
3.5.1. Deneysel İşlemin Uygulama Basamakları.....	109
3.6. Veri Analizi.....	112
BÖLÜM IV.....	115
BULGULAR VE YORUM	115
4.1. Birinci Alt Probleme İlişkin Bulgular ve Yorumlar	115
4.2. İkinci Alt Probleme İlişkin Bulgular ve Yorumlar	117
4.3. Üçüncü Alt Probleme İlişkin Bulgular ve Yorumlar	119
4.4. Dördüncü Alt Probleme İlişkin Bulgular ve Yorumlar	121

BÖLÜM V	124
SONUÇ, TARTIŞMA VE ÖNERİLER.....	124
5.1. Sonuç ve Tartışma.....	124
5.2. Öneriler	134
5.2.1. Uygulamaya Yönelik Öneriler	134
5.2.2. Araştırmaya Yönelik Öneriler	135
KAYNAKLAR.....	136
EKLER	161



TABLÖLAR LİSTESİ

Tablo 1: <i>Araştırmanın Deneysel İşlem Kısımına Katılan Öğrenciler</i>	94
Tablo 2: <i>Uygulamadaki Deney ve Kontrol Gruplarının Cinsiyet Değişkenine Göre Dağılımı</i>	94
Tablo 3: <i>Öğretim Materyali İçerik Bilgisi</i>	101
Tablo 4: <i>Deney ve Kontrol Grubuna Uygulanan Deneysel İşlem</i>	109
Tablo 5: <i>Normallik Dağılım Test Sonucu</i>	114
Tablo 6: <i>Deney Grubu İle Kontrol Grubunun Öntest Puanları Arasındaki Farklılığa İlişkin Mann-Whitney U Testi Sonuçları</i>	116
Tablo 7: <i>Kontrol Grubunun Öntest Puanları ile Sontest Puanları Arasındaki Farklılığa İlişkin Wilcoxon İşaretli Sıralar Testi</i>	118
Tablo 8: <i>Deney Grubunun Öntest Puanları ile Sontest Puanları Arasındaki Farklılığa İlişkin Wilcoxon İşaretli Sıralar Testi</i>	120
Tablo 9: <i>Deney Grubu İle Kontrol Grubunun Sontest Puanları Arasındaki Farklılığa İlişkin Mann-Whitney U Testi Sonuçları</i>	122

ŞEKİLLER LİSTESİ

<i>Şekil 1.</i> Dijital vatandaşlık alt boyutları	19
<i>Şekil 2.</i> Bütünsel yeterlik modeli	35
<i>Şekil 3.</i> Dijital yeterliğin kavram haritası	38
<i>Şekil 4.</i> Araştırmanın deneysel işleminin akış şeması	93
<i>Şekil 5.</i> Çevrim içi destekleyici öğrenme aracının içerik oluşturma aşamalarını gösteren akış şeması.....	102
<i>Şekil 6.</i> Çevrim içi destekleyici öğrenme aracının ilk bölümünde konu anlatım amacıyla hazırlanan animasyon videoya ait örnek bir görüntü	103
<i>Şekil 7.</i> Çevrim içi destekleyici öğrenme aracının ikinci bölümünde yer alan önemli kavramlara ait örnek bir görüntü.....	104
<i>Şekil 8.</i> Çevrim içi destekleyici öğrenme aracının üçüncü bölümünde yer alan özete ait örnek bir görüntü.....	105
<i>Şekil 9.</i> Çevrim içi destekleyici öğrenme aracının dördüncü bölümünde yer alan teste geçişe ait örnek bir görüntü.....	106
<i>Şekil 10.</i> Çevrim içi destekleyici öğrenme aracının dördüncü bölümünde yer alan teste ait örnek bir görüntü.....	106
<i>Şekil 11.</i> Oluşturulan SCORM paketlerine ait örnek bir görüntü	107
<i>Şekil 12.</i> Oluşturulan SCORM paketlerinin ÖYS’de sunumuna ait örnek bir görüntü	108
<i>Şekil 13.</i> Araştırmanın deneysel sürecinin akış şeması.....	112

SİMGE VE KISALTMALAR LİSTESİ

MEB	Milli Eğitim Bakanlığı
Akt.	Aktaran
Çev.	Çeviren
Ed.	Editor
Edt.	Edition
Eds.	Editors
f	Frekans
vd.	Ve diğerleri
S	Standart sapma
$\bar{x}$	Aritmetik ortalama
F	F değeri (Varyans)
KMO	Kaiser Mayer-Olkin
n	Denek sayısı
p	Anlamlılık düzeyi
pp	Page paper
s	Sayfa
ss	Sayfa sayısı
sd	Serbestlik derecesi
vb.	Ve benzeri

SPSS	Statistical Package For The Social Sciences
SBDÖP	Sosyal Bilgiler Dersi Öğretim Programı
TDK	Türk Dil Kurumu
TÜİK	Türkiye İstatistik Kurumu



BÖLÜM I

GİRİŞ

Bu bölümde araştırmanın problem durumu, amacı, önemi, varsayımları, sınırlılıkları ile tanımlara yer verilmiştir.

1.1. Problem Durumu

Son yıllarda bilgi ve iletişim teknolojilerinde yaşanan gelişmeler bu teknolojilerin verimlilik düzeyini artırmıştır. Bilgi ve iletişim teknolojilerinin yüksek verimlilik düzeyleri neticesinde bireyler tarafından bu teknolojiler yoğun bir şekilde benimsenmiştir (McCormac vd, 2017, s.40). Öyle ki 2022’de 7.91 milyarlık dünya nüfusunun büyük çoğunluğu dijital araçları ve interneti kullanmaktadır (We Are Social ve Hootsuite, 2022a). Bu durum Türkiye’de de benzer şekildedir ve hatta Türkiye ortalaması dünya geneline oranla daha yüksektir (We Are Social ve Hootsuite, 2022b; Türkiye İstatistik Kurumu [TÜİK] 2022). Dolayısıyla günümüzde hem Dünya’da hem Türkiye’de nüfusun önemli bir kısmı dijital topluma katılım sağlamaktadır.

Bilgi ve iletişim teknolojilerinin kitleler tarafından sıklıkla tercih edilmesinin sebeplerinden biri de topluma ait birçok bilginin bu teknolojiler ve internet aracılığıyla hızlıca erişilip yayılmasıdır ve bu durum dijital ortamı büyük bir bilgi kaynağı haline getirmiştir. Öyle ki aranan birçok bilgi, içerik ve ürün dijital ortamda mevcut haldedir. Üstelik bu ürün, bilgi ve içeriklere erişim dijital kullanıcıların kullandığı arama motorları (örneğin Google, Yandex, Bing, Yahoo vs.) ile oldukça basit hale gelmiştir. O’Reilly (2005) örneğin Google’ın Web

2.0'nin standart taşıyıcısı olduğunu belirtmekle birlikte bunun bilgiye ulaşmak için bir aracı olduğunu ifade etmiştir (s.3). Bu atılımlarla bilginin sır olarak kalmadığı, her şeyin hızlıca yayınlandığı ve yayıldığı dijital ortam ile insan sadece etrafındaki sosyal alanlara ve yaşamlara vakıf olma durumundan çıkarak yaşamının kapsamını genişletmiştir. Castells' in (2004) ağ toplumu olarak adlandırdığı düşünceye göre ağların büyüklüğü insanların küresel toplumda konumlarını da belirlemiştir. Örneğin, toplum 5.0 ile yüksek yaşam kaliteli, her bilgiye erişilebilen geniş bir toplum yaratmak amaçlanmaktadır (Fukuyama, 2018, s.48). Kısacası teknolojik devrimlerle insana dair her konuya da temas edebilen dijital bir toplum oluşturmak istenmektedir.

Günümüzde bilgi ve iletişim teknolojilerinde yaşanan gelişimler neticesinde büyüyen dijital toplum ve dijital ortamın avantajları dijital dönüşümü beraberinde getirmiştir. Bozkurt, Hamitoğlu, Liman Kaban, Taşçı ve Aykul (2021)'a göre *“dijital dönüşüm, dijital teknolojileri kullanarak yeni fırsatlar ve değerler yaratma; sosyal yapıları dijital teknolojilerle güçlendirme ve daha verimli hale getirme süreci”* olarak tanımlanmıştır (s.40). Tanımdan da anlaşılacağı üzere dijital dönüşümün aslında pek çok duruma katkısı bulunmaktadır ve dijital dönüşüm gelişim esaslı bir harekettir. Kavramın temel amacından ve işlevinden ötürü günümüzde pek çok alan dijital dönüşüm yolundadır. Ayrıca dijital dönüşümün yayılım alanının genişlemesi ve bu alanlara uyum sağlamak dijital dönüşümü keyfi bir süreç olmaktan çıkarıp zorunlu bir katılım sürecine dönüştürmüştür. Başka bir ifadeye göre dijital ortamlar aracılığıyla sosyal ve politik çevre ile etkileşim içinde olan bireylerin, dönüşüm içinde olan dijital topluma daha fazla uyum sağlamak için dijital araçları ve platformları kullanması zorunlu hale gelmiştir (Hintz, Dencik ve Jorgensen, 2017, s.731). Çünkü bilgi teknolojilerinin verimliliğini kullanmamak gelişimin ardında kalmaktır ve bu durum bireyleri dönüşüme katılmaya zorlamaktadır (Kocaman Karoğlu, Bal ve Çimşir, 2020, s.148).

Dijital dönüşümün insanların yaşamsal ihtiyaçlarına pratiklik getirmesi amacıyla yapıldığı ifade edilmektedir (Kocaman Karoğlu vd., 2020, s.148) ve bu alanlar bilindiği üzere sağlık, finans, ekonomi, devlet hizmetlerine erişim, eğitim gibi alanlar olmuştur. Bununla birlikte Dünya Sağlık Örgütü tarafından 2020 yılının başlarında Covid 19 salgınından dolayı pandemi ilan edilmiş ve birçok ülkede eğitime ara verilmiştir. Bu sebeple uzaktan eğitime geçilen pandemi sürecinde dijital dönüşüm eğitim alanında acil bir şekilde ilerlemiştir. Zaten

dijital dönüşüm yolunda olan eğitim alanında pandemi ile birlikte kullanılan teknolojik kullanımı artmış, video projektör, akıllı tahta, e-kitap, indirilebilir müzik kullanılırken (Kocaman Karoğlu vd., 2020, s.148) bunlara ek olarak uzaktan eğitim platformları, mobil araçlar, süresiz ağ içerikleri, dijital içeriklerin kullanım oranı artmıştır. Bununla birlikte sıklıkla kullanılan dijital araç ve platformlardan bir kısmı da şöyledir; akıllı telefonlar, bilgisayarlar, tabletler ve bu dijital araçlar aracılığıyla erişilen sosyal ağ platformları, çevrim içi alışveriş platformları, çeşitli içeriklere sahip web siteleri, ülkemizde eğitim öğretim portalı olarak kurulan ve kullanılan EBA. Kısacası dijital dönüşüme uğrayan alanlar arasında eğitimin de var olduğu ve bu alanda paydaşların dijital dönüşüme ve dijital topluma uyumu önemli hale gelmiştir. Özellikle eğitim paydaşları arasında yer alan çocukların dijital beceri ve yeterliklerinin düzeyi önemli hale gelmiştir.

Günümüzün çocuklarına dijital yerliler de denilmektedir. Dijital yerliler ifadesi ilk kez Prensky (2001) tarafından kullanılmıştır (s.1). Burada dijital yerliler, dijital araçları, dijital oyunları ve interneti çok iyi kullanan kuşak olarak tasvir edilmektedir. Buna ek olarak Prensky (2001) dijital yerlilerin dijital becerilerinin gelişmiş olduğunu ve öğretim tekniklerine dijital teknolojilerin entegre edilmesi gerektiğini, bunu da yaparken eski şeyleri yapmanın yeni yollarını öğretmekten geçtiğini, yani dijital yollarla özellikle de dijital oyunlar ile yapmanın onların diline daha uygun olacağını ifade etmektedir (s.4). Tüm bunlardan anlaşılıyor ki dijital yerliler artık dijital ortamlarda zaman geçirmekten hoşlanıyor. Dijital yerliler tarafından tercih edilen dijital teknolojilere rağbet oranının fazla olmasının sebepleri arasında yaşlılarının bu ortamda olması, geleneksel oyun kültürünün azalması, dijital platformlardaki eğlence amaçlı ürünlerin çekiciliği ve tüm bunları kullanırken süre ve yer bağlamında bağımlılık yaşanmaması yer almaktadır. Bununla birlikte dijital yerliler öğrenirken artık daha farklı yaklaşım ve içeriklere ihtiyaç duymaktadır. Çünkü algı ve yaşamsal faaliyetleri diğer kuşaklardan farklıdır. Deyim yerindeyse dijital yerliler aslında sanal bir hayat yaşamaktadır. Bu sebeple eğitimin hedef kitlesi dijital yerlilerken, teknolojik yaklaşımların yaşanması kaçınılmaz olma yolundadır. Fakat dijital teknoloji devrimleri ve dijital toplumun genişlemesiyle birlikte dijital yetkinlikler de çeşitlenmekte ve bu yetkinlikleri gelişmelerle aynı hızda kazandırmak zorlaşmaktadır. Çünkü günümüzde teknolojinin gelişimi bir insanın yetkinlik gelişimine göre çok daha hızlı gelişebilmektedir.

Bu durum gençleri teknolojiye ve teknolojinin yanlış kullanımına karşı bilinçsiz ve savunmasız bırakabilmektedir (Miles, 2011, s.1).

Dijital teknolojilerin kullanımı konusunda, dijital ortamda uygun olmayan kullanımları önlemek ve dijital dönüşümün hızına yetişmek amacıyla dijital becerilerin geliştirilmesi önem arz etmektedir. Bu sebeple dijital yetkinliklerin ve dijital vatandaşlık eğitiminin çocuk yaşta başlaması gerektiğini savunan Ribble ve Bailey (2007) öğretmenlerin, dijital teknolojilere iletişim ve etkileşim aracı olarak bakmaları, öğrencilerin bu araçlar aracılığıyla dijital toplumları oluşturmalarına izin vermeleri, aynı zamanda sınırları belli olmayan bu dijital topluma onları hazırlamaları gerektiğini belirtmiştir (s.10). Bu sebeple öğrencilerin dijital ortamı anlamaları ve bilinçli bir uyum sağlamaları için okullarda dijital vatandaşlık eğitiminin verilmesi gerekmektedir. Ayrıca dijital eğitimin çeşitli yollarla dijital toplumun diğer paydaşlarına da verilmesi önem arz etmektedir. Bu konuda öğretim elemanlarının ve öğretmenlerin dijital durumlarını, yeterliklerini ve öz yeterliklerini tespit etmeyi amaçlayan ve bunların geliştirilmesi gerektiğini ifade eden çeşitli araştırmalar mevcuttur (Binay Eyuboğlu ve Karaoğlu Yılmaz, 2018; Fidan ve Cura Yeleğen, 2022; Gökbulut, Keserci ve Akyüz, 2021; Göçen Kabaran ve Uşun, 2021; Gümüş, 2021; Korkmaz, Arıkaya ve Altıntaş, 2019; Tatlı, 2018). Eğitimin tüm paydaşlarının dijital yeterlikler açısından eğitildiği toplumda dijital gelişimler daha mantıklı şekilde ilerleyecektir. Böylelikle dijital vatandaşlık gibi ortak bir çerçeve yaratılan bu yeni toplumda tüm bireylerin birbirini anlaması için yeni bir başlangıç olacaktır (Ribble ve Bailey, 2007, s.12). Tabii ki dijital çağda ortaya çıkan pek çok sorunu da çözmek için dijital vatandaşlık büyük bir mücadelenin önemli bir adımı olacaktır.

Dijital vatandaşlık kavramı ile ilgili alanyazın incelendiğinde genel ve ortak bir görüş olarak “teknolojiyi uygun ve sorumlu bir şekilde kullanan vatandaş” ifadeleri yer almaktadır. Örneğin, Ribble ve Bailey (2007) dijital vatandaşlığı, “*bilgi ve iletişim teknolojilerini uygun kullanım davranışları*” olarak tanımlamıştır (s.10). Diğer bir tanıma göre dijital vatandaşlık “*çevrim içi topluma katılma yeteneğidir*” (Mossberger, Tolbert ve McNeal, 2007, s.1). Dijital vatandaşlık ve alt boyutları örgün öğretimde öğrencilerin bilişim teknolojilerini uygun kullanımıyla ilgili eğitimin paydaşlarına önerilerde bulunan bir yöntembilim olarak alanyazına girmiştir (Çubukçu ve Bayzan, 2013, s.3). Bu ifadelerden hareketle, çevrim içi topluma katıldığında uygun ve sorumlu davranış normlarını

içselleştiren ve uygulayan vatandaşların iyi bir dijital vatandaş olabileceği söylenebilir. Bu amaçla hızla dönüşen bu dünyada nasıl davranacağımızı ve dijital vatandaşlık aracılığıyla uygun kullanım yöntemleri içselleştirilebilir (Oxley, 2010, s.1). Dijital vatandaşların, dijital vatandaşlığın ne demek olduğunu ve dijital teknolojilerin uygun kullanımlarının ne olduğunu anlamaları için Ribble ve Bailey (2007) dokuz alt boyuttan bahsetmektedir ve bu boyutlar; erişim, iletişim, ticaret, etik, hukuk, sağlık, hak ve sorumluluk, okuryazarlık ve güvenlidir (s.10).

Dijital vatandaşlık boyutlarını ilgilendiren önemli meselelerden biri de ortaya çıkan problemlere karşı çözüm üretmek ya da çıkabilecek sorunlara karşı önlem almaktır. Burada söz konusu boyut güvenlidir. Bugün medya takip edildiğinde gizlilik ve güvenlik ile ilgili dijital olayların sıklıkla yer işgal ettiği görülmektedir. Özellikle dijital bağımlılıkla, dijital dolandırıcılıkla (son zamanlarda sıkça duyulan twitch dolandırıcılığı, kripto para), uygunsuz içeriklere sahip yabancı menşeli dizi ve film platformlarıyla (Netflixe yayınlanan çocuk dizisi Jurassic World Kretase Kampı, Lightyear vb.) ve dijital oyunlarla ilgili haberlerle karşılaşmakta ve bu sorunlar çocukları tehdit etmektedir. Bununla birlikte son zamanlarda bazı dijital oyunlar (Squid Game, Mavi Balina vb.), olumsuz içeriklere sahip çizgi film ve videoların ruhsal etkileri, dijital toplumda özellikle gençlerin sıkça maruz kaldığı dijital zorbalık çeşitleri dijital güvenlik ile ilgili medyaya yansıyan haberlerin başında gelmektedir. Medya, günlük yaşamda duyulan/karşılaşılan dijital olaylar ve riskler dijital güvenliğin günümüzde daha da önem kazandığını göstermektedir.

Dijital vatandaşlığın yaklaşım alanlarından biri olarak karşımıza çıkan dijital güvenlik Ribble ve Bailey (2007)'e göre *“tüm teknoloji kullanıcılarının kişisel güvenliğini ve ağlarının güvenliğini garanti etmek için alması gereken önlemlerdir”*(s.33). Ayrıca *“dijital güvenlik, meydana çıkan veya çıkma ihtimali olan dijital tehditlere karşı önlem almaktır ve bu sayede çevrim içi ortamda dijital cihazları kullanırken güvende olmaktır”* (Ribble, Bailey ve Ross, 2004, s.9). Bireylerin sanal ortamda güvenliklerini sağlamak, kendilerini korumak için alabilecekleri elektronik önlemler; bireysel olarak veri yedekleme, virüs koruma önlemlerinin alınması dijital güvenlik kapsamına girmektedir (Peker Ünal, 2017, s.185). Buna ek olarak dijital güvenlik elektronik önlemlerin haricinde, sosyal ve fiziksel riskleri engellemek için de çevrim içi ortamda bilinçli ve sorumlu davranış normlarına uygun hareket ederek de sağlanmalıdır. Çevrim içi teknolojiler ve diğer dijital platformların

güvenli, bilinçli ve doğru kullanımı pek çok araştırmaya konu olmuştur (Çağiltay, İslim, Kaşıkçı, Kurşun ve Yılmaz, 2017; Çömlekçi, 2019; Erdoğan, 2017; Helsper ve Smahel, 2020; Holloway, Green ve Livingstone, 2013; Nannatt, Tariat, Gowda ve Devassy, 2022; Topal ve Akgün, 2015).

Snyder (2016), dijital vatandaşlık unsurları arasında belki de en popüler unsurun güvenlik olduğunu belirtmiş ve diğer unsurlara göre şemsiye niteliğinde olduğunu ifade etmektedir (s.96). Dijital güvenliğin diğer unsurları da kapsayıcı olarak görülmesindeki temel sebep, diğer alt boyutları ilgilendiren konularda da ortaya çıkan risklerle alakalı olmasıdır. Güvenlik unsurunun kapsayıcılığı aslında sadece teknik yönden dijital cihazlarımızı güvence almaktan ibaret olmayarak, dijital etkileşimler ve eylemler sonucunda dijital zorbalık, kişisel verilerin tehdidi, bilişim suçlarına alet edilme, dijital bağımlılık, zararlı içeriklere maruz kalma, dijital dolandırıcılık, dijital etik kurallarının ihlali gibi risklerin varlığının bireylerin güvenliğini fazlaca tehdit etmesine de dayanmaktadır. Her gün çok sayıda kişinin çevrim içi ortamda çeşitli risklere maruz kaldığını ve güvenlik problemi yaşadığını çeşitli araştırmalar ortaya koymuştur (Anderson ve Agarwal, 2010; Stanton ve Stam, 2006). Bununla birlikte çocuk yaş grubunun da risklerle karşılaştığı ifade edilmektedir (Livingstone vd., 2017, s.2; Nawaila, Kani ve Kanbul, 2021, s.3). Çünkü günümüzde insanlar artık birçok işi dijital araçlar aracılığıyla çevrim içi yapmaktadır. Dolayısıyla bireylerin çevrim içi ortamda fırsatlardan kaynaklı vakit geçirme süresi arttıkça karşılaştığı riskler de o kadar artmaktadır (Livingstone vd., 2017, s.4). Bunun sebebi ise bireyler tarafından kişisel verilerin kontrolsüz olarak paylaşımı, hızlı medya akışına yetişme arzusu, tıklama dürtüsüdür. Bu ve benzeri davranışsal kontrolsüzlükler riskleri kişinin kendine çekmesine sebep olmaktadır.

Dijital güvenliğı tam olarak sağlamak pek mümkün görülmemektedir, çünkü işin içerisinde insan faktörü yer almaktadır ve hiçbir filtreleme kişinin güvenliğini tam anlamıyla sağlayamaz (Robinson, Brown ve Green, 2010, s.14). Bununla birlikte dijital güvenliğı sağlamak için sadece bilgi ve iletişim teknolojilerini kullanmaktan kaçınmak ya da sadece güvenilir siteleri ziyaret etmek, güvenlik yazılımı kullanmak yetersiz kalacaktır. Bunların haricinde sonuçları hemen ortaya çıkmayan, yıllar sonra doğurabileceğı sonuçlar hesap edilemeyen pek çok veri paylaşımı yapılmakta ve dijital ayak izleri bırakılmaktadır. Bu durumu Ribble ve Bailey (2007) şöyle ifade etmiştir; *“elektronik ortamlarda kişisel bilgiler güvende olmalı çünkü teknolojinin davetsiz misafirleri ön kapıdan girmez, sadece virüs*

koruması yetmez bunun yanı sıra kişilerin bilinçli birer kullanıcı olmaları gerekir ki çoğu zaman güvenlik sorunları ekipmanlardan değil, kullanıcı hatalarından kaynaklanır” (s.34).

Dijital ortamda güvenliği sağlayabilmek adına literatürde bir dizi önlemler sıralanmıştır ve kişilerin kendilerince aldıkları birçok önlem bulunmaktadır. Bireysel olarak kişinin kendini dijital dünyadan tamamen soyutlaması ya da riskleri görmezden gelmesi bir çözüm değildir. Bu durumu çocuk yaş grubu üzerinde düşündüğümüzde ebeveyn kısıtlaması akla gelmektedir ve bu durum da kesin bir çözüm değildir. Çünkü ebeveyn arabuluculuğu her ne kadar risklere maruz kalmayı etkileyen bir durum olsa da hem dijital ortamın fırsatlarından yararlanma hem de riskleri azaltma durumu mümkün değildir (Stoilova, Livingstone ve Khazbak, 2021, s.29). Bunun yerine kullanıcıların her gün yenisi eklenen bu dijital tehditler karşısında takipte olmaları ve bu tehditlere karşı alınabilecek önlemleri, kullanılacak stratejileri öğrenip işe koşmalıdırlar (Çolak, 2019, s.13). Kişilerin dijital güvenliğini sağlaması için farkındalık düzeyini yükseltebilecek (Yılmaz, Şahin ve Akbulut, 2016, s.28) ve dijital güvenlik yeterliğini artıracak eğitimlerden geçmektedir. Bratina ve Krasna’a (2011) göre eğitim alanında dijital güvenlik dijital yeterlikler arasında kabul edilmektedir ve eğitim açısından en yaygın riskin dijital güvenlik olduğunu belirtmektedir (s.2). Bu açıdan dijital vatandaşlık ve onun günümüzde çok popüler olan alt boyutu dijital güvenlik eğitimi çocuklara erken yaştan itibaren verilmeye başlanmalıdır. Bu noktada ülkemizde öğretmenlerin dijital vatandaşlık ile ilgili beceri düzeylerini belirlemek amacıyla çeşitli çalışmalar yapılmıştır (Arcagök, 2020; Görmez, 2017; Sari, 2019; Yılmaz vd., 2016). Bu çalışmaların sonuçlarına göre öğretmenlerin dijital vatandaşlık becerilerinin yeterli düzeyde olmadığı anlaşılmaktadır. Benzeri şekilde öğrencilerin de dijital vatandaşlık beceri ve algı düzeylerini ortaya koymayı amaçlayan çalışmalar da vardır (Çepni, Oğuz ve Kılcan, 2014; Karaduman ve Öztürk, 2014; Kavuk, 2011; Korkmaz ve Kıran Esen, 2012). Yine bu çalışmalardan anlaşıldığı üzere ilköğretim öğrencilerinin dijital vatandaşlık becerilerinin yeterli düzeyde olmadığı belirtilmiştir. Dijital güvenlik, dijital vatandaşlığın bir alt boyutu olduğu için çalışmaların güvenlik alt boyutu ile ilgili bulgulara bakıldığında benzer sonuçlar görülmektedir.

Bu çalışmada ortaokul öğrencileri açısından dijital güvenlik yeterlik göstergelerini belirlemek amacıyla dijital güvenlik becerileri, dijital güvenlik yeterlikleri, dijital riskler, 21. yüzyıl dijital becerileri açısından alanyazın taraması yapılmış ve Sosyal Bilgiler Dersi

Öğretim Programı (SBDÖP) incelenmiştir. Bu doğrultuda alanyazında dijital güvenlikle ilgili çalışmalarda teknik becerileri ve yeterlikleri merkeze alan çalışmalara (M. Tekerek ve Tekerek, 2013; Şahinaslan, Kandemir ve Şahinaslan, 2009) ve daha kapsamlı olarak dijital zorbalık, çevrim içi alışveriş, hak ve sorumluluk, sağlık gibi boyutları da kapsama alan (Bayındır, 2020; Çolak, Yalçın ve Korkmaz, 2011; Çolak, 2019; Durmaz ve Ulukol, 2022; Talan ve Aktürk, 2021) çalışmalara da rastlanmıştır. Ayrıca çocuk yaş grubu üzerinde dijital güvenliği etkileyen etmenler hakkında yapılan araştırmalar (Çubukçu ve Bayzan, 2013; Demirel, Yörük ve Özkan, 2012; Vural ve Sağıroğlu, 2008) ve risk alanlarını araştıran çalışmalar da bulunmaktadır (Byrne vd., 2016; Çelen, Çelik ve Seferoğlu, 2011, Karakuş, Çağıltay, Kaşıkçı, Kurşun ve Ogan, 2014). Bu çalışmalarda çocuk yaş grubunun dijital güvenlik yeterlik ve becerileri üzerinde risk ve ihmallerin etkili olduğu ifade edilmektedir.

Bu çalışmada dijital güvenlik yeterlik göstergelerini tespit etmek amacıyla incelenen SBDÖP’nda yer alan yetkinlikler, özel amaçlar, beceriler, değerler, programın uygulanmasında dikkat edilecek hususlarda “sanal ticaret, sosyal medya, dijital bölünmüşlük, kimlik hırsızlığı, kişisel bilginin gizliliği, siber dolandırıcılık, siber zorbalık” kavramlarının yer aldığı görülmektedir. Bununla birlikte programdaki kazanım ve ders kitaplarında ise “bilginin doğruluğu ve güvenilirliği, internet alışverişi, internetin doğru ve bilicli kullanımı, kimlik hırsızlığı, güvenli teknoloji kullanımı, bilginin korunması/veri güvenliği, dijital araçların etki alanlarında yaşanan güvenlik sorunları, sanal ortamda güvenlik kuralları, dijital oyunların güvenlik açısından etkileri, kaynak kullanımında güvenlik problemleri, telif ve patent, dijital haklar ve sorumluluklar, dijital bağımlılık ve zararlı içeriklerin etkileri” ele alınmıştır. Buradan hareketle Milli Eğitim Bakanlığı [MEB], SBDÖP ve alanyazın incelemesi neticesinde dijital güvenlik yeterlik göstergeleri teknik, psikososyal, çevrim içi alışveriş, hak ve sorumluluk ve sağlık olarak boyutlandırılmıştır.

Teknik, psikososyal, çevrim içi alışveriş, hak ve sorumluluk ve sağlık boyutlarıyla ele alınan dijital güvenlik yeterlik göstergeleri çerçevesinde ortaokul 7. sınıf öğrencilerine yönelik olarak çevrim içi öğrenme yaklaşımında uygulanmak üzere çevrim içi destekleyici öğrenme aracı geliştirilmiştir. Çevrim içi öğrenme ortamı iyi tasarımıandığı ve öğrenci ihtiyaçlarına yönelik olduğu taktirde öğrenmeyi hedefe ulaştırabilecek bir ortamdır. Çünkü burada öğrenci kendi öğrenme hızında öğrenebilecek aynı zamanda kullanılan dijital materyaller sayesinde motivasyon ve ilgi düzeyi yükselerek konuya daha iyi adapte olabilecektir.

Günümüzde son yıllarda uzaktan eğitim, çevrim içi öğrenme, oyunlaştırılmış öğrenme ortamları dijital yerlilere hitap edebilmek amacıyla tercih edilirlilik oranını artırmıştır. Çünkü bahsettiğimiz gibi özellikle ortaokul yaş seviyesindeki çocuklar bu öğrenme materyallerine ve ortamlarına ihtiyaç duymaktadırlar. Ayrıca 2021 yılında yayınlanan “Millî Eğitim Bakanlığı Ders Kitapları ve Eğitim Araçları Yönetmeliğinde” öğrencilerin kullanabileceği, öğrenme alanlarıyla ilişkilendirilmiş, öğrenmeyi destekleyici, öğrenen özelliklerine göre hazırlanmış, interaktif soruların da yer aldığı dijital içeriklere yer verilebileceği ifade edilmektedir (MEB, 2021). Bu amaçla animasyon videoların ve dijital görsellerin kullanıldığı, geri dönüt veren, aynı zamanda öğrenme ortamını kendinin yönetebildiği bir araç sayesinde dijital güvenlik eğitimi gerçekleştirilmiştir.

Bu doğrultuda gerçekleştirilen araştırmada sosyal bilgiler dersinde 7. sınıf öğrencilerinin dijital güvenlik yeterlikleri için geliştirilen çevrim içi destekleyici öğrenme aracının öğrencilerin dijital güvenlik öz yeterlik algılarına etkisini belirlemek amaçlanmıştır. Dijital güvenlik ile ilgili yapılan araştırmalar incelendiğinde, sosyal bilgiler kapsamında dijital yerlilere daha iyi hitap edebilmek adına çevrim içi destekleyici öğrenme aracı ile ortaokul öğrencilerinin (7.sınıf) dijital güvenlik yeterliklerini geliştirmeye ve bu eğitimin öz yeterliğe etkisini belirlemeye yönelik bir çalışmanın yapılmasının alanyazına katkı sağlayacağı düşünülmüştür. Ayrıca yapılmış olan bu çalışma ile SBDÖP’nda ilgili kazanımlarda “dijital güvenlik” konusunda çevrim içi öğrenme yaklaşımında çevrim içi öğrenme materyali ile öğretimine bir örnek oluşturmak istenmiştir.

1.2.Araştırmanın Amacı

Bu araştırmanın amacı, sosyal bilgiler dersinde dijital güvenlik yeterliği için geliştirilen çevrim içi destekleyici öğrenme aracının öğrencilerin dijital güvenlik öz yeterlik algılarına etkisini ortaya koymaktır. Bu temel amaç doğrultusunda aşağıdaki sorulara cevap aranmıştır:

1. Deney grubu öğrencileri ile kontrol grubu öğrencilerinin dijital güvenlik öz yeterlik envanterine ait ön test puan ortalamalarına bağlı sıra ortalamaları arasında istatistiksel olarak anlamlı bir fark var mıdır?

2. Kontrol grubu öğrencilerinin dijital güvenlik öz yeterlik envanterinde ön test ve son testten aldığı puan ortalamalarına bağlı sıra ortalamaları arasında istatistiksel olarak anlamlı bir fark var mıdır?
3. Deney grubu öğrencilerinin dijital güvenlik öz yeterlik envanterinde ön test ve son testten aldığı puan ortalamalarına bağlı sıra ortalamaları arasında istatistiksel olarak anlamlı bir fark var mıdır?
4. Deney grubu öğrencileri ile kontrol grubu öğrencilerinin dijital güvenlik öz yeterlik envanterinde son test puan ortalamalarına bağlı sıra ortalamaları arasında istatistiksel olarak anlamlı bir fark var mıdır?

1.3.Araştırmanın Önemi

Bu araştırmada, sosyal bilgiler dersinde dijital güvenlik yeterliğini geliştirmek için hazırlanmış olan çevrim içi destekleyici öğrenme aracının, öğrencilerin dijital güvenlik öz yeterliğine etkisini belirlemek amaçlanmıştır. Kişilerin öz yeterlik durumlarına etkisi olduğu düşünülen çevrim içi destekleyici öğrenme aracının ne derece etkili olduğu da tespit edilmeye çalışılmıştır.

Bilgi ve iletişim teknolojilerinde meydana gelen gelişimler ve dijital dönüşüm neticesinde vatandaşların yaşam tarzlarında ve rutinlerinde de dönüşüme sebep olmuştur. Bu dönüşüm ortamının içine doğmuş olan çocuk yaş grubunun dijital ortamı kullanmayı tercih ettiği görülmektedir. Bilgi ve iletişim teknolojilerinin istenilen seviyede doğru, bilinçli güvenli, sağlıklı ve diğer kullanıcıların hak ve sorumluluklarına duyarlı olarak kullanımı için çocuk yaş grubunun dijital güvenlik öz yeterliklerinin geliştirilmesi önem arz etmektedir. Ayrıca çocuk yaş grubunun dijital ortamın risklerine karşı farkındalığının, mahremiyet konusuna uygun davranışları gerçekleştirebilme, dijital ortamı zaman, içerik ve fiziksel olarak sağlıklı kullanabilme konusunda yeterliklerinin ve öz yeterliklerinin geliştirilmesi gerekmektedir.

İlgili alanyazın incelendiğinde öğrencilerin, öğretmenlerin, öğretmen adaylarının, öğretim elemanlarının, dijital yerlilerin ve dijital göçmenlerin veri güvenliği, bilgi güvenliği, siber güvenlik ve dijital güvenlik öz yeterlik, yeterlik, farkındalık ve risk alma eğilimini ve bunları etkileyen unsurları tespit etmeyi amaçlayan çalışmaların olduğu tespit edilmiştir. Ayrıca

dijital güvenlik öz yeterliği ile ilgili üniversite öğrencileri bağlamında yapılmış çalışma da mevcuttur.

Bu çalışma alanyazında varolan çalışmalardan farklı olarak dijital güvenlik öz yeterliği konusunda, hedef kitle açısından ortaokul 7. sınıf öğrencilerine yönelik olmasıyla ve ortaokul öğretim programına uygunluk açısından farklılık göstermektedir. Ayrıca dijital güvenlik öz yeterliğinin geliştirilmesi için bu çalışmada yine farklı olarak MEB SBDÖP ve alanyazın esas alınarak araştırmacı tarafından geliştirilmiş çevrim içi destekleyici öğrenme aracı kullanılmıştır. Bu bakımdan sosyal bilgiler dersinde dijital güvenlik yeterliği için geliştirilmiş olan çevrim içi destekleyici öğrenme aracının öğrencilerin öz yeterliğine etkisinin ortaya konması çalışmaya değer bulunmuştur. Ayrıca bu çalışmanın, dijital güvenlik eğitimi açısından SBDÖP’ndaki dijital vatandaşlık ve dijital güvenlik konusunda benzer kazanımların bulunduğu Bilgisayar ve Öğretim Teknolojileri Eğitimi alanına da katkı sağlayacağı düşünülmektedir.

1.4. Varsayımlar

Bu araştırmada;

- Kontrol altına alınamayan değişkenlerin deney ve kontrol gruplarını seçkisiz atama olmadığından dolayı eşit şekilde etkilediği,
- Araştırmaya katılan öğrencilerin objektif ve içten olduğu varsayılmıştır.

1.5. Sınırlılıklar

Bu araştırma;

- 2021-2022 eğitim- öğretim yılı ile,
- Uygulama boyutunda Ankara ilindeki bir devlet ortaokulunda 7. sınıfta öğrenim görmekte olan 67 öğrenci ile,
- Sosyal Bilgiler Dersi Öğretim Programı ile,
- Dijital güvenlik yeterliği için geliştirilen çevrim içi destekleyici öğrenme aracının kullanıldığı çevrim içi öğrenme ile,

- Araştırmada kullanılan ölçme araçlarına öğrencilerin verdikleri cevaplar ile sınırlıdır.

1.6. Tanımlar

Dijital Güvenlik: Tüm teknoloji kullanıcılarının kişisel güvenliğini ve ağlarının güvenliğini garanti etmek için almaları gereken önlemlerdir (Ribble ve Bailey, 2007, s. 33).

Dijital Güvenlik Yeterliği: Dijital ortamda güvenliğini sağlayabilme sürecinde kullanılacak bilgi, beceri ve tutumlara sahip olma durumudur.

Dijital Güvenlik Öz Yeterliği: Dijital ortamda güvenliğini sağlamak ve kendini korumak için gerekli olan bilgi, beceri ve tutumlara sahip olma konusunda kişinin kendine olan inancıdır.

Öz Yeterlik: Kişinin ileriye dönük durumları yönetmek için ihtiyaç duyduğu hareket biçimlerini planlama ve gerçekleştirme konusunda kendi yeteneklerine olan inancıdır (Bandura, 1977, s.203).

Yeterlik: Bir konuda bilgi, beceri ve uyumlu durumlar arasındaki ilişkilerin birleşimidir (Krasna ve Bratina, 2011, s.1).

Dijital Yeterlik: İnternet ve dijital teknolojiyi eğitimsel ve eleştirel bir yaklaşımla kullanabilmek için farklı dijital cihazları ve yazılımlarını yönetmek ve takip etmektir (Amhag, Hellström ve Stigmar, 2019, s.2).

Dijital Vatandaşlık: Bilgi ve iletişim teknolojilerinin uygun ve sorumlu davranış kuralları (Ribble ve Bailey, 2007, s.10).

BÖLÜM II

KURAMSAL ÇERÇEVE

2.1. Vatandaşlık Kavramı ve Tarihsel Gelişimi

İnsan doğası gereği doğal ve toplumsal ihtiyaçları olan bir varlıktır. Birey tek başına yaşayabilen, kendine yetebilen bir varlık değildir ve varlığını devam ettirebilmesi için doğal ihtiyaçlarından ziyade toplumsal ihtiyaçları gereği diğer insanlara ihtiyaç duymaktadır. Bu sebeple insanlık yaratılışından beri bir arada yaşama ihtiyacı ve arzusunda olmuştur. Böylece günümüz toplumlarının temelleri yavaş yavaş atılmaya başlamıştır.

Toplumu meydana getiren üyeleri bir arada tutan, o insanların aynı olması değil, onların ortak amaç ve yaşam tarzlarıdır. Bu ortak özellikler onları birer vatandaş yapmakta ve bunun sonucunda ortaya bir vatandaşlık kavramı çıkmaktadır. Kısacası toplumun vatandaş kavramına dair tutum ve davranışları o toplumun vatandaşlık kavramına da yansımaktadır (Sönmez, Kaymakçı ve Merey, 2010, s.127). Bu sebeplerle oluşan vatandaşlık kavramı farklı dönemlerde farklı olarak tanımlanmasına rağmen en kabul görmüş anlayışın temelini aidiyetlik duygusu oluşturmuştur. Bu doğrultuda oluşan genel anlayışa göre “*vatandaşlık bir ülkeye karşı aidiyet duygusu ve o ülkenin toplumsal kurallarına ve değerlerine uymaktır*” (Uğurlu, 2011, s.154). Dolayısıyla toplumu ve devletin devamlılığını sağlayan temel unsur orada yaşayan insanların vatandaş ve vatandaşlık kavramına yükledikleri anlamlar ile vatandaşlık aktarımını ne kadar başarılı yaptıklarıdır. Toplumun ve devletin devamlılığı amacından ötürü vatandaşlık anlayışının aktarımı ihtiyaç haline gelmiştir.

Vatandaşlık kavramı ilk çağlardan günümüze dek tüm toplumların gündeminde olmuş ve bütün politik sistemler kendi devamlılıkları için buna ihtiyaç duymuştur (Ekinci, 2016, s. 3).

Yüzyıllardır toplumların öncelikli amaçlarından biri devletin ve toplumun beklentilerini benimsemiş ve bunları karşılamayı ödev edinmiş iyi insan, iyi vatandaş yetiştirmek olmuştur (Hablemitoğlu ve Özmete, 2012, s.41).

Toplumların vatandaşlık anlayışı, başlangıçta düzene uyan davranışlar sergileyen sorumlu vatandaşlar yetiştirmektir (Kan, 2009, s.25). Fakat gün geçtikçe toplumun ihtiyaçları da gelişip şekillendiğinde vatandaşlık anlayışında olduğu gibi vatandaş yetiştirme konusunda da değişimler meydana gelişmiştir. Artık vatandaşlık eğitiminde toplumun ihtiyacı sadece iyi ve uyumlu insan yetiştirmek değildi. Aynı zamanda kendini gerçekleştiren, özsaygısı yüksek, kendinin ve başkalarının potansiyelinin farkında olan, farklılıklara saygı duyan, hak ve sorumluluklarını bilen, yaratıcı, eleştirel düşünebilen yeni teknolojileri aktif ve doğru olarak kullanabilen bireyler yetiştirmektir (Acun, Demir ve Göz, 2010, s.111).

Vatandaşlık kavramı Yunanistan'da Arkaik çağda (M.Ö.776-479) ortaya çıktı (Heater, 2004, s.4). Etimolojik olarak Antik Yunan'daki şehir devletlerini işaret eden vatandaşlık kavramı "*cite*" ya da "*city*" sözünden türetilerek, şehir devletine mensubiyeti belirten "*citizen*" ya da citoyen" kelimesinden doğmuştur (Polat, 2011, s.129). Antik Yunan site devletlerinin vatandaşlık anlayışının temelinde ayrımcı ve katılımcı bir anlayış mevcuttur. Burada ayrımcılıktan olumsuz anlamda etkilenen kesim, köleler, kadınlar ve yabancılar idi. Yani Antik Yunan'da vatandaşlık statüsüne sahip olanlar orada yaşayanlardan sadece reşit olan ve özgür olan erkeklerdir (Erdem, 2012, s.51). Antik Yunan'da vatandaşlar site devletini ilgilendiren konulara aktif olarak katılmak ve askerlik görevini yerine getirme hak ve ödevine sahipti (Heater, 2004). Yunan tarihçi John Myers'e dayanarak Berry şöyle yazıyor: "Eğer bir insanın davranışı ve söylemi politik olmaktan çıkarsa, o zaman o kişi idiot-benmerkezci ve komşusunun ihtiyacından habersizdir (Berry'den aktaran Parker, 2003, s.3). Buradan da anlaşılacağı üzere Antik Yunan'da vatandaşlığın temel gereği politik anlayışlar ve davranışlardan geçmekteydi. Antik Yunan'da vatandaşlığın diğer gerekleri ise kanunları tartışma ve oylama, yöneticileri seçme, vergi vermektir (Erdem, 2012, s.51). Yunan şehir devletinde vatandaşlığı hak etmenin ön koşullarından bazıları da aile reisi olmak, savaşçı olmak, köle sahibi olmaktır (Korkut, 2015, s.6). Tüm bu koşul ve haklara bakıldığında Antik Yunan'da vatandaşlık kavramı kural koyucu, siyasete aktif katılım ve yöneticilik anlayışından oluşmaktadır.

Roma’da ise durum Antik Yunan’ın vatandaşlık kavramına yüklediği anlamdan farklıydı. Antik Yunan Vatandaşlığı bir şehre aidiyet olarak algılarken, Roma vatandaşlık kavramını bu anlayıştan kurtarmıştır. Roma’da vatandaşlık başta Antik Yunan’daki gibi olsa da sonrasında değişmiştir. Bu farklılıktan ilki vatandaşlık artık “şehir aidiyeti” olmaktan çıkmış “yasal statü” haline gelmiştir. Diğer farklılık ise Roma’da vatandaşın oy kullanmayan ve siyasi katılımcı rolü olmayan bir vatandaş olarak görülmesiydi (Korkut, 2015, s.7).

Orta çağda vatandaşlık kavramı, feodalitenin etkisi altında kalmıştır. Öyle ki vatandaşlık Hristiyanlığa hizmet eden bir kavram haline gelmiştir. Orta Çağ’da Dünyevi anlamda doğulan yeri ve bölgeyi ifade eden patria (vatan) kavramı da anlamını yitirmiş (Polat, 2011, s.130) ve vatandaşlık artık kamusal bir hak ve sorumluluktan çıkmış, uhrevi bir boyuta dönüşmüştür. Feodalitenin egemen olduğu Avrupa’da senyör/vassal ilişkilerinde siyasi haklar kullanılmış ve bu dönemde kişi hakları ihlal edilmiştir. Dini değerlerin baskın hale geldiği bu çağda katılım, eşitlik gibi değerler önem kaybetmiştir.

Modern vatandaşlık anlayışının başladığı dönem “aydınlanma” dönemidir. Bu dönemde çağdaş vatandaşlığın temelleri atılmış, insan hak ve özgürlükleri önemsenmeye başlamıştır. Aydınlanma döneminde merkeziyetçiliğe dönüş devlet kavramını tekrardan önemli hale getirmiş ve birey-devlet ilişkisi yeniden güçlenmeye başlamıştır. Böylelikle vatan ve vatandaşlık kavramının değişmesi sağlanmıştır.

Aydınlanma çağının başlaması, özgür bir düşünce ortamının olduğu İtalya’da bazı bilim adamları tarafından başlatılan Rönesans hareketiyle meydana gelmiş ve Rönesans döneminde, yeniden merkezi otoritenin kurulmaya çalışılması sonucunda insanların yönetim süreçlerine dâhil edilmesi ile vatandaşlık anlayışına katılımcılık ilkesi hâkim olmuştur (Smith, 2002, s.105). Bu yönüyle Antik Yunan’daki vatandaşlık anlayışına benzerlik göstermektedir.

Fransız Devrimi ile vatandaşlık kavramı, bir hükümdara tabilik değil, yaşadığı yerdeki diğer insanlarla aynı haklara sahip olan vatandaş anlamı taşımaktadır. Durum birey ve devlet ilişkisinde bir tür sözleşme niteliği taşımaya evrilmiştir. Aslında vatandaşlığa dair liberallik Fransız devriminin katkısıyla oluşmuştur. Bu dönemde vatandaşların sahip olduğu hakların taşıdığı öneme ek olarak Anayasaya bağlılık, mensup olunan etnik bir kökene kıyasla daha değerlidir (Töre, 2017, s.26). Fransız Devriminin vatandaşlık temelinde, hukuk kurallarına uymak, itaatle yükümlü bulunmak, özgür bir düşünce ortamının olması ve düşündüklerini

özgürce ifade edebilmesi, gelir durumuna göre vergi mükellefiyeti sözkonusudur (Erbay, 2009, s.3). Tüm bu bilgiler göz önüne alındığında modern dönemde vatandaşlık kavramına artık bir sınıf olarak bakılmamakta, birey-devlet ilişkisi içinde vatandaşa bir takım hakların tanındığı statü gözüyle bakılmaktadır.

Vatandaşlık kavramının tarihsel gelişiminden de anlaşılacağı üzere bu kavrama dönem dönem farklı anlamlar yüklenmiştir. Bunun sebebi toplumu meydana getiren unsurların zamanla değişim ve gelişime uğramasıdır. Toplumda meydana gelen değişimler etkisini vatandaşlık kavramı üzerinde de göstermiş ve ortaya çok sayıda vatandaşlık yaklaşımı çıkmıştır. Bu vatandaşlık yaklaşımlarına örnek verecek olursak; aktif vatandaşlık, pasif vatandaşlık, sivil vatandaşlık, liberal vatandaşlık, küresel vatandaşlık, çokkültürlü vatandaşlık, anayasal vatandaşlık, avrupa birliği vatandaşlığı ve dijital vatandaşlık gibi ifadeler sıralanabilir.

2.2. Dijital Vatandaşlık

Bu çalışma, belirtilen vatandaşlık perspektiflerinden dijital vatandaşlık ifadesiyle ilintilidir. Dolayısıyla dijital vatandaşlık kavramı üzerine özlü bir açıklama yapılması gerekmektedir. Dijital kavramı Türk Dil Kurumu (TDK) tarafından sıfat niteliğinde “*sayısal*” olarak tanımlanmaktadır. Öte yandan benzer şekilde “Cambridge International Dictionary of English (2022a)” tarafından dijital kelimesi, “*sesleri veya görüntüleri kaydetmek veya göndermek eyleminden önce sayı biçiminde sinyallere dönüştüren elektronik sistem*” olarak tanımlanmıştır. Dijital kavramı “*1 ve 0’ların bir araya gelerek veri dizelerinin anlamlı hale getirilmesi*” demektir (Bozkurt vd. , 2021, s.36). Bu tanımlardan hareketle dijital kelimesi elektronik işlemleri nitelendiren bir kavram olarak ortaya çıkmış ve bilgiyi sayısal yollarla nitелеmek anlamı taşımaktadır. Dijital çağ ise “*birçok şeyin bilgisayar tarafından yapıldığı ve bilgisayar teknolojisi nedeniyle büyük miktarda bilginin mevcut olduğu şimdiki zaman*” olarak tanımlanmıştır (Cambridge International Dictionary of English, 2022b).

Dijital çağ olarak adlandırılan günümüzde bilgi, dijital ortam sayesinde hızlı bir şekilde yayılıp çoğalmaktadır. İnsanlar bilgiye, bilgi ve iletişim teknolojileri olarak adlandırılan bilgisayar, akıllı telefon, tablet ve internet gibi araçlar aracılığıyla dijital ortamda erişmektedir. Bilgi ve iletişim teknolojilerinin erişim ve dağıtım hızı gibi avantajları ise

insanların dijital ortamı tercih etmesine olanak vermektedir. Bu sayede dijital bir toplum oluşmaktadır.

Dijital toplumun genişleme hızı her yıl yenilenen oranlarla raporlaştıran ve sunan kurumlar aracılığıyla sayısal olarak da bilinmektedir (We Are Social ve Hootsuite, 2022a; TÜİK, 2022). Dijital toplumun hızla büyümesi hem dünyada hem de ülkemizde görülmektedir. Böylece genişleyen dijital topluma vatandaşlar olarak katılım sağlamak artık tercih olmaktan çıkmış, bir zorunluluk haline dönüşmüştür. Bununla birlikte geçmişte sınırlı bir bilgi kaynağına sahip vatandaşlık mevcutken, bilgi ve iletişim teknolojilerinin gelişmesi daha fazla kaynağa ulaşmayı ve e-vatandaşlık işlerini kullanmayı önemli kılmış, bunları yapabilen vatandaş yetiştirmeyi de zorunlu kılarak vatandaşlık eğitimini de şekillendirmiştir. Bu sebeple dijital vatandaşlık kavramı günümüzde incelenmesi gereken alanlar arasında yerini almıştır.

Dijital vatandaşlık Ribble (2011) tarafından “*bilgi ve iletişim teknolojilerini uygun ve sorumlu kullanım kuralları*” olarak tanımlanmaktadır (s.10). Yani dijital vatandaşlık teknoloji için çeşitli sorumluluk düzeylerinden bahsetmektedir (Ribble vd., 2004, s.7). Hobbs ve Jensen (2009) ise dijital vatandaşlığı “*sosyal medyada gerekli olan bilgi ve beceriler topluluğu*” olarak ifade etmiştir (s.5). Daha geniş bir bakış açısıyla “*dijital vatandaşlık, bilgi ve iletişim teknolojilerinin uygun, sorumlu ve etik bir şekilde kullanım normlarının dijital ortamda uygulanmasıdır*” (The International Society for Technology in Education [ISTE], 2007) cümlesiyle tanımlanmaktadır.

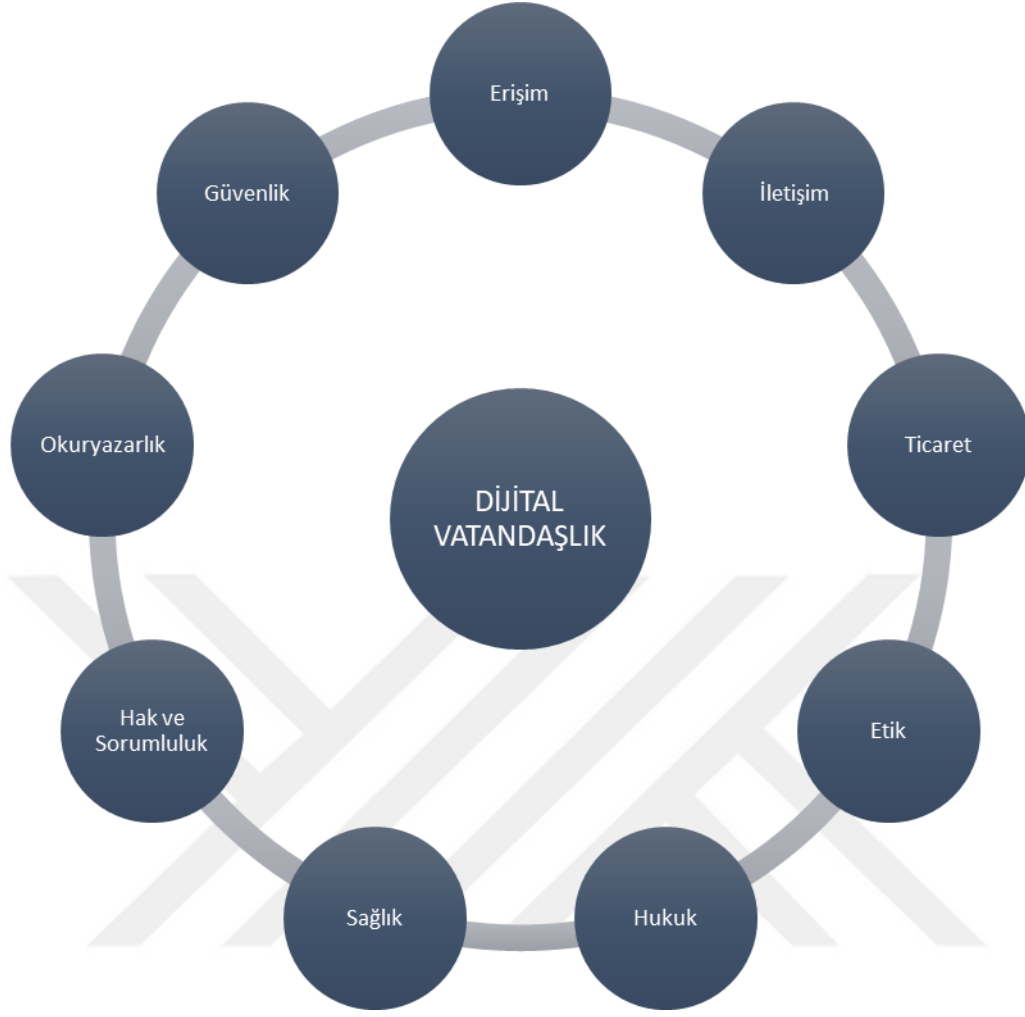
Dijital vatandaşlık teknolojiyi sadece etkin kullanmak, doğru anlamak demek değildir. Aslında dijital vatandaşlık bir ya da iki boyut ya da bakış açısıyla sınırlandırılmaz. Dijital vatandaşlık için pek çok unsur, pek çok beceri, pek çok platform ve dijital araç söz konusudur. Örneğin, dijital vatandaş olabilmek için kullanıcıların bilgi ve iletişim teknolojilerini kullanırken pek çok beceriyi işe koşması gerekmektedir. Dijital vatandaşlık düzenli ve etkili internet erişimi ve teknolojiyi kullanabilmenin dışında, dijital ortamlarda karşısına çıkabilecek bilgileri değerlendirebilmek ve kendi sınırlarını çizebilmesi adına teknik beceriler, eleştirel düşünme becerisi, krizi yönetme becerisi, ihtiyaçları doğrultusunda hareket edebilme becerilerini de gerektirir (Mossberger, Tolbert ve Hamilton, 2012, s.2493). Bununla birlikte dijital vatandaşlık mevcut teknoloji ve sosyal medya kullanımı ile ilgili birçok beceri gerektirir ve bu beceriler uygun, sorumlu ve sağlıklı davranış normlarını içerir

(Common Sense Kids Action, 2017, s. 13). Buna göre dijital vatandaş nedir ve nasıl olunur sorusu önemlidir.

A Common Sense Media'a (2017) göre dijital vatandaşlığın başlıca alanları olarak güvenlik ve okuryazarlık becerilerinin geliştirilmesi gerektiği ifade edilmektedir ve bu eğitimin 21. yüzyıl dijital teknoloji becerileri ile verilmesi gerektiğini ifade etmektedir. ISTE (2007), ise dijital vatandaşlığın yapılmaması gerekenler konusunda uzun bir liste olmaması gerektiğini, bununla birlikte etik sorunlarla mücadele edebilecek empati becerisine sahip dijital vatandaşlar yetiştirilmesi gerektiğini ifade etmektedir. ISTE (2007) yapılması gerekenler arasında teknolojiyi kullanmak, çevrim içi ortamda diğer vatandaşlara karşı saygılı davranmak, fikirlerini duyurmak için teknolojiyi kullanmak, olumlu ve etkili bir dijital ayak izi bırakırken olasılıkları ve fırsatları görmenin olması gerektiğini ifade ederek dijital vatandaşlığın çevrim içi güvenlikten çok daha fazlası demek olduğunu belirtmiştir. Tüm bu ifadelerden yola çıkarak dijital vatandaşlık kavramı karmaşık bir yapıdır ve bu yapı tek bir beceri ile veya tek yönlü bir bakış açısı ile çözümlenemez yapıdadır.

Ribble vd., (2004) dijital vatandaşlığın karmaşık yapısını ve teknolojinin doğru kullanımını ve de dijital ortamın kötüye kullanımı ile ilgili konuları anlamının yolunun öncelikle dijital vatandaşlığın alt boyutlarından geçtiğini ifade etmektedir (s.7). Bu sayede gerçekten iyi bir dijital vatandaş olmanın yolu açılabilir. Ribble ve Bailey (2007) dijital dünyayı anlamak için dijital vatandaşlığın alt unsurlarından bahsetmektedir (s.10). Bu boyutlar dijital etik, dijital ticaret, dijital sağlık, dijital okuryazarlık, dijital erişim, dijital hak ve sorumluluk, dijital hukuk, dijital iletişim ve dijital güvenlik şeklinde belirtilmiştir.

Dijital vatandaşlığın alt boyutları Şekil 1'de gösterilmiştir.



Şekil 1. Dijital vatandaşlık alt boyutları

2.2.1. Dijital Vatandaşlığın Alt Boyutları

2.2.1.1. Dijital Erişim

Ribble ve Bailey (2007) dijital erişimi “*toplumda tam elektronik katılım*” olarak tanımlamıştır (s.14). Dijital toplumun üyeleri artık bilgiye erişim için fiziki ortamlardan daha çok dijital cihazlar aracılığıyla internetten bilgiye erişimi tercih etmektedir. Bilgi ve iletişim teknolojilerinin bilgiye hızlı erişim avantajı bu teknolojilerin yaygın kullanımını da artırmıştır. Ayrıca teknoloji internet sayesinde aynı anda birden fazla kişinin etkileşim kurmasına da olanak sağlar. Fakat vatandaşların teknolojinin faydalarından yararlanma konusunda aynı derecede fırsat eşitliğine sahip değildir ve bu fırsat eşitsizliğine sebep olan

birçok faktör vardır. Ribble ve Bailey (2007) dijital erişim için fırsat eşitliğinde etken faktörler arasında sosyoekonomik düzey, fiziksel konum, anında erişim imkânı, kullanımları için tasarlanmış özel araçlara yeterli erişime sahip olmayan özel ihtiyaçları olan vatandaşlar ve yüksek hızlı internet imkânının olduğunu belirtmiştir(s.14-15). Bununla birlikte Ribble ve Bailey (2007) dijital erişim açısından erişim eksikliği kişilerin haklarından mahrum kalmasına sebep olabileceğini ifade ederek bu duruma örnekler vermiştir; “*evde teknolojiye sahip olmak için finansal durumu olmayan aileler, öğrenciler için yeterli bilgisayara sahip olmayan okul bölgeleri, yüksek hızlı internet bağlantılarına erişimi olmayan kırsal bölgeler veya erişime gün boyunca sahip olmayıp kısıtlı vakitlerde erişim imkanı bulabilenler*” (s.15). Fırsat eşitsizliği konusunda açığı gidermek için de eğitim kurumlarının telafi edebilecek imkanlar sunması gerekmektedir. Örneğin, okul saatleri içerisinde herkese açık teknoloji laboratuvarlarının olması bu durum için telafi yöntemi olabilir.

Dijital vatandaşlığın erişim boyutunda özellikle okullarda uygun olmayan yaklaşımlar bulunabilmektedir. Örneğin, okul erişim imkanı olmayan kişilerin problemini yok sayarsa ve çözüm üretmeye çalışmazsa dijital erişim konusunda fırsat eşitsizliği büyüyerek dijital vatandaşlık eğitimini zorlaştırabilir. Bu konuda uygun olan yaklaşım ise teknoloji fırsatları yaratmaktır.

2.2.1.2. Dijital İletişim

Ribble vd., (2004) dijital iletişimi “*elektronik bilgi alışverişi*” olarak tanımlamıştır (s.7). Günümüzde dijital cihaz ve iletişim araçlarının çoğalmasıyla birlikte elektronik bilgi alışverişi hızlanmıştır. Cep telefonları, anlık mesajlaşma ve e-posta, aynı zamanda teknoloji kullanıcılarının iletişim kurma şeklini de değiştirmiş ve bu iletişim biçimleri insanların kimle, nasıl ve ne zaman etkileşime girdiğine dair yeni bir sosyal alt yapı oluşturmuştur (Ribble vd., 2004, s.7-8). Dijital ortamda iletişimin büyük bir bölümünün internet teknolojisiyle çevrim içi ortamda ve özellikle sosyal ağları kullanarak yapılması internette çeşitli temas riskleriyle karşı karşıya kalılabileceğini göstermektedir (Çubukçu ve Bayzan, 2013, s.6). Ülkemizde oluşan bu yeni sosyal alt yapının giderek popülerleşmesi gençleri bu riskler ile daha sık karşı karşıya getirmektedir. Lenhart vd., (2011) dijital iletişimin Amerika’da da özellikle gençler arasında sosyal medyada giderek artmakta olduğunu belirtmiştir ve gençlerin günlük olarak sosyal ağlara girdiğini ve sıklıkla zorbalığa maruz

kaldığını ifade etmektedir (s.16) ve benzer risklerin diğer ülkelerde de varolduğu çeşitli araştırmalar aracılığıyla ifade edilmektedir.

Dijital iletişimde önemli diğer bir husus ise dijital ortamın kaydetme ya da veri yedekleme özelliğidir. Bu özellik dijital ortamda iletişim kurarken kişilerin çok dikkatli olmasını gerektirmektedir. Ribble ve Bailey (2007), dijital iletişim sırasında kişilerin uygun kullanım kurallarına dikkat edilmesi gerektiğini aksi halde farklı kişiler tarafından farklı şekilde algılanmalar yüzünden kişilerin sıkıntılı durumlar içerisine girebileceğini ifade etmektedir (s.19). Bununla birlikte dijital teknolojiler aracılığıyla okulda iletişim kurmak dikkat dağıtmaktadır ve davranışsal bozukluklara sebep olabilmektedir. Bu durumda dijital iletişim sırasında kullanılan araçların kullanım şekli ve sıklığı, araçların bildirim seslerine kadar birçok konuyu içine almaktadır. Bununla birlikte anlık mesajlaşmalar bu durumun sıklıkla yaşanmasına sebep olabilmektedir. Bu noktada dijital iletişim araçlarının uygun kullanım davranışlarının vatandaşlar tarafından benimsenmesinin gerekliliği öne çıkmaktadır. Kısacası dijital iletişim sırasında uygunsuz kullanımlar ve davranış tarzlarından kaynaklı risklerden korunmanın yolu dijital iletişim eğitiminden geçmektedir ve bu sebeple günümüzde dijital iletişim eğitiminin önemini artırmaktadır.

2.2.1.3. Dijital Ticaret

Ribble ve Bailey (2007), dijital ticareti “*çevrim içi mal satın alma ve satma*” olarak tanımlamıştır (s.16). Bilinçli bir tüketici olmak, çevrim içi alışverişi güvenli bir şekilde yapabilmek dijital vatandaş olmak açısından önemli bir boyuttur. Örneğin, çevrim içi alışveriş sırasında malları nasıl ve nereden satın alacağını bilmemek, kaliteli ve doğru hizmet alabilmek için gerekli araştırma becerisine sahip olmamak, internet dolandırıcılığına ve kimlik hırsızlığına karşı bizleri savunmasız bırakabilir. Bu sebeple öğretmenler öğrencileri hayatlarının geri kalanına hazırlamak için, dijital ticareti ele almalıdır (Ribble ve Bailey, 2007, s.17). Dijital ticaret eğitiminin önemini ortaya koyan bir durum, e-ticaret hacminin son yıllarda fazlasıyla artmasıdır. Ticaret bakanlığının e-ticaret verilerine göre pandemiyle birlikte e-ticaret hacmi 2020’nin sadece ilk altı ayında %64 artmış, bu oran 2021 yılında %69’a ulaşarak e-ticaret hacmini 381,5 milyar TL’ye ulaştırmıştır (Elektronik Ticaret Bilgi Platformu, 2021). Önemli olan konu ise e-ticaret oranındaki bu artış hızı aynı zamanda kişilerin çevrim içi alışveriş becerilerinin gelişiminde de yaşanması noktasıdır. Diğer bir

önemli husus ise e-ticaret ya da çevrim içi alışverişi sadece yetişkinler tarafından mı yapılıyor olmasıdır. Bu konuda TÜİK (2021) verilerine göre 9-15 yaş grubu çocuk katılımcılardan düzenli internet kullanan çocukların internet kullanım amaçları arasında %9,1 oranında çevrim içi alışveriş yapma davranışını gerçekleştirdiği belirtilmektedir. Ayrıca EU Kids Online (2020) raporunda katılımcı çocuklar arasında düşük oranda da olsa çevrim içi ortamda para kaybedenlerin olduğu vurgulanmıştır. Bu durum çocukların çevrim içi olarak kullanabileceği bir maddi imkanın verildiği anlamına da gelmektedir. Bu sebeple dijital ticaret eğitiminin hem yetişkinlere hem de okulda öğrencilere verilmesi gerekmektedir.

Ribble ve Bailey'e (2007) göre dijital ticaretin eğitimciler bakımından sınıfta konuşmak için dijital vatandaşlık unsurları arasında en zor unsur olduğunu belirtmiştir (s.16). Bu eğitim hem dikkatli bir tüketici olmaları konusunda hem de ileride çevrim içi alışveriş yapacakları sırada güvenli yolları seçmeleri adına önemlidir. Bununla birlikte akıllı bir tüketici olmanın iyi bir vatandaş olmak için önemli bir yön olduğunu ve çocukların çevrim içi alışveriş yapma oranlarının nadiren olmadığını ve bu durumun eğer dikkatli bir tüketici değilse çevrim içi dolandırıcılığa ve kimlik hırsızlığına maruz kalılabileceği belirtilmektedir. Bu açıdan hem iyi bir dijital vatandaş olmak ve de bilinçli bir tüketici olmak, hem de çevrim içi dolandırıcılığa ve kimlik hırsızlığına maruz kalmamak için dijital ticaret eğitiminin vatandaşlara özellikle de okullarda çocuk yaşta verilmesi gerekmektedir.

2.2.1.4. Dijital Etik

Ribble ve Bailey (2007) dijital etiği *“diğer dijital teknoloji kullanıcıları tarafından beklenen davranış standartları”* olarak tanımlamıştır (s.24). Özcan (2021) ise dijital etiği şöyle tanımlamıştır; *“teknoloji ile gelişen mecralarda başkalarına zarar vermemek ve bu platformlarda gerçekleştirilen her türlü insan eylemi esnasında sistemin iyi niyetle devamını sağlamak için doğru davranışı teşvik eden kurallar”* (s.93). Yapılan tanımlardan hareketle dijital etik ile dijital ortamda varolan kişilerin birbirlerine karşı saygılı davranışları ve bir ahlak sistemi oluşturma amaçlandığı söylenebilir.

Günümüzde dijital ortamda varolmuş bir takım iletişim şekilleri bulunmaktadır. Fakat bu iletişim içerisinde her davranış etiğe uygun değildir. Elçi ve Sarı (2016)dijital etiğe aykırı

davranışlar arasında yasa dışı paylaşımlar, diğer kullanıcıları küçük düşürücü söylemler gibi durumların var olduğunu ifade etmiştir (s.89). Bu durum dijital ortamda benimsenen davranışların etik açıdan sorgulanması gerektiğini göstermektedir.

Dijital ortamda benimsenen davranışlar yalnızca bizi değil diğer kullanıcıları da etkileyebilir. Maalesef dijital teknolojileri kullanırken, beklenen davranış standartları ihlal edilmekte ve böylece diğer kullanıcıları rahatsız edici durumlar ortaya çıkabilmektedir. Üstelik bu durum diğerleri tarafından tolere edilebiliyor ve uygunsuz davranışlar artıp tahammül sınırlarını zorlayabilir veya istemediğimiz durumlarla karşı karşıya bırakabilir. Örneğin toplantılarda, iş görüşmelerinde anlık mesajlaşma, cep telefonumuzun zil sesinin açık olması ve dikkat dağıtması, diğer insanlarla iletişim sırasında cep telefonlarımızla ilgilenmemiz vs. durumlar dijital etiğe aykırı durumlardandır. Bu durum okullar için de geçerlidir ve okullarda dijital etik eğitimin verilmesi gerekmektedir. Örneğin dijital etik eğitiminde öğretmenler günlük hayattaki etik kavramlarına paralel bir eğitim verebilir ve bunu rehberlik yaparak başarabilir (Görmez, 2016, s.131). Ribble ve Bailey (2007)’e göre ise dijital etik eğitiminde teknoloji liderleri, öğretmen ve öğrenciler için sağlam bir örnek sunmalıdır ve örneklerle uygun olarak öğretmen ve öğrenciler, ders sırasında kendi elektronik ekipmanlarını susturmak veya kapatmak zorunda kalmalıdır, dijital oyun oynamamalıdır veya anlık mesajlaşma kullanmamalıdır (s.13). Böylece dijital etik konusunda okulda gündelik hayata örnek oluşturabilecek davranışlar benimsetilebilir.

2.2.1.5. Dijital Hukuk

Ribble ve Bailey (2007) dijital hukuku “*bilgi ve iletişim teknolojilerinin kullanımını düzenleyen hukuki kurallar*” olarak tanımlamıştır (s.26). Dijital hukuk, kişinin teknolojiyi kullanımı sırasında bir takım hatalar yapabileceğini ve suç işleyerek yasalarla karşı karşıya kalabileceğinden bahsetmektedir. Dijital kullanım hataları bilerek ya da bilmeyerek günümüzde pek çok kullanıcı tarafından gerçekleştirilebilmektedir ve bunun birçok örneği vardır. Çubukçu ve Bayzan (2013)’a göre dijital vatandaşların gerçek hayattaki suç niteliği taşıyan davranışların dijital ortamda da aynı kategoride olacağını bilerek davranması gerekmektedir ve benzeri durumlarla karşılaştığında da şikayet etmenin sorumluluk kapsamında olduğunu bilmelidir (s.157). Bu durum aslında dijital hukuk boyutunun gerçek

yaşam ile paralel olduğunu belirtmektedir. Gerçek yaşam ile kopuk ve internette herşeyi yapabileceğine dair inançlar dijital ortamda hukuki boyutta risk alanları oluşturabilmektedir.

Ribble ve Bailey (2007) dijital hukukun başlıca sorunlarını, *“dosya paylaşım sitelerini kullanma ve bu sitelerden telifsiz ürünleri atıfta bulunmadan kopyalamak veya adil kullanım kotasına aykırı davranmak, korsan yazılım kullanmak, dijital haklar yönetimi teknolojilerinin altüst edilmesi, sistemleri veya ağları hacklemek, birinin kimliğini çalmak”* olarak belirtmektedir (s.26). Özellikle gençler teknoloji kullanım haklarını ve kısıtlamalarını bilmiyor olabilir. Üstelik çevrim içi ortamda bu hataların bir kısmını yapmak çok kolaydır. Kopyala ve yapıştır adımları bunun için yeterlidir. Proje, ödev ve sunum hazırlamak için veya çevrim içi gönderi paylaşımı yaparken arama motorlarında karşısına çıkan materyalleri izinsiz bir şekilde ve sınırsız kullanabilmektedirler. Bu durumu önlemek amacıyla seçilen materyallerin telifsiz olduğuna emin olunmalı veya adil kullanım kotasına uygun şekilde hareket edilmelidir. Öte yandan kimlik hırsızlığı, hacklemek gibi diğer sorunlar ciddi düzeyde bilişim yeteneği gerektirebilir ve bilişim yeteneğine sahip olmayan vatandaşlarımız bu risklere karşı savunmasız kalabilir. Dijital hukukun sorunlarını azaltmak için özellikle yeni yasal düzenlemelerden haberdar olmayan gençleri öğretmenler uyarmalı ve bilgilendirmelidir.

2.2.1.6. Dijital Sağlık

Ribble ve Bailey (2007) dijital sağlığı *“bilgi ve iletişim teknolojilerinin kullanımı sırasında kişinin sağlığına zarar vermemesi”* olarak tanımlamıştır (s.31). Dijital vatandaşlar dijital ortamda tehditler ve riskler ile karşı karşıya kalmaktadır (Stoilova vd., 2021) ve bu durum özellikle çocuk yaş grubunu fazlaca etkilemektedir (Livingstone vd. , 2017). Bu riskler arasında dijital ortamın sağlıksız bir şekilde kullanımından kaynaklı riskler mevcuttur. Vally, Laconi ve Kaliszewska-Czeremska (2020), dijital ortamın sağlıksız bir şekilde kullanımından kaynaklı risklerin sağlığı tehdit ettiğini vurgulamaktadır (s.588).

Dijital ortamın sağlıksız kullanımını Nannatt vd. (2022) sağlıksız, patolojik internet kullanımı olarak ifade etmektedir (s.341). Dijital ortamın sağlıksız kullanımında söz konusu davranışlar dijital araç ve interneti aşırı kullanım (Nannatt vd., 2022, s.341), fiziksel olarak uygun olmayan şekillerde kullanım (Muslu ve Bolışık, 2009, s.446), aşırı içerik tüketimi,

aşırı sosyal medya kullanımı ve zararlı içerik kullanımıdır (Vally vd., 2020, s.588). Bu aşırı, zararlı ve uygun olmayan kullanımlar sağlık bakımından risk teşkil etmektedir. Dolayısıyla kişilerde bir takım fiziksel rahatsızlıklara sebep olabilmektedir ve yaygın olarak görülenler arasında baş, boyun, bilek, el ile ilgili problemlerin yanı sıra, görme problemi ve kilo artışı gibi problemler de yaratabilmektedir (Güvenli Web, 2017). Güvenli Web (2017), bununla birlikte sağlıksız dijital kullanımların psikolojik sorunlara da yol açabileceği belirtmiş ve sıklıkla görülen rahatsızlıklar arasında kaygı bozukluğu, asosyallik, depresiflik, ekran bağımlılığı gibi rahatsızlıklar da belirtilmiştir.

Bunların haricinde günümüzde yaygın olarak görülen ve dijital sağlıkla ilişkilendirilen risk ise internette sağlık bilgilerini araştırma ve kendine tanı koymaktır. Bu durum aslında bir nevi dijital ortam dezenformasyonudur. Günümüzde bu hastalığa siberhondri denilmektedir. Batu ve Güler İplikçi (2021), siberhondrikleri şu şekilde tanımlamıştır; *“sahip olduğunu düşündükleri rahatsızlık hakkında dijital ortamda herhangi bir enformasyon, çözüm veya tedavi yöntemlerine bakarak kendilerine tanı koymaya çalışanlar”* (s.642). Batu ve Güler İplikçi (2021), dijital ortamın aşırı kullanımından kaynaklı ek olarak nomofobi (dijital cihaz bağımlılığı), ego sörfü (arama motorunda kendini sıklıkla arama), google takibi (arama motorlarında başkalarını sıklıkla takip), crackberry (her ortamda telefon kontrolü), cheesepodding (sürekli içerik ve mp3 indirme), blog ifşacılığı (sürekli faydalı bilgi yayımlama) gibi rahatsızlıkların da mevcut olduğunu ifade etmiştir (s.645-647). Bu bilgilerden hareketle dijital araç ve interneti kullanan bireylerde bu risklere karşı bilinç ve farkındalık oluşturmak güvenlik açısından dijital sağlık boyutunda önemlidir.

2.2.1.7. Dijital Hak ve Sorumluluklar

Dijital hak ve sorumlulukları Ribble ve Bailey (2007) *“dijital kullanıcıların sahip olduğu hak ve diğer kullanıcılara karşı duyması istenen sorumluluklar”* olarak tanımlamıştır (s.29). Ribble (2011), dijital hak ve sorumluluğun ihtiyaç ve özgürlük olduğunu ifade etmiştir (s.35). Çatlı ve Keskin (2021) ise dijital hak ve sorumluluğu *“dijital platformu kullanan bireylerin hukukun sınırları içerisinde bu platformdan yararlanma ve kullanmaya yetkilerinin olması ile bu dijital faaliyetlerinin sonuçlarına katlanması ve hesabını verebilmesi”* olarak tanımlamıştır (s.217). Buradan hareketle dijital ortamda gerçek hayatta hukuk çerçevesinde davranmak ve başkalarının sahip olduğu haklara karşı saygılı olma

sorumluluğu bulunmaktadır. Her toplumun kuralları ve vatandaşlarının hakları olduğu gibi dijital toplumun üyelerinin de bazı hakları ve diğerlerine karşı sorumlu olduğu durumlar vardır. Toplum düzeni ve huzuru için temel hak ve sorumlulukların varlığı günümüz dünyasında gerekli kılınmıştır. Dijital vatandaşların dijital ortamda hak ve sorumlulukları konusunda farkındalık düzeyi önemli bir konudur. Çünkü farkındalık düzeyi ne kadar yüksek olursa diğer kullanıcıların hakları konusunda empati kurma becerisi de gelişecektir.

Dijital vatandaşlar haklarının farkında olduğu kadar başkalarının da haklarının farkında olmalı, bu hakların ihlali söz konusu olduğunda yasaların ve dijital toplumun yaptırımları ile karşı karşıya kalacağını ve dijital ortamda özgürlüğünün sınırsız olmadığını bilmelidir.

Bayzan (2019), dijital hakları şöyle sıralamıştır;

1. Özel hayatın gizliliğinin korunması,
2. Kişilik haklarının ihlal edilmemesi,
3. Kişisel verilerin korunması,
4. İnternette düşüncenin ifade edilmesi,
5. İnternet yoluyla yönetime katılma,
6. İnternet üzerinden şikayet hakkı,
7. İnternette lekelenmeme hakkı.

Çatlı ve Keskin (2021) dijital sorumlulukları ise şöyle sıralamıştır;

1. Suç sayılabilecek uygunsuz durumları şikayet,
2. Bilimsel etiğe uygun davranma ve intihal yapmama,
3. Telif ve patent haklarına karşı saygılı kullanımlar,
4. Başkalarına ait verileri izinsiz kullanmama ve yayınlamama (s.218).

Bunlara ek olarak uygunsuz kullanımların şikayet edileceği mecraları bilme ve değerlere saygılı davranma gibi sorumluluklar dijital sorumluluklarımız arasındadır.

2.2.1.8. Dijital Okuryazarlık

Ribble ve Bailey (2007) “*Dijital teknolojiyi kullanma yeteneği ve ne zaman, nasıl kullanılacağını bilmek*” olarak tanımlamıştır (s.21). Ribble (2011) buna ek olarak dijital okuryazarlığın dijital vatandaşlığın en önemli boyutlarından biri olduğunu ve teknolojiyi

anlamanın önemli bir konu olduğunu ifade etmektedir (s.27). Tyger (2011) ise dijital okuryazarlığın, internet erişimi ve dijital araç kullanımı için gerekli bilgi ve beceriden çok daha fazlası olduğunu belirtmektedir (s.17).

Hamutoğlu, Güngören, Uyanık ve Erdoğan (2017)'a göre dijital okuryazarlıkta olması gereken beceriler arasında bilginin doğruluğunu ayırt etme ve doğru bilgiye erişim, internette doğru olan bilgileri paylaşma, teknolojiyi öğrenme amaçlı kullanabilme ve farklı teknolojileri doğru bir şekilde kullanabilme becerileri olmalıdır (s.411).

Dijital okuryazarlık Gilster (1997)'a göre 3 ilkeye dayanmalıdır; donanım ve yazılımlara erişim ve kullanma becerisi; içerikleri anlamak ve eleştirel yaklaşım; içerik oluşturma becerisi (Gilster'dan aktaran Onursoy, 2018, s. 993). Bu bilgilere göre dijital okuryazarlığın bilişsel ağırlıklı bir süreç olduğu söylenebilir. Dijital vatandaşlık için ilk ve önemli adımlardan biri olarak görülen dijital okuryazarlık düzeyinin yükseltilmesi gerekir çünkü okuryazarlık çeşitli risklerle bağlantılıdır. Kozan ve Bulut Özek'e (2019) göre dijital okuryazarlık ile dijital zorbalığa maruz kalma arasında anlamlı bir ilişki bulunmaktadır (s.119). Ayrıca ödev yaparken, proje hazırlarken, araştırma yaparken karşılarına çıkan içerikleri seçme ve kullanma aşamasında zararlı ve yanlış bilgilere maruz kalabilir veya sosyal medyada çevrim içi iken dijital ortamın ve dijital medyanın etkisinde kalabilir. Öğrenciler dijital araçları kullanırken çeşitli kullanım yollarını araştırmaz ve dijital aracı ne zaman kullanacaklarına dair değerlendirmeler yapamazsa, kendilerini dijital vatandaşlar olarak yetersiz hissedebilirler (Snyder, 2016, s.49). Bu bağlamda dijital kullanıcıların dijital okuryazarlık becerilerinin üst düzeye gelmesi gerekmektedir.

2.2.1.9. Dijital Güvenlik

Dijital güvenlik alt boyutunu Ribble ve Bailey (2007) *“tüm dijital kullanıcılarının kişisel güvenliğini ve ağlarının güvenliğini koruması için önlemler topluluğu”* olarak tanımlamıştır (s.33). Snyder (2016) dijital güvenliğin, dijital vatandaşlığın boyutları arasında en popüler boyut olduğunu ve şemsiye niteliği taşıdığını ifade etmiştir (s.96).

Dijital güvenliğin şemsiye niteliği taşıma sebebi diğer boyutlarda karşımıza çıkabilecek risklere karşı mücadele yöntemlerini içermesi olabilir. Ayrıca güvenliğin önemini artıran

diğer bir etken ise kişinin güvenliğidir ve kişisel güvenlik için diğer dijital kullanıcılara güvenmek bir çözüm değildir.

Dijital güvenliğin kapsamı günümüzde dijital araçların, platformların ve internetin çeşitlenmesi sebebiyle genişlemiştir. Bu bağlamda teknik açıdan kişisel güvenliğı sağlamak önemli bir boyuttur fakat yeterli değildir. Çünkü günümüzde dijital ortamlardaki uygunsuz ve bilinçsiz davranışlar ve sosyal ağlarda şahsına ait bilgileri açık etmek sadece teknik boyutla ilgili değildir. Örneğın, dijital güvenliğın psikososyal ve sağık boyutu sanal ataklardan çok daha fazla etki yaratmaktadır. Bu bağlamda Snyder (2016)'ın *“siber zorbalık, literatürde bulunan ve öğrencileri aşırı yönde etkileme potansiyeline sahip olan bir başka dijital güvenlik sorununun”* olduğunu belirtmesi (s.97) bu ifadeyi desteklemektedir. Bu bağlamda dijital güvenliğe geniş bir perspektiften bakmak yerinde olacaktır.

2.3. Dijital Teknolojiler, Dijital Dönüşüm ve Dijital Güvenlik

Dijital araçların ve internetin giderek artan avantajları tercih edilebilirliğinin artmasına paralel olarak kullanıcı sayısını da artırmaktadır. Geçtiğimiz yıllarda dijital teknolojilerin kullanıcı sayısındaki artışın üzerine Covid-19 salgınından kaynaklı pandemi sürecinin yaşanması, daha da hızlanmasına sebep olmuş ve dijital dönüşümü hızlandırmıştır. Yaşam şartlarının ve alışkanlıkların üzerinde büyük etkisi görülen pandemi süreci ile insanlar işlerini, ihtiyaçlarını, iletişimlerini, sosyalleşme ihtiyaçlarını evden dijital teknolojiler aracılığıyla gerçekleştirmiştir. Dijital teknolojilerin ve internetin kullanımında yaşanan dönüşümler ve değişimlere Dünya’da ve Türkiye’de yapılan araştırmalar aracılığıyla ulaşılmaktadır (Bkz. CIA World Factbook, 2022; Committed to Connecting The World [ITU], 2021; Internet World Stats, 2022; TÜİK, 2022; We Are Social ve Hootsuite, 2022).

We Are Social ve Hootsuite’ ın işbirliği yaparak oluşturduğu “Dijital 2022” raporuna göre dünyanın toplamda 7,98 milyarlık toplam nüfusunun %66,9’luk oranı (5,43 milyar) mobil telefon kullanmakta, toplam nüfusun %63,1’i (5,03 milyar) internet kullanıcısı, toplam nüfusun %59,0’u (4,70 milyar) aktif sosyal medya kullanıcısıdır (We are Social ve Hootsuite, 2022a). Dünya çapında diğer kaynakların yayınladığı internet kullanımlarına bakıldığında, ITU (2022) dünyada 5.3 milyar kişinin internet kullanıcısı olduğunu, CIA World Factbook Verisi (2022) dünya nüfusunun %63,0’ünün, Internet World Stats Verisi

(2022) dünya nüfusunun %69'unun internet kullanıcısı olduğunu belirtmektedir. Türkiye'de ise bu durum biraz daha fazla olup, toplam nüfusun %82,0'sinin internet kullandığı görülmektedir (We Are Social ve Hootsuite, 2022b). Tüm bu araştırma sonuçlarına göre Dünya'da ve Türkiye'de internet ve dijital cihazların kullanım oranının oldukça yüksek olduğu söylenebilir.

We Are Social ve Hootsuite'in "Dijital Türkiye 2022" raporuna göre dijital cihazların kullanımı kendi içinde farklılık göstermekte ve bu rapora göre web trafiğinin herhangi bir cihaz üzerindeki payı şu şekildedir; Trafiğin %54,56'sı mobil telefon ile, %2,52'si tablet ile, %46,83'ü bilgisayar ile, kalan %0,10'u ise diğer cihazlar (oyun konsolu vb.) ile meydana gelmektedir. Yine bu rapora göre internetin kullanma nedenleri sırasıyla; bilgi bulmak, yakınlarla iletişim, haber ve etkinlikleri takip, bir şeyler izleme, araştırma yapmak, yeni fikirler aramak, ürün ve marka takibi, müzik dinleme, boş zaman geçirme, eğitim, turizm ve seyahat, sağlık, finans, oyun, işletme ve insanlarla tanışmaktır. Bu gibi nedenler dolayısıyla dünyada en çok ziyaret edilen ilk beş web sitesi; google.com, youtube.com, facebook.com, wikipedia.com, amazon.com siteleridir.

Türkiye genelinde dijital konularda araştırmalar yapan TÜİK (2022)'in, "Hane halkı bilişim teknolojileri kullanım araştırması" raporuna göre toplam nüfusa oranla evde internet erişimi olan hane oranının %94,1 olduğu tespit edilmiştir. Bu tespite göre; internet kullanan bireylerin toplam nüfusa oranla %85 olduğu, internet kullanan bireylerin %82,7'sinin düzenli internet kullanıcısı olduğu, internet kullanan bireylerde çevrim içi alışveriş yapma oranının %46,2 olduğu, en fazla kullanılan dijital içeriğin %26,4 ile dizi ve film izleme içerikleri olduğu ifade edilmektedir.

Dünya çapında internet kullanımıyla ilgili yapılmış araştırmalardan bir diğeri ise Statista'dır (2022). Bu araştırma raporuna göre Temmuz 2022 itibariyle dünya nüfusunun %63,1'inin aktif internet kullanıcısı olduğu, yine dünya nüfusunun %59'unun sosyal medya kullanıcısı olduğu ifade edilmiştir (Statista, 2022). Ayrıca Dünya'da en çok erişim imkanının BAE, Danimarka ve İrlanda'da ve en az erişim imkanının Kuzey Kore'de olduğu, en çok internet kullanıcısının ise Çin, Hindistan ve ABD'de olduğu ifade edilmektedir (Statista, 2022).

TÜİK (2021) 6-15 yaş grubu çocukların internet kullanımı araştırmasında 2013 yılında %50,8 olan durumun 2021 yılında %82,7 olduğunu, internet kullanan çocukların %90,1'inin düzenli internet kullandığını, internet kullanım amaçlarının çevrim içi ders, ödev, oyun

oynama, video izleme, iletişim kurma vd. olduğunu, düzenli internet kullananların %31,3'ünün sosyal medya kullandığını, %64,4'ünün akıllı telefon kullandığını, erkekler için en fazla savaşı, kızlar için en fazla aksiyon oyunlarının tercih edildiği ifade edilmiştir.

Birçok araştırmada 21. yüzyıl, çeşitli isimlerle anılmaktadır ve bilgi çağı, dijital çağ olarak adlandırılmıştır. Bu çağın en belirgin özellikleri teknolojiye, internette ve uzay biliminde yaşanan gelişmelerdir. İçinde bulunduğumuz çağın gereklerine hitap edebilmek için insanlar dijital teknolojilere adapte olmuş ve olmaya çalışmaktadır. İnsanların yaşamının dijitalleşmesi, dijital dönüşümün yaşandığı bu dönemde kaçınılmaz bir durumdur. Dijital kelimesi sadece elektronik bir araç değil, bilgiyi sayısal olarak işlemektir (Bozkurt vd., 2021, s.36). Dijitalleşme ise bir alanda dijital teknolojilerin işe koşulması olarak tanımlanabilir. Bugün dijitalleşme yaşamın her alanında yaşanmaktadır ve kullanım alanları giderek daha da çeşitlenmektedir. İnsan ihtiyaçları çok farklı alanlarda çeşitlenmesiyle birlikte internette kişilerin bu ihtiyaçlarını giderdiği platformlar da çeşitlenmiştir. İnsanların zamanlarının çoğunu harcadıkları bu platformların başında sosyal ağlar gelmektedir.

Yetişkinlerin ve çocukların internet ve dijital teknolojiler aracılığıyla erişim sağladığı tek platform sosyal ağlar değildir. Her gün milyonlarca insan çevrim içi alışveriş yapmakta, dijital oyunlar satın almakta, internet ve dijital araçlar aracılığıyla iletişim kurmakta ve daha pek çok kişisel ve kurumsal ihtiyaçlar bu teknolojiler aracılığıyla giderilmektedir. Bu durumlar sadece yetişkinler için değil çocuklar için de geçerlidir. Dijital ortamdaki alışkanlıkların sebebi dijital teknolojilerin avantajlarıdır. Bu avantajların başında bilişim teknolojilerinin sağladığı hizmetlerin iş ve zaman bakımından ekonomik olması, zengin bir içeriğe sahip olması yer almaktadır. Bilişim teknolojilerini popülerleştiren bu avantajların haricinde tabi ki dezavantajları da mevcuttur. Özellikle çocuklar dijital ortamı denetimsiz kullanmaktadır ve yetişkinlere göre risklere karşı daha savunmasız kalmaktadırlar (Karakuş vd., 2014, s.232). Bu açıdan özellikle çocukların dijital becerilerinin geliştirilmesi ve dijital konularda daha yeterli hale getirilmesi önemli hususlar arasındadır.

Dijital vatandaşlığın temel unsurları aslında dijital araçları kullanan her bir vatandaşta olması gereken becerilerdir ve temel görevi görmektedir (Ribble, 2007, s.11). Dijital dünyaya adapte olmuş ve dijital teknolojileri uygun bir şekilde kullanabilen vatandaşlar “dijital vatandaş” olarak kabul edilmektedir. İyi bir dijital vatandaşta olması gereken beceriler dijital vatandaşlığın alt boyutları ile açıklanmaktadır. Hemen hemen her boyuta yönelik uygun

olmayan davranışlar neticesinde belirgin riskler doğmakta ve bu da dijital güvenliği ilgilendirmektedir. Zaruri ihtiyaç niteliğindeki becerilerden biri olan dijital güvenlik boyutu popülerliğini buradan almaktadır. Çünkü riskler çok boyutlu ve çeşitlidir. Üstelik dijital ortamda var olan riskler kullanıcı sayısının artması ve kullanıcı yaşının da giderek düşmesi sonucunda doğal bir artış göstermektedir Buna ek olarak dijital teknolojilerin sağladığı fırsatların risklerle ilişkili olduğu ifade edilmektedir (Helsper ve Smahel, 2020; Livingstone, Mascheroni ve Staksrud, 2018). Ayrıca şunu diyebiliriz ki dijital ortamın avantajları, kullanıcı niceliği ve kullanıcı yaş seviyesi, kullanım niteliği risklerle doğrudan ilişkilidir. Bu noktada etkili olan unsurlardan doğabilecek her türlü risk ve dijital beceriler dijital güvenliği ilgilendirmektedir.

Bennet ve Maton' a (2010) göre gençler teknolojiye maruz kala kala farklı düşünür hale gelmiş, davranış tarzları değişmiş, öğrenme tarzları farklılaşmış ve bununla birlikte “dijital yerliler” ve “net nesil” gibi sıfatlar almışlardır (s.321). Dijital yerli ifadesi Prensky (2001) tarafından kullanılmıştır ve Prensky' e (2001) göre dijital yerlilerin düşünce yapılarının, davranışlarının diğer nesillere göre farklı olmasının temelinde tüm hayatlarını bilgisayarlarla, video oyunları, dijital müzik çalarlarla ve dijital çağın diğer tüm oyuncak ve araçlarıyla çevrili geçirmeleri yer almaktadır (s.1). Aynı durumlar gençler kadar çocuklar için de geçerlidir. Bu konuda Livingstone vd. (2017) çocukların günün çoğunu dijital ortamda geçirdiğini ve risklere sıklıkla temas ettiğini belirtmektedir (s.2). Hasebrink, Livingstone, Haddon ve Olafsson (2009) EU Kids Online raporuna göre ebeveynler çocuklarının zararlı içeriklere çok sık temas ettiğini ve bu risklerin çok olduğunu, çocuklarının bu konuda yetersiz olduğunu belirtmektedirler (s.33-89). Buradan anlaşılacağı üzere gençlerin ve çocukların dijital ortamda risklerle karşılaşma olasılığı yüksektir ve dijital güvenlik açığı vermesi muhtemeldir. Bu sonuçları belki de onların dünyasını anlamadan çözümlememiz imkansız olacaktır. Çocukların dünyasını anlamak için eğitimin tüm paydaşlarının dijital dünyaya adapte olarak dijital becerilerini geliştirmeleri gerekmektedir. Aksi halde çocukları dijital dünyanın risklerinden korumak zor olacaktır. Robinson vd. (2010), günümüzde siber güvenlikten zarar gören gençlerin ve çocukların fazlaca olduğunu (s.6) ve bilgi işlem alt yapısının devam eden gelişiminin ve dijital dünyaya erişimin artmasıyla okul bölgelerinin güvenlik konularını incelemesinin teşvik edildiğini belirtmiştir (s.7).

Ribble ve Bailey (2007) dijital güvenliği “*tüm teknoloji kullanıcılarının kişisel güvenliklerini ve ağlarının güvenliğini garanti altına almak için almaları gereken önlemler*” olarak tanımlamıştır (s.33). The Online Safety and Technical Working Group [OSTWG] (2010) ‘un yayınladığı “Yaşayan İnternette Gençlik Güvenliği” raporunda ise dijital güvenlik, “*interneti ve dijital araçları kullanırken fiziksel güvenlik, psikolojik güvenlik, itibar-yasal güvenlik ve kimlik mülkiyet-toplum güvenliğini sağlama*” olarak belirtilmiştir (s.4-5). Bu rapora göre dijital güvenlik alanlara ayrılmış ve teknik güvenlik merkeze alınmamış, daha detaylı olarak dijital güvenliğe sağlık, psikoloji, ticaret, hak ve sorumluluk, hukuk ve sosyal boyut dahil edilmiştir.

Buna göre dijital güvenliğin sadece cihaz güvenliği olmadığı söylenebilir. Ancak günümüzde dijital güvenlik denildiğinde çoğu kişinin aklına zararlı yazılımlar ve dijital cihazların bu zararlı yazılımlara karşı güvenliğini sağlamak gelmektedir. Fakat dijital güvenlik sadece dijital cihazların güvenliği söz konusu değildir. Zaten bu gibi güvenlik sorunları güvenlik yazılımları aracılığıyla halledilebilmektedir. Yılmaz vd., (2016) dijital güvenlikten pekte farklı olmayan dijital veri güvenliğinin sadece teknik boyuttan ibaret olmadığını, insan faktörünün önemli olduğunu ve çevrim içi ortamda insan davranışlarından kaynaklı oluşabilecek problemlerin de alana dahil edilmesi gerektiğini ifade etmektedir (s.28). Bu doğrultuda dijital güvenlikte insan faktörü ve onun dijital ortamdaki davranışlarından kaynaklı risklerin önemli boyutta olduğu söylenebilir.

Alanyazın incelendiğinde dijital güvenliğin farklı alanlar halinde incelendiği görülmektedir. Ribble (2011) dijital güvenliği donanım ve ağ güvenliği, kişisel güvenlik, okul güvenliği ve toplum güvenliği olarak incelemiştir (s.41). Hendrix, Al- Sherbaz ve Bloom (2016) ise dijital güvenliği teknik boyuttan psikolojik boyuta kadar birçok açıdan ele almıştır (s.58). OSTWG (2010) ise risklerden yola çıkılarak fiziksel, psikolojik, sosyal itibar ve yasal güvenlik, kimlik, mülkiyet ve toplum güvenliği olarak dört alanda incelenmiştir (s.5). Robinson vd. (2010) ve Schneier (2004) ise dijital güvenlikte insan faktörünün çok önemli bir faktör olduğunu düşünmektedir. Bu doğrultuda dijital güvenliğin aslında geniş bir çerçevesi bulunmaktadır ve dijital güvenliğin geniş bir çerçeve ile ele alınmasındaki temel sebep çevrim içi risklerin çok çeşitli ve birçok alanı etkiliyor olmasıdır.

Vanlanduyt ve De Cleyn (2007) dijital güvenliği etkileyen risk faktörlerini beş alanda incelemiştir; “*Birincisi internetin sosyal ilişkiler üzerinde olumsuz etkilemesi; ikincisi*

pornografi, şiddet ve açık bir dile istenmeyen şekilde maruz kalınması; üçüncüsü fiziksel sağlığa etkisi; dördüncüsü zaman yönetimi konusunda olumsuz etkisi ve beşinci olarak bilinçsiz tüketim ile ticari istismara yol açmasıdır” (Vanlanduyt ve De Cleyn’den aktaran Valcke, Bonte , De Wever ve Rots, 2010, s.455). Canbek ve Sağıroğlu (2007) ise çevrim içi ortamda çocuk ve gençlerin karşılaşabileceği risk ve tehditleri 3 alanda incelemiştir. Bu alanlar; *“teknik riskler, fiziksel, sosyal ve psikolojik riskler, hayati risklerdir”* (s.35). Canbek ve Sağıroğlu (2007) bunlara ek olarak çevrim içi alışveriş, ile hak ve sorumluluk boyutunu içine alacak riskleri de internette karşılaşılabilecek tehditler başlığı altında ele almıştır (s.35).

Ülkemizde Bilgi Teknolojileri ve İletişim Kurumu [BTK] internet risklerini şöyle sınıflandırmıştır;

“Siber zorbalık, yanlış ve/veya zararlı bilgiye erişim, sanal dolandırıcılık, kişisel bilgilerin paylaşımı ve kimlik hırsızlığı (identity theft), zararlı yazılımlar, oltalama (phishing), pornografi /çocuk istismarı/ fuhuş, yasadışı kumar internet bağımlılığı, sağlık sorunları, yabancılarla çevrimiçi ve çevrimdışı iletişim, şiddet/nefret/ırkçılık faaliyetleri, silah ve madde kullanımı, telif hakları ihlali” (BTK, 2019, s.1).

Dijital güvenlik çerçevesi alanyazın incelendiğinde sadece riskler ile belirlenmediği görülmüştür. Bu konuda çeşitli çalışmalar ve bu çalışmaların dijital güvenliğin merkezine alındığı boyutlar yer almaktadır. Ayrıca alanyazında dijital güvenliğin çerçevesini etki alanları, yeterlik ve becerilerin de belirlediği görülmektedir. Bazı çalışmalarda dijital güvenlik teknik beceriler ile ele alınmış (M. Tekerek ve Tekerek, 2013; Şahinaslan vd., 2009), bazı çalışmalarda ise dijital zorbalık, çevrim içi alışveriş, hak ve sorumluluk, sağlık boyutların da kapsama alındığı görülmektedir (Bayındır, 2020; Çolak vd., 2011; Çolak, 2019; Durmaz ve Ulukol, 2022; Talan ve Aktürk, 2021). Bunların haricinde çevrim içi ortamda güvenlik açısından çocuklar üzerinde olası etkilerin incelendiği çalışmalar (Çubukçu ve Bayzan, 2013; Demirel vd, 2012; Vural ve Sağıroğlu, 2008) ve dijital güvenliği etkileyen riskleri inceleyen çalışmalar (Byrne vd., 2016; Çelen vd., 2011, Karakuş vd., 2014) da mevcuttur.

Bu çalışmada dijital güvenliğin çerçevesinin belirlenmesi için hem alanyazın hem de MEB SBDÖP ve 7. sınıf öğrenci yaş seviyesi dikkate alınmıştır. SBDÖP incelendiğinde programda *“sanal ticaret”, “sosyal medya”, “dijital bölünmüşlük”, “kimlik hırsızlığı”, “kişisel bilginin gizliliği”, “siber dolandırıcılık”, “siber zorbalık”* kavramlarına yer verildiği görülmüştür (SBDÖP, 2018). Bununla birlikte sosyal bilgiler 4., 5., 6. ve 7. sınıf kazanım ve ders kitaplarında *“bilgi güvenliği”, “doğru bilgiye erişim”, “internet*

alışverişi”, “internet bilinçli ve doğru kullanımı”, “kimlik hırsızlığı”, “dijital cihazların güvenli olarak kullanılması”, “veri kaybı ve veri güvenliği”, “dijital araçların uygunsuz kullanımında yaşamımızda oluşabilecek güvenlik sorunları”, “dijital ortamda güvenlik kuralları”, “dijital oyunlar ve güvenliğe etkisi”, “kaynak kullanımında intihal vb. dijital güvenlik problemleri”, “dijital ortamda telif ve patent kavramlarına güvenlik açısından dikkat”, “dijital hak ve sorumluluklar”, “dijital bağımlılık” ve “zararlı içeriklerin etkisine” rastlanmıştır (SBDÖP, 2018). Bu açıdan bu çalışmada dijital güvenlik, alanyazın ile SBDÖP arasında bağ kurularak ve ortaokul yaş seviyesine göre düzenlenmiş, ilintili konular birleştirilerek boyutlandırılmıştır. Bu bağlamda dijital güvenlik teknik, psikososyal, çevrim içi alışveriş, hak ve sorumluluk ve sağlık boyutlarında ele alınmıştır. Bu boyutlar ve boyutlara dayalı yeterlik göstergelerine aşağıdaki bölümde “Dijital Güvenlik Yeterliği” başlığı altında yer verilmiştir.

2.4. Yeterlik, Dijital Yeterlik ve Dijital Güvenlik Yeterliği

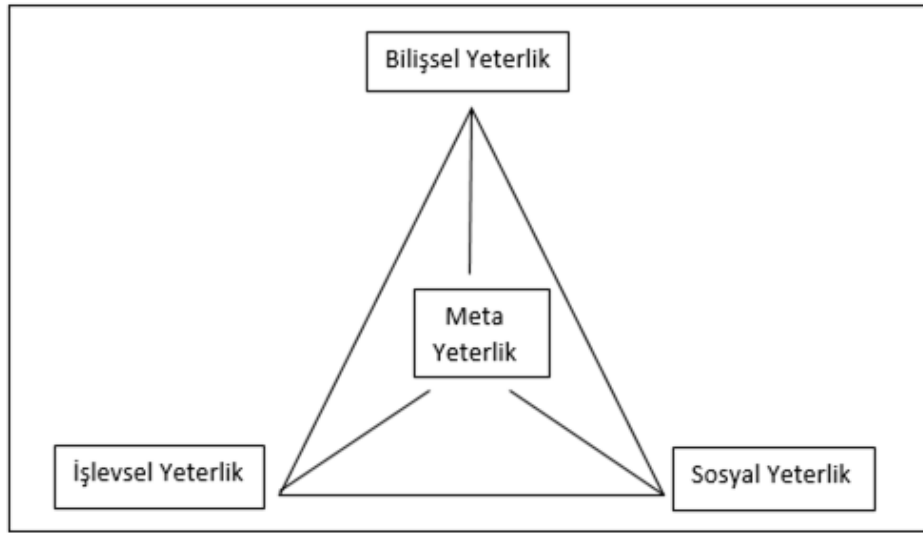
2.4.1. Yeterlik

Eğitim alanyazınında yeterlik kavramı eş değer sözcüklerden dolayı zor olarak görülen kavramlardan biridir. Genellikle yetkinlik kavramı ile muadil olarak kullanılan yeterlik kavramı hakkında pek çok tanım bulunmaktadır. Yeterlik, bir amaca ulaşmak, bir işin yapabilmek için kişinin ihtiyacı olan beceri, tutum, bilgi ve algıların tümü demektir. Literatürde ve sözlüklerde “*iyi nitelikte olma durumu*”, “*bir şeyi başarılı veya iyi bir şekilde yapabilme yeteneği*”, “*gerekli bilgi, beceri, nitelik ve kapasiteye sahip olma durumu*”, “*belirli bir beceri, bilgi ve yetenek yelpazesi*” gibi tanımlar yer almaktadır (Kilpatrick, 2014, s.85).

Yeterlik kavramı açıklanmaya çalışıldığında yetkinlik, yetenek, kapasite gibi sözcüklerle iç içedir. Fakat yeterlik geniş kapsamlı bir kavram olarak düşünülmelidir ve yetkinliğin içinde var olan ilişkileri ifade etmektedir. Yani yeterlik karmaşık bir yapıdadır ve bütünsel olarak ele alınmalıdır. Alex’ e (1991) göre yeterlik, “*bireyin edindiği davranış kalıpları ve becerileri de dahil olmak üzere tüm bilgi ve yeteneklerini kapsamaktadır*”. Yeteneklerden yola çıkılarak yapılan tanımlardan başka anlayışla yapılmış bazı tanımlar da bulunmaktadır.

Gibb (1990) yeterlikte motivasyonun da önemli bir unsur olduğunu ifade etmektedir. Burada duyuşsal alandan bahsedilmektedir. Eraut (1998) ise bireyin işi gerçekleştirdiği andaki performansından da bahsetmekte ve kavramın aslında işin yapılış esnasındaki gerçek yapabilme durumu olduğunu belirtmektedir (s.128). Krasna ve Bratina (2011) ise yeterlik kavramını genel geçer bir şekilde “*bilgi, beceri ve gerekli durumlar arasındaki ilişkilerin tümü*” olarak ifade etmiştir (s.1). Tanımlarda bazı noktalarda ortak bir anlayışa varılamamasının sebebi kimi araştırmacıların kavrama geniş kimilerinin ise kavrama belirli bir alan üzerinden bakmasından kaynaklı olabilir. Le Deist ve Winterton (2005) yeterliğin bütünsel olarak ele alınması gerektiğini savunmuş ve bilişsel, işlevsel ve sosyal boyutlarla birlikte alınması gerektiğini öne sürmüştür (s.39-40). Buradan hareketle yeterlik hakkında kapsayıcı anlayışın ortaya çıkması için onun çok boyutlu ve bütünsel bir yaklaşımla ele alınması gerekmektedir, ancak bu sayede söz konu alanın çerçevesi çizilebilmektedir.

Bütünsel Yeterlik Modeli



Şekil 2. Bütünsel yeterlik modeli. Le Deist, F.D. ve Winterton, J. (2005). What Is Competence?. Human Resource Development International, 8(1), 27-46.

Yeterlik kavramının ortak bir anlayışta buluşması için söz konusu kavramın hangi alanla ilgili olduğunun belirlenmesi gerekmektedir. Yukarıdaki görselde yeterlik bütünsel olarak ele alınmış ve meta yeterlik olarak adlandırılmıştır. Le Deist ve Winterton (2005) bütünsel bir bakış açısıyla ele alınan yeterlikte işlevsel yeterlik alanı, sosyal yeterlik alanı ve bilişsel yeterlik alanlarının olduğu Şekil 2 ile gösterilmiştir. Bu anlayışa göre ilgili alanda yeterliğin

çerçevesi çizilirken o alandaki bilişsel durum, işlevleri ve sosyal konular ele alınabilir ve bu sayede örgün eğitim ve deneyimleyerek öğrenme arasındaki bağdan yararlanılmış olacaktır. Günümüzde yeterlik kavramı farklı farklı alanlarda kullanılmaktadır. Örneğin, siyaset, eğitim, mesleki, sosyal, bilimsel, ticaret, dijital vb farklı alanlarda yeterlik kavramı kullanılmaktadır. Yeterlik kavramı diğer alanlarda olduğu gibi eğitim alanına da girmiş ve Türk Milli Eğitimi tarafından öğrencilerde 21. yüzyıl becerileri çerçevesinde olması gereken yeterlikleri “Türkiye Yeterlikler Çerçevesi (TYÇ)” başlığı ile yayınlamıştır. TYÇ’de bahsi geçen yeterlikler; anadilde iletişim, yabancı dillerde iletişim, matematiksel yetkinlik ve bilim/teknolojide temel yetkinlikler, dijital yetkinlik, öğrenmeyi öğrenme, sosyal ve vatandaşlıkla ilgili yetkinlikler, inisiyatif alma ve girişimcilik, kültürel farkındalık ve ifade olarak belirtilmiştir (MEB, 2018). Ayrıca TYÇ’de yer alan 8 anahtar yetkinlikte bulunması gereken özellikler MEB (2018) tarafından detaylı bir şekilde açıklanmıştır. Bununla birlikte TYÇ’de belirlenen yeterlik alanları ile ülkemizde eğitim aracılığıyla vatandaşların sahip olması gereken yeterliklerin çerçevesi çizilmiş ve her vatandaşa kazandırmak amaçlanmıştır.

2.4.2. Dijital Yeterlik

Dijital yeterlik, *“bireyin dijital ortamda dağınık ve farklı biçimlerde bulunan bilgilere erişebilme, anlayabilme ve kullanabilme sürecindeki bilgi, beceri ve tutumlarıdır”* (Lankshear ve Knobel’dan aktaran Toker, Akgün, Cömert ve Edip, 2021, s.303). Dijital yeterlikler sadece eğitim için değil hayatın diğer alanlarında yaşam boyu öğrenmeyi desteklemek için de gerekli olan yeterliktir. Dijital yeterlikleri etkileyen temel faktörler arasında dijital teknolojilerde yaşanan gelişmeler ve dijital dönüşümdür. Öyleki dijital teknolojilerin gelişimi ve dijital dönüşüm hızı dijital yeterliklerin kazandırılması zorunluluk haline gelmiştir (Akkoyunlu ve Soylu, 2010, s.755).

Dijital vatandaşların dijital yeterliklerini ifade etmesi bakımından European Commission (2006) tarafından Avrupa Yeterlikler Çerçevesi içerisinde 8 anahtar yetkinlikten biri olarak görülen “dijital yetkinlik” şu şekilde ifade edilmiştir;

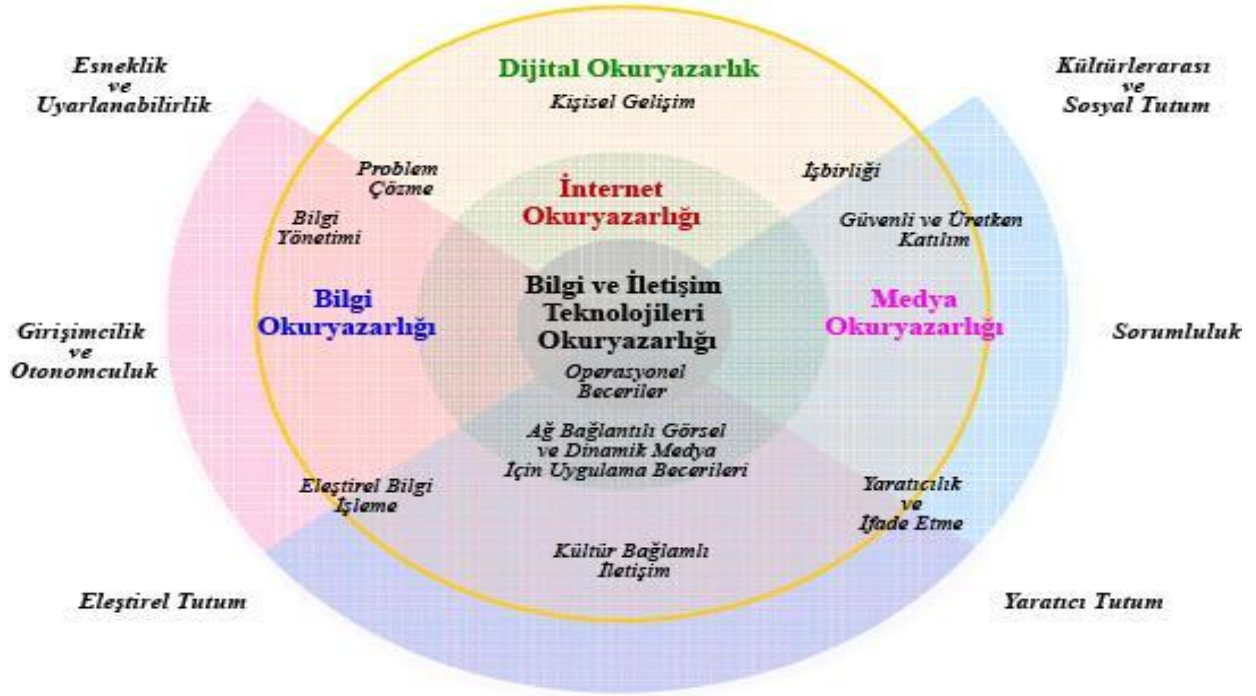
“İş, günlük yaşam ve iletişim için bilgi toplumu teknolojilerinin güvenli ve eleştirel şekilde kullanılmasını kapsamaktadır. Dijital yetkinlik, bilgi ve iletişim alanındaki temel becerilerle: bilgiye erişim, bilginin değerlendirilmesi, saklanması, üretimi, sunulması ve alışverişi için bilgisayarların kullanılması ve internet aracılığıyla ortak ağlara katılım sağlanması ve iletişim kurulması yoluyla desteklenmektedir.”(European Council, 2006, s. 6).

Ferrari ve Punie (2013) European Commission tarafından geliştirilen dijital yeterliği “iş, yerleşiklik, eğitim, topluma katılım ile ilgili amaçlara erişebilmek için bilgi ve iletişim teknolojilerini özgüvenli, eleştirel ve üretken kullanımı” olarak tanımlanmıştır ve tüm vatandaşlar tarafından edinilmesi gereken 21. yüzyıl becerilerinin tümüyle ilgili olduğu ifade edilmektedir (s.2).

Ferrari ve Punie (2013) European Commission tarafından geliştirilen Dijital Yeterlik Çerçevesi’nde 5 alanın olduğunu belirtmiş ve bu alanları şöyle isimlendirmiştir; bilgi, iletişim, içerik oluşturma, güvenlik ve problem çözme. Ferrari ve Punie (2013) tarafından bu alanlar şöyle açıklanmıştır:

1. Bilgi: Dijital bilgileri, alaka düzeyini ve amacını değerlendirerek tanımlama, bulma, alma, saklama, düzenleme ve analiz etme.
2. İletişim: Dijital toplumda iletişim, kaynakları internette paylaşma, diğer kullanıcılarla iletişim kurma, işbirliği yapma, topluluklara katılma.
3. İçerik oluşturma: Yeni içerik oluşturma, varolan içerikleri ve bilgileri parçalı şekilde kullanabilme, üretken ve orijinal içerik oluşturma, fikri mülkiyet hakları ve lisanslı içeriklerle ilgilenme ve bunları uygulama.
4. Güvenlik: Kişisel koruma, veri koruma, dijital kimlik koruması, güvenlik önlemleri, güvenli ve sürdürülebilir kullanım yapabilme.
5. Problem çözme: Dijital ihtiyaçları ve kaynakları belirleme, amaca veya ihtiyaca göre en uygun dijital araçların hangileri olduğuna dair bilinçli kararlar verme, kavramsal sorunları dijital yollarla çözme, teknolojileri yaratıcı kullanma, teknik sorunları çözme, kişinin kendi ve başkalarının yetkinliklerini güncelleme.” (Ferrari ve Punie, 2013, s.4).

Avrupa Yeterlikler Çerçevesi’nde temel yeterlikler arasında gösterilen dijital yeterliğin kavram haritası şekil 3’te gösterilmiştir.



Şekil 3. Dijital yeterliğin kavram haritası. Ala-Mutka, K. (2011). Mapping digital competence: Towards a conceptual understanding. Sevilla: Institute for Prospective Technological Studies, 7-60.

2.4.3. Dijital Güvenlik Yeterliği

Dijital ortama tam anlamıyla adapte olmak için gerekli tüm yeterlikleri ifade eden dijital yeterlikler yaşadığımız dijital çağda birçok alanda yaşanan dijital dönüşümden kaynaklı olarak giderek önemini artırmaktadır. Dijital yeterlik ve yeterlik tanımlarından hareketle dijital güvenlik yeterliği; dijital ortamda güvenliğini sağlayabilme sürecinde kullanılacak bilgi, beceri ve tutumlara sahip olma durumu olarak tanımlanabilir.

Dijital güvenlik yeterliği kısaca kişinin dijital ortamda hem dijital araçlarının güvenliğini hem kişisel güvenliğini sağlamak hem de diğer kullanıcıların dijital güvenliklerini ihlal etmemektir. Artık günlük yaşamımızın büyük çoğunluğunda dahil olduğumuz dijital toplumda dijital güvenliği tehdit eden sayısız risk ve tehdit vardır. Çevrim içi ortamda ve dijital araçların kullanımı sırasında kişilerin dijital güvenliğini sağlama yolunda bir takım önlemsel ve tepkisel eylemler açığa çıkmaktadır. Bu eylemler hakkında gerekli bilgi, beceri ve tutuma sahip olmaya yeterlik denilmektedir. Bu bağlamda dijital güvenlik yeterliği, dijital

araçlar (akıllı telefon, tablet, bilgisayar vb.) sayesinde çevrim içi ortama katılım sırasında kişinin güvenliğini sağlaması için bilişsel, duyuşsal ve teknik becerilerin tümünü işe koşabilmesidir. Dijital güvenlik yeterliğini risk ve tehditlerin kaynağına ve etki alanına göre sınıflandırmak mümkündür.

Ortaokul 7. sınıf öğrencilerinin dijital güvenlik yeterliklerini geliştirmek için hazırlanmış çevrim içi öğrenme aracının içeriğinin belirlenmesi amacıyla dijital güvenlik yeterlik göstergeleri belirlenmeye çalışılmıştır. Bu amaçla bu çalışmada hem MEB'in SBDÖP hem de ilgili alanyazın incelenmiştir. Bu incelemeler neticesinde özel olarak dijital güvenlik yeterliklerinin ve becerilerinin detaylı bir şekilde ele alınmadığı görülmüştür. SBDÖP'nda ise özel amaçlar, yetkinlikler, özel amaçlar, beceriler, değerler ve programın uygulanmasında dikkat edilecek hususlarda doğrudan dijital güvenlikle ilgili olan “*sanal ticaret, sosyal medya, dijital bölünmüşlük, kimlik hırsızlığı, kişisel bilginin gizliliği, siber dolandırıcılık, siber zorbalık*” kavramlarından bahsedilmiştir. Bunun yanında daha açık ve detaylı olarak programdaki kazanım ve kazanıma dair açıklamalarda ve ders kitaplarında “*dijital ortamda doğru bilgiye erişim, güvenli bilgi ve bilgi kaynağına erişim, çevrim içi alışveriş, güvenli internet kullanımı, kimlik hırsızlığı, dijital araçların kullanımında güvenlik, veri güvenliği, bilgi güvenliği, dijital araçların etki alanlarında yaşanabilecek risk ve tehditler, dijital ortamda güvenlik kuralları, dijital oyunların kişisel güvenliğe etkileri, erişilen kaynakların kullanımı ve kaynakça gösteriminde güvenliği tehdit eden durumlar, dijital ortamdaki telif ve patent hakkına sahip bilgi ve belgelerin kullanımı, dijital ortamda haklar ve sorumluluklar, dijital bağımlılık ve zararlı içeriklerden kaynaklı olumsuz etkilerinin*” ele alındığı görülmüştür.

İncelemeler neticesinde hem SBDÖP hem de alanyazın doğrultusunda ortaokul 7. sınıf öğrencilerinin hedef kitle olarak belirlendiği bu çalışmada bu yaş grubunun çevrim içi faaliyetlerinden yola çıkılarak olması gereken dijital güvenlik yeterlikleri 5 boyutta ele alınmıştır. Bu boyutlara dair yeterlik göstergeleri hem alanyazında yer alan risk ve tehditler hem de SBDÖP'nda yer alan konularla açıklanarak aşağıda sunulmuştur.

2.4.3.1. Teknik Boyutta Dijital Güvenlik Yeterliđi

Bu boyutta kiřinin evrim ii ortamda ve bu ortama katılımda hem dijital cihazlarını hem de kiřisel verilerini koruması yolunda ihtiyacı olan teknik iřlem ve kontrolleri yapma durumu ele alınmıřtır. Teknik boyutta řifre gvenliđini sađlama, cihaz gvenliđini sađlama, eriřim gvenliđini sađlama, eriřtiđi kanallarda dođru ve gvenli bilgiyi ayırt etme ve dijital ortamda dijital ayak izini ynetme konuları hem alanyazın hem de SBDP kapsamında btnleřtirilerek ele alınmıřtır.

Teknik boyutu dijital gvenlik iin gerekli kılan temel dayanak, cihazların verilerin gvenliđi konusunda birok kiřinin kendini yetersiz hissetmesi ve oltalama (phishing), kimlik avcılıđı, virs bulařtırma vb. iřlemlerinin sıka kullanılmasıdır. İnsanlar genellikle dijital cihazları ve cihazlarında mevcut olan verileri veya bundan sonra cihazları aracılıđıyla kendileri ile ilgili verileri girdiklerinde gizlilik konusunda endiře duymaktadır (Ackerman, Cranor ve Reagle, 1999; Dodel ve Mesch, 2018; Hadlington, 2017). Fakat bu endiřeye rađmen Ackerman vd. (1999)'ne gre kiřiler gvenlik aıđı vermeye devam etmektedir (s.2). Bu durumun birok sebebi olabilir. Kiřilerin endiře duymasına rađmen gelen řpheli e-postaları drtsel davranıřlardan dolayı aması, nasıl gl řifre oluřturacađını bilmemesi, halka aık cihazlarda nemli dosyalarını ve hesaplarını amaması gerektiđini dřnememesi, gvenli ıkıř yapmayı tercih etmemesi veya tm endiře duymasına rađmen gvenli yolları tercih etmemesi teknik anlamda gvenlik aıđı vermesine sebep olarak grlebilir.

Teknik boyutta gvenliđin sađlanmaması durumunda dijital vatandařların karřılařabileceđi riskler: sosyal mhendislik, hackleme (dos atakları vb.), zararlı yazılımlar aracılıđıyla cihaza bulařan virs, truva atı ve solucanlar, korsan yazılım ve erezlerin cihaz ve veri kaynađında birtakım deđiřiklikler yaratmasıdır.

Dijital cihazlarımızı ve hesaplarımızı tehdit eden teknik risklerle karřılařmamak neredeyse imkansızdır ve bu riskleri tam anlamıyla kontrol altında tutamayız. Her ne kadar ocuklar ve genler dijital yerli olsalar da teknik risklere karřı btnsel olarak korunabilecek yazılım bilgisine ve dijital yeterliklerin tmne sahip deđiller. Robinson vd. (2010) teknik anlamda ađ gvenliđini ve cihaz gvenliđini tam anlamıyla sađlama konusunda bilgisayar uzmanlarının bile korktuđunu ve zaten teknik gvenliđin tam anlamıyla mmkn

olmayacağını ancak bazı önlemlerle risklerin en aza indirilebileceğini belirtmektedirler (s.57).

Yapılan bazı araştırmalarda ilgili boyutta ele alınan konularda yaşanabilecek risklerin dijital güvenlikte kritik olduğu vurgulanmıştır. Sosyal bilgiler 5. sınıf “Bilim, Teknoloji ve Toplum” öğrenme alanında 3. kazanım doğrultusunda “güçlü şifre oluşturma ve şifre koruma yöntemlerine” değinilmiştir (5. sınıf sosyal bilgiler ders kitabı, s.104-105) ve bu konu alanyazında da önemli bulunmuş, dijital güvenlik araştırmalarında sıklıkla ele alınmıştır. NordPass (2021) dünya vatandaşların çoğunun zayıf şifreleri tercih ettiğini ve bu durumun risk teşkil ettiğini ifade etmiştir. Bu konuda güçlü şifre oluşturma yöntemlerinin bilinmesi ve şifre güvenliğini sağlama yollarının tercih edilmesi riski azaltacaktır. Cihaz güvenliği SBDÖP’nda da ele alınmıştır (5. sınıf sosyal bilgiler ders kitabı, s.103). Teknik becerilerin ihtiyaç duyulduğu konu hakkında Luo, Liu, Liu ve Fan (2009) zararlı yazılımların cihaz güvenliğini tehdit ettiğini ve bu riskin sosyal mühendislik tehdidine de yol açtığını belirtmiştir (s. 648). Bu konuda güvenlik yazılımlarının kullanılması, lisanslı yazılımların tercih edilmesi ve internette şüpheli bağlantılara tıklama yapılmaması önleme yöntemlerindendir. Erol vd. (2015) bu durumu dijital güvenlikte önemli bulmuş ve geliştirdiği ölçekte “güvenilmeyenden kaçınma” boyutunda ele almıştır. Bu boyutu Makhabbat ve Gülseçen (2021) de siber güvenliğin değişkenlerini belirlemeyi amaçladığı çalışmasında siber güvenlikte teknik becerilerin gerekli olduğu boyutta kullanmıştır (s.43). Dijital ortamda doğru ve güvenli bilgiyi ayırt etme konusu hem SBDÖP’nda (5. sınıf sosyal bilgiler ders kitabı, s.98-100) ve hem de alanyazındaki ilgili çalışmalarda ele alınmıştır. Ayrıca doğru ve güvenli bilginin bir takım teknik kontroller aracılığıyla tespit edilmesinden kaynaklı bu çalışmada teknik boyutta ele alınmıştır. Bu konunun risk teşkil etmesinin sebepleri internette bilgi üretme ve yayma oranının fazlaca olması ve bu durumla alakalı günümüzde bilgi dezenformasyonunun yaşanmasıdır. Doğru olmayan bilgi ve güvenli olmayan kaynaklar sonucunda hem gündelik hayatta olumsuz etkiler (ekonomik, siyasi, kültürel, sosyal alanlar) hem de psikolojide olumsuz etkiler (infobezite, dijital istifçilik, siberhondrik ve aşırı bilgi yükleme) yaşanabilmektedir (Demir, 2022, s. 16-35). UNICEF (2021) raporunda çocukların bilgi dezenformasyonunun hedefi haline geldiğini belirterek konuyu önemine vurgu yapmıştır. Çömlekçi (2019) ise doğru ve güvenli olmayan bilginin büyük risk taşıdığını belirtmiştir (s.1550). Bu konuda söz konusu güvenlik problemlerinin

yaşanmaması için erişilen kaynağın güvenliğini kontrol etmek amacıyla “SSL Sertifikası kontrolü” ve adres çubuğunda site güvenlik bilgilerini görüntüleme yöntemleri, bilginin doğruluğunu kontrol etmek amacıyla ulaşılan sitede iletişim, adres, hakkında bölümlerinin kontrolü, içerik kıyaslama kontrollerinin yapılması gerekmektedir. Son olarak dijital ayak izi yönetimi konusunda teknik kontrollerin yapılmasından kaynaklı teknik boyutta ele alınmıştır. SBDÖP’nda ise 5. sınıf 4. Öğrenme alanında “Çok tanınıyorsun! Farkında mısın?” konu başlığı ile internette dijital ayak izleri konusu ele alınmıştır (5. sınıf sosyal bilgiler ders kitabı, s. 105). Alanyazın incelendiğinde Yavanoğlu, Sağıroğlu ve Çolak (2012) dijital ayak izlerin sonucunda çocukların pedofili tehdidi ile karşı karşıya kalabildiğini belirtmiş (s.18) ve bu boyutu Erol vd. (2015) de incelemiştir. Dijital ayak izi yönetimi konusunda güvenlik problemi yaşanmaması adına alınabilecek önlemler arasında özellikle halka açık bilgisayarlar da dahil olmak üzere tüm dijital araçların kullanımında internet gezinimi sırasında gizli sekme kullanılabilir. Gizli sekme kullanımında arama motorunda yapılan işlemler kaydedilmez ve dijital ayak izi bırakılmamış olur. Bunun yanında dijital ayak izi yönetimi konusunda istemsiz tıklamalar yapılmamalı, güvenli olmayan veya uygun olmayan sitelere erişim yapılmamalı, arama yapılacak konulara dikkat edilmeli ve güvenlik gerektiren işlemlerde halka açık olarak kullanılan cihazlar tercih edilmemelidir. Ayrıca gizli kalmasını istediğimiz bilgiler cihazın internet geçmesinden ve çöp kutusundan temizlenmelidir. İnternette dijital kimliğimize aykırı bilgilerin dolaşmamasını istiyorsak arama motorlarında adımızı aratıp kimliğimizi zedeleyecek bilgilerin silinmesi için temizlememiz gerekmekte veya bu bilgiler başkaları tarafından oluşturulmuşsa şikayet hakkımızı kullanmamız gerekmektedir.

Teknik boyutta dijital güvenlik yeterli göstergeleri:

- Şifre hatırlatmada kullanılan güvenlik sorularına başkalarının tahmin edemeyeceği cevaplar oluşturma
- Güçlü şifre oluşturma
- Her uygulama için farklı şifre kullanma.
- Şifre güvenliği için “iki faktörlü kimlik doğrulama” yöntemi kullanma.
- Akıllı telefon, tablet, bilgisayar, kablosuz ağ modemini şifreli kullanma.
- Dijital cihazlarda güvenlik yazılımı kullanma.
- Dijital cihazlarda lisanslı yazılım kullanma.

- Dijital cihazlarda önemli dosyaları yedekleme.
- İstenmeyen postaları “istenmeyen posta” olarak işaretleme.
- İnternet sitelerinin güvenlik sertifikalarını kontrol etme.
- Şüpheli görünen web linklerini açmama.
- İnternet tarayıcısının (Google, firefox vb.) güvenlik ayarlarını düzenleme.
- Güvenilir olmayan internet sitelerinden dosya indirmeme.
- Akıllı telefon, tablet ve bilgisayarda kullanılan uygulamaları düzenli olarak güncelleme.
- İnternet tarayıcısında (Google, firefox vb.) güvenli filtreleme seçeneğini düzenleme.
- Halka açık dijital cihazları (akıllı telefon, tablet, bilgisayar) kullandıktan sonra bilgilerini temizleme.
- Halka açık bilgisayarları güvenlik gerektiren işlemlerde kullanmama.
- Halka açık bilgisayarlarda internet tarayıcılarının gizli sekmelerini kullanarak gezinti yapma (Incognito vb.)
- “Güvenli İnternet Hizmeti” kullanma.
- İnternette ulaşılan bilgi kaynağının güvenilirliğini kontrol etme.
- İnternette ulaşılan bilginin doğruluğunu teyit etme.

2.4.3.2. Psikososyal Boyutta Dijital Güvenlik Yeterliği

Bu boyutta dijital güvenlik yeterliği kişinin kendisinin ve diğer kullanıcıların psikolojik ve sosyal durumunu ve de itibarını olumsuz etkileyebilecek davranışların bilincinde olarak çevrim içi ortama katılabilme ve oluşabilecek risklerle mücadele yöntemlerini bilme konusu ele alınmıştır. Çevrim içi ortamda bireyin psikolojik ve sosyal durum ve itibarını olumsuz etkileyebilecek durumlara yol açan temel sebeplerin başında bireyin kişisel verilerinin bir şekilde (istemli veya teknik ihlaller sonucu) açığa çıkması ve bunun kötüye kullanılma isteği, suça teşvik amacı, kötü niyetli kişilerce hedefe alınması veya tesadüfi olarak tuzağa düşmesi gibi zorbalıklar gelmektedir. Bahsi geçen zorbalıklar arasında özellikle cinsel anlamda çocukları tuzağa düşürme amacı taşıyan kötü niyetli kullanıcıların çok sayıda bulunabilmesidir (Franklin ve Smeaton, 2017, s.1). Robinson vd. (2010) tarafından “yırtıcılar” olarak bahsedilen bu zorbaları şöyle tanımlamaktadır: “*Yırtıcılar gençleri cinsel avtiviteye dahil etmeye çalışan kötü niyetli insanlardır*” ve araştırmacılar FBI’ den

edindikleri bilgileri şöyle aktarmışlardır: “*ABD Federal Soruşturma Bürosu’na (FBI) göre dijital iletişim, gençleri yasadışı cinsel ilişkilere dahil etmek ve müstehcen görüntüleri paylaşmak için pedofiller¹ tarafından kullanılan en yaygın tekniklerden biri olmuştur*” (s.24). Nawaila vd. (2021) ise dijital fırsatların dijital zorbalık risklerini çektiğini ve bununla birlikte pek çok riski de çektiğini ifade etmektedirler (s.1). Buradan da anlaşılabacağı üzere dijital ortamda bu risklerin psikososyal açıdan ciddiyetle ele alınması gerekmektedir.

Çevrim içi ortamda zorbalık ve istismar gibi risklerin haricinde dolandırıcılık, sanal kumar, terör ve çeşitli organize suç örgütlerine teşvik etmek amacıyla her yaştan kullanıcı tuzağa çekilmeye çalışılmaktadır. Ayrıca hackleme ve sosyal mühendislik gibi siber suçlar için bilgi toplamak amacıyla yine sosyal ağlarda açılan sahte hesaplar kötü niyetli kişilerce kullanılmaktadır. Bu ve benzeri psikososyal durumlardan korunmak kişinin bilinç ve farkındalık düzeyinin yükseltilmesi ile mümkündür ve bu durumun kilit noktası insandır. Fakat özellikle çocuk yaştaki dijital kullanıcılar kişisel bilgilerini yayınlamaktan çekinmemektedirler (Karakuş vd., 2017; Krasna ve Bratina, 2011, s.3). Bu durum insan faktörünün önemine dikkat çekmektedir. Schneier (2004) da dijital güvenliğin en zayıf halkasının insan olduğunu, bir başkasının veya bir yazılımın kişiyi tam anlamıyla koruyamayacağını belirtmektedir ve bunu şu sözleri ile daha net bir şekilde anlatmaya çalışmıştır: “*İnsanlar ve hemen hemen her şey arasındaki etkileşimi güvence altına almak gerçekten büyük bir sorundur*” (s.255). Buradan anlaşılabacağı üzere kişiyi aslında en iyi kendisi koruyabilmektedir ve bunu da ancak farkındalık ile yapabilecektir.

Dijital ortamda psikolojik ve sosyal durumu etkileyecek riskleri barındıran ve psikososyal olarak adlandırdığımız bu boyutta dijital zorbalık tehditi ele alınmıştır ve dijital zorbalığı kapsamına alan çalışmalar bulunmaktadır. Erol vd. (2015), dijital zorbalık ile ilgili boyutu “*kişisel gizliliği koruma*” olarak adlandırmıştır. Ekinci ve Kayapalı Yıldırım (2019) ise dijital zorbalığı siber mobbing ölçeğinde “*karşılaşılan siber mobbingin biçimi ve sıklığı*” ve “*siber mobbinge karşı verilen tepki düzeyi*” faktöründe ele almıştır. Güldüren, Çetinkaya ve Keser (2016) de bu boyutu “*mahremiyet*” olarak adlandırarak çalışma kapsamında incelemiştir. SBDÖP’nda da “siber zorbalık” kavramının kullanıldığı görülmektedir. Yine

¹ Pedofili, bir yetişkinin çocukları cinsel açıdan çekici bulmasına neden olan psikoseksüel bir rahatsızlıktır. <https://tr.wikipedia.org/wiki/Pedofili>.

bu konu SBDÖP’nda 7. sınıf “Birey ve Toplum” öğrenme alanında “Medyanın Hayatımızdaki Yeri” konu başlığında (7. sınıf sosyal bilgiler ders kitabı, s.21-27) ele alınmıştır. Bu açıdan çocuk yaş grubunu etkileyen bu risk ve mücadele yöntemleri psikolojik ve sosyal çevre ile iletişimle ilgili olduğu için psikososyal boyutta ele alınmıştır.

Psikososyal boyutta dijital güvenlik yeterlik göstergeleri:

- Sosyal medyada yabancı kişilerden gelen arkadaşlık isteklerini kabul etmeme,
- İnternet ortamında kişisel bilgileri (TC No, doğum tarihi, telefon no, konum, okul numarası vb.) paylaşmama,
- Dijital ortamda tehdit ve şantaja maruz kaldığında durumu güvenilir bir yetişkin ile paylaşması gerektiğini bilme,
- Dijital ortamda zorbalığa maruz kaldığında saldırgana boyun eğmeme,
- Güvenlik politikası uygun olmayan sosyal medya sitelerine katılmama,
- Kötü niyetli olduğundan emin olunan kişilerin hesaplarını engelleme,
- İnternette tanışılan kişilerin sahte olma ihtimaline karşı temkinli olma,
- İnternette kişi veya grupların, interneti kötü niyet için kullanma ihtimalini düşünme.

2.4.3.3. Çevrim İçi Alışveriş Boyutunda Dijital Güvenlik Yeterliği

Kişilerin internet alışverişi sırasında karşısına çıkabilecek risk ve tehditlerden olumsuz etkilenmemesi için alışverişin her aşamasının bilinçli ve güvenli alışveriş yollarını tercih eden bir tüketici olarak tamamlama yeterliğine sahip olması gerekmektedir. Bu boyutta çevrim içi dolandırıcılık, kimlik hırsızlığı, kredi kartı bilgileri gibi verilerin hırsızlığı, kişisel verilerin kopyalanması, özel bilgi ve ilgi alanlarının depolanması ve depolanan bu bilgilerin diğer firmalar ile paylaşılması söz konusu risk ve tehditler arasındadır. Bu risk ve tehditler alanyazında çevrim içi alışveriş, mesafeli alışveriş, dijital ticaret kapsamında ele alınmaktadır. SBDÖP’nda ise “*mesafeli alışveriş*” kavramı kullanılmaktadır. Ayrıca SBDÖP’nda 5. sınıf “Bilim, Teknoloji ve Toplum” öğrenme alanında “mesafeli alışveriş” olarak ele alınmıştır (5.sınıf sosyal bilgiler ders kitabı, s. 104-105). Bu sebeple internet üzerinden yapılan alışverişler ve bu alışverişler sırasında kişilerin karşılaşılabileceği risk ve tehditler çevrim içi alışveriş boyutunda ele alınmıştır.

Çevrim içi alışveriş sırasında kişilerin karşılaşılabileceği riskler arasında kişinin kredi kartı bilgilerinin güvenilir olmayan ve güvenli ödeme sertifikası bulunmayan siteler tarafından kopyalanması bulunmaktadır. Yine günümüzde sıkça duyduğumuz risklerden bir diğeri de dolandırıcılık amaçlı kurulmamış ve sıkça kullanılan alışveriş sitelerinin güvenlik açığı sebebiyle siber saldırılara maruz kalması ile üye bilgilerinin çalınarak kötüye kullanılmasıdır. Diğer bir risk ise ödeme sırasında güvenli yolların tercih edilmemesidir. Bununla birlikte çevrim içi alışveriş sırasında kullanıcıların önemsemeden kaydettiği kredi kartı bilgisi, telefon numarası, ikametgah adresi, iş adresi gibi kişisel veriler dijital ortamda kişinin fazlaca tanınmasına sebep olabilmekte ve bu yolla çok farklı zorbalık senaryolarıyla karşılaşmasına sebep olabilmektedir. Ne yazık ki günümüzde çevrim içi alışveriş sadece yetişkinler yapmamaktadır. EU Kids Online (2020) raporunda Avrupa'daki çocuklara uygulanan anketler neticesinde ankete katılan çocukların %3'ünün çevrim içi ortamda para kaybettiğini ifade etmiştir. TÜİK (2021) ise 6-15 yaş grubu çocukların çevrim içi alışveriş yaptığını ifade etmiştir. Thaichon (2017) çevrim içi alışveriş konusunda çocukların alım gücünün giderek arttığını ve bu durumun kaçınılmaz olduğunu ifade etmiştir (s.45). Bu bilgiler güvenli çevrim içi alışveriş yöntemleri konusunda çocuk yaş grubunun bilinç ve farkındalık düzeylerini yükseltecek bir eğitimin önemini göstermektedir. Bu sebeple bu çalışmada çocuk yaş grubunun 18 yaş öncesi ailesiyle birlikte yapacağı çevrim içi alışveriş sırasında güvenli yolları seçme ve önermesi ve 18 yaşına geldiğinde ise bu yöntemleri bireysel olarak kullanarak çevrim içi alışveriş yapabilmesi için gerekli bulunmuş, çalışma kapsamında çevrim içi alışveriş boyutuna dahil edilmiştir.

Çevrim içi alışveriş boyutunda dijital güvenlik yeterlik göstergeleri:

- Ailesiyle birlikte yaptığı çevrim içi alışverişlerde kredi kartı bilgilerinin temizlenmesini önerme.
- Ailesiyle birlikte yaptığı çevrim içi alışverişlerde kullanıcı yorum ve şikayetlerinin kontrol edilmesini önerme.
- Ailesiyle birlikte yaptığı çevrim içi alışverişlerde güvenli ödeme yöntemlerini önerme.
- Ailesiyle birlikte yaptığı çevrim içi alışveriş sırasında tercih edilecek sitenin güvenilirliğinin kontrol edilmesini önerme.

- Ailesiyle birlikte yaptığı çevrim içi alışverişte “bilgilendirme metninin” dikkatlice okunması gerektiğini önerme.

2.4.3.4. Hak ve Sorumluluk Boyutunda Dijital Güvenlik Yeterliği

Kişilerin çevrim içi ortamda sahip olduğu hakları bilme ve koruma, haklarının ihlal edilmesi durumunda şikayet edilecek mecraları bilme ve bu mecraları kullanabilme, çevrim içi ortamda diğer kullanıcılara ve sosyal kültürel olarak sorumlu olduğu konuları bilme ve buna uygun davranışlarda bulunabilme, diğer kullanıcıların haklarına saygı duyma dijital güvenlik açısından hak ve sorumluluk boyutunda yeterli sayılabilmesi için gerekmektedir. Bu boyutta kişilerin karşılaşılabileceği söz konusu risk ve tehditler dijital haklarının ihlal edilebilmesi ve bu ihlalleri gerekli kişilere/mecralara bildirmemesi halinde zorbalık durumunun devam edebilmesi, dijital sorumluluklarına aykırı uygunsuz davranışlarından sorumlu tutulmasıdır.

Diğer ülkelerde olduğu gibi ülkemizde de vatandaşların dijital ortamda sahip olduğu bir takım temel haklar mevcuttur. Bu haklar BTK (2019) tarafından, “*özel hayatın gizliliği, kişisel verilerin korunması, kişisel hakların ihlal edilmemesi, bilişim suçlarını şikayet hakkı, internette düşünce ifade özgürlüğü, internette itibar kaybını engelleme ve şikayet hakkı*” olarak ifade edilmiştir. Bu hakları ihlal eden bilişim suçlarını BTK (2019) “*Bilişim Hukuku ve Bilişim Suçu*” başlığında şu şekilde sıralamıştır; “*bilgi ve iletişim teknolojilerine izinsin erişim, dijital cihaz sabotajı, dijital hırsızlık, yazılım ve programları kaçak kullanım, kişisel bilgilerin kötü amaçlı kullanılması, sahte profil ile başkalarını dolandırma, yasal olmayan içerikler, ticaret amaçlı kullanılan özel bilgilerin ifşası, terörizme hizmet eden eylemler, çocuk istismarı, başkalarının hesaplarını çalma ve diğer suçlar (organ, fuhuş, tehdit, uyuşturucu, vb.)*”.

Günümüzde dijital hak ve sorumluluk boyutunda karşılaşılabilecek risk ve tehditler fazlaca bulunmaktadır. Bunun sebebi ise internet ortamına kötü niyetli kullanıcıların kolayca dahil olabilmesidir (Nawaila vd., 2021). Franklin ve Smeaton (2017), çocuk istismarının, suça teşvikin, kötü alışkanlıklara bulaştırmanın, dijital zorbalığın günümüzde çok arttığını ifade etmektedir (s.1-2).

Dijital ortamda hem yetişkinler hem de çocukların dijital hak ve sorumlulukları tehdit edici davranışlarda bulunabilmektedir. Nawaila vd. (2021), istismar ve dijital zorbalık tehditine

karşı çocukların mücadele edebilme yeterliğine sahip olması gerektiğini ifade etmiştir (s.12). SBDÖP’nda bu boyutla ilgili olarak “*kişisel bilginin gizliliği, kaynak kullanımında güvenlik problemleri, telif ve patent hakları, dijital haklar ve sorumluluklar*” gibi kavramlar yer almaktadır ve ilgili kazanımlara yer verilmiştir. Ayrıca dijital hak ve sorumluluklar konusunda kişisel güvenliği sağlama 7. sınıf “Birey ve Toplum” öğrenme alanında “Özgürüm, Sorumluluklarımın Olduğu Yere Kadar” konu başlığı ile (7. sınıf sosyal bilgiler ders kitabı, s. 25-29), telif ve patent hakkı ise 6. sınıf “Bilim, Teknoloji ve Toplum” öğrenme alanında ise “Emeğe Saygı Duyuyorum” konu başlığı ile (6. sınıf sosyal bilgiler ders kitabı, s.150-154) ele alınmıştır. Bu sebeple bu çalışmada yukarıda bahsi geçen konular dijital güvenlik açısından dijital hak ve sorumluluklar boyutunda ele alınmıştır.

Hak ve sorumluluk boyutunda dijital güvenlik yeterlik göstergeleri:

- Başkalarının özel bilgilerine ve özel hayatıyla ilgili bilgilere izinsiz erişmenin suç olduğunu bilme,
- Başkalarına ait bilgi ve belgeleri (video, fotoğraf, ses vb.) izinsiz kullanma ve yaymanın suç olduğunu bilme,
- Bilgi ve iletişim teknolojileri ile ilgili hakların devlet tarafından yasalarla korunduğunu bilme,
- Başkalarına ait belgelerin (video, fotoğraf, ses, bilgi vb.) aslını değiştirici müdahaleler (montaj, intihal vb.) yapmanın suç olduğunu bilme,
- Değer kavramları (din, vatan, bayrak, aile, ırk vs.) hakkında rencide edici davranmanın suç olduğunu bilme,
- Dijital ortamda uygunsuz içerikli (şiddet, nefret söylemi, cinsellik vb.) paylaşımların yasal olmadığını bilme,
- Dijital ortamda şahsına zarar verici durumları şikayet hakkının olduğunu bilme,
- Dijital ortamda işlenen suçları şikayet edebileceği kişi ve mecraları bilme.

2.4.3.5. Sağlık Boyutunda Dijital Güvenlik Yeterliği

Kişilerin dijital araçları (akıllı telefon, tablet, bilgisayar vb.) ve interneti zaman yönetimi, fiziki olarak kullanma şekli ve tercih edilen içerikten kaynaklı fiziksel ve ruhsal sağlığının kötü etkilenmemesi için bu araç ve platformları uygun kullanabilmesi sağlık boyutunda

dijital güvenlik açısından yeterli sayılabilmesi için gereklidir. Bu boyutta sağlıklı dijital kullanım davranışları arasında zamanı yönetememe, dijital araçları fiziksel olarak sağlığa zararlı şekilde kullanma, zararlı içerik tercihi, içerik tercihi için filtreleme yöntemlerini bilmeme ve akıllı işaretlere uygun davranmama gibi davranışlar yer almaktadır. Bu uygunsuz davranışlar neticesinde kişinin fiziksel ve psikolojik sağlığında problemler görülebilmektedir. Alanyazında bu durum “problemlili internet kullanımı” olarak adlandırılmıştır. Problemlili internet kullanımı, “*dijital araçların ve çevrim içi ortamın kullanımında aşırı meşgulliyet, dürtü ve davranışları kapsayan sıkıntılı davranışlar bütünüdür*” (McLean’den aktaran Nannatt vd., 2022, s.341). Problemlili internet kullanımının sağlık yönünden risk teşkil ettiği bilinmektedir (Muslu ve Bolışık, 2019, s.446; Vally vd., 2020, s.588). Alanyazında problemlili internet kullanımı ile psikolojik sağlık arasında negatif yönlü bir ilişki olduğu belirtilmektedir (Akın ve İskender, 2011; Tahiroğlu vd., 2010).

Güvenli Web (2017), dijital ortamın uygunsuz kullanımı sonucunda kişinin fiziksel ve psikolojik sağlığında problemler yaşanabileceğini ve yaşanabilecek bu problemler arasında fiziksel olarak; “*boyun ve sırt ağrısı, ellerde ağrı ve karpal tünel sendromu, görme bozukluğu, baş ağrısı ve migren, obezite*” problemleri, psikolojik olarak ise; “*anksiyete, stres depresyon, asosyalite, depresyon, internet bağımlılığı*” problemlerinin yaşanabildiğini ifade etmiştir. Bunun yanında internette aşırı zaman geçirme ve zararlı içerik tüketimi neticesinde saldırganlık, şiddete eğilim psikolojik problemler ve bunların sonucunda da sosyal becerilerde zayıflama ve akademik başarıda düşüş gibi problemler yaşanmaktadır. Fernandes, Biswas, Mansukhani, Casarín ve Essau (2020), problemlili internet kullanım düzeyi yüksek olan kişilerde desresyon, yalnızlık, düşük uyku kalitesi, isteksizlik ve kaygı bozukluğu olduğunu belirtmişlerdir (s.62). Buzkıran (2017) çalışmasında internet kullanım süresi arttıkça problemlili internet kullanım oranının da arttığını, problemlili internet kullanımı arttıkça da sosyal bilgiler dersi başarı ortalamasının düştüğünü belirtmektedir (s.429).

SBDÖP’nda (2018) bu boyutla ilgili olarak “*güvenli internet kullanımı*”, “*güvenli teknoloji kullanımı*”, “*dijital oyunların güvenlik açısından etkileri*”, “*dijital bağımlılık*”, “*zararlı içeriklerin etkileri*” gibi kavramlar yer almaktadır ve ilgili kazanımlara yer verilmiştir. Ayrıca sosyal bilgiler 4. Sınıf “Bilim, Teknoloji ve Toplum” öğrenme alanında “Zarar Vermeden Kullanım” konu başlığı altında dijital cihazların sağlığa etkisi ele alınmış (4. sınıf sosyal bilgiler ders kitabı, s.114-118), 5. sınıf “Bilim, Teknoloji ve Toplum” öğrenme

alanında (5. sınıf sosyal bilgiler ders kitabı, s.103) “Genel Ağ’ı Nasıl Kullanmalıyım?” konu başlığı altında dijital bağımlılık konusuna vurgu yapılmıştır. Bu sebeple bu çalışmada yukarıda bahsi geçen konular dijital güvenlik açısından sağlık boyutunda ele alınmıştır.

Sağlık boyutunda dijital güvenlik yeterlik göstergeleri:

- Eğlence amaçlı internet kullanımlarında (sosyal medya, dijital oyun, video vb.) aşırı zaman harcamaktan kaçınma,
- Dijital cihazları (akıllı telefon, tablet, bilgisayar vb.) kullanırken oturuş biçimi ve izleme mesafesini sağlığa uygun şekilde ayarlama,
- Dijital cihazları kullanırken ses, ışık ve ekran parlaklığını sağlığa zarar vermeyecek şekilde ayarlama,
- Yaşa uygun olan içerikleri tercih etme,
- Uygun olmayan içerikleri fark ettiğinde kullanmayı bırakması gerektiğini bilme,
- Karşılaşılan içeriklerin uygunluğunu anlamak için akıllı işaret bilgilendirmelerini dikkate alma.

Dijital güvenliğin boyutları doğrultusunda tüm öğrenciler, gençler ve diğer dijital kullanıcıların dijital güvenliğini sağlaması için gerekli olan yeterlik göstergeleri dijital araçları kullanabilen ve internet erişimi sağlayabilen kişilerin kolaylıkla uygulayabileceği adımlardır. Her biri birer dijital vatandaş olan dijital kullanıcılar teknoloji çağında her gün her an dijital risklerle karşı karşıya kalmaktadır. Yukarıda boyutlar dahilinde bahsedilmiş yeterlik göstergeleri dijital kullanıcıların aslında tümüyle uygulaması gereken güvenli kullanım adımlarıdır. Aynı ayrı uygulandığında ya da sadece tek bir boyuta bağlı kalıp dijital güvenliği sağlamak mümkün değildir çünkü dijital dünyada riskler birbiriyle ilişkilidir. Örneğin sosyal ağlarda bizi tehdit eden sadece psikososyal boyut kapsamında siber zorbalık değildir ve bu sadece psikososyal boyuttaki yetersizlikten dolayı başımıza gelmez. Bu sebeple dijital güvenlik yeterliklerinin tümünün eğitim aracılığıyla öğrencilere kazandırılması gerekmektedir.

2.5. Öz Yeterlik ve Dijital Güvenlik Öz Yeterliği

Öz yeterlik kavramı insanın inanç, algı, beklenti ve duygu durumlarının davranışlarla ilişkili olduğunu ileri süren bir kavramdır ve kavram ilk kez Bandura tarafından ele alınmıştır.

Sosyal bilişsel öğrenme teorilerinin öncülüğünü yapan Bandura, insanların sosyal ortamda gözlem ve deneyimleri sonucunda davranışlarını kontrol ettiğini, düzenlediğini öne sürmekle birlikte sosyal öğrenmelerin davranış değişikliklerinde çok etkili olduğunu ve inançların öğrenme üzerinde diğerlerine göre daha fazla etkiye sahip olduğunu belirtmiştir. Özellikle bir şeye olan inancın o şeyin kendisinden daha hızlı davranışsal değişikliğe ve sonuca yaklaştırdığı da yine bu teoride açıklanmıştır (Bandura, 1977, s.192). Burada belirtilen inanç bir sonuç beklentisi veya ödüldür. Bu teoride sonuç beklentisi bir kişinin bir davranışın belirli sonuçlara yol açacağına yönelik inancıdır. İnanç neticesinde tercih edilecek olan davranış ise sosyal gözlemden ulaşılan öngörüye göre de şekillenir (Bandura, 1977, s.193). Bu biraz da öngörü kapasitesiyle alakalıdır ve bunun sonucunda davranışlarına yön verme ve öz düzenleme yaşanır. Etkinlik beklentisi ise bir sonucu meydana getirmek için gereken davranışı başarılı bir şekilde meydana getirebileceğine olan inançtır (Bandura, 1977, s.193). Sonuç beklentisi için kişide beliren etkinlik beklentisine olan inanç ise kişinin durum ile başa çıkma davranışını etkileyebilir ve bu durum davranış ortamlarını seçme konusunu da başlangıçta etkileyebilir (Bandura, 1977, s.193). Öyle ki bir kişi bir sonuca ulaşmak için heveslendiği durumda kendisinin gerekli olan davranışı yapıp yapamayacağına olan inancı kişiyi ya davranışa götürür ya da davranıştan kaçınma eğilimi belirir. Kısacası öz yeterlik algısı ile etkinlik ve sonuç beklentisi birbirlerini etkileyen faktörlerdir.

Bandura'ya (2001) göre algılanan öz yeterlik ne kadar yüksek olursa performans eğilimi o kadar aktif olur. Ancak bileşen yetenekleri eksikse yine tek başına istenen performans gerçekleşmeyecektir. Bu noktada aynı zamanda kişinin performans için yeterli becerilere sahip olması gerekmektedir. Bu noktada da yeterlik durumu davranışın seçiminde etkili hale gelmektedir. Bununla birlikte daha geniş bir pencereden bakıldığında, gerekli beceri, teşvik de etkinlik beklentisini, etkinlik seçimini, çaba seviyesini ve mücadele etme süresini belirleme konusunda önemlidir (Bandura, 1977, s.194). O halde yeterlik durumu ve öz yeterlik algısının davranış değişikliği için gerekli unsurlardan olduğu söylenebilir.

Öz yeterliğin insan davranışları üzerinde etkisi sosyal bilişsel öğrenme teorisine göre açıklanmıştır. Günümüzde eğitim ve psikoloji alanlarında yapılan çalışmaların bir kısmının temelinde bu teorinin var olması bu anlayışı da doğrulamaktadır. Öz yeterlik alanyazına bakıldığında harekete geçme ve eylemi yerine getirme için gerekli olan bir durumdur. Bandura (2001) tarafından bu durum *“söz konusu eylem için kişinin kendine olan inanç*

durumu” olarak ifade edilmiştir (s.10). Alanyazında öz yeterlik kavramı öz yeterlik algısı, öz yeterlik inancı gibi farklı farklı kullanılsa da aslında bu iki kullanım da aynı şeyi ifade etmektedir ve birbirlerinin muadili olarak kullanılmaktadır. Öz yeterlik algısı, kişinin kendini geliştirmesi, öğrenmesi ve başarması için aslında temel niteliği taşımaktadır. Başarı ya da davranış değişikliği için kalan tüm basamakların organize edilmesinde, planlanmasında, motivasyonunda ve sürdürülmesinde öz yeterlik algısı etkilidir. Aynı zamanda gelecek kaygılarını, seçimlerini, kariyerlerini, yaşam kalitesini, zorluklarla mücadelede kaygı düzeyine kadar birçok şeyi etkisi altında bırakır.

Bir kişinin bir davranışı yapabileceğine olan inancı anlamına gelen öz yeterlik algısı sosyal psikoloji alanında doğmuş ve genellikle farklı farklı alanlarda uyarlanarak kullanılmaktadır. Her ne kadar farklı alanlara uyarlanmış olsa da temelinde kişinin kendine olan başarı algısı niteliğini kaybetmeyecektir. Bandura’ya (1977) göre “*öz yeterlik inancı dört faktörden etkilendir ve bu faktörler; 1.ustalık deneyimi (kişinin kendisine ilişkin deneyimleri), 2.dolaylı deneyimler (kişinin başkalarının deneyimlerine ilişkin gözlemleri), 3.sözel ikna(kişiyi başkalarının motive etmesi), 4.psikolojik ve duygusal durumlardır*” (s.197-198). Bu dört faktörden olumlu şekilde etkilenecek öz yeterliği yüksek olan kişiler genelde seçtiği davranışları gerçekleştirme konusunda başarılı olabilmektedirler.

Öz yeterlik bugün psikolojide olduğu kadar eğitim bilminde de sıklıkla kullanılmaktadır. Özellikle dijital dönüşüm ve teknolojik gelişmeler neticesinde eğitimde sıklıkla yordanan durumlar arasında teknolojinin eğitimde kullanılması yer almaktadır. Aynı zamanda teknoloji kullanımlarının öğrenme durumlarını ne derece etkilediği ve nasıl yönlendirdiği de tespit edilmek istenenler arasındadır. Bu konuda araştırma kapsamına sadece çocuklar değil, öğretmenler ve öğretmen adaylarının da dijital becerileri dahil edilmektedir. Çünkü eğitime yön veren ve rehberlik eden kişi öğretmenlerdir. Gerekli davranışların şekillenmesinde ve istendik durumların ortaya çıkmasında günümüzde dijital araçlar ve bu araçların kullanımına dair beceriler etkilidir. Bununla birlikte eğitim paydaşlarının dijital ortamları kullanım davranışları da hem gündelik hayatı hem de eğitim yaşantılarını etkilemektedir ve bugün öğretim programlarına dijital beceriler entegre edilmiş durumdadır. Öğretim programlarına entegre edilmiş dijital beceriler konusunda çeşitli kazanımlar bulunmakta ve özellikle ortaokul derslerinin öğretim programlarında bu becerilere yönelik kazanımlar sıklıkla bulunmaktadır. Kazanım olarak amaçlanan dijital becerilerin ne kadarının kazandırıldığı

birçok araştırmacının çalışma konusu haline gelmiştir. Fakat bu becerileri doğrudan dijital ortamda ölçmek ve tespit etmek zor bir durumdur ve yaş gurubuna ait verilerin elde edilmesinde etik durumlardan dolayı zorluk yaşanmaktadır. Bu açıdan öz yeterlik inanç ve algılarına sıklıkla başvurulmaktadır. Bu amaçla algılanan öz yeterlik kavramı ölçüm araçlarını şekillendirmektedir. Çünkü eğitim açısından yeterlik durumlarını gözlemlemek, deney sürecini kontrol etmek ve ölçümlemek zahmetli, uzun bir süreçtir. Öz yeterlik durumlarını tespit etmek ise daha pratiklik sağlamaktadır. Günümüzde eğitimde kullanılan öz yeterlik ölçekleri likert tipinde sıkça kullanılmaktadır (Arslan, Dil, Çetin ve Yazıcı, 2017, s.2798). Bu sebeple bu araştırmada öğrencilerin öz yeterlik algıları likert tipinde ölçekler aracılığıyla tespit edilmeye çalışılmıştır.

Bu araştırmada dijital güvenlik öz yeterliliğinin tespit edilmesi amaçlanmıştır. Alanyazın incelendiğinde dijital güvenlik öz yeterlik inancı özel olarak ele alınmadığı görülmüştür. Dijital güvenlik, yeterlik ve öz yeterlik tanımlarından hareketle dijital güvenlik öz yeterliği; dijital ortamda güvenliğini sağlayabilme sürecinde kullanılacak bilgi, beceri ve tutumlara sahip olma konusunda kişinin kendine olan inancı olarak tanımlanabilir. Bu hususta alanyazın incelendiğinde dijital vatandaşlık öz yeterlik algılarını tespit etmeyi amaçlayan bazı çalışmalar mevcuttur (Kolata, 2022; Tatlı, 2018). Bununla birlikte alanyazın incelemesinde dijital güvenlik ile ilgili konularda öz yeterlik algısını tespit etmeyi amaçlayan bazı çalışmalara rastlanmıştır. Bunlar; Çolak (2019) tarafından yapılan üniversite öğrencilerinin dijital güvenlik öz yeterliklerini tespit etmeyi amaçlayan doktora tez çalışması ve Doğanç ve Korucu (2020) tarafından öğretmen adaylarının güvenli internet kullanımı öz yeterlik algısını belirlemeyi amaçlayan ölçek geliştirme çalışmasıdır.

2.6. Çevrim İçi Öğrenme

Çevrim içi öğrenme web tabanlı öğrenme, internet tabanlı öğrenme, teknoloji destekli öğrenme, e-öğrenme, sanal öğrenme kavramlarıyla sıklıkla karıştırılmaktadır. Bu kavramlar ayrı kavramlar değil, açık ve uzaktan öğrenmenin uygulama biçimleridir (Holmberg'dan aktaran Bağrıacık Yılmaz, 2020, s.5). Üstündağ (2012) da buna benzer olarak çevrim içi öğrenmeyi uzaktan eğitim kapsamında ele almıştır. Horton (2006) çevrim içi öğrenmeyi, *“bilgi ve bilgisayar teknolojilerinin öğrenme deneyimleri oluşturmak için eğitimde işe koşulması”* olarak tanımlanmıştır (s.1). Means, Toyama, Murphy, Bakia ve Jones (2009) ise

çevrim içi öğrenmeyi “*kısmen veya tamamen internet üzerinden gerçekleşen öğrenme*” olarak tanımlamış ve çevrim içi öğrenmenin iki amaçla yapıldığını ifade ederek bu amaçları şöyle açıklamıştır; çevrim içi öğrenmenin yüzyüze öğrenmeye alternatif olarak yapılması ve öğrenmeyi geliştirmek için yüzyüze öğretimle birleştirilmiş veya harmanlanması (s.9). Carliner (2004) çevrim içi öğrenmeyi, “*öğrenme ve destekleyici araçlara bilgisayar ve ağ teknolojileri aracılığıyla erişim*” olarak ifade etmiştir (s.1). Lynch ve Dembo (2004) ise çevrim içi öğrenmeyi “*internetin kullanılarak ulaşıldığı tüm teknoloji destekli öğrenme etkinlik ve araçları ile öğrenmenin gerçekleştiği ortam*” olarak tanımlamıştır (s.2).

Carliner (2004), çevrim içi öğrenmenin öğretici liderliği, öğrenci liderliğinde, asenkron ve senkron olarak 4 farklı biçiminin bulunduğunu ifade etmiştir (s.19-23). Öğretici liderliğinde çevrim içi öğrenme, öğretmen liderliğinde bir grup öğrencinin çevrim içi ortamda aynı zamanda öğrenme deneyimlerini oluşturmalarıdır. Öğrenci liderliğinde çevrim içi öğrenme, öğrencinin çevrim içi ortamda kendi istediği hızda öğrenmesidir. Senkron çevrim içi öğrenme, öğreticinin ve öğrencinin aynı zamanda çevrim içi olmaları ve aynı zamanda eğitime katılmalarıdır. Asenkron çevrim içi öğrenme ise, öğreticinin ve öğrencinin aynı zamanda öğrenmeye dahil olmaması ve öğrencinin kendi hızında öğrenme deneyimini oluşturmalarıdır. Horton (2006) çevrim içi öğrenme biçimlerinin uygulandığı çeşitli uygulamaların olduğunu belirtmekte ve bunları şu şekilde sıralamaktadır; “bağımsız kurslar, sanal sınıf dersleri, öğrenme oyunları ve simülasyonları, gömülü çevrim içi öğrenme, karma öğrenme, mobil öğrenme ve bilgi yönetimi” (s.2). Bunların her biri biçimsel olarak farklı oluşturulmuş çevrim içi öğrenme ortamlarıdır.

Çevrim içi öğrenmenin öğretim açısından birçok yararı bulunmaktadır. Oliveira, Siqueira ve Braz (2018), çevrim içi öğrenmenin yararlarını esneklik, ekonomiklik, zaman ve mekan kısıtlaması olmadan ulaşılabilirlik olarak sıralamıştır (s. 353). Öyle ki günümüzde çevrim içi öğrenme zaman ve mekan bağlamında pratik olması açısından tercih edilebilmektedir. Çevrim içi öğrenmede öğrenme deneyimlerini artırmak için teknolojik imkanların verimli şekilde çevrim içi öğrenme biçimleri çerçevesinde kullanılması gerekmektedir. Horton (2006) teknolojinin imkanlarını kullanmasından dolayı çevrim içi öğrenmenin bazen sınıf içi eğitimden iyi olabileceğini bazen ise daha kötü olabileceğini belirtmiştir (s.3). Burada belirleyici unsur teknolojinin çevrim içi öğrenmede ne kadar etkili kullanıldığıdır.

Etkili bir çevrim içi öğrenme için hem iyi bir tasarıma ihtiyaç vardır hem de geliştirmeye. Carliner (2004)' a göre çevrim içi öğrenmede hem basit şekilde öğrenciye bir araç sunulabilir, hem öğrenci etkileşimine göre araç şekillenmiş olabilir hem de öğrenciye uygun öğrenme materyali öneren bir program olabilir (s.1-2). Burada çevrim içi öğrenmede öğrencinin öğrenme deneyimini oluşturmak için sunulan araca materyal denilmektedir. Konu ile ilgili basit veya karmaşık her türlü öğrenme materyali çevrim içi ortamda kullanılabilir. Carliner (2004), çevrim içi öğrenmede basitten karmaşığa öğrenmelerin oluşturulabileceğini şöyle belirtmiştir; *“basit düzeyde grafik, metin sınırlı miktarda etkileşim ile verilebilmekte, karmaşık olarak ezberci becerilerin tatbikat haliyle öğretilmesi, daha karmaşık sistemlerde simülatörlerin kullanıldığı öğrenmeler, daha da karmaşık olarak düşünme becerilerinin öğretildiği tasarımlar oluşturulabilir”* (s.1-2).

Miller ve Miller (2000) çevrim içi öğrenmeyi sınıf eğitiminden ayıran 3 özelliğın olduğunu belirtmiştir: 1. doğrusal olmayan, ilişkisel ve hiyerarşik yapı, 2. gelişmiş çoklu ortam seçenekleri, 3. eşzamanlı ve eşzamansız iletişim olanakları (Miller ve Miller'dan aktaran Üstündağ, 2012, s.1). Bu özellikler çevrim içi öğrenmeyi farklılaştıran ve zenginleşmesini sağlayan özelliklerdir. Üstündağ (2012) çevrim içi öğrenmede yeterli düzeyde etkileşim, uygun ortam ve araç ile, öğrenmeyi sağlayacak niteliklere hakim, derse katılımı iyi düzeyde sağlayabilecek bir ortam ile öğrenmenin deneyimlerinin artırılabilceğini ifade etmiştir (s.2).

Çevrim içi öğrenme ile sınıf eğitiminin farklarını ortaya koyan ve bu iki ortamı karşılaştıran çeşitli araştırmalar bulunmaktadır. Carliner (2004: 6) ve Horton (2006: 3)'a göre çevrim içi öğrenmeyi sınıf eğitime göre daha etkilidir diyebilmek için çevrim içi öğrenmenin içeriğine bakmak gerektiğini ifade etmektedir. Örneğın, yalnızca eşzamansız olarak yürütölen çevrim içi derslerde sadece süre kısalmaktadır. Carliner (2004), aynı materyalle hem sınıfta hem de çevrim içi ortamda verilen eğitimlerin karşılaştırılmasında çevrim içi öğrenmenin sınıf eğitimi kadar etkili olduğunu fakat çevrim içi öğrenme sırasında öğrencilerin değerlendirmeler de yapmaları gerektiğini ifade etmiştir (s. 6-7). Buradan hareketle şunu söyleyebiliriz ki çevrim içi ortamda uygun araç ve yöntemler ile öğrenmenin etkililiğı artırılabilir.

Etkili bir çevrim içi öğrenme için dikkat edilecek hususlardan belki de en önemlisi ise bu öğrenme ortamlarının öğrenen özelliklerine göre yapılandırılmış olmasıdır. Bu noktada öğrenenlerin bireysel farklılıklarının farklı farklı olabileceğı düşünölmeli ve tüm öğrenenleri

kapsayıcı bir ortam olmasına dikkat edilmelidir. Çünkü bireysel farklılıklar öğrenmeyi tümüyle etkilemekte ve şekillendirmektedir. Öyle ki bugün herkes için aynı öğrenme materyali başarılı olmayabilir.

Kuzgun ve Deryakulu (2004) eğitimde öğrencilerin bireysel farklılıklarına ilişkin düzenlemelerle ilgili şunları ifade etmiştir:

1. Öğitmen tarafından kullanılacak olan yöntem, yaklaşım ve stratejinin seçimi,
2. İçeriğin şekli, içeriğin sunuş hızı ve sürecin ne kadar süreceği,
3. Dikkat çekme,
4. Alıştırma ve uygulamaların türü, zorluk düzeyi, bağlamı ve sayısı,
5. Öğrenmenin grup halinde mi yoksa bireysel mi olacağı,
6. Öğretim sürecinde verilecek ipuçların niteliği ve miktarı,
7. Öğrenciden gelecek tepkilerin türü,
8. Öğretim ortam ve materyallerinin seçimi,
9. Geri bildirim ve pekiştireçlerin nerelerde ve hangi sıklıkta kullanılacağı,
10. İçerikte kullanılan kelime ve materyallerin düzeyi,
11. Ölçme ve değerlendirme yaklaşımlarının seçimi,
12. Ne tür bir rehberlik hizmetinin verileceği öğrenme ortamının bireysel özelliklere göre şekillenmesinde dikkat edilecek hususlardır (Kuzgun ve Deryakulu'ndan aktaran Üstündağ, 2012, s.3).

Bu bilgilerden hareketle çevrim içi ortamda kullanılan materyallerin niteliği, bu ortamda kullanılan etkileşim biçimi ve bireysel farklılıkların esas alınması çevrim içi öğrenme açısından önemlidir.

Çevrim içi öğrenme ortamlarında önemli konulardan biri de bu ortamda öğrenme süreci boyunca oluşabilecek problemler ve bu problemlerde çözüm önerilerinin neler olabileceğidir. Tabii ki her öğrenme ortamında olduğu gibi çevrim içi öğrenme ortamında da birtakım problemler yaşanabilmektedir. Çevrim içi öğrenme bahsettiğimiz gibi açık ve uzaktan öğrenmenin bir uygulaması biçimi olduğu için bu konu açık ve uzaktan öğrenme

ortamlarında yaşanabilecek problemler ile açıklanabilir. Özcan (2020), bu öğrenme ortamlarında yaşanabilecek problemleri sistem yaklaşımına dayanarak şöyle açıklamıştır:

1. Öğrenci ile ilgili problemler: Öğretim elemanı ile etkileşim, geri bildirim alamama, sistemde kendini yalnız hissetme gibi problemlerden kaynaklı olarak öğrencinin sistemi bırakması olası problemdir.
2. Öğretim elemanı ile ilgili problemler: Pedagojik sorunlar, politikalar, teşvik ve ödül eksikliği, destek ve yardım eksikliği, ödemeler ve zaman kısıtlılığı, duyuşsal engeller olası problemlerdir.
3. Teknik/teknolojik problemler: Teknik alt yapı, teknik destek ve erişim olası problemlerdir.
4. Program/ders tasarımı problemleri: İçeriğin ya da materyalin tekdüze tasarlanması, bireysel farklılığa göre hazırlanmayan içerikler, sadece geleneksel ölçme değerlendirme yöntemlerinin kullanılması ve telif haklarına dikkat edilmemesi olası problemlerdir.
5. Yasal politika sorunları: Finansman sorunları, öğrenci sayısı olası problemlerdir.
6. Yönetim ve organizasyon sorunları: Planlama, ekonomi, değerlendirme ve kalite güvencesi olası problemlerdir (Özcan, 2020, s.198-208).

Çevrim içi öğrenme sırasında öğrenciden, sistemden, eğitmenen, programdan, tasarımdan ve diğerlerinden kaynaklı pek çok sorun çıkabilmektedir. Önemli olan çevrim içi öğrenme sırasında oluşabilecek bu sorunların önceden öngörülüp çözüm önerileri geliştirmek ve olası problemlere alternatifler üretmektir. Bunun için sürecin önceden iyi bir şekilde planlanmış olması gerekmektedir.

2.7. Çevrim İçi Destekleyici Öğrenme Aracı

Çevrim içi öğrenme araçları çevrim içi ortamda öğrenmeyi sağlayan asıl araçlardır. Bu araçların daha fazla duyuyu harekete geçirmesi ve öğrenmeyi etkili kılabilmesi için iyi tasarlanmış ve geliştirilmiş olması gerekir.

Başarmak (2020), çevrim içi öğrenme aracını dijital öğretim materyali olarak adlandırmış ve dijital öğretim materyallerini *“bilgisayarlardan ve diğer mobil cihazlardan oluşturulan,*

görüntülenen, dağıtılan, değiştirilen, depolanan ve erişilen materyaller” olarak tanımlamıştır (s. 241). Jones, Fox ve Weeks (2017), bu materyalleri *“bilgisayar programları, dijital görüntüler, dijital ses, dijital video, web siteleri, veri tabanları, elektronik kitaplar”* olarak örneklemiştir (Jones vd.’den aktaran Başarmak, 2020, s.241).

Çevrim içi öğrenme araçlarının geliştirilmesinde en önemli husus içeriğin ve amacın belirlenmesidir. Çevrim içi öğrenme aracı öğretim içerikleri ve öğretimin asıl amacı doğrultusunda planlanmalıdır. İyi tasarlanmış ve planlanmış çevrim içi öğrenme aracı olması gerekenler öğrenme hedefleri, kullanılacak teknoloji ve süreç boyunca oluşabilecek sorunların belirlenmesidir (Carliner, 2004, s.8).

Carliner (2004), bunları şöyle açıklamıştır: İlk olarak çevrim içi öğrenme aracının programı için öncelikle öğrenme hedeflerinin dikkatli bir şekilde belirlenmesi ve öğrenmeyi en iyi destekleyen bağlamın seçilmesi gerekir; İkinci olarak çevrim içi öğrenmeyi desteklemek için hangi teknolojinin gerekli olduğunun belirlenmesi gerekir; Üçüncü olarak proje sorunlarının çevrim içi öğrenme programlarının tasarlama, geliştirme, başlatma, değerlendirme ve desteklemedir (s.8-14).

Başarmak (2020) da materyal geliştirme sürecine başlamadan önce kapsamlı bir şekilde analiz yapılması gerektiğini belirtmiş ve analizde dikkat edilmesi gereken unsurları şöyle açıklamıştır:

1. Hedef kitle: Öğrenim görececek olan hedef kitlenin özelliklerinin belirlenmesi ve materyalin bu özellikler doğrultusunda hangi kriterlere göre tasarlanacağına karar verilmelidir.
2. Teknoloji ortamı/araçları: Hedef kitlenin teknoloji ortamlarına ilişkin hazırbulunuşluk düzeyine göre teknoloji ortamı ve araçları belirlenmelidir. Burada dikkat edilecek hususlar ders içeriği ile ilişkilendirilmiş ve bütünleştirilmiş araç ve içerik belirleme, öğrenci motivasyonuna uygun araç seçme, kolay ulaşılabilir uygun web ortamı seçimidir.
3. İçerik: Öğrenen ihtiyaçları ve öğretim amaçlarına uygun içerik ve etkinlik tasarlanması gerekmektedir. Bu doğrultuda materyal ders içeriğini yansıtacak şekilde yapılandırılmalıdır. Böylece öğrenme ortamı için geliştirilecek video, animasyon, benzetim gibi materyaller içeriğe göre şekillenecektir.

4. Öğrenme yaklaşımı: Öğrenme yaklaşımı hedef kitle, teknoloji ortamı ve içerik analizi doğrultusunda belirlenmelidir. Burada amaç öğrenenlerin etkin katılımını sağlamak ve öğrenme adımlarında rehberlik etmek olmalıdır. Bu sayede öğrenen hedefe daha kolay ulaşacaktır (Başarmak, 2020, s.242-245).

Çevrim içi öğrenme materyalinin geliştirilmesi sürecinde başarılı bir analizin ardından tasarım ve geliştirme süreci başlar. Tasarım ve geliştirme sürecinde çevrim içi öğrenme materyalinin rolü, türleri ve materyali hazırlayabilme yeteneği son derece önemlidir. Tasarım ve geliştirme sürecine başlamadan önce bu sürecin hangi ilkeler ve sıralamalar doğrultusunda ilerleyeceğini belirleyen stratejik bir plan oluşturulmalıdır. Tasarım ve geliştirme aşaması için uygulanacak olan stratejik plan doğrultusunda geliştirilen materyalin anlaşılabilirliği ve kullanımının karmaşık olmaması da materyalin etkililiği açısından önemlidir.

Başarmak' a (2020) göre geliştirilecek olan materyalde olması gereken özellikler şunlardır:

1. Zamandan ve mekandan bağımsızlık,
2. Erişim kolaylığı,
3. Ortam ve sürece uyarlabilirlik,
4. Etkileşim öğelerini içinde barındırma,
5. Amaca ve hedef kitleye uygunluk (s.246).

Çevrim içi öğrenme aracının tasarım ve geliştirme süreci tasarım ilkelerine, bireysel özelliklere ve içeriğe göre elverişli şekilde hazırlandığında çevrim içi öğrenmenin kalitesi artacak ve öğrenen hedefe ulaşabilecektir. Carliner (2004)'a göre kapsamlı şekilde hazırlanmış çevrim içi öğrenme materyali çevrim içi yollarla desteklenirse öğrenme kalitesi daha da artacaktır (s.33). Ayrıca bu süreçte aracın, öğrencilere nasıl ulaştırılacağı, öğrenci katılımının nasıl olacağı, performans kayıtlarının ve süreç boyunca çıkan sorunların nasıl çözüleceği ve güncellenmenin nasıl yapılacağı da bu aracın geliştirilmesinde önemli hususlardandır. Carliner (2004) bu süreçte aynı zamanda kullanılan programın da hatasız çalışması gerektiğini, örneğin öğrencinin doğru cevabı verdikten sonra yanlış dönütü alması ya da yalnızca internetle çalışan aracın internete erişimi olmayan öğrenciler için öğrenme programının anlamsızlaşmasına sebep olacağını ifade etmektedir (s.29). Bu sebeple çevrim

içi öğrenme sırasında kullanılacak olan aracın kapsamlı olarak hazırlanması ve sistemin de güvenilir olması gerekmektedir.

Çevrim içi öğrenme araçlarını etkileyen diğer bir durum ise etkileşimdir. Etkileşimin, çevrim içi öğrenme araçlarında hangi yollarla sağlanacağı, bu yolların neler olduğu ve ne gibi özelliklere sahip olması gerektiği çevrim içi öğrenme aracında dikkatle yapılandırılması gereken önemli hususlardandır. Moore (1989) bu konuda 3 etkileşim türünden bahsetmektedir: öğretmen-eğrenci, öğrenci-eğrenci ve öğrenci-içerik (s.3-4). Çevrim içi öğrenme aracında bu etkileşim türlerinin hepsi mümkün olmakla birlikte, çevrim içi öğrenme ortamına göre de kullanım seçimi şekillenmektedir. Bu etkileşim türlerinin kullanımı çevrim içi öğrenme aracının etkililiği açısından önemlidir.

Çevrim içi öğrenme araçlarının günümüzde çok çeşitli biçimlerde şekillendirilmektedir. Öğretim elemanı-eğrenci etkileşim türünde çevrim içi öğrenmede özellikle zoom, googlemeet gibi araçlar kullanılmaktadır ve bu araçlar çeşitli materyallere erişimle zenginleştirilmektedir. Bu ortamlarda özellikle öğrenci-eğrenci etkileşim türü mesajlaşma, tartışma panoları, sohbet oturumları, e-posta yolları ile de sağlanabilmektedir. Öğrenci-içerik etkileşim türünde ise çevrim içi öğrenme aracı ile öğrencinin çevrim içi ortamda başbaşa bırakılmasıdır.

Çevrim içi öğrenme aracının zenginleştirilmesi için çeşitli etkileşim yöntemleriyle desteklenmesi gerekmektedir. Bu konuda web teknolojilerinden yararlanmak öğrenmeyi desteklemektedir. Çevrim içi öğrenme aracını destekleyen bir başka durum ise sadece araç ve arayüz ile öğrenciyi başbaşa bırakmanın dışında aynı zamanda süreç boyunca öğrenciye çevrim içi iletişim teknolojileri aracılığıyla da teknik destek vermek, çevrim içi öğrenme ortamına adapte etmek ve öğretmen-eğrenci etkileşimi ile süreci desteklemektir. Özellikle çevrim içi iletişim yolları ile çevrim içi öğrenme ortamında belirli aralıklarla verilen dönüt ve değerlendirme etkinlikleri öğrencide pekiştirme ve güdüleme etkisi yaratabilir. Bu yöntemler ile çevrim içi öğrenme aracı desteklenmiş olup güçlü ve etkili hale getirilmektedir.

2.8. Öğrenme Yönetim Sistemleri

Çevrim içi öğrenme aracının öğrenciye sunumu günümüzde Öğrenme Yönetim Sistemleri (ÖYS) ile de sağlanabilmektedir. ÖYS, çevrim içi öğrenmede oluşturulan aracın öğrenciye öğrenme süreci boyunca zaman ve mekan kısıtlaması olmadan sunulması için geliştirilmiş bir yazılımdır. Günümüzde kullanılan ÖYS yazılımlarından biri de çalışma kapsamında kullanılan LMS'dir. Günümüzde pek çok ÖYS yazılımı kullanılmaktadır ve bu yazılımların çevrim içi öğrenmeyi destekleyen birtakım özellikleri bulunmaktadır.

Ellis (2009), verimli bir ÖYS'nin özelliklerini şöyle sıralamıştır:

- 1.Yönetimi otomatikleştiren ve merkezileştiren,
- 2.Kendine özgü servisleri barındıran,
- 3.Öğrenme aracını paketleyen ve dağıtan,
- 4.Çevrim içi öğrenme platformu üzerinden eğitim girişimlerini birleştiren,
- 5.Standartları ve taşınabilirliği destekleyen,
- 6.İçeriğin kişiselleştirilmesine ve tekrar kullanılabilmesine olanak sağlama gibi özellikleri bulunmalıdır (Ellis'den aktaran Süral, 2012, s.12).

Bu özelliklere ek olarak ÖYS'lerde çevrim içi değerlendirme yapma, süreci izleme, raporlama, eşzamanlı ve eşzamansız iletişim sağlama gibi özellikleri de barındırmaktadır. (Naidu'dan aktaran Süral, 2012, s.11).

ÖYS yazılımları öğrenme aracını sunma ve çevrim içi öğrenmeyi yönetme açısından yararları olan bir sistemdir ve günümüzde uzaktan eğitim birimleri tarafından da çevrim içi öğrenmeyi sağlamak için kullanılmaktadır. ÖYS özellikleri sayesinde çevrim içi öğrenme sırasında hem öğrenci ile etkileşim sağlanmakta hem çevrim içi değerlendirmeler yapılmakta, hem bu süreç izlenmekte ve raporlanmaktadır. Dolayısıyla ÖYS çevrim içi öğrenmede özellikle araç ve süreç kısmını desteklemesi açısından kullanılabilir bir sistemdir.

2.9. Dijital Güvenliğin Sosyal Bilgiler Dersi Öğretim Programı (SBDÖP) ile İlişkisi

Genel itibariyle geçmişten günümüze kadar insan yaşamında varolan gelişmeleri vatandaşlık bağlamında ele alan SBDÖP teknolojinin gelişimiyle insan yaşamında oluşan değişimleri

programına entegre etmek durumundadır. Bu sebeple SBDÖP günümüz koşullarına uyarlanarak çağı gerçekçi bir şekilde temsil etmelidir. Temel amaçlarından biri iyi bir vatandaş yetiştirmek olan sosyal bilgiler dersi, öğretim programı açısından ihtiyaçlar ve koşullar doğrultusunda 2018 yılında yeniden düzenlenmiştir. Programa yön veren değişimlerden biri de dijital teknolojilerde yaşanan gelişimler ve dijital dönüşümdür. Dijital teknolojilerin gelişimiyle birlikte yaygınlaşması insanları dijital ortamda daha aktif hale getirmiş ve dijital dönüşüm bu aktifliği zorunlu kılmıştır. Çağın gerisinde kalmamak adına yaşanan bu adaptasyon dijital vatandaşlık kavramını gündeme getirmiş ve temel amaçlar doğrultusunda SBDÖP’nda da vatandaşlık eğitimi konusunda şekillendirmiştir.

Bilim ve iletişim teknolojilerindeki gelişim, toplumun ve bireyin temel ihtiyaçları Türk Milli Eğitiminin genel amaçlarını ve temel ilkelerini de değiştirmiştir. Bu doğrultuda MEB’in öğretim programlarına “hayat boyu öğrenme” kapsamında TYÇ’de yer alan beceri ve yetkinlikler girmiştir. Bu yetkinliklerde bütünleşmiş bilgi, beceri ve davranışları kazanmış bireyler yetiştirmeyi amaçlayan eğitim sistemimiz TYÇ kapsamında 8 anahtar yetkinlik belirlemiş ve bu yetkinlikleri programları kapsamında ele almıştır. Böylelikle eğitim sistemi doğrultusunda SBDÖP da teknolojik ihtiyaçlar doğrultusunda dijital vatandaşlık ve onun alt boyutlarını da içermektedir.

Eğitim sisteminde genel olarak hedeflenmiş teknoloji entegrasyonu çerçevesinde öğretim programlarının tümünde yer alan yetkinliklerde dijital yetkinlikler yer almaktadır. Programda dijital yetkinlik, çalışma ve gündelik hayatta iletişim için bilgi ve iletişim teknolojilerinin doğru ve bilinçli şekilde kullanılmasını kapsar. Dijital yetkinlik, “bilgiye ulaşım ve bilginin kullanılması, korunması, üretilmesi, paylaşılması ve alışverişi için bilgisayarların kullanılması ayrıca internet aracılığıyla topluluklara katılım sağlanması ve diğer kullanıcılarla iletişim kurulması gibi temel beceriler yoluyla desteklenmektedir” şeklinde ifade edilmektedir (MEB, SBDÖP, 2018).

2018 SBDÖP’da yer alan özel amaçlarda ise 7., 11. ve 12. maddeler dijital vatandaşlığın alt boyutu olan dijital güvenlikle ilişkilendirilmiştir.

MEB 2018 SBDÖP’ da yer alan özel amaçlarda ilgili maddeler şöyle açıklanmıştır:

7. Doğru ve güvenilir bilgiye ulaşma yollarını bilen bireyler olarak eleştirel düşünme becerisine sahip olmaları,

11. Bilim ve teknolojinin gelişim sürecini ve toplumsal yaşam üzerindeki etkilerini kavrayarak bilgi ve iletişim teknolojilerini bilinçli kullanmaları,

12. Bilimsel düşünmeyi temel alarak bilgiye ulaşma, bilgiyi kullanma ve üretmede bilimsel ahlakı gözetmeleri (MEB, SBDÖP, 2018, s.8).

Programda yer alan özel amaçlardaki bu maddelerde bilgi ve iletişim teknolojilerinin kullanımında “*eleştirel düşünme becerisi, bu teknolojileri bilinçli kullanma ve bilimsel etik*” konuları dijital güvenlik yeterlikleri arasındadır ve konu ile ilişkilidir.

Yine SBDÖP’nda yer alan beceriler arasında dijital vatandaşlık ve onun alt boyutu olan dijital güvenlik ile ilişkili beceriler şunlardır; “*araştırma, dijital okuryazarlık, eleştirel düşünme, empati, finansal okuryazarlık, iletişim, sosyal katılım becerisi, hukuk okuryazarlığı ve medya okuryazarlığı becerileri*” (MEB, SBDÖP, 2018, s.9). Günlük hayatta gerekli olan bu beceriler dijital ortamda da bireyin ihtiyaçları arasındadır ve bu beceriler dijital ortamın etkin, bilinçli ve güvenli bir şekilde kullanımında gerekli beceriler arasındadır.

SBDÖP’nda yer alan değerlerden “*adalet, bilimsellik, duyarlılık, dürüstlük, eşitlik, saygı ve sorumluluk*” değerleri dijital ortamın uygun kullanım normları açısından dijital vatandaşlarda olması gereken değerlerdir ve bu değerler diğer kullanıcıların haklarına saygı ve bu kullanıcılara karşı bireysel olarak sorumluluğumuzda olan değerler arasındadır. Bununla birlikte söz konusu değerlerin dijital ortamda yoksunluğu kişinin ve diğer kullanıcıların güvenliği açısından risk teşkil ettiğinden dijital güvenlikle ilişkilendirilmiştir.

SBDÖP’nda (2018) “programın uygulanmasında dikkat edilecek hususlar” başlığı altında yer alan 10. madde doğrudan dijital vatandaşlık ve dijital güvenlik ile ilişkilidir;

10. Son yıllarda dijital teknolojideki gelişmelere bağlı olarak vatandaşlık hak ve sorumluluklarıyla ilgili yeni durumlar (dijital vatandaşlık, e-Devlet, sanal ticaret, sosyal medya vb.) ve birtakım sorunlar (dijital bölünmüşlük, kimlik hırsızlığı, kişisel bilginin gizliliği, siber dolandırıcılık, siber zorbalık vb.) ortaya çıkmıştır. Öğrencilerin dijital vatandaşlık yeterliklerini geliştirmek amacıyla konuyla ilgili ders içi ve ders dışı etkinliklere yer verilmelidir (MEB, SBDÖP, 2018, s. 10).

SBDÖP’nın uygulanmasında dikkat edilmesi gerekenler arasında vatandaşlık hak ve sorumluluklarıyla ilgili dijital ortamda ortaya çıkan “*dijital bölünmüşlük, kimlik hırsızlığı, kişisel verilerin gizliliği, dijital hırsızlık, dijital zorbalık vb.*” sorunlarla vatandaşların mücadele edebilmesi amacıyla dijital vatandaşlık ve dijital güvenlik yeterliklerinin

geliştirilmesi program tarafından da öngörülerek kapsama alınmıştır. Bu doğrultuda sosyal bilgiler dersi kapsamında bu kavramlara ve dijital ortamda oluşabilecek diğer risklerle mücadele edebilmek amacıyla dijital vatandaşlık ve dijital güvenlik yeterliğinin geliştirilmesi gereklidir.

SBDÖP’nda yer alan öğrenme alanları ve onun içeriğindeki kazanımlarda da 4., 5., 6. ve 7. sınıf düzeyinde dağınık olarak dijital vatandaşlığa ve onun alt boyutu olan dijital güvenliğe ilişkin kazanımlar yer almaktadır. Programda yer alan ilgili kazanımlar ve kazanımlar doğrultusunda ders kitaplarında ele alınan konular çalışma doğrultusunda incelenen dijital güvenliğin boyutlarıyla doğrudan ve dolaylı olarak ilişkilendirilmiştir

SBDÖP’nda dijital güvenliğin teknik boyutu ile ilişkilendirilmiş olan kazanımlar;

SB.5.4.2. Sanal ortamda ulaştığı bilgilerin doğruluk ve güvenilirliğini sorgular (Medya okuryazarlığı üzerinde durulur)

SB.5.4.3. Sanal ortamı kullanırken güvenlik kurallarına uyar (Mesafeli alışveriş, güvenli internet kullanımı, kimlik hırsızlığı gibi konular ele alınır)

SB.7.4.1. Bilginin korunması, yaygınlaştırılması ve aktarılmasında değişim ve sürekliliği inceler.(Yazının icadından günümüze kadar farklı depolama, yaygınlaştırma ve aktarma teknikleri üzerinde kısaca durulur) (MEB, SBDÖP, 2018, s.17-24).

SBDÖP’nda dijital güvenliğin psikososyal boyutu ile ilişkilendirilmiş kazanımlar;

SB.4.4.2. Teknolojik ürünlerin geçmişteki ve bugünkü kullanımlarını karşılaştırır (Teknolojinin hayatımızda ve çevremizde meydana getirdiği olumlu ve olumsuz etkilerine dikkat çekilir)

SB.5.4.1. Teknoloji kullanımının sosyalleşme ve toplumsal ilişkiler üzerindeki etkisini tartışır

SB.6.7.4. Popüler kültürün, kültürümüz üzerindeki etkilerini sorgular (Kültürümüze ait olmayan unsurların, medya araçları yoluyla toplum hayatını nasıl etkilediği fark ettirilir)

SB.7.1.3. Medyanın sosyal değişim ve etkileşimdeki rolünü tartışır (Seçilen bir iletişim kanalının (TV, İnternet, akıllı telefonlar vb.) bireyler arasındaki iletişimi ve toplumsal olarak da kültürü nasıl değiştirdiği ele alınır) (MEB, SBDÖP, 2018, s.15-23).

SBDÖP’nda dijital güvenliğin çevrim içi alışveriş boyutu ile ilişkilendirilmiş kazanımlar;

SB.5.4.3. Sanal ortamı kullanırken güvenlik kurallarına uyar

(Mesafeli alışveriş, güvenli İnternet kullanımı, kimlik hırsızlığı gibi konular ele alınır)

SB.7.5.6. Dijital teknolojilerin üretim, dağıtım ve tüketim ağında meydana getirdiği değişimleri analiz eder (E-ticaret (gerçek ürünler kadar bilgisayar oyunları gibi sanal/dijital ürünler) üzerinde durulur) (MEB, SBDÖP, 2018, s.15-25).

SBDÖP’nda dijital güvenliğin hak ve sorumluluk boyutu ile ilişkilendirilmiş kazanımlar;

SB.4.4.5. Teknolojik ürünleri kendisine, başkalarına ve doğaya zarar vermeden kullanır

SB.5.4.5. Yaptığı çalışmalarda bilimsel etiğe uygun davranır (Yapılan çalışmalarda yararlanılan kaynakları göstermenin ve kaynakların aslını korumanın önemi üzerinde durulur)

SB.5.6.1. Bireysel ve toplumsal ihtiyaçlar ile bu ihtiyaçların karşılanması için hizmet veren kurumları ilişkilendirir (Kazanım kapsamında e-devlet portalı ve bu portal üzerinden sağlanan hizmetlere değinilir)

SB.6.4.4. Telif ve patent hakları saklı ürünlerin yasal yollardan temin edilmesinin gerekliliğini savunur

SB.7.1.4. İletişim araçlarından yararlanırken haklarını kullanır ve sorumluluklarını yerine getirir (Özel hayatın gizliliği, düşünceyi açıklama özgürlüğü ve doğru bilgi alma hakkı ile kitle iletişim özgürlüğü arasındaki ilişki ele alınır) (MEB, SBDÖP, 2018, s.15-23).

SBDÖP’nda dijital güvenliğin sağlık boyutu ile ilişkilendirilmiş kazanımlar;

SB.4.4.2. Teknolojik ürünlerin geçmişteki ve bugünkü kullanımalarını karşılaştırır (Teknolojinin hayatımızda ve çevremizde meydana getirdiği olumlu ve olumsuz etkilerine dikkat çekilir)

SB.5.1.3. Sahip olduğu haklarının farkında olan bir birey olarak katıldığı gruplarda aldığı rollerin gerektirdiği görev ve sorumluluklara uygun davranır (Kişisel zamanını planlarken oyun oynama, ders çalışma, kitap okuma, uyuma, aile ve arkadaşlar ile nitelikli zaman geçirme ve kitle iletişim araçlarını kullanma durumlarını dikkate almanın önemine değinilir) (MEB, SBDÖP, 2018, s. 14-17).

2.10. İlgili Araştırmalar

Yurt içinde ve yurt dışında dijital vatandaşlık ve onun alt boyutu olan dijital güvenlik ile ilgili yapılan çalışmalar bu başlık altında sunulmuştur.

2.10.1. Yurt İinde Yapılmış Arařtırmalar

Kavuk (2011), “İlköğretim Öğrencilerinin Sanal Zorba ve Sanal Kurban Olma Durumlarının İncelenmesi” adlı yüksek lisans tez arařtırmasında ortaokul 6, 7 ve 8. sınıf öğrencilerinin siber zorba ve siber kurban olma durumlarını ortaya koymayı amaçlamıştır. Tarama modelinde yapılmış olan arařtırmanın alışma grubu tabakalı örnekleme yöntemiyle belirlenerek 2082 öğrenciden oluşturulmuştur. Öğrencilerin demografik bilgilerini belirlemek amacıyla anket, siber zorbalık ve siber kurban olma durumlarını belirlemek amacıyla da Ayas ve Horzum (2010) tarafından geliştirilen “Siber Zorba ve Kurban Öleđi” kullanılmıştır. alışma sonuçlarında, siber zorba ve siber kurban olma ile cinsiyet, internete bağlanma yeri, internet kullanım süresi ve internet kullanım amaçları arasında anlamlı farklılıklar bulunmuş, ilgili kurumlarca, siber zorbalık farkındalığını artırıcı ve siber zorbalığı önleyici eğitim programlarının düzenlenmesinin gerekliliđi önerilmiştir.

Kocadağ Ünver (2012), “Öğretmen Adaylarının Dijital Vatandaşlık Düzeylerinin Belirlenmesi” adlı alışmasında eğitim fakültelerinde öğrenim gören öğretmen adaylarının dijital vatandaşlık düzeylerini belirlemek için geçerli ve güvenilir bir ölek geliştirip bu ölekten alınan puanların cinsiyet, yaş, ailesinin ortalama gelir düzeyi deđişkenleri açısından deđerlendirmiştir. Bu alışma tarama modelinde, 2010-2011 eğitim öğretim yılında iki aşama şeklinde gerçekleştirilmiştir. İlk aşamada Gaziosmanpaşa Üniversitesi Eğitim Fakültesinde öğrenim gören 1063 öğretmen adayı ile ölme aracının geçerlik güvenirlik alışması yapılmış ve yedi boyutlu bir ölek geliştirilmiştir. İkinci aşamada ise Dijital Vatandaşlık Öleđi’nin Karadeniz Teknik Üniversitesi Fatih Eğitim Fakültesi’nde öğrenim gören 2200 öğretmen adayına uygulanarak dijital vatandaşlık düzeylerinde cinsiyet, yaş, aile gelir düzeyi deđişkenlerine göre ilişkisini belirlemeye alışmıştır. Elde edilen bulgulardan hareketle arařtırmacı, dijital vatandaşlık düzeyinin cinsiyet deđişkeni ile arasında anlamlı bir farklılık olduđu, örneklem kapsamındaki öğretmen adaylarının %0,36’sının aşırı zayıf, %33,32’sinin ok iyi düzeyde olduđu sonucuna ulaşmıştır. Öğretmen adaylarının dijital vatandaşlığı noktasında iyi bir şekilde yetiştirilmesinin, teknolojinin daha uygun bir şekilde kullanılmasına öncülük edeceğine dair öneride bulunulmuştur.

Korkmaz ve Kıran Esen (2012), “Güvenli İnternet Kullanımı Konusunda Uygulanan Akran Eğitiminin Ergenler Üzerindeki Etkisi” adlı alışmalarında akran eğitimci öğrencilerin,

akranlarına güvenli internet kullanımı konusunda eğitim vermelerinin ergenler üzerindeki etkisini belirleme amaçlanmıştır. Araştırmanın çalışma grubunu 6., 7. ve 8. sınıf öğrencilerden 825 öğrenci oluşturmuştur. Araştırma kapsamında veri toplama aracı olarak Yılmazhan ve Gültutan (2007) tarafından geliştirilen “İnternet Kullanma Alışkanlıkları Ölçeği” kullanılmıştır. Akran eğitimcisi olarak kullanılmak üzere seçilen 12 öğrenciye eğitim verilmiş ve bu öğrenciler akranlarına; internet, internet kullanımı, aşırı kullanım, dijital bağımlılığını tanıma ve mücadele etme, internet kullanım kuralları ve güvenlik yazılımlarının kullanımı ile ilgili kırk dakikadan oluşun iki eğitim vermiş ve 40 dakikalık iki oturum ile eğitim vermiş ve bu eğitimi alan öğrencilerin internet kullanım alışkanlıklarının olumlu yönde değiştiği sonucuna ulaşılmıştır.

Mert, Bülbül ve Sağiroğlu (2012), “Milli Eğitim Bakanlığına Bağlı Okullarda Güvenli İnternet Kullanımı” çalışmalarında ortaokul 8. Sınıf düzeyinde öğrenim gören öğrencilerin güvenli internet kullanımı davranışlarını belirlemek amaçlanmıştır. Araştırmanın çalışma grubunu 149 öğrenci oluşturmuş ve veriler güvenli internet kullanımı ile ilgili anket aracılığıyla toplanmıştır. Çalışmadan elde edilen bulgular ve diğer çalışmalarla karşılaştırmalar sonucunda internet güvenliğinin hemen tamamlanabilecek bir beceri olmadığı, bu davranışın yerleşmesinin bir dizi alışkanlıklar ve eğitim sürecinden geçtiği ve bu sürece öğrenciler dışında öğretmenler, okul yöneticileri ve velilerin de yer alması gerektiği sonucuna ulaşılmıştır.

Demirel, Yörük ve Özkan (2012), “Çocuklar İçin Güvenli İnternet: Güvenli İnternet Hizmeti ve Ebeveyn Görüşleri Üzerine Bir Araştırma” çalışmalarında ebeveynlerin BTK tarafından 2011 yılında çocuklar ve gençler için başlattığı “Güvenli İnternet Hizmeti” konusundaki görüşlerini tespit etmeyi amaçlamışlardır. Araştırmanın çalışma grubunu 247 öğrencinin ebeveynleri oluşturmuş ve veriler anket aracılığıyla toplanmıştır. Çalışma sonucunda ebeveynlerin çoğunluğunun BTK’nın Güvenli İnternet Hizmetini desteklediği fakat bu hizmetten yararlanma hususunda çok da istekli görünmedikleri bulgularına rastlanmıştır.

Çubukçu ve Bayzan (2013), “Türkiye’de Dijital Vatandaşlık Algısı ve Bu Algıyı İnternetin Bilinçli, Güvenli Ve Etkin Kullanımı ile Artırma Yöntemleri” çalışmalarında dijital vatandaşlık algısı ve alt boyut olarak internet kullanıcılarının bilinçli, güvenli ve etkin kullanımına yönelik Türkiye’de ve dünyada mevcut düzenlemeler irdelenmiştir. Araştırma sonucunda mevcut düzenlemelerin geliştirilmesi için özellikle Türkiye’de atılması gereken

adımlardan bahsedilmiştir. Çalışmada internet riskleri; içerik riskleri, temas riskleri ve ticari riskler olmak üzere üç kategoride incelenmiştir. Sonuç olarak, dijital vatandaşlığın dokuz boyutu, internet risklerinin üç boyutu ile eşleştirilerek mevcut durum ve öneriler açıklanmıştır.

Çetin ve Özgiden (2013), “Dijital Kültür Sürecinde Dijital Yerliler ve Dijital Göçmenlerin Twitter Kullanım Davranışları Üzerine Bir Araştırma” adlı çalışmalarında dijital yerli ve dijital göçmenlerin özelliklerine değinmiş ve onların Twitter’ı kullanım davranışlarını ortaya çıkarmak amacıyla online anket uygulamışlardır. Anket, 1 hafta süreyle survey.com sitesinde yayında kalmış, bu anket ile çeşitli değişkenlere odaklanarak iki grup arasında davranış farkı olup olmadığı belirlenmeye çalışılmıştır.

Karakuş, Çağıltay, Kaşıkçı, Kurşun ve Ogan (2014), “Türkiye ve Avrupa’daki Çocukların İnternet Alışkanlıkları ve Güvenli İnternet Kullanımı” adlı çalışmalarında Avrupa Çevrim İçi Çocuklar Projesi’ne dahil olan Türkiye ve 23 Avrupa ülkesinin bulgularını incelemişlerdir. Söz konusu projede çalışma grubu yaş aralığı 9-16 yaşındaki çocuklardır. Çalışma sonucunda, katılımcı çocukların çoğunluğunun internet kullanma becerilerinin yeterli olmadığı ve internet risklerine karşı savunmasız olduğu kanaatine ulaşılmıştır. Ayrıca araştırmacıların çalışmada elde ettikleri diğer bir sonuç ise Türkiye’deki ebeveynlerin çocuklarını internet kullanım becerisi edindirme ve risklere karşı koruma yetisine yeteri kadar sahip olmadığıdır.

Kaya ve Kaya (2014), “Öğretmen Adaylarının Dijital Vatandaşlık Algısı” adlı çalışmalarında Bilgisayar ve Öğretim Teknolojileri Eğitimi bölümünde 3. ve 4. Sınıfta öğrenim gören öğretmen adaylarının dijital vatandaşlık algısını belirlemeyi amaçlamışlardır. Nitel araştırma yöntemi kullanılan araştırmada veriler yarı yapılandırılmış görüşme tekniği ile toplanmış, betimsel analiz yöntemi ile analiz edilmiştir. Öğretmen adaylarının büyük çoğunluğunun dijital vatandaşlık kavramını doğru bir şekilde ele aldığı sonucuna ulaşılan çalışmada, öğretmen adaylarının okullarda dijital vatandaşlıkla ilgili eğitim verilmesinin gerekli olduğu kanaatinde oldukları sonucuna ulaşılmıştır. Ayrıca öğretmen adaylarının dijital teknolojileri sosyal ağlara katılmak, alışveriş ve ödev araştırmak için de kullandığı sonucuna ulaşılmıştır.

Karaduman ve Öztürk (2014), “Sosyal Bilgiler Dersinde Dijital Vatandaşlığa Dayalı Etkinliklerin Öğrencilerin Dijital Vatandaşlık Tutumlarına Etkisi ve Dijital Vatandaşlık

Anlayışlarına Yansımaları” adlı çalışmalarında 6. sınıf sosyal bilgiler dersinde dijital vatandaşlığa dayalı olarak gerçekleştirilen etkinliklerin, öğrencilerin dijital vatandaşlık tutumlarına etkisini ve dijital vatandaşlık anlayışlarına yansımaları incelenmiştir. Ön test-son test ve kontrol gruplu yarı deneysel desen ile yapılan araştırmada etkinliklerin uygulanma sürecinin betimlenmesinde nitel veriler de kullanılmıştır. Yöntem çeşitlemesi yapılan araştırmada, dijital vatandaşlığa dayalı etkinliklerin öğrencilerin dijital ortama dair tutumlarını olumlu yönde etkilediği sonucuna da ulaşılmıştır.

İşman ve Göngören (2014), “Dijital Citizenship” adlı çalışmalarıyla Ribble ve Bailey (2007)’nin açıkladığı 9 boyuta dayanarak dijital vatandaşlık ölçeği geliştirmeyi amaçlamıştır. Araştırma kapsamında ölçek geliştirme sürecinde katılımcı olarak 2012-2013 eğitim öğretim yılında Sakarya Üniversitesi Eğitim Fakültesinde Okul Öncesi Öğretmenliği, Türkçe Öğretmenliği, Din Kültürü ve Ahlak Bilgisi Öğretmenliği ve Sınıf Öğretmenliği bölümünde öğrenim gören 229 öğretmen adayına ulaşılmıştır. Geçerlik ve güvenirlik çalışmaları yapılan çalışma sonucunda 9 boyut ve 34 maddeden oluşan bir ölçek geliştirilmiştir.

Çepni, Oğuz ve Kılcan (2014), “İlköğretim Öğrencilerinin Dijital Vatandaşlığa Yönelik Görüşleri” adlı araştırmalarıyla ilköğretim öğrencilerinin internet kullanımına (dijital vatandaşlığa) yönelik tutumlarını belirlemeye çalışmışlardır. Araştırma için gerekli veriler Karaduman (2011) tarafından geliştirilen “Dijital Vatandaşlık Tutum Ölçeği” ile toplanmış ve araştırmanın çalışma grubunu 2011–2012 eğitim-öğretim yılında Ankara’da Milli Eğitim Bakanlığı’na bağlı 6 ilkokul’da sekizinci sınıfta öğrenim gören 557 öğrenci oluşturmuştur. Araştırmada tarama modeli ve tesadüfi örneklem yöntemi kullanılmıştır. Araştırma bulguları incelendiğinde, öğrencilerin dijital vatandaşlık tutumlarına ilişkin görüşleri cinsiyet, anne eğitim durumu, aylık gelir, evde internet bağlantısı bulunma, internet kullanma sıklığı, internet kullanma geçmişi, e-posta adresine sahip olma durumlarına göre anlamlı farklılık göstermiş, baba eğitim durumuna göre anlamlı bir farklılığa rastlanmamıştır.

Erol, Şahin, Yılmaz ve Haseki (2015), “Kişisel Siber Güvenliği Sağlama Ölçeği Geliştirme Çalışması” adlı çalışmanın amacı çevrim içi ortamda kişilerin siber güvenlik ile ilgili davranışlarını belirleme amacı taşıyan bir ölçek geliştirmektir. Çalışma sonucunda gerekli istatistiksel işlemlerden geçmiş “Kişisel Siber Güvenliği Sağlama Ölçeği” oluşturulmuştur.

Küçükali ve Bülbül (2015), “Fatih Projesi Kapsamında İnternetin Bilinçli ve Güvenli Kullanımının Artırılması” adlı çalışmalarında internetin bilinçli ve güvenli kullanımı konusunda farkındalık oluşturabilmek için yönlendirici internet siteleri oluşturmak ve bu çerçeveyi belirlemeyi amaçlamışlardır. Araştırmanın çalışma grubunu Fatih projesinde görev alan öğretmenlerden “internetin bilinçli ve güvenli kullanımı semineri” ne katılan 214 öğretmen ve 30 internet sitesi oluşturmaktadır. Veri toplamak amacıyla oluşturulan 22 adet soruluk bir anket geliştirilmiştir. Verilerden elde edilen sonuçlara göre aştırmacılar, öğretmenlerin güncel platformlarla desteklenen, etkileşimli ve içerik bakımından zengin internet sitelerine gerek duyduğunu belirtmiştir.

Öztürk (2015), “Ortaokul Öğrencilerinin Dijital Vatandaşlık Düzeyleri” adlı yüksek lisans tezinde ortaokul öğrencilerinin dijital vatandaşlık düzeylerine tespit etmek amaçlanmış ve dijital vatandaşlığın öğrenme-öğretmede etkisi incelenmiştir. Araştırmada karma model kullanılmış, örnekleme belirlemede ise maksimum çeşitlilik örnekleme kullanılmıştır ve toplamda 829 öğrenci dahil edilmiştir. Öğrencilerin dijital vatandaşlık düzeylerini belirlemek için araştırmacı tarafınca geliştirilen “Ortaokul Öğrencilerinin Dijital Vatandaşlık Düzeyleri” isimli veri toplama aracı kullanılmıştır. Araştırmanın nitel boyutu için ise 6,7 ve 8. Sınıftan 12 öğrenci ile görüşülmüştür. Nicel verilerin istatistik çözümlemesi SPSS 21 programında yapılmıştır. Dijital vatandaşlık düzeyleriyle ilgili olan verilerin analizinde tek yönlü varyans analizi (Anova), t testi, yüzde frekans analizleri kullanılmıştır. Nitel verilerin çözümlenmesinde betimsel analizden yararlanılmıştır. Bulgulardan hareketle araştırmacı öğrencilerin teknolojik araçları kullandıklarını fakat dijital vatandaşlığın alt boyutlarına vakıf olmadıklarını, genelde ödev, sosyal medya, araştırma yapmak gibi amaçlarla teknolojiden yararlandıkları sonuçlarına ulaşmıştır.

Sakallı (2015), “Sınıf Öğretmeni Adaylarının Dijital Vatandaşlık Düzeyleri İle Siber Zorbalık Eğilimleri Arasındaki İlişkinin İncelenmesi” adlı yüksek lisans tez araştırmasında sınıf öğretmeni adaylarının dijital vatandaşlık düzeyleri ile siber zorbalık eğilimlerini belirlemek ve aralarındaki ilişkiyi ortaya çıkarmaya çalışmıştır. Bu araştırmada nicel araştırma yöntemlerinden tarama modeli uygulanmıştır. Araştırmanın çalışma grubunu 2014-2015 eğitim öğretim yılında Adnan Menderes Üniversitesi Eğitim Fakültesi Sınıf Öğretmenliği bölümünde öğrenim gören sınıf öğretmeni adayları oluşturmaktadır. Veri toplamak amacıyla İşman ve Güngören (2014) tarafından geliştirilen “Dijital Vatandaşlık

Ölçeği” ve Türkoğlu (2013) tarafından geliştirilen “Siber Zorbalık Tutum Ölçeği” kullanılmıştır. Elde edilen bulgulardan hareketle araştırmacı, sınıf öğretmenleri adaylarının dijital vatandaşlık düzeyleri ile siber zorbalık eğilimleri arasında, orta düzeyde, pozitif yönlü ve anlamlı bir ilişki olduğunu tespit etmiştir.

Elçi (2015), “Bilişim Teknolojileri ve Yazılım Dersi Öğretim Programına Yönelik Öğrenci Görüşlerinin Dijital Vatandaşlık Bağlamında İncelenmesi” adlı yüksek lisans tez araştırmasında Bilişim Teknolojileri ve Yazılım dersi öğretim programının dijital vatandaşlık kazanımlarını ne ölçüde kazandırdığı ile ilgili öğrenci görüşleri, dijital vatandaşlığın 7 boyutunu kapsayan ölçek aracılığıyla belirlemeye çalışmıştır. Araştırma nicel bir araştırma olup, tekil tarama modeli kullanılmıştır. Adana il merkezindeki ortaokullara devam eden 5. ve 6. sınıflardan yansız küme örnekleme yoluyla örneklem seçimi yapılmıştır. Veri toplamada “BTY Dersinde Dijital Vatandaşlık Ölçeği(BTY-DVÖ)” kullanılmıştır. Çalışmadan elde edilen bulgulara göre, araştırmacı BYT dersinin, dijital vatandaşlığın bilgi, beceri ve değerlerinin kazanılmasında orta düzeyde katkıda bulunduğu sonucuna ulaşmıştır.

Görmez (2016), “Öğretmen Adaylarının "Dijital Vatandaşlık ve Alt Boyutları" Hakkındaki Görüşleri (Bir Durum Çalışması)” adlı çalışma öğretmen adaylarının “dijital vatandaşlık ve boyutları” hakkındaki görüşlerini ortaya koymayı amaçlamıştır. Araştırma, nitel araştırma yöntemlerinden örnek olay deseni kullanılmıştır. Veri toplamak amacıyla sınıf öğretmenliği bölümünden 68, sosyal bilgiler öğretmenliği bölümünden 74 ve türkçe öğretmenliği bölümünden 58 öğretmen adayı ile standartlaştırılmış açık uçlu görüşme formu kullanılarak görüşme yöntemi kullanılmıştır. Elde edilen veriler, içerik analizi yöntemiyle çözümlenmiştir. Bulgulardan elde edilen sonuçlara göre; Dijital vatandaşlık ve alt boyutları ile ilgili yeterli bilgiye sahip olma konusunda bölümlere göre kıyaslama yapıldığında en az bilgi düzeyi sosyal bilgiler, sonra türkçe ve en son sınıf öğretmenliği bölümü takip etmektedir.

Bakır (2016), “Sınıf Öğretmeni Adaylarının Dijital Vatandaşlık Seviyelerinin Dijital Vatandaşlık Alt Boyutlarına Göre İncelenmesi” adlı yüksek lisans tez araştırmasında sınıf öğretmenleri adaylarının dijital vatandaşlık ve alt boyutları yönünden algılarını ortaya koymayı amaçlamıştır. Araştırma nitel araştırma yöntemlerinden özel durum çalışması olarak yürütülmüştür. Veri toplama aracı olarak ölçek, görüşme, gözlem kullanılmıştır. Çalışma

grubunu 11 sınıf öğretmen adayı oluşturmuş, Kocadağ (2012) tarafından oluşturulan “Dijital Vatandaşlık Ölçeği” kullanılmıştır. Nicel veriler betimleyici istatistik tekniği ile analiz edilmiştir. Nitel verilerin analizinde ise betimsel analiz tekniği kullanılmıştır. Bulgulardan hareketle araştırmacı, nicel verilerden elde edilen sonuçların nitel verilerle tutarlı olmadığı, nicel verilere göre dijital vatandaşlık düzeylerinin yüksek olduğu nitel verilere göre ise bu düzeyin düşük olduğunu tespit etmiştir.

Som Vural (2016), “Üniversite Öğrencilerinin Bakış Açısıyla Dijital Vatandaşlık Göstergelerinin İncelenmesi” adlı doktora tez araştırmasında, üniversite öğrencilerinin dijital vatandaşlık düzeylerini ortaya çıkarmak amacıyla ölçek geliştirilerek dijital vatandaşlığa ve alt faktörlere ilişkin ortalamalar arasındaki ilişkiler ile öğrencilerin cinsiyetleri, üniversiteleri, fakülteleri, sınıfları, internet kullanım sıklıkları ve aylık gelir durumu ile olan ilişkileri incelenmiştir. Üniversite öğrencilerinin dijital vatandaşlık düzeylerini tespit etmek için tarama modeli kullanılmıştır. Bu sebeple bu çalışma tarama modelinde bir araştırmadır. Araştırma iki aşamadan oluşmuştur. İlk aşamada bir üniversitenin farklı fakültelerinden seçilen 625 üniversite öğrencisinin görüşleri doğrultusunda ölçek geliştirilmiş, ikinci aşamada ise güvenilirlik ve geçerlik sağlanmış, beş faktörden oluşan ölçek, beş farklı üniversitenin öğrenim gören 2148 öğrencisine uygulanmıştır. Araştırma sonucunda üniversite öğrencilerinin dijital vatandaşlığa ilişkin ortalamaları cinsiyet açısından kadın öğrencilerin lehine anlamlı bir farklılık görüldüğü, üniversiteler arasında anlamlı farklılıkların olduğu fakat fakülte bazında anlamlı düzeyde farklılaşmadığı, ayrıca sınıf düzeyi, internet kullanım sıklığı, gelir yüksekliği ile anlamlı farklılık olduğu belirtilmiştir.

Aslan (2016), “İlköğretim Sosyal Bilgiler Öğretmen Adaylarının Dijital Vatandaşlık Davranışlarının Bazı Değişkenler Açısından İncelenmesi (Fırat, Dicle, Siirt, Adıyaman Üniversiteleri Örneği)” adlı yüksek lisans tez çalışmasında sosyal bilgiler öğretmen adaylarının dijital vatandaşlık ve alt boyutlarına yönelik algılarını çeşitli değişkenler açısından incelemiştir. Bu çalışmada nitel araştırma yöntemlerinden özel durum çalışması deseni tercih edilmiştir. Çalışma grubunu 2015-2016 eğitim öğretim yılında Fırat, Dicle, Siirt ve Adıyaman sosyal bilgiler öğretmenliği bölümü 1,2,3 ve 4. sınıfta öğrenim gören 682 öğretmen adayı oluşturmuştur. Veri elde etmek amacıyla Kocadağ (2012) tarafından hazırlanan Dijital Vatandaşlık Ölçeği, yedi değişken (cinsiyet, yaş, ailenin aylık ortalama

geliri, kendine ait bilgisayar, sosyal ağ üyeliği, sınıf düzeyi, internete kalma süresi) üzerinde uygulama yapılmıştır. Toplanan verilerin nicel boyutu betimleyici istatistik tekniği ile, nitel boyutu ise betimsel analiz tekniği ile analiz edilmiştir. Araştırmacı bulgulardan hareketle sosyal bilgiler öğretmen adaylarının dijital vatandaşlık seviyelerinin yüksek çıktığı sonucuna ulaşmıştır. Ayrıca dijital hak ve sorumluluklar vatandaşlık kavramı ile bağdaştırıldığında öğretmen adaylarının algısal yanılgılarının olduğu tespit edilmiş, bu doğrultuda çeşitli önerilerde bulunulmuştur.

Yılmaz, Şahin ve Akbulut (2016), “Öğretmenlerin Dijital Veri Güvenliği Farkındalığı” adlı çalışmalarında Milli Eğitim Bakanlığı’na bağlı okullarda görev yapan öğretmenlerin dijital veri güvenliği farkındalıklarını çeşitli değişkenlere göre inceleyerek ortaya koymaya çalışmışlardır ve tarama modeli benimsenmiştir. Tarama modeline ek olarak nedensel karşılaştırmalı modellere özgü bazı analizlerden yararlanılmıştır. Araştırmanın örneklemini Balıkesir ilinde görev yapan 870 öğretmen oluşturmaktadır. Veri elde etmek amacıyla örnekleme Dijital Veri Güvenliği Farkındalık Ölçeği (DVGFO) uygulanmıştır. Toplanan verilerden elde edilen bulgulardan hareketle araştırmacılar, öğretmenlerin dijital veri güvenliği farkındalıklarının oldukça yüksek olduğu sonucuna ulaşmıştır. Farkındalık değerlerinin cinsiyet, günlük bilgisayar kullanım süresi, günlük internet kullanım süresi ve farklı teknolojilere sahip olma durumlarına göre değiştiği; branş, öğrenim kademesi, öğrenim durumu ve mesleki kıdem bağlamında değişmediği sonucuna da ulaşılmıştır.

Elçi ve Sarı (2016), “Bilişim Teknolojileri ve Yazılım Dersi Öğretim Programına Yönelik Öğrenci Görüşlerinin Dijital Vatandaşlık Bağlamında İncelenmesi” adlı çalışmalarında Bilişim Teknolojileri ve Yazılım (BTY) dersi öğretim programına yönelik öğrenci görüşlerini dijital vatandaşlık bağlamında incelemişlerdir. Araştırmaya, Adana ili merkez ilçelerindeki ortaokullara devam eden 264 öğrenci katılmıştır. Veriler, Elçi ve Sarı (2016) tarafından geliştirilen “BTY Dersinde Dijital Vatandaşlık Ölçeği (BTY-DVÖ) kullanılarak toplanmıştır. Verilerin analizinde t-testi ve varyans analizi kullanılmıştır. Elde edilen bulgulara göre dijital etik-kanun ve buna bağlı hak ve sorumluluklar boyutuyla ilgili bilgi, beceri ve değerlerin kazandırılmasında BTY dersi ortanın üzerinde; dijital okuryazarlık boyutuyla ilgili bilgi, beceri ve değerlerin kazandırılmasında ortanın çok az altında, dijital güvenlik ve dijital iletişim boyutlarıyla ilgili bilgi, beceri ve değerlerin kazandırılmasında ise ortanın biraz üzerinde katkıda bulunmaktadır. Araştırmanın sonuçlarına göre BTY-DVÖ

puanları arasında sınıf düzeyi ve cinsiyete göre anlamlı farklar bulunmamakta iken; evinde bilgisayar ve internet bağlantısı bulunan öğrenciler lehine anlamlı farklar belirlenmiştir.

Peker Ünal (2017), “Bir Öğretim Programındaki Dijital Vatandaşlık Öğeleri ve Ortaöğretim Öğrencilerinin Dijital Vatandaşlık Öğelerine Sahip Olma Durumları” adlı çalışmasında “Bilgi ve İletişim Teknolojileri” dersi öğretim programında yer alan dijital vatandaşlık öğelerinin ve katılan öğrencilerin dijital vatandaşlık öğelerine sahip olma düzeyleri belirlenmeye çalışılmıştır. Bu amaçla “Bilgi ve İletişim Teknolojileri” dersi öğretim programı ve ders kitapları içerik analizi ile incelenmiş, katılan öğrencilere başarı testi ve senaryo durumları ile Karaduman (2011) tarafından hazırlanan “Dijital Vatandaşlık Tutum Ölçeği” uygulanmıştır. Çalışma grubunu 9. sınıf öğrencilerinden 34 kişi oluşturmuştur. Bu çalışmada, program ve ders kitabında yer alan dijital vatandaşlık öğelerini öğrencilere kazandırmada sayıca yetersiz olduğu bulgusuna ulaşılmıştır. Bu kapsamda dijital vatandaşlık öğelerine programda ve ders kitaplarında daha fazla yer verilmesi gerektiğini öneri olarak sunmuştur.

Eser Akkuş (2017), “Türkiye’deki Azınlıkların Dijital Vatandaşlık Pratikleri” adlı yüksek lisans tez araştırmasında dezavantajlı gruplar arasında yer alan azınlıkların vatandaşlara imkanlar sağlayan dijital vatandaşlık pratiklerini, dijital platformların olanakları ve bu olanaklardan azınlıkların ne kadar bilgi sahibi olduğu, nerelerde yararlandıklarını, karşılarına çıkan sorunları ortaya koymaya çalışmıştır. Nitel araştırma yöntemi kullanılan bu çalışmada veri toplamak amacıyla derinlemesine mülakat tekniğinden yararlanılmıştır. Araştırmanın çalışma grubunu 12 azınlık vatandaş oluşturmaktadır. Bu kişilerin dijital vatandaşlık pratikleri hem gözlem yoluyla hem de mülakat sorularına verdikleri cevaplarla değerlendirilmeye çalışılmıştır. Bulgular sonucunda azınlıkların dijital platformlarda pratiklerinin yüksek olduğu gözlemlenmiştir.

Karacı, Akyüz & Bilgici (2017), “Üniversite Öğrencilerinin Siber Güvenlik Davranışlarının İncelenmesi” adlı çalışmalarında çeşitli değişkenler açısından üniversite öğrencilerinin siber güvenlik davranışları incelenmiştir. Çalışma grubunu 170 üniversitesi öğrencisi oluşturmaktadır ve verilerin toplanmasında Siber Güvenlik Ölçeği (SGÖ) kullanılmıştır. Çalışmanın sonuçlarına göre öğrencilerin siber güvenliğe yönelik davranışlarının siber güvenliği sağlayacak düzeyde olduğu belirlenmiştir.

Bıkmaz (2017), “Sağlık Yönetimi Bölümü Öğrencilerinin Mobil Güvenlik Farkındalığı Ve Dijital Veri Güvenliği Farkındalıklarının Belirlenmesi” adlı çalışmasında üniversite öğrencilerinin mobil güvenlik ile dijital veri güvenliği farkındalığı ve bu iki beceri arasındaki ilişkiyi belirlemeyi amaçlamıştır. Veriler soru formu, “mobil güvenlik farkındalık anketi”, ve “dijital veri güvenliği farkındalık ölçeği” aracılığıyla toplanmış ve öğrencilerin dijital veri güvenliği farkındalığının güvenlik yazılımları ve kötücül yazılımlardan haberdar olmak, kişisel verilere ulaşma isteği gibi değişkenlere göre değiştiği sonucuna ulaşılmıştır.

Görmez (2017), “Öğretmenlerin Dijital Vatandaşlık ve Alt Boyutları Hakkındaki Düzeyleri (Van İli Örneği)” adlı çalışmasında sadece bir bölümün değil, farklı branşlarda görev yapan öğretmenlerin dijital vatandaşlık ve boyutları hakkındaki düzeylerini belirlemeye çalışmıştır. Bu araştırma örnek olay deseninde yapılmış, nitel bir çalışmadır. Araştırmanın çalışma grubunu 69 sınıf öğretmeni, 34 sosyal bilgiler öğretmeni, 21 görsel sanatlar ve beden eğitimi öğretmeni, 35 türkçe öğretmeni, 25 yabancı dil öğretmeni, 23 fen bilimleri öğretmeni, 23 matematik öğretmeni, 15 teknoloji ve tasarım öğretmeni ve diğer branşlardan 20 öğretmen oluşturmuştur. Çalışma grubu seçiminde maksimum çeşitlilik örnekleme tercih edilmiştir. Veri toplamada ise açık uçlu görüşme formu kullanılmıştır. Elde edilen veriler, içerik analizi yöntemi ile çözümlenmiştir. Bulgulara göre ulaşılan sonuçlar, öğretmenlerin çoğunun dijital vatandaşlığın alt boyutlarına dair bilgi sahibi olmadığı, dijital ticaret ve dijital iletişim kavramlarına sosyal medya ve internet alışverişi aracılığıyla vakıf olduklarıdır.

Turan ve Karasu Avcı (2018), “2018 Sosyal Bilgiler Öğretim Programı'nın Dijital Vatandaşlık Bağlamında İncelenmesi” adlı çalışmalarıyla 2018 SBDÖP'nda yer alan yetkinlikleri ve programda yer alan değerler, beceriler ve kazanımların verildiği öğrenme alanlarında dijital vatandaşlığı incelemektir. Araştırmada nitel araştırma yöntemlerinden biri olan doküman incelemesi tekniği kullanılmıştır. Elde edilen veriler içerik analizi tekniği ile çözümlenmiştir. 2018 SBDÖP'nda "Matematiksel Yetkinlik ve Bilim/Teknolojide Temel Yetkinlikler" ve "Dijital Yetkinlik" dijital vatandaşlıkla ilgili olan yetkinlikler olarak tespit edilmiştir. "Araştırma, çevre okuryazarlığı, dijital okuryazarlık, finansal okuryazarlık, harita okuryazarlığı, hukuk okuryazarlığı, kanıt kullanma, karar verme, konum analizi, medya okuryazarlığı, mekânı algılama, politik okuryazarlık, sosyal katılım, tablo, grafik ve diyagram çizme ve yorumlama, yenilikçi düşünme ve zaman ve kronolojiyi algılama"

doğrudan dijital vatandaşlık ile ilişkilendirilebilen becerilerdir. "Bilimsellik ve dürüstlük" değerleri de doğrudan dijital vatandaşlık ile ilişkilendirilebilen değerlerdir. Öğrenme alanları arasında ise "Bilim, Teknoloji ve Toplum" öğrenme alanı ile "İnsanlar, Yerler ve Çevreler" dijital vatandaşlık ile ilişkilendirilmiştir.

Elçiçek, Erdemci ve Karal (2018), "Online Eğitim Almış Lisansüstü Öğrenciler İçin Dijital Vatandaşlık Düzeyleri ile Sosyal Varlık Arasındaki İlişkinin İncelenmesi" adlı çalışmalarında uzaktan eğitim gören lisansüstü öğrencilerinin dijital vatandaşlık ve sosyal varlık düzeylerini belirlemeyi ve bu iki değişken arasındaki ilişkiyi ortaya koymaya çalışmışlardır. Araştırma Karadeniz Teknik Üniversitesi uzaktan eğitim ile lisansüstü programlarına kayıtlı 50 kadın (%35) ve 93 (%65) erkek öğrenci ile gerçekleştirilmiştir. Veriler "Bireysel Bilgi Formu", "Sosyal Varlık Ölçeği" ve "Dijital Vatandaşlık Ölçeği" ile toplanmıştır. Çalışmada, öğrencilerin dijital vatandaşlık ve sosyal varlık düzeylerini belirlemek için tanımlayıcı istatistikler kullanılmıştır. Değişkenler arasındaki ilişki için korelasyon analizi ve öngörü gücü için doğrusal regresyon kullanılmıştır. Sonuçlar, öğrencilerin dijital vatandaşlık ve sosyal varlıkta yüksek seviyelere sahip olduklarını ve aralarında anlamlı ilişki olduğu anlaşılmıştır. Ayrıca burada cinsiyet açısından anlamlı farklılık görülmemiştir.

Sebetci, Topal, Hanaylı ve Gürel Dönük (2018), "Dijital Ortamda Kişisel Veri Güvenliği ve Sosyal Medya Reklamcılığı Üzerine Bir Değerlendirme" adlı çalışmalarında sosyal medya araçlarının üyelik ve güncellemeler aracılığıyla kişisel verileri depolayıp, başka firmalar ile paylaşmaları sorunundan kaynaklı, kişisel verilerin korunması adına düzenlemelerin yapılmasının zorunlu hale geldiğini ve bu sebeple 2012-2017 yılları arasında Türkiye’de sosyal medya reklamcılığı, veri madenciliği, kişisel veri güvenliği üzerine yapılan çalışmalar incelenmiş, 48 makaleyi derleyip tablolastırmışlardır. Bu çalışmalar ile ilgili içerik analizi yapılmış ve çalışmalar yorumlanarak, genel durum ve eksiklikler ortaya koyarak bu doğrultuda firmalar ve tüketiciler için veri güvenliği hakkında bir takım önerilerde bulunulmuştur. Bu önerilerden biri de sadece medya okuryazarlığının yetmeyeceği, bunu yanı sıra dijital ortamda kişisel veri okuryazarlığının da ele alınmasını ve bunun küçük yaştan itibaren verilmesi gerektiği öneri olarak sunulmuştur.

Özbek (2019), "Öğretmen Adaylarının Siber Güvenlik Farkındalıklarının İncelenmesi" adlı çalışmasında öğretmen adaylarının kişisel siber güvenliğini sağlama durumlarını ortaya

koymayı amaçlamıştır. Bu doğrultuda çalışmada öğretmen adaylarının demografik özellikleri ile kişisel siber güvenliği sağlama durumu arasındaki ilişki incelenmiştir. Araştırmanın örneklemini 809 öğretmen adayı oluşturmuştur ve bu çalışmada ilişkisel tarama yöntemini kullanan araştırmacı çalışmada öğretmen adaylarının kişisel siber güvenliğini sağlama durumlarının orta düzeyde olduğu sonucuna ulaşmış, ayrıca erkek öğretmen adaylarının kadın öğretmen adaylarına göre kişisel siber güvenlik farkındalığının daha fazla olduğu sonucuna ulaşmıştır.

Atasoy ve Ormanlı(2019), “Teknoloji ve Siber Güvenlik: Dijital Toplumun Geleceği” adlı çalışmalarında dijitalleşmeyle birlikte oluşacak dijital toplumun geleceğinde bireyin karşılaşacağı zorluklar, teknolojik gelişmelerin ortaya çıkardığı açıklar, karşılaşılabilecek problemler ve siber güvenlik meselesi eleştirel bir yaklaşımla nitel yöntem doğrultusunda ele alınmıştır.

Dere ve Yavuzay (2019), “Sosyal Bilgiler Öğretmen Adaylarının Dijital Vatandaşlık Göstergelerinin İncelenmesi” adlı çalışmalarında sosyal bilgiler öğretmen adaylarının, dijital vatandaşlık ile ilgili davranışlarını incelemek amacıyla sosyal bilgiler öğretmen adaylarının dijital vatandaşlık ölçeğinden aldıkları puanların üniversite, günlük ortalama internet kullanımı ve e-devlet kullanım sıklığına göre farklılaşıp farklılaşmadığı incelenmiştir. Araştırmada nicel araştırma yöntemlerinden betimsel tarama modeli kullanılmıştır. Bu araştırmanın örneklemini Necmettin Erbakan Üniversitesi, Kastamonu Üniversitesi, Ege Üniversitesi ve Pamukkale Üniversitesi eğitim fakültelerinin sosyal bilgiler Öğretmenliği bölümünde okuyan 401 öğretmen adayı oluşturmaktadır. Verileri toplamak için Som-Vural (2016) tarafından geliştirilen ve 23 maddeden oluşan “Dijital Vatandaşlık Ölçeği” adlı ölçek kullanılmıştır. Analiz sonuçlarına göre; sosyal bilgiler öğretmen adaylarının dijital vatandaşlık ölçeğinden aldıkları puanlar ile okudukları üniversiteler ve günlük ortalama internet kullanım süreleri arasında anlamlı farklılık bulunamamıştır. Buna karşın öğretmen adaylarının e-devlet kullanım sıklığına göre gruplar arasında anlamlı farklılık bulunmuştur.

Sarı (2019), “Sosyal Bilgiler Eğitiminde Öğretmenlere Uygulanan Seminer ve Öğrencilere Yapılan Etkinliklerin Katkıları Bakımından Dijital Vatandaşlık Olgusu” adlı doktora tez araştırmasında dijital vatandaşlık kapsamında sosyal bilgiler eğitiminde gerçekleştirilen etkinliklerin 7. sınıf öğrencilerinin ve sosyal bilgiler öğretmenlerine yapılan seminerin dijital vatandaşlık becerisine katkısını incelemiştir. Bu çalışma deneysel yöntemde karma

metodolojik desen ile yürütülmüştür. Araştırmanın öğrencilerle ilişkili uygulamasında çalışma grubunu 7.sınıfta öğrenim göre 66 öğrenci, öğretmenlerle ilişkili uygulamasında ise 25 sosyal bilgiler öğretmeni ile gerçekleştirilmiştir. Araştırmacı, çalışma kapsamında gerçekleştirilen uygulamaların hem öğretmenlere hem de öğrencilere dijital vatandaşlığın alt boyutları konusunda becerilerinin gelişmesinde katkı sağladığı sonucuna ulaşmıştır. Bu doğrultuda dijital vatandaşlıkla ilgili hizmetiçi seminerlerinin ve yine dijital vatandaşlık doğrultusunda sınıf içi etkinliklerin sosyal bilgiler öğretim programıyla bütünleştirilmesini önermiştir.

Kara ve Atasoy (2019), “Sosyal Bilgiler Öğretim Programı ve Ders Kitaplarının (2018) Dijital Vatandaşlık Kavramı ve Alt Boyutları Bağlamında İncelenmesi” adlı çalışmada yeniden yapılandırılan ve 2018 yılında güncellenen SBDÖP’nin öğrenme alanı ve içeriklerinin dijital vatandaşlık ve alt boyutları açısından değerlendirmesini yapmak ve dijital vatandaş yetiştirmek açısından yeterliliğini ortaya koymayı amaçlamıştır. Bu araştırma nitel araştırma yöntemi, doküman inceleme tekniğinden yararlanılarak uluslararası ve ulusal literatürde yer alan çalışmaları tarayarak oluşturulmuştur. 2018 SBÖP ve ders kitaplarında dijital vatandaş oluşturmada rol oynayabilecek konuların tespiti için içerik analizi kullanılmıştır. Araştırma sonucunda dijital vatandaşlığın ve alt boyutlarının 2018 SBÖP’nde yer alan kazanımlarda yeterli düzeyde yer almadığı, sınıflar bazında ve öğrenme alanlarında yer alan konuların dağılımının ise düzensiz olduğu tespit edilmiştir.

Yalçınkaya ve Cibaroglu (2019), “Dijital Vatandaşlık Algısının İncelenmesi: Ampirik Bir Değerlendirme” adlı çalışmalarında Marmara Üniversitesi Bilgi ve Belge Yönetimi bölümü öğrencilerinin dijital vatandaşlık algısını ölçmek amacıyla yapılmıştır. Bu çalışmada dijital vatandaşlığın 8 alt boyutu doğrultusunda yapılmıştır, toplamda 267 öğrenciye e-posta ile çevrim içi anket gönderilmiş ve 174’ü cevaplamıştır. Elde edilen bulgulara göre öğrencilerin dijital vatandaşlığın alt boyutlarından dijital okuryazarlık, dijital ticaret, dijital etik, dijital iletişim, dijital erişim, dijital güvenlik ve dijital hukuk kavramlarını benimsemiş oldukları görülmüş, fakat dijital sağlık faktörünü dikkate almadıkları anlaşılmıştır.

Aksoy (2019), “Ortaokul Öğrencilerinin Riskli İnternet Davranışları ve Güvenli İnternet Kullanımı Hakkında Öğrenci ve Ebeveyn Görüşleri” adlı yüksek lisans tez çalışmasında ortaokul öğrencilerinin riskli internet davranışlarını ve ebeveynlerinin aldıkları önlemleri belirlemek amaçlanmıştır. Çalışma betimsel araştırma yöntemi ile yürütülmüş, çalışma

grubunu 1102 öğrenci ve 865 ebeveyn oluşturmuştur. Çalışma sonucunda katılımcı öğrencilerden her 4’te 1’inin internet kullanımı sırasında riske maruz kalarak rahatsızlık duyduğu, öğrencileri en çok rahatsız edenler arasında insan ve hayvana şiddet, siber zorbalık, siber tuzak, uygunsuz içerikli ve istemsiz açılan reklamlar, cinsel içerikli paylaşımlardır. Ayrıca internet risklerine karşı savunma konusunda kendilerinden çok ebeveynlerine güvindikleri, ebeveynlerin ise çocuklarının kişisel bilgilerini internette paylaşmalarına izin vermedikleri ve tarayıcı geçmişini kontrol ettikleri sonucuna ulaşılmıştır. Bununla birlikte, öğrencilerin yaşadıklarından rahatsız olma, kendine güven, ebeveyne güven ve öğretmene güven ile cinsiyet, sosyal medya üyeliği, internet kullanım sıklığı arasında anlamlı farklılık olduğu tespit edilmiştir.

Arcagök (2020), “Öğretmenlerin Dijital Vatandaşlığa Yönelik Algılarının İncelenmesi” adlı çalışmasında öğretmenlerin dijital vatandaşlığa yönelik algılarını ve bu algıların cinsiyet, yaş, mesleki kıdem değişkenlerinden ne derece etkilendiğini ortaya koymaya çalışmıştır. Betimsel tarama modelinden yararlanılan araştırmada seçkisiz örnekleme yöntemi kullanılarak, 215 öğretmenden oluşan örneklemden “Dijital Vatandaşlık Ölçeği” aracılığıyla veri toplanmıştır. Elde edilen veriler SPSS paket programı ile analiz edilmiştir. Bulguların normal dağılım gösterdiği saptandığından bağımsız örneklem t testi ve tek yönlü Anova analizleri kullanılmıştır. Araştırma sonucunda öğretmenlerin dijital vatandaşlık algılarının orta düzeyde olduğu, branş değişkeninden etkilenmediği, cinsiyet değişkeni açısından incelendiğinde erkeklerin daha yüksek düzeyde olduğu ve kıdem olarak daha yeni olan öğretmenlerin algı düzeylerinin daha yüksekte olduğu saptanmıştır.

Derin ve Gençoglu (2020), “Ortaokul Öğrencilerinin Bilgi Güvenliği Farkındalığı” adlı çalışmalarında ortaokul öğrencilerinin bilgi güvenliği farkındalığını tespit etmek amacıyla 5,6 ve 7, sınıflarda öğrenim gören 400 öğrenciye araştırmacılar tarafından hazırlanan 30 soruluk “Bilgi Güvenliği Farkındalık Anketi” uygulanmıştır. Elde edilen veriler neticesinde katılımcıların bilgi güvenliği farkındalıkları arasında; cinsiyet, yaş, sınıf, internette geçirdiği süre ve interneti kullanım amacı arasında anlamlı farklılık olduğu belirlenmiştir.

Gökçearslan, Günbatar ve Sarıtepeci (2021), “Ortaöğretim Öğrencilerinin Bilgi Güvenliği Farkındalıklarının İncelenmesi” adlı çalışmalarında bilgi güvenliği farkındalığının çeşitli değişkenler (kişisel bilgisayar, akıllı telefon sahibi olma, bilişim teknolojileri dersi alma ve faydalanma) açısından incelenmesi amaçlanmıştır. Çalışma grubunu 9-12 sınıf aralığında

359 öğrenci oluşturmuş ve tarama modelinde yürütülmüştür. Veri toplama amacıyla Güldüren vd., (2016) tarafından geliştirilmiş “Bilgi Güvenliği Farkındalık Ölçeği” kullanılmış, elde edilen veriler CHAID analizi ile çözümlenmiştir. Bulgular neticesinde, kişisel bilgisayar olma durumu, akıllı telefon sahipliği, BT dersinden alınan fayda değişkenleri anlamlı etkiye sahip olduğu sonucuna ulaşılmıştır.

Gölpek Sarı ve Seferoğlu (2021), “Çevrim İçi Güvenlik ve Risk ile İlgili Eğitime Yönelik Geliştirilmiş Bir Çevrim İçi Ortamın Ortaokul Öğrencilerinin Bilgi Düzeylerine Etkileri” adlı çalışmalarında çevrim içi güvenlik ve riske yönelik tasarlanan eğitime yönelik çevrim içi ortamda yapılan eğitimlerin çevrim içi güvenlik ve risk bilgi düzeyine etkisini incelemek amaçlanmıştır. Çalışmada zayıf deneysel desenlerden tek grup ön test-son test deseni ile yürütülmüş, veriler açık uçlu anket aracılığıyla toplanmıştır. Çalışma grubunu Ankara’da bir ortaokulda öğrenim gören ve bilişim teknolojileri dersi almış olan 30 6. sınıf öğrencisi oluşturmuştur. Çalışmada öğrencilerin çevrim içi güvenlik ve risk bilgi düzeyinin günlük internet kullanım süresi ve çevrim içi güvenlik hakkında bir eğitim almaya yönelik anlamlı bir değişiklik olmadığı sonucuna ulaşılmış, ayrıca çevrim içi güvenlik eğitiminin öğrencilerin çevrim içi güvenlik ve risk bilgi düzeylerine katkıda bulunduğu sonucu tespit edilmiştir.

2.10.2. Yurt Dışında Yapılmış Araştırmalar

Oxley (2010), “Dijital Vatandaşlık: Etik ve Sorumlu Bir Çevrim İçi Kültür Geliştirmek” adlı çalışmasında dijitalleşmenin ve internetin yaygınlaşmasıyla birlikte internetin sorumlu ve etik kullanımının, her yaş grubunu etkilediğini ve dijital ortamda var olan risklerin fazlaca olduğunu buna karşılık korunmasız olan çocukların eğitilmesi gerektiğini savunmuştur. Bu konuda özellikle gençlerin algılanan anonimlikler, dijital ayak izler ve düşüncesin veya kötü niyetli eylemlerin yasal sorumlulukları konusunda etik ve sorumlu bir kültüre sahip olması için bir takım önerilerde bulunmaktadır. Bu açıdan da çevrim içi davranışlarına yönelik nasıl bilinçlendirilebileceğine ve dijital ortamda karşılaştıkları problemleri çözmeye yönelik nasıl eğitilmeleri gerektiğine dair bir takım önerilerde bulunmuştur.

Hollandsworth, Dowdy ve Donovan (2011), “K-12’de Dijital Vatandaşlık: O Bir Köy Gerektirir” adlı çalışmalarında Lübnanlı öğretmenlerin dijital vatandaşlıkla ilgili bilgi ve öz

yeterlik durumlarını tespit etmeyi amaçlamışlardır. Bu amaçla Lübnan’da görev yapmakta olan 378 öğretmenden nicel veri toplanmış ve rastgele örnekleme yöntemiyle 8 öğretmen ile odak grup görüşmeleri yaparak nitel veri toplanmıştır. Bu çalışmada araştırmacılar öğretmenlerin dijital vatandaşlık bilgi ve öz yeterlik düzeyinin yeterli olmadığını ortaya koymuştur. Bu sebeple bu çalışma vatandaşların gerçek bir dijital vatandaş olması amacıyla bir dizi öneriler sunmaktadır.

Krasna ve Bratina (2011), “Dijital Yerliler Arasında Dijital Güvenlik Algısı” adlı çalışmalarında Slovenya’da yaşamakta olan 147 öğrenciye (1. ve 3. sınıfta olan iki kuşak öğrenci) çevrim içi anket uygulanarak dijital güvenlik algıları hakkında veri toplanmıştır. Araştırmada veri güvenliğine odaklanılmıştır (dolandırıcılığı tanıma ve kimlik hırsızlığı). Araştırmadan elde edilen verilere göre araştırmacılar, öğrencilerin dolandırıcılığı tanıma konusunda son derece bilgili olduğunu, kimlik hırsızlığı konusunda daha kısıtlı bilgi sahibi ve veri güvenliği anlamında son derece yetersiz olduklarını tespit etmişlerdir.

Bratina ve Krasna (2011), “Dijital Güvenliğe Karşı Öğrencilerin Tutumu” adlı çalışmalarında e-öğrenme materyalleri dağıtımında yeni yaklaşımların, öğrenme yönetim sistemlerinden yararlandığı için dijital yeterliklerin değerinin daha da yükseldiğini belirtmişlerdir. Bu çalışmada dijital yetkinliğin dijital güvenlik konusunun genişletilmesi gerektiği vurgulanmaktadır. Sosyal ağlar ve anlık mesajlaşma programlarının, kullanıcıların yabancılarla iletişim kurmalarını sağladığı ve dijital yerlilerin de dijital güvenlik konusunda yetersiz olduğu belirtilmiştir. Çalışmalarla öğrencileri farklı eğitim düzeylerinde gözlemleyerek, dijital güvenlik sorununa neredeyse kayıtsız olduklarını ve kişisel verileri tereddüt etmeden yayınladıklarının keşfedildiğini ve Web hizmetlerinin güvenli kullanımını teşvik etmek için öğretmenlerin, öğrencilerine güvenilir ve yetkin bilgiler vermesi gerektiğini ileri sürmektedirler. Araştırmacılar Slovenya’daki ilkökul ve ortaokul müfredatının analizi, dijital güvenlik konularının eğitime dahil edilmediğini belirtmişler. Bu sorunlar yaygınlaştığı için öğretmenlere yönelik öneriler ders kitapları, Web sayfaları, eğitim CD’leri şeklinde mevcut olduğunu fakat onlardan dahi haberdar olmadıklarını belirterek, potansiyel dijital tehditin öğrenciler tarafından ne düzeyde tanındığını ortaya koymak amacıyla anketler yapılmıştır.

Krasna ve Bratina (2012), “Eğitim Bilimlerinde Dijital Güvenlik Dersi Tasarımı” adlı çalışmalarında daha önce geliştirilen anketi kullanarak öğrencilerin ve öğretmenlerin dijital

güvenlik algılarını tespit ederek dijital güvenlik dersi tasarımı yapmayı amaçlamışlardır. Araştırmacılar eğitimde dijital güvenliğin ihmal edildiğini ve bunun da son 2 yılda yapılan çalışmalardan elde edilen bulgularla desteklendiğini ifade etmektedirler. Ayrıca bu çalışmada Slovenya’da uygulanan çevrim içi anketten elde edilen bulgulardan hareketle öğrencilerin dijital güvenlikte tamamen yetersiz olduğu sonucuna da ulaşılmıştır. Araştırmacılar dijital güvenlik eğitimi amacıyla 2012 yılında yüksek lisans kursu oluşturduklarını belirtmişlerdir. Bununla birlikte bu çalışmada dijital güvenlik dersinde hangi konuların olması gerektiğine odaklanılmıştır ve eğitimin içeriğinde veri güvenliği, bilgisayar virüsleri, bilgisayar dolandırıcılığı, casus yazılım ve kimlik hırsızlığı konularının olması gerektiği ifade edilmiştir.

Ribble (2012), “Eğitimde Değişim İçin Dijital Vatandaşlık” adlı çalışmasında dijital teknolojilerle çok iç içe bir yaşamı olan öğrencilerin, bu ortamlardan oldukça etkilendikleri ve öğretmenlerin de bu konuda onları denetleyemediklerini, yönlendirme konusunda yetersiz kaldıklarını belirtmiştir. Bu sebeple öğretmenlerin yetiştirilmesi gerektiğini ve bunun için okullarında teknoloji personelleri ile birlikte çalışmaları, eğitim müfredatı ile de desteklenmesi ve dijital vatandaşlığın derslere nasıl entegre edileceğinin planlanması gerektiğini savunmuştur. Teknolojinin etkisinin giderek büyümesiyle birlikte, hem okul içinde hem de okul dışında etkili dijital vatandaşlar olmaları için gerekli becerilerin giderek artacağını ve bu sebeple eğitimin hemen gerekli olduğunu vurgulamıştır.

Al-Zahrani (2015), “Dijital Vatandaşlığa Doğru: Yüksek Öğretim Öğrencileri Arasında İnternet Toplumuna Katılım ve Katılımı Etkileyen Faktörleri İncelemek” adlı çalışmasında Üniversite öğrencilerinin dijital vatandaşlık düzeyi ve onu etkileyen faktörleri incelemeyi amaçlamıştır. Bu amaç doğrultusunda Suudi Arabistan’da Kral Abdilaziz Üniversitesinde öğrenim görmekte olan 174 öğrenciden “İnternet Tutum Ölçeği”, “Bilgisayar Öz-Yeterlik Ölçeği” ve “Dijital Vatandaşlık Ölçeği” aracılığıyla veri toplanarak nicel bir araştırma gerçekleştirilmiştir. Çalışmada elde edilen bulgulardan hareketle öğrencilerin internet tutumu, bilgisayar öz yeterliliği ve dijital vatandaşlığa, özellikle de çevrim içi olarak kendine ve başkalarına saygı duyma açısından iyi seviyelere sahip olduğu sonucuna ulaşılmıştır. Dijital vatandaşlığı etkileyen faktörler bilgisayar deneyimi, günlük ortalama teknoloji kullanımı, öğrencilerin internete yönelik tutumları ve bilgisayar öz yeterliliği olarak belirlenmiştir.

Snyder (2016), “Öğretmenlerin Sosyal Medya ve Küresel İşbirlikçi Projeler Kullanarak Ortaokul Öğrencilerinde Dijital Vatandaşlık Algılarının Gelişimi” adlı doktora tez araştırmasının kuramsal çatısı, Ribble’ın dijital vatandaşlık teorisine dayalı olarak nitel bir yöntem ile oluşturulmuştur. Veri elde etmek amacıyla görüşme tekniği uygulanmış, 7 öğretmen ve 1 proje danışmanı ile görüşülmüştür. Araştırmada elde edilen verilerden hareketle araştırmacı, küresel işbirliği ve sosyal medya proje çalışmalarının öğrencilerin dijital vatandaşlık algıları üzerinde etkili olduğu, öğrencileri güdülediği sonucuna ulaşmıştır.

Byrne, Dvorak, Peters, Ray, Howe ve Sanchez (2016), “Kullanıcı Açısından: İnternet Kullanımı İle İlgili Faydalara Göre Risk Algısı” adlı çalışmalarında kullanıcıların kendi kullanımları açısından algıları belirlenmiştir. Bu doğrultuda katılımcılar internet kullanımları sırasındaki eylemlerini listelemeleri istenmiş ve bu eylemleri neden yaptıkları anket aracılığıyla ölçülmüştür. Araştırmacıların çalışmadan elde ettikleri verilere göre ulaşılan eylem listesinin riskleri ve faydaları da sıralanmıştır. Çalışmanın sonucunda ortaya çıkan liste gelecekte çalışmalarda kullanılabilecek internet eylem listesi sağlamıştır.

Bratina (2016), “Gelecekteki Öğretmenlerin Dijital Riskleri ve Deneyimleri” adlı çalışmasında Slovenya Maribor Üniversitesindeki öğretmen adaylarının dijital ortamda maruz kaldığı riskler ve bu risklere karşı davranışlarını tespit etmeyi amaçlamıştır. Bu amaçla üniversitenin ilkokul, okul öncesi eğitim, pedagoji, güzel sanatlar ve müzik eğitimi bölümlerinde öğrenim görmekte olan 18-24 yaş aralığında 153 öğrenciye çevrim içi bir anket uygulanarak veri toplanmıştır. Bulgulardan hareketle öğrencilerin kimlik avı riskini anlayabildiğini ve bu kavrama aşına oldukları sonucuna ulaşılmıştır. Bununla birlikte kötü amaçlı yazılım riskinin anlaşılma oranının düşük olduğu, dolandırıcılığın tanınabildiği de ifade edilmiştir. Fakat yine de öğrencilerin bu konularda yeterli düzeyde olmadığı ve gerekli eğitimlerin verilmesi gerektiği önerilmiştir.

Holland (2017), “Ortaokul Öğreniminde Dijital Vatandaşlık Algısı” adlı doktora tez araştırmasını nitel araştırma yöntemi ile yürütmüş ve dijital vatandaşlığa dayalı etkinliklerin öğrencilerin dijital vatandaşlık algıları üzerindeki etkisini araştırmıştır. Bu çalışmanın çerçevesi Ribble’ın (2006) dijital vatandaşlık teorisine, Siemens’ in (2005) bağıcılık teorisine ve dijital okuryazarlık teorilerine dayanmaktadır. Araştırmanın çalışma grubunu üstün yetenekli ve ortaokul programına kayıtlı yedi öğrenci oluşturmuştur. Veri toplamak amacıyla röportaj, anket ve gözlem kullanılmıştır. Veri analizinde içerik analizi tekniği kullanılmıştır.

Araştırma sonucunda, dijital vatandaşlığa ilişkin olumlu algıların arttığı gözlenmiş, özellikle eğilimler arasında 3 boyuta daha fazla katkı sağladığı tespit edilmiştir. Bunlar: Dijital etik, dijital iletişim ve dijital okuryazarlıktır.

Hadlington (2017), “Siber Güvenlikte İnsan Faktörleri; İnternet Arasındaki Bağlantının İncelenmesi Bağımlılık, Dürtüsellik, Siber Güvenliğe Yönelik Tutumlar ve Riskli Siber Güvenlik Davranışları” adlı çalışmasında siber güvenlik, internet bağımlılığı ve dürtüsellik davranış ve tutumlarını incelemeyi amaçlamıştır. Araştırmada veri toplamak amacıyla Birleşik Krallıkta istihdam eden 515 kişiye yanıt alınan çevrim içi anket (dürtüsellik, siber güvenlik, internet bağımlılığı ve riskli siber güvenlik davranış ölçeği içermektedir) uygulanmış ve internet bağımlılığının riskli siber güvenlik davranışında önemli bir faktör olduğu sonucuna ulaşılmıştır. Ayrıca siber güvenliğe karşı olumlu tutumun riskli siber güvenlikte negatif yordayıcı olduğu, dürtüsellüğün ise pozitif yordayıcı olduğu sonucuna ulaşılmıştır.

Hintz, Dencik ve Jorgensen (2017), “Dijital Vatandaşlık ve Gözetim Toplumu” adlı çalışmalarında dijital vatandaşlığın bileşenlerini ve koşullarını araştırmayı amaçlamıştır. Bu amaç doğrultusunda Birleşik Krallıkta disiplinlerarası bir ekip ile 2014-2016 yılları arasında Snowden sızıntılarının teknoloji, politika, haber medyası ve sivil toplum olarak adlandırılan tematik alanlardaki etkilerini inceledi. Bu doğrultuda politika belgesi analizi, odak grupları, uzman görüşmeleri ve medya içeriği analizi yaparak karma bir yöntem kullanıldı. Araştırma sonuçlarında Snowden ifşaları hem devlet mekanizmalarını hem teknoloji firmalarını hem de vatandaşların faaliyetlerini etkilediği belirtilmektedir. Buna göre aslında bu araştırma gizlilik ve güvenliğin dijital vatandaşlığı önemli ölçüde etkilediğini ifade etmektedir.

Walters (2018), “İlköğretim Öğretmenlerinin Bilgi, İnanç ve Dijital Vatandaşlık için Planlanan ve Uygulanan Uygulamaları” adlı doktora tez çalışmasında ilköğretim öğrencilerinin dijital vatandaşlık hakkındaki bilgi ve inançlarını belirlemek, dijital vatandaşlık eğitimi ile ilgili plan ve uygulamalarını, desteklerini ve engellerini anlamak amaçlanmıştır. Araştırma kapsamında literatürden geliştirilen anket ile 74 eğitmenen veri toplanmıştır. Araştırmadan elde edilen sonuçlara göre eğitmenlerin dijital hukuk haricinde dijital vatandaşlık kavramları hakkında yüksek bilgi ve inançlara sahip olduğu tespit edilmiştir. Buna ek olarak teknoloji-cihaz entegrasyonunun dijital vatandaşlık eğitim ve

uygulamalarında etkili olduđu ve öğrenciler üzerinde sosyal değişime katkıda bulunduđu tespit edilmiştir.

Gleason ve Gillern (2018), “Sosyal Medya ile Dijital Vatandaşlık: Ortaöğretimde Öğretmen ve Öğrenmenin Katılımcı Uygulamaları” adlı çalışmalarında ortaokul öğrencilerine yönelik olarak sosyal medya kullanımının dijital vatandaşlığın gelişimi üzerindeki etkisini araştırmayı amaçlamaktadır. Bu amaçla deneysel desende yürütölen bu araştırma dijital vatandaş olarak sivil katılımın kavramsal bir analizini sunmuş ve dijital medya uygulamalarının dijital vatandaşlık eğitimini geliştirmekte nasıl destek olabileceğini araştırmıştır. Ayrıca bu araştırma dijital vatandaşlığın her iki boyutunun (okul içi ve okul dışı faaliyetler) sosyal medya tarafından kolaylaştırılmış bir müfredat ile okullara entegre edilebileceğini göstermektedir.

Dodel ve Mesch (2018), “Dijital Becerilerde Eşitsizlik ve Çevrim İçi Güvenlik Davranışlarının Benimsenmesi” adlı çalışmalarında siber güvenliğin değişkenlerini belirlemek amaçlanmıştır. Amaç doğrultusunda dijital güvenlik becerisinde cinsiyet, yaş, eğitim ve erişim kalitesi yordanmıştır. Araştırma verileri İsrail’de yaşayan 1850 kişiden toplanmıştır. Elde edilen verilere göre dijital güvenlik becerisi ile yaş, cinsiyet, eğitim ve erişim kalitesinin ilişkili olduđu sonucuna da ulaşılmıştır. Sonuçlara göre dijital beceri ile yaş olumsuz yönde ilişki, cinsiyete göre ise erkekler kadınlardan daha iyi teknik beceri eğilimine sahip ve sosyoekonomik durumlar kadınları dijital beceriler konusunda olumsuz yönde etkilemektedir. Ayrıca çalışmanın sonuçlarına göre sosyal ve dijital eşitsizlik çevrim içi riskleri önleme davranışını da olumsuz anlamda etkilediğı belirtilmiştir.

Hartikainen, Livari ve Kinnula (2019), “Çevrim İçi Güvenlik Eğitimi İçin Çocuk Tasarım Önerileri” adlı çalışmalarında çocukların çevrim içi güvenlik eğitimine yönelik algılarını belirlemek amaçlanmıştır. Bu amaçla 11-12 yaş aralığındaki çocuklarla atölye çalışmaları yürütölmüş ve gelecekteki eğitim için beyin fırtınası önerileri hazırlanmıştır. Schwartz'ın temel insani değerler teorisinin merceğini kullanarak sonuçların analiz edildiğı çalışmada, çevrim içi güvenlik eğitimi uygulayıcılarının eğitim paketleri geliştirirken göz önünde bulundurulması gereken hususları şöyle açıklamışlardır: hem çocuk hem de eğitimcilerin amaç ve ilgili değerleri göz önünde bulundurulmalı, çocukların medya kültürü dikkate alınmalı, olumlu bir ses tonu kullanılmalı hem çocukların hem de eğitimcilerin tasarım ve değerlendirmeye dahil edilmelidir.

Kumar, Chetty, Clegg ve Vitak (2019), “İlkokullarda Dijital Teknoloji Kullanımı için Gizlilik ve Güvenlik Hususları” adlı çalışmalarında gizlilik ve güvenliğin ilköğretim eğiticileri için ne anlama geldiğini daha iyi anlamak amacıyla ABD'nin kuzeydoğusundaki üç metropol bölgesinde 25 eğitimciyle dokuz odak grubu gerçekleştirilmiştir. Araştırma sonuçlarında, teknoloji kullanımının ilköğretim sınıfları için gerekliliği, eğitimcilerin dijital gizlilik ve güvenliği müfredat ve sınıf yönetimi konusunda önemseyişi, derslerde çocuklara dijital gizlilik ve güvenlik hakkında eğitimin nadiren görüldüğü bulgularına rastlanmıştır. Bu doğrultuda dijital gizlilik ve güvenlik eğitiminde teknolojinin entegre edilmesi gerektiği ve çocukların dijital gizlilik ve güvenlik hakkında bilgi edinmelerine yardımcı olmak için tasarım fırsatları belirlenmiştir.

Allema (2019), “Siber Zorbalık ve Cinsiyet: Ortaokul Kızlarının Siber Zorbalığı Nasıl Yaşadıklarına Dair Nitel Bir Çalışma” adlı doktora tez çalışmasında ortaokul personeli ile görüşülerek ortaokul kız öğrencilerinin siber zorbalık deneyimlerini daha iyi anlamak amaçlanmıştır. Nitel araştırma modeli kapsamında görüşme yöntemi ile veriler toplanmış ve elde edilen veriler neticesinde 3 tema ortaya çıkmıştır. Ortaya çıkan temalar, kızların siber zorbalık konusunda savunmasız olduğu, siber zorbalık deneyimlerinin önemi ve katılan personellerin siber zorbalık sonrası deneyimleridir. Bu çalışmada, siber zorbalığın mağdurlar üzerindeki akademik, sosyal ve psikolojik etkiler üzerinde olumsuz etkisinin olduğu ifade edilmiştir.

Desimpelaere, Hudders ve Sompel (2020), “Gizliliği Koruma Stratejisi Olarak Bilgi: Gizlilik Okuryazarlığı Eğitiminin Çocukların Çevrim İçi İfşa Davranışlarına Etkisi” adlı çalışmalarında gizlilik okuryazarlığı eğitiminin 9-13 yaş arası çocukların gizlilik okuryazarlığına, çevrim içi ifşa davranışlarını nasıl etkilediğini ve gizlilik maliyetleriyle ilgili kaygılarını nasıl etkilediğini tespit etmek amaçlanmıştır. Bu amaçla çalışma kapsamında gizlilik okuryazarlığı ile ilgili çevrim içi olarak 2 eğitim verilmiş, 1. eğitimde 214, 2. eğitimde 366 katılımcı bulunmaktadır. Eğitimler neticesinde çocukların gizlilik okuryazarlığının iyileştiği tespit edilmiştir. Bununla birlikte küçük çocuklar arasında ifşa davranışının arttığı sonucuna da ulaşılmıştır. Çalışma kapsamında çocukların çevrim içi gizlilikleriyle ilgili başa çıkma davranışlarında kapsamlı bir anlayış sunulmuş ve politika yapımcılar ve eğitimciler için önerilerde bulunulmuştur.

Manotipya ve Ghazinour (2020), “Ebeveynlerin Bakış Açısından Çocukların Çevrim İçi Gizliliği” adlı çalışmalarında ebeveynlerin çocuklarının çevrim içi gizliliği hakkında algılarını tespit etmek ve çocuklarının bilgilerini çevrim içi paylaşıırken gizliliğe dikkat etmeleri hususunda oyun tabanlı bir öğrenme kullanmak amaçlanmıştır. Çalışmada ebeveynlerin çocukları hakkında algılarını tespit etmek için anket kullanılmış ve sonuç olarak ebeveynlerin çocuklarının çevrim içi gizliliği konusunda farkındalık düzeylerinin yüksek olmasına rağmen çevrim içi ortamda onların gizliliğini tehlikeye attıkları tespit edilmiştir. Ayrıca ebeveynlerin çocukların kişisel bilgilerini sosyal medyada paylaşıırken daha dikkatli olmaları gerektiği sonucuna ulaşılmıştır. Bununla birlikte çalışmada çocukların sosyal medya kullanımında çevrim içi gizlilik konusunda eğitilmesi için araçların geliştirilmesi ve ebeveynlerin de eğitilmesi gerektiği önerilmiştir.

Macaulay, Boulton, Betts, Boulton, Camerone, Down, Hughes, Kirkbride ve Kirkham (2020), “Birleşik Krallık'ta Çocukların Algılanan Çevrim İçi Güvenliği ve E-Güvenlik Eğitimine Yönelik Tutumlarının Belirleyicileri Olarak Çevrim İçi Güvenlik / Tehlikelere İlişkin Özel ve Nesnel Bilgi” adlı çalışmalarında çocukların özel ve nesnel bilgilerinin algılanan çevrim içi güvenlikleri ve e-güvenlik eğitime yönelik tutumları üzerindeki etkisini belirlemeyi amaçlamışlardır. Bu amaçla 8-11 yaş aralığındaki 329 öğrenciye uygulanan anket sonuçlarında katılımcıların çoğu (özellikle erkekler ve küçük çocuklar) çevrim içi ortamda kendini güvende hissettiğini ve çevrim içi tehlikeler hakkında farkındalıklarının iyi düzeyde olduğu, kaçınma yollarını bilseler de tehlikelerin tam olarak ne olduğunu ve kişisel güvenlikleri için kaçınma yollarını ifade etmekte zayıf oldukları tespit edilmiştir. Bununla birlikte bazı çocukların çevrim içi ortamda nasıl güvende kalacaklarını bildikleri ancak gerçekte güvenliklerini sağlamak için nesnel bilgidен yoksun oldukları, bunu en azından ifade edemedikleri bulgularına da rastlanmıştır. Çalışma sonunda çocukların çevrim içi güvenlik ve tehditleri hakkında nesnel bilgilere yönelik eğitimin verilmesi gerektiği önerilmektedir.

Quayyum, Cruzes ve Jaccheri (2021), “Çocuklar İçin Siber Güvenlik Bilinci: Sistematiк Bir Literatür Taraması” adlı çalışmalarında çocuklarda siber güvenlik bilincine dair yapılan araştırmalara ilişkin mevcut bulguların özetlenmesi ve gelecekteki çalışmalara yol göstermek amaçlanmıştır. Siber güvenlik risk ve bilinçlendirme yaklaşımlarıyla ilgili 56 çalışma incelenerek literatür taraması yapılan bu çalışmada çocuklar için siber güvenlik

riskleriyle ilgili bir liste, çocuklar arasında siber güvenlik bilincini artırmak için kullanılan yaklaşım ve teorilerin listesi ve araştırmacıların bu konularla ilgili değerlendirmelerinde göz önünde bulundurdıkları faktörlerin listesi sunulmuştur.

Al-Rob (2021), “Filistinli Ergenler Arasında Siber Zorbalık ve İnternet Bağımlılığı” adlı çalışmada Filistinli ergenlerde siber zorbalık davranışı ile internet bağımlılığı arasındaki ilişkiyi belirlemek amaçlanmıştır. Çalışma grubunu 500 katılımcı oluşturmaktadır. Elde edilen bulgulara göre, internet bağımlılığının yanlış ve sık teknoloji kullanımından kaynaklandığı ve siber zorbalık derecesinin orta düzeyde olduğu belirlenmiştir. Bununla birlikte bu çalışmada internet bağımlılığı ile siber zorbalık davranışı arasında anlamlı düzeyde pozitif bir ilişkinin olduğu tespit edilmiştir.

Ong'ong'a (2021), “Kenya'da Çevrim İçi Dijital Güvensizlik Bildiren 12-14 Yaş Arası Gençler Hakkında Öğretmenlerin Algısı, Deneyimleri ve Zorlukları” adlı çalışmasında öğretmenlerin Kenya'da çevrim içi güvenlik sorunları bildiren 12-14 yaşındaki gençler üzerindeki algıları, deneyimleri ve yaşanan zorlukların belirlenmesi amaçlanmıştır. Çalışma amacı doğrultusunda, içsel vaka çalışması deseni çerçevesinde 23 okul yöneticisi ve öğretmen ile derinlemesine görüşme tekniği kullanılarak veri toplanmış ve veriler tematik olarak analiz edilmiştir. Çalışma neticesinde, öğretmenlerin gençleri korumak için çevrim içi güvenlik becerileri ve yetkinliği konusunda yetersiz olduğu belirlenmiştir. Bu çalışmada dijital güvensizliğin müfredata entegre edilmesi, öğretmenlerin dijital okuryazarlık eğitimi alması gerektiği önerilmektedir.

Mordecai (2021), “Öğrenci Veri Gizliliğini ve Yenilikçiliği Dengeleme: Hawai'i Devlet Okullarında Uygulamalar ve Algılar” adlı doktora tez çalışmasında devlet okullarında mahremiyet ve inovasyonu dengelemenin karmaşıklıklarını araştırmak amaçlanmıştır. Çalışma keşif vaka çalışması yöntemiyle, Hawai'deki bir okul bölgesindeki K-12 öğrenci veri gizliliği uygulamalarını farklı bölge düzeyinde ve okul düzeyinde personel perspektifinde anlamak için 3 farklı çalışma yapılmıştır. Çalışma sonucunda öğrenci veri gizliliği için iletişimin iyileştirilmesi, eğitimin artırılması ve mevcut uygulamaların öğrenci merkezli olarak planlanması gerektiği bulgusuna ulaşılmıştır. Çalışma okul bölgelerine etkili ve güvenli veri paylaşımı uygulamaları için önerilerde bulunmuştur.

Walsh, Pink, Ayling, Sondergeld, Dallaston, Tournas, Serry, Trotter, Spanos ve Rogic (2022), “Çevrim İçi Güvenlik Eğitimi İçin En İyi Uygulama Çerçevesi: Uluslararası

Literatürün Hızlı Bir Şekilde Gözden Geçirilmesi, Uzman İncelemesi ve Paydaş Danışmanlığının Sonuçları” adlı çalışmalarında keşif sıralı karma yöntemler kullanılarak çevrim içi güvenlik eğitimi çerçevesi oluşturulmak amaçlanmıştır. Bu amaç çerçevesinde ilk aşamada mevcut uygulamalar sıralı bir şekilde incelenmiş, ikinci aşamada mevcut çerçeveyi test etmek, iyileştirmek ve sonuçlandırmak için uzman incelemesi ve paydaş danışmanlığı yapılmıştır. Araştırma sonucunda dijital güvenlik eğitiminin çerçevesi oluşturulmuş ve bu çerçevede 5 boyut ortaya çıkmıştır. Bu boyutlar, Öğrencilerin hak ve sorumlulukları, dayanıklılık ve risk, etkili olan bütün okul yaklaşımları, entegre ve özel müfredat, gözden geçirme ve değerlendirme yoluyla sürekli iyileştirme.



BÖLÜM III

YÖNTEM

Bu bölümde araştırmanın yöntemi, araştırmada kullanılan desen, çalışma grubu, öğretim materyali, veri toplama araçları, uygulama süreci ve verilerin analizi ile ilgili bilgilere yer verilmiştir.

3.1. Araştırmanın Modeli

Bu çalışmada, sosyal bilgiler dersinde 7. sınıf öğrencilerinin dijital güvenlik yeterliği için geliştirilen çevrim içi destekleyici öğrenme aracının dijital güvenlik öz yeterlik algılarına etkisi belirlenmeye çalışılmıştır. Çalışmada belirlenen amaç doğrultusunda deneysel araştırma yöntemi kullanılmıştır. Büyüköztürk, Kılıç Çakmak, Akgün, Karadeniz ve Demirel (2020) deneysel araştırmayı “*araştırmacı tarafından oluşturulan farkların bağımlı değişken üzerindeki etkisini test etmeye yönelik çalışmalar*” olarak tanımlamıştır (s.202).

Deneysel araştırma yönteminin bilimsel araştırmalar için olumlu özellikleri bulunmaktadır. Deneysel araştırma yönteminin önemli özelliklerinden biri karşılaştırmalı işlemler uygulayarak bunların etkisini incelemesidir ve en kesin sonuca ulaşılan güçlü bir metodoloji olarak görülmektedir (Büyüköztürk vd., 2020, s.19).

Fraenkel, Wallen ve Hyun (2011), geçmiş araştırmalara bakıldığında sebep sonuç çalışmaları için en etkili yöntemin deneysel araştırmalar olduğunu belirterek, deneysel araştırma yöntemini kısaca şöyle ifade etmiştir; “*bazı şeyleri dene ve neler olup bittiğini sistematik olarak gözle*”(s.266). Bu bilgiler doğrultusunda deneysel araştırma modelinin,

araştırmacı tarafından üretilen ürünün yine araştırmacı kontrolünde olan ortamda neden sonuç ilişkisinin izlenmesi için etkili ve kesin sonuca ulaştıran bir yöntem olduğu söylenebilir.

Fraenkel vd. (2011) deneysel araştırmayı diğer araştırmalardan ayıran iki benzersiz özellik bulunduğunu ve birinci özelliğin, deneysel araştırmanın belirli bir değişkeni direkt etkilemeye çalışan tek tür olduğunu, ikincisinin ise araştırmacı tarafından değişkenin manipüle edilebilme özelliği olduğunu belirtmiştir (s.265). Burada deneysel yöntemi özel kılan durumlardan biri de değişkenin araştırmacı tarafından manipüle edilebilmesidir. Bu açıdan eğitim araştırmalarında deneysel yöntem etkili ve yaratıcı bir şekilde kullanılabilir. Bu konuda Fraenkel vd. (2011) deneysel araştırmaların eğitim araştırmalarında nasıl kullanıldığını şöyle ifade etmektedir;

“Eğitim araştırmalarında sıklıkla manipüle edilen bağımsız değişkenler arasında öğretim yöntemleri, ödev türleri, öğrenme materyalleri, öğrencilere verilen ödüller ve öğretmenler tarafından sorulan soru türleri bulunur. Sıklıkla çalışılan bağımlı değişkenler arasında başarı, bir konuya ilgi, dikkat süresi, motivasyon ve okula yönelik tutumlar yer alır” (s. 265).

Deneysel yöntemin eğitim araştırmalarında kullanılmasındaki temel amaç, problem durumunun seçilen çözüm yöntemi sonucunda fark yaratıp yaratmadığının görülmek istenmesidir. Bu durumu araştırmacı ilk durum ile son durum arasındaki puan farkına bakarak ortaya koymaktadır.

Her araştırma modelinde olduğu gibi deneysel araştırma yönteminde de olması gereken özellikler bulunmaktadır ve araştırmanın yöntemine uygun olarak yapılması için bu kriterlere uyulması gerekmektedir.

Fraenkel vd. (2011) ise deneysel araştırmaların dört temel özelliğinden bahsetmektedir:

1. Grupların karşılaştırılması
2. Bağımsız değişkenin manipüle edilmesi
3. Seçkisizlik
4. Dışsal değişkenlerin kontrolü (s.266-267)

Büyüköztürk vd. (2020) deneysel araştırma türlerini öncelikli olarak denek sayısına göre sınıflandırarak tek denekli desenler ve çok denekli desenler olmak üzere ikiye ayırmaktadır (s.206). Tek denekli desenler tek bir denekle yürütülür ve genellikle birçok aşamadan oluşan

faktörlerin kontrol edildiği uzun süreli bir desendir. Bu desende aşamalı ölçümler yapılabilmektedir ve genellikle klinik psikoloji, özel eğitim vb. alanlarda kullanılır.

Büyüköztürk vd. (2020), denek sayısına göre yapılan sınıflandırmada çok denekli desenleri bağımlı değişken üzerinde etkisi incelenen faktör sayısı bakımından ele alındığında çok denekli desenlerin tek faktörlü desen ve çok faktörlü desen olarak 2'ye ayrıldığını belirtmiştir. Faktör sayısı açısından sınıflandırılan çok denekli desenler 4 türden oluşmaktadır;

1.*Zayıf deneysel desenler*

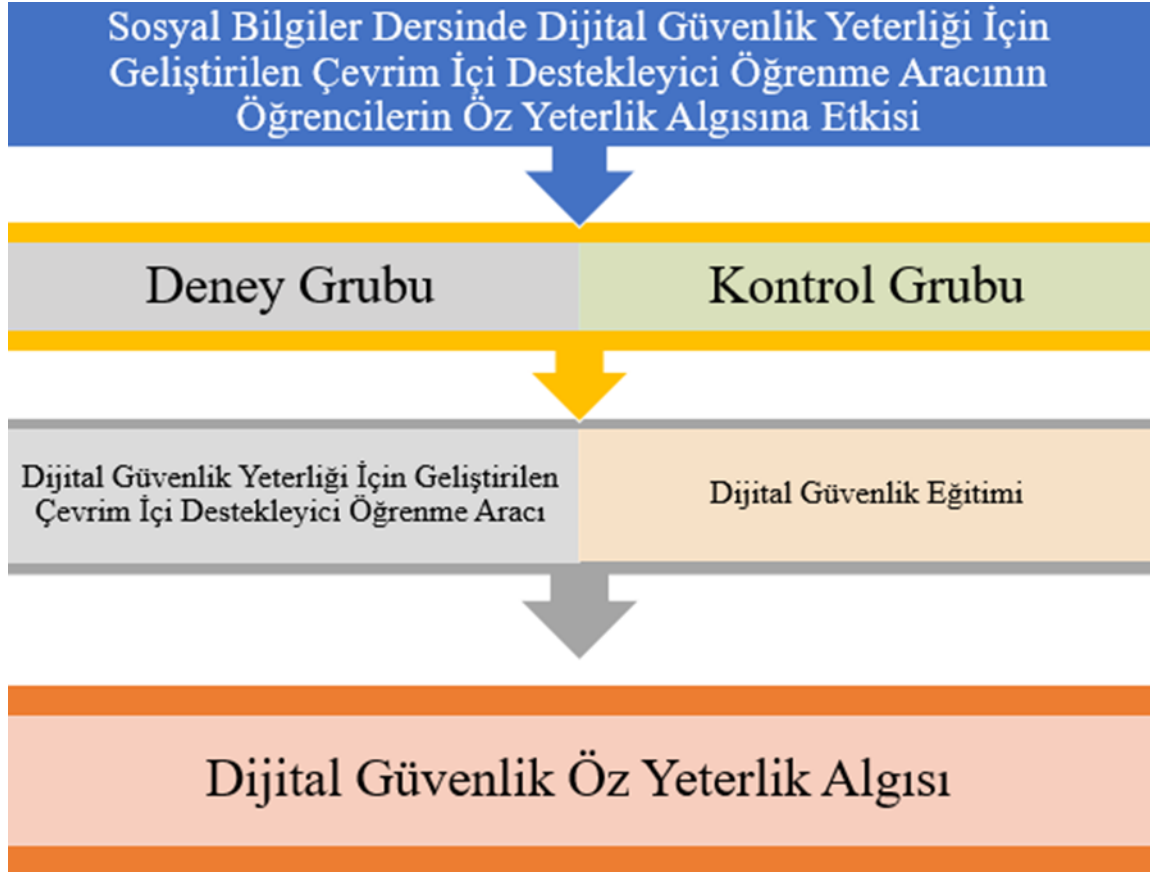
2.*Gerçek deneysel desenler*

3.*Faktöryel desenler*

4.*Yarı deneysel desenler* (Büyüköztürk vd., 2020, s.266).

Bu çalışmada denek sayısına göre sınıflandırılan deneysel araştırma türlerinden çok denekli desenlerden yarı deneysel desen tercih edilmiştir. Yarı deneysel desen, seçkisiz atama içermeyen ve iki türü olan bir desendir. Bu sınıflandırmaya göre çalışmada yarı deneysel desenlerden Campbell ve Stanley (1996)'in geliştirdiği” *ön test-son test eşleştirilmiş kontrol gruplu yarı deneysel desen*” tercih edilmiştir. Bu desenin tercih edilmesinde temel sebep, desenin araştırmacı tarafından geliştirilen araçların denenmesinde kontrol edebilme fırsatı sunmasıdır. Gerçek deneysel desenden farkı ise seçkisiz atama kullanılmamasıdır. Fakat seçkisiz atama okul ve sınıf ortamında pek mümkün kılınmadığı için kullanımı zordur. Bu sebeple deneyin iç geçerliğini sağlamak için birbirine eşit olmasa da ön test puanları birbirine denk sayılabilecek ve karşılaştırılabilir deney ve kontrol grupları kullanılmaktadır (Campbell ve Stanley, 1996).

Çalışmanın araştırma değişkenleri incelendiğinde ortaokul 7. sınıf öğrencilerinin dijital güvenlik öz yeterlik düzeyleri, üzerinde bir değişkenin etkisinin ölçümlenebilir olmasından dolayı bağımlı değişken; dijital güvenlik yeterliği için geliştirilmiş olan çevrim içi destekleyici öğrenme aracı araştırmacı tarafından manipüle edilebilme ve değiştirilebilme özelliğinden dolayı bağımsız değişken konumundadır ve kontrol altına alınmıştır.



Şekil 4. Araştırmanın deneysel işleminin akış şeması

3.2. Çalışma Grubu

Bu araştırmada, çalışma grubunun belirlenmesinde seçkisiz olmayan örnekleme yöntemlerinden uygun (elverişli) örnekleme yöntemi kullanılmıştır. Uygun (elverişli) örnekleme çalışmaya hazır olan ve yakın olan bir grubun seçildiği örneklemedir. Çalışma grubunun kolaylık ve uygun olma durumuna göre seçildiği bu örnekleme yöntemini kimi araştırmacılar uygun, elverişli kimileri ise kolay ulaşılabilir örnekleme yöntemi olarak adlandırmıştır. Fraenkel vd. (2011) çoğunlukla rastgele veya sistematik olmayan örneklem seçmenin zor olduğunu ve bu durumlarda uygun (elverişli) örneklemenin kullanılabileceğini belirterek bu örnekleme yöntemine göre çalışma grubunun seçildiği araştırmalarda genellemeden kaçınılması gerektiğini vurgulamıştır (s.99).

Bu doğrultuda çalışma grubunun belirlenmesi için 2021-2022 yılının bahar döneminde çalışma için uygun ve elverişli olan bir devlet ortaokulu seçilmiştir. Belirlenen ortaokulda 7.

sınıfta öğrenim görmekte olan 5 şube arasında birbirine denk sayılabilecek iki şubenin belirlenmesi için tüm şubelere “Dijital Güvenlik Öz Yeterlik Envanteri” ön test olarak uygulanmış ve gerekli istatistiki işlemlere tabi tutulmuştur. İstatistiki işlemler sonucunda 7/A ile 7/B şubelerinin birbirine denk olduğu ve 7C ile 7/D şubelerinin de birbirine denk olduğu görülmüştür. Birbirine denk bu iki grup arasında kura yöntemi uygulanmış ve çalışma grubu olarak 7/A ile 7/B şubeleri belirlenmiştir.

Tablo 1.

Araştırmanın Deneysel İşlem Kısımına Katılan Öğrenciler

Gruplar	Sınıflar	Sınıf Mevcudu	%
Deney	7/B	39	54,17
Kontrol	7/A	33	45,83
Toplam		72	100

Tablo 1’de görüldüğü üzere araştırmanın çalışma grubu, deney grubunda 39, kontrol grubunda 33 olmak üzere toplamda 72 öğrenciden oluşmaktadır. Deney ve kontrol gruplarının belirlenmesinde ele alınan istatistiksel işlemlere bulgular ve yorum kısmında yer verilmiştir.

Araştırmanın uygulama sürecinde devamsızlık sebebi ile deney grubundan 4 öğrenci, kontrol grubundan ise 1 öğrenci çalışma kapsamı dışında bırakılmıştır. Bu sebeple deney grubunda 35 öğrenci, kontrol grubunda ise 32 öğrenci çalışma kapsamında değerlendirilmiştir.

Deney ve kontrol grubu amacıyla seçilen 7/A ve 7/B sınıfında katılımcı öğrencilerin nitelikleri Tablo 2’de sunulmuştur.

Tablo 2.

Uygulamadaki Deney ve Kontrol Gruplarının Cinsiyet Değişkenine Göre Dağılımı

Gruplar	Kız		Erkek		Toplam
	N	%	n	%	n
Deney Grubu	15	42,86	20	57,14	35
Kontrol Grubu	17	53,12	15	46,88	32
Toplam	32	47,77	35	52,23	67

Tablo 2'ye bakıldığında deney grubunda yer alan 35 öğrencinin %42,85'i kız öğrenci, %57,14'ü ise erkek öğrencidir. Kontrol grubunda yer alan 32 öğrencinin ise %53,12'si kız öğrenci, %46,87'si ise erkek öğrencidir. Araştırmanın çalışma grubunda toplamda 67 öğrenci bulunmaktadır ve çalışma grubunun %47,76'sı kız öğrenci, %52,23'ü ise erkek öğrencidir.

3.3. Veri Toplama Aracı

Sosyal bilgiler dersinde 7. sınıf öğrencilerinin dijital güvenlik yeterliği için geliştirilen çevrim içi destekleyici öğrenme aracının öğrencilerin dijital güvenlik öz yeterlik algılarına etkisini belirlemeyi amaçlayan bu çalışmada dijital güvenlik öz yeterlik algısının belirlenmesi için likert tipinde bir ölçme aracı kullanılmıştır.

Büyüköztürk vd. (2020) tarafından ölçme, *“birey ya da nesnelerin niteliklerinin uygun araçlar kullanılarak gözlenip, gözlem sonuçlarının sayı veya sembollerle ifade edilmesi”* olarak tanımlanmıştır (s.106). Deneysel yöntemle yapılan bu çalışmada ölçülmek istenen özelliğin öz yeterlik algısı olması sebebiyle nicel verilerin ölçülmesine elverişliliğinden dolayı ölçek uygulanmıştır. Çalışmada veri toplama amacıyla Üstündağ, Akcan, Ceran ve Çakmak (2022) tarafından geliştirilen “Dijital Güvenlik Öz Yeterlik Envanteri” kullanılmıştır.

3.3.1. Dijital Güvenlik Öz Yeterlik Envanteri

Dijital Güvenlik Öz Yeterlik Envanteri ortaokul 7. sınıf öğrencilerinin dijital güvenlik öz yeterlik algılarını teknik, psikososyal, çevrim içi alışveriş, hak ve sorumluluk ve sağlık bağlamında ölçmek amacıyla geliştirilmiştir. MEB SBDÖP ortaokul 7. sınıf öğrenci düzeyi ve ilgili alanyazın taraması sonucunda oluşturulan envanterde toplamda 5 alt ölçek yer almaktadır. Envanterde yer alan alt ölçekler sırasıyla teknik alt ölçeği, psikososyal alt ölçeği, çevrim içi alışveriş alt ölçeği, hak ve sorumluluk alt ölçeği ve sağlık alt ölçeğidir.

Envanterde yer alan teknik alt ölçeği 15 madde, psikososyal alt ölçek 8 madde, çevrim içi alışveriş alt ölçeği 5 madde, hak ve sorumluluk alt ölçeği 7 madde ve sağlık alt ölçeği 5 maddeden oluşmaktadır. 5'li likert tipinde geliştirilen envanter 1 (hiç katılmıyorum) ile 5

(tamamen katılıyorum) aralığında değer almaktadır. 5 alt ölçekten oluşan bu envanterin en önemli özelliği hem ortaokul öğretim programına uygun olması hem de ortaokul 7. sınıf düzeyinde kullanılabilir durumda olmasıdır.

Dijital Güvenlik Öz Yeterlik Envanteri'ne ait alt ölçeklerin istatistiksel işlemler neticesinde geçerliği ve güvenirliği kanıtlanmıştır. Her alt ölçeğe ait geçerlik ve güvenirlik çalışmalarının sonuçları aşağıda sunulmuştur.

3.3.1.1. Teknik Alt Ölçeği

Envanterde yer alan teknik alt ölçeğinin faktör analizine uygunluğunu test etmek amacıyla yapılan Kaiser-Mayer-Olkin (KMO) ve Bartlett testleri sonucunda hesaplanan KMO uyum ölçüsü değeri 0,91'dir. Kaiser, bulunan değer 1'e yaklaştıkça mükemmel, 0,50'in altında kaldığında ise kabul edilemez durumda olduğunu belirtmiştir (Tavşancıl, 2010). Hesaplanan Bartlett Küresellik Testi 4349,77'dir ve 0,01 düzeyinde anlamlıdır ($X^2_{105}=4349,77$). Buna göre ön uygulama sonucunda teknik alt ölçeğinin KMO değeri faktör analizi için çok iyi bir yapı oluşturduğunu göstermektedir ve Bartlett Küresellik Testinin anlamlı hesaplanması da faktör analizine uygun olduğunu göstermektedir.

Teknik alt ölçeği toplam varyansın %43,15'ünü açıklayan 15 madde ve iki faktörden oluşmuştur. Alt ölçekte yer alan 1. faktör 8 maddeden oluşmuş ve faktör yük değerleri 0,45-0,83 arasında değişmiş, özdeğeri 4,93 olarak hesaplanmış ve toplam varyansın %32,86'nı açıkladığı görülmüştür. 1. faktör araştırmacılar tarafından "güvenilir olmayandan kaçınma" olarak isimlendirilmiştir. Alt ölçekte yer alan 2. faktör ise 7 maddeden oluşmuş ve faktör yük değerleri 0,47-0,72 arasında değişmektedir. Öz değeri 1,54 olarak hesaplanan 2. faktör toplam varyansın %10,29'unu açıklamaktadır ve araştırmacılar tarafından "önlem alma" olarak isimlendirilmiştir. Bulgular neticesinde teknik alt ölçeğinin yapı geçerliğinin tatmin edici düzeyde olduğu görülmektedir. Madde toplam korelasyonları incelendiğinde maddelerin 0,47-0,60 arasında değer aldığı görülmüş ve maddenin ölçülecek özelliği ayırt etme açısından yeterli olduğu ifade edilmiştir.

Teknik alt ölçeğin DFA analizi sonucunda χ^2/sd değeri 4,86 olarak hesaplanmış ve bu değer kabul edilebilir düzeydedir. Ayrıca ölçeğin RMSEA uyum indeksi kabul edilebilir düzeyde, TLI/NNFI, CFI ve NFI değerleri kabul edilebilir düzeyde, AGFI ve GFI mükemmel uyum

indeksine sahiptir. Dolayısıyla teknik alt ölçeğinin DFA sonucunda model doğrulanmaktadır.

Teknik alt ölçeğinin güvenilirliğini test etmek amacıyla Cronbach Alpha değeri hesaplanmış ve bu değer 0,85'tir (1. faktör 0,80, 2. faktör 0,77). Buna göre Teknik alt ölçeğinin geçerli ve güvenilir bir ölçme aracı olduğu söylenebilir.

3.3.1.2. Psikososyal Alt Ölçeği

Envanterde yer alan psikososyal alt ölçeğinin faktör analizine uygunluğunu test etmek amacıyla araştırmacılar tarafından yapılan Kaiser-Mayer-Olkin (KMO) ve Bartlett testleri sonucunda hesaplanan KMO uyum ölçüsü değeri 0,85'tir. Kaiser, bulunan değer 1'e yaklaştıkça mükemmel, 0,50'in altında kaldığında ise kabul edilemez durumda olduğunu belirtmiştir (Tavşancıl, 2010). Hesaplanan Bartlett Küresellik Testi 2046,61'dir ve 0,01 değerine göre anlamlıdır ($X^2_{28}=2046,61$). Buna göre ön uygulama sonucunda psikososyal alt ölçeğinin KMO değeri faktör analizi için çok iyi bir yapı oluşturduğunu göstermektedir ve Bartlett Küresellik Testinin ise anlamlı hesaplanması faktör analizine uygun olduğunu göstermektedir.

Psikososyal alt ölçeği toplam varyansın %40,33'ünü açıklayan 8 madde ve tek faktörden oluşmuştur. Özdeğeri 3,22 olarak hesaplanmış ve sonraki maddeler 1,00 özdeğerinden küçük olduğu için tek faktörlü olmasına karar verilmiştir. Faktör yük değerleri ise 0,47 ile 0,74 arasında değişmektedir ve maddeler yapıda yer alabilecek değere sahiptir. Bulgular neticesinde psikososyal alt ölçeğinin yapı geçerliğinin tatmin edici düzeyde olduğu görülmektedir. Madde toplam korelasyonları incelendiğinde maddelerin 0,35 ile 0,62 arasında değer aldığı görülmüş ve maddenin ölçülecek özelliği ayırt etme açısından yeterli olduğu ifade edilmiştir.

Psikososyal alt ölçeğin DFA analizi sonucunda χ^2/sd değeri 3,79 olarak hesaplanmış ve bu değer kabul edilebilir düzeydedir. Ayrıca ölçeğin RMSEA uyum indeksi 0,05 değerindedir ve mükemmel düzeyde, TLI/NNFI, CFI ve NFI değerleri kabul edilebilir düzeyde, AGFI ve GFI mükemmel uyum indeksine sahiptir. Dolayısıyla psikososyal alt ölçeğinin DFA sonucunda model doğrulanmaktadır.

Psikososyal alt ölçeğinin güvenilirliğini test etmek amacıyla Cronbach Alpha değerine bakılmış ve 0,77 olarak hesaplanmış. Bu değer kabul edilebilir düzeyde güvenilir. Buna göre Psikososyal alt ölçeğinin geçerli ve güvenilir bir ölçme aracı olduğu söylenebilir.

3.3.1.3. Çevrim İçi Alışveriş Alt Ölçeği

Envanterde yer alan çevrim içi alışveriş alt ölçeğinin faktör analizine uygunluğunu test etmek amacıyla araştırmacılar tarafından yapılan Kaiser-Mayer-Olkin (KMO) ve Bartlett testleri sonucunda hesaplanan KMO uyum ölçüsü değeri 0,79'dur. Kaiser, bulunan değer 1'e yaklaştıkça mükemmel, 0,50'in altında kaldığında ise kabul edilemez durumda olduğunu belirtmiştir (Tavşancıl, 2010). Hesaplanan Bartlett Küresellik Testi 1199,13'tür ve 0,01 değerine göre anlamlıdır ($X^2_{10}=1199,13$). Buna göre ön uygulama sonucunda çevrim içi alışveriş alt ölçeğinin KMO değeri faktör analizi için çok iyi bir yapı oluşturduğunu göstermektedir ve Bartlett Küresellik Testinin ise anlamlı hesaplanması faktör analizine uygun olduğunu göstermektedir.

Çevrim içi alışveriş alt ölçeği toplam varyansın %49,79'unu açıklayan 5 madde ve tek faktörden oluşmuştur. Özdeğeri 2,49 olarak hesaplanmış ve sonraki maddeler 1,00 özdeğerinden küçük olduğu için tek faktörlüdür. Faktör yük değerleri ise 0,61 ile 0,77 arasında değişmektedir ve maddeler yapıda yer alabilecek değere sahiptir. Bulgular neticesinde çevrim içi alışveriş alt ölçeğinin yapı geçerliğinin tatmin edici düzeyde olduğu görülmektedir. Madde toplam korelasyonları incelendiğinde maddelerin 0,41 ile 0,58 arasında değer aldığı görülmüş ve maddenin ölçülecek özelliği ayırt etme açısından yeterli olduğu ifade edilmiştir.

Çevrim içi alışveriş alt ölçeğin DFA analizi sonucunda χ^2/sd değeri 1,52 olarak hesaplanmış ve bu değer mükemmel uyum indeksine sahiptir. Ayrıca ölçeğin RMSEA uyum indeksi 0,02 değerindedir ve mükemmel uyum indeksine, TLI/NNFI, CFI ve NFI değerleri mükemmel uyum indeksine, AGFI ve GFI mükemmel uyum indeksine sahiptir. Dolayısıyla çevrim içi alışveriş alt ölçeğinin DFA sonucunda model doğrulanmaktadır.

Çevrim içi alışveriş alt ölçeğinin güvenilirliğini test etmek amacıyla Cronbach Alpha değerine bakılmış ve 0,74 olarak hesaplanmıştır. Bu değer kabul edilebilir düzeyde güvenilir. Buna

göre Çevrim içi alışveriş alt ölçeğinin geçerli ve güvenilir bir ölçme aracı olduğu söylenebilir.

3.3.1.4. Hak ve Sorumluluk Alt Ölçeği

Envanterde yer alan hak ve sorumluluk alt ölçeğinin faktör analizine uygunluğunu test etmek amacıyla araştırmacılar tarafından yapılan Kaiser-Mayer-Olkin (KMO) ve Bartlett testleri sonucunda hesaplanan KMO uyum ölçüsü değeri 0,81'dir. Kaiser, bulunan değer 1'e yaklaştıkça mükemmel, 0,50'in altında kaldığında ise kabul edilemez durumda olduğunu belirtmiştir (Tavşancıl, 2010). Hesaplanan Bartlett Küresellik Testi 2046,09'dur ve 0,01 değerine göre anlamlıdır ($X^2_{21}=2046,09$). Buna göre ön uygulama sonucunda hak ve sorumluluk alt ölçeğinin KMO değeri faktör analizi için çok iyi bir yapı oluşturduğunu göstermektedir ve Bartlett Küresellik Testinin ise anlamlı hesaplanması faktör analizine uygun olduğunu göstermektedir.

Hak ve sorumluluk alt ölçeği toplam varyansın %44,32'sini açıklayan 7 madde ve tek faktörden oluşmuştur. Öz değeri 3,10 olarak hesaplanmış ve sonraki maddeler 1,00 özdeğerinden küçük olduğu için tek faktörlüdür. Faktör yük değerleri ise 0,51 ile 0,74 arasında değişmektedir ve maddeler yapıda yer alabilecek değere sahiptir. Bulgular neticesinde hak ve sorumluluk alt ölçeğinin yapı geçerliğinin tatmin edici düzeyde olduğu görülmektedir. Madde toplam korelasyonları incelendiğinde maddelerin 0,38 ile 0,59 arasında değer aldığı görülmüş ve maddenin ölçülecek özelliği ayırt etme açısından yeterli olduğu ifade edilmiştir.

Hak ve sorumluluk alt ölçeğin DFA analizi sonucunda χ^2/sd değeri 3,14 olarak hesaplanmış ve bu değer kabul edilebilir uyum indeksine sahiptir. Ayrıca ölçeğin RMSEA uyum indeksi 0,04 değerindedir ve mükemmel uyum indeksine, TLI/NNFI, CFI ve NFI değerleri mükemmel uyum indeksine, AGFI ve GFI mükemmel uyum indeksine sahiptir. Dolayısıyla hak ve sorumluluk alt ölçeğinin DFA sonucunda model doğrulanmaktadır.

Hak ve sorumluluk alt ölçeğinin güvenilirliğini test etmek amacıyla Cronbach Alpha değerine bakılmış ve 0,78 olarak hesaplanmıştır. Bu değer kabul edilebilir düzeyde güvenilirlerdir. Buna göre hak ve sorumluluk alt ölçeğinin geçerli ve güvenilir bir ölçme aracı olduğu söylenebilir.

3.3.1.5. Sağlık Alt Ölçeği

Envanterde yer alan sağlık alt ölçeğinin faktör analizine uygunluğunu test etmek amacıyla araştırmacılar tarafından yapılan Kaiser-Mayer-Olkin (KMO) ve Bartlett testleri sonucunda hesaplanan KMO uyum ölçüsü değeri 0,78'dir. Kaiser, bulunan değer 1'e yaklaştıkça mükemmel, 0,50'in altında kaldığında ise kabul edilemez durumda olduğunu belirtmiştir (Tavşancıl, 2010). Hesaplanan Bartlett Küresellik Testi 1199,38'dir ve 0,01 değerine göre anlamlıdır ($X^2_{10}=1199,38$). Buna göre ön uygulama sonucunda sağlık alt ölçeğinin KMO değeri faktör analizi için çok iyi bir yapı oluşturduğunu göstermektedir ve Bartlett Küresellik Testinin ise anlamlı hesaplanması faktör analizine uygun olduğunu göstermektedir.

Sağlık alt ölçeği toplam varyansın %49,82'sini açıklayan 5 madde ve tek faktörden oluşmuştur. Öz değeri 2,49 olarak hesaplanmış ve sonraki maddeler 1,00 özdeğerinden küçük olduğu için tek faktörlüdür. Faktör yük değerleri ise 0,61 ile 0,74 arasında değişmektedir ve maddeler yapıda yer alabilecek değere sahiptir. Bulgular neticesinde sağlık alt ölçeğinin yapı geçerliğinin tatmin edici düzeyde olduğu görülmektedir. Madde toplam korelasyonları incelendiğinde maddelerin 0,51 ile 0,65 arasında değer aldığı görülmüş ve maddenin ölçülecek özelliği ayırt etme açısından yeterli olduğu ifade edilmiştir.

Sağlık alt ölçeğin DFA analizi sonucunda χ^2/sd değeri 2,85 olarak hesaplanmış ve bu değer mükemmel uyum indeksine sahiptir. Ayrıca ölçeğin RMSEA uyum indeksi 0,04 değerindedir ve mükemmel uyum indeksine, TLI/NNFI, CFI ve NFI değerleri mükemmel uyum indeksine, AGFI ve GFI mükemmel uyum indeksine sahiptir. Dolayısıyla sağlık alt ölçeğinin DFA sonucunda model doğrulanmaktadır.

Sağlık alt ölçeğinin güvenilirliğini test etmek amacıyla Cronbach Alpha değerine bakılmış ve 0,75 olarak hesaplanmıştır. Bu değer kabul edilebilir düzeyde güvenilir. Buna göre sağlık alt ölçeğinin geçerli ve güvenilir bir ölçme aracı olduğu söylenebilir.

3.4. Öğretim Materyali

Bu araştırmada kullanılan öğretim materyali, sosyal bilgiler dersinde 7. sınıf öğrencilerinin dijital güvenlik yeterliği için araştırmacı tarafından geliştirilmiştir. Öğretim materyali, çevrim içi destekleyici öğrenme aracı olarak deney grubuna uygulanmıştır. Çevrim içi destekleyici öğrenme aracının teorik içeriği SBDÖP ve alanyazın incelemesi sonucunda

belirlenen dijital güvenlik yeterlik göstergeleri doğrultusunda oluşturulmuştur. İncelemeler sonucunda SBDÖP da göz önünde bulundurularak dijital güvenlik teknik, psikososyal, çevrim içi alışveriş, hak ve sorumluluk ve sağlık olmak üzere 5 boyutta ele alınmış ve bunlar kendi içerisinde konulara ayrılmıştır. Her konuya ilişkin SCORM paketleri oluşturulmuştur. Çevrim içi destekleyici öğrenme aracı toplamda “*Articulate Storyline*” platformunda hazırlanan 11 adet SCORM paketinden oluşmaktadır.

Tablo 3.

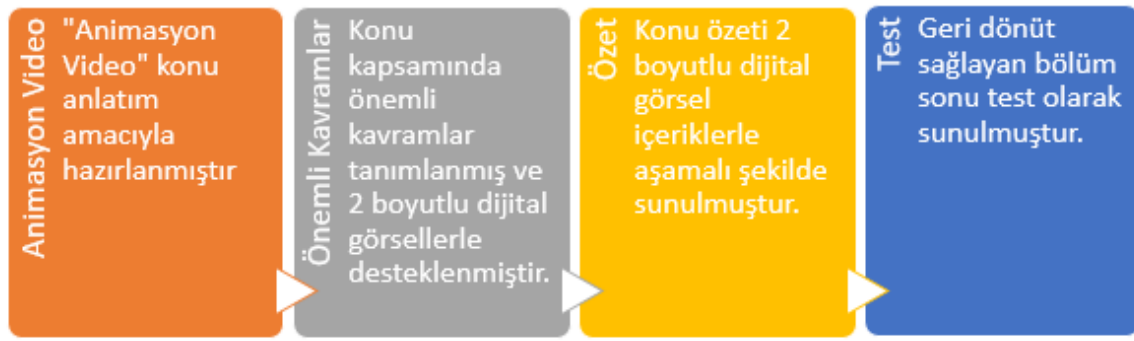
Çevrim İçi Destekleyici Öğrenme Aracı İçerik Bilgisi

Boyutlar	SCORM Paketlerinin Konuları	SCORM Paket Sayısı
Teknik	Şifre Güvenliği	1
	Dijital Cihaz ve İçindekileri Koruma	1
	Erişim Güvenliği	1
	Dijital Ayak İzi Yönetimi	1
	Doğru ve Güvenli Bilgiye Erişim	1
Psikososyal	Dijital Zorbalık Nedir ve Nasıl Önlenir	1
	Dijital Zorbalıkla Nasıl Mücadele Edilir	1
Hak ve Sorumluluk	Çevrim İçi Ortamda Hak ve Sorumluluklarımız Nelerdir	1
	Dijital Hakların İhlalini Şikayet Edebileceğimiz Mecralar	1
Çevrim Alışveriş	İç Güvenli Çevrim İçi Alışveriş Yöntemleri	1
Sağlık	Dijital Cihazları ve İnterneti Kullanırken Sağlığa Dikkat	1

Tablo 3’te görüldüğü üzere çevrim içi destekleyici öğrenme aracı teknik, psikososyal, çevrim içi alışveriş, hak ve sorumluluk ve sağlık boyutlarında 11 SCORM paketinden oluşmaktadır. Çevrim içi destekleyici öğrenme aracı üç aşamada oluşturulmuştur. Birinci aşama içerik bölümlerinin oluşturulması, ikinci aşama içeriklerin SCORM paketlerine dönüştürülmesi, üçüncü aşama ÖYS üzerinden öğrencinin erişimine hazır hale getirilmesidir.

3.4.1. Araç İçeriğinin Oluşturulması

Araç içeriğinin oluşturulma aşamasında 2018 SBDÖP ve alanyazın incelemesi neticesinde belirlenen dijital güvenlik yeterlik göstergeleri konu konu ayrılmış ve her konunun içeriği 7. sınıf öğrencilerinin yaş seviyesine uygun bir şekilde hazırlanmıştır. Aracın içeriği konu anlatım videosu, anahtar kelimeler bölümü, konu özeti bölümü ve test bölümü olmak üzere 4 aşamalıdır. İçeriğe ait bölümler aşağıda akış şeması olarak gösterilmiş ve ilgili başlıkta detaylı olarak açıklanmıştır.



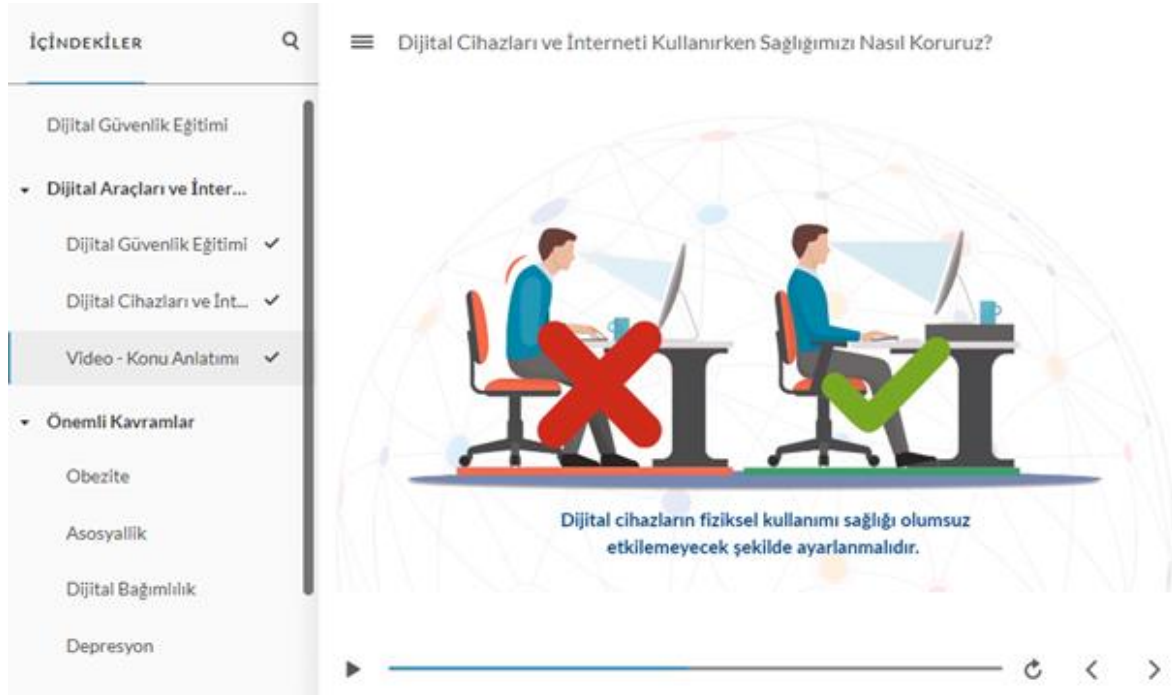
Şekil 5. Çevrim içi destekleyici öğrenme aracının içerik oluşturma aşamalarını gösteren akış şeması

3.4.1.1. Animasyon Video Bölümü

Bu bölümde 3 sekme yer almaktadır. İlk sekmede genel başlık ve ilgili görseller kullanılmıştır. İkinci sekmede konu başlığı ve konu ile ilgili dijital simgeler kullanılarak öğrencilere neleri öğreneceği konusunda bilgilendirme yapılmıştır. Üçüncü sekmede ise konu anlatımı amacıyla hazırlanmış “animasyon video” bulunmaktadır.

Animasyon videoların senaryoları alanyazın ve 2018 SBDÖP incelemesi neticesinde belirlenen dijital güvenlik yeterlik göstergeleri doğrultusunda belirlenen boyutlar çerçevesinde oluşturulmuştur. Animasyon videolar bilgi verici düzeyde hazırlanmış ve aynı zamanda konu içeriğindeki önemli işlemlerin nasıl yapılacağını dijital görseller aracılığıyla göstermektedir. Kullanılan dijital görseller “www.shutterstock.com” ve “www.freepik.com” adreslerinden seçilerek 2 boyutlu hale getirilmiştir. Hazırlanan senaryo ve 2 boyutlu dijital

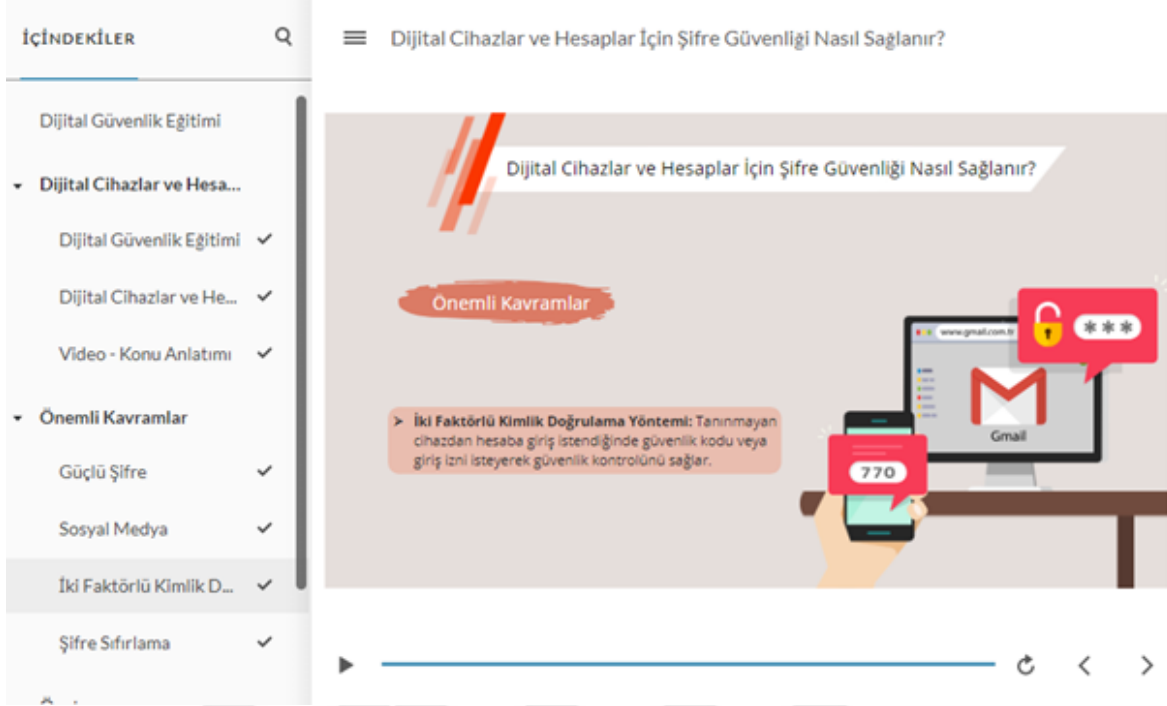
görseller “Adobe Edge” programı kullanılarak animasyon video haline dönüştürülmüştür. Daha sonra içerik seslendirilerek düzenleme yapılmıştır. SCORM paketine yüklenen animasyon videoda hızlı ilerletme, bölümü atlama/geçme özelliği yoktur. Bu sayede öğrenci konu anlatım videosunu izlemeden diğer bölümlere geçemeyecektir.



Şekil 6. Çevrim içi destekleyici öğrenme aracının ilk bölümünde konu anlatım amacıyla hazırlanan animasyon videoya ait örnek bir görüntü

3.4.1.2. Önemli Kavramlar Bölümü

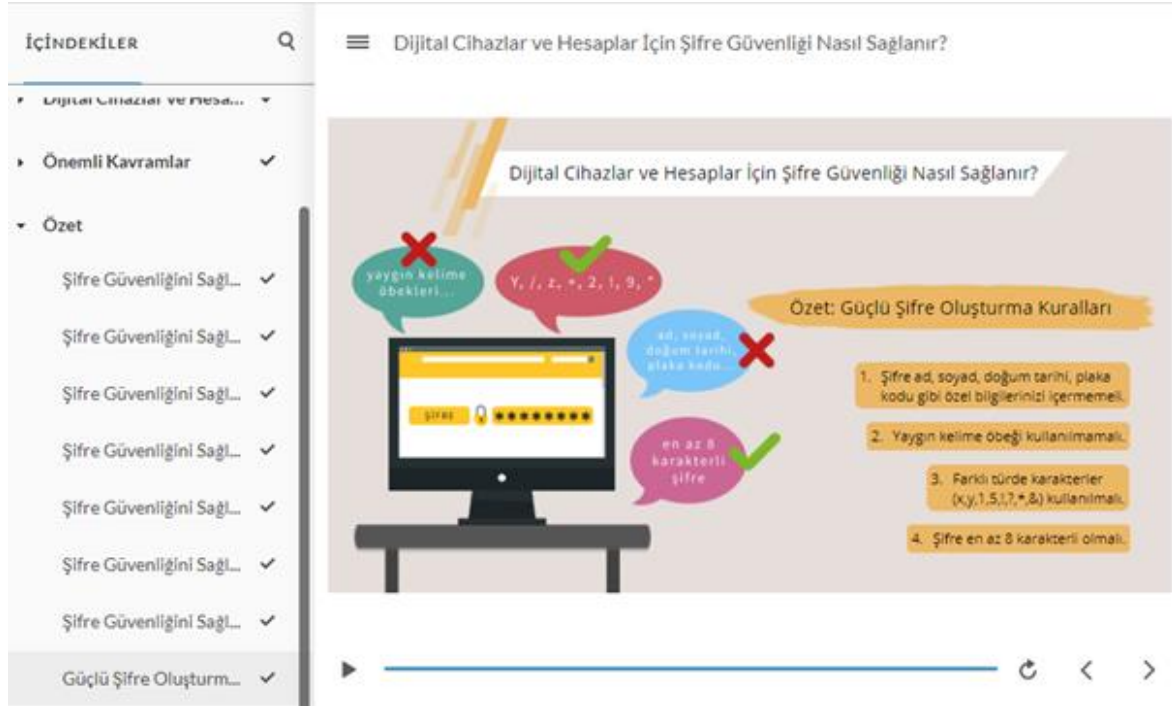
Bu bölümde ilk bölüm için hazırlanan konu anlatım videosunda geçen önemli kavramlar yer almaktadır. Her kavram için ayrı bir sekme açılmış ve kavram tanımlaması yapılmıştır. Ayrıca kavrama dahil önemli işlemler 2 boyutlu dijital görseller ile gösterilmektedir. İçeriklerdeki dijital görseller “www.shutterstock.com” ve “www.freepik.com” adreslerinden seçilerek 2 boyutlu hale getirilerek kullanılmıştır. Bu bölümde bölüm içi ilerletme serbest bırakılmıştır. Bunun sebebi öğrenciye her ekranı ve sekmeyi kendi istediği sürede inceleme olanağı sunmaktır.



Şekil 7. Çevrim içi destekleyici öğrenme aracının ikinci bölümünde yer alan önemli kavramlara ait örnek bir görüntü

3.4.1.3. Özet Bölümü

Bu bölümde ilk bölüm için hazırlanan konu anlatımı aşamalı bir şekilde özetlenmiştir. İçerikte kullanılacak olan dijital görseller yine “www.shutterstock.com” ve “www.freepik.com” adreslerinden seçilerek 2 boyutlu hale getirilmiştir. Konunun aşamalı olarak özetlendiği bu bölümde ayrıca yapılması gereken önemli işlemler de dijital görseller aracılığıyla gösterilmiştir. Bu bölümde bölüm içi ilerletme serbest bırakılmıştır. Bunun sebebi öğrenciye her ekranı ve sekmeyi kendi istediği sürede inceleme olanağı sunmaktır.



Şekil 8. Çevrim içi destekleyici öğrenme aracının üçüncü bölümünde yer alan özete ait örnek bir görüntü

3.4.1.4. Test Bölümü

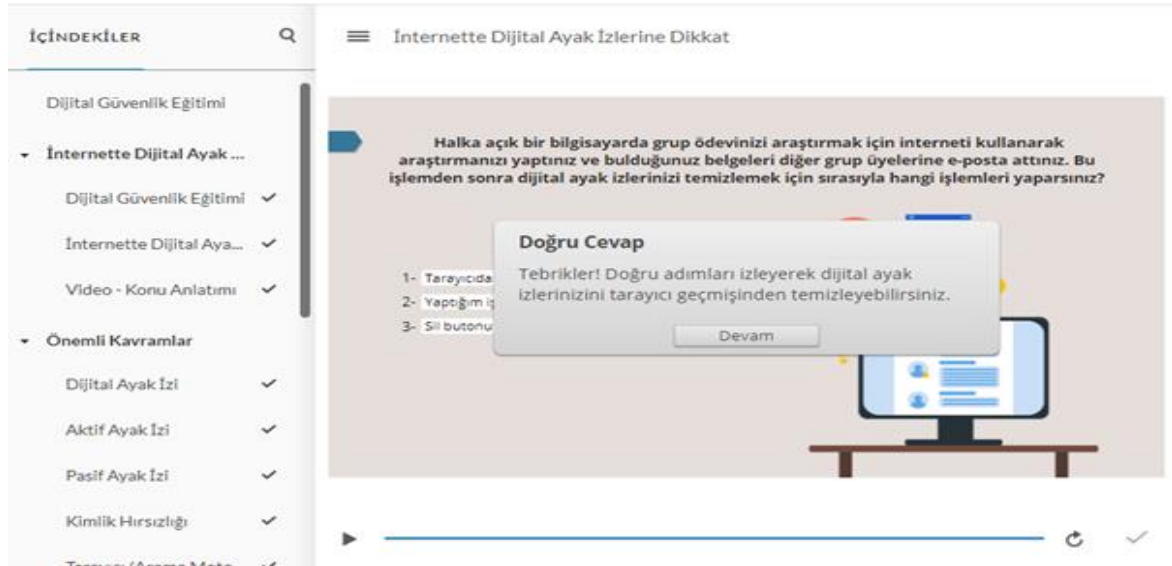
Bu bölümde konuyu kapsayacak şekilde hazırlanan sorular bulunmaktadır. Sorular çoktan seçmeli, doğru yanlış ve eşleştirmeli biçimlerde oluşturulmuş ve her ekranda dijital görseller kullanılmıştır. Kullanılan dijital görseller “www.shutterstock.com” ve “www.freepik.com” adreslerinden seçilerek 2 boyutlu hale getirilmiştir. Ayrıca bu bölüm “*Articulate Storyline*” içeriğinde “*quiz*” özelliği kullanılarak oluşturulmuştur.

SCORM paketi içeriğinde en sonda bulunan test bölümünün başlaması için önceki bölümlerin %100 bitirilmesi gerekmektedir. Öğrencinin %100 bitirdiğini anlaması için her bitirdiği bölüm ve sekme sonunda içerik ağacında “tik” işareti oluşmaktadır. Bölümler bitirildikten sonra test ekranı açılmaktadır. Açılan test ekranında “Teste Hazır mısınız?” butonu yer almakta ve öğrenci hazır olduğunda butona basarak testi başlatabilmektedir. Sorular sıralı şekilde ilerlemekte ve her soru cevaplandırıldığında diğer ekranla birlikte sıradaki soru açılmaktadır. Ekranı gelen soru için belirlenen bir süre yoktur ve cevap işaretlendikten sonra doğru veya yanlış olarak geri dönüt verilmektedir. Test bitiminde

öğrencinin 100 üzerinden aldığı puan bildirilmiştir. Puan bildirim ekranında ayrıca “eğitimi sonlandır” butonu yer almaktadır.



Şekil 9. Çevrim içi destekleyici öğrenme aracının dördüncü bölümünde yer alan teste geçişe ait örnek bir görüntü



Şekil 10. Çevrim içi destekleyici öğrenme aracının dördüncü bölümünde yer alan teste ait örnek bir görüntü

3.4.2. SCORM Paketlerin Oluşturulması

Oluşturulan bölümler “*Articulate Storyline*” platformunda “*SCORM paketi*” olarak hazırlanmıştır. Her SCORM paketi içerisinde öğrencinin içeriği yönetmesi için “*içerik ağacı*” kullanılmıştır ve “*içindekiler*” olarak isimlendirilmiştir. İçerik ağacında 4 bölümün sıralı şekilde gösterimi için “*bölümler arası ilerletme*” kısıtlanmış, böylelikle bir bölüm bitmeden diğerine geçilememektedir. Ayrıca konu anlatım videosu için de önemli yerlerin atlanmaması amacıyla ilerletme kısıtlanmıştır. Buna ek olarak dijital cihazdan SCORM paketlerine erişim sağlandığında erişilen sekme dışında başka ekrana erişim sağlandığında konu anlatım videosu duraklamaktadır. Burada temel amaç öğrencinin içeriği sadece ses olarak değil, aynı zamanda görüntü olarak da takip etmesidir.

Her SCORM paketinin sonuna gelindiğinde öğrenci eğitimi bitirme oranını % olarak görmekte, bununla birlikte eğitimi tamamlama süresini ve başarı puanını da görüntüleyebilmektedir. Çevrim içi öğrenme ortamında kullanılmak üzere geliştirilen çevrim içi destekleyici öğrenme aracı aynı zamanda internet olmadan da öğrenme amaçlı kullanılabilir. Fakat bu kullanım şekli eğitime veri sağlamamaktadır.

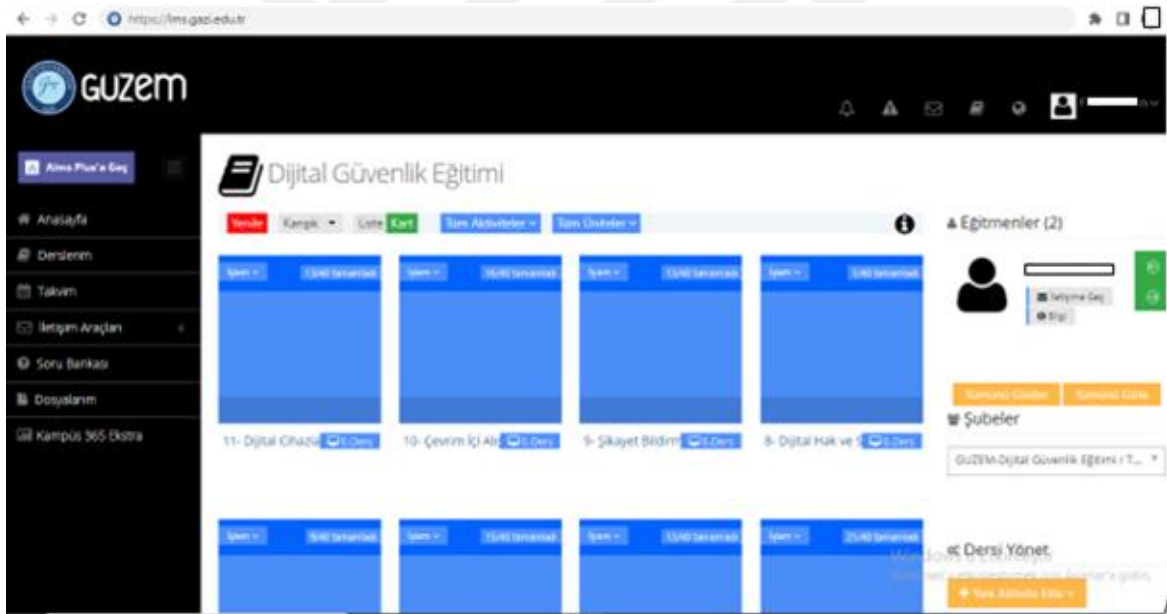


Şekil 11. Oluşturulan SCORM paketlerine ait örnek bir görüntü

3.4.3. SCORM Paketlerinin Öğrenci Erişimine Sunulması

Hazırlanan SCORM paketleri Gazi Üniversitesi'nin kullandığı ÖYS (LMS yazılımı) üzerinden sunulmuştur. ÖYS'de oluşturulan “Dijital Güvenlik Eğitimi” adlı sanal sınıfta deney grubunda yer alan öğrencilerin her birine ayrı profil oluşturulmuş, kullanıcı ad ve şifreleri oryantasyon sürecinde öğrencilere verilmiştir. Öğrenciler sisteme kullanıcı ad ve şifreleri ile erişim sağladığında yüklenmiş olan eğitim paketlerini görebilmektedir.

ÖYS'de oluşturulan sanal sınıfa araştırmacı eğitmen olarak atanmıştır. “Dijital Güvenlik Eğitimi” adlı sanal sınıfta eğitmen her SCORM pakete ait detaylı raporu ÖYS sisteminden elde edebilmektedir. Eğitmen her SCORM paketine ait detaylı raporda öğrenci kullanıcı adını, pakete ilk ve son giriş tarih ve saatini, eğitimi tamamlama süresini, giriş sayısını, alınan puanları ve tamamlama oranını (%) görüntüleyebilmektedir. Bu rapor sürekli güncellenmekte ve sistemde kayıtlı olarak tutulmakta veya eğitmen tarafından bilgisayara indirilebilmektedir.



Şekil 12. Oluşturulan SCORM paketlerinin ÖYS’de sunumuna ait örnek bir görüntü

3.5. Araştırmanın DeneySEL Süreci

Araştırmada uygulama yapılan deney ve kontrol grubu öğrencilerine uygulanan deneySEL işlem Tablo 4’te gösterilmiştir.

Tablo 4.

Deney ve Kontrol Grubuna Uygulanan Deneysel İşlem

Gruplar	Ön Test	Deneysel İşlem (Uygulama)	Son Test
Deney Grubu	Dijital Güvenlik Öz Yeterlik Envanteri	Dijital Güvenlik Yeterliği İçin Geliştirilmiş Olan Çevrim İçi Destekleyici Öğrenme Aracı	Dijital Güvenlik Öz Yeterlik Envanteri
Kontrol Grubu	Dijital Güvenlik Öz Yeterlik Envanteri	Dijital Güvenlik Eğitimi (sınıf içi eğitim)	Dijital Güvenlik Öz Yeterlik Envanteri

Tablo 4’e göre deney grubu, sosyal bilgiler dersinde dijital güvenlik yeterliği için geliştirilen çevrim içi destekleyici öğretim aracının uygulandığı grubu; kontrol grubu ise çalışma kapsamında hazırlanan dijital güvenlik eğitiminin sınıf ortamında verildiği grubu belirtmektedir. Araştırmada bağımsız değişken olarak sosyal bilgiler dersinde dijital güvenlik yeterliği için geliştirilmiş olan çevrim içi destekleyici öğrenme aracı belirlenmiştir. Bağımlı değişken ise öğrencilerin dijital güvenlik öz yeterlik algısıdır. Ayrıca kontrol grubu üzerinde ölçülen özellikleri olumlu ya da olumsuz etkileyebilecek bir değişken kullanılmamıştır. Bu doğrultuda araştırmada deney ve kontrol grubunda aynı bağımlı değişken (dijital güvenlik öz yeterlik algısı) dijital güvenlik öz yeterlik envanteri aracılığıyla ölçülmüş ve ön test-son test puanları ile hem grup içi hem gruplar arası karşılaştırmalar yapılmıştır.

3.5.1. Deneysel İşlemin Uygulama Basamakları

1. Araştırmanın deneysel sürecinde ön test ve son test olarak kullanılacak ölçme aracı belirlenmiştir (Dijital Güvenlik Öz Yeterlik Envanteri).
2. Araştırmanın çalışma grubunun belirlenmesinde, uygun (elverişlilik) örnekleme yöntemi kullanılmıştır.
3. Deneysel araştırma için gerekli izinler gösterilerek gönüllülük esasına dayalı olarak belirlenen ortaokuldaki 5 adet 7. sınıf şubesine geçerlik ve güvenirlilik çalışmaları

tamamlanmış olan “Dijital Güvenlik Öz Yeterlik Envanteri” ön test olarak uygulanmış ve istatistiksel işlemler yapılmıştır.

4. Çalışma, hem deney hem de kontrol grubunda araştırmacı tarafından 2021-2022 eğitim öğretim yılında yürütülmüştür. Deney grubu okuldan bağımsız olarak çevrim içi ortamda uygulama sürecini tamamlamış, kontrol grubu ise okul ortamında sosyal bilgiler dersinde tamamlamıştır.

5. Araştırmanın uygulama süreci toplamda 9 hafta sürmüştür. Uygulama süreci 18 Nisan 2022 tarihinde ön test ile başlatılmıştır.

6. Ön testin uygulanmasından sonraki ilk derste her iki gruba da okul ortamında süreç hakkında bilgilendirme amaçlı “oryantasyon” yapılmıştır. Oryantasyon dersinde deney grubunda çevrim içi ortamda yürütülecek olan eğitim için “Teknoloji Laboratuvarı” kullanılmıştır. Öğretim materyalinin sunulacağı ÖYS Gazi Üniversitesi’nin kullandığı LMS yazılımıdır. LMS’de önceden sanal sınıf oluşturulmuş ve her öğrenciye ait profil açılmıştır. Oryantasyon dersinde LMS’de bulunan sanal sınıfa öğrencilerin giriş yapmaları için tanımlanan kullanıcı adları ve şifreleri dağıtılmış, sisteme giriş yapmaları ve sistemi nasıl kullanacakları gösterilerek öğretilmiştir. Kontrol grubunun oryantasyon dersi ise sosyal bilgiler dersinde kendi sınıflarında yapılmıştır.

7. Deney grubunun uygulama sürecinde bir ÖYS yazılımı olan LMS’de 7 hafta boyunca ortalama 4-5 günde bir, hazırlanmış olan 11 adet SCORM paketi sırasıyla yüklenmiş, tüm değerlendirme ve raporlar sistemde kaydedilmiştir. 1. SCORM paketinde “*Şifre Güvenliği*”, 2. SCORM paketinde “*Dijital Cihazları ve İçindekileri Koruma*”, 3. SCORM paketinde “*Dijital Ayak İzlerini Yönetme*”, 4. SCORM paketinde “*Erişim Güvenliği*”, 5. SCORM paketinde “*Doğru ve Güvenli Bilgiye Erişim*”, 6. SCORM paketinde “*Dijital Zorbalık Nedir ve Nasıl Önlenir*”, 7. SCORM paketinde “*Dijital Zorbalıkla Nasıl Mücadele Edilir*”, 8. SCORM paketinde “*Çevrim İçi Ortamda Hak ve Sorumluluklarımız Nelerdir*”, 9. SCORM paketinde “*Dijital Hakların İhlalini Şikayet Edebileceğimiz Mecralar*”, 10. SCORM paketinde “*Güvenli Çevrim İçi Alışveriş Yöntemleri*”, 11. SCORM paketinde “*Dijital Cihazları ve İnterneti Kullanırken Sağlığa Dikkat*” konuları yer almaktadır.

8. Deney grubunda LMS’ye her SCORM paketinin yüklenmesinin ardından öğrenciler sistemde posta yoluyla ve sınıf Whatsapp gruplarıyla haberdar edilmiştir. Haftada 1 saat

deney grubu ile yüklenmiş olan eğitim paketleri hakkında değerlendirme “Googlemeet” uygulaması üzerinden, soru-cevap yöntemi ile çevrim içi ortamda yapılmıştır. Ayrıca öğrencilerin süreç boyunca yaşadıkları sıkıntıları, LMS üzerinden posta yoluyla haberleşme sağlanarak teknik destek verilmek suretiyle çözülmüştür.

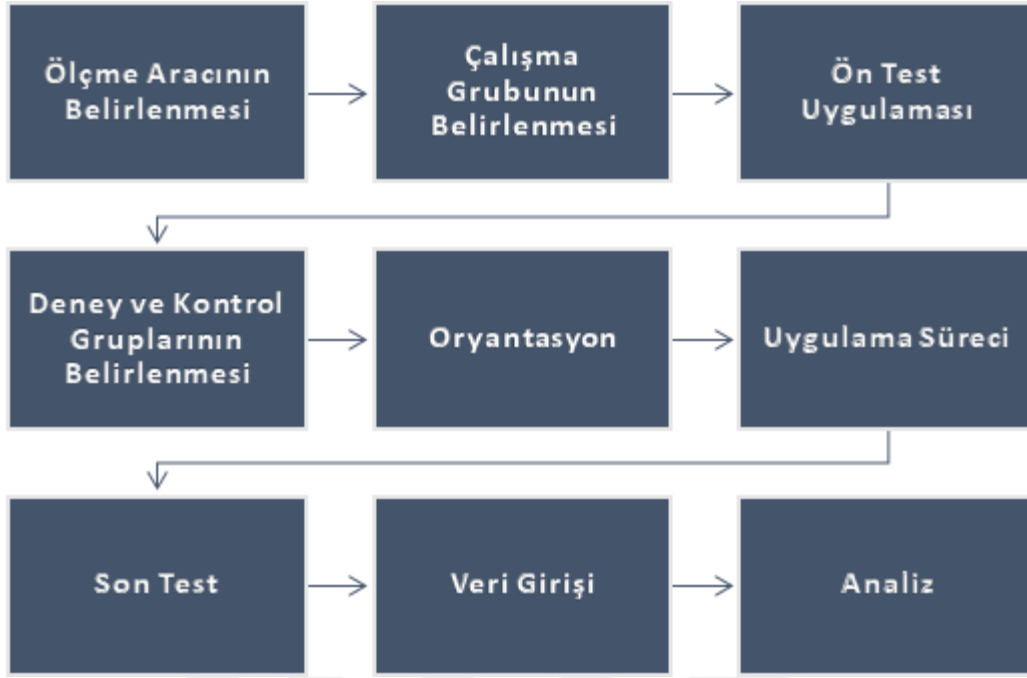
9. Kontrol grubunun uygulama sürecinde dijital güvenlik eğitimi sınıf ortamında yüz yüze verilmiştir. Her konu ders içerisinde araştırmacı tarafından işlenmiştir. Süreçte verilmiş olan eğitim EK 3’te sunulmuştur. Konu sonunda deney grubuna sunulmuş SCORM paketlerinin sonunda yer alan test soruları kontrol grubuna da değerlendirme yapılması amacıyla “çalışma kağıdı” olarak verilmiştir. Çalışma kağıtları EK 4’te sunulmuştur.

10. Kontrol grubunda uygulama süreci haftada 3 saat olacak şekilde yürütülmüştür. Uygulama sürecinde kontrol grubunda işlenen konular çevrim içi öğrenme aracında yer alan konulardır. 1. konu “*Şifre Güvenliği*”, 2. konu “*Dijital Cihazları ve İçindekileri Koruma*”, 3. konu “*Dijital Ayak İzlerini Yönetme*”, 4. konu “*Erişim Güvenliği*”, 5. konu “*Doğru ve Güvenli Bilgiye Erişim*”, 6. konu “*Dijital Zorbalık Nedir ve Nasıl Önlenir*”, 7. konu “*Dijital Zorbalıkla Nasıl Mücadele Edilir*”, 8. konu “*Çevrim İçi Ortamda Hak ve Sorumluluklarımız Nelerdir*”, 9. konu “*Dijital Hakların İhlalini Şikayet Edebileceğimiz Mecralar*”, 10. konu “*Güvenli Çevrim İçi Alışveriş Yöntemleri*”, 11. konu “*Dijital Cihazları ve İnterneti Kullanırken Sağlığa Dikkat*” konusudur.

11. Uygulama süreci deney ve kontrol grubuna verilmiş olan eğitim bitiminde 13 Haziran 2022 tarihinde son test ile sonlandırılmıştır. Ön test ve son test olarak kullanılan “Dijital Güvenlik Öz Yeterlik Envanteri” EK 1’de sunulmuştur.

12. Uygulanan ön test ve son test verileri SPSS paket programına girilerek gerekli istatistiki işlemler yapılarak analiz edilmiştir.

Araştırmanın uygulama basamakları Şekil 13’de akış şeması olarak gösterilmiştir.



Şekil 13. Araştırmanın deneysel sürecinin akış şeması

3.6. Veri Analizi

Araştırmada ön test ve son test için ölçme aracı olarak “Dijital Güvenlik Öz Yeterlik Envanteri” kullanılmıştır. Bu ölçme aracından elde edilen verilerin analizinde araştırmanın alt problemleri doğrultusunda SPSS-24 ve AMOS-21 paket programları kullanılmıştır.

Araştırmada elde edilen veriler üzerinden deney ile kontrol gruplarının ön test ve son test sonuçlarının karşılaştırmasında “Normallik Testi” yapılmış, dağılım homojen olmadığı için nonparametrik istatistik yapılmıştır. Bu doğrultuda elde edilen veriler çözümlenirken “Mann-Whitney U Testi” ve “Wilcoxon İşaretli Sıralar Testi” yapılan istatistiksel işlemlerdir.

Deney ve kontrol gruplarının oluşturulması aşamasında 7/A ve 7/B sınıflarının başlangıçta dijital güvenlik öz yeterlik durumlarını belirlemek amacıyla “Dijital Güvenlik Öz Yeterlik Envanteri” ön test olarak uygulanmıştır. 7/A ve 7/B sınıflarının ön test sonuçlarında “Mann-Whitney U Testi” yapılmıştır. Mann -Whitney U testinde öntest puan ortalamalarına bağlı sıra ortalamaları arasında farklılık olup olmadığına bakılmıştır.

Deney grubunun kendi içerisinde gelişimini ortaya koymak için ön test ve son test puan ortalamalarının karşılaştırılmasında “Wilcoxon İşaretli Sıralar Testi” uygulanmıştır. Yine kontrol grubunun kendi içinde gelişimini ortaya koymak için ön test ve son test puan ortalamalarının karşılaştırılmasında “Wilcoxon İşaretli Sıralar Testi” uygulanmıştır.

Deney ve kontrol gruplarının son test puanlarının karşılaştırılmasında ise yine “Mann-Whitney U Testi” yapılmıştır.

Araştırmada veri analizinde kullanılan “Mann -Whitney U Testi” ve “Wilcoxon İşaretli Sıralar Testi” sonuçları için .05 anlamlılık düzeyi göz önünde bulundurularak yorum yapılmıştır.



Tablo 5.

Normallik Dağılım Test Sonucu

Grup		Shapiro-Wilk				
		İstatistik	sd	P	Çarpıklık	Basıklık
Deney	Teknik alt ölçeği ön test	<u>,938</u>	<u>35</u>	<u>,048</u>	-0,89	1,07
	Psikososyal alt ölçeği ön test	,896	35	,003	-1,23	1,57
	Çevrim içi alışveriş alt ölçeği ön test	<u>,940</u>	<u>35</u>	<u>,055</u>	-0,61	-0,31
	Hak ve sorumluluk alt ölçeği ön test	,914	35	,010	-0,61	-0,76
	Sağlık alt ölçeği ön test	<u>,939</u>	<u>35</u>	<u>,051</u>	-0,63	-0,38
	Teknik alt ölçeği son test	,828	35	,000	-1,65	2,72
	Psikososyal alt ölçeği son test	,896	35	,003	-1,04	1,15
	Çevrim içi alışveriş alt ölçeği son test	,799	35	,000	-1,04	0,14
	Hak ve sorumluluk alt ölçeği son test	,893	35	,003	-0,64	0,14
	Sağlık alt ölçeği son test	,868	35	,001	-1,25	2,04
Kontrol	Teknik alt ölçeği ön test	<u>,968</u>	<u>32</u>	<u>,455</u>	-0,47	1,44
	Psikososyal alt ölçeği ön test	,956	32	<u>,209</u>	-0,65	0,39
	Çevrim içi alışveriş alt ölçeği ön test	,913	32	,013	-0,43	-0,92
	Hak ve sorumluluk alt ölçeği ön test	,915	32	,016	-0,65	-0,16
	Sağlık alt ölçeği ön test	,885	32	,003	-1,27	1,73
	Teknik alt ölçeği son test	<u>,954</u>	<u>32</u>	<u>,189</u>	-0,75	0,89
	Psikososyal alt ölçeği son test	,913	32	,014	-0,31	-1,01
	Çevrim içi alışveriş alt ölçeği son test	,862	32	,001	-0,95	0,00
	Hak ve sorumluluk alt ölçeği son test	,921	32	,023	-0,78	0,26
	Sağlık alt ölçeği son test	,906	32	,009	-0,54	-0,80

Tablo 5 incelendiğinde italik ve altı çizili verilen değerler normal dağılım gösteriyor fakat karşılaştırma yapıldığında karşılığına denk gelen puan normal dağılmadığı için nonparametrik istatistik yapılmıştır. Bu doğrultuda analizde Mann-Whitney U Testi yapılmıştır.

BÖLÜM IV

BULGULAR VE YORUM

Bu bölümde sosyal bilgiler dersinde dijital güvenlik yeterliği için geliştirilen çevrim içi destekleyici öğrenme aracının öğrencilerin dijital güvenlik öz yeterlik algılarına etkisinin belirlenmesi için yapılan deneysel çalışma sonucunda deney grubundan elde edilen veriler, dijital güvenlik eğitiminin sınıf içi ortamda uygulandığı kontrol grubundan elde edilen verilerle karşılaştırılarak gerekli analizler yapılmıştır.

Bu amaçla sosyal bilgiler dersinde dijital güvenlik yeterliği için geliştirilen çevrim içi destekleyici öğrenme aracının öğrencilerin dijital güvenlik öz yeterlik algılarına etkisi nedir? sorusuna yanıt aranmıştır. Bu doğrultuda “Dijital Güvenlik Öz Yeterlik Envanteri” ile elde edilen veriler istatistiksel tekniklerle analiz edilmiş, analiz sonucu elde edilen bulgular alt problemler dikkate alınarak tablolaştırılmış ve yorumlanmıştır.

4.1. Birinci Alt Probleme İlişkin Bulgular ve Yorumlar

Deney grubu öğrencileri ile kontrol grubu öğrencilerinin dijital güvenlik öz yeterlik envanteri ön test puan ortalamalarına bağlı sıra ortalamaları arasında istatistiksel olarak anlamlı bir fark var mıdır?

Yukarıda ifade edilen birinci alt probleme ilişkin sosyal bilgiler dersinde dijital güvenlik yeterliği için geliştirilen çevrim içi destekleyici öğrenme aracının uygulandığı deney grubu öğrencileri ile sınıf içi ortamda dijital güvenlik eğitiminin uygulandığı kontrol grubu öğrencilerinin, deneysel işlem öncesi “Dijital Güvenlik Öz Yeterlik Envanterinden” aldıkları

puanlar arasındaki farklılığa ilişkin Mann-Whitney U Testi sonuçları Tablo 6’da görülmektedir.

Tablo 6.

Deney Grubu İle Kontrol Grubunun Öntest Puanları Arasındaki Farklılığa İlişkin Mann-Whitney U Testi Sonuçları

Öntest	Grup	n	$\bar{X}$	S	Sıra Ortalaması	Sıra Toplamı	U	p
Teknik Alt Ölçeği	Deney	35	55,29	11,29	33,81	1183,50	553,50	,935
	Kontrol	32	56,34	7,80	34,20	1094,50		
Psikososyal Alt Ölçeği	Deney	35	33,94	5,10	33,14	1160,00	530,00	,705
	Kontrol	32	34,78	4,09	34,94	1118,00		
Çevrim İçi Alışveriş Alt Ölçeği	Deney	35	21,20	2,91	33,74	1181,00	551,00	,909
	Kontrol	32	21,19	3,23	34,28	1097,00		
Hak ve Sorumluluk Alt Ölçeği	Deney	35	29,89	3,66	34,04	1191,50	558,50	,985
	Kontrol	32	29,84	3,35	33,95	1086,50		
Sağlık Alt Ölçeği	Deney	35	18,91	3,95	34,03	1191,00	559,00	,990
	Kontrol	32	18,56	4,96	33,97	1087,00		

*p<,05

Tablo 6 incelendiğinde; deney grubu ve kontrol grubu öğrencilerinin dijital güvenlik öz yeterlik envanterine ait alt ölçeklerden aldıkları puan ortalamalarına bağlı sıra ortalamaları arasında farklılık olup olmadığına bakılmıştır.

Teknik alt ölçeğinde deney grubu öğrencilerinin ortalama puanlarına ait sıra ortalamaları ile kontrol grubu öğrencilerinin puan ortalamalarına bağlı sıra ortalamaları arasında $U=553,50$, $p=,935>,05$ ’e göre anlamlı farklılık olmadığı yani grupların birbirine denk olduğu görülmektedir.

Psikososyal alt ölçeğinde deney grubu öğrencilerinin ortalama puanlarına ait sıra ortalamaları ile kontrol grubu öğrencilerinin puan ortalamalarına bağlı sıra ortalamaları arasında $U=530,00$, $p=,705>,05$ ’e göre anlamlı farklılık olmadığı yani grupların birbirine denk olduğu görülmektedir.

Çevrim içi alışveriş alt ölçeğinde deney grubu öğrencilerinin puan ortalamalarına bağlı sıra ortalamaları ile kontrol grubu öğrencilerinin puan ortalamalarına bağlı sıra ortalamaları arasında $U=551,00$, $p=,909>,05$ 'e göre anlamlı farklılık olmadığı yani grupların birbirine denk olduğu görülmektedir.

Hak ve sorumluluk alt ölçeğinde deney grubu öğrencilerinin puan ortalamalarına bağlı sıra ortalamaları ile kontrol grubu öğrencilerinin puan ortalamalarına bağlı sıra ortalamaları arasında $U=558,50$, $p=,985>,05$ 'e göre anlamlı farklılık olmadığı yani grupların birbirine denk olduğu görülmektedir.

Sağlık alt ölçeğinde deney grubu öğrencilerinin puan ortalamalarına bağlı sıra ortalamaları ile kontrol grubu öğrencilerinin puan ortalamalarına bağlı sıra ortalamaları arasında $U=559,00$, $p=,990>,05$ 'e göre anlamlı farklılık olmadığı yani grupların birbirine denk olduğu görülmektedir.

4.2. İkinci Alt Probleme İlişkin Bulgular ve Yorumlar

Kontrol grubu öğrencilerinin dijital güvenlik öz yeterlik algısı ile ilgili ön test ve son testten aldığı puan ortalamalarına bağlı sıra ortalamaları istatistiksel olarak anlamlı bir fark var mıdır?

Yukarıda ifade edilen ikinci alt probleme ilişkin sosyal bilgiler dersinde sınıf içi ortamda dijital güvenlik eğitiminin uygulandığı kontrol grubu öğrencilerinin, dijital güvenlik öz yeterlik algısı ile ilgili öntest ve son testten aldıkları puanlar arasındaki farklılığa ilişkin Wilcoxon İşaretli Sıralar Testi sonuçları Tablo 7'de görülmektedir.

Tablo 7.

Kontrol Grubunun Öntest Puanları ile Sontest Puanları Arasındaki Farklılığa İlişkin Wilcoxon İşaretli Sıralar Testi

Kontrol Grubu	Test	n	$\bar{X}$	S	Sıra Ortalaması	Sıra Toplamı	Z	p
Teknik Alt Ölçeği	Öntest	32	56,34	7,80	2,75	5,50	-4,75	,000*
	Sontest	32	67,94	4,74	16,91	490,50		
Psikososyal Alt Ölçeği	Öntest	32	34,78	4,09	12,35	123,50	-1,82	,069
	Sontest	32	36,41	2,82	15,69	282,50		
Çevrim İçi Alışveriş Alt Ölçeği	Öntest	32	21,19	3,23	6,60	33,00	-3,21	,001*
	Sontest	32	23,03	2,04	13,50	243,00		
Hak ve Sorumluluk Alt Ölçeği	Öntest	32	29,84	3,35	8,89	80,00	-3,16	,002*
	Sontest	32	31,94	2,41	18,33	385,00		
Sağlık Alt Ölçeği	Öntest	32	18,56	4,96	10,44	83,50	-2,34	,019*
	Sontest	32	20,94	3,52	14,86	267,50		

*p<,05

Tablo 7’de kontrol grubu öğrencilerinin dijital güvenlik öz yeterlik envanterine ait alt ölçeklerden aldıkları öntest puan ortalamalarına bağlı sıra ortalamaları ile sontest puan ortalamalarına bağlı sıra ortalamaları arasında anlamlı farklılık olup olmadığına bakılmıştır.

Teknik alt ölçeğinde kontrol grubu öğrencilerinin öntest puan ortalamalarına bağlı sıra ortalamaları ile sontest puan ortalamalarına bağlı sıra ortalamaları arasında $Z=-4,75$, $p=,000<,05$ ’e göre anlamlı farklılık olduğu yani bu anlamlı farklılık kontrol grubu öğrencilerinin sontest puan ortalamalarına bağlı sıra ortalamaları daha yüksek olmasından kaynaklandığı görülmektedir.

Psikososyal alt ölçeğinde kontrol grubu öğrencilerinin öntest puan ortalamalarına bağlı sıra ortalamaları ile sontest puan ortalamalarına bağlı sıra ortalamaları arasında $Z=-1,82$, $p=,069>,05$ 'e göre anlamlı farklılık olmadığı görülmektedir.

Çevrim içi alışveriş alt ölçeğinde kontrol grubu öğrencilerinin öntest puan ortalamalarına bağlı sıra ortalamaları ile sontest puan ortalamalarına bağlı sıra ortalamaları arasında $Z=-3,21$, $p=,001<,05$ 'e göre anlamlı farklılık olduğu yani bu anlamlı farklılık kontrol grubu öğrencilerinin sontest puan ortalamalarına bağlı sıra ortalamalarının daha yüksek olmasından kaynaklandığı görülmektedir.

Hak ve sorumluluk alt ölçeğinde kontrol grubu öğrencilerinin öntest puan ortalamalarına bağlı sıra ortalamaları ile sontest puan ortalamalarına bağlı sıra ortalamaları arasında $Z=-3,16$, $p=,002<,05$ 'e göre anlamlı farklılık olduğu yani bu anlamlı farklılık kontrol grubu öğrencilerinin sontest puan ortalamalarına bağlı sıra ortalamalarının daha yüksek olmasından kaynaklandığı görülmektedir.

Sağlık alt ölçeğinde kontrol grubu öğrencilerinin öntest puan ortalamalarına bağlı sıra ortalamaları ile sontest puan ortalamalarına bağlı sıra ortalamaları arasında $Z=-2,34$, $p=,019<,05$ 'e göre anlamlı farklılık olduğu yani bu anlamlı farklılık kontrol grubu öğrencilerinin sontest puan ortalamalarına bağlı sıra ortalamalarının daha yüksek olmasından kaynaklandığı görülmektedir.

4.3. Üçüncü Alt Probleme İlişkin Bulgular ve Yorumlar

Deney grubu öğrencilerinin dijital güvenlik öz yeterlik algısı ile ilgili ön test ve son testten aldığı puan ortalamalarına bağlı sıra ortalamaları istatistiksel anlamlı bir fark var mıdır?

Yukarıda ifade edilen üçüncü alt probleme ilişkin sosyal bilgiler dersinde dijital güvenlik yeterliliği için geliştirilen çevrim içi destekleyici öğrenme aracının uygulandığı deney grubu öğrencilerinin, dijital güvenlik öz yeterlik algısı ile ilgili öntest ve son testten aldıkları puanlar arasındaki farklılığa ilişkin Wilcoxon İşaretli Sıralar Testi sonuçları Tablo 8'de görülmektedir.

Tablo 8.

Deney Grubunun Öntest Puanları ile Sontest Puanları Arasındaki Farklılığa İlişkin Wilcoxon İşaretili Sıralar Testi

Deney Grubu	Test	n	$\bar{X}$	S	Sıra Ortalaması	Sıra Toplamı	Z	p
Teknik Alt Ölçeği	Öntest	35	55,29	11,29	,00	,00	-5,16	,000*
	Sontest	35	70,60	3,95	18,00	630,00		
Psikososyal Alt Ölçeği	Öntest	35	33,94	5,10	8,17	49,00	-4,26	,000*
	Sontest	35	37,83	1,92	19,50	546,00		
Çevrim İçi Alışveriş Alt Ölçeği	Öntest	35	21,20	2,91	6,00	18,00	-4,72	,000*
	Sontest	35	24,03	1,15	18,10	543,00		
Hak ve Sorumluluk Alt Ölçeği	Öntest	35	29,89	3,66	7,17	21,50	-4,45	,000*
	Sontest	35	33,00	1,80	16,95	474,50		
Sağlık Alt Ölçeği	Öntest	35	18,91	3,95	1,50	1,50	-4,76	,000*
	Sontest	35	22,94	1,53	15,98	463,50		

*p<,05

Tablo 8’de deney grubu öğrencilerinin dijital güvenlik öz yeterlik envanterine ait alt ölçeklerden aldıkları ön test puan ortalamalarına bağlı sıra ortalamaları ile son test puan ortalamalarına bağlı sıra ortalamaları arasında anlamlı bir farklılık olup olmadığına bakılmıştır.

Teknik alt ölçeğinde deney grubu öğrencilerinin öntest puan ortalamalarına bağlı sıra ortalamaları ile sontest puan ortalamalarına bağlı sıra ortalamaları arasında $Z=-5,16$, $p=,000<,05$ ’e göre anlamlı farklılık olduğu yani bu anlamlı farklılık deney grubu öğrencilerinin sontest puan ortalamalarına bağlı sıra ortalamalarının daha yüksek olmasından kaynaklandığı görülmektedir.

Psikososyal alt ölçeğinde deney grubu öğrencilerinin öntest puan ortalamalarına bağlı sıra ortalamaları ile sontest puan ortalamalarına bağlı sıra ortalamaları arasında $Z=-4,26$, $p=,000<,05$ 'e göre anlamlı farklılık olduğu yani bu anlamlı farklılık deney grubu öğrencilerinin sontest puan ortalamalarına bağlı sıra ortalamalarının daha yüksek olmasından kaynaklandığı görülmektedir.

Çevrim içi alışveriş alt ölçeğinde deney grubu öğrencilerinin öntest puan ortalamalarına bağlı sıra ortalamaları ile sontest puan ortalamalarına bağlı sıra ortalamaları arasında $Z=-4,72$, $p=,000<,05$ 'e göre anlamlı farklılık olduğu yani bu anlamlı farklılık deney grubu öğrencilerinin sontest puan ortalamalarına bağlı sıra ortalamalarının daha yüksek olmasından kaynaklandığı görülmektedir.

Hak ve sorumluluk alt ölçeğinde deney grubu öğrencilerinin öntest puan ortalamalarına bağlı sıra ortalamaları ile sontest puan ortalamalarına bağlı sıra ortalamaları arasında $Z=-4,45$, $p=,000<,05$ 'e göre anlamlı farklılık olduğu yani bu anlamlı farklılık deney grubu öğrencilerinin sontest puan ortalamalarına bağlı sıra ortalamalarının daha yüksek olmasından kaynaklandığı görülmektedir.

Sağlık alt ölçeğinde deney grubu öğrencilerinin öntest puan ortalamalarına bağlı sıra ortalamaları ile sontest puan ortalamalarına bağlı sıra ortalamaları arasında $Z=-4,76$, $p=,000<,05$ 'e göre anlamlı farklılık olduğu yani bu anlamlı farklılık deney grubu öğrencilerinin sontest puan ortalamalarına bağlı sıra ortalamalarının daha yüksek olmasından kaynaklandığı görülmektedir.

4.4. Dördüncü Alt Probleme İlişkin Bulgular ve Yorumlar

Deney grubu öğrencileri ile kontrol grubu öğrencilerinin son test puan ortalamalarına bağlı sıra ortalamaları arasında istatistiksel olarak anlamlı bir fark var mıdır?

Yukarıda ifade edilen dördüncü alt probleme ilişkin sosyal bilgiler dersinde dijital güvenlik yeterliği için geliştirilen çevrim içi destekleyici öğrenme aracının uygulandığı deney grubu öğrencileri ile sınıf içi ortamda dijital güvenlik eğitiminin uygulandığı kontrol grubu öğrencilerinin, deneysel işlem sonrası “Dijital Güvenlik Öz Yeterlik Envanterinden”

aldıkları puanlar arasındaki farklılığa ilişkin Mann-Whitney U Testi sonuçları Tablo 9’da görülmektedir.

Tablo 9.

Deney Grubu İle Kontrol Grubunun Sontest Puanları Arasındaki Farklılığa İlişkin Mann-Whitney U Testi Sonuçları

Sontest	Grup	N	$\bar{X}$	S	Sıra Ortalaması	Sıra Toplamı	U	P
Teknik Alt Ölçeği	Deney	35	70,60	3,95	39,91	1397,00	353,00	,009*
	Kontrol	32	67,94	4,74	27,53	881,00		
Psiko-Sosyal Alt Ölçeği	Deney	35	37,83	1,92	38,54	1349,00	401,00	,043*
	Kontrol	32	36,41	2,82	29,03	929,00		
Çevrim İçi Alışveriş Alt Ölçeği	Deney	35	24,03	1,15	38,30	1340,50	409,50	,049*
	Kontrol	32	23,03	2,04	29,30	937,50		
Hak ve Sorumluluk Alt Ölçeği	Deney	35	33,00	1,80	38,10	1333,50	416,50	,067
	Kontrol	32	31,94	2,41	29,52	944,50		
Sağlık Alt Ölçeği	Deney	35	22,94	1,53	38,67	1353,50	396,50	,038*
	Kontrol	32	20,94	3,52	28,89	924,50		

*p<,05

Tablo 9’da deney grubu öğrencilerinin son test puan ortalamalarına bağlı sıra ortalamaları ile kontrol grubu öğrencilerinin son test puan ortalamalarına bağlı sıra ortalamaları arasında istatistiksel olarak anlamlı bir fark olup olmadığına bakılmıştır.

Teknik alt ölçeğinde deney grubu öğrencilerinin son test puan ortalamalarına bağlı sıra ortalamaları ile kontrol grubu öğrencilerinin son test puan ortalamalarına bağlı sıra ortalamaları arasında $U=353,00$, $p=,009>,05$ ’e göre deney grubu lehine anlamlı bir farklılık olduğu yani bu anlamlı farklılık deney grubu öğrencilerinin son test puan ortalamalarına bağlı sıra ortalamalarının daha yüksek olmasından kaynaklandığı görülmektedir.

Psikososyal alt ölçeğinde deney grubu öğrencilerinin son test puan ortalamalarına bağlı sıra ortalamaları ile kontrol grubu öğrencilerinin son test puan ortalamalarına bağlı sıra

ortalamları arasında $U=401,00$, $p=,043>,05$ 'e göre deney grubu lehine anlamlı bir farklılık olduğu yani bu anlamlı farklılık deney grubu öğrencilerinin son test puan ortalamalarına bağlı sıra ortalamalarının daha yüksek olmasından kaynaklandığı görülmektedir.

Çevrim içi alışveriş alt ölçeğinde deney grubu öğrencilerinin son test puan ortalamalarına bağlı sıra ortalamaları ile kontrol grubu öğrencilerinin son test puan ortalamalarına bağlı sıra ortalamaları arasında $U=409,50$, $p=,049>,05$ 'e göre deney grubu lehine anlamlı bir farklılık olduğu yani bu anlamlı farklılık deney grubu öğrencilerinin son test puan ortalamalarına bağlı sıra ortalamalarının daha yüksek olmasından kaynaklandığı görülmektedir.

Hak ve sorumluluk alt ölçeğinde deney grubu öğrencilerinin son test puan ortalamalarına bağlı sıra ortalamaları ile kontrol grubu öğrencilerinin son test puan ortalamalarına bağlı sıra ortalamaları arasında $U=416,50$, $p=,067>,05$ 'e göre deney grubu lehine puanlar yüksek olsa da anlamlı farklılık olmadığı görülmektedir.

Sağlık alt ölçeğinde deney grubu öğrencilerinin son test puan ortalamalarına bağlı sıra ortalamaları ile kontrol grubu öğrencilerinin son test puan ortalamalarına bağlı sıra ortalamaları arasında $U=396,50$, $p=,038>,05$ 'e göre deney grubu lehine anlamlı bir farklılık olduğu yani bu anlamlı farklılık deney grubu öğrencilerinin son test puan ortalamalarına bağlı sıra ortalamalarının daha yüksek olmasından kaynaklandığı görülmektedir.

Bu bilgiler doğrultusunda deneysel işlem sonrası deney grubu öğrencilerinin dijital güvenlik öz yeterlik algıları, kontrol grubu öğrencilerine göre daha olumludur. Bu bulgu, sosyal bilgiler dersinde 7. sınıf öğrencilerinin dijital güvenlik yeterlikleri için geliştirilmiş olan çevrim içi destekleyici öğrenme aracı ile çevrim içi ortamda öğrenme yaklaşımının dijital güvenlik öz yeterlik algısını artırdığını gösterir.

BÖLÜM V

SONUÇ, TARTIŞMA VE ÖNERİLER

Bu bölümde araştırmanın bulgularına dayalı olarak sonuç, tartışma ve önerilere yer verilmiştir.

5.1. Sonuç ve Tartışma

Bu bölümde 7. sınıf sosyal bilgiler dersinde öğrencilerin dijital güvenlik yeterlikleri için geliştirilen çevrim içi destekleyici öğrenme aracının dijital güvenlik öz yeterlik algısına etkisini belirlemeyi amaçlayan bu çalışmanın bulgularından hareketle ortaya çıkan sonuçlara yer verilmiştir. Bu doğrultuda araştırmanın bulgularından hareketle elde edilen sonuçlar aşağıda açıklanmıştır.

Bu çalışmada deney ve kontrol grubu öğrencilerinin deneysel işlemler öncesi dijital güvenlik öz yeterlik algısını tespit etmek amacıyla ön test olarak “Dijital Güvenlik Öz Yeterlik Envanteri” uygulanmıştır. Elde edilen sonuçlar envanterde yer alan alt ölçeklere ilişkin olarak ayrı ayrı ele alınmıştır.

Bu doğrultuda;

- Teknik alt ölçeğinde deney ve kontrol gruplarının ön test puan ortalamalarına bağlı sıra ortalamaları arasında anlamlı bir farklılık olmadığı,
- Psikososyal alt ölçeğinde deney ve kontrol gruplarının ön test puan ortalamalarına bağlı sıra ortalamaları arasında anlamlı bir farklılık olmadığı,

- Çevrim içi alışveriş alt ölçeğinde deney ve kontrol gruplarının ön test puan ortalamalarına bağlı sıra ortalamaları arasında anlamlı bir farklılık olmadığı,
- Hak ve sorumluluk alt ölçeğinde deney ve kontrol gruplarının ön test puan ortalamalarına bağlı sıra ortalamaları arasında anlamlı bir farklılık olmadığı,
- Sağlık alt ölçeğinde deney ve kontrol gruplarının ön test puan ortalamalarına bağlı sıra ortalamaları arasında anlamlı bir farklılık olmadığı görülmektedir.

Bu sonuçlar, deneysel işlem öncesinde deney ve kontrol grubu öğrencilerinin ön test puanlarının birbirine denk olduğunu göstermektedir. Böylece deneysel işlemler öncesi deney ve kontrol gruplarının birbirine denk olma koşulu yerine getirilmiştir.

Araştırmada kontrol grubu öğrencilerinin dijital güvenlik öz yeterlik envanterine ait ön test ve son testten aldığı puan ortalamalarına bağlı sıra ortalamaları arasında istatistiksel olarak anlamlı bir farklılık olup olmadığına da bakılmıştır. Buna göre kontrol grubunun ön test ve son testten aldıkları puan ortalamalarına bağlı sıra ortalamaları her bir alt ölçekte ayrı ayrı ele alınmıştır.

Bu doğrultuda;

- Teknik alt ölçeğinde kontrol grubu öğrencilerinin öntest puan ortalamalarına bağlı sıra ortalamaları ile sontest puan ortalamalarına bağlı sıra ortalamaları arasında anlamlı farklılık olduğu,
- Psikososyal alt ölçeğinde kontrol grubu öğrencilerinin öntest puan ortalamalarına bağlı sıra ortalamaları ile sontest puan ortalamalarına bağlı sıra ortalamalarına bakıldığında, her ne kadar son test puanları yüksek çıksa da anlamlı düzeyde farklılık olmadığı,
- Çevrim içi alışveriş alt ölçeğinde kontrol grubu öğrencilerinin öntest puan ortalamalarına bağlı sıra ortalamaları ile sontest puan ortalamalarına bağlı sıra ortalamaları arasında anlamlı farklılık olduğu,
- Hak ve sorumluluk alt ölçeğinde kontrol grubu öğrencilerinin öntest puan ortalamalarına bağlı sıra ortalamaları ile sontest puan ortalamalarına bağlı sıra ortalamaları arasında anlamlı farklılık olduğu,
- Sağlık alt ölçeğinde kontrol grubu öğrencilerinin öntest puan ortalamalarına bağlı sıra ortalamaları ile sontest puan ortalamalarına bağlı sıra ortalamaları arasında anlamlı farklılık olduğu görülmektedir.

Bu sonuçlar, kontrol grubu öğrencilerine sınıf içi ortamda verilen “dijital güvenlik eğitiminin” öğrencilerin dijital güvenlik öz yeterlik algılarını teknik, çevrim içi alışveriş, hak ve sorumluluk ve sağlık alt ölçeğinde yükselttiğini ve ön test ile son test arasındaki farkın anlamlı bir farklılık olduğunu göstermektedir. Ancak kontrol grubu öğrencilerinin psikososyal alt ölçeğinde her ne kadar son test puanları yüksek olsa da ön test puanlarıyla karşılaştırıldığında anlamlı bir farklılık görülmemektedir. Bu durumun sebebi psikososyal alt ölçekte ele alınan dijital zorbalık hakkında karamsarlık algısı olabilir. Smith vd. (2008) dijital zorbalıkla mücadele konusunda kişilerde genelde karamsarlık olduğunu belirtmiş, bununla birlikte yapılan çalışmada öğrencilerin dijital zorbalığa maruz kaldıklarında kaçınma davranışı gösterdiğini ifade etmektedirler. Kaçınma davranışının karamsarlık ve yetersizlik algısından kaynaklı olabileceği söylenebilir. Yani kontrol grubu öğrencilerinin karamsarlık duygusunu aşamaması ve yetersizlik hissetmesinden kaynaklı psikososyal öz yeterlik durumları anlamlı düzeyde yükselmemiş olabilir. Ayrıca Hsin, Mu ve Selman (2021) dijital zorbalığın sosyal ve davranışsal bir durum olduğunu, bu konuda duygusal empati yapma konusunda bireylerin eksik olabileceğini ve bu sebeplerin dijital zorbalık yeterlik ya da öz yeterliğini kazandırmayı zorlaştırabileceğini belirtmiştir. Bununla birlikte kontrol grubu öğrencilerinin psikososyal alt ölçeğinde ele alınan dijital zorbalık hakkındaki öz yeterlik algısında anlamlı bir değişim olmayışının diğer bir sebebi ise sınıf içi ortamda sosyal ve davranışsal boyutta dijital bir yeterliğin kazandırılmaya çalışılmasından kaynaklı zorluk olabilir. Çünkü öğrenciler sosyal ve davranışsal bir konuda olan dijital bir beceri ve yetkinliği yine aynı ortamda görerek benzer ortama şahit olarak öğrenmek isteyecektir ve bu durum kişinin öz yeterlik algısının yükselmesinde de etkili olabilir ki deney grubu bu konuyu çevrim içi ortamda daha iyi öğrenmiş ve ön test son test puan ortalamalarına bağlı sıra ortalamaları arasında anlamlı bir farklılık ortaya çıkmıştır.

Karakuş vd. (2014) dijital zorbalıkla mücadele konusunda öğrencilerin yarısına yakınının kendisine güvenmediğini ifade etmektedir. Özbek (2019) ise öğretmen adaylarının kişisel siber güvenliği sağlama durumlarına bakmış ve “kişisel gizliliği koruma” alt boyutunda siber güvenliği sağlama durumlarının düşük düzeyde olduğu sonucuna ulaşmıştır. Burada “kişisel gizliliği koruma” olarak isimlendirilen boyutta yer alan maddeler psikososyal alt ölçeğinde ele alınan “dijital zorbalık” konusu ile ilişkilidir. Buna göre Karakuş vd. (2014)’nin çalışma sonuçları dijital zorbalık konusunda öğrencilerin öz yeterlik algısının düşük olduğunu,

Özbek (2019)' in çalışmasındaki sonuç ise dijital zorbalıkla mücadele konusunda yetişkinlerin bile zorlanabildiğini ifade etmektedir. Bu açıdan kontrol grubu öğrencilerinin psikososyal alt ölçeğinden almış oldukları ön test- son test puan ortalamalarına bağlı sıra ortalamalarının anlamlı düzeyde değişmeme durumu açıklanabilmektedir.

Alanyazında mevcut bazı çalışmalarda ise dijital zorbalık konusunda öğrencilerin çoğunluğunun sorun yaşadığını ve bu konuda farkındalık, mücadele edebilme düzeylerinin düşük olduğu sonucuna ulaşılmıştır (Agatston, Kowalski ve Limber, 2007; Ang, 2015; Li, Sidibe, Shen ve Hesketh, 2019). Raskauskas ve Huynh (2015) yapılmış olan çalışmalardan farklı olarak dijital zorbalık konusunda sistematik bir derleme yapmış, hem dijital zorbalıkla mücadelede kullanılan stratejileri derlemiş hem de yapılmış olan çalışmalar aracılığıyla mücadele etme davranışının üzerinde olumsuz etkileri ortaya koymaya çalışmıştır. Nitekim çalışmada dijital zorbalıkla mücadelede gençlerin özellikle çevrim içi ve çevrim dışı alanda teknik yöntemleri bildiğini fakat bu yöntemleri kaçınma sebepli ya da öz yeterlik düşüklüğü sebebiyle etkili olarak kullanmamış olabileceğini belirtilmiştir. Öz yeterliğin dijital zorbalıkla mücadelede önemli bir yerinin olduğunu savunan Raskauskas ve Huynh (2015) öz yeterliğin depresif belirtilere aracılık ettiğini, sosyal öz yeterliğin ise dijital zorbalığı denetleyen koruyucu bir faktör olduğunu belirtmektedir. Ayrıca bu çalışmada teknik becerilerin bilinmesine rağmen ve bilgi düzeyinin yüksek olmasına rağmen sosyal öz yeterlik sayesinde arabuluculara erişim özgüveni düşük olduğu sürece mücadele edebilmeye olan güvenin her zaman çok yükselemeyeceği belirtilmektedir. Dolayısıyla kontrol grubu öğrencilerinin psikososyal alt ölçeğinden ön test ve son test puan ortalamalarına bağlı sıra ortalamalarının anlamlı düzeyde farklılığa erişememiş olmasında sosyal öz yeterlik algılarının düşük olma ihtimali de etken olabilir.

Araştırmada deney grubu öğrencilerinin dijital güvenlik öz yeterlik envanterinden aldığı ön test ve son test puan ortalamalarına bağlı sıra ortalamaları arasında istatistiksel olarak anlamlı bir farklılık olup olmadığına bakılmıştır. Buna göre deney grubunun deneysel işlem sonrasında araştırmada ölçme aracı olarak kullanılan “Dijital Güvenlik Öz Yeterlik Envanterine” ait ön test ve son testten aldıkları puan ortalamalarına bağlı sıra ortalamaları her bir alt ölçekte ayrı ayrı ele alınmıştır.

Bu doğrultuda;

- Teknik alt ölçeğinde deney grubu öğrencilerinin öntest puan ortalamalarına bağlı sıra ortalamaları ile sontest puan ortalamalarına bağlı sıra ortalamaları arasında anlamlı farklılık olduğu,
- Psikososyal alt ölçeğinde deney grubu öğrencilerinin öntest puan ortalamalarına bağlı sıra ortalamaları ile sontest puan ortalamalarına bağlı sıra ortalamaları arasında anlamlı farklılık olduğu,
- Çevrim içi alışveriş alt ölçeğinde deney grubu öğrencilerinin öntest puan ortalamalarına bağlı sıra ortalamaları ile sontest puan ortalamalarına bağlı sıra ortalamaları arasında anlamlı farklılık olduğu,
- Hak ve sorumluluk alt ölçeğinde deney grubu öğrencilerinin öntest puan ortalamalarına bağlı sıra ortalamaları ile sontest puan ortalamalarına bağlı sıra ortalamaları arasında anlamlı farklılık olduğu,
- Sağlık alt ölçeğinde deney grubu öğrencilerinin öntest puan ortalamalarına bağlı sıra ortalamaları ile sontest puan ortalamalarına bağlı sıra ortalamaları arasında anlamlı farklılık olduğu görülmektedir.

Bu doğrultuda, deney grubu öğrencilerine araştırma kapsamında çevrim içi öğrenme yaklaşımında uygulanan “çevrim içi destekleyici öğrenme aracının” öğrencilerin dijital güvenlik öz yeterlik algılarını teknik, psikososyal, çevrim içi alışveriş, hak ve sorumluluk ve sağlık alt ölçeğinde yükselttiği ve ön test ile son test arasında anlamlı bir farklılık oluşturduğu görülmüştür. Buna göre çevrim içi öğrenme yaklaşımında uygulanan “çevrim içi destekleyici öğrenme aracının” öğrencilerin dijital güvenlik öz yeterlik algısını yükseltmekte başarılı olduğu söylenebilir. Aynı zamanda bu durum çevrim içi öğrenme yaklaşımında bazı dezavantajların olmasına rağmen kullanılan öğrenme aracının öğrencilerin çevrim içi öğrenmeye yönelik ilgi ve motivasyon düzeylerini yükseltebildiği şeklinde de yorumlanabilir. Ayrıca alanyazın incelendiğinde çevrim içi öğrenme araçlarının günümüzde sıklıkla kullanıldığı ve öğrenmede etkisinin büyük olduğu vurgusu görülmektedir. Bu durumu Başarmak (2020), çevrim içi (dijital) öğrenme materyallerinin

öğrenen özelliklerine göreliğı ve de kaliteli, zengin bir içeriğı sahip olmasıyla açıklamıştır (s.256).

Çevrim içi öğrenme ortamı dışında alanyazında dijital materyallerin kullanımının da dijital güvenlik konusunda öğrenmeye etkisini inceleyen araştırmalar bulunmaktadır. Kuh Karyeli ve Dağhan (2020) da dijital teknolojilerle tasarlanmış olduğı öğrenme ortamında dijital ayak izi, araştırma, etik, gizlilik ve güvenlik konularında çalışma grubu üzerinde anlamlı düzeyde farklılığına ulaşmıştır. Bunun haricinde günümüzde çevrim içi öğrenme ortamlarının öğrencilerin öz yeterlik algılarına etkisini inceleyen deneysel çalışmaların sayısı da artmaktadır. Buna ek olarak çevrim içi öğrenme ortamlarının öğrencilerin öz yeterlik algılarındaki etkisinin olumlu anlamda değıştiğı sonucuna da ulaşan çalışmalar bulunmaktadır (Kaptanoğlu, 2022; Öktelik, 2022; Tekinarslan, 2022; Temel, 2022; Yanç, 2022). Öktelik (2022), kısmen benzer olarak ortaokul öğrencilerine yönelik olarak bilgi güvenliğı farkındalığı konusunda geleneksel yöntem ile çevrim içi öğrenmeyi karşılaştırarak deneysel yöntem kullanmıştır. Çalışmada öğrencilerin bilgi güvenliğı farkındalığına etkisi ölçülmüş ve çevrim içi öğrenme yaklaşımının bilgi güvenliğı farkındalığı üzerinde etkisi olumlu yönde anlamlı bir sonuca ulaşmıştır. Günümüzde dijital dönüşümün eğitimde de hızlı bir şekilde yaşanması sonucu çevrim içi öğrenme ortamlarına yönelik çalışmalar artmakta ve çevrim içi öğrenmenin etkililiğı savunulmaktadır. Bu bakımdan çalışmanın deney grubu lehine anlamlı farklılık göstermesi alanyazındaki diğeri sonuçlarla örtüşmektedir.

Araştırmada deney grubu öğrencileri ile kontrol grubu öğrencilerinin dijital güvenlik öz yeterlik envanterinden aldıkları son test puan ortalamalarına bağılı sıra ortalamaları arasında istatistiksel olarak anlamlı bir farklılık olup olmadığına bakılmıştır. Buna göre deney ve kontrol grubunun deneysel işlem sonrasında araştırmada ölçme aracı olarak kullanılan “Dijital Güvenlik Öz Yeterlik Envanterine” ait ön test ve son testten aldıkları puan ortalamalarına bağılı sıra ortalamaları her bir alt ölçekte ayrı ayrı ele alınmıştır.

Bu doğrultuda;

- Teknik alt ölçeğinde deney grubu öğrencilerinin son test puan ortalamalarına bağılı sıra ortalamaları ile kontrol grubu öğrencilerinin son test puan ortalamalarına bağılı sıra ortalamaları arasında deney grubu lehine anlamlı bir farklılık olduğı,

- Psikososyal alt ölçeğinde deney grubu öğrencilerinin son test puan ortalamalarına bağlı sıra ortalamaları ile kontrol grubu öğrencilerinin son test puan ortalamalarına bağlı sıra ortalamaları arasında deney grubu lehine anlamlı bir farklılık olduğu,
- Çevrim içi alışveriş alt ölçeğinde deney grubu öğrencilerinin son test puan ortalamalarına bağlı sıra ortalamaları ile kontrol grubu öğrencilerinin son test puan ortalamalarına bağlı sıra ortalamaları arasında deney grubu lehine anlamlı bir farklılık olduğu,
- Hak ve sorumluluk alt ölçeğinde deney grubu öğrencilerinin son test puan ortalamalarına bağlı sıra ortalamaları ile kontrol grubu öğrencilerinin son test puan ortalamalarına bağlı sıra ortalamaları arasında deney grubu lehine puanlar yüksek olsa da anlamlı farklılık olmadığı,
- Sağlık alt ölçeğinde deney grubu öğrencilerinin son test puan ortalamalarına bağlı sıra ortalamaları ile kontrol grubu öğrencilerinin son test puan ortalamalarına bağlı sıra ortalamaları arasında deney grubu lehine anlamlı bir farklılık olduğu görülmektedir.

Bu sonuçlar, deney grubu öğrencilerine araştırma kapsamında çevrim içi öğrenme yaklaşımında uygulanan “çevrim içi destekleyici öğrenme aracının”, kontrol grubu öğrencilerine sınıf içi ortamda uygulanan “dijital güvenlik eğitime” göre dijital güvenlik öz yeterlik algısını yükseltmekte daha etkili olduğunu göstermektedir. Günümüzde teknolojinin gelişimiyle birlikte daha çok tercih edilen çevrim içi öğrenme materyalleri pek çok araştırmaya konu olmuş ve etkisi ölçülmektedir. Ayrıca çevrim içi öğrenme materyalleri ile sınıf içi öğrenme ortamlarında kullanılan yöntemleri karşılaştıran araştırmalar da mevcuttur. Bu noktada Karademir Coşkun ve Alper (2019), çevrim içi (dijital) öğrenme materyallerinin öğrencilerin dijital olmayan materyallere göre daha çok dikkatini toplama ve yönetme konusunda başarılı olduğunu vurgulamaktadır (s.135). Çalışmada elde edilen sonuçlar ise bunu desteklemektedir. Ek olarak “öğrenme ortamı” denildiğinde akla sadece okulun geldiği dönemlerden günümüzde öğrenme sadece okulda değil dijital ortamda da olabilir anlayışına dönen kültür desteklenmektedir. Güneş (2020) davranışçı/bilişsel yaklaşımda içeriğin kaliteli bir şekilde planlanması ve oluşturulması öğrenmenin artacağı yönüne işaret edeceğini vurgulamıştır (s.292). Bu doğrultuda davranışsal ve bilişsel yönde

öğrenme oluşturulmak istendiğinde içerik iyi örüntülendiği taktirde çevrim içi ortamda da öğrenen hedefe ulaşabilecektir.

Bu araştırmada teknik, psikososyal, çevrim içi alışveriş ve sağlık alt ölçeğine ait son test puanlarının karşılaştırılmasında deney grubu öğrencilerinin lehine anlamlı bir farklılık çıkmasına rağmen hak ve sorumluluk alt ölçeğinde aynı sonuç izlenmemiştir. Bu durum hak ve sorumluluk alt ölçeğinde ele alınan “dijital haklar ve sorumluluklar” ile “dijital hakların ihlalinde şikayet edilebilecek mecralar” konusunun sosyal ve davranışsal bir yönünün olması ve bu becerinin kazandırılmasının zor olmasından kaynaklandığı söylenebilir. Hsin vd. (2021) bu durumu dijital hak ve sorumluluklarla ilgili düşünce ve davranışlarda duygusal empati eksikliğinin yaşandığını, sosyal ve davranışsal beceri ve yeterlikleri içermesinden kaynaklı da kazandırılmasının hiç de kolay olmadığını vurgulayarak açıklamıştır (s.551). Ayrıca Hsin vd. (2021), konunun bu yaş aralığındaki öğrencilerle yüksek düzeyde ilişkili olduğunu fakat varsayımsal davalar üzerinden ele aldığımız bu konuda bireyin çözüm konusunda çelişkili bakış açılarının olabileceğini ve bu yüzden farklı düşüncelere sahip olabileceğini belirtmektedir. Bununla birlikte öğrencilerin hak ve sorumluluk konusuna dair her ne kadar olabilecek gerçekçi senaryolar üzerinden konuya yaklaşılsa da diğer kullanıcılara karşı sorumlulukları, dijital hak ihlalleri ve bu konuda şikayet oluştuğunda gerçek bir müdahalenin yapılıp yapılmayacağı konusunda farklı düşünebilmektedirler. Dijital toplumun sanal olması ve orada yaşanan olayların sanal dünyada kalacağı düşüncesinden de beklenen düzeyde farklılık oluşmamasında etken olabilir.

Elçiçek (2022) yapmış olduğu çalışmasında fikri haklar, erişim, gizlilik gibi etik sorunların herkes tarafından benzer şekilde algınamadığını ve yeterince anlaşılmadığını ifade etmektedir. Aksoy (2019) ise çalışmamızın hak ve sorumluluk alt ölçeğinde ele alınan dijital etik konusunda öğrencilerin dörtte birinin intihal yaptığını, çeşitli araştırmalarda da durumun buna benzer olduğunu, etik ve telif hakları ihlalinin davranışsal alışkanlık yarattığını ve puan kaygısı sebebiyle de yapılabildiğini ifade etmektedir. Buradan hareketle hak ve sorumluluk konusunun içeriğinin tam olarak anlaşılammama, herkese göre farklı anlayışlar ortaya çıkma durumu, alışkanlık ve kaygı durumu öğrencilerin hak ve sorumluluk konusunda kendine olan inanç durumunu düşürebileceği söylenebilir.

Bayındır (2020) ise öğretmen adaylarının dijital güvenlik ihtiyaçlarını tespit etmeyi amaçlayan çalışmasında dijital hak ve sorumluluk konusunda özellikle bilişim suçları

konusunda bilgi düzeyinin yeterli olmadığı, bu konuda oluşan risklere maruz kaldıklarında mücadele yöntemlerini bilmediği sonucuna ulaşmıştır. Araştırmacı buradan hareketle hak ve sorumluluk konusunda ihtiyacın yüksek düzeyde olduğunu ve kişisel bilgi güvenliği eğitimlerinin önemli olduğunu vurgulamıştır. Bu sonuçlar hak ve sorumluluk konusunda öz yeterlik durumuna dikkat çekmektedir.

O'Reilly, Levine ve Law (2020) gençlerde dijital hak ve sorumluluk bağlamında yapmış oldukları çalışmalarında özellikle sorumluluk duygusunun ergenliğin sonlarına doğru tam olarak geliştiği, gelişimsel psikolojiye göre çocukluk ve erken ergenlik dönemlerinde empati, sorumluluk duygusunun yaşanmadığını, dijital ortamda ekran ardında bu durumun daha zor gerçekleştiğini ifade etmiştir. Özellikle çevrim içi etkileşimler sırasında ya da çevrim içi kullanımlar sırasında sanal dünya yaşama algısından dolayı ahlaki düşünme ve davranış arasında kopukluk yaşandığı da bu çalışmada ifade edilmiştir. Bu bakımdan ahlaki gelişim, sorumluluk duygusu ve empati kurma becerilerinin çocukluk döneminde yeterince gelişmemesi dijital ortamda hak ve sorumlulukların benimsenmesini ve öz yeterlik algısının yükselmesinde zorluk yaşatabilmektedir. Öyle ki hak ve sorumluluk vatandaşlık eğitimi açısından da kazandırılması zor bir beceridir ve çocukların gelişimsel dönemleri açısından soyut kalabilmektedir.

Dijital güvenlik ve dijital vatandaşlık konusunda yapılmış olan çalışmalara bakıldığında ise deneysel olarak yapılmış olan çalışmalarda geleneksel yaklaşımların dışında etkinlik temelli ve dijital teknolojilerin entegre edilmesiyle verilen eğitimler ile dijital vatandaşlık bağlamında alt boyut olan dijital güvenlikte farkındalık, öz yeterlik ve algının yükseldiği görülmektedir (Bayrakdar ve Şahinkaya, 2021; Karaduman ve Öztürk, 2014; Sari, 2019)

Karacı, Akyüz ve Bilgici (2017) üniversite öğrencilerine yönelik yaptıkları çalışmalarında internet-bilgisayar güvenliği eğitimi alan ve bu konuda iş deneyimi olan öğrencilerin siber güvenlik davranışlarının daha olumlu olduğu sonucuna ulaşmıştır. Bu konuda internet ve bilgisayar ortamında deneyimlemek siber güvenlik davranışını daha olumlu etkilediği söylenebilir. Ayrıca araştırmacılar çalışmada meslek lisesi bilgisayar bölümü mezunu olan öğrencilerin diğer liselerden mezun olan öğrencilere göre özellikle iz bırakmama durumlarının daha olumlu olduğu sonucuna da ulaşmıştır. Özbek (2019) ise öğretmen adaylarının kişisel siber güvenliğini sağlama durumunu tespit etmeyi amaçladığı çalışmasında bilgisayar eğitimi alan öğrencilerin (BÖTE) diğer bölüm öğrencilerine oranla

siber güvenlik durumunun daha iyi olduđu sonucuna ulaşmıştır. Buradan hareketle dijital becerilere yönelik eğitim alan kişilerin siber güvenlikle ilgili davranışlarının olumlu yönde etkilemiş olduđu sonucu ile çevrim içi öğrenme ortamında verilen eğitim arasında bir bağ kurulabilir.

Genel olarak deney grubundaki öğrencilere çevrim içi destekleyici öğrenme aracı ile çevrim içi öğrenme yaklaşımında verilen eğitimin dijital güvenlik öz yeterlik algılarını yükselttiği ve geliştirilen materyalin dijital güvenlik öz yeterlik durumunu geliştirmede başarılı olduđu söylenebilir. Bu konuda alanyazın incelendiğinde ortaokul öğrencilerine yönelik çevrim içi ortamda dijital güvenlik çerçevesinde tasarlanmış eğitimin öğrencilerin bilgi düzeyleri üzerindeki etkisine yönelik Gölpek Sarı ve Seferoğlu (2021) tarafından yapılan çalışmada verilen çevrim içi eğitim sonucunda öğrencilerin dijital güvenlik bilgi düzeyinin yükseldiği görülmüştür. Bu çalışmada çevrim içi öğrenme ortamlarının önemi vurgulanmakla birlikte bu konuda yapılacak olan deneysel çalışmaların önemine dikkat çekilmektedir. Buna benzer olarak Kuh Karyeli ve Dağhan (2020) çalışmalarında ortaokul 5.-6. sınıf öğrencilerine yönelik dijital materyallerle tasarlanmış sayısal ayak izi eğitiminin akademik başarıya etkisinin anlamlı düzeyde olduğunu ve çevrim içi öğrenme ortamı aracılığıyla bu eğitimin öğrenme üzerinde etkisinin önemli olduđu ifade etmektedir. Yapılmış olan çalışmada çalışmamızın içeriğinde yer alan dijital etik, internette araştırma yapma, dijital zorbalık, dijital ayak izi, gizlilik ve güvenlik ile ilgili kazanımlar yer almaktadır. Yine benzer olarak Gündüzalp (2021) çevrim içi öğrenme ortamlarının zenginleştirilerek öğrenme hedeflerine ulaşabileceğini, bu tür bir öğrenmenin farklı düşünme becerilerini de gerçekleştirebileceğini ve özgüveni yükselttiğini ifade etmektedir.

Çevrim içi öğrenme ortamları dijital çağa uygun bir öğrenme ortamıdır ve dijital yerlilerin ilgisini çekebilmektedir. Verimlilik düzeyi yüksek ve zenginleştirilmiş öğrenme ortamları sayesinde öğrencilerin ilgisinin az olduđu ders ve konularda bile motivasyon düzeyi yükseltilebilmekte, bu sayede öğrenme daha iyi gerçekleştirilebilmektedir. Bu konuda alanyazında çevrim içi destekleyici öğrenme aracının yanı sıra harmanlanmış çevrim içi öğrenme ortamları, oyunlaştırılmış çevrim içi öğrenme ortamı gibi çalışmaların da yapıldığı görülmekte ve bu çalışmalar neticesinde öğrenme düzeyi iyileştirilebilmektedir. Burada temel faktör öğrenme ortamında kullanılmış olan teknolojilerle içeriğin anlamlı şekilde tasarlanmasıdır. Buna ek olarak kişiselleştirilmiş çevrim içi öğrenme ortamlarının da önemi

giderek artmaktadır ve uyarlanmış öğrenme araçları kullanılmaktadır. Bu doğrultuda dijital çağa yakışır bir öğrenmenin gerçekleştirilmesi mümkün kılınabilmektedir.

Dijital çağda insanların yaşamsal durumlarının da değişime uğramış olması ve bu ortama doğan ortaokul yaş grubundaki öğrencilerin yaşamsal faaliyetlerinde dijital ortamı seçmesinde bir etkidir. Bu bakımdan dijital ortama uyum sağlanabilmesi için öğrencilerin dijital güvenlik beceri ve yetkinlikleriyle donatılmış olması ve öz yeterlik durumlarının da geliştirilmesi ihtiyaç haline gelmiştir. Ayrıca öğrencilerin bu konuda öz yeterlik algılarının da tespit edilebilmesi de benzer şekilde önemlidir. Bu bağlamda bu çalışmada dijital güvenlik konusunda çevrim içi öğrenme ortamının ve çevrim içi destekleyici öğrenme aracının öğrenmede etkisi ortaya konulmuştur. Yine bu çalışmada dijital güvenlik konusunda çevrim içi öğrenme yaklaşımında çevrim içi destekleyici öğrenme aracının sınıf içi ortamda verilen eğitime göre öğrencilerin dijital güvenlik öz yeterlik algısında anlamlı düzeyde olumlu etkisinin bulunduğu ortaya konulmuştur.

5.2. Öneriler

Sosyal bilgiler dersinde 7. sınıf öğrencilerinin dijital güvenlik yeterlikleri için geliştirilen çevrim içi destekleyici öğrenme aracının dijital güvenlik öz yeterlik algısına etkisini belirleme amacıyla gerçekleştirilen bu çalışmanın sonuçlarından hareketle araştırmacılara ve uygulamaya yönelik öneriler sunulmuştur. Öneriler uygulamaya yönelik ve araştırmaya yönelik olarak iki başlık altında toplanmıştır.

5.2.1. Uygulamaya Yönelik Öneriler

- Bu çalışmada uygulama sürecinden önce yapılan oryantasyon sürecinde öğrenenlerin bilgisayar kullanma becerilerinin birbirinden farklı olduğu izlenmiştir. Bu amaçla çalışma grubunun süreç öncesinde bilgisayar kullanma beceri düzeylerinin tespit edilmesi ve oryantasyon sürecinin bu düzey doğrultusunda ilerletilmesi önerilmektedir.
- Çevrim içi öğrenme yaklaşımında dijital eşitsizlik konusu önemlidir. Bu konuda hâlâ bilgisayarı olmayan veya internet erişimi olmayan öğrenciler bulunmaktadır. Dijital eşitsizlik probleminde kaynaklı ise bu çalışmada deney grubunda öğrenci kaybı

yaşanmıştır. Bu sebeple yapılacak olan çalışmalarda uygulama öncesinde dijital eşitsizlik konusunda oluşabilecek problemlere çözüm üretilmesi önerilmektedir.

5.2.2. Araştırmaya Yönelik Öneriler

- Dijital vatandaşların dijital ortamın doğru, güvenli ve bilinçli kullanımı için dijital güvenlik farkındalık düzeyleri de önemli bir etkidir. Bu sebeple yapılacak olan araştırmalarda benzer yaklaşım ve çevrim içi öğrenme materyali aracılığıyla öğrencilerin dijital güvenlik farkındalık düzeyini tespit ederek geliştirmek amaçlanabilir.
- Günümüzde dijital dönüşüm sebebiyle dijital vatandaşlık eğitimi önemli görülmektedir, fakat dijital vatandaşlık eğitimi çok boyutludur ve tüm boyutları tek bir araştırma ile vermek kısıtlı kalabilmektedir. Bu sebeple benzer bir araştırma yaklaşımı dijital vatandaşlığın diğer boyutların eğitimi için de önerilebilir.
- Bu araştırma kapsamında geliştirilen çevrim içi destekleyici öğrenme materyali orta okul 7. sınıf öğrencileri düzeyinde etkinlikler içermektedir. Benzer araştırmalar farklı yaş gruplarında da gerçekleştirilebilir.

KAYNAKLAR

- Ackerman, M. S., Cranor, L. F. & Reagle, J. (1999). Beyond concern: understanding net users' attitudes about online privacy. In I. Vogelsang, & B. M. Compaine (Eds.), *The Internet upheaval: Raising questions, seeking answers in communications policy* (pp. 47e72). Cambridge, MA: MIT.
- Acun, İ., Demir, M. & Göz, N.L. (2010). Öğretmen adaylarının vatandaşlık yeterlikleri ile eleştirel düşünme becerileri arasındaki ilişki. *Sosyal Bilgiler Eğitimi Araştırmaları Dergisi*, 1(1), 107-123.
- Agatston, P. W., Kowalski, R., & Limber, S. (2007). Students' perspectives on cyber bullying. *Journal of Adolescent Health*, 41(6), 59-60. <https://doi.org/10.1016/j.jadohealth.2007.09.003>
- Akın, A. & İskender, M. (2011). Internet addiction and depression, anxiety and stress. *International Online Journal of Educational Sciences*, 3(1), 138-148.
- Akkoyunlu, B. & Soylu, Y. (2010). Öğretmenlerin sayısal yetkinlikleri üzerine bir çalışma. *Türk Kütüphaneciliği*, 24(4), 748-768. <https://dergipark.org.tr/en/download/article-file/812096> sayfasından erişilmiştir.
- Aksoy, A. (2019). *Ortaokul öğrencilerinin riskli internet davranışları ve güvenli internet kullanımı hakkında öğrenci ve ebeveyn görüşleri*. Yüksek Lisans Tezi, Marmara Üniversitesi Eğitim Bilimleri Enstitüsü, İstanbul.
- Ala-Mutka, K. (2011). Mapping digital competence: Towards a conceptual understanding. *Sevilla: Institute for Prospective Technological Studies*, 7-60. http://ftp.jrc.es/EURdoc/JRC67075_TN.pdf sayfasından erişilmiştir

- Alex, L. (1991). Description and classification of qualifications: Defining qualification. *Vocational Training*, 2, 21-24.
- Alleva, N. (2019). *Cyberbullying and gender: a qualitative study of how middle school girls experience cyberbullying*. Doktora Tezi, Northeastern University, Boston.
- Al-Rob, E.A. (2021). Cyberbullying and internet addiction among palestinian adolescents. *Journal of Concurrent Disorders*, 3(2), 88-98. https://cdspress.ca/wp-content/uploads/2021/04/MS008_FINAL.pdf sayfasından erişilmiştir.
- Al-Zahrani, A. (2015). Toward digital citizenship: examining factors affecting participation and involvement in the internet society among higher education students. *International Education Studies*, 8(12), 203-217.
- Amhag, L., Hellström, L., & Stigmar, M. (2019). Teacher educators' use of digital tools and needs for digital competence in higher education. *Journal of Digital Learning in Teacher Education*, 35(4), 203-220. <https://doi.org/10.1080/21532974.2019.1646169>
- Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS quarterly*, 34(3), 613-643. <https://doi.org/10.2307/25750694>
- Ang, R. P. (2015). Adolescent cyberbullying: A review of characteristics, prevention and intervention strategies. *Aggression and violent behavior*, 25, 35-42. <https://doi.org/10.1016/j.avb.2015.07.011>
- Arcagök, S. (2020). Öğretmenlerin dijital vatandaşlığa yönelik algılarının incelenmesi. *Van Yüzüncü Yıl Üniversitesi Eğitim Fakültesi Dergisi*, 17(1), 534-556. <https://doi.org/10.33711/yyuefd.693832>
- Arslan, H., Dil, K., Çetin, E., & Yazıcı, S. (2017). Aktif yurttaşlık öz-yeterlik ölçeği: Bir geçerlik ve güvenirlik çalışması. *Journal of Human Sciences*, 14(3), 2797-2809. <https://www.j-humansciences.com/ojs/index.php/IJHS/article/view/4771> sayfasından erişilmiştir.
- Aslan, S. (2016). *İlköğretim sosyal bilgiler öğretmen adaylarını dijital vatandaşlık davranışlarının bazı değişkenler açısından incelenmesi (Fırat, Dicle, Siirt,*

Adıyaman Üniversiteleri örneği). Yüksek Lisans Tezi, Fırat Üniversitesi Eğitim Bilimleri Enstitüsü, Elazığ.

Atasoy, İ. & Ormanlı, O. (2019). Teknoloji ve siber güvenlik: Dijital toplumun geleceği. *İstanbul Aydın Üniversitesi Dergisi*, 11(4), 399-409. <https://dergipark.org.tr/tr/pub/iaud/issue/48524/615832> sayfasından erişilmiştir.

Bağrıacık Yılmaz, A. (2020). *Açık ve uzaktan eğitim öğrencilerinin öğrenimi bırakma ve öğrenime devam nedenlerinin incelenmesi*. Doktora Tezi, Gazi Üniversitesi Eğitim Bilimleri Enstitüsü, Ankara.

Bakır, E. (2016). *Sınıf öğretmeni adaylarının dijital vatandaşlık seviyelerinin dijital vatandaşlık alt boyutlarına göre incelenmesi*. Yüksek Lisans Tezi, Karadeniz Teknik Üniversitesi Eğitim Bilimleri Enstitüsü, Trabzon.

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review*, 84(2), 191–215. <https://doi.org/10.1037/0033-295X.84.2.191>

Bandura, A. (2001). Social cognitive theory: An agentic perspective. *Annual Review of Psychology*, 52, 1–26. <https://doi.org/10.1146/annurev.psych.52.1.1>

Başarmak, U. (2020). Açık ve uzaktan öğrenmede öğretim materyali geliştirme. S. Karataş & E. Kılıç Çakmak (Ed.) *Açık ve uzaktan öğrenme* (ss.239-259). Ankara: Pegem A.

Batu, M., & Güler-İplikçi, H. (2018). Yeni medya rahatsızlıkları: Yeni nesil medyaya farklı bir bakış. B. E. Darıcı (Ed.), *International Conference on Applied Economics and Finance IV. Extended with Social Sciences* (s.637-651). Kuşadası. https://www.researchgate.net/profile/Handan-Gueler-Iplikci/publication/330441059_YENI_MEDYA_RAHATSIZLIKLARI_YENI_NESIL_MEDYAYA_FARKLI_BIR_BAKIS/links/5c403c2e92851c22a37ae51b/YENI-MEDYA-RAHATSIZLIKLARI-YENI-NESIL_MEDYA_YAFARKLI-BIR-BAKIS.pdf sayfasından erişilmiştir.

Bayındır, N., (2020). Sınıf öğretmeni adaylarının dijital eğitimde dijital güvenlik ihtiyaçlarının belirlenmesi. VIIth International Eurasian Educational Research Congress, (s.627-634). Eskişehir, Turkey.

- Bayrakdar, C. & Şahinkayası, H. (2021). Bir köy ortaokulunda dijital hikâyeleme yönteminin öğrencilerin etik ve güvenlik ünitesi erişilerine etkisi. *Mustafa Kemal Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 18(47), 147-173. <https://dergipark.org.tr/en/pub/mkusbed/issue/62012/896130> sayfasından erişilmiştir.
- Bayzan, Ş. (2019). *Dijital hak ve sorumluluklarımız nelerdir?*. <https://www.guvenliweb.org.tr/haber-detay/dijital-hak-ve-sorumluluklarmiz-nelerdir> sayfasından erişilmiştir.
- Bilgi Teknolojileri ve İletişim Kurumu (2019). İnternetin riskleri ve zararları. <https://internet.btk.gov.tr/internetin-riskleri-ve-zararlari> sayfasından erişilmiştir.
- Binay Eyuboğlu, F. A., & Karaoğlu Yılmaz, F. G. (2018). Öğretmenlerin yaşam boyu öğrenme tutumları, dijital yerli olma durumları ve teknoloji kabulü arasındaki ilişkinin birbirleri ile ve çeşitli değişkenler açısından incelenmesi. *Uluslararası Eğitim Bilim ve Teknoloji Dergisi*, 4(1), 1-17. <https://dergipark.org.tr/tr/pub/uebt/issue/37056/397202> sayfasından erişilmiştir.
- Bozkurt, A., Hamutoğlu, N.B., Liman Kaban, A., Taşçı, G. & Aykul, M. (2021). Dijital bilgi çağı: Dijital toplum, dijital dönüşüm, dijital eğitim ve dijital yeterlikler. *Açıköğretim Uygulamaları ve Araştırmaları Dergisi (AUAd)*, 7(2), 35-63. <https://doi.org/10.51948/auad.911584>
- Bratina, T. (2016, July). Digital risks and experiences of future teachers. 39th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia.
- Bratina T. & Krasna, M. (2011). Students' Attitude Toward Digital Security. 5th International Technology, Education and Development Conference (INTED), Valencia. file:///C:/Users/ab153269/Downloads/Studentsattitudetowarddigitalsecurity_inte2011.pdf sayfasından erişilmiştir.
- Buzkıran, B. (2017). 8. sınıf öğrencilerinin sosyal bilgiler dersi başarı düzeylerinin problemli internet kullanımı ve bazı değişkenler açısından incelenmesi. *TRT Akademi*, 2(4),

- 418-439. <https://dergipark.org.tr/tr/pub/trta/issue/45884/579135> sayfasından erişilmiştir.
- Büyüköztürk, Ş., Kılıç Çakmak, E., Akgün, Ö.E., Karadeniz, Ş. ve Demirel, F. (2012). *Bilimsel araştırma yöntemleri*. (11. Baskı). Ankara: Pegem Akademi.
- Byrne, Z. S., Dvorak, K. J., Peters, J. M., Ray, I., Howe, A., & Sanchez, D. (2016). From the user's perspective: Perceptions of risk relative to benefit associated with using the Internet. *Computers in Human Behavior*, 5(9), 456-468. <https://doi.org/10.1016/j.chb.2016.02.024>
- Cambridge International Dictionary of English (2022a). <https://dictionary.cambridge.org/dictionary/english-turkish/digital> sayfasından erişilmiştir.
- Cambridge International Dictionary of English (2022b). <https://dictionary.cambridge.org/dictionary/english/digital-age> sayfasından erişilmiştir.
- Campbell, D. T., & Stanley, J. C. (1996). *The post test-only control group design*. Experimental and quasi-experimental designs for research. Chicago; Rand McNally College, 25-31.
- Canbek, G., & Sağıroğlu, Ş. (2007). Çocukların ve gençlerin bilgisayar ve internet güvenliği. *Politeknik Dergisi*, 10(1), 33-39. <https://dergipark.org.tr/tr/pub/politeknik/issue/33024/367138> sayfasından erişilmiştir.
- Carliner, S. (2004). *An overview of online learning*. Amherst, MA: Human Resource Development.
- Castells, M. (2004). The network society: A cross cultural perspective. *Edward Elgar*. <https://doi.org/10.4337/9781845421663>
- CIA- The World Factbook (2022). Internet Users. <https://www.cia.gov/the-world-factbook/field/internet-users/> sayfasından erişilmiştir.

- Committed to Connecting The World [ITU] (2021). Measuring digital development: Facts and figures 2021. <https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx> sayfasından erişilmiştir.
- Common Sense Kids Action (2017). Creating access to digital citizenship and media literacy education. https://www.common sense media.org/sites/default/files/featured-content/files/2017_dig-cit-white-paper_final.pdf sayfasından erişilmiştir.
- Çağıltay, K., İslim, Ö. F., Kaşıkçı, D. N., Kurşun, E., & Yılmaz, T. K. (2017). Çocukların sosyal ağlarda kişisel bilgi paylaşım eğilimleri. *Kastamonu Eğitim Dergisi*, 25(2), 597-610. <https://dergipark.org.tr/tr/pub/kefdergi/issue/29416/314234> sayfasından erişilmiştir.
- Çatlı, M. & Keskin, S. (2021). İnsan haklarının değişime açık konusu: dijital vatandaşlık kavramı üzerine bir inceleme. *Ombudsman Akademik*, 7(14), 199-229. <https://dergipark.org.tr/tr/pub/ombudsmanakademik/issue/63284/932597> sayfasından erişilmiştir.
- Çelen, F. K., Çelik, A., & Seferoğlu, S. S. (2011). Çocukların internet kullanımları ve onları bekleyen çevrim-içi riskler. *Akademik Bilişim*, 2(4), 645-652. https://yunus.hacettepe.edu.tr/~%20sadi/yayin/AB11_Celen-Celik_Seferoglu_Cocuklar-Internet-Riskler.pdf sayfasından erişilmiştir.
- Çepni, O., Oğuz, S. & Kılcan, B. (2014). The perceptions of primary school students regarding digital citizenship . *Türkiye Sosyal Araştırmalar Dergisi*, 183 (183), 251-266. <https://dergipark.org.tr/tr/pub/tsadergisi/issue/21495/230453> sayfasından erişilmiştir.
- Çetin, M. & Özgiden, H. (2013). Dijital kültür sürecinde dijital yerliler ve dijital göçmenlerin twitter kullanım davranışları üzerine bir araştırma. *Gümüşhane Üniversitesi İletişim Fakültesi Elektronik Dergisi*, 2(1), 172-189. <https://dergipark.org.tr/tr/pub/e-gifder/issue/7470/98369> sayfasından erişilmiştir.
- Çolak, B., Yalçın, B. ve Korkmaz, S. (2011). Türkiye’de internet kullanımının toplumsal yansımaları. XVI. Türkiye’de İnternet Konferansı, 30 Kasım-2 Aralık 2011, Ege Üniversitesi Atatürk Kültür Merkezi, Konak, İzmir.

- Çolak, C. (2019). *Üniversite öğrencilerinin dijital güvenlik öz yeterlikleri ve çevrim içi risk alma eğilimlerinin incelenmesi*. Doktora Tezi, Anadolu Üniversitesi Eğitim Bilimleri Enstitüsü, Eskişehir.
- Çömlekçi, M. F. (2019). Sosyal medyada dezenformasyon ve haber doğrulama platformlarının pratikleri. Gümüşhane Üniversitesi İletişim Fakültesi Elektronik Dergisi, e-gifder, cilt: 7, Uluslararası Türk Dünyası Basın Sempozyumu Özel Sayısı, Aralık, 2019, 1549-1563. <https://doi.org/10.19145/e-gifder.583825>
- Çubukçu, A. & Bayzan, Ş. (2013). Türkiye’de dijital vatandaşlık algısı ve bu algıyı internetin bilinçli, güvenli ve etkin kullanımı ile artırma yöntemleri. *Middle Eastern & African Journal of Education Research*, 5, 148-174.
- Demir, M. V. (2022). *Üniversite öğrencilerinin dijital ortamlarda doğru ve güvenli bilgi erişim, teyit ve paylaşım davranışları ölçeğinin geliştirilmesi*. Yüksek Lisans Tezi, Trakya Üniversitesi Fen Bilimleri Enstitüsü, Edirne.
- Demirel, M., Yörük, M., & Özkan, O. (2012). Çocuklar için güvenli internet: güvenli internet hizmeti ve ebeveyn görüşleri üzerine bir araştırma-safe internet for children: a study on safe internet service and parental views. *Mehmet Akif Ersoy Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 4(7), 54-68. <https://dergipark.org.tr/en/download/article-file/181790> sayfasından erişilmiştir.
- Dere, İ. & Yavuzay, M. (2019). Sosyal bilgiler öğretmen adaylarının dijital vatandaşlık göstergelerinin incelenmesi. *MANAS Sosyal Araştırmalar Dergisi*, 8(3), 2400-2411.
- Desimpelaere, L., Hudders, L. & Sompel, D.V. (2020). Knowledge as a strategy for privacy protection: How a privacy literacy training affects children's online disclosure behavior. *Media and Communication*, 8(4), 163-174. <https://doi.org/10.1016/j.chb.2020.106382>
- Dodel, M., & Mesch, G. (2018). Inequality in digital skills and the adoption of online safety behaviors. *Information, Communication & Society*, 21(5), 712-728. <https://doi.org/10.1080/1369118X.2018.1428652>

- Doğanç, E. & Korucu, A.T (2020). Öğretmen adayları için güvenli internet kullanımı öz-yeterlik ve algı ölçeği. *Eğitim Teknolojisi Kuram ve Uygulama*, 10 (1) , 201-218. <https://doi.org/10.17943/etku.623650>
- Durmaz, N. & Ulukol, B. (2022). Dijital yerliler ve dijital göçmenler: sağlık çalışanı ebeveynlerin çocuklarının internet güvenliği ve dijital oyunlar hakkında farkındalıkları. *Journal of History School*, 58, 1949-1970. <http://dx.doi.org/10.29228/Joh.57592>
- Ekinci, İ. (2016). *Sosyal bilgiler öğretmenlerinin vatandaşlık algıları ve vatandaşlık eğitimi ile ilgili düşüncelerinin incelenmesi*. Doktora Tezi, Dumlupınar Üniversitesi Eğitim Bilimleri Enstitüsü, Kütahya.
- Ekinci, O. & Kayapalı Yıldırım, S. (2019). Siber mobbing ölçeği geçerlilik ve güvenirlik çalışması. *Mavi Atlas*, 7(2), 294-320. <https://doi.org/10.18795/gumusmaviatlas.627092>
- Elçi, A. C. & Sarı, M. (2016). Bilişim teknolojileri ve yazılım dersi öğretim programına yönelik öğrenci görüşlerinin dijital vatandaşlık bağlamında incelenmesi, *Çukurova Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 25(3), 87-102. <https://dergipark.org.tr/tr/pub/cusosbil/issue/32038/353253> sayfasından erişilmiştir.
- Elçi, C. (2015). *Bilişim teknolojileri ve yazılım dersi öğretim programına yönelik öğrenci görüşlerinin dijital vatandaşlık bağlamında incelenmesi*. Yüksek Lisans Tezi, Çukurova Üniversitesi Sosyal Bilimler Enstitüsü, Adana.
- Elçiçek, M., Erdemci, H. & Karal, H. (2018). Examining the relationship between the levels of digital citizenship and social presence for the graduate students having online education. *Turkish Online Journal of Distance Education-TOJDE*, 19(1), 203-214. <https://doi.org/0.17718/tojde.382801>
- Elçiçek, M. (2022). Çevrimiçi ortamlarda öğrenim gören üniversite sistemlerindeki bilişim etiğine yönelik imge ve algıları: Bir metafor analizi. *Osmaniye Korkut Ata Üniversitesi Fen Bilimleri Enstitüsü Dergisi*, 5(1), 205-223. <https://doi.org/10.47495/okufbed.1042317>

- Eraut, M. (1998). Concepts of Competence. *Journal of Interprofessional Care*, 1(2), 127-139. <https://doi.org/10.3109/13561829809014100>
- Erbay, A. (2009,Ocak). *İnsan hakları ve demokrasi açısından yurttaşlık*. Human Beings, Society, Intercultural Dialogue And Education At The Beginnings Of The 21st Century Kongresi'nde sunulmuş bildiri, Uludağ Üniversitesi, Bursa.
- Erdem, F.H. (2012). Anayasal vatandaşlık ve yeni anayasa. *Liberal Düşünce Dergisi*, 17(66), 49-56. <https://dergipark.org.tr/tr/pub/liberal/issue/48166/609456> sayfasından erişilmiştir.
- Erdoğan, A. (2017). *Üniversite öğrencilerinin bilgi güvenliği kazanımları, farklılıkları üzerindeki etkilerinin analizi: Afyon Kocatepe Üniversitesi örneği*. Yüksek Lisans Tezi, Afyon Kocatepe Üniversitesi Fen Bilimleri Enstitüsü, Afyon.
- Eser Akkuş, D. (2017). *Türkiye'deki azınlıkların dijital vatandaşlık pratikleri*. Yüksek Lisans Tezi, Marmara Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.
- EU Kids Online (2020). *New European study on children and the internet in 19 countries*. The London School of Economics and Political Science (LSE). London: England.
- European Council. (2006). *Recommendation of the european parliament and of the council on key competences for lifelong learning*. <https://eurlex.europa.eu/legal-content/EN/TXT/?uri=celex:32006H0962> sayfasından erişilmiştir.
- Elektronik Ticaret Bilgi Platformu (2021). 2021 yılı e-ticaret verileri. <https://www.eticaret.gov.tr/haberler/10040/detay> sayfasından erişilmiştir.
- Fernandes, B., Biswas, U. N., Mansukhani, R. T., Casarín, A. V. ve Essau, C. A. (2020). The impact of COVID-19 lockdown on internet use and escapism in adolescents. *Revista de Psicología Clínica Con Niños y Adolescentes*, 7(3), 59–65. https://www.revistapcna.com/sites/default/files/010_0.pdf sayfasından erişilmiştir.
- Ferrari, A. (2013). DIGCOMP: A framework for developing and understanding digital competence in Europe.

- Fidan, M. & 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>
- Fraenkel, J. R., Wallen, N. E., & Hyun, H. H. (2011). *How to design and evaluate research in education*. New York: McGraw-Hill Humanities/Social Sciences/Languages.
- Franklin, A., & Smeaton, E. (2017). Recognising and responding to young people with learning disabilities who experience, or are at risk of, child sexual exploitation in the UK. *Children and Youth Services Review*, 73, 474-481. <https://doi.org/10.1016/j.childyouth.2016.11.009>
- Fukuyama, M. (2018). Society 5.0: Aiming for a new human-centered society. *Japan Spotlight*, 27, 47-50.
- GEF. (2020). GEF Vision: Educational ecosystems for societal transformation. Global Education Futures. http://www.globaledufutures.org/images/people/GEF_EducationalSystemsforSocietalTransformation_report.pdf sayfasından erişilmiştir.
- Gibb, A. (1990). Training the trainers for small business. *Journal of European Industrial Training*, 14(1), 17-25. <https://doi.org/10.1108/03090599010138543>
- Gleason, B. & Gillern, S. (2018). Digital citizenship with social media: Participatory practices of teaching and learning in secondary education. *Educational Technology & Society*, 21(1), 200–212. [2018_GleasonB_Digital_Citizenship_with_Social_Media.pdf](https://www.elsevier.com/locate/jtse/2018_GleasonB_Digital_Citizenship_with_Social_Media.pdf) sayfasından erişilmiştir.
- Gökbulut, B., Keserci, G., & Akyüz, A. (2021). Eğitim fakültesinde görev yapan akademisyen ve öğretmenlerin dijital materyal tasarım yeterlikleri. *Journal of Social Sciences And Education*, 4(1), 11-24. <https://doi.org/10.53047/josse.917536>
- Gölpek Sarı, F. & Seferoğlu, S.S. (2021). Çevrimiçi güvenlik ve risk eğitimi için geliştirilen çevrimiçi ortamın ortaokul öğrencilerinin bilgi düzeylerine etkisi. *Ondokuz Mayıs Üniversitesi Eğitim Dergisi*, 40 (2), 901-961. <https://dergipark.org.tr/en/download/article-file/1753871> sayfasından erişilmiştir.

- Görmez, E. (2016). Öğretmen adaylarının dijital vatandaşlık ve alt boyutları hakkındaki görüşleri (Bir durum çalışması). *International Periodical for the Languages, Literature and History of Turkish or Turkic*, 11(21), 125- 144.
- Görmez, E. (2017). Öğretmenlerin dijital vatandaşlık ve alt boyutları hakkındaki düzeyleri (Van ili örneği). *Akademik Bakış Dergisi*, 60, 52-74. <https://dergipark.org.tr/tr/pub/abuhbsd/issue/32973/366488> sayfasından erişilmiştir.
- Gündüzalp, C. (2021). Web 2.0 araçları ile zenginleştirilmiş çevrimiçi öğrenmenin öğrencilerin üst bilişsel ve yaratıcı düşünme becerilerine etkisi. *Uluslararası Türkçe Edebiyat Kültür Eğitim (TEKE) Dergisi*, 10(3), 1158-1177. <https://dergipark.org.tr/en/download/article-file/1994896> sayfasından erişilmiştir.
- Güneş, E. (2020). Açık ve uzaktan eğitimin geleceği araştırma ve değerlendirme. S. Karataş ve E. Kılıç Çakmak (Ed.) *Açık ve uzaktan öğrenme* (ss.281-302). Ankara: Pegem A.
- Gümüş, M. M. (2021). *Öğretmenlerin dijital yeterlikleri*. Yüksek Lisans Tezi, Amasya Üniversitesi Fen Bilimleri Enstitüsü, Amasya.
- Güvenli Web (2017). İnternet ve sağlık. <https://www.guvenliweb.org.tr/dokuman-detay/internet-ve-saglik> sayfasından erişilmiştir.
- Hablemitoğlu, Ş. & Özmete, E. (2012). Etkili vatandaşlık eğitimi için bir öneri. *Ankara Sağlık Bilimleri Dergisi*, 1(3), 39-54. https://doi.org/10.1501/Asbd_00000000028
- Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, 3(7), e00346. <https://doi.org/10.1016/j.heliyon.2017.e00346>
- Hamutoğlu, N. B., Güngören, Ö. C., Uyanık, G. K., & Erdoğan, D. G. (2017). Dijital okuryazarlık ölçeği: Türkçe'ye uyarlama çalışması. *Ege Eğitim Dergisi*, 18(1), 408-429. <https://doi.org/10.12984/egeefd.295306>
- Hartikainen, H., Livari, N. & Kinnula, M. (2019). Children's design recommendations for online safety education. *International Journal of Child-Computer Interaction*, 22(6), 100-146. <https://doi.org/10.1016/j.ijcci.2019.100146>
- Hasebrink, U., Livingstone, S., Haddon, L., & Olafsson, K. (2009). *Comparing children's online opportunities and risks across Europe: Cross-national comparisons for EU*

Kids Online. LSE, London: EU Kids Online (2nd edition). http://eprints.lse.ac.uk/24368/1/D3-2_Report-Cross-national_comparisons-2nd-edition.pdf sayfasından erişilmiştir.

Heater, D. (2004). *A history of education for citizenship*. London: Routledge.

Helsper, E. J., & Smahel, D. (2020). Excessive internet use by young Europeans: psychological vulnerability and digital literacy?. *Information, Communication & Society*, 23(9), 1255-1273. <https://doi.org/10.1080/1369118X.2018.1563203>

Hendrix, M., Al-Sherbaz, A. & Bloom, V. (2016). Game based cyber security training: are serious games suitable for cyber security training?. *International Journal of Serious Games*, 3(1), 53-61.

Hintz, A., Dencik, L. & Jorgensen, K.W. (2017). Dijital citizenship and surveillance society. *International Journal of Communication*, 11, 731-739. <https://ijoc.org/index.php/ijoc/article/view/5521/1929> sayfasından erişilmiştir.

Hobbs, R. & Jensen, A. (2009). The past, present, and future of media literacy education. *The Journal of Media Literacy Education*, 1(1), 1-11. <https://doi.org/10.23860/jmle-1-1-1>

Holland, L.M. (2017). *The Perceptions of Digital Citizenship in Middle School Learning*. Doktora Tezi, Carson- Newman University, Jefferson.

Hollandsworth, R., Dowdy, L. & Donovan, J. (2011). Digital citizenship in k-12: It takes a village. *Tech Trends: Linking Research & Practice to Improve Learning*, 55(4), 37-47. <https://doi.org/10.1007/s11528-011-0510-z>

Holloway, D., Green, L., & Livingstone, S. (2013). Zero to eight: young children and their internet use. EU Kids Online. EU Kids Online, The London School of Economics and Political Science, London, UK. [file:///C:/Users/ab153269/Downloads/ZerotoEight-libre%20\(1\).pdf](file:///C:/Users/ab153269/Downloads/ZerotoEight-libre%20(1).pdf) sayfasından erişilmiştir.

Horton, W. (2006). *E-Learning by Design*. San Francisco, CA, ABD: Pfeiffer.

- Hsin, L.B., Mu, N., & Selman, R.L. (2021). Rights and Responsibilities With Tech: Students' Take on Classroom Policies. *Read Teach*, 74(5), 549–558. <https://doi.org/10.1002/trtr.1986>
- Internet World Stats (2022). World Internet Users and 2022 Population Stats. <https://www.internetworldstats.com/stats.htm> sayfasından erişilmiştir.
- ISTE, (2007). Digital citizenship in schools. <http://www.iste.org/images/excerpts/digcit-excerpt.pdf> sayfasından erişilmiştir.
- İşman, A. & Güngören, Ö.C. (2014). Digital citizenship. *The Turkish Online Journal of Educational Technology*, 13(1), 73-77. <https://files.eric.ed.gov/fulltext/EJ1018088.pdf> sayfasından erişilmiştir.
- Kan, Ç. (2009). Sosyal bilgiler eğitiminde küresel vatandaşlık. *Pamukkale Üniversitesi Eğitim Fakültesi Dergisi*, 26(26), 25-30. <https://dergipark.org.tr/tr/pub/pauefd/issue/11117/132948> sayfasından erişilmiştir.
- Kaptanoğlu, M. Y. (2022). *Self-regulation and self-efficacy of Turkish efl learners in online learning within hybrid education context*. Yüksek Lisans Tezi, Yıldız Teknik Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.
- Kara, T. & Atasoy, E. (2019). Sosyal bilgiler öğretim programı ve ders kitaplarının (2018) dijital vatandaşlık kavramı ve alt boyutları bağlamında incelenmesi. *Balıkesir Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 22(41), 133-153. <https://doi.org/10.31795/baunsobed.581917>
- Karademir Coşkun, T., & Alper, A. (2019). Usage of digital learning material in special education. *Ankara Üniversitesi Eğitim Bilimleri Fakültesi Özel Eğitim Dergisi*, 20(1), 119-142. <https://doi.org/10.21565/ozelegitimdergisi.423349>
- Karaduman, H. & Öztürk, C. (2014). Sosyal bilgiler dersinde dijital vatandaşlığa dayalı etkinliklerin öğrencilerin dijital vatandaşlık tutumlarına etkisi ve dijital vatandaşlık anlayışlarına yansımaları. *Journal of Social Studies Education Research*, 5(1), 38-78. <https://dergipark.org.tr/tr/pub/jsser/issue/19102/202728> sayfasından erişilmiştir.
- Karakuş, T., Çağıltay, K., Kaşıkçı, D., Kurşun, E., & Ogan, C. (2014). Türkiye ve Avrupa'daki çocukların internet alışkanlıkları ve güvenli internet kullanımı. *Eğitim*

ve Bilim, 39(171), 230-243. file:///C:/Users/ab153269/Downloads/1867-26352-2-PB%20(1).pdf sayfasından erişilmiştir.

Kavuk, M. (2011). *İlköğretim öğrencilerinin sanal zorba ve sanal kurban olma durumlarının incelenmesi*. Yüksek Lisans Tezi, Ankara Üniversitesi Eğitim Bilimleri Enstitüsü, Ankara.

Kaya, A. & Kaya, B. (2014). Öğretmen adaylarının dijital vatandaşlık algısı. *International Journal of Human Science*, 11(2), 346-361. <https://www.j-humansciences.com/ojs/index.php/IJHS/article/view/2917/1337> sayfasından erişilmiştir.

Kilpatrick, J. (2014). Encyclopedia of Mathematics Education. S. Lerman. (eds) *Competency Frameworks in Mathematics Education* (s. 85-87). Dordrecht: Springer. https://doi.org/10.1007/978-94-007-4978-8_27

Kocadağ, T. (2012). *Öğretmen adaylarının dijital vatandaşlık düzeylerinin belirlenmesi*. Yüksek Lisans Tezi, Karadeniz Teknik Üniversitesi Eğitim Bilimleri Enstitüsü, Trabzon.

Kocaman Karoğlu, A., Bal Çetinkaya, K., & Çimşir, E. (2020). Toplum 5.0 sürecinde Türkiye’de eğitimde dijital dönüşüm. *Üniversite Araştırmaları Dergisi*, 3(3), 147-158. <https://dergipark.org.tr/en/pub/uad/issue/57871/815428> sayfasından erişilmiştir.

Kolata, F. (2022). *Okul Öncesi Öğretmen Adaylarının Dijital Vatandaşlık ile 21. Yüzyıl Becerileri Özyeterlilik Algılarının İncelenmesi*. Yüksek Lisans Tezi, Necmettin Erbakan Üniversitesi Eğitim Bilimleri Enstitüsü, Konya.

Korkmaz, M. & Kıran Esen, B. (2012). Güvenli internet kullanımı konusunda uygulanan akran eğitiminin ergenler üzerindeki etkisi. *Turkish Psychological Counseling and Guidance Journal*, 4(38), 180-187.

Korkmaz, Ö., Arıkaya, C., & Altıntaş, Y. (2019). Öğretmenlerin dijital öğretim materyali geliştirme öz-yeterlilik ölçeğinin geliştirilmesi çalışması. *Turkish Journal of Primary Education*, 4(2), 40-56. <https://dergipark.org.tr/tr/pub/tujped/issue/50537/609625> sayfasından erişilmiştir.

- Korkut, L. (2015). Siyasi kimlik olarak vatandaşlık: Türkiye’de ve dünya devletlerinde anayasal vatandaşlık tanımları. *İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi*, 1(2), 5-41. <https://dergipark.org.tr/tr/pub/imuhfd/issue/54304/736943> sayfasından erişilmiştir.
- Kozan, M., & Bulut Özek, M. (2019). BÖTE bölümü öğretmen adaylarının dijital okuryazarlık düzeyleri ve siber zorbalığa ilişkin duyarlılıklarının incelenmesi. *Fırat Üniversitesi Sosyal Bilimler Dergisi*, 29(1), 107-120. <https://doi.org/10.18069/firatsbed.538657>
- Krasna, M. & Bratina, T. (2011). *The perception of digital security among digital natives*. Proceedings of the 34th International Convention MIPRO.
- Krasna, M. ve Bratina, T. (2012). Designing digital security course in educational sciences. *Int. J. Knowledge Engineering and Soft Data Paradigms*, 3(4), 280-293. <https://doi.org/10.1504/IJKEBDP.2012.050723>
- Kuh Karyeli, G. & Dağhan, G. (2020). Sayısal ayak izi ders tasarımının öğrencilerin sayısal vatandaşlık konusundaki akademik başarılarına etkisi. *Erzincan Üniversitesi Eğitim Fakültesi Dergisi*, 22(1), 256-275. <https://doi.org/10.17556/erziefd.622919>
- Lenhart, A., Madden, M., Smith, A., Purcell, K., Zickuhr, K., & Rainie, L. (2011). *Teens, Kindness and Cruelty on Social Network Sites: How American Teens Navigate the New World of "Digital Citizenship"*. Pew Internet & American Life Project. <https://files.eric.ed.gov/fulltext/ED537516.pdf> sayfasından erişilmiştir.
- Le Deist, F.D. & Winterton, J. (2005). What Is Competence?. *Human Resource Development International*, 8(1), 27–46. <https://doi.org/10.1080/1367886042000338227>
- Livingstone, S., Ólafsson, K., Helsper, E. J., Lupiáñez-Villanueva, F., Veltri, G. A. & Folkvord, F. (2017). Maximizing opportunities and minimizing risks for children online: The role of digital skills in emerging strategies of parental mediation. *Journal of Communication*, 67(1), 82-105. <https://doi.org/10.1111/jcom.12277>
- Livingstone, S., Mascheroni, G., & Staksrud, E. (2018). European research on children’s internet use: Assessing the past and anticipating the future. *New media & society*, 20(3), 1103-1122. <https://doi.org/10.1177/14614448166859>

- Li, J., Sidibe, A. M., Shen, X., & Hesketh, T. (2019). Incidence, risk factors and psychosomatic symptoms for traditional bullying and cyberbullying in Chinese adolescents. *Children and Youth Services Review*, 107: 104511. <https://doi.org/10.1016/j.chidyouth.2019.104511>
- Lynch, R. & Dembo, M. (2004). The relationship between self-regulation and online learning in a blended learning context. *The International Review of Research in Open and Distributed Learning*, 5(2), 1-16. <https://doi.org/10.19173/irrodl.v5i2.189>
- Manotipya, P. & Ghazinour, K. (2020). Children's online privacy from parents' perspective. *Procedia Computer Science*, 177(2020), 178-185. <https://doi.org/10.1016/j.procs.2020.10.026>
- Macaulay, P. J. R., Boulton, M. J., Betts, L. R., Boulton, L., Camerone, E., Down, J., Hughes, J., Kirkbride, C., & Kirkham, R. (2020). Subjective versus objective knowledge of online safety/dangers as predictors of children's perceived online safety and attitudes towards e-safety education in the United Kingdom. *Journal of Children and Media*, 14(3), 376–395. <https://doi.org/10.1080/17482798.2019.1697716>
- McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and Information Security Awareness. *Computers in Human Behavior*, 69, 151–156. <https://doi.org/10.1016/j.chb.2016.11.065>
- Means, B., Toyama, Y., Murphy, R., Bakia, M., & Jones, K. (2009). Evaluation of evidence-based practices in online learning: A meta-analysis and review of online learning studies. U.S. Department of Education Office of Planning, Evaluation, and Policy Development, Policy and Program Studies Service. <http://www2.ed.gov/rschstat/eval/tech/evidence-based-practices/finalreport.pdf> sayfasından erişilmiştir.
- Miles, D. (2011). Youth Protection: Digital Citizenship– Principles & New Resources. Paper presented at the Cybersecurity Summit (WCS), 2011 Second Worldwide. <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5978778> sayfasından erişilmiştir.
- Milli Eğitim Bakanlığı [MEB] (2018). *Sosyal bilgiler dersi öğretim programı*. <http://mufredat.meb.gov.tr/Dosyalar/201812103847686->

SOSYAL%20B%C4%B0LG%C4%B0LER%20%C3%96%C4%9ERET%C4%B0M%20PROGRAMI%20.pdf sayfasından erişilmiştir.

Milli Eğitim Bakanlığı [MEB] (2021). Millî Eğitim Bakanlığı ders kitapları ve eğitim araçları yönetmeliği. <https://www.resmigazete.gov.tr/eskiler/2021/10/20211014-1.htm> sayfasından erişilmiştir.

Milli Eğitim Bakanlığı [MEB] (2022). 4. sınıf sosyal bilgiler ders kitabı. Tuna Matbaacılık, Ankara.
<https://drive.google.com/file/d/1LIUvV2A824Z4CWltspNfJgxcbBaNOV9p/view> sayfasından erişilmiştir.

Milli Eğitim Bakanlığı [MEB] (2022). 5. sınıf sosyal bilgiler ders kitabı. Milli Eğitim Bakanlığı Yayınları, Ankara. <https://drive.google.com/file/d/15JzPNtjPybyhPcd-9iUy6Oyt4qU-p2xQ/view> sayfasından erişilmiştir.

Milli Eğitim Bakanlığı [MEB] (2022). 6. sınıf sosyal bilgiler ders kitabı. Milli Eğitim Bakanlığı Yayınları, Ankara.
https://drive.google.com/file/d/11UD_PujqpSq9GWGk0yKlR-loB3t7yVN5/view sayfasından erişilmiştir.

Milli Eğitim Bakanlığı [MEB] (2022). 7. sınıf sosyal bilgiler ders kitabı. Milli Eğitim Bakanlığı Yayınları, Ankara.
https://drive.google.com/file/d/1gBJKGIZzbVA71stqFJnweHYWDSaJ_V6L/view sayfasından erişilmiştir.

Mordecai, M. (2021). *Balancing student data privacy and innovation: Practices and perceptions in hawai'i public schools*. Doktora Tezi, Hawai University, Hawai.

Moore, M. G. (1989). Editorial: Three types of interaction. *American Journal of Distance Education*, 3(2), pp. 1-7.

Mossberger, K., Tolbert, C. J., & Hamilton, A. (2012). Broadband adoption measuring digital citizenship: Mobile access and broadband. *International Journal of Communication*, 6, 37. <https://ijoc.org/index.php/ijoc/article/view/1777/808> sayfasından erişilmiştir.

- Mossberger, K., Tolbert, C., & S. McNeal, R. (2007). *Digital citizenship: The internet, society and participation*. London, England: The MIT Press.
- Muslu, G. K. & Bolışık, B. (2009). Çocuk ve Gençlerde İnternet Kullanımı. *TAF Preventive Medicine Bulletin*, 8(5), 445-450.
- Nannatt, A., Tariang, N. M., Gowda, M. & Devassy, S. M. (2022). Family factors associated with problematic use of the internet in children: a scoping review. *Indian Journal of Psychological Medicine*, 44(4), 341-348. <https://doi.org/10.1177/02537176221090862>
- Nawaila, M. B. , Kani, U. M. , & Kanbul, S. (2021). Digital children's right: human right perspective. In (Ed.), *Human Rights in the Contemporary World*. IntechOpen. <https://doi.org/10.5772/intechopen.97048>
- Onursoy, S. (2018). Üniversite gençliğinin dijital okuryazarlık düzeyleri: anadolu üniversitesi öğrencileri üzerine bir araştırma. *Gümüşhane Üniversitesi İletişim Fakültesi Elektronik Dergisi*, 6(2), 989-1013. <https://doi.org/10.19145/e-gifder.422671>
- Ong'ong'a, D. O. (2021). Teachers' perception, experiences, and challenges about teens of ages 12-14 years who have reported online digital insecurity in Kenya. *European Journal of Interactive Multimedia and Education*, 2(1), e02102. <https://doi.org/10.30935/ejimed/9360>
- Oliveira, E. W., Siqueira, S. W. M., & Braz, M. H. L. B. (2008). Structuring segments of e-learning multimedia objects with LOM and MPEG-7. In *Proceedings of the 11th IASTED International Conference on Computers and Advanced Technology in Education, Creta* (Vol. 1, ss. 353-358).
- Oxley, C. (2010September-October). *Digital citizenship: Developing an ethical and responsible online culture*. School Library Association of Queensland and the International Association of School Librarianship Conference incorporating the International Forum on Research in School Librarianship Konferansı'nda sunulmuş bildiri. Brisbane QLD Australia. <https://files.eric.ed.gov/fulltext/ED518512.pdf> sayfasından erişilmiştir.

- O'Reilly, T. (2005). *What is Web 2.0 – Design patterns and business models for the next generation of software*. O'Reilly Media, Inc.
- O'Reilly, M., Levine, D. ve Law, E. (2020). Applying a 'digital ethics of care' philosophy to understand adolescents' sense of responsibility on social media. *Pastoral Care in Education*, 39(2), 91-107. <https://doi.org/10.1080/02643944.2020.1774635>
- Öktelik, B. (2022). *Bilgi güvenliği farkındalığının geliştirilmesinde görev temelli çevrimiçi öğrenme ortamının etkililiği*. Yüksek Lisans Tezi, Çanakkale Onsekiz Mart Üniversitesi Eğitim Bilimleri Enstitüsü, Çanakkale.
- Özbek, Y. (2019). *Öğretmen adaylarının siber güvenlik farkındalıklarının incelenmesi*. Doktora Tezi, Necmettin Erbakan Üniversitesi Eğitim Bilimleri Enstitüsü, Konya.
- Özcan, N. (2021). Dijital etik üzerine nitel bir araştırma. *Gençlik Araştırmaları Dergisi*, 9 (25), 89-108. <https://doi.org/10.52528/genclikarastirmalari.1004342>
- Özcan, S. (2020). Açık ve uzaktan öğrenmede sorunlar ve çözüm önerileri. S. Karataş ve E. Kılıç Çakmak (Ed.) *Açık ve uzaktan öğrenme* (ss.195-212). Ankara: Pegem A.
- Öztürk, M. (2015). *Ortaokul öğrencilerinin dijital vatandaşlık düzeyleri*. Yüksek Lisans Tezi, Kastamonu Üniversitesi Sosyal Bilimler Enstitüsü, Kastamonu.
- Parker, W. C. (2003). *Teaching democracy: Unity and diversity in public life*. New York: Teachers College.
- Peker Ünal, D. (2017). Bir öğretim programındaki dijital vatandaşlık öğeleri ve ortaöğretim öğrencilerinin dijital vatandaşlık öğelerine sahip olma durumları. *Karaelmas Eğitim Bilimleri Dergisi*, 5, 180-195. <https://dergipark.org.tr/tr/pub/kebd/issue/67222/1049150> sayfasından erişilmiştir.
- Polat, E. G. (2011). Osmanlı'dan günümüze vatandaşlık anlayışı. *Ankara Barosu Dergisi*, 2011 (3), 127-158.
- Prensky, M. (2001). Digital natives, digital immigrants. *From On the Horizon*, MCB University, 9(5), 1-6. <https://www.marcprensky.com/writing/Prensky%20-%20Digital%20Natives,%20Digital%20Immigrants%20-%20Part1.pdf> sayfasından erişilmiştir.

- Quayyum,F., Cruzes, D. & Jaccheri, L. (2021). Cybersecurity awareness for children: A systematic literature review. *International Journal of Child-Computer Interaction*, 30(2), 100-343. <https://doi.org/10.1016/j.ijcci.2021.100343>
- Raskauskas, J., & Huynh, A. (2015). The process of coping with cyberbullying: A systematic review. *Aggression and Violent Behavior*, 23, 118-125. <https://doi.org/10.1016/j.avb.2015.05.019>
- Ribble, M. & Bailey, G. D. (2007). *Digital citizenship in schools, (1st Edition)*. WashingtonDC: The International Society for Technology in Education (ISTE).
- Ribble, M. (2011). *Digital citizenship in schools (2nd Edition)*. Washington DC: The International Society for Technology in Education.
- Ribble, M. (2012). Digital citizenship for education change. *Kappa Delta Pi Record*, 48(4), 148-151.
- Ribble, M., Bailey, G. D. & Ross, T. W. (2004). Digital citizenship: Addressing appropriate technology behavior. *Learning & Leading With Technology*, 32(1), 6-9.
- Robinson, L.K., Brown, A.H. & Green, T.D. (2010) Security vs. Access: Balancing safety and productivity in the digital school. Eugene, Oregon: International Society for Technology in Education.
- Sakallı, H. (2015). *Sınıf öğretmenleri adaylarının dijital vatandaşlık düzeyleri ile siber zorbalık eğilimleri arasındaki ilişkinin incelenmesi*. Yüksek Lisans Tezi, Adnan Menderes Üniversitesi Sosyal Bilimler Enstitüsü, Aydın.
- Sari, İ. (2019). *Sosyal bilgiler eğitiminde öğretmenlere uygulanan seminer ve öğrencilere yapılan etkinliklerin katkıları bakımından dijital vatandaşlık olgusu*. Doktora Tezi, Necmettin Erbakan Üniversitesi Eğitim Bilimleri Enstitüsü, Konya.
- Schneier, B. (2004). *Secret and lies: Digital security in a networked world*. Indianapolis, IN: Wiley Inc.
- Sebetci, Ö., Topal, A., Hanaylı, M.C. & Gürel Dönük, G. (2018). Dijital ortamda kişisel veri güvenliği ve sosyal medya reklamcılığı üzerine bir değerlendirme. *Kesit Akademi Dergisi (The Journal of Kesit Academy)*, 4(16), 389-409.

- Smith, P. K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S., & Tippett, N. (2008). Cyberbullying: Its nature and impact in secondary school pupils. *Journal of Child Psychology and Psychiatry*, 49(4), 376-385. <https://doi.org/10.1111/j.1469-7610.2007.01846.x>
- Smith, R. M. (2002). Modern citizenship. In E. F. Isin & B. S. Turner (Eds.), *Handbook of citizenship studies* (pp.105-115). London: Sage.
- Snyder, S.E. (2016). *Teachers' perceptions of digital citizenship development in middle school students using social media and global collaborative projects*, Doctoral Dissertation, Walden University, Minneapolis.
- Som Vural, S. (2016). *Üniversitesi öğrencilerinin bakış açısıyla dijital vatandaşlık göstergelerinin incelenmesi*. Doktora Tezi, Anadolu Üniversitesi Eğitim Bilimleri Enstitüsü, Eskişehir.
- Sönmez, Ö. F., Kaymakçı, S., & Merey, Z. (2010). 1998 ve 2006 sosyal bilgiler lisans programlarına göre sosyal bilgiler öğretmen adaylarının vatandaşlık bilgisi öğretiminde kullanılan bazı kavramları anlama düzeyi. *Sosyal Bilimler Araştırmaları Dergisi*, 5(1), 126-138. <https://dergipark.org.tr/en/download/article-file/802086> sayfasından erişilmiştir.
- Statista (2022). Number of internet and social media users worldwide as of July 2022. <https://www.statista.com/statistics/617136/digital-population-worldwide/> sayfasından erişilmiştir.
- Stanton, J. M., & Stam, K. R. (2006). *The visible employee: using workplace monitoring and surveillance to protect information assets--without compromising employee privacy or trust*. Information Today, Inc. (e-book)
- Stoilova, M., Livingstone, S. ve Khazbak, R. (2021). Investigating risks and opportunities for children in a digital world: A rapid review of the evidence on children's internet use and outcomes. *Innocenti Discussion Papers*, 2020(03), UNICEF Office of Research - Innocenti, Florence.

- Süral, İ. (2012). *Çevrimiçi öğrenmede kişiselleştirmenin öğrenci performansı ve memnuniyet düzeyi ile ilişkisi*. Doktora Tezi, Anadolu Üniversitesi Sosyal Bilimler Enstitüsü, Eskişehir.
- Şahinaslan, E., Kandemir, R., & Şahinaslan, Ö. (2009). Bilgi güvenliği farkındalık eğitimi örneği. *Akademik Bilişim*, 9, 189-194. https://ab.org.tr/ab09/kitap/sahinaslan_kandemir_AB09.pdf sayfasından erişilmiştir.
- Tahiroğlu, A. Y., Çelik, G. G., Fettahoğlu, Ç., Yıldırım, V., Toros, F. & Avcı, A. (2010). Psikiyatrik bozukluğu olan ve olmayan ergenlerde problemlerli internet kullanımı. *Nöropsikiyatri Arşivi*, 4(7), 241-246.
- Talan, T., & Aktürk, C. (2021). Orta öğretim öğrencilerinin dijital okuryazarlık ve bilgi güvenliği farkındalığı seviyelerinin incelenmesi. *Kahramanmaraş Sütçü İmam Üniversitesi Sosyal Bilimler Dergisi*, 18(1), 158-180. <https://doi.org/10.33437/ksusbd.668255>
- Tatlı, A. (2018). *Öğretmenlerin dijital vatandaşlık düzeylerinin bilgi okuryazarlığı ile internet ve bilgisayar kullanım özyeterlilikleri bağlamında değerlendirilmesi*. Doktora Tezi, Necmettin Erbakan Üniversitesi Eğitim Bilimleri Enstitüsü, Konya.
- Tavşancıl, E. (2010). *Measurement of attitudes and data analysis with SPSS (Fourth Edition)*. Nobel, Ankara.
- Tekerek, M. ve Tekerek, A. (2013). Öğrencilerin bilgi güvenliği farkındalıkları üzerine bir araştırma. *Çevrimiçi Başvuru*, 2(3), 61-70. <https://files.eric.ed.gov/fulltext/ED593953.pdf> sayfasından erişilmiştir.
- Tekinarslan, R. (2022). *Çevrimiçi öğrenme ortamlarında öğrenme analitiği verileri ve makine öğrenmesi kullanarak akademik başarının değerlendirilmesi*. Yüksek Lisans Tezi, Başkent Üniversitesi Fen Bilimleri Enstitüsü, Ankara.
- Temel, T. (2022). *Exploring the effects of gamification with web 2.0 tools on efl learners' academic achievement, motivation, and learning self-efficacy in online learning environments*. Doktora Tezi, Çanakkale Onsekiz Mart Üniversitesi Lisansüstü Eğitim Enstitüsü, Çanakkale.

- Thaichon, P. (2017). Consumer socialization process: The role of age in children's online shopping behavior. *Journal of Retailing and Consumer Services*, 34, 38-47.
- The Online Safety and Technical Working Group [OSTWG] (2010). *Youth safety on a living internet: Report of the online safety and technology working group*. https://www.ntia.doc.gov/files/ntia/publications/ostwg_final_report_070610.pdf sayfasından erişilmiştir.
- Toker, T., Akgün, E., Cömert, Z. & Edip, S. (2021). Eğitimciler için dijital yeterlik ölçeği: uyarlama, geçerlik ve güvenirlik çalışması. *Milli Eğitim Dergisi*, 50 (230), 301-328. <https://doi.org/10.37669/milliegitim.801607>
- Topal, M. & Akgün, Ö. (2015). Eğitim fakültesi son sınıf öğrencileri için hazırlanan eğitim amaçlı internet kullanımı öz-yeterliliğini geliştirme programının etkililiği. *İlköğretim Online*, 14 (2) , 697-712. <https://doi.org/10.17051/io.2015.43304>
- Töre, N. (2017). Değişen dünyada vatandaşlık. *Uyuşmazlık Mahkemesi Dergisi*, 5(10), 553-595. <https://dergipark.org.tr/tr/download/article-file/394401> sayfasından erişilmiştir.
- Turan, S. & Karasu Avcı, E. (2018). 2018 sosyal bilgiler öğretim programının dijital vatandaşlık bağlamında incelenmesi. *Eğitim ve Yeni Yaklaşımlar Dergisi*, 1(1), 28-38. <https://dergipark.org.tr/tr/pub/jena/issue/42984/519671> sayfasından erişilmiştir.
- Türk Dil Kurumu [TDK] (2022). <https://sozluk.gov.tr/> sayfasından erişilmiştir.
- Türkiye İstatistik Kurumu [TÜİK] (2021). Çocuklarda bilişim teknolojileri kullanım araştırması. <https://data.tuik.gov.tr/Bulten/Index?p=Cocuklarda-Bilisim-Teknolojileri-Kullanim-Arastirmasi-2021-41132> sayfasından erişilmiştir.
- Türkiye İstatistik Kurumu [TÜİK] (2022). Hanehalkı Bilişim Teknolojileri (BT) Kullanım Araştırması, 2022. [https://data.tuik.gov.tr/Bulten/Index?p=Hanehalki-Bilisim-Teknolojileri-\(BT\)-Kullanim-Arastirmasi-2022-45587](https://data.tuik.gov.tr/Bulten/Index?p=Hanehalki-Bilisim-Teknolojileri-(BT)-Kullanim-Arastirmasi-2022-45587) sayfasından erişilmiştir.
- Tyger, R. L. (2011). Teacher candidates' digital literacy and their technology integration efficacy. Doktora Tezi, Georgia Southern University. <https://digitalcommons.georgiasouthern.edu/cgi/viewcontent.cgi?article=1557&context=etd> sayfasından erişilmiştir.

- Uğurlu, C.T. (2011). Avrupa Birliği ülkeleri ve Türkiye’de vatandaşlık eğitimi. *Elektronik Sosyal Bilimler Dergisi*, 10(37), 153-169. www.esosder.org sayfasından erişilmiştir.
- Üstündağ, M.T. (2012). *Çevrimiçi öğrenme ortamlarında uyarlanmış sosyal etkileşim araçlarının öğrencilerin akademik başarılarına ve sosyal bulunuşluk algılarına etkisi*. Doktora Tezi, Gazi Üniversitesi Eğitim Bilimleri Enstitüsü, Ankara.
- Üstündağ, M. T. , Akcan, F. , Ceran, O. & Çakmak, M. A. (2022). Development of the digital security self-efficacy inventory. *Türk Akademik Yayınlar Dergisi (TAY Journal)* , 6 (2) , 175-206. <https://dergipark.org.tr/tr/download/article-file/2708347> sayfasından erişilmiştir.
- Vural, Y., & Sağıroğlu, Ş. (2008). Kurumsal bilgi güvenliğinde güvenlik testleri ve öneriler. *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi*, 26(1), <https://dergipark.org.tr/en/download/article-file/75726> sayfasından erişilmiştir.
- Walsh, K., Pink, E., Ayling, N., Sondergeld, A., Dallaston, E., Tournas, P., Serry, E., Trotter, S., Spanos, T. & Rogic, N. (2022) Best practice framework for online safety education: results from a rapid review of the international literature, expert review, and stakeholder consultation. *International Journal of Child-Computer Interaction*, 33, 100-474. <https://doi.org/10.1016/j.ijcci.2022.100474>
- We Are Social & Hootsuite (2021a). Digital 2021 Turkey: All the data, trends and insights you need to help you understand how people uses the internet, mobile, social media and ecommerce. <https://www.webolizma.com/blog/hootsuite-ve-we-are-social-2021-dijital-turkiye-raporu> sayfasından erişilmiştir.
- We Are Social & Hootsuite (2022a). Digital 2022: Global overview report. The essential guide to the world’s connected behaviours. <https://wearesocial.com/us/blog/2022/01/digital-2022/> sayfasından erişilmiştir.
- We Are Social & Hootsuite (2022b). Digital 2022 Turkey: The essential guide to the latest connected behaviours. <https://www.guvenliweb.org.tr/dokuman-detay/we-are-social-subat-2022-turkiye-raporu> sayfasından erişilmiştir.

- Vally, Z., Laconi, S. & Kaliszewska-Czeremska, K. (2020). Problematic internet use, psychopathology, defense mechanisms, and coping strategies: A cross-sectional study from the United Arab Emirates. *Psychiatric Quarterly*, 91(2), 587-602.
- Valcke, M., Bonte, S., De Wever, B., & Rots, I. (2010). Internet parenting styles and the impact on Internet use of primary school children. *Computers & Education*, 55(2), 454- 464.
- Vuorikari, R., Punie, Y., Gomez, S. C., & Van Den Brande, G. (2016). DigComp 2.0: The digital competence framework for citizens. Update Phase 1: The Conceptual Reference Model (No. JRC101254). Joint Research Centre (Seville site).
- Yalçinkaya, B. ve Cıbaroğlu, M.O. (2019). Dijital vatandaşlık algısının incelenmesi: Ampirik bir değerlendirme. *Business & Management Studies: An International Journal*, 7(4), 1188-1208.
- Yanç, C. (2022). *Investigating high school efl learners' self-efficacy beliefs in the online learning environment*. Yüksek Lisans Tezi, Çağ Üniversitesi Sosyal Bilimler Enstitüsü, Mersin.
- Yavanoğlu, U., Sağıroğlu, Ş. & Çolak, İ. (2012). Sosyal ağlarda bilgi güvenliği tehditleri ve alınması gereken önlemler. *Politeknik Dergisi*, 15(1), 15-27.
- Yılmaz, E., Şahin, Y. L. & Akbulut, Y. (2016). Öğretmenlerin dijital veri güvenliği farkındalığı. *Sakarya University Journal of Education*, 6(2), 26-45.



EK 1. Dijital Güvenlik Öz Yeterlik Envanteri

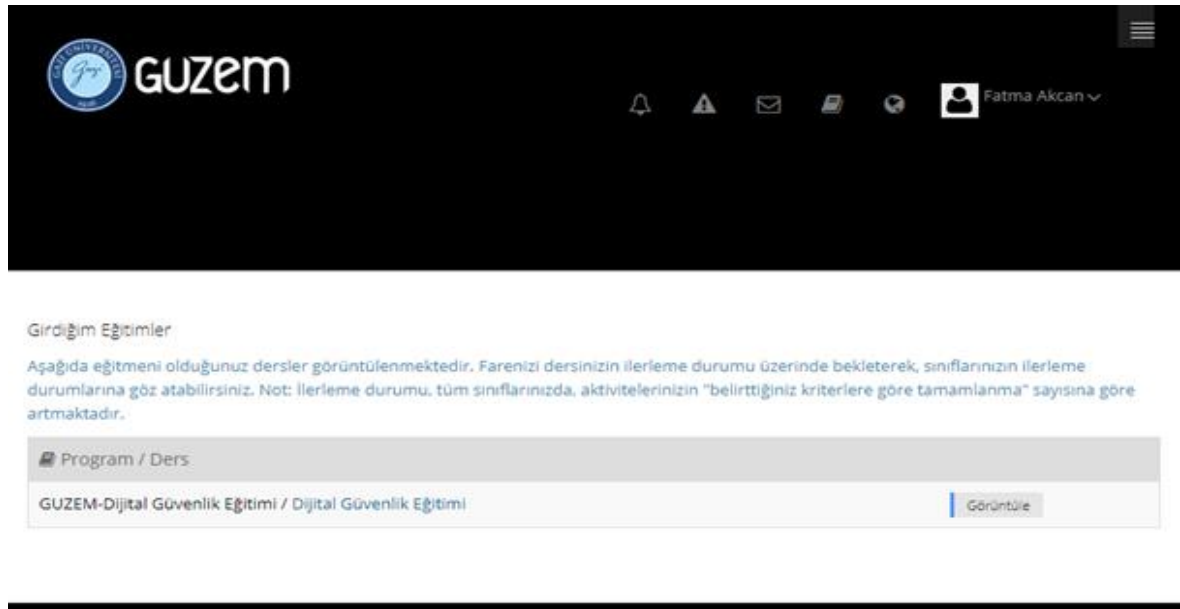
DİJİTAL GÜVENLİK ÖZ YETERLİK ENVANTERİ	Hiç Katılmıyorum	Katılmıyorum	Biraz Katılıyorum	Katılıyorum	Tamamen
Teknik Alt Ölçeği					
1.Şifre sıfırlamada kullanılan güvenlik sorularına başkalarının tahmin edemeyeceği cevaplar oluşturabilirim.	1	2	3	4	5
2.Güçlü şifre oluşturabilirim.	1	2	3	4	5
3.Dijital cihazlarda (akıllı telefon, tablet, bilgisayar vb.) güvenlik yazılımları (antivirüs yazılımı vb.) kullanabilirim.	1	2	3	4	5
4.Şifre güvenliği için “iki faktörlü kimlik doğrulama” yöntemini kullanabilirim.	1	2	3	4	5
5.Dijital cihazlarımda (akıllı telefon, tablet, bilgisayar vb.) lisanslı yazılım kullanabilirim.	1	2	3	4	5
6.Dijital ortamda önemli dosyaları yedekleyebilirim.	1	2	3	4	5
7.Dijital cihazları (akıllı telefon, tablet, bilgisayar vb.) kullanırken güvenlik bildirimlerine uygun davranabilirim.	1	2	3	4	5
8.İstenmeyen e-postaları “istenmeyen posta” olarak işaretleyebilirim.	1	2	3	4	5
9.İnternet tarayıcısının (Google Chrome, Firefox vb.) güvenlik ayarlarını düzenleyebilirim.	1	2	3	4	5
10.Dosya indirmeden önce güvenlik kontrollerini yapabilirim.	1	2	3	4	5
11.Halka açık bilgisayarları kullandıktan sonra cihazda kalan bilgilerimi temizleyebilirim.	1	2	3	4	5
12.Güvenli internet hizmetlerini seçebilirim.	1	2	3	4	5
13.Şüpheli görünen bağlantıları açmaktan kaçınabilirim.	1	2	3	4	5

14.İnternette bilgi edineceğim kaynağın güvenilirliğini kontrol edebilirim.	1	2	3	4	5
15.İnternette ulaştığım bilgilerin doğruluğunu kontrol edebilirim.	1	2	3	4	5
Psikososyal Alt Ölçeği					
1.Sosyal medyada yabancıların arkadaşlık isteklerini kabul etmemeyi tercih edebilirim.	1	2	3	4	5
2.Dijital ortamda kişisel bilgilerimi (TC No, doğum tarihi, telefon no, konum vb.) paylaşmaktan kaçınabilirim.	1	2	3	4	5
3.Dijital ortamda tehdit ve şantaja maruz kaldığımda durumu güvenilir bir yetişkin ile paylaşabilirim.	1	2	3	4	5
4.Dijital ortamda zorbalığa maruz kaldığımda saldırgana itiraz edebilirim.	1	2	3	4	5
5.Sosyal medya sitelerine üye olmadan önce gizlilik-güvenlik politikasını inceleyebilirim.	1	2	3	4	5
6.Kötü niyetli olduğuna emin olduğum kişileri engelleyebilirim.	1	2	3	4	5
7.İnternette tanışılan kişilerin sahte olma ihtimaline karşı temkinli(ölçülü) olabilirim.	1	2	3	4	5
8.İnternette kişilerin kötü niyetli olma ihtimaline karşı temkinli(ölçülü) olabilirim.	1	2	3	4	5
Çevrim içi Alışveriş Alt Ölçeği					
1.Ailemle birlikte yaptığım internet alışverişlerinde kredi kartı bilgilerinin kaydedilmemesini önerebilirim.	1	2	3	4	5
2.Ailemle birlikte yaptığım internet alışverişlerinde kullanıcı yorum ve şikayetlerini kontrol edebilirim.	1	2	3	4	5
3.Ailemle birlikte yaptığım internet alışverişlerinde güvenli ödeme yöntemlerini önerebilirim.	1	2	3	4	5
4.Ailemle birlikte yaptığım internet alışverişi sırasında tercih edeceğimiz sitenin güvenilirliğini kontrol edebilirim.	1	2	3	4	5
5.Ailemle birlikte yaptığım internet alışverişlerinde “bilgilendirme metninin” dikkatlice okunmasını önerebilirim.	1	2	3	4	5
Hak ve Sorumluluk Alt Ölçeği					
1.Dijital ortamda kişilerin haklarına saygılı davranabilirim.	1	2	3	4	5

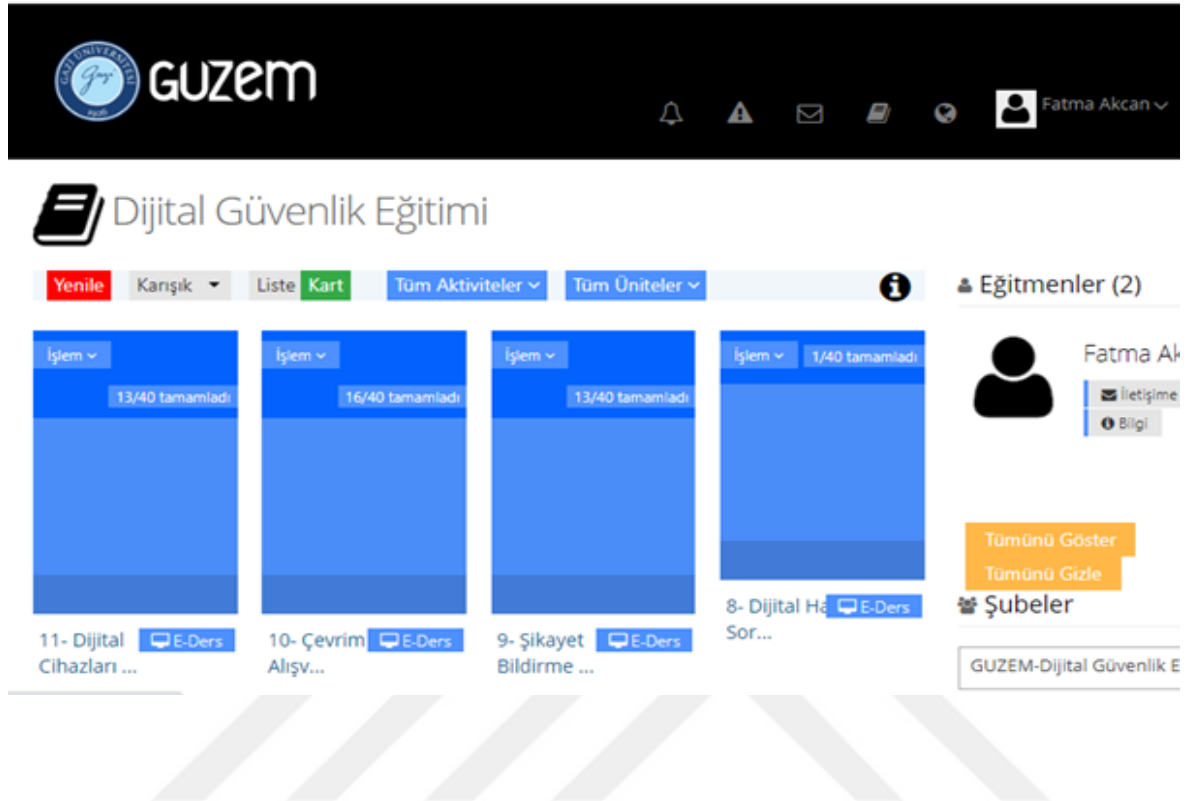
2.Dijital ortamda kişilik haklarını ihlal eden durumları şikayet edebilirim.	1	2	3	4	5
3.Dijital ortamda zararlı içerik ve paylaşımları şikayet edebilirim.	1	2	3	4	5
4.Dijital ortamda değer kavramlarına (din, vatan, bayrak, aile, ırk vs.) saygılı davranabilirim.	1	2	3	4	5
5.Dijital ortamda başkalarına ait belgeleri (video, fotoğraf, ses vb.) izinsiz kullanmaktan kaçınabilirim.	1	2	3	4	5
6.Dijital ortamda başkalarına ait belgeler (video, fotoğraf, ses vb.) üzerinde değişiklikler yapmaktan kaçınabilirim.	1	2	3	4	5
7.Araştırmalarımda internetten yararlandığım kaynakları kaynakçada belirtebilirim.	1	2	3	4	5
Sağlık Alt Ölçeği					
1.Eğlence amaçlı internet kullanımlarında (sosyal medya, dijital oyun, video vb.) aşırı zaman harcamaktan kaçınabilirim.	1	2	3	4	5
2.Dijital cihazları (akıllı telefon, tablet, bilgisayar vb.) kullanırken oturuş biçimi ve izleme mesafesini sağlığa uygun şekilde ayarlayabilirim.	1	2	3	4	5
3.Dijital cihazlarımı kullanırken ses, ışık ve ekran parlaklığını sağlığa uygun ayarlayabilirim.	1	2	3	4	5
4.Zararlı içeriklerden (nefret, şiddet, cinsel içerikli video, film, oyun, fotoğraf vb.) uzak durabilirim.	1	2	3	4	5
5.Akıllı işaretlere (olumsuz öğeler içerir, +13 vb.) göre içerik tercihi yapabilirim.	1	2	3	4	5

EK 2. Deney Grubuna Uygulanan Çevrim İçi Destekleyici Öğrenme Aracına Ait Ekran Görüntüleri

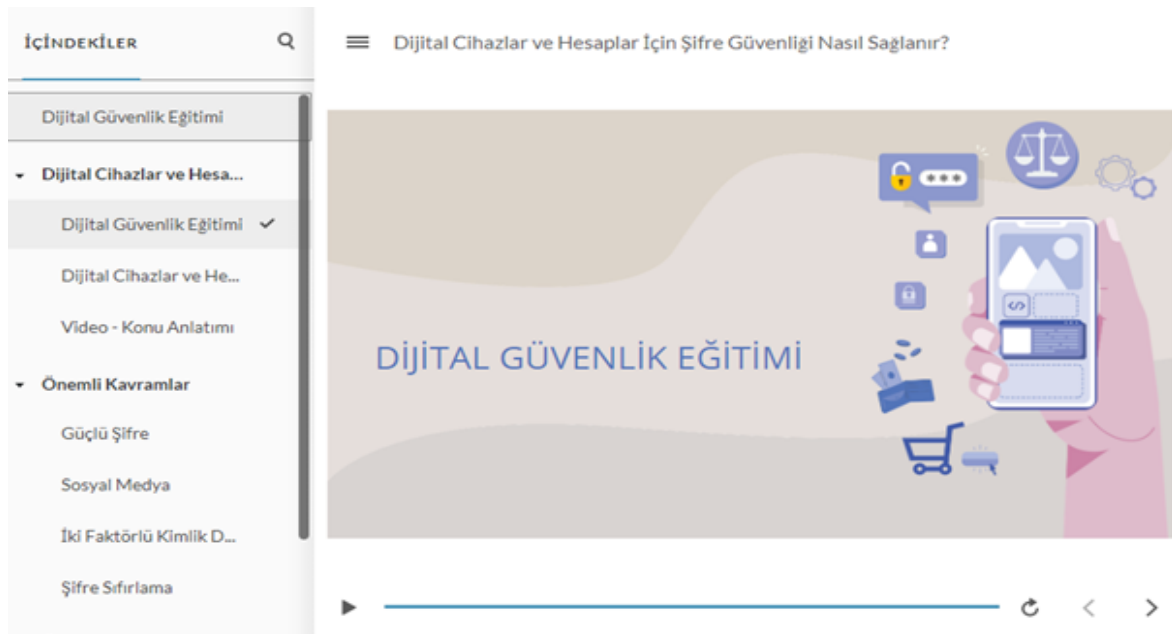
Ekran 1: Çevrim İçi Destekleyici Öğrenme Aracının Giriş Kısmını Gösteren Ekran



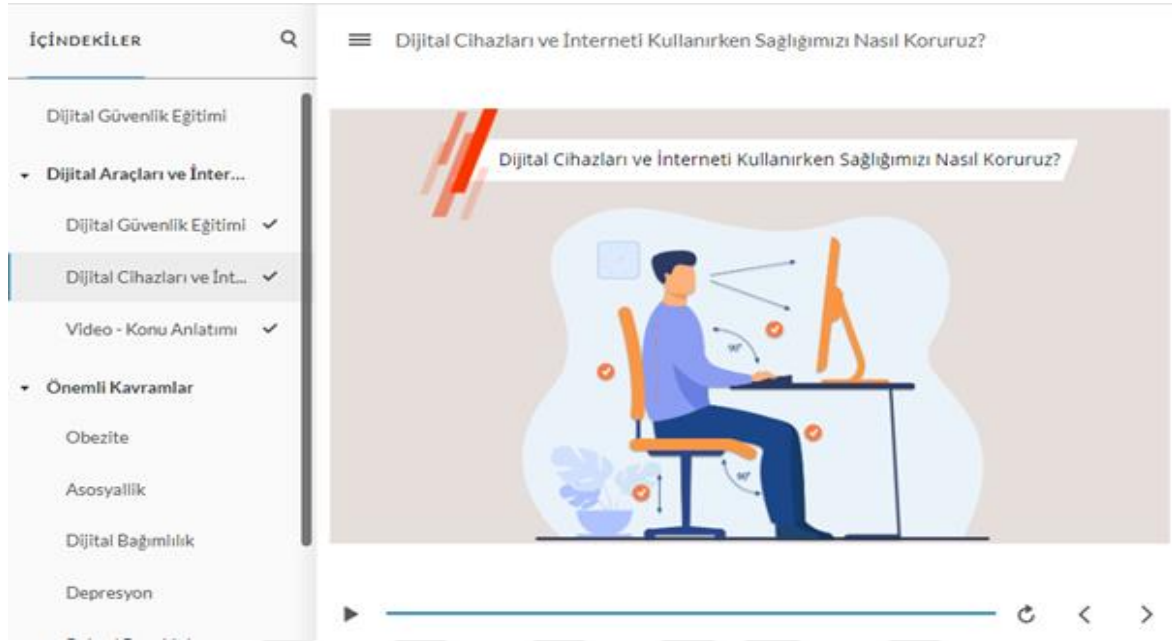
Ekran 2: Çevrim İçi Destekleyici Öğrenme Aracının Profile Giriş Kısımını Gösteren Ekran



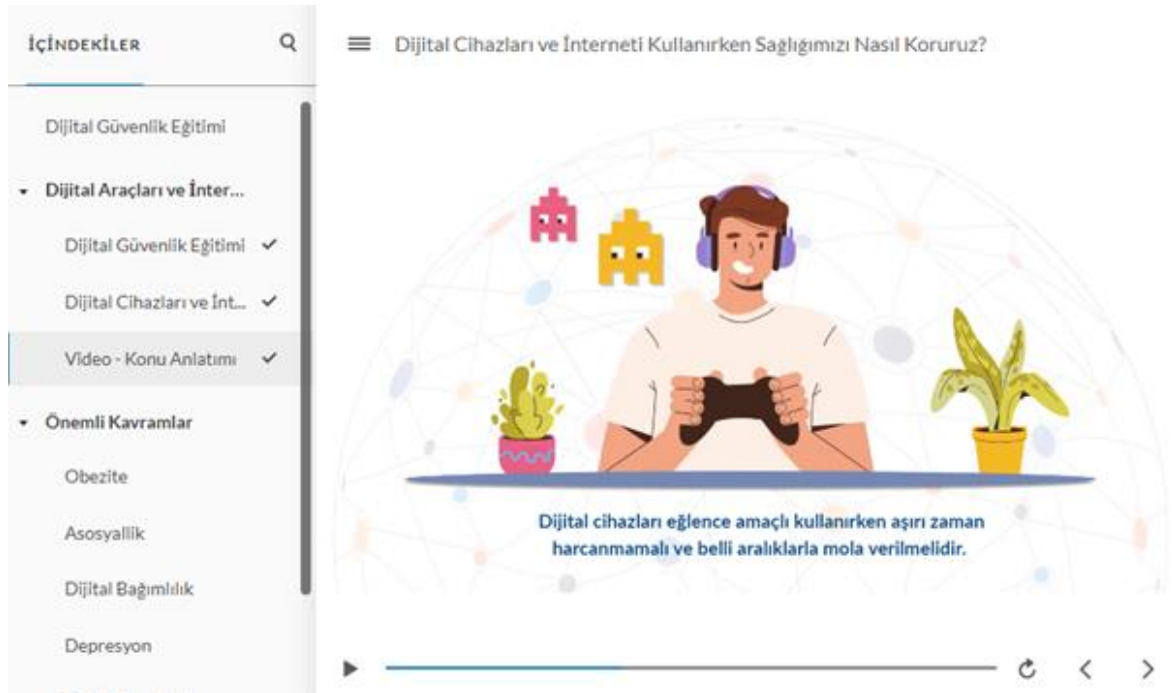
Ekran 3: Çevrim İçi Destekleyici Öğrenme Aracının SCORM Paketine Girişte Başlık Sayfasını Gösteren Bir Ekran



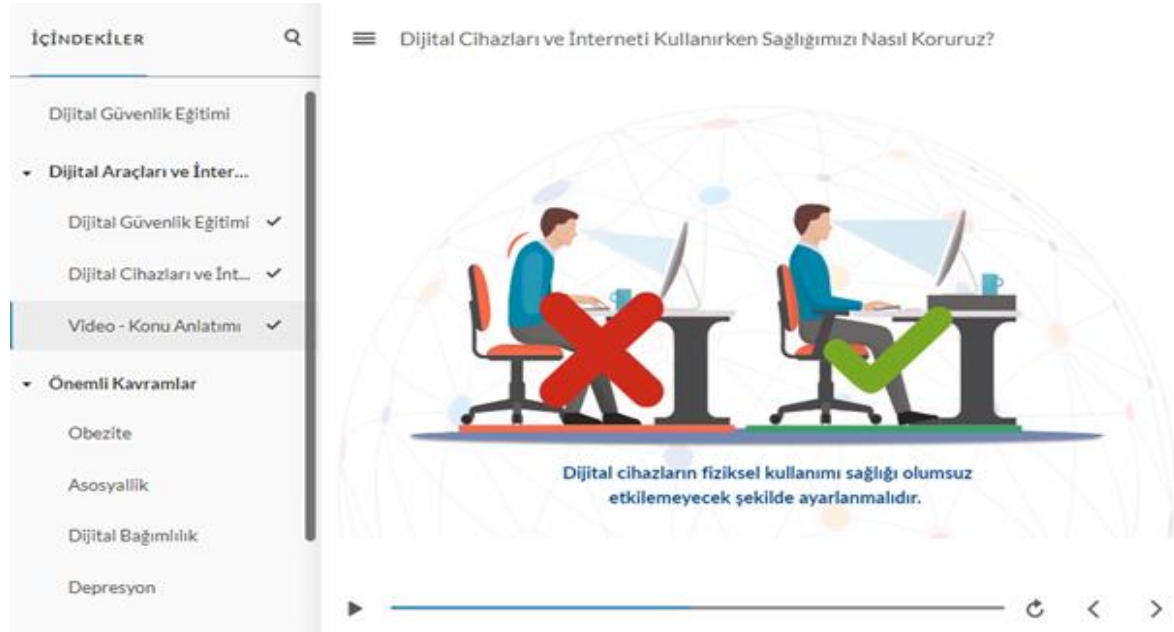
Ekran 4: Çevrim İçi Destekleyici Öğrenme Aracının SCORM Paketine Girişte Konu Başlığı Kısmını Gösteren Bir Ekran



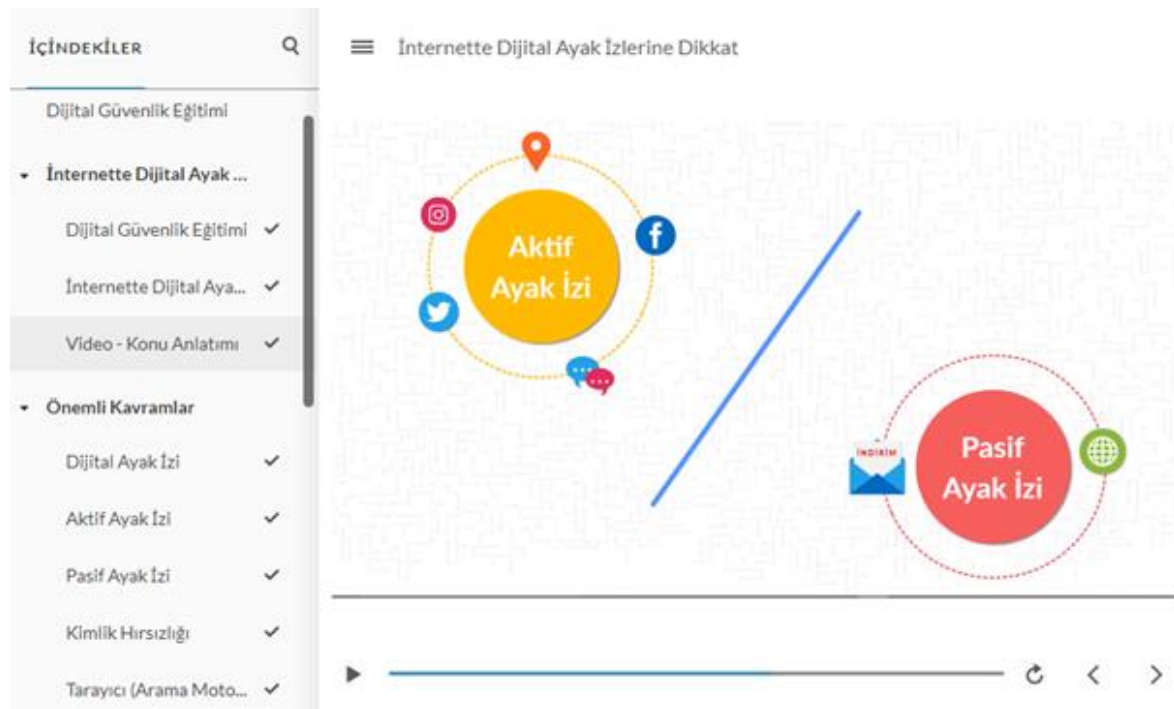
Ekran 5: Çevrim İçi Destekleyici Öğrenme Aracının SCORM Paketine Girişte Animasyon Video Bölümünü Gösteren Bir Ekran



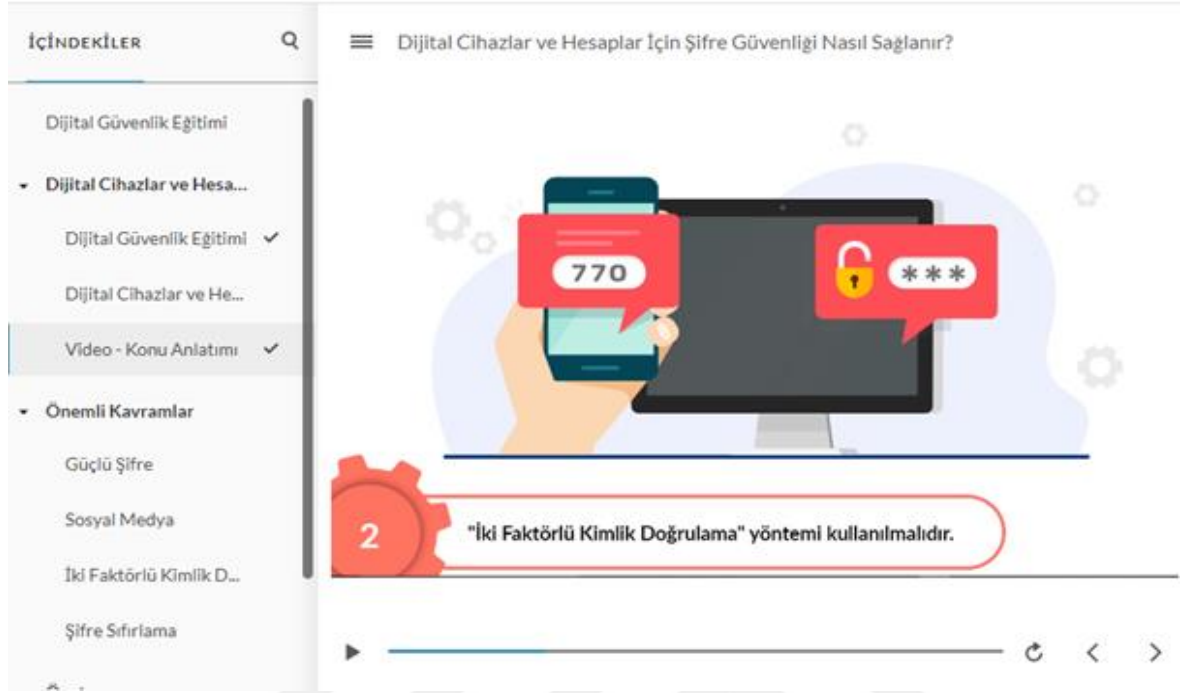
Ekran 6: Çevrim İçi Destekleyici Öğrenme Aracının SCORM Paketine Girişte Animasyon Video Bölümünü Gösteren Bir Ekran



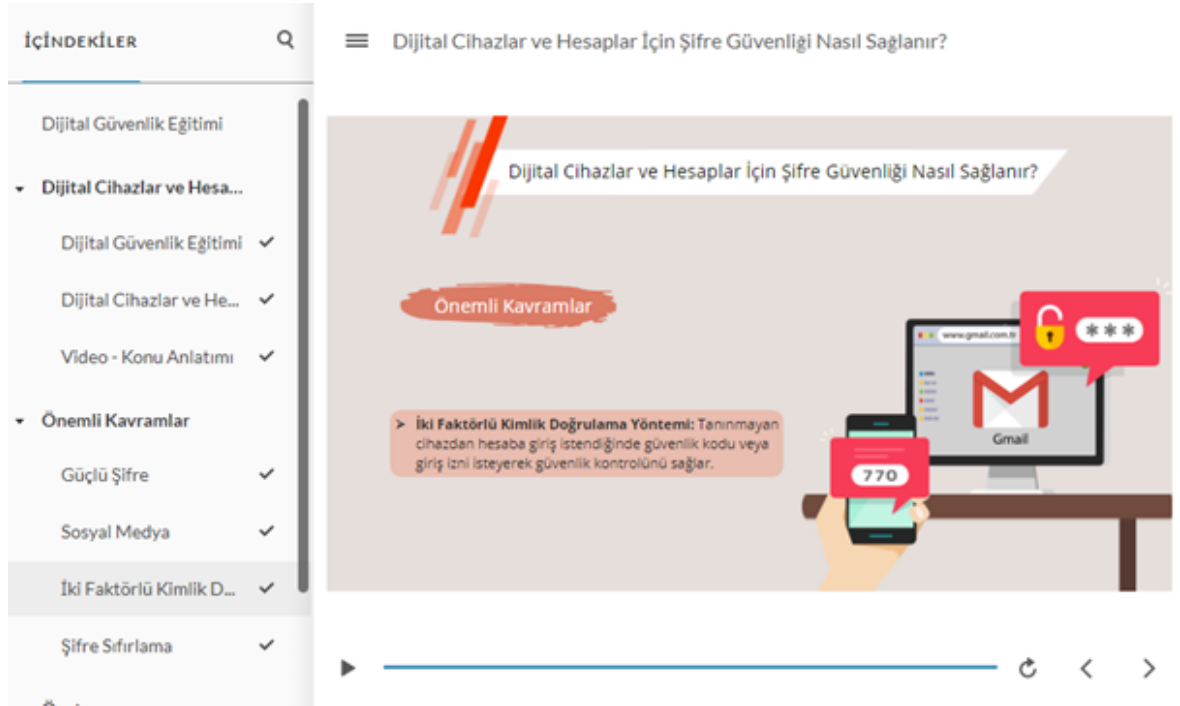
Ekran 7: Çevrim İçi Destekleyici Öğrenme Aracının SCORM Paketine Girişte Animasyon Video Bölümünü Gösteren Bir Ekran



Ekran 8: Çevrim İçi Destekleyici Öğrenme Aracının SCORM Paketine Girişte Animasyon Video Bölümünü Gösteren Bir Ekran



Ekran 9: Çevrim İçi Destekleyici Öğrenme Aracının SCORM Paketine Girişte Önemli Kavramlar Bölümünü Gösteren Bir Ekran



Ekran 10: Çevrim İçi Destekleyici Öğrenme Aracının SCORM Paketine Girişte Özet Bölümünü Gösteren Bir Ekran

İÇİNDEKİLER

Dijital Cihazlar ve Hesaplar İçin Şifre Güvenliği Nasıl Sağlanır?

Özet

Şifre Güvenliğini Sağl... ✓

Şifre Güvenliğini Sağl... ✓

Şifre Güvenliğini Sağl... ✓

Şifre Güvenliğini Sağl... ✓

Şifre Güvenliğini Sağl... ✓

Şifre Güvenliğini Sağl... ✓

Şifre Güvenliğini Sağl... ✓

Güçlü Şifre Oluşturm... ✓

Dijital Cihazlar ve Hesaplar İçin Şifre Güvenliği Nasıl Sağlanır?

Özet: Güçlü Şifre Oluşturma Kuralları

1. Şifre ad, soyad, doğum tarihi, plaka kodu gibi özel bilgilerinizi içermemelidir.
2. Yaygın kelime öbeği kullanılmamalı.
3. Farklı türde karakterler (x,y,1,5,!,?,*,&) kullanılmalıdır.
4. Şifre en az 8 karakterli olmalıdır.

Yaygın kelime öbekleri... ✗

Y, /, z, +, 2, !, 9, * ✓

ad, soyad, doğum tarihi, plaka kodu ✗

en az 8 karakterli şifre ✓

Ekran 11: Çevrim İçi Destekleyici Öğrenme Aracının SCORM Paketinde Teste Giriş Bölümünü Gösteren Bir Ekran

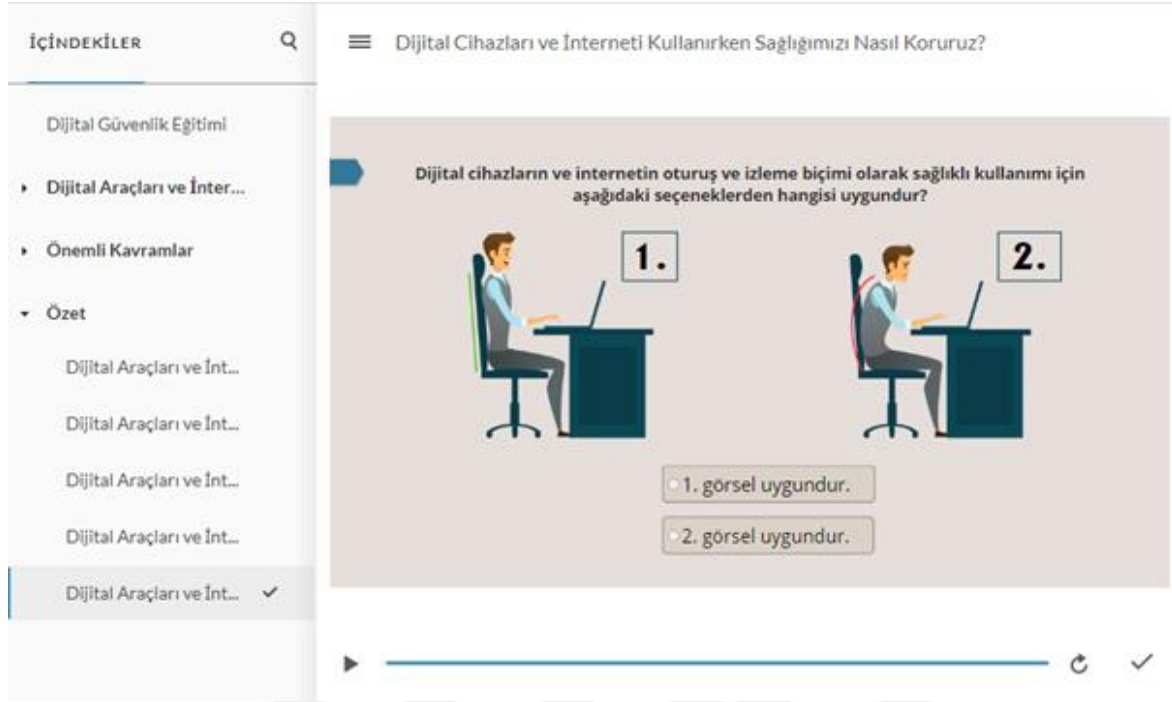
Dijital Cihazları ve İnterneti Kullanırken Sağlığımızı Nasıl Koruruz?

Teste Hazır Mısınız?

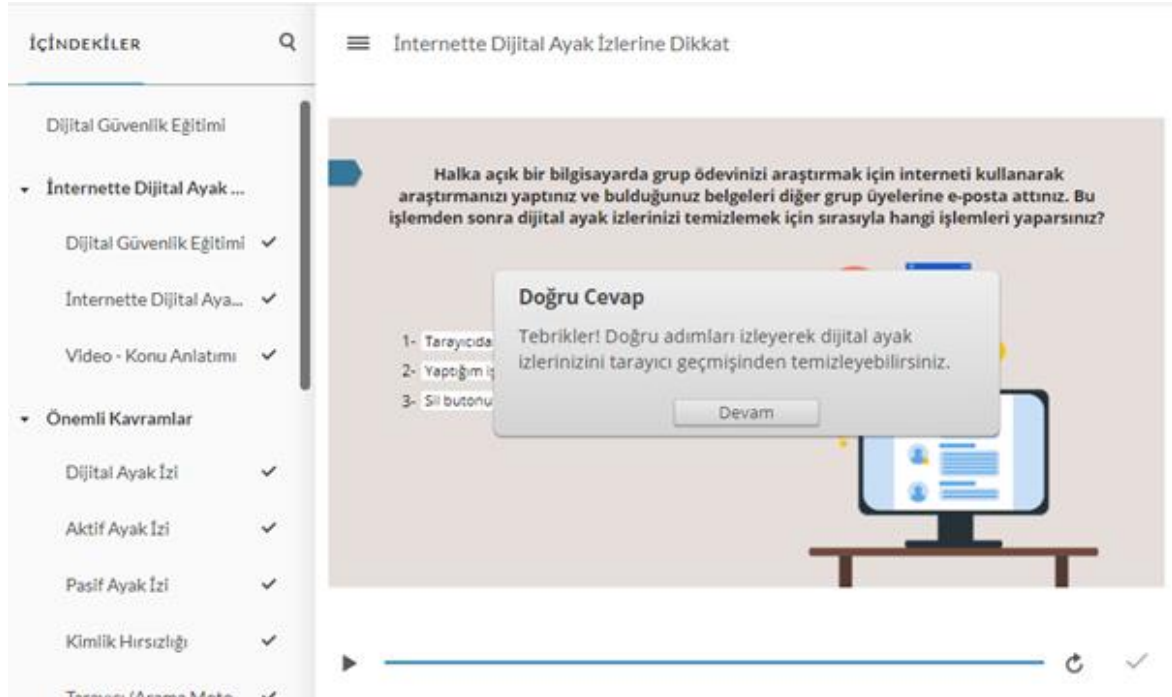
Dijital cihazları ve interneti sağlıklı kullanım yöntemleri ile ilgili test sorularını görmek için butona tıklayın.

Teste Başla

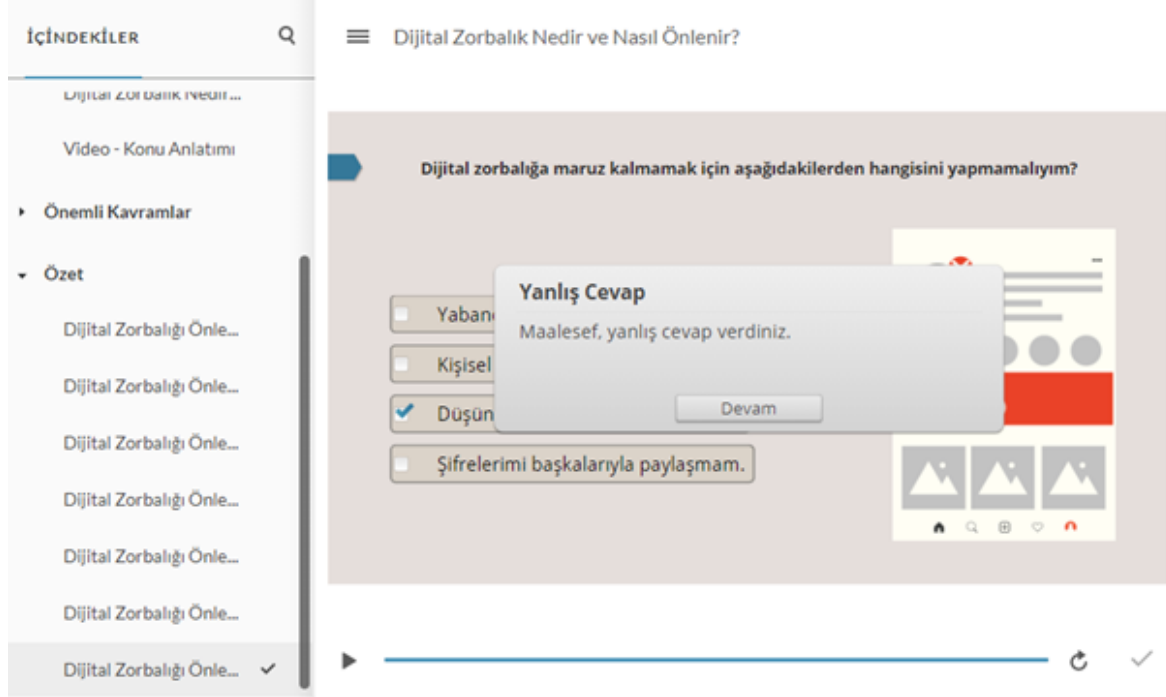
Ekran 12: Çevrim İçi Destekleyici Öğrenme Aracının SCORM Paketinde Test Bölümünü Gösteren Bir Ekran



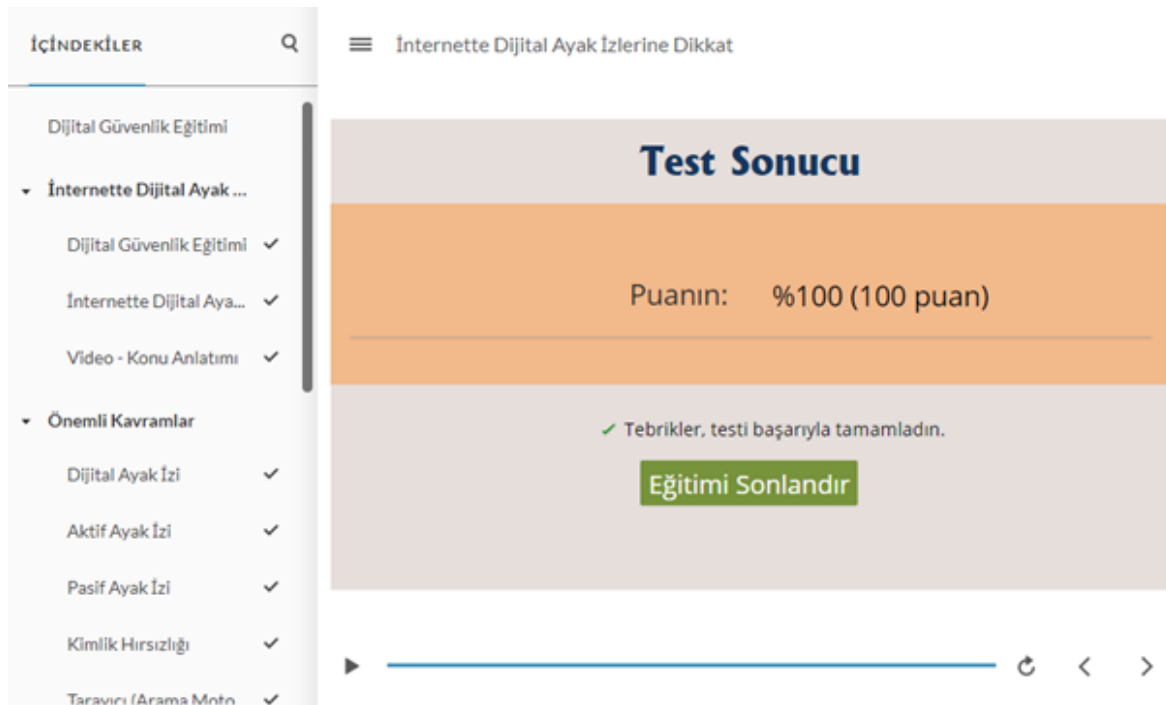
Ekran 13: Çevrim İçi Destekleyici Öğrenme Aracının SCORM Paketinde Test Geri Dönütünden (Doğru Cevap) Örnek Bir Ekran



Ekran 14: Çevrim İçi Destekleyici Öğrenme Aracının SCORM Paketinde Test Geri Dönütünden (Yanlış Cevap) Örnek Bir Ekran



Ekran 15: Çevrim İçi Destekleyici Öğrenme Aracının SCORM Paketinde Test Bölüm Sonu Puan Ekranını Gösteren Örnek Bir Ekran



EK 3. Kontrol Grubuna Uygulanan “Dijital Güvenlik Eğitimi” Ders Planı

EĞİTİM 1

Ders: Sosyal bilgiler

Sınıf: 7/A

Ders Saati: 40 + 40

Konu: Dijital cihazlar ve hesaplar için şifre güvenliği nasıl sağlanır?

SBDÖP’nda yer alan ilişkili kazanımlar:

SB.5.4.3. Sanal ortamı kullanırken güvenlik kurallarına uyar.

Beceriler: Dijital okuryazarlık, eleştirel düşünme, karar verme

Değerler: Sorumluluk

Önemli kavramlar

- Güçlü şifre: Başkaları tarafından tahmin edilmesi zor ve deneme yanılma yoluyla bulunması kolay olmayan şifrelerdir.
- Şifre güvenliği: Şifrenin çalınması ve kırılmasını zorlaştıran teknik önlemler bütünüdür.
- Sosyal medya: Kişilerin zaman ve mekana bağlı kalmadan internet aracılığıyla içerik tükettiği ve ürettiği, ya da diğer kullanıcılarla bilgi paylaşımı yaptığı ve iletişim kurduğu alandır.
- İki faktörlü kimlik doğrulama yöntemi: İki faktörlü kimlik doğrulama saldırganların cihazlarınıza veya hesaplarınıza erişimini zorlaştıran ek bir güvenlik özelliğidir.
- Dijital cihazlar (araçlar): Akıllı telefon, tablet, bilgisayardır.
- Şifre sıfırlama güvenlik sorusu: Şifrenizi unuttuğunuz durumlarda, web sitelerinin sizin siz olduğunuza kanaat getirmesine yarayan, daha öncesinde sizin seçtiğiniz ve cevabınızı verdiğiniz soru.

•Şifre sıfırlama: Şifre Sıfırlama, hesap açtığınız sitenin çeşitli yöntemlerle hesabın size ait olduğuna emin olup yeni şifre oluşturmanızı sağlamasıdır.

Araç ve gereçler: Slayt, projektör, akıllı tahta, çalışma kağıdı.

Yöntem ve teknikler: Sunuş yoluyla öğretim, soru cevap tekniği.

Dikkat çekme: Daha önce şifreniz çalındı mı? Sorusu yöneltilerek derse giriş yapılır.

Gözden geçirme: Daha önce sosyal bilgiler dersinde işlenen şifre güvenliği konusunda neleri hatırlıyoruz?

Öğrenme- Öğretme Süreçleri:

Güçlü şifreler başkaları tarafından tahmin edilmesi zor ve deneme yanılma yoluyla bulunması kolay olmayan şifrelerdir. İnternet ortamında güvenliği sağlamak için birçok uygulama sizden güçlü bir şifre oluşturmanızı ve şifrenizi korumanızı ister.

Peki şifre güvenliği nasıl sağlanır?

1. Her uygulama için farklı şifre kullanılmalıdır. Örneğin okul şifreniz ile sosyal medya hesaplarınızın şifresi birbirinden farklı olmalı.
2. “İki Faktörlü Kimlik Doğrulama” yöntemi kullanılmalıdır.

İki faktörlü kimlik doğrulama saldırganların cihazlarınıza veya hesaplarınıza erişimini zorlaştıran ek bir güvenlik özelliğidir. Bu yöntem tanınmayan cihazdan hesabınıza giriş yapılmak istendiğinde güvenlik kodu veya giriş izni isteyerek güvenlik kontrolü sağlanır.

3. Akıllı telefon, tablet, bilgisayar gibi dijital araçları ve kablosuz ağ modemleri şifreli kullanılmalıdır. -Aksi halde bir başkası cihazlarınıza ve ağınıza sızarak kişisel bilgilerinize kolaylıkla ulaşabilir.

4. Şifre sıfırlamada güvenlik sorularına tahmin edilmesi zor cevaplar oluşturulmalıdır. Örneğin; “şifremi unuttum” yöntemi ile şifre yenileme işleminde gizlilik için sorulan “evcil hayvanınızın adı nedir? sorusuna doğru cevabı vererseniz sizi tanıyan kişi kolaylıkla şifrenizi yenileyip hesabınızı ele geçirebilir.

5. Şifreler düzenli olarak en az altı ayda bir değiştirilmelidir.

6. Oluşturulan şifrenin başkası tarafından kullanıldığı düşünülüyorsa güvenli doğrulama yolları ile şifre sıfırlanmalıdır.

7. Güçlü bir şifre oluşturulmalıdır.

Peki güçlü bir şifre nasıl olur?

- Kendini tanımlayıcı sözcükler kullanılmamalıdır. Örneğin; 2005 doğumlu, adı ve soyadı Ayşe Yılmaz olan kişinin oluşturduğu şifre ayseyilmaz05 olursa bu tahmin edilebilir bir şifre olur.
- Yaygın kelime öbeği kullanılmamalıdır. Örneğin; “1453istanbul” birçok kişinin tahmin edebileceği bir şifre olabilir.
- Farklı türde karakterler kullanılmalıdır. Örneğin; büyük küçük harf ve semboller ile karmaşık bir şifre oluşturulabilir. XuJ.18.*M karmaşık şifreye bir örnektir.
- Oluşturulan şifre en az 8 karakterden oluşmalıdır. Örneğin; YuJ.09.*p

Bölüm Sonu Değerlendirmesi:

Konu kısaca değerlendirilerek ardından çalışma kağıdı verilir (EK 4: 1. Çalışma Kağıdı).

EĞİTİM 2

Ders: Sosyal bilgiler

Sınıf: 7/A

Ders Saati: 40 + 40

Konu: Dijital cihazımı ve içindekileri nasıl korurum?

SBDÖP’nda yer alan ilişkili kazanımlar:

SB.7.4.1. Bilginin korunması, yaygınlaştırılması ve aktarılmasında değişim ve sürekliliği inceler.(Yazının icadından günümüze kadar farklı depolama, yaygınlaştırma ve aktarma teknikleri üzerinde kısaca durulur).

SB.5.4.3. Sanal ortamı kullanırken güvenlik kurallarına uyar (Mesafeli alışveriş, güvenli internet kullanımı, kimlik hırsızlığı gibi konular ele alınır).

Beceriler: Dijital okuryazarlık, eleştirel düşünme, karar verme.

Değerler: Duyarlılık, sorumluluk.

Önemli kavramlar:

- Dijital cihazlar (Araçlar): Akıllı telefon, tablet, bilgisayardır.
- Güvenlik yazılımı: Kötü amaçlı yazılımlara karşı cihazı korumak için komut almış programdır.
- Yazılım: Bilgisayara ne yapacağını söyleyen, kodlanmış komutlar toplamıdır.
- Lisanslı yazılım: Biri tarafından üretilen ve üreticinin iznine göre süreli veya süresiz olarak kullanılan ve satın alınan güvenli yazılımlardır.
- Google drive: Google'ın oluşturduğu çevrim içi ortamda dosya yedeklemeye ve düzenlemeye imkan sağlayan bir hizmettir ve gmail hesabına bağlı çalışır.
- Güvenlik bildirimi: bilgisayarın ve güvenlik yazılımlarının güvenliği riske eden durumları haber vermesidir.

Araç ve gereçler: Slayt, Projektör, USB Bellek, Çalışma Kağıdı.

Yöntem ve teknikler: Sunuş yoluyla öğretim, soru cevap tekniği.

Dikkat çekme: Bugün kullandığınız akıllı telefon ve bilgisayarınız bozulursa veya içindekiler tamamen silinirse ne hissedersiniz? sorusu ile giriş yapılır.

Gözden geçirme: Daha önce sosyal bilgiler dersinde işlenen “güvenli genel ağ kullanımı” konusunda cihaz ve veri güvenliğiyle ilgili neleri hatırlıyoruz?

Öğrenme- Öğretme Süreçleri:

Dijital araçlarımızı kullanırken her gün sayısız risk ile karşı karşıya kalıyoruz. Bunların bir kısmı erişimden bir kısmı ise ihmal ettiğimiz güvenlik önlemlerinden kaynaklanmaktadır. Dijital cihazımızı ve içindekileri bu risklere karşı koruma yöntemlerine bir bakalım.

1. Güvenlik yazılımı kullanılmalıdır. Yazılım bilgisayara ne yapacağını söyleyen, kodlanmış komutlar toplamıdır. Güvenlik yazılımları ise kötü amaçlı yazılımlara karşı cihazı korur. Örneğin, günümüzde popüler güvenlik yazılımları arasında Norton, İntego, Avira, Panda, McAfee, Avast, Eset Nod32 bulunmaktadır.

2. Dijital cihazlarda lisanslı yazılım kullanılmalıdır. Lisanslı yazılım orijinal yazılımdır ve güvenlidir. Lisanslı olmayan yazılım korsandır ve bu bilgisayarın donanımını bozabilir. Örneğin, Microsoft Office, Windows XP, lisanslı yazılımlardır.
3. Önemli dosya ve bilgiler güvenli bir yere yedeklenmelidir. Örneğin; Google Drive gibi internet üzerinden depolama yapan veya usb bellek gibi harici araç ile yedekleme yapabilirsiniz. Google Drive, Google'ın oluşturduğu çevrim içi ortamda dosya yedeklemeye ve düzenlemeye imkan sağlayan bir hizmettir. Google drive'ı kullanabilmeniz için Gmail hesabına sahip olmalısınız. Gmail hesabınıza giriş yaptıktan sonra uygulamalar sekmesinden Google Drive'a ulaşabilirsiniz.
4. Kullanılan uygulamalar düzenli olarak güncellenmelidir. Güncellenmiş uygulamaların güvenlik önlemleri daha yüksektir.
5. Dijital cihazlar kullanılırken güvenlik bildirimlerine dikkat edilmelidir.
6. Güvenli olmayan sitelerden dosya ve uygulama indirilmemelidir. Örneğin telefona yükleyeceğiniz uygulamaları App Store veya Google Play Store'dan indirebilirsiniz.
7. Uygulama ve site izinleri erişim amacı ile uyumlu değilse ve işlem için gerekli değilse kabul edilmemelidir. Örneğin, konum bulma uygulamasının “fotoğraflara erişim isteği” gereksizdir ve kabul edilmemelidir.
8. Halka açık ve şifresi olmayan wifi ağlarına bağlanıldığında dikkatli olunmalıdır. Örneğin, halka açık wifi ağına bağlanıldığında şifreli işlemler ve dosya paylaşımı yaparken dikkat etmelisiniz.

Bölüm Sonu Değerlendirmesi:

Konu kısaca değerlendirilerek ardından çalışma kağıdı verilir (EK 4: 2. Çalışma Kağıdı).

EĞİTİM 3

Ders: Sosyal bilgiler

Sınıf: 7/A

Ders Saati: 40 + 40

Konu: İnternette dijital ayak izlerine dikkat!

SBDÖP’nda yer alan ilişkili kazanımlar:

SB.5.4.3. Sanal ortamı kullanırken güvenlik kurallarına uyar (Mesafeli alışveriş, güvenli internet kullanımı, kimlik hırsızlığı gibi konular ele alınır).

Beceriler: Konum analizi, medya okuryazarlığı.

Değerler: Duyarlılık.

Önemli kavramlar:

- Dijital ayak izi: İnternette tüm işlemlerin dijital ortama kaydedilmesidir.
- Aktif ayak izi: İnternette kullanıcıların isteyerek bıraktığı izlerdir.
- Pasif ayak izi: İnternette kullanıcıların istemsiz bıraktığı izlerdir.
- Dijital kimlik: internette bugüne kadar yaptığımız eylem ve söylemlerimiz sonucunda hakkımızda söylenenler ve çıkan izler bütünüdür.
- Kimlik hırsızlığı: Kötü niyetli kullanıcıların yani saldırganların, birini kişisel veya gizli bilgilerini elde etmek için aldatması ve elde ettiği bilgileri ekonomik kazanç ve kötü niyet için kullanması suçudur.
- Tarayıcı (arama motoru): Kullanıcıların, internet üzerinde bulunan bilgilere ulaşmasını sağlayan yazılımdır.
- Gizli sekme: internet tarayıcısında gizlilik amaçlı oluşturulan sekmedir ve arama geçmişini kaydetmez.

Araç ve gereçler: Slayt, Projektör, Çalışma kağıdı.

Yöntem ve teknikler: Sunuş yoluyla öğretim, soru cevap tekniği.

Dikkat çekme: Derse girişte öğrenciye “internette arama motorlarında adınızı ve soyadınızı hiç yazdınız mı?” ve “yazdıysanız neler karşınıza çıktı” soruları yöneltilir.

Gözden geçirme: Daha önce sosyal bilgiler dersinde işlenen “kimlik hırsızlığı, dijital izler” gibi konulara dair neler hatırlıyorsunuz?

Öğrenme- Öğretme Süreçleri:

Dijital ayak izi, internette tüm işlemlerimizin dijital ortama kaydedilmesidir. Örneğin, tarayıcı geçmişimiz, kullandığımız uygulamalar, paylaştığımız konumlar, üye olduğumuz sosyal ağlar, kısacası tüm adımlarımız dijital ayak izi bırakır.

Dijital ayak izleri aktif ve pasif olarak ikiye ayrılır.

•Aktif ayak izleri, internette kullanıcıların isteyerek bıraktığı izlerdir. Örneğin, katıldığımız sosyal ağlar ve gönderdiğimiz anlık iletiler aktif ayak izleridir.

•Pasif ayak izleri, internette kullanıcıların istemsiz bıraktığı izlerdir. Örneğin, arama geçmişimiz ve istemsizce tıkladığımız reklamlar pasif ayak izleridir.

İnternette bıraktığınız izler dijital kimliğinizi kötü yönde etkileyebilir. Veya bazı izler güvenliğinizi tehdit edebilir. Örneğin, paylaştığınız konumlar üçüncü şahıslar tarafından takip edilebilir ve zorbalığa maruz kalabilirsiniz. Ya da istemsizce tıkladığınız bir bağlantı sizi kimlik hırsızlarıyla karşı karşıya bırakabilir.

Dijital kimliğinizi iyi yönde etkileyen ayak izleri de vardır. Örneğin, internette yayınladığınız proje ve ödevleriniz dijital kimliğinizi iyi yönde etkileyecektir.

Peki dijital ayak izleri nasıl yönetebilirsiniz?

1. Halka açık bilgisayarları kullandıktan sonra tarayıcı geçmiş ve cihazın çöp kutusu temizlenmelidir. Örneğin, tarayıcı geçmiş google chrome’da sağ üst köşede “Geçmiş” sekmesi olarak bulunmaktadır.
2. Halka açık bilgisayarlardan kişisel hesaplara erişilmemelidir.
3. Halka açık bilgisayarlarda internet tarayıcılarının gizli sekme özelliği kullanılarak gezinti yapılabilir. Örneğin, Google Chrome’da “Yeni Gizli Sekme Aç” ile gizli gezinti yapabilirsiniz. . Bu özellik ile internet gezintiniz tarayıcının geçmişinde gösterilmez.
4. Ortaya çıkması istenmeyen veya güvenliği tehdit eden paylaşımlar yapılmamalıdır.
5. Şüpheli olan bağlantılara tıklama yapılmamalıdır.
6. Arama motorlarında adını araştırıp rahatsız eden şeyler belirlenmelidir. Böylece istenmeyen bilgiler kaynağa giderek silinebilir veya itiraz hakkı kullanılabilir.

7. Sosyal ağların ve cihazın gizlilik ayarları kontrol edilmelidir.

Bölüm Sonu Değerlendirmesi:

Konu kısaca değerlendirilir ve çalışma kağıdı verilir (EK 4: 3. Çalışma Kağıdı).

EĞİTİM 4

Ders: Sosyal bilgiler

Sınıf: 7/A

Ders Saati: 40 + 40

Konu: Erişim güvenliği nasıl sağlanır?

SBDÖP’nda yer alan ilişkili kazanımlar:

SB.5.4.3. Sanal ortamı kullanırken güvenlik kurallarına uyar (Güvenli ağ kullanımı ele alınır).

Beceriler: Dijital okuryazarlık, öz denetim.

Değerler: Sorumluluk, duyarlılık.

Önemli kavramlar:

- Dijital erişim: Dijital araçlar ile internetteki verilere ulaşmaktır.
- Güvenli erişim: Güvenilir olan site, bağlantı ve içeriklere erişmektir.
- Zararlı yazılım: 'Kötü amaçlı yazılım' olarak da bilinir ve bir cihaz, ağ ya da hizmete zarar vermek amacıyla hazırlanan program veya dosyadır.
- İstenmeyen posta: Spam olarak da bilinir ve toplu olarak gönderilen ve istenmeyen iletileri ifade eder.
- Güvenli internet hizmeti: İnternetteki zararlı içeriklerden sizi ve ailenizi büyük oranda koruyan güvenli erişim yöntemidir.

Araç ve gereçler: Slayt, projektör, çalışma kağıdı.

Yöntem ve teknikler: Sunuş yoluyla öğretim, soru cevap yöntemi.

Dikkat Çekme: Derse girişte öğrenciye “internete bağlandığınızda ne kadar güvendesiniz” sorusu yöneltilir.

Gözden Geçirme: Daha önce sosyal bilgiler dersinde “güvenli internet kullanımı” konusuna dair neleri hatırlıyorsunuz?

Öğrenme- Öğretme Süreçleri:

Dijital erişim, dijital araçlar ile internetteki verilere ulaşmaktır. Güvenli erişim ise güvenilir olan site, bağlantı ve içeriklere erişmektir.

İnternete erişim sırasında güvenli olmayan sitelere bağlanmak, bilinçsiz tıklamalar yapmak güvenliğinizi riske atabilir.

Örneğin eriştiğiniz web site güvenli değil ise ve “güvenli değil” uyarısına rağmen bağlanmaya devam ediyorsanız zararlı yazılımlara maruz kalmak üzere olabilirsiniz.

Veya şüpheli görünen e-postalardaki bağlantılara tıkladığınızda muhtemelen bir kimlik hırsızının tuzağına yaklaşıyorsunuz. Bu gibi durumlar ile güvenliğinizi tehlikeye atmamak için güvenli erişim yollarını tercih etmelisiniz.

Peki erişim güvenliği nasıl sağlanır?

1. Şüpheli görünen web bağlantıları açılmamalıdır. Örneğin hediye çekilişi veya kampanya sloganlarıyla gelen bağlantılar günümüzde kötü niyetli kullanıcılar tarafından çevrim içi dolandırıcılık ya da kimlik hırsızlığı amacıyla sıkça kullanılmaktadır.
2. İnternet sitesinin güvenilirliği kontrol edilmelidir. Örneğin; Güvenli olan bağlantılar adres çubuğundaki https ve anahtar kilit göstergesi kontrol edilerek ayırt edilebilir.
3. İstenmeyen postalar “istenmeyen posta” olarak işaretlenmeli ve içeriğindeki bağlantılara tıklama yapılmamalıdır. Örneğin, “Hesabınızı kurtarın” gibi başlıklarla gönderilen postalar buna örnektir. İstenmeyen Posta, Spam olarak da adlandırılmaktadır.
4. Tarayıcının güvenlik ayarları düzenlenmelidir. Örneğin, Güvenlik ayarlarınızı Google Chrome tarayıcısının sağ üst köşesinde yer alan “ayarlar” ve “gizlilik ve güvenlik” sekmesinden düzenleyebilirsiniz.

5. Güvenli internet hizmeti kullanılabilir. Güvenli internet hizmeti ücretsiz olarak sunulan ve internetteki zararlı içerikleri kısıtlayan güvenli erişim yöntemlerindendir. Bu hizmet “guvenlinet.org.tr” tarafından sunulmaktadır.

Güvenli internet hizmeti için iki adet profil bulunmaktadır.

1. Çocuk profili: Bu profil ile erişebileceğiniz tüm siteler uzman kontrolünden geçmiş belirli kriterlere göre onaylanmış sitelerdir.

2. Aile Profili: Bu profil yasadışı ve zararlı içerikleri barındıran siteler; Sağlık Bakanlığı'nın zararlı olduğunu açıkladığı ürünlerin siteleri ve dolandırıcılık sitelerine bağlantı kurmaz. İsteğe göre oyun ve sosyal medya sitelerini de erişim sağlayan bir profildir.

Güvenli internet hizmeti alabilmek için “guvenlinet.org.tr” adresini ailenizle birlikte inceleyebilirsiniz.

Bölüm Sonu Değerlendirmesi:

Konu kısaca değerlendirilir ve çalışma kağıdı verilir (EK 4: 4. Çalışma Kağıdı).

EĞİTİM 5

Ders: Sosyal bilgiler

Sınıf: 7/A

Ders Saati: 40 + 40

Konu: Doğru ve güvenli bilgiye erişmenin yolları nelerdir?

SBDÖP’nda yer alan ilişkili kazanımlar:

SB.5.4.2. Sanal ortamda ulaştığı bilgilerin doğruluk ve güvenilirliğini sorgular.

Beceriler: Kanıt kullanma, karar verme, araştırma, medya okuryazarlığı.

Değerler: Bilimsellik, dürüstlük.

Önemli kavramlar:

•Adres çubuğu: Girmiş olduğunuz sitenin tam bağlantı adını gösteren yerdir ve yeri genellikle aynıdır ve tarayıcının en üstüdür.

•Bağlantı (link): Web sitelerini birbirine bağlayan koda denir ve mavi renkli altı çizilidir.

Örnek: <https://www.guvenliweb.org.tr/>

•Montaj: Birbirinden anlamsız parçaları bir araya getirerek ortaya farklı bir anlam çıkarma işlemidir. Montajlı görseller eğer çok iyi hazırlanmamışsa farkedilebilmektedir.

Araç ve gereçler: Slayt, projektör, çalışma kağıdı.

Yöntem ve teknikler: Sunuş yoluyla öğretim, soru cevap tekniği.

Dikkat Çekme: Derse girişte öğrenciye “internetten edindiğiniz her bilgiye inanır mısınız?” sorusu yöneltilir

Gözden Geçirme: Daha önce “sanal ortamda doğru ve güvenli bilgi” konusuna dair neleri hatırlıyorsunuz?

Öğrenme- Öğretme Süreçleri:

İnternet, bilgiye ulaşmak için kullanılan en kolay ve ekonomik kaynaktır. Fakat internette herhangi bir konu hakkında pek çok farklı siteden yüzlerce bilgiye erişilebiliyor. Bu kadar bilgi çeşitliliği arasında bilginin doğruluğu ve güvenilirliğini bir bakışta anlamak zordur. Herkes rastgele bir içeriği çevrim içi olarak oluşturabilir ve yayabilir. Kimileri ise bilerek yanıltıcı bilgi paylaşımı yapmaktadır.

Bu sebeple merak ettiğiniz konuda en doğru ve güvenilir bilgiye ulaşmanız için bazı kontrolleri yapmanız gerekir.

İnternette ulaştığınız bilgi kaynağının “güvenirliğini” nasıl kontrol edebiliriz?

1. Kurumsal ve konu uzmanları tarafından yayınlanan bir kaynağa erişilmelidir. Örneğin; Güvenilir bir sitede, “Hakkında” ve “İletişim” kısmı ve kullanıcılara sunulmuş içerikler olmalıdır.
2. Kaynak, konu ile ilgili kurum veya uzman kişilerce oluşturulmuş olmalıdır. Bunun haricindeki kaynakların yanıltma payı yüksek olacaktır. Örneğin; Türkiye’de internet kullanımıyla ilgili bilgi edinmek için Bilgi Teknolojileri ve İletişim Kurumu’na ait web sitesi ziyaret edilmelidir.

3. Kaynak adresi kontrol edilerek sitenin taklit site olup olmadığı konusunda emin olmalısınız. Taklit eden siteler, genelde güvenilir olan sitelerden birkaç harf farkı ile kurulur.
4. Bilgiye ulaştığınız adres çubuğundan kaynağın güvenilirliğini sorgulamalısınız. Adres çubuğundaki simgeye tıkladığınızda bağlantının güvenliği hakkında bilgi edinebilirsiniz.

İnternette ulaştığınız bilginin “doğruluğunu” nasıl kontrol edebilirsiniz?

1. Bilgiyi asıl kaynaktan edinmeye çalışmalısınız ve birden fazla kaynaktan tarayarak karşılaştırma yapmalısınız.
2. Kaynağın içerdiği bilgi ile yer ve tarihin uyumlu olmasına dikkat etmelisiniz.
3. Haberin gerçeğe yakın olmasına dikkat etmelisiniz. (sarı ünlem koy). Örneğin, günümüzde mümkün olmayan bilgilerin kullanıldığı haberler gerçeklikten uzak, hayal ürünü haberlerdir.
4. Başlığın ve noktala işaretlerinin abartılı olup olmadığına dikkat etmelisiniz. Bu tip başlıkla oluşturulmuş haberler tıklama amacıyla kurgulanmış haberlerdir.
5. İçeriğindeki fotoğraf ve videolarda montaj olup olmadığına bakabilirsiniz. Montaj, birbirinden anlamsız parçaları bir araya getirerek ortaya farklı bir anlam çıkarma işlemidir. Montajlı görseller eğer çok iyi hazırlanmamışsa farkedilebilmektedir.

Bölüm Sonu Değerlendirmesi:

Konu kısaca değerlendirilir ve çalışma kağıdı verilir (EK 4: 5. Çalışma Kağıdı).

EĞİTİM 6

Ders: Sosyal bilgiler

Sınıf: 7/A

Ders Saati: 40 + 40

Konu: Dijital zorbalık nedir ve nasıl önlenir?

SBDÖP’nda yer alan ilişkili kazanımlar:

SB.4.4.2. Teknolojik ürünlerin geçmişteki ve bugünkü kullanımlarını karşılaştırır (Teknolojinin hayatımızda ve çevremizde meydana getirdiği olumlu ve olumsuz etkilerine dikkat çekilir)

SB.5.4.1. Teknoloji kullanımının sosyalleşme ve toplumsal ilişkiler üzerindeki etkisini tartışır.

SB.7.1.3. Medyanın sosyal değişim ve etkileşimdeki rolünü tartışır (Seçilen bir iletişim kanalının (TV, İnternet, akıllı telefonlar vb.) bireyler arasındaki iletişimi ve toplumsal olarak da kültürü nasıl değiştirdiği ele alınır).

Beceriler: Kanıt kullanma, medya okuryazarlığı, sosyal katılım, eleştirel düşünme.

Değerler: Özgürlük, saygı

Önemli kavramlar:

•Dijital zorbalık: Dijital teknolojiler aracılığıyla sosyal medyada, telefonlarda, mesajlaşma ve oyun platformlarında hedef seçilen kişileri korkutmaya, kızdırmaya ya da utandırmaya yönelik yapılan davranışlardır.

•Dijital teknoloji: İki makine arasında bir mesaj veya iletişim biçimini ikili koda dönüştürmeyi içeren bir aktarma türüdür.

•Gizlilik politikası: Site veya uygulamanın, kullanıcıya hangi kişisel bilgilerinin toplanacağı ve toplanan verilerin ne şekilde işleneceğini açıklayan resmi metindir.

•Güvenlik politikası: Sitenin sahip olduğu teknoloji altyapısına ve içeriğine erişmesine izin verilen kişilerin uymak zorunda olduğu kurallardır.

Araç ve gereçler: Slayt, projektör, USB bellek, medya haberi.

Yöntem ve teknikler: Sunuş yoluyla öğretim, soru cevap tekniği.

Dikkat Çekme: Derse girişte öğrenciye “Dijital Zorbalık” ile ilgili bir medya haberi gösterilir ve bu konuda ne düşündükleri sorulur.

Gözden Geçirme: Daha önce sosyal bilgiler dersinde işlenen dijital zorbalık kavramına dair neleri hatırlıyorsunuz?

Öğrenme- Öğretme Süreçleri:

İnternetin zengin iletişim ve etkileşim olanakları kullanıcıların fazlaca zaman geçirmesinde etkili olmaktadır. Fakat her gün dijital ortamda birçok kişi, “zorba” olarak adlandırılan kötü niyetli kişilerin saldırısına uğramaktadır.

Peki dijital zorbalık nedir?

Dijital zorbalık dijital teknolojiler aracılığıyla sosyal medya, telefon, mesajlaşma ve oyun platformlarında hedef seçilen kişileri korkutmaya, kızdırmaya ya da utandırmaya yönelik yapılan davranışlardır.

Örneğin, dijital teknolojilerin ardına sığınarak mesajlaşma yoluyla hakaret etmek, sosyal medyada bir kişi hakkında yalanlar yaymak, sahte hesap ile başkası adına kötü mesajlar göndermek dijital zorbalık türlerindendir.

Bu gibi dijital zorbalıklara maruz kalan kişilerde psikolojik rahatsızlıklar oluşabilmektedir.

Peki dijital zorbalığı nasıl önleriz?

1. Sadece yayınlanması istenen bilgiler paylaşılmalıdır. Örneğin; görüntü ve bilgi paylaşımı yapmadan önce bu paylaşımların başkaları tarafından size zarar vermek amacıyla kullanılma ihtimalini de düşünmelisiniz.
2. Yabancı kişilerden gelen arkadaşlık istekleri kabul edilmemeli ve istek gönderen her hesaba sorgulayıcı yaklaşılmalıdır. Örneğin; bir hesabın kullanıcı adı, ismi, profil fotoğrafı, takip ve takipçi sayısı, ortak bağlantılarınızın olup olmadığı konusunda eleştirel bir şekilde inceledikten sonra tanıyor iseniz ve gerçek hesap olduğuna artık eminseniz kabul edebilirsiniz.
3. İnternette iletişim kurmak isteyen kişilerin sahte veya kötü niyetli olma ihtimaline karşılık temkinli yani ölçülü olunmalıdır. Örneğin; tanımadığınız ya da güvenmediğiniz kişinin yüz yüze görüşme isteğini kabul etmek riskli bir davranıştır.
4. Üye olmak istenen sosyal ağların güvenlik politikaları incelenmeli ve bu ağlarda güvenlik-gizlilik kontrolleri sağlanmalıdır. Örneğin; üye olmak istediğiniz sosyal ağın güvenlik politikasını okumalı, üye olduğunuzda da gizlilik ayarlarını verilerinizi güvende tutacak şekilde düzenlemelisiniz. Tüm bu işlemler birçok uygulamanın “ayarlar” ve “gizlilik-güvenlik” sekmesinde bulunmaktadır.

5. İnternette yabancı kişilerle kişisel bilgiler paylaşılmamalıdır. Örneğin; TC Kimlik numaranız, doğum tarihiniz, telefon numarası, adres ve okul bilgileriniz kişisel bilgilerdir.
6. Özel hayat ve aile ile ilgili ipucu veren konuşma ve paylaşımlardan uzak durulmalıdır. Örneğin, okul veya ev adresinizi açığa çıkarıcı bilgi paylaşımı yapmamalısınız.
7. Kötü niyetli olduğuna emin olunan kişiler engellenmelidir. Engellemek de bir çeşit önleme yöntemidir.

Bölüm Sonu Değerlendirmesi:

Konu kısaca değerlendirilir ve çalışma kağıdı verilir (EK 4: 6. Çalışma Kağıdı).

EĞİTİM 7

Ders: Sosyal bilgiler

Sınıf: 7/A

Ders Saati: 40 + 40

Konu: Dijital zorbalık ile nasıl mücadele edilir?

SBDÖP’nda yer alan ilişkili kazanımlar:

SB.4.4.2. Teknolojik ürünlerin geçmişteki ve bugünkü kullanımlarını karşılaştırır (Teknolojinin hayatımızda ve çevremizde meydana getirdiği olumlu ve olumsuz etkilerine dikkat çekilir)

SB.5.4.1. Teknoloji kullanımının sosyalleşme ve toplumsal ilişkiler üzerindeki etkisini tartışır.

SB.7.1.3. Medyanın sosyal değişim ve etkileşimdeki rolünü tartışır (Seçilen bir iletişim kanalının (TV, İnternet, akıllı telefonlar vb.) bireyler arasındaki iletişimi ve toplumsal olarak da kültürü nasıl değiştirdiği ele alınır).

Beceriler: Kanıt kullanma, medya okuryazarlığı, sosyal katılım, eleştirel düşünme.

Değerler: Özgürlük, saygı

Önemli kavramlar:

- Saldırgan/dijital zorba: İnternette diğer kullanıcılara zarar verme amacıyla harekete geçen kişidir.
- Hesap dondurma: kullanılan sosyal medya hesabını çeşitli sebeplerden dolayı belli süreliğine kapatma işlemidir.
- Şantaj: Birini istemediği davranışa zorlamak için, bir durumu kötüye kullanarak baskı yapmak.

Araç ve gereçler: Slayt, Projektör, USB Bellek.

Yöntem ve teknikler: Sunuş Yoluyla Öğretim, Soru Cevap Tekniği.

Dikkat çekme: Derse girişte öğrenciye “çevrenizde dijital zorbalığa uğrayan kişilere rastladınız mı?” sorusu sorulur.

Gözden Geçirme: Daha önce sosyal bilgiler dersinde işlenen dijital zorbalık kavramına dair neleri hatırlıyorsunuz?

Öğrenme- Öğretme Süreçleri:

Dijital ortamda her gün çocuk veya yetişkin pek çok kişi zorbalığa maruz kalmakta ve bu durumdan sosyal ve psikolojik açıdan zarar görmektedir.

Dijital zorbalığın pek çok çeşidi bulunmaktadır.

Kişisel bilgilerinize ulaşarak sizi bu bilgileri başkalarıyla paylaşmak ile tehdit etmeleri, çevrim içi ortamda size hakaret edilmesi veya alay etmeleri, paylaştığınız bilgilerin izini sürerek size ulaşmaya çalışmaları “dijital zorbalığa” birer örnektir.

Zorbaların kişiler üzerinde bıraktığı korku ve endişe hissi ise saldırgan ile mücadele etmeyi zorlaştırmaktadır.

Siz de durumun farkında olup korkmadan zorba ile mücadele edebilirsiniz.

Nasıl mı?

1. Dijital ortamda sizi rahatsız eden zorbalarla iletişiminizi kesmelisiniz. İletişime devam ettiğiniz sürece zorbalık devam edecektir.

2. Dijital zorbalığa maruz kaldığınızda korku ve endişe hissinden kurtulmaya çalışın. Unutmayın yalnız değilsiniz ve amaç sizi psikolojik olarak yıpratmak.
3. Zorbalık devam ediyor ise durumu görmezden gelmeyin ve size ulaştığı platformlardaki hesaplarınızı silin veya dondurun.
4. Size zarar verici eylemlerde bulunan ve tehdit eden kişilerin isteklerini yerine getirmemelisiniz.
5. Zorbalık olayı bir sosyal platformda gerçekleşiyorsa kişinin davranışlarını platformun kendisine bildirebilirsiniz. Sosyal medya şirketlerinin, kullanıcılarını güvende tutma yükümlülükleri vardır.
6. Neler olup bittiğini ortaya koymak açısından kanıt toplanması yararlı olabilir. Örneğin; size dijital zorbalık yapan kişinin mesaj ve sosyal medya paylaşımlarının fotoğraflarını silmeden kaydedebilirsiniz.
7. Dijital ortamda size şantaj ve tehdit yoluyla isteklerini yerine getirtmeye çalışan kişileri ebeveyniniz ya da çevrenizdeki güvendiğiniz bir yetişkin ile paylaşarak yardım isteyebilirsiniz.
8. Dijital zorbalığa maruz kaldığınızda güvenliğiniz için durumu ailenize bildirerek yasal yollar ile şikayet etmelisiniz. Bu konuda ilgili mecralara ulaşabileceğiniz telefon hattı, şahsen başvuru veya internet aracılığıyla ihbar yolları bulunmaktadır.

Bölüm Sonu Değerlendirmesi:

Konu kısaca değerlendirilir ve çalışma kağıdı verilir (EK 4: 7. Çalışma Kağıdı).

EĞİTİM 8

Ders: Sosyal bilgiler

Sınıf: 7/A

Ders Saati: 40 + 40

Konu: Ailem ile birlikte çevrim içi alışveriş yaparken nelere dikkat etmeliyiz?

SBDÖP’nda yer alan ilişkili kazanımlar:

SB.4.5.3. Sorumluluk sahibi bir birey olarak bilinçli tüketici davranışları sergiler.

SB.5.4.3. Sanal ortamı kullanırken güvenlik kurallarına uyar (Mesafeli alışveriş, kimlik hırsızlığı gibi konular ele alınır).

SB.7.5.6. Dijital teknolojilerin üretim, dağıtım ve tüketim ağında meydana getirdiği değişimleri analiz eder (E-ticaret (gerçek ürünler kadar bilgisayar oyunları gibi sanal/dijital ürünler) üzerinde durulur).

Beceriler: Dijital okuryazarlık, finansal okuryazarlık, medya okuryazarlığı.

Değerler: Sorumluluk, tasarruf.

Önemli kavramlar:

- Çevrim içi alışveriş: İnternet üzerinden ürün ve hizmeti kredi kartı, internet bankacılığı veya kapıda ödeme yöntemi ile satın alma işlemidir.
- Çevrim içi dolandırıcılık: İnternet ortamında gerçekleştirilen dolandırıcılıktır.
- Kredi kartı: Bankaların müşterilerine verdiği ve ödeme yapmak için kullanılan karttır.
- Site uzantısı: Kısacası sitenin tam adres adıdır. Adres Çubuğunda gösterilir.
- 3D güvenli ödeme: Kredi ve banka kartıyla yapılan ödemelerde güvenliğini sağlamak için geliştirilmiş bir sistemdir.
- Sanal kart: Kredi kartına bağlı ve limitini sizin belirlediğiniz bir karttır. Bu kart ile hesap bilgilerini vermek zorunda kalmadan hızlı ve güvenli bir şekilde çevrim içi alışveriş yapılabilir.

Araç ve gereçler: Slayt, projektör, çalışma kağıdı, USB bellek, medya haberi.

Yöntem ve teknikler: Sunuş yoluyla öğretim, soru cevap tekniği.

Dikkat çekme: Derse girişte öğrenciye “dijital dolandırıcılık” ile ilgili medya haberi sunulur ve beraber değerlendirme yapılır.

Gözden geçirme: Daha önce sosyal bilgiler dersinde işlenen “mesafeli alışveriş” konusuna dair hatırladıklarınız nelerdir? sorusu ile işlenen konu gözden geçirilir.

Öğrenme- Öğretme Süreçleri:

Çevrim içi alışveriş, internet üzerinden ürün ve hizmeti kredi kartı, internet bankacılığı veya kapıda ödeme yöntemi ile satın alma işlemidir.

Günümüzde pek çok yetişkin satın alacağı ürünleri internet üzerinden sipariş vererek almaktadır. Çevrim içi alışverişe anne ve babanız internet üzerinden ürün satın alırken şahit olmuş olabilirsiniz.

Günümüzde “çevrim içi dolandırıcılık” ile ilgili haberlere sıklıkla rastlamaktayız. Örneğin; sipariş edilen ürünün beklenilenden farklı gelmesi, kredi kartı bilgilerinin sanal dolandırıcılar tarafından çalınması, hizmetten memnun kalınmadığı halde bilgilendirme metnini okumadan onaylaması sonucu ürünün iade edilememesi bu mağduriyetlere örnektir.

Siz de ailenizle birlikte alışveriş yaparken mağdur olmamak için “güvenli çevrim içi alışveriş yöntemlerini” öğrenebilir ve ailenizi bu konuda uyarabilirsiniz.

Lütfen 18 yaşınıza gelmeden tek başına çevrim içi alışveriş yapmaktan uzak durunuz.

Peki güvenli bir çevrim içi alışveriş için neler yapılmalı?

1. Ailenizle birlikte yapacağınız alışveriş için seçilen sitenin güvenliği kontrol edilmeli ve güvenilir olan siteler tercih edilmelidir. Örneğin, site uzantısını kontrol etmeli, site hakkında yorumlar araştırılmalı ve güvenilirliği şüpheli olan siteler tercih edilmemelidir.
2. Ailenizle birlikte seçtiğiniz çevrim içi alışveriş kanalında daha önce alışveriş yapanların satıcı ve ürün hakkında yorum ve şikayetleri kontrol edilmeli ve dikkate alınmalıdır. Örneğin, ailenizle birlikte yemek siparişi vermeden önce restoran, ürün ve hizmet kalitesi hakkında puana ve yorumlara bakmalısınız.
3. Aileniz, çevrim içi alışveriş sırasında satıcı tarafından sunulan “aydınlatma metni” ve bilgilendirmeleri dikkatli okuduktan sonra uygunsa onaylamalı. Örneğin, satıcının sunduğu aydınlatma metninde yazan “değişim ve iade yoktur” bilgisi dikkatli okunmadığında farkedilemez ve onaylandığında bu durum kabul edilmiş olur. Alışveriş sonrasında mağdur olmamak için ailenizi bu konuda uyarmanızdır.
4. Güvenli bir teslimat için diğer güvenlik kuralları uygunsa iletişim ve adres bilgileri doğru yazılmalıdır. Örneğin, iletişim ve adres bilgileri doğru yazılmadığında sipariş verdiğiniz ürünü güvenli bir şekilde teslim alamazsınız.

5. Aileniz ile birlikte yapacağınız alışveriş sırasında 3D Güvenli Ödeme seçeneğinin tercih edilmesini önermelisiniz. 3D Güvenli Ödeme, kredi ve banka kartıyla yapılan ödemelerde güvenliği sağlamak için geliştirilmiş bir sistemdir. 3D ile ödeme yapılırken, ekranda banka tarafından sunulan özel bir ekran açılır. Aynı anda ödeme yapmak isteyen kart sahibinin cep telefonuna onay kodu gönderilir. İşlem ekranında istenen alana kod girilir ve ödeme güvenli bir şekilde tamamlanır. Eğer onay kodu girilmezse ödeme işlemi gerçekleşmez.
6. 3D sistemi yoksa aileniz sanal kart ya da kapıda ödeme seçeneğini tercih edilebilir. Sanal kart, kredi kartına bağlı ve limitini sizin belirlediğiniz bir karttır. Bu kart ile hesap bilgilerini vermek zorunda kalmadan hızlı ve güvenli bir şekilde çevrim içi alışveriş yapılabilir.
7. Ailenizle birlikte yapacağınız çevrim içi alışverişin ödemesi yapılırken sistem tarafından sunulan “kredi kartı bilgilerini kaydet” isteği onaylanmamalı ve bu konuda ailenizi uyarmalısınız.

Siz de ileride “çevrim içi alışveriş” yapacağınız sırada bu güvenlik ilkelerine uyarak çevrim içi dolandırıcılığa maruz kalmaktan kaçınabilirsiniz.

Bölüm Sonu Değerlendirmesi:

Konu kısaca değerlendirilir ve ardından çalışma kağıdı verilir (EK 4: 8. Çalışma Kağıdı).

EĞİTİM 9

Ders: Sosyal bilgiler

Sınıf: 7/A

Ders Saati: 40 + 40

Konu: Çevrim içi ortamda hak ve sorumluluklarımız nelerdir?

SBDÖP’nda yer alan ilişkili kazanımlar:

SB.4.4.5. Teknolojik ürünleri kendisine, başkalarına ve doğaya zarar vermeden kullanır

SB.5.4.5. Yaptığı çalışmalarda bilimsel etiğe uygun davranır (Yapılan çalışmalarda yararlanılan kaynakları göstermenin ve kaynakların aslını korumanın önemi üzerinde durulur)

SB.5.6.1. Bireysel ve toplumsal ihtiyaçlar ile bu ihtiyaçların karşılanması için hizmet veren kurumları ilişkilendirir (Kazanım kapsamında e-devlet portalı ve bu portal üzerinden sağlanan hizmetlere değinilir)

SB.6.4.4. Telif ve patent hakları saklı ürünlerin yasal yollardan temin edilmesinin gerekliliğini savunur

SB.7.1.4. İletişim araçlarından yararlanırken haklarını kullanır ve sorumluluklarını yerine getirir (Özel hayatın gizliliği, düşünceyi açıklama özgürlüğü ve doğru bilgi alma hakkı ile kitle iletişim özgürlüğü arasındaki ilişki ele alınır).

Beceriler: Empati, öz denetim, hukuk okuryazarlığı, sosyal katılım.

Değerler: Adalet, dürüstlük, saygı, sorumluluk.

Önemli kavramlar:

•Dijital vatandaşlık; interneti bilinçli ve güvenli bir şekilde kullanabilme, çevrimiçi ortamlarda başkalarının haklarına saygı gösterme ve şahit olduğu uygunsuz bir olayı ilgili kurumlara şikayet yoluyla bildirmeyi kapsar.

•Hak: Hukukun getirdiği ve kişinin kendisine sağladığı kazanç

•Sorumluluk: Bir kişinin yapmak zorunda olduğu konu ve gerektiğinde o konu ile ilgili hesap verme durumu.

Araç ve gereçler: Slayt, projektör, USB bellek.

Yöntem ve teknikler: Sunuş yoluyla öğretim, soru cevap tekniği, beyin fırtınası.

Dikkat çekme: Derse girişte öğrencilere “internette diğer kullanıcılara karşı ne gibi sorumluluklar hissediyorsunuz? Diğer kullanıcıların size karşı yapmasını istemediğiniz davranışlar nelerdir? Soruları yöneltilerek beyin fırtınası yapılır.

Gözden geçirme: Daha önce sosyal bilgiler dersinde işlenen “dijital hak ve sorumluluklar” konusuna dair hatırladıklarınız nelerdir? sorusu ile işlenen konu gözden geçirilir.

Öğrenme- Öğretme Süreçleri:

Dijital vatandaşlar olarak internette hak ve sorumluluklarımız bulunmaktadır. Dijital vatandaşlık; interneti bilinçli ve güvenli bir şekilde kullanabilme, çevrimiçi ortamlarda başkalarının haklarına saygı gösterme ve şahit olduğu uygunsuz bir olayı ilgili kurumlara şikayet yoluyla bildirmeyi kapsar.

Peki dijital ortamda haklarımız nelerdir?

1. Kişilik haklarının korunması. Örneğin, dijital ortamda kişilere hakaret edilmesi uygunsuzdur.
2. Özel hayatın gizliliği. Örneğin, özel hayatınızla ilgili bilgilerin başkaları tarafından yayınlanması uygunsuzdur.
3. Kişisel verilerin korunması. Örneğin, projenizin, izniniz olmadan yayınlanması uygunsuzdur.
4. İnternette düşünceyi ifade edebilme. Örneğin, bir konu ile ilgili fikrinizi dijital ortamda yayınlatabilirsiniz. Fakat ifade ettiğiniz fikir nefret, şiddet ve suça teşvik edici olursa bu uygunsuz bir davranış olur ve hak olmaktan çıkar.
5. Uygunsuz dijital kullanımları şikayet hakkı. Örneğin, dijital ortamda zararlı içerik, site ve kullanıcıları şikayet etmek hem bir hak hem de bir sorumluluktur.
6. İnternette lekelenmeme hakkı. Örneğin, dijital ortamda birine iftira atmak uygunsuzdur.

Peki dijital toplumda çocuk olarak sorumluluklarınız nelerdir?

1. Okulda ve sosyal hayatta teknoloji kullanımı sırasında okulun uygun kullanım kurallarına göre hareket etmelisiniz.
2. Çevrim içi ulaştığınız bilgi ve belgeleri (video, ses, görsel, yazılı doküman vb.) kaynak belirterek ve izin alarak kullanmalısınız.
3. Çevrim içi ulaştığınız bilgi ve belgeleri size aitmiş gibi kullanmamalısınız.
4. Okul içinde ve okulu ilgilendiren uygulamalarda (sınav, mülakat, sözlü, ödev vb.) teknolojiyi kullanarak hile yapmamalısınız.
5. Okul içinde ve dışında dijital teknolojileri kullanarak (akıllı telefon, internet görseli koy burada) başkalarını rahatsız edici veya küçük düşürücü davranışlarda bulunmamalısınız.

6. Teknolojiyi kullanarak okul ile ilgili bilgi yayımı ve aktarımı yapmamalısınız. Örneğin; okul içinden video çekip paylaşmanız okul kurallarına aykırıdır.
7. Dijital teknolojiler kullanılarak yapılan uygunsuz kullanımları veliniz ile birlikte şikayet etmelisiniz.

Bölüm Sonu Değerlendirmesi:

Konu kısaca değerlendirilir ve ardından çalışma kağıdı verilir (EK 4: 9. Çalışma Kağıdı).

EĞİTİM 10

Ders: Sosyal bilgiler

Sınıf: 7/A

Ders Saati: 40 + 40

Konu: Dijital haklarımızı ihlal eden uygunsuz kullanımları hangi mecralara şikayet edebiliriz?

SBDÖP’nda yer alan ilişkili kazanımlar:

SB.7.1.4. İletişim araçlarından yararlanırken haklarını kullanır ve sorumluluklarını yerine getirir (Özel hayatın gizliliği, düşünceyi açıklama özgürlüğü ve doğru bilgi alma hakkı ile kitle iletişim özgürlüğü arasındaki ilişki ele alınır).

Beceriler: Hukuk okuryazarlığı, politik okuryazarlık.

Değerler: Adalet, eşitlik, özgürlük.

Önemli kavramlar:

•Bilgi Hırsızlığı: Kaynak göstermeden bir başkasının fikrini kendi fikri gibi göstermek ya da kullanmak.

•Uygunsuz Dijital Kullanım: İnternet ve dijital araçlar aracılığıyla başkalarının haklarına zarar verici eylem ve hareketlerdir.

Araç ve gereçler: Slayt, projektör, USB bellek, çalışma kağıdı.

Yöntem ve teknikler: Sunuş yoluyla öğretim, soru cevap tekniği, beyin fırtınası.

Dikkat çekme: Derse girişte öğrenciye “İnternette sıkça duyduğunuz haksızlıklar nelerdir ve bunun için ilk hangi kanala şikayette bulunursunuz? sorusu yöneltilir ve söylenen uygunsuz durumlar ve şikayet mecraları tahtaya yazılır.

Gözden Geçirme: Daha önce sosyal bilgiler dersinde işlenen dijital hak ve sorumluluklar konusunda uygunsuz durumları şikayet etme konusuna dair neleri hatırlıyorsunuz? Sorusu ile bilinen mecralar tahtaya yazılır, dersin sonunda yeni öğrenilen mecralar eklenir.

Öğrenme- Öğretme Süreçleri:

Dijital ortamda kullanıcılar bilişim teknolojilerini uygunsuz kullanarak diğer kullanıcıların haklarını ihlal edebilmektedir.

İnternette bilgi hırsızlığı yapmak, başkalarının verilerine izinsiz erişmek, edindiği bilgileri karşındakine zorbalık yapmak için kullanmak, başkalarını rahatsız edici söylem ve eylemlerde bulunmak dijital teknolojilerin uygunsuz kullanımlara birer örnektir.

Siz de güvenliğinizi tehdit eden uygunsuz dijital kullanımları ilgili mecralara bildirerek üzerinize düşen sorumluluğu yerine getirmelisiniz.

Uygunsuz dijital kullanımları şikayet edebileceğiniz mecralar 4’e ayrılmaktadır.

1. Okul ile ilgili uygunsuz dijital kullanımları öncelikle okul yetkililerine şikayet etmelisiniz. Okul yetkilileri; “okul yöneticisi, sınıf öğretmeni, okul rehber öğretmenidir. Dilerseniz bir başka öğretmeninize de durumu bildirebilirsiniz.
2. Okul içi veya okul dışında oluşmuş uygunsuz dijital durumları veliniz ile birlikte “internet üzerinden” şikayet edebilirsiniz.

Bu mecralar şunlardır

İhbar Web (<https://www.ihbarweb.org.tr>)

Çocuk ve yetişkinlere karşı işlenen dijital suçlar ile ilgili içeriği bu sitedeki şikayet başvuru kısmında yer alan ilgili alandan veliniz ile birlikte seçim yaparak ihbar edebilirsiniz.

Bilgi Teknolojileri ve İletişim Kurumu (<https://www.btk.gov.tr>)

İnternette oluşan uygunsuz kullanımları ve uygunsuz içerikleri Bilgi Teknolojileri ve İletişim Kurumu'na ait internet sitesinden veliniz ile birlikte ihbar başvurusu yapabilirsiniz.

Kişisel Verileri Koruma Kurumu (<https://www.kvkk.gov.tr>)

Bu kurumun web sitesi ile kişisel verilere saldırı niteliği taşıyan uygunsuz dijital kullanımları veliniz ile birlikte şikayet edebilirsiniz.

3. Okul içi veya okul dışında gerçekleşmiş uygunsuz dijital kullanımları veliniz ile birlikte “telefon hattı” üzerinden şikayet edebilirsiniz.

Bu mecralar;

ALO 112- Acil Çağrı Merkezi

ALO 166- İnternet Bilgi İhbar Hattı

4. Okul içi veya okul dışında gerçekleşmiş uygunsuz dijital kullanımları veliniz ile birlikte “şahsen” şikayet edebilirsiniz.

Bu mecralar;

Cumhuriyet savcılıkları

Emniyet veya jandarma karakolları

Siber Suçlar Şube Müdürlüğü

Unutmayın dijital hak ve sorumluluklarınız kanunlarca ve okul kurallarınca korunmaktadır.

Bölüm Sonu Değerlendirmesi:

Konu kısaca değerlendirilir ve ardından çalışma kağıdı verilir (EK 4: 10. Çalışma Kağıdı).

EĞİTİM 11

Ders: Sosyal bilgiler

Sınıf: 7/A

Ders Saati: 40 + 40

Konu: Dijital araçları ve interneti kullanırken sağlığını nasıl koruruz?

SBDÖP’nda yer alan ilişkili kazanımlar:

SB.5.1.3. Sahip olduğu haklarının farkında olan bir birey olarak katıldığı gruplarda aldığı rollerin gerektirdiği görev ve sorumluluklara uygun davranır (Kişisel zamanını planlarken oyun oynama, ders çalışma, kitap okuma, uyuma, aile ve arkadaşlar ile

nitelikli zaman geçirme ve kitle iletişim araçlarını kullanma durumlarını dikkate almanın önemine değinilir).

Beceriler: Zaman ve kronolojiyi algılama, tablo, grafik ve diyagram çizme ve

Değerler:

Önemli kavramlar:

- Obezite: Vücutta sağlığı bozacak ölçüde aşırı yağ birikmesidir.
- Asosyallik: Sosyal etkileşime girmeyi tercih etmeme, empati kurmakta sıkıntı yaşama halidir.
- Dijital bağımlılık: Kişinin zamanının çoğunu dijital ortamda geçirmesi; telefon, tablet ve bilgisayardan uzak duramaz hale gelmesidir. Ruhsal ve fiziksel tehlikeleri vardır.
- Depresyon: Hisleri, düşünce sistemini ve davranışları olumsuz etkileyen bir hastalıktır.
- Ruhsal bozukluk: Akıl sağlığının ve zihinsel işlevlerin bozulmasıdır.
- Zararlı içerik: Çocuğun yaşı veya gelişimi için uygun olmayan içeriklerdir.
- Akıllı işaretler: Televizyon ve internet yayınlarının içeriğiyle ilgili bilgilendirici bir sınıflandırma sistemidir.

Araç ve gereçler: Slayt, Projektör, USB Bellek, Çalışma Kağıdı.

Yöntem ve teknikler: Sunuş Yoluyla Öğretim, Soru Cevap Tekniği, Beyin Fırtınası.

Dikkat çekme: Derse girişte öğrenciye “dijital araç ve internetin uygunsuz kullanımından kaynaklı oluşan sağlık problemlerine örnek olacak yaşına ve psikososyal durumuna uygun medya haberleri” gösterilir.

Gözden geçirme: Daha önce sosyal bilgiler dersinde işlenen “dijital oyunları oynarken ve dijital cihazları kullanırken zamanı yönetme, dijital cihazların kullanımının sağlığa etkileri, zararlı içerikler ve akıllı işaretler” konularına dair neleri hatırlıyorsunuz? sorusu ile ön bilgiler gözden geçirilir.

Öğrenme- Öğretme Süreçleri:

İnternetin zengin içeriği ve bize sunduğu olanaklar zamanımızın çoğunu dijital araçlar ve internet ile geçirmemize sebep olmaktadır. Birçok kullanıcı zamanın nasıl geçtiğini

anlamadığını söylemektedir. Üstelik dijital teknolojileri kullanırken zarara uğrayacağımız tek konu “kaybettiğimiz zamanımız” değildir. Dijital teknolojileri kullanım sırasında sağlığımız çeşitli yönlerden olumsuz etkilenebilir.

Dijital teknolojileri kullanırken sağlığımız iki yönde olumsuz etkilenebiliyor.

- Fiziksel problemler: Dijital teknolojileri zaman ve şekil olarak uzun süre uygunsuz kullandığımızda fiziksel sağlığımızda sorunlar ortaya çıkabilir. Kas ve iskelet yapısında bozukluk, baş, boyun ve göz gibi organlarda etkilene ve obezite gibi rahatsızlıklar bu sorunlara örnektir.
- Psikolojik problemler: Dijital teknolojileri zaman ve içerik tercihiyle ilgili uygunsuz kullanımlarımız sonucu psikolojik sorunlar ortaya çıkabilir. Dijital bağımlılık, asosyalite, depresyon ve ruhsal bozukluklar bu sorunlara örnektir.

Peki dijital güvenliğimizi sağlık açısından nasıl koruruz?

1. Dijital araçları eğlence amaçlı kullanırken geçirdiğimiz zamanın farkında olmalıyız ve aşırı zaman harcamamalıyız. Örneğin, dijital oyun ve sosyal medya günlük kullanım süresi belirlemeliyiz ve bu süreyi aşmamaya özen göstermeliyiz.
2. Dijital cihazları kullanırken oturma biçimi ve izleme mesafesini sağlığa uygun şekilde ayarlamalıyız. Örneğin, bilgisayarınızı izleme mesafesini çok yakın tutmadan, dik bir oturma pozisyonunda belli aralıklara mola vererek kullanmalısınız.
3. Dijital cihazlarınızı kullanırken ses, ışık ve ekran parlaklığını göz sağlığınıza zarar vermeyecek şekilde ayarlamalısınız. Örneğin, ekran parlaklığını çok yüksek şekilde kullandığınızda bir süre sonra göz ve baş ağrısı yaşayabilirsiniz.
4. Zararlı içeriklerden (nefret, şiddet içerikli video, film, oyun, fotoğraf vb.) uzak durmalısınız. Örneğin, şiddet içerikli dijital oyunlar oynamanız sizi şiddete eğilimli bir birey haline getirebilir.
5. Akıllı işaretlere göre içerik tercihi yapmalısınız. Akıllı İşaretler, yayınların içeriğiyle ilgili bilgilendirici bir sınıflandırma sistemidir. İnternette karşılaştığınız içeriklerden önce cihazınızın ekranında akıllı işaretlere rastlarsınız. Siz de bu işaretleri dikkate almalı, yaşınıza uygun ve zararlı olmayan içerikleri tercih etmelisiniz.

*Akıllı işaretler simgeleriyle birlikte akıllı tahtada gösterilir.

Bölüm sonu değerlendirmesi:

Konu kısaca değerlendirilir ve ardından çalışma kağıdı verilir (EK 4: 11. Çalışma Kağıdı).



EK 4. Kontrol Grubuna Verilen Dijital Güvenlik Eğitimi Kapsamında Kullanılan Çalışma Kağıtları

1.ÇALIŞMA KAĞIDI

1.Soru: Aşağıdaki güçlü ve zayıf olan şifreleri yerlerine yazınız.

sevg134	B4L2*b1?
---------	----------

GÜÇLÜ ŞİFRE	
ZAYIF ŞİFRE	

2.Soru: Aşağıdaki güçlü ve zayıf olan şifreleri yerlerine yazınız.

Tb09d.!Aa	betvl.95
-----------	----------

ZAYIF ŞİFRE	
GÜÇLÜ ŞİFRE	

3.Soru: Aşağıdaki güçlü ve zayıf olan şifreleri yerlerine yazınız.

ayse.2002	F6.aw!XQp
-----------	-----------

GÜÇLÜ ŞİFRE	
ZAYIF ŞİFRE	

4. Soru: Şifrenizin güvende olması için aşağıdaki seçeneklerden hangilerini gerçekleştirmelisiniz.

(Doğru cevapları yuvarlak içine alınız)

- 1.İki Faktörlü Kimlik Doğrulama
- 2.Şifre sıfırlamanın güvenlik sorusuna tahmin edilmesi zor cevap oluşturma
- 3.Güvenli İnternet Hizmeti
- 4.3D Güvenlik Yöntemi
- 5.Akıllı İşaretler
- 6.Güçlü Şifre Oluşturma

5.Soru: Aşağıda verilen bilgi sizce doğru mudur?

“Güçlü bir şifre oluşturmak için farklı türde karakterler kullanılmamalıdır”.

A)	DOĞRU
B)	YANLIŞ

2. ÇALIŞMA KAĞID

1.Soru: Bilgisayarınızı korumak için hangi programı “güvenlik yazılımı” olarak seçemezsiniz.

a)Norton

b)İntego

c)Avira

d)Windows XP



2.Soru: Önemli bir ödev dosyanızı yedeklemek için aşağıdaki seçeneklerden hangileri güvenlidir?

A) Google Drive yedekleme

B) USB Bellek

C)Arkadaşının Bilgisayarı

D)Telefona

3.Soru: Dijital oyun oynadığınız esnada uygulama tarafından sunulan “Oyun fotoğraflarına erişmek istiyor” sorusuna yanıtınız ne olmalıdır?

A)	Reddet
B)	İzin Ver

4.Soru: Halka açık bilgisayarların kullanımı esnasında neleri yapmanız güvenli değildir?

	Gizli sekme ile internette arama yaparım
	Şifreli kaydet butonunu onaylarım
	USB belleğimi takar ve kullanırım

5.Soru: İnternet sitesinin güvenlik kontrollerini aşağıdaki hangi seçenekler ile yapabiliriz?

	Anahtar kilit
	HTTPS
	Yer İşareti
	Ayarlar

3. ÇALIŞMA KAĞIDI

1.Soru:

“GÖNDERDİĞİNİZ MESAJLAR” Aşağıdaki dijital ayak izlerinden hangisine dahildir?	
A)	AKTİF AYAK İZİDİR
B)	PASİF AYAK İZİDİR

2.Soru:

“BİLGİSAYARINIZIN IP ADRESİ” Aşağıdaki dijital ayak izlerinden hangisine dahildir?	
A)	AKTİF AYAK İZİDİR
B)	PASİF AYAK İZİDİR

3.Soru: Halka açık bilgisayarda grup ödevinizi araştırmak için interneti kullanarak araştırmanızı yaptınız ve bulduğunuz belgeleri diğer grup üyelerine e-posta olarak gönderdiniz. Bu işlemden sonra dijital ayak izlerinizi nasıl silersiniz?

(İşlem önceliğine göre [1-2-3 olarak] numara veriniz)

Yaptığım işlemleri seçerim	
Sil butonu ile temizlerim	
Tarayıcıdan “Geçmiş” sekmesine tıklarım	

4. Soru: Sosyal medya kullanırken her gün neler yaptığınızı gösteren fotoğraflar paylaşarak aktif ayak izleri bırakmak güvenlidir.

A)	DOĞRU
B)	YANLIŞ

5. Soru: Halka açık bilgisayarlardan araştırma yapmak için “GİZLİ SEKME” özelliğini kullandınız. Bu işlemin güvenlik derecesi aşağıdakilerden hangisidir?

A)	GÜVENLİ DEĞİL
B)	BİRAZ GÜVENLİ
C)	GÜVENLİ

4. ÇALIŞMA KAĞIDI

1.Soru: Aşağıda verilen web site uzantılarından hangisi “Güvenli İnternet Hizmeti” hakkında bilgi vermektedir?

A)	https://www.guvenlinet.org.tr
B)	https://www.btk.gov.tr
C)	https://www.turkiye.gov.tr

2. Soru: Güvenli İnternet Hizmeti vermek amacıyla kurulan sitede sunulmuş olan “Profil Seçenekleri” seçenekleri aşağıdakilerden hangisidir?

A)	Çocuk Profili
B)	Okul Profili
C)	Öğretmen Profili
D)	Aile Profili

3. Soru: İstenmeyen bir e-posta alındığında ne yapılmalıdır?

A)	E-posta açılıp bakılmalı
B)	İstenmeyen e-posta olarak işaretlenmeli

4) Soru: İnternet gezintisi yaparken karşınıza çıkan web sitesini incelemeden önce ne yapmalısınız?

A)	Adres çubuğundan web sitesinin uzantısını kontrol edilmeli
B)	Web sitesi kullanmaya devam edilmeli

5. Soru: Şüpheli görünen web bağlantısının bulunduğu bir e-posta aldığınızda vereceğiniz tepki ne olmalıdır?

A)	E-postadaki bağlantıya tıklanılmalı
B)	Bağlantıya tıklama yapılmamalı

5. ÇALIŞMA KAĞIDI

1.Soru: <https://data.tuik.gov.tr/> web sitesinde araştırma yapmak istediniz. Sizce bu güvenilir bir kaynak mıdır?



A)	GÜVENİLİR	B)	RİSKLİ
----	-----------	----	--------

2. Soru: <https://www.institu.com/blog/bilisimteknolojileri> web sitesinde araştırma yapmak istediniz. Sice bu güvenilir bir kaynak mıdır?

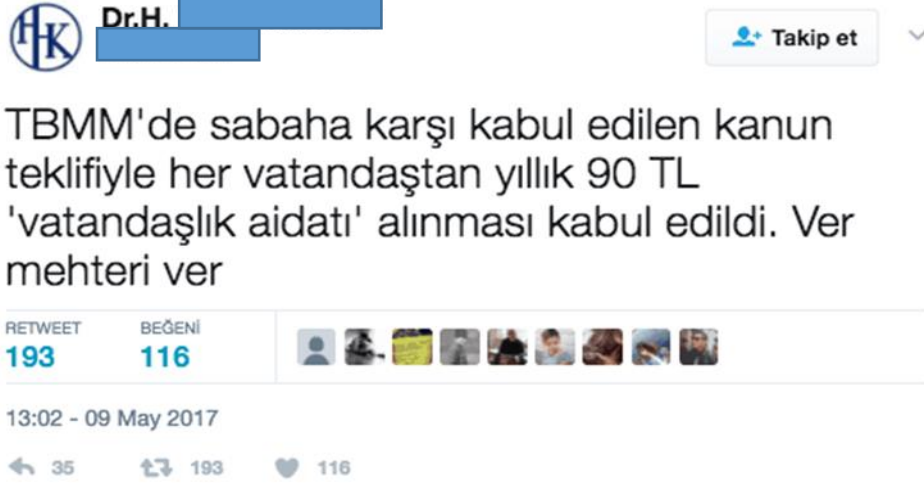


A)	GÜVENİLİR	B)	RİSKLİ
----	-----------	----	--------

3. Soru: Aşağıdaki bağlantılardan hangisi güvenlidir?

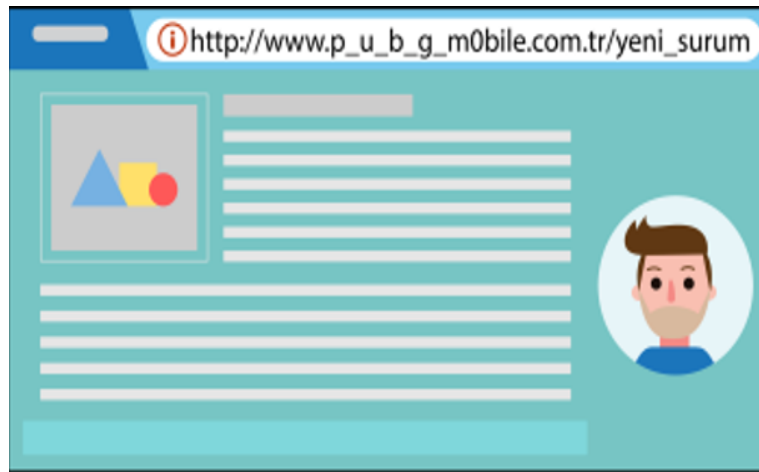
A)	https://www.btk.gov.tr/ Bilgi Teknolojileri ve İletişim Kurumu
B)	http://www.bt4.gov.tr/ Bilişim Teknolojileri Kurumu

4. Soru: Arkadaşınız size aşağıdaki görselde yer alan bu haberi Mart 2022 tarihinde göndererek doğru olduğunu iddia etmektedir. Haberin doğru olup olmadığını nereden anlarsınız?



A)	Gönderinin saatine ve tarihine bakarım.
B)	Gönderinin beğeni sayısına bakarım.
C)	Gönderiyi paylaşan kullanıcı adına bakarım.
D)	Gönderiyi paylaşan kullanıcının takipçi sayısına bakarım.

5. Soru: Arkadaşınız oynadığınız bir dijital oyun ile ilgili sosyal medyada ücretsiz sürüm haberi ve sürümün indirilecek site uzantısını sizinle paylaştı. Bu durumda ne yapmalısınız?



A)	Bağlantıyı açıp indiririm.
B)	Habere bakarım fakat uzantıya tıklama yapmam.
C)	Bağlantıyı arkadaşım gönderdiği için güvenirim ve ben de paylaşıyorum.

6. ÇALIŞMA KAĞIDI

1.Soru: Ali, Buse ve Selin birlikte internette oyun oynamaya karra vermişlerdir. Fakat Selin iyi oynayamadığı için Ali onu birden oyundan atmış yerine bir başkasını almıştır. Bu arkadaşlardan hangisi dijital zorbalığa maruz kalmıştır?

A)	Ali	B)	Buse	C)	Selin
----	-----	----	------	----	-------

2. Soru: Serkan ve Umut sosyal medyada sınıftan Zeynep isimli bir arkadaşlarının yeni paylaştığı fotoğrafın altına yorumlar yapmışlardır. Yorumlarda Umut' un Zeynep' in saç rengiyle dalga geçtiği görülmektedir. Bu arkadaşlardan hangisi dijital zorbalık yapmıştır?

A)	Serkan	B)	Umut	C)	Zeynep
----	--------	----	------	----	--------

3. Soru: Tanımadığın biri sana sosyal medyada sürekli takip isteği gönderiyor ve kabul etmen, tanışmanız gerektiğini belirten mesajlar gönderiyor. Bu durumda ne yapılmalı?

A)	Mesajına cevap verilmeli.	B)	Engellenmeli.
----	---------------------------	----	---------------

4.Soru: Aşağıdakilerden hangisi dijital zorbalık davranışlarından değildir?

A)	Şantaj yapmak	B)	Kaba sözler söylemek
C)	Alay etmek	D)	Mesajlaşmak

5. Soru: Dijital zorbalığa maruz kalmamak için aşağıdakilerden hangisi yapılmamalıdır?

A)	Yabancıların arkadaşlık isteği kabul edilmemeli
B)	Kişisel bilgiler paylaşılmalı
C)	Düşünmeden fotoğraf paylaşılmamalı.
D)	Şifreler başkalarıyla paylaşılmamalı

7. ÇALIŞMA KAĞIDI

1.Soru: Dijital zorbalığa karşı mücadele için aşağıdaki görsellerdeki hangi davranışı seçmemelisiniz?



A)	Üzülürüm ve endişelenirim.	B)	Zorbayı ihbar ederim
----	----------------------------	----	----------------------

2. Soru: Sosyal medyada dijital zorbalığa maruz kaldığında kimden yardım istemelisin?

A)	Ailemden yardım istemeliyim.	B)	Sosyal medyada tanıştığım kişiden yardım istemeliyim.
----	------------------------------	----	---

3. Soru: Sosyal medyada bir tehdit ve şantaj mesajı geldi. Bu durumda ne yapılmalı?

A)	Mesajı hemen kimse görmeden silerim.	B)	Ekran görüntüsü alırım.
----	--------------------------------------	----	-------------------------

4. Soru: “Dijital zorbalığa uğradığımı ailemden gizlimeliyim”

Bu davranış dijital güvenlik açısından doğru mudur?

A)	Doğru	B)	Yanlış
----	-------	----	--------

5. Soru: “Dijital ortamda tehdit ya da şantaja maruz kalındığında saldırganın isteğini yerine getirmemelidir”

Bu davranış dijital güvenlik açısından doğru mudur?

A)	Doğru	B)	Yanlış
----	-------	----	--------

8. ÇALIŞMA KAĞIDI

1.Soru: Ailenizle birlikte yaptığımız çevrim içi alışveriş sırasında güvenli bir ödeme yöntemi olarak aşağıdaki ödeme yöntemlerinden hangisini önerirsiniz?

A)	3-D Ödeme Yöntemi	B)	Kayıtlı kredi kartı ile ödeme
----	-------------------	----	-------------------------------

2. Soru: “Sitenin güvenliğini adres çubuğundaki anahtar kilide tıklayarak kontrol ederiz”. Bu çevrim içi alışveriş için güvenli bir kontrol yöntemi midir?

A)	Güvenli değil	B)	Güvenli
----	---------------	----	---------

3. Soru: Ailenizle birlikte yapacağınız çevrim içi alışveriş sırasında kredi kartı ile ödeme yaptıktan sonra “kart bilgilerini kaydet” butonu çıktığında ne yapmalısınız?

A)	Onaylarım	B)	Onaylamam
----	-----------	----	-----------

4. Soru: Ailenizle birlikte yapacağınız çevrim içi alışveriş sırasında satıcı tarafından sunulan “Aydınlatma Metni” çıktığında ne yapmalısınız?

A)	Okumadan onaylarım	B)	Okuyup, uygunsa onaylarım
----	--------------------	----	---------------------------

5. Soru: Ailenizle birlikte yapacağınız çevrim içi alışveriş sırasında aşağıdakilerden hangisi güvenli değildir?

A)	Sitede satıcı hakkında yorumlara ve puanlamalara dikkat edilmelidir
B)	Sitede ürünü daha önce alan kişilerin yaptığı yorumlar ve puanlamalar incelenmelidir
C)	İnternette çıkan reklama tıklayıp alışveriş yapılabilir.

9. ÇALIŞMA KAĞIDI

1.Soru: Ödeviniz için araştırma yapıyorsunuz. Bazı kaynaklardan yararlanarak ödevinizi tamamladınız. Bu durumda ödev dosyanızı sunarken “Hak ve Sorumluluk” adına ne yapmanız gerekmektedir?

A)	Yararlandığım kaynakları kaynakçada belirtirim.	B)	Ödevimi tamamen kendi bilgilerimle hazırladığımı söylerim
----	---	----	---

2.Soru: Aşağıdaki eşleştirmelerden hangisi doğrudur?

1. İnternette düşünceyi	a. şikayet hakkı
2. Dijital suçları	b. ifade edebilme hakkı
3. Kişisel verilerin	c. hakkı
4. İnternette lekelenmeme	d. korunması hakkı

- A) 1-a/ 2-b/ 3-c/ ve 4-d
B) 1-d/ 2-b/ 3-a ve 4-c
C) 1-b/ 2-d/ 3-c ve 4-a
D) 1-b/ 2-a/ 3-d ve 4-c

3. Soru: Aşağıdakilerden hangisi “Dijital Hak ve Sorumluluklar” bakımından uygun değildir?

A)	İnternette ulaştığım bilgi ve belgeleri kaynak olarak belirtmeliyim
B)	İnternette ulaştığım bilgi ve belgeleri izinsiz kullanabilirim
C)	İnternette diğer kullanıcıları rahatsız edici davranışlarda bulunamam.

4. Soru: “Teknolojiyi kullanarak okul ile ilgili bilgi yayımı ve aktarımı”. Bu cümledeki boşluk hangisi ile doldurulmalıdır?

A)	Yapma hakkım var	B)	Yapmamalıyım
----	------------------	----	--------------

5. Soru: Dijital ortamda biri, kişilik haklarını zedeleyen bir konuda zarar verdiğinde ne yapılmalıdır?

A)	Benzer şekilde davranılır	B)	Şikayet edilmelidir
----	---------------------------	----	---------------------

10. ÇALIŞMA KAĞIDI

1.Soru: Sosyal medyada hakkınızda sahte hesap üzerinden yalan haber yayınlayan kötü niyetli kullanıcıyı ailenize anlattıktan sonra aileniz ile birlikte internet üzerinden şikayet etmek istediniz. Bu tür şikayetlerin yapılması ve problemin çözülmesi için kurulmuş olan site hangisidir?

A)	İhbar Web- https://www.ihbarweb.org.tr/
B)	Güvenli Net- https://www.guvenlinet.org.tr/
C)	Güvenli Çocuk- https://www.guvenlicocuk.org.tr/

2. Soru: Sosyal medyada sizi sürekli tehdit ve şantajla rahatsız eden kötü niyetli kullanıcıyı ailenize anlattıktan sonra aileniz ile birlikte telefonla polise şikayet etmek istediniz. Hangi numarayı aramalısınız?

A)	Alo 112 Acil Çağrı Merkezi	B)	Alo 199 Vatandaş Etkileşim Merkezi	C)	Alo 118 Bilinmeyen Numaralar
----	-------------------------------	----	--	----	------------------------------------

3. Soru: İnternette herkese açık ortamda sizi zarar vermekle tehdit eden ve takipte olduğunu belirterek korkutmaya çalışan kişiyi ailenize bildirdikten sonra şahsen (yüz yüze) nereye şikayet edebilirsiniz?

A)	Cumhuriyet Savcılığına	B)	Okul Müdürüne	C)	İhbar Web'e
----	---------------------------	----	---------------	----	-------------

4. Soru: Amacı Türkiye’de telekomünikasyon sektörünü düzenleyip denetlemek olan “Bilgi Teknolojileri ve İletişim Kurumu” tarafından oluşturulan “Alo- İnternet Bilgi İhbar Hattı” aşağıdaki seçeneklerden hangisidir?

A)	Alo 112	B)	Alo 166
----	---------	----	---------

5. Soru: TUBİTAK Proje Yarışması için hazırladığınız projeyi dijital ortamda verilerinize sızarak çalan “Veri Hırsızını” hangi mecraya şikayet etmelisiniz?

A)	Kişisel Verileri Koruma Kurumu- https://www.kvkk.gov.tr/
B)	Bilgi Teknolojileri ve İletişim Kurumu- https://www.btk.gov.tr/
C)	E-devlet Kanalı- https://www.turkiye.gov.tr/

11. ÇALIŞMA KAĞIDI

1.Soru: Dijital cihazları ve interneti sağlıklı kullanım açısından aşağıdaki seçeneklerden hangisi uygundur?

A)	Ses ve ekran parlaklığı Orta Seviye	
B)	Ses ve ekran parlaklığı Yüksek Seviye	

2. Soru: Dijital cihazları ve interneti sağlıklı kullanım açısından oturuş ve izleme biçimi olarak aşağıdakilerden hangisi uygundur?

A)		B)	
----	--	----	---

3. Soru: Hangisi dijital oyun oynamak için uygun bir zaman yönetimidir?

A)	Her gün okuldan gelir gelmez 3 saat oynamak
B)	Hafta sonu ödevleri bitirip 1-2 saat oynamak
C)	2 günde bir akşamları 4-5 saat oynamak.

4. Soru: İnternette bir video içeriğinde bazı şiddet sahnelerine rastladınız ve video size ürkütücü geldi. Benzeri zararlı içerikli video ve filmlere bir daha rastlamamak için yapılması gereken aşağıdakilerden hangisidir?

A)	Bir daha şiddet sahnesi görülürse yine video kapatılır.	B)	Güvenli Net sitesinden “Güvenli İnternet Hizmeti” alınmalı.
----	---	----	---

5. Soru: Aşağıdaki akıllı işaretlerden hangilerini gördüğünüzde içeriği izlemeye devam edebilirsiniz?

			
Genel İzleyici Kitlesi	7 Yaş ve Üzeri	Şiddet/Korku	18 Yaş ve Üzeri İçin
A)	B)	C)	D)

EK 5. Kontrol Grubuna Uygulanan “Dijital Güvenlik Eğitiminin” Uygulama Programı

SÜRE			EĞİTİM KONUSU: DİJİTAL GÜVENLİK			
AY	TARİH	SAAT	KONULAR	KATILIMCI SAYISI	YÖNTEM VE TEKNİKLER	ARAÇ VE GEREÇLER
Nisan	20-22 Nisan	2 SAAT	1.Dijital Cihazlar ve Hesaplar İçin Şifre Güvenliği Nasıl Sağlanır?	35	ANLATIM, SORU CEVAP, BEYİN FIRTINASI, ÖRNEK OLAY İNCELEME	SUNU, MEDYA HABERLERİ, USB BELLEK
Nisan	25-27 Nisan	2 SAAT	2.Dijital Cihazımı ve İçindekileri Nasıl Korurum?	35		
Nisan-Mayıs	29 Nisan-6 Mayıs	2 SAAT	3.İnternette Dijital Ayak İzlerine Dikkat	35		
Mayıs	9-11 Mayıs	2 SAAT	4.Erişim Güvenliği Nasıl Sağlanır?	35		
Mayıs	13-16 Mayıs	2 SAAT	5.Doğru ve Güvenli Bilgiye Erişmenin Yolları Nelerdir?	35		
Mayıs	18-20 Mayıs	2 SAAT	6.Dijital Zorbalık Nedir ve Nasıl Önlenir?	35		
Mayıs	23-25 Mayıs	2 SAAT	7.Dijital Zorbalık ile Nasıl Mücadele Edilir?	35		
Mayıs	27-30 Mayıs	2 SAAT	8.Ailem ile Birlikte Çevrim İçi Alışveriş Yaparken Nelere Dikkat Etmeliyiz	35		
Haziran	1-3 Haziran	2 SAAT	9.Çevrim İçi Ortamda Hak ve Sorumluluklarımız Nelerdir?	35		

Haziran	6-8 Haziran	2 SAAT	10.Dijital Haklarımızı İhlal Eden Uygunsuz Kullanımları Hangi Mecralara Şikayet Edebiliriz?	35		
Haziran	10-13 Haziran	2 SAAT	11.Dijital Araçları ve İnterneti Kullanırken Sağlığımızı Nasıl Koruruz?	35		



EK 6. Deney Grubuna Çevrim İçi Öğrenme Yaklaşımında Uygulanan “Çevrim İçi Destekleyici Öğrenme Aracının” Uygulama Programı

SÜRE			EĞİTİM KONUSU: DİJİTAL GÜVENLİK			
AY	YÜKLEME TARİH	SAAT	KONULAR	KATILIMCI SAYISI	YÖNTEM VE TEKNİKLER	ARAÇ VE GEREÇLER
Nisan	20 Nisan	Süresiz	1.Dijital Cihazlar ve Hesaplar İçin Şifre Güvenliği Nasıl Sağlanır?	39	Çevrim İçi Öğrenme Yaklaşımı	Çevrim İçi Destekleyici Öğrenme Aracı, ÖYS, Dijital Cihaz, Google Meet Uygulaması
Nisan	24 Nisan	Süresiz	2.Dijital Cihazımı ve İçindekileri Nasıl Korurum?	39		
Nisan	29 Nisan	Süresiz	3.İnternette Dijital Ayak İzlerine Dikkat	39		
Mayıs	3 Mayıs	Süresiz	4.Erişim Güvenliği Nasıl Sağlanır?	39		
Mayıs	8 Mayıs	Süresiz	5.Doğru ve Güvenli Bilgiye Erişmenin Yolları Nelerdir?	39		
Mayıs	13 Mayıs	Süresiz	6.Dijital Zorbalık Nedir ve Nasıl Önlenir?	39		
Mayıs	18 Mayıs	Süresiz	7.Dijital Zorbalık ile Nasıl Mücadele Edilir?	39		
Mayıs	23 Mayıs	Süresiz	8.Ailem İle Birlikte Çevrim İçi Alışveriş Yaparken Nelere Dikkat Etmeliyiz	39		
Mayıs	28 Mayıs	Süresiz	9.Çevrim İçi Ortamda Hak ve Sorumluluklarımız Nelerdir?	39		

Haziran	2 Haziran	Süresiz	10.Dijital Haklarımızı İhlal Eden Uygunsuz Kullanımları Hangi Mecralara Şikayet Edebiliriz?	39		
Haziran	7 Haziran	Süresiz	11.Dijital Araçları ve İnterneti Kullanırken Sağlığımızı Nasıl Koruruz?	39		



EK 7. Etik Kurul Belgesi

Evrak Tarih ve Sayısı: 08.02.2022-E.281365



T.C.
GAZİ ÜNİVERSİTESİ
Etik Komisyonu

Sayı : E-77082166-302.08.01-281365
Konu : Bilimsel ve Eğitim Amaçlı

08.02.2022

EĞİTİM BİLİMLERİ ENSTİTÜSÜ MÜDÜRLÜĞÜNE

Üniversitemiz Eğitim Bilimleri Enstitüsü Türkçe ve Sosyal Bilimler Eğitimi Anabilim Dalı, Sosyal Bilgiler Eğitimi Bilim Dalı **Doktora Öğrencisi Fatma AKCAN'ın, Prof.Dr.Mehmet Ali ÇAKMAK'ın** danışmanlığında yürüttüğü "*Sosyal Bilgiler Dersinde Dijital Güvenlik Yeterliliği İçin Geliştirilen Oyun Tabanlı Destekleyici Öğretim Aracının Öğrencilerin Öz Yeterlilik Algılarına Etkisi*" adlı tez çalışması ile ilgili konu Komisyonumuzun **25.01.2022** tarih ve **02** sayılı toplantısında görüşülmüş olup,

İlgilinin çalışmasının, yapılması planlanan yerlerden izin alınması koşuluyla yapılmasında etik açıdan bir sakınca bulunmadığına oybirliği ile karar verilmiş ve karara ilişkin imza listesi ekte gönderilmiştir.

Bilgilerinizi rica ederim.

Araştırma Kod No: 2022 - 137

Prof. Dr. İsmail KARAKAYA
Komisyon Başkanı

Ek:1 Liste

DAĞITIM

Cereği:

Sayın Prof. Dr. Mehmet Ali ÇAKMAK

Bilgi:

Eğitim Bilimleri Enstitüsü Müdürlüğüne

Bu belge, elektronik ortamda imza ile onaylanmıştır.

Bu be

EK 8. Ankara Valiliği Milli Eğitim Müdürlüğü Tarafından Verilen Uygulama İzin Belgesi

Evrak Tarih ve Sayısı: 14.03.2022-E.313629

Evrak Tarih ve Sayısı: 11.03.2022-E.313150



T.C.
ANKARA VALİLİĞİ
Milli Eğitim Müdürlüğü

Sayı : E-14588481-605.99-45501735
Konu : Araştırma İznı

11.03.2022

GAZİ ÜNİVERSİTESİNE
(Öğrenci İşleri)

İlgi : a)MEB Yenilik ve Eğitim Teknolojileri Genel Müdürlüğü'nün 2020/2 nolu Genelgesi.
b)01.03.2022 tarihli ve 303252 sayılı yazınız.

Üniversiteniz Eğitim Bilimleri Enstitüsü, Türkçe ve Sosyal Bilimler Eğitimi Ana Bilim Dalı, Sosyal Bilgiler Eğitimi Bilim Dalı Doktora Öğrencisi Fatma AKCAN'ın "**Sosyal Bilgiler Dersinde Dijital Güvenlik Yeterliliği İçin Geliştirilen Oyun Tabanlı Destekleyici Öğretim Aracının Öğrencilerin Öz Yeterlilik Algılarına Etkisi**" konulu çalışması kapsamında ilimiz 25 ilçesindeki Ortaokullarda, uygulama talebi ilgi (a) Genelge çerçevesinde incelenmiştir.

Yapılan inceleme sonucunda, söz konusu araştırmanın Müdürlüğümüzde muhafaza edilen ölçme araçlarının; Türkiye Cumhuriyeti Anayasası, Milli Eğitim Temel Kanunu ile Türk Milli Eğitiminin genel amaçlarına uygun olarak, ilgili yasal düzenlemelerde belirtilen ilke, esas ve amaçlara aykırılık teşkil etmeyecek, eğitim-öğretim faaliyetlerini aksatmayacak şekilde okul ve kurum yöneticilerinin sorumluluğunda gönüllülük esasına göre uygulanması Müdürlüğümüzce uygun görülmüştür.

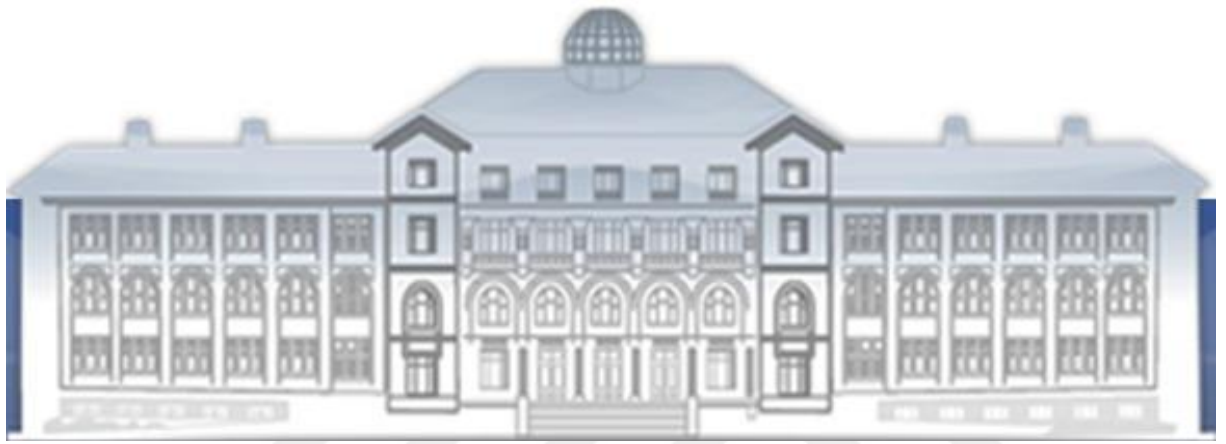
Bilgilerinizi ve gereğini rica ederim.

Harun FATSA
Vali a.
Milli Eğitim Müdürü

Dağıtım:
Gereği:
Gazi Üniversitesi

Bilgi:
25 İlçe MEM

Aİ
Tİ
E-
Kİ



GAZİLİ OLMAK AYRICALIKTIR...