

## Öğretmenlerin Dijital Veri Güvenliği Farkındalığı

Eray YILMAZ\*

Yusuf Levent ŞAHİN\*\*

Yavuz AKBULUT\*\*\*

### Öz

Geçmişte çoğunlukla basılı materyallerle çalışan öğretmenler, günümüzde bilgi ve iletişim teknolojileri yardımıyla bilgiyi dijital ortamlarda üretmekte ve saklamaktadır. Eğitim öğretim etkinliklerinde teknolojiyi sıklıkla kullanmaları beklenen öğretmenlerin sahip oldukları dijital verilerin güvenliği son derece önemlidir. Bu bağlamda araştırmanın amacı, Milli Eğitim Bakanlığı'na bağlı okullarda görev yapan öğretmenlerin dijital veri güvenliği farkındalıklarını irdelemektir. Çalışma kapsamında Balıkesir ilinde 29 farklı okulda görev yapan toplam 870 öğretmenden dijital veri güvenliği farkındalık ölçeği (DVGFO) yardımıyla veri toplanmıştır. Bulgular, öğretmenlerin dijital veri güvenliği farkındalıklarının oldukça yüksek olduğunu göstermiştir. Farkındalık değerlerinin cinsiyet, günlük bilgisayar kullanım süresi, günlük İnternet kullanım süresi ve farklı teknolojilere sahip olma durumlarına göre değiştiği; ancak branş, öğrenim kademesi, öğrenim durumu ve mesleki kıdem bağlamında değişmediği gözlemlenmiştir.

**Anahtar Kelimeler:** Dijital veri, veri güvenliği, öğretmenler.

## Digital Data Security Awareness of Teachers

### Abstract

Teachers were used to study with printed materials in the past; but nowadays, they produce and store information in digital environments thanks to emerging information and communication technologies. Since teachers are expected to employ emerging technologies in their instructional practices, the security of their digital data carries utmost importance. In this context, the current study aimed to investigate the digital data security awareness of teachers, who are employed in different schools of the National Ministry of Education. The data were collected through the Digital Data Security Awareness Scale which was administered to 870 teachers in 29 different schools in Balıkesir. Descriptive statistics indicated that participants' digital data security awareness levels were quite high. While the awareness levels varied with regard to gender, duration of daily computer and Internet use, and ownership of different digital technologies; it did not change with regard to teachers' branch, school type, educational background and experience.

**Keywords:** Digital data, data security, teachers.

\* Dr., T.C. Ziraat Bankası Balıkesir Fen Lisesi, eray\_yilmaz@yahoo.com

\*\* Yrd. Doç. Dr., Anadolu Üniversitesi, Eğitim Fakültesi, Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü, ylsahin@anadolu.edu.tr

\*\*\* Doç. Dr., Anadolu Üniversitesi, Eğitim Fakültesi, Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü, yavuzakbulut@anadolu.edu.tr

## 1. GİRİŞ

Bilgi ve iletişim teknolojileri, günümüzdeki bilgi üretme ve üretilen yeni bilgiye erişme hızına paralel olarak günlük yaşamı değiştirmeye başlamıştır. Günlük alışkanlıklarımızı da etkileyen bu teknolojiler; aynı zamanda eğitimden ticarete, bankacılıktan iletişime kadar pek çok alanda yaşamı kolaylaştırmıştır. Bilindik kavramlar, elektronik sözcüğünün ilk harfi ile birleşmeye başlamış; e-posta, e-devlet, e-okul, e-imza gibi yeni kavramlar ortaya çıkmıştır. Dijital ortamlarda üretilen ve yine dijital ortamlarda saklanan bilginin artması, bilgi güvenliğine ilişkin çeşitli risk ve tehditleri de beraberinde getirmektedir.

Bilgi ve iletişim teknolojilerini kullananların çoğu, oluşabilecek risk ve tehditlerin farkında değildir. Oysa söz konusu tehditler bireyleri maddi kayba uğratabilmekte, sahip oldukları bilgilere izinsiz olarak erişmeyi olanaklı kılmakta, bu bilgilerin silinmesi ya da değiştirilmesi sonucu tamiri olanaksız hasarlara neden olabilmektedir (Özenç, 2007).

Bilgi güvenliği kavramı, bilgiye sürekli olarak erişilebilen bir ortamda, bu bilginin göndericiden alıcıya kadar gizlilik içinde, bozulmadan, değiştirilmeden ve başkalarının eline geçmeden güvenli olarak iletilmesi biçiminde tanımlanabilir (Schmidt, 2004). Bu kavram, önceleri daha çok yazılı ve basılı ortamlardaki bilgilerin fiziksel anlamda güvenliğinin sağlanması olarak düşünülmüştür (Henkoğlu ve Yılmaz, 2013). Günümüzde ise süreç bilişim teknolojileri açısından değerlendirilmekte ve dijital veri güvenliği kavramı ön plana çıkmaktadır. Örneğin, Canbek ve Sağiroğlu (2006), dijital veri güvenliğini, elektronik ortamlardaki verilerin bütünlüğü bozulmadan ve izinsiz erişimlerden korunarak saklanması ve taşınması için bilgi işleme platformlarının güvenli hale getirilmesi biçiminde tanımlamaktadır.

Dijital veri güvenliğini tehdit eden birçok etmeden söz edilebilir. Doğal afetler nedeniyle güç kaynaklarının, kamera sistemlerinin ve telefon santrallerinin arızalanması; e-posta, İnternet bankacılığı, çevrimiçi alışveriş ve donanım kaynaklı sorunlar; bilgisayar virüsleri, yetkili erişimlerin kötüye kullanılması gibi maddeler bunlardan yalnızca birkaçıdır. Başlıca sorun ise Wagner ve Brooke'un da (2007) belirttiği gibi bilgi güvenliğini oluşturan zincirin en zayıf halkası olan insan kaynaklı tehditlerdir. Bu tehditler, kullanıcıların bilinçsizce ya da yeterli eğitime sahip olmadan teknoloji kullanması sonucunda ortaya çıkabildiği gibi, bilinçli olarak sisteme zarar verme biçiminde de ortaya çıkabilir (Tekerek, 2008). Örneğin, Symantec (2013) tarafından yayınlanan 18. İnternet Güvenlik Tehdit Raporu (ISTR) verilerine göre 2012'de gerçekleşen siber saldırılar, bir önceki yıla göre % 42 artmıştır. Rapora göre Avrupa ülkeleri arasında Türkiye; istem dışı e-posta (spam) saldırılarında beşinci, olta (phishing) saldırılarında sekizinci, virüs saldırılarında ise yine beşinci sırada yer almaktadır. Bu bağlamda dijital veri güvenliğine ilişkin ampirik araştırmaların önemi her geçen gün daha da artmaktadır.

Birey, kurum ve kuruluşlar genellikle bilgi güvenliği konusunda önceden sıkı önlemler almak yerine, ciddi bir olay baş gösterdiğinde harekete geçme eğilimindedirler. Bu bakımdan bilgi güvenliği konusunda farkındalığın artırılmasına gereksinim duyulmaktadır. Özellikle yönetim seviyesindeki kişilerin farkındalık ve anlayışı, bilgi güvenliği kültürü oluşturulması bakımından büyük önem taşımaktadır (Kocamustafaogulları, 2013). Bu konuyu ön planda tutmak ve kendilerini yetiştirmek zorunda olan bir başka kurum da bilginin üretme, öğretme, sunma ve dağıtma işinden sorumlu üniversiteler ve öğretim elemanlarıdır (Keser ve Güldüren, 2015). Milli Eğitim Bakanlığı Bilgi İşlem Dairesi Başkanlığı (2012) tarafından yayımla-

nan “Bilgi ve Sistem Güvenliği Yönergesi” ise, bakanlığın kurum olarak konuyu oldukça önemseyişinin bir göstergesidir. Yönergenin amacı, Bakanlık merkez ve taşra teşkilatındaki tüm personel ile kendilerine herhangi bir nedenle Bakanlık bilişim kaynaklarını kullanma yetkisi verilen konukların, Millî Eğitim Bakanlığı bünyesinde bulunan bilişim kaynaklarının kullanımına yönelik usul ve esasları belirlemektir.

Dijital veri güvenliğine yönelik riskler bazen maddi zararlara bazen de hayati tehlikelere yol açabilmektedir. Alınabilecek bireysel önlemler ile sanal dünyanın tehlikelerinden korunmak mümkün olabilir. Yapılmış çalışmalar ve çözüm yolları incelendiğinde alınabilecek önlemlerden bazıları; güvenlik yazılımlarının güncel tutulması, lisanslı yazılımların kullanılması, parolaların birbirinden bağımsız olması, güvenli olmayan e-postaların açılmadan silinmesi, sosyal paylaşım ağlarında kişisel bilgilerin paylaşılması, elektronik bankacılık ve çevrimiçi alışverişte kişisel bilgisayarların kullanılması biçiminde sıralanabilir (Karakoç, 2011; Yavanoğlu, Sağiroğlu ve Çolak, 2012). Bireysel önlemlerin yanı sıra yasalar yoluyla da bilgi güvenliğine ilişkin önlemler alınabilir. Karakoç (2011) çalışmasında bilişim suçları ile ilgili kanuna değinmiştir. Buna göre Türk Ceza Kanunu’nun 10. bölümünde “Bilişim Alanında Suçlar” başlığı altında yer alan 243. madde “Bilişim Sistemine Girme”, 244. madde “Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme”, 245. madde ise “Banka veya Kredi Kartlarının Kötüye Kullanılması” ile ilgilidir ve bu suçlara ilişkin cezalar öngörülmüştür.

Dijital veri güvenliğine yönelik riskleri en aza indirmenin yolu bireyler üzerinde farkındalık oluşturmaktan geçmektedir. Günlük yaşamda sıkça kullanılan farkındalık kavramı, bireyin tüm duyu organlarını kullanarak, diğer bireylerle veya çevresiyle iletişime geçerken yaşa-

dıklarının ayırında olması biçiminde tanımlanabilir (Acar, 2004). Bilgi ve iletişim teknolojilerinin yoğun kullanımı ve Symantec (2013) benzeri raporlarda gözlemlendiği üzere Türkiye’nin bilgi güvenliği karnesi dikkate alındığında, bireylerin dijital veri güvenliği konusundaki farkındalıkları önemli bir çalışma alanı olarak karşımıza çıkmaktadır.

Dijital veri güvenliğinin sağlanabilmesi için elbette bir takım teknik önlemler de alınabilir. Ancak alınabilecek önlemlerin başında insan faktörü gelmektedir. Teknoloji kullanımında insan faktörü göz ardı edilirse alınan önlemler sonuç vermeyecektir. Çünkü bu konuda bilinci ve farkındalığı olmayan bireyler, güvenlik sürecinin işleminde farklı aşamalarda aksaklıklara neden olacaktır. Dikkatli ve iyi eğitilmiş bireyler ise oluşabilecek güvenlik ihlallerini engelleyebilir. Bu nedenle, toplumun dijital veri güvenliği konusunda bilinçlendirilmesi ve bu konuda farkındalık yaratılması gereklidir.

### 1.1 Öğretmenler için Dijital Veri Güvenliği

Tüm dünya ile birlikte ülkemizde de kamu ve özel kuruluşlar, bilgi ve iletişim teknolojilerinin sunduğu olanakları kullanarak, verdikleri hizmetlerin daha hızlı, yer ve zamandan bağımsız, çağdaş ve kaliteli hale getirilmesi için yeni arayışlara girmişlerdir. Millî Eğitim Bakanlığı da (MEB) e-devlet uygulamaları kapsamında MEBBİS (Millî Eğitim Bakanlığı Bilişim Sistemleri) projesini hayata geçirmiştir. Öğretmenler ve okul yöneticileri; MEBBİS ile kadro, terfi, izin işlemleri ile kimlik, öğrenim, sicil bilgilerine erişim gibi işlemleri İnternet üzerinden gerçekleştirebilmektedir (İnci, 2002). Ayrıca web tabanlı okul yönetimi yazılımı olan e-Okul sayesinde; öğrenci işlemleri (kayıt, nakil, devam takibi, karne, veli bilgilendirme vb.), ders ve sınav işlemleri (ders programı, sınav takvimi, not girişi vb.) İnternet aracılığıyla yapılabilmektedir (MEB, 2009). Bu sistemlerle birlikte öğretmenler, sınav sorusu hazırlan-

masından, ders içeriklerinin dijital ortama aktarılmasına kadar eğitim ve öğretim hizmetlerinde bilişim teknolojilerini yoğun olarak kullanmaktadır.

MEB'in eğitimde teknoloji entegrasyonuna yönelik geliştirdiği projeler de bulunmaktadır. 1990 yılında yürürlüğe giren Milli Eğitimi Geliştirme Projesi (MEGP) kapsamında 208 Müfredat Laboratuvar Okulu (MLO); bilgisayar, yazıcı, tarayıcı, TV, video kamera, tepegöz gibi eğitim materyalleri ile donatılmıştır (MEB, 2002). Halen yürütülmekte olan Fırsatları Artırma ve Teknolojiyi İyileştirme Hareketi (FATİH) projesinin amacı ise; eğitim ve öğretimde fırsat eşitliğini sağlamak ve okullardaki teknolojik olanakları iyileştirmek amacıyla güncel bilişim teknolojilerinin öğretim süreçlerinde daha etkin kullanımını sağlamaktır (FATİH Projesi, 2012).

Öğretmen yetiştirme noktasında güncel hizmet içi eğitim programları incelendiğinde, 2. seviye modül programlar arasında "Eğitimde Bilişim Teknolojilerinin Kullanımı Kursu" yer almaktadır. Bu etkinliğin üniteleri; bilgi teknolojisi bileşenleri, İnternet'i etkin kullanma, etkili sunum teknikleri ve bilişim teknolojilerini kullanarak ders işleme biçimindedir (Öğretmen Yetiştirme ve Geliştirme Genel Müdürlüğü, 2013).

MEB'in uygulamaya koyduğu, eğitimde teknoloji entegrasyonunu hedefleyen makro ölçekli projelerdeki öğretmen eğitimleri ve yürütülen hizmet içi eğitim etkinlikleri incelendiğinde dijital veri güvenliği konusuna yeterince yer verilmediği görülmektedir. Oysa öğretmenlerin hem karşılaşabilecekleri zararları, hem de yaşanabilecek sorunların hukuki boyutlarını bilmeleri, dijital veri güvenliği farkındalığı çerçevesinde büyük önem taşımaktadır.

Dijital veri güvenliği üzerine, katılımcıları öğretmenler olan pek çok uluslararası araştır-

ma bulunmaktadır. Bunlardan İnternet Güvenliğinde Öğretmen Farkındalığı (Teacher Awareness of Internet Safety-TAIS) projesi oldukça dikkat çekicidir. Bu proje, 2000-2009 yılları arasında Tayvan'daki ilkokul ve ortaokul öğretmenlerine yönelik olarak geliştirilmiştir. Projede; eğitim seminerleri, atölye çalışmaları, konferanslar gibi çok çeşitli etkinlikler yer almıştır. Ayrıca 7/24 hizmet veren e-Öğretmen web sitesi sayesinde; çevrimiçi öğretmen-öğrenme toplulukları kurulmasına yardımcı olunmuş, öğretim programına uygun güvenli içerikler ve öğretmenlerin sınıflarında kullanılabileceği üniteler sunulmuştur (Chou ve Peng, 2011).

Ulusal düzeyde de dijital veri güvenliği konulu çalışmalara rastlamak mümkündür. Örneğin, birkaç yıl önce MEB Bilgi İşlem Dairesi Başkanlığı (2012) tarafından 7484 katılımcıya anket uygulanmış ve personelin bilgi güvenliği farkındalık düzeyleri ölçülmüştür. Katılımcılara; MEB Bilgi ve Sistem Güvenliği Yönergesi, parolalar, sosyal ağlar ve e-posta konularında sorular yöneltilmiştir. Bazı konularda farkındalığın yüksek olduğu, bazı konularda ise yeterli bilinç düzeyinin oluşmadığı görülmüştür. Bir başka çalışmada Mart (2012) geliştirdiği anket formunu farklı meslek gruplarından 157'si öğretmen 501 katılımcıya uygulamış; öğretmenlerin bilgi güvenliği farkındalık düzeylerinin diğer meslek gruplarından farklı olmadığı sonucuna ulaşmıştır. Ölçek geliştirme çalışmalarından birinde Keser ve Güldüren (2015) örneklem olarak üniversitelerde görevli öğretim elemanlarını seçmiş ve bilgi güvenliği farkındalıklarını ortaya koymayı amaçlamıştır. Kaşıkçı, Çağıltay, Karakuş, Kurşun ve Ogan (2014) ise çalışmalarında ebeveynlerin sadece % 29'unun İnternet kullandığını, ancak bu düşük orana rağmen % 72'den fazlasının çocuklarının İnternet'te karşılaştıkları rahatsız edici durumlarda onlara yardım edebilecekleri konusunda kendilerine güvendiğini belirtmiştir. Ebeveynlerin çok az

bilgiye rağmen kendilerine bilgisizce güven duydukları söylenebilir. Çavuş ve Erçağ da (2016) öğretmenlerin güvenli İnternet kullanımına yönelik öz-yeterlik algılarını belirlemeyi hedeflemiştir. Gökmen ve Akgün (2015), Bilgisayar ve Öğretim Teknolojileri Eğitimi öğretmen adayların büyük çoğunluğunun, bilişim güvenliğini sağlamaya yönelik bir kurs veya ders almadıklarını, bilişim güvenliği konularını öğretebilme bakımından yeterli olmadıklarını belirlemiştir. Yılmaz, Yılmaz ve Sezer (2014) çalışmalarında farklı olarak, hem nicel hem de nitel verilerle çalışmış, eğitim fakültesi öğrencilerinin bilgi güvenliğine ilişkin davranış durumlarını ortaya koymak istemiştir. Bulgulara göre bilgi güvenliği eğitimlerinin gerekli olduğu vurgulanmıştır. Araştırmalardan da anlaşılacağı üzere öğretim görevlilerinin, öğretmenlerin, öğretmen adaylarının, velilerin ve hatta öğrencilerin veri güvenliğine yönelik farkındalıklarının belirlenmesi bir ihtiyaçtır.

Bilgi güvenliğinin sağlanması noktasında gerek donanım, gerekse yazılım destekli önlemler alınmaya çalışılsa da güvenliğin zayıf halkası çoğunlukla insan faktörüdür. Geliştirilen bu donanım ve yazılımları, veri güvenliğinin farkında olan bireyler bilinçli bir şekilde kullandığında çoğu veri kaybı önlenemez. Veri kaybının bireyler ve kurumlar için önemi, ekonomik ve hukuki boyutları dikkate alındığında dijital veri güvenliği konusunda gereken hassasiyetin gösterilmesi ve bireylerde farkındalık oluşturulması gerekmektedir. Özellikle de ülkemizde teknoloji kullanımının yaygınlaşması, bilişim teknolojilerinin eğitim öğretim ortamlarına entegrasyonu kapsamında geliştirilen projeler ve ayrılan bütçeler dikkate alındığında, öğretmenlerin dijital veri güvenliğine yönelik farkındalıklarının belirlenmesi gerekmektedir. MEB tarafından uygulamaya konan iki büyük projeden MEGP ve FATİH projesi kapsamında açılan kurslar ile yürütülen hizmet içi eğitim etkinlikleri incelendiğinde, öğretmenlerin diji-

tal veri güvenliğine yönelik farkındalıkları ile ilgili bir eğitim başlığına rastlanmamaktadır. Bu bağlamda öğretmenlerin farkındalıklarının ortaya konması bu araştırmayı önemli kılmaktadır.

Özetle bu araştırmanın amacı, MEB'e bağlı resmi ve özel okullarda görev yapan öğretmenlerin mevcut dijital veri güvenliğine yönelik farkındalıklarını ortaya koymak; farkındalık düzeylerinin cinsiyet, branş, görev yapılan öğrenim kademesi, mesleki deneyim, öğrenim durumu, günlük bilgisayar ve günlük İnternet kullanım süresi ve farklı teknolojilere sahip olma gibi değişkenlere göre değişip değişmediğini incelemektir.

## 2. YÖNTEM

Bu araştırmada öğretmenlerin dijital veri güvenliği konusundaki farkındalıklarını ortaya koyabilmek için tarama modelinden yararlanılmıştır. Bu model, bireylerin bir konu hakkındaki görüşlerine, tutumlarına, davranışlarına yönelik veri toplamak ve bu bireylerin konuya ilişkin genel yapısını ortaya koymak için kullanılmaktadır (Huck, 2012). Ayrıca öğretmenlerin dijital veri güvenliği farkındalıkları çeşitli değişkenlere göre incelenmiş, tarama modeline ek olarak nedensel karşılaştırmalı modellere özgü bazı analizlerden de yararlanılmıştır.

### 2.1 Evren ve Örneklem

Araştırmanın evreni, 2014-2015 eğitim-öğretim yılında Balıkesir ilindeki resmi ve özel okullarda görev yapan 12760 öğretmendir. İlkokul, ortaokul ve lise düzeyinde farklı okul türlerinde görev yapan öğretmenler arasından tabakalı örnekleme yöntemi ile belirlenmiş 1446 öğretmen ise araştırmanın örneklemini oluşturmuştur. Dağıtılan veri toplama araçlarının 870'i (% 60.2) yanıtlanmış bir biçimde geri dönmüştür.

Dönen veri toplama araçlarından 33'ü (% 4) uygun biçimde doldurulmadığından değerlendirilmeye alınmamıştır. Sonuç olarak analizler, 837 öğretmene ait veri toplama aracı ile gerçekleştirilmiştir.

Araştırma evreni için yüzde 95 güven aralığı ve yüzde 5 hata payı dikkate alındığında ulaşılması gereken örneklem büyüklüğü 373; yüzde 4 hata payı dikkate alındığında ise 573 olarak hesaplanmıştır. Analizlerin gerçekleştirildiği 837 katılımcıdan oluşan örneklem yüzde 95 güven aralığı ve yüzde 3.5 hata payı için gerekli olan 739 katılımcının da üzerinde olduğu görülmüş; mevcut örneklem Balıkesir iline genelleme yapabilmek için yeterli olduğu sonucuna varılmıştır (Bartlett, Kotrlık ve Higgins, 2001; Krejcie ve Morgan, 1970).

## 2.2 Veri Toplama Araç ve Teknikleri

Araştırma verilerinin toplanmasında kişisel bilgi formu ile birlikte Yılmaz'ın (2015) Dijital Veri Güvenliği Farkındalık Ölçeği (DVGFO) kullanılmıştır. Veri toplama aracının ilk bölümünde yer alan kişisel bilgi formunda öğretmenlerin cinsiyet, branş, görev yapılan öğrenim kademesi, mesleki deneyim, öğrenim durumu, günlük bilgisayar kullanım süresi, günlük İnternet kullanım süresi, bilgisayar, tablet bilgisayar veya akıllı telefon sahibi olma durumu bilgilerini belirlemek amacıyla 10 madde yer almaktadır.

Veri toplama aracının ikinci bölümündeki DVGFO, bir doktora tezi kapsamında Yılmaz (2015) tarafından geliştirilmiştir. Alanyazın taraması ve alan uzmanlarının görüşü ile geliştirilen formun pilot çalışması 79 öğretmen ile yapılmış; daha sonra 529 öğretmenle açımlayıcı faktör analizi, 335 farklı öğretmenle de doğrulayıcı faktör analizi gerçekleştirilmiştir. Tek faktörlü yapıya sahip ölçekteki maddelerin faktör yükleri .506 ile .689 arasında değişmektedir. İç tutarlılık katsayısı ( $\alpha=.945$ ) oldukça

yüksek olan ölçeğin açıkladığı toplam varyans % 36.053'tür. Tamamı olumlu ifadeler içeren ve farkındalığa ilişkin 32 maddeden oluşan ölçekteki ifadeler beşli Likert tipinde "Kesinlikle Katılıyorum (5)", "Katılıyorum (4)", "Kararsızım (3)", "Katılmıyorum (2)", "Kesinlikle Katılmıyorum (1)" biçimindedir. Ölçekten alınan toplam puan arttıkça dijital veri güvenliği farkındalığı da artmaktadır.

## 2.3 Veri Toplama Süreci

Kişisel bilgi formu ve DVGFO'den oluşan veri toplama aracının uygulanabilmesi için Balıkesir İl Milli Eğitim Müdürlüğü Araştırma Değerlendirme Komisyonu'ndan izin alınmıştır. Çoğaltılan veri toplama aracı, araştırma kapsamındaki 29 okula dağıtılarak 1446 öğretmene ulaştırılmıştır. Geri dönen veri toplama aracı sayısı 870, geri dönüş oranı % 60'tur. Ayrıca uygun biçimde doldurulmayan 33 veri toplama aracı elenmiş, analizler 837 öğretmene ait veriler ile gerçekleştirilmiştir.

## 2.4 Verilerin Analizi

Verilerin analizine başlamadan önce veri seti gözden geçirilmiş ve bazı kayıp değerler olduğu görülmüştür. Ölçekte yer alan maddelerin her birinde kayıp değerler % 5'in oldukça altında olduğu için boş hücreler aritmetik ortalama ile doldurulmuştur (Little ve Rubin, 2002). Yapılan analizlerde verilerin sola çarpık dağılım gösterdiği belirlenmiş ve ortalama puanların kareleri alınarak dönüştürme işlemi uygulanmıştır. Dönüştürme sonrasında elde edilen dağılım ölçüleri (çarpıklık -.396, basıklık -.061) daha sonraki parametrik testleri gerçekleştirebilmek için uygun bulunmuştur. Şöyle ki, çarpıklık ve basıklık değerleri -1 ile +1 değerleri arasında ise puanların normal dağılım gösterdiği söylenebilir ve parametrik testler kullanılabilir (Büyüköztürk, 2011; Huck, 2012).

Farkındalık bağlamında farklı bağımsız değişkenleri irdelerken; cinsiyet ve branşın yanı sıra

bilgisayar, tablet bilgisayar veya akıllı telefon sahibi olma durumu için bağımsız örneklem t-testi; görev yapılan öğrenim kademesi, mesleki deneyim, öğrenim durumu, günlük bilgisayar kullanım süresi ve günlük İnternet kullanım süresi için tek faktörlü ANOVA kullanılmıştır. ANOVA anlamlı çıktığında varyans eşleşliği şartının sağlanıp sağlanmamasına göre uygun olan çoklu karşılaştırma testi ile yola devam edilmiştir.

Uygulanan fark testlerinin tümünde, APA (2010) yazım rehberinin altıncı basımında raporlama gereği kesinlik kazanan etki büyüklükleri de hesaplanmış ve eta-kare ( $\eta^2$ ) değeri verilmiştir. Eta kare değeri .01-.06 arası ise küçük, .06 ve üzeri ise orta, .14 ve üzeri ise geniş etki olarak yorumlanmıştır (Cohen, 1988;

Huck, 2008). Yapılan analizlerde anlamlılık düzeyi .05 olarak alınmıştır. Verilerin çözümlenmesi ve değerlendirilmesinde SPSS 18.0 yazılımı kullanılmıştır.

### 3. BULGULAR

Bu bölümde, öncelikle demografik değişkenlere ait frekans ve yüzde dağılımları tartışılmış; ardından tüm farkındalık ifadelerine ilişkin betimsel değerler özetlenmiştir. Son olarak çalışmada dikkate alınan demografik değişkenlere göre dijital veri güvenliği farkındalığında yaşanan farklılıklara ilişkin analizlere yer verilmiştir.

#### 3.1 Demografik Bilgiler

Araştırmaya katılan 837 öğretmene ait kişisel özellikler Tablo 1’de özetlenmiştir.

**Tablo 1.** Katılımcı Özelliklerine İlişkin Frekans ve Yüzde Dağılımları

		f	%
Cinsiyet	Kadın	431	51.5
	Erkek	394	47.1
Branş	Sınıf Öğretmeni	152	18.2
	Branş Öğretmeni	669	79.9
Görev yapılan öğrenim kademesi	İlkokul	207	24.7
	Ortaokul	213	25.4
	Lise	417	49.8
Mesleki deneyim	0-4 yıl	21	2.5
	5-9 yıl	96	11.5
	10-14 yıl	141	16.8
	15-19 yıl	212	25.3
	20 yıl ve üzeri	339	40.5
Öğrenim durumu	Ön Lisans	64	7.6
	Lisans	690	82.4
	Yüksek Lisans	56	6.7
	Doktora	4	.5
Günlük bilgisayar kullanım süresi	Hiç Kullanmıyorum	31	3.7
	1-2 saat	528	63.1
	3-4 saat	166	19.8
	4 saatten fazla	89	10.6
Günlük İnternet kullanım süresi	Hiç Kullanmıyorum	30	3.6
	1-2 saat	561	67.0
	3-4 saat	131	15.7
Kendime ait bilgisayarım var	4 saatten fazla	78	9.3
	Evet	719	85.9
Tablet bilgisayarım var	Hayır	96	11.5
	Evet	399	47.7
Akıllı telefonum var	Hayır	400	47.8
	Evet	536	64.0
	Hayır	268	32.0

Öğretmenlerin cinsiyete göre dağılımı incelendiğinde, frekanslar birbirine yakın olmakla birlikte kadınların daha çok olduğu görülmektedir. Katılımcıların büyük çoğunluğu branş öğretmenidir. Dikkate alınan üç öğrenim kademesi arasında yalnızca ilkokullarda sınıf öğretmeni bulunduğundan branş öğretmenlerine göre sayılarının daha az olması normaldir. Görev yapılan öğrenim kademesi incelendiğinde katılımcıların yarısının lise öğretmeni olduğu görülmektedir.

Mesleki deneyime göre bir değerlendirme yapıldığında kıdem arttıkça bu kıdem basamağında yer alan katılımcı sayısının da arttığı görülmektedir. Hizmet puanına göre yer değiştirme isteği dikkate alındığında bu normal bir durumdur. Şöyle ki, Türkiye'nin en batısındaki illerden biri olan Balıkesir'deki öğretmenlerin hizmet puanına bağlı olarak mesleki deneyimleri de yıl olarak fazladır. Öğretmenlerin büyük bir bölümü lisans mezunu olup ön lisans ya da lisansüstü öğrenim gören öğretmen sayısı oldukça sınırlıdır.

Günlük bilgisayar kullanım süreleri incelendiğinde öğretmenlerin yüzde dördünden daha azının hiç bilgisayar kullanmadığı görülmektedir. İnternet kullanımına ilişkin bulgular da bu çıkarım ile paraleldir. Haftada 15 ila 30 saat

arasında derse giren öğretmenlerin ders planlamaya, yazılı sınavları ve performans ödevlerini değerlendirmeye ayırdıkları süreler dikkate alındığında günlük bilgisayar ve İnternet kullanımına çoğunlukla 4 saatten az zaman ayırdıkları söylenebilir.

Araştırmaya katılan öğretmenlerin büyük bir bölümü kişisel bilgisayara sahiptir. Yine tablet bilgisayar ya da akıllı telefona sahip olanların oranı oldukça yüksektir. FATİH projesi kapsamındaki okullarda görev yapan öğretmenlere MEB tarafından ücretsiz tablet bilgisayar verilmesi bu oranları etkilemiş olabilir. Bununla birlikte günümüzde mobil cihaz kullanımının hızla artmasının sonucu olarak öğretmenlerin de çoğunlukla akıllı telefona sahip olduğu görülmektedir.

### 3.2 Betimsel İstatistikler

Veri toplama aracının ikinci bölümünü oluşturan DVGfÖ maddelerine ilişkin betimsel istatistikler Tablo 2'de verilmiştir. Dijital veri güvenliğine ilişkin gereksinim analizi yapmak isteyen öğretim tasarımcılarına hangi konularda eksiklik olduğu konusunda yardımcı olabilmek için ölçekte yer alan göstergeler, en yüksek ortalamadan en düşük ortalamaya doğru sıralanmıştır.

**Tablo 2.** DVGfÖ Maddelerine İlişkin Tanımlayıcı İstatistikler

Ölçek Maddesi	$\bar{X}$	SS
2. Parola oluştururken harf, sayı ve özel karakter kullanmanın önemini bilirim.	4.44	.84
13. Parola hatırlatmak için kullanılan güvenlik sorularına başkalarının tahmin edemeyeceği cevaplar verilmesi gerektiğini bilirim.	4.41	.78
8. E-posta ile gelen kimlik bilgilerini doğrulama mesajlarına (parola, kredi kartı vb.) itibar edilmemesi gerektiğini bilirim.	4.41	.83
14. Parola oluştururken karakter sayısının fazla olmasının önemini bilirim.	4.38	.78
12. Antivirüs yazılımı kullanmanın önemini bilirim.	4.35	.82
28. Cep telefonuna gelen tek kullanımlık parola ile yapılan giriş işlemlerinin, güvenliği arttırdığını bilirim.	4.35	.86
10. Güvenli olmadığını düşündüğüm e-postaları açmadan silmeye dikkat ederim.	4.34	.86
15. Parolaların herhangi bir ortamda saklanması güvenlik riski oluşturacağına farkındayım.	4.32	.81
18. Başkalarının tahmin edemeyeceği parolalar oluşturmaya dikkat ederim.	4.32	.84



30. İnternet sitelerinde kullanıcı oturumunu kapatırken “güvenli çıkış” bağlantısını kullanmanın önemini bilirim.	4.31	.92
3. Farklı işlemler için farklı parola kullanmanın önemini bilirim.	4.29	.86
25. Kendime ait olmayan cihazlarda, parola gerektiren işlemler yapmamaya dikkat ederim.	4.27	.81
24. İzinsiz kullanılmaması için cihazlara (akıllı telefon, tablet, bilgisayar vb.) parola konulabileceğinin farkındayım.	4.27	.86
9. Taşınabilir depolama birimlerini (Flash bellek, taşınabilir sabit disk) kullanmadan önce virüs taraması yapılması gerektiğini bilirim.	4.25	.87
17. Üzerinde çalışma yapılan dosyaların birden fazla ortamda yedeklenmesi gerektiğini bilirim.	4.21	.88
26. İşletim sisteminin (Windows, Android vb.) güvenlikle ilgili uyarılarını dikkate alırım.	4.19	.85
27. Elektrik kesintisine karşı dizüstü bilgisayarları bataryası ile kullanmanın önemini bilirim.	4.17	.90
11. Programların, üreticinin kendi sitesinden indirilmesinin önemini bilirim.	4.13	.90
4. İzinsiz kullanılmaması için dosyalara parola konulabileceğinin farkındayım.	4.12	.92
6. Flash bellekleri, veri saklamak yerine sadece veri taşımak için kullanmanın farkını bilirim.	4.12	.97
32. Lisanslı olmayan yazılımların güvenlik açıkları oluşturabileceğinin farkındayım.	4.06	.96
20. Taşınabilir depolama birimlerini (Flash bellek, taşınabilir sabit disk) “Donanımı Güvenle Kaldır” seçeneğini kullanarak çıkartmaya dikkat ederim.	4.05	1.03
22. Parolaların belirli aralıklarla değiştirilmesi gerektiğinin farkındayım.	4.01	.97
29. Sanal klavye kullanmanın önemini bilirim.	3.94	1.06
7. İşletim sisteminin (Windows, Android vb.) güncel olmasına dikkat ederim.	3.93	1.00
1. Zararlı yazılımlar (virüs, solucan, truva atı vb.) konusunda bilgi sahibiyim.	3.91	1.11
23. Almak istemediğim çöp e-postaları “spam/gereksiz/önemsiz” olarak işaretlemeye dikkat ederim.	3.90	1.04
19. İnternet adres çubuğunda yanlış yönlendirme olup olmadığına dikkat ederim.	3.87	1.03
21. Karmaşık yapıdaki parolaların kırılabileceğini bilirim.	3.80	1.09
16. Verilerin, çeşitli uygulamalar (Dropbox, Google Drive vb.) kullanılarak İnternet ortamında saklanabileceğini bilirim.	3.69	1.13
31. İnternet sitelerinde kullanılan güvenlik sertifikaları hakkında bilgi sahibiyim.	3.64	1.11
5. Güvenlik duvarı yazılımları konusunda bilgi sahibiyim.	3.36	1.23
<b>Genel ortalama</b>	<b>4.16</b>	<b>2.15</b>

5 puan üzerinden değerlendirilen her bir maddeye göre ölçekten alınan ortalama puan 4.16'dır. Bu da öğretmenlerin dijital veri güvenliği konusundaki farkındalıklarını “Katılıyorum” düzeyine çok yakın ifade ettiklerini göstermektedir. Ölçekte yer alan maddeler bireysel olarak incelendiğinde, ortalama puanların 3.36 ile 4.44 arasında değiştiği görülmektedir. Örneğin 2. madde en yüksek ortalama puanı ( $\bar{X}=4.44$ ,  $SS=.84$ ) sahiptir. Buna göre öğretmenler parola oluştururken harf, sayı ve özel karakter kullanmanın önemi konusunda yüksek farkındalı-

ğa sahiptir. Yüksek ortalama puanı sahip diğer iki madde ise; 8. madde ( $\bar{X}=4.41$ ,  $SS=.83$ ) ve 13. maddedir ( $\bar{X}=4.41$ ,  $SS=.78$ ). Buna göre öğretmenler, e-posta ile gelen kimlik bilgilerini doğrulama mesajlarına (parola, kredi kartı vb.) itibar edilmemesi gerektiğinin ve parola hatırlatmak için kullanılan güvenlik sorularına başkalarının tahmin edemeyeceği yanıtlar verilmesi gerektiğinin farkındadır denilebilir.

Ölçekteki en düşük ortalama puanı ( $\bar{X}=3.36$ ,  $SS=1.23$ ) sahip 5. maddeye göre öğretmenlerin güvenlik duvarı yazılımları konusundaki far-

kındalıkları diğer maddelere göre en azdır. Düşük ortalamaya sahip diğer iki madde ise; 31. madde ( $\bar{X}=3.64$ ,  $SS=1.11$ ) ve 16. maddedir ( $\bar{X}=3.69$ ,  $SS=1.13$ ). Buna göre öğretmenlerin, İnternet sitelerinde kullanılan güvenlik sertifikaları ve verilerin çeşitli uygulamalar (Drop-box, Google Drive vb.) kullanılarak İnternet ortamında saklanabileceği konularındaki farkındalıkları daha düşüktür.

**Tablo 3.** Dijital Veri Güvenliği Farkındalığının Cinsiyete Göre Karşılaştırılması

Cinsiyet	N	$\bar{X}$	SS	sd	t	p
Kadın	431	4.10	2.15	823	-3.393	<.001
Erkek	394	4.23	2.13			

Tablo 3'e göre kadınların ve erkeklerin ölçekten aldıkları ortalama puanlar arasında cinsiyete göre istatistiksel olarak anlamlı bir fark olduğu görülmektedir [ $t_{(823)}=-3.393$ ,  $p<.05$ ,  $\eta^2=.014$ ]. Erkeklerin dijital veri güvenliği farkındalıklarının kadınlara göre daha yüksek olduğu söylenebilir. Bu farka ilişkin hesaplanan etki büyüklüğü değeri ise küçük bir etkiye işaret etmektedir.

### 3.3.2 Branş

Öğretmenlerin dijital veri güvenliği farkındalıklarının branşa göre fark gösterip göstermediğine ilişkin yapılan bağımsız örneklem t-testi sonucunda sınıf öğretmenleri ( $\bar{X}=4.14$ ,  $SS=2.18$ ) ile branş öğretmenleri ( $\bar{X}=4.17$ ,  $SS=2.14$ ) arasında istatistiksel olarak anlamlı bir fark gözlemlenmemiştir [ $t_{(819)}=-.583$ ,  $p=.56$ ]. Bu durum, MEB tarafından öğretmenlere sunulan, öğretim etkinliklerinde teknoloji kullanımına yönelik hizmet içi eğitim seminerlerinin branş ayrımı yapılmaksızın tümüne zorunlu olarak uygulanması ile açıklanabilir.

### 3.3.3 Öğrenim Kademesi

Öğretmenlerin dijital veri güvenliği farkındalıklarının görev yaptıkları öğrenim kademesine göre değişip değişmediğine ilişkin yapılan bağımsız gruplar için tek faktörlü ANOVA

## 3.3 Demografik Değişkenler Bazında Gerçekleştirilen Fark Analizleri

### 3.3.1 Cinsiyet

Öğretmenlerin dijital veri güvenliği farkındalıklarının cinsiyete göre fark gösterip göstermediğine ilişkin yapılan bağımsız örneklem t-testi sonuçları Tablo 3'te verilmiştir.

sonucunda istatistiksel olarak anlamlı bir fark gözlemlenmemiştir [ $F_{(2-834)}=1.347$ ,  $p=.261$ ]. FA-TİH projesi liselerden başlanarak ortaokullara, daha sonra da ilkokullara uygulanacağından ilgili proje Balıkesir ilinde bugüne kadar henüz yalnızca liselerde hayata geçirilmiş ve bu kapsamda lise öğretmenleri "Güvenli İnternet Kullanımı" kursuna katılmıştır. Buna rağmen araştırmaya katılan lise öğretmenlerinde dijital veri güvenliği farkındalığı konusunda bir fark oluşmadığı söylenebilir.

### 3.3.4 Mesleki Deneyim

Öğretmenlerin dijital veri güvenliği farkındalıklarının mesleki deneyimlerine göre fark gösterip göstermediğine ilişkin yapılan bağımsız gruplar için tek faktörlü ANOVA sonucunda istatistiksel olarak anlamlı bir bulguya ulaşılamamıştır [ $F_{(4-804)}=.839$ ,  $p=.500$ ]. Teknolojinin son yıllardaki hızlı değişimi ile eğitim öğretim ortamlarında bilişim teknolojilerinin kullanımı hızla artarken bu teknolojileri genç neslin daha etkili kullandığı düşünülmektedir (Prensky, 2001). Oysa mevcut bulgulara göre dijital veri güvenliği farkındalığının öğretmenlik mesleğinde geçirilen yıla göre değişmediği görülmüştür.

### 3.3.5 Öğrenim Durumu

Öğretmenlerin dijital veri güvenliği farkındalıklarının öğrenim durumuna göre fark gösterip göstermediğine ilişkin yapılan bağımsız gruplar için tek faktörlü ANOVA da istatistiksel olarak anlamlı bir sonuç üretmemiştir [ $F_{(3-810)}=.183$ ,  $p=.908$ ]. Daha önceleri ön lisans mezunu olarak mesleğe başlayan ve halen sürdüren öğretmenler olsa da, günümüzde en az lisans mezunu olan öğretmenler Milli Eğitim Bakanlığı'na bağlı okullarda görev yapmakta, mevcut

örnekleme göre çok azı lisansüstü öğrenime yönelmektedir. Bununla birlikte öğrenim durumunun öğretmenlerin dijital veri güvenliği farkındalıkları üzerinde bir fark yaratmadığı söylenebilir.

### 3.3.6 Bilgisayar ve İnternet Kullanım Süresi

Öğretmenlerin dijital veri güvenliği farkındalıklarının günlük bilgisayar kullanım süresine göre fark gösterip göstermediğine ilişkin yapılan bağımsız gruplar için tek faktörlü ANOVA sonuçları Tablo 4'te verilmiştir.

**Tablo 4.** Dijital Veri Güvenliği Farkındalığının Günlük Bilgisayar Kullanım Süresine Göre Karşılaştırılması

Varyansın Kaynağı	Kareler Toplamı	sd	Kareler Ortalaması	F	P	Anlamlı Fark
Gruplar arası	1073.851	3	357.950	17.758	<.001	3,4>2>1
Gruplar içi	16327.723	810	20.158			
Toplam	17401.574	813				

(1=Hiç kullanmıyorum, 2=1-2 saat, 3=3-4 saat, 4=4 saatten çok)

Tablo 4'te özetlenen bulgular incelendiğinde, günlük bilgisayar kullanım süresi arttıkça farkındalık düzeylerinin de anlamlı bir biçimde arttığı söylenebilir [ $F_{(3-810)}=17.758$ ,  $p<.05$ ,  $\eta^2=.062$ ]. Gruplar arasındaki farklılığı ortaya koyabilmek için yapılan Scheffe testi sonucunda; hem günde 4 saatten çok, hem de günde 3-4 saat bilgisayar kullananların, günde 1-2 saat bilgisayar kullananlardan; günde 1-2 saat bilgisayar kullananların da hiç kullanmayanlardan

dijital veri güvenliği konusunda daha farkında oldukları görülmektedir. Buna göre günlük bilgisayar kullanım süresi arttıkça dijital veri güvenliği farkındalığının da arttığı söylenebilir.

Benzer bir biçimde öğretmenlerin dijital veri güvenliği farkındalıklarının günlük İnternet kullanım süresine göre fark gösterip göstermediğine ilişkin yapılan ANOVA sonuçları da istatistiksel olarak anlamlı bulunmuş ve Tablo 5'te özetlenmiştir [ $F_{(3-796)}=19.453$ ,  $p<.05$ ,  $\eta^2=.068$ ].

**Tablo 5.** Dijital Veri Güvenliği Farkındalığının Günlük İnternet Kullanım Süresine Göre Karşılaştırılması

Varyansın Kaynağı	Kareler Toplamı	sd	Kareler Ortalaması	F	p	Anlamlı Fark
Gruplar arası	1168.129	3	389.376	19.453	<.001	3,4>1,2
Gruplar içi	15932.576	796	20.016			
Toplam	17100.705	799				

(1=Hiç kullanmıyorum, 2=1-2 saat, 3=3-4 saat, 4=4 saatten fazla)

Gruplar arasındaki farklılığı ortaya koyabilmek için, varyans eşleşliği şartı sağlanmadığından

Dunnett C yapılmıştır. Test sonucunda; hem günde 4 saatten çok, hem de günde 3-4 saat

İnternet kullananların; hem günde 1-2 saat bilgisayar kullananlardan, hem de hiç kullanmayanlardan dijital veri güvenliği konusunda daha farkında oldukları görülmektedir. Buna göre günlük İnternet kullanım süresi günde 3 saatin üzerine çıktığında dijital veri güvenliği farkındalığının da arttığı söylenebilir. Günlük bilgisayar ve İnternet kullanım sürelerine ilişkin veriler birbiriyle oldukça paralel olduğu için Tablo 4 ve Tablo 5'te yer alan analizlerin benzer bir biçimde sonuçlanması oldukça normaldir. Her iki analizde bulunan anlamlılık

düzeyini değerlendirmek için hesaplanan etki büyüklüğü değerleri ise orta düzeyde bir etkiye işaret etmektedir.

### 3.3.7 Farklı Teknolojilere Sahip Olma

Öğretmenlerin dijital veri güvenliği farkındalıklarının kişisel bilgisayar, tablet bilgisayar ya da akıllı telefon sahibi olma durumlarına göre farklılık gösterip göstermediğine ilişkin 3 farklı t testi yapılmış ve bu testler Tablo 6'da özetlenmiştir.

**Tablo 6.** Dijital Veri Güvenliği Farkındalığının Farklı Teknolojilere Sahip Olma Durumlarına Göre İncelenmesi

Kişisel bilgisayar	N	$\bar{X}$	SS	sd	t	p
Evet	719	4.19	2.13	813	4.562	<.001
Hayır	96	3.91	2.20			
Tablet bilgisayar	N	$\bar{X}$	SS	sd	t	p
Evet	399	4.23	2.14	797	3.930	<.001
Hayır	400	4.08	2.15			
Akıllı telefon	N	$\bar{X}$	SS	sd	t	p
Evet	535	4.19	2.14	801	2.561	.011
Hayır	268	4.09	2.18			

Tablo 6'da görüldüğü üzere kişisel bilgisayar, tablet bilgisayar ya da akıllı telefona sahip olan öğretmenlerin bu teknolojilere sahip olmayan öğretmenlere göre farkındalık düzeyleri anlamlı derecede daha yüksektir. Etki büyüklüğü değerleri kişisel bilgisayar için .025, tablet bilgisayar için .019, akıllı telefon için .008 biçiminde hesaplanmıştır. Kendine ait bir bilgisayarı olan öğretmenlerin daha çok dijital veri üretmeleri, bilgisayarlarında kişiye özel veri saklamaları ve bunların güvenliğini sağlayabilmek adına farkındalıklarının yüksek olması normal karşılanabilir. Ayrıca İnternet bağlantısı olan mobil cihazlar, veri güvenliği noktasında bir tehdit oluşturmaktadır ve bireyler mobil cihazlarındaki kayıtlı parolalar, fotoğraflar ve dokümanlar konusunda endişe duymaktadır. Bu nedenlerle tablet bilgisayarı veya akıllı telefonu olan

öğretmenlerin dijital veri güvenliği farkındalıkları, bu teknolojilere sahip olmayan öğretmenlere göre daha yüksek çıkmış olabilir.

## 4. TARTIŞMA, SONUÇ VE ÖNERİLER

Bu çalışmada Balıkesir ilindeki öğretmenlerin dijital veri güvenliği farkındalıklarını belirlemek için DVGfÖ kullanılarak toplanan veriler analiz edilmiştir. Bununla birlikte bazı demografik değişkenlere ilişkin tanımlayıcı istatistikler ve bu değişkenler ile dijital veri güvenliği farkındalığı arasındaki ilişkiler de dikkate alınmıştır.

Öğretmenlerin dijital veri güvenliği farkındalıkları oldukça yüksek bulunmuştur. Elbette bu bulguların öz bildirimine dayalı olduğu dikkate

alınmalıdır. En yüksek ortalama puan ile öne çıkan başlıca maddeler dikkate alındığında; öğretmenler, parola oluştururken harf, sayı ve özel karakter kullanmanın önemi, e-posta ile gelen kimlik bilgilerini doğrulama mesajlarına itibar edilmemesi ve parola hatırlatmak için kullanılan güvenlik sorularına başkalarının tahmin edemeyeceği yanıtlar verme konularında yüksek farkındalığa sahiptir. Öte yandan Kruger, Drevin ve Steyn (2010) araştırmalarına katılan üniversite öğrencilerinin %48'inin "güçlü parola" kavramının ne anlama geldiğini bilmediğini belirlemiştir. Bu bağlamda öğretmenlerin parola konusundaki farkındalıklarının yüksek olması dikkat çekicidir. Yüksek farkındalık oranına sahip bir başka madde ise antivirüs yazılımı kullanmanın önemi ile ilgilidir. Benzer şekilde Yılmaz vd. (2014) çalışmalarında, üniversite öğrencilerinin %85'inin antivirüs yazılımı kullandığını ve %86'sının bu yazılımları güncellediğini belirlemiştir.

Ölçekteki en düşük ortalama puanına sahip maddeler dikkate alındığında; öğretmenlerin güvenlik duvarı yazılımları, İnternet sitelerinde kullanılan güvenlik sertifikaları ve verilerin çeşitli uygulamalar kullanılarak İnternet ortamında güvenle saklanabileceği konularındaki farkındalıkları daha düşüktür. Tekerek ve Tekerek (2013) öğrenciler ile gerçekleştirdiği çalışmasında benzer bir sonuca ulaşmıştır. Buna göre öğrencilerin; zararlı yazılım denetlemesi, dijital ortamda belge koruma, kişisel bilgisayar güvenliği, güvenlik duvarı ve filtreleme yazılımları kullanımı konularında farkındalık düzeylerinin çok düşük olduğu belirlenmiştir.

Şahinaslan, Şahinaslan, Borandağ ve Şahinaslan (2013) güvenlik duvarının önemine dikkat çekerek; İnternet üzerinden gelebilecek yetkisiz kaynak erişimlerini engellediğini, son kullanıcı ve sistemleri korumada bir süzgeç görevi gördüğünü, ağ trafiği üzerinde güvenlik riskine karşı ilk savunma hattı olduğunu belirtmiştir.

Öte yandan mevcut bulgular, bu konudaki farkındalığın ciddi düzeyde düşük olduğunu göstermektedir. Şöyle ki ortalama puanı en düşük olan ölçek maddesine göre öğretmenlerin farkındalıklarının en düşük olduğu konu güvenlik duvarı yazılımlarıdır. Tüm bu farkındalık ifadeleri hakkındaki ortalamaların potansiyel hizmet içi eğitimlerde hedef kitlenin gereksinimlerini belirleme bağlamında kullanılabilmesi mümkündür.

Araştırmada erkeklerin kadınlara göre dijital veri güvenliği farkındalıkları daha yüksek bulunmuştur. Alanyazında farklı sonuçlara ulaşan araştırmalar bulunmaktadır. Mart (2012), farklı meslek gruplarından oluşan 501 katılımcı ile gerçekleştirdiği çalışmasında, bilgi güvenliği farkındalığı bağlamında cinsiyete göre anlamlı bir fark bulmuş; ancak kadınların erkeklere göre karşılaşılabilecekleri tehlikelerden daha haberdar oldukları sonucuna ulaşmıştır. Buna göre öğretmenlik mesleğinde bilgi güvenliği farkındalığı söz konusu olduğunda, erkeklerin farkındalığı daha yüksek iken sağlık personeli, mühendis, avukat gibi farklı meslek gruplarında kadınların farkındalıklarının daha yüksek olduğu söylenebilir. Cinsiyete göre farklılığın araştırıldığı bir başka çalışmada Tekerek ve Tekerek (2013) ilköğretim ve lise öğrencilerinin bilgi güvenliği farkındalıklarını incelemiş ve kız öğrencilerin, erkek öğrencilere göre anlamlı şekilde daha olumlu görüşe sahip olduklarını ortaya koymuştur. Mühendislik fakültesi öğrencilerinden oluşan 218 katılımcı ile çalışan Arıtürk (2015), bilgi güvenliği ve bilgi farkındalığı durumlarını incelemiş, kadınların erkeklere göre bilgi güvenliği ve bilgi farkındalığı konusundaki tutumlarının daha yüksek olduğunu gözlemlemiştir. Öte yandan öğrenci ve öğretmenler arasında ya da farklı meslekler arasındaki farklara ilişkin söz konusu çıkarımları destekleyecek yeni araştırmalara gereksinim vardır.

Araştırma sonunda ulaşılan bir başka sonuç, sınıf öğretmenleri ile branş öğretmenleri arasında dijital veri güvenliği farkındalığı konusunda istatistiksel olarak anlamlı bir fark bulunmadığıdır. Dijital veri güvenliği farkındalığına ilişkin yeterli sayıda benzer çalışma olmadığından bu bulgu, teknolojiye yönelik tutum çalışmaları ile paralel bir biçimde değerlendirilebilir. Çünkü Kağıtçıbaşı'na göre (1999) farkındalık, tutumlara ulaşmayı kolaylaştırmakta ve farkındalık yükseldikçe ilgili tutumun ne olduğu daha iyi bilinmekte, bu tutumlar belleğe daha kolay çağrılarak davranışları daha kolay etkilemektedir. Örneğin, Oktay ve Çakır (2012) öğretmenlerin teknolojiye yönelik tutumlarının, Çelik ve Bindak ise (2005) öğretmenlerin bilgisayara yönelik tutumlarının branşa göre değişmediğini belirlemiştir. Bu çalışmada dikkate alınan dijital veri güvenliği farkındalığı da branş bağlamında bu tür tutum çalışmaları ile paralellik göstermiştir.

Öğretmenlerin dijital veri güvenliği farkındalıkları, görev yapılan öğrenim kademesine göre de değişmemektedir. Bir başka deyişle ilkokul, ortaokul ve lise öğretmenlerinin dijital veri güvenliği farkındalıkları arasında istatistiksel olarak anlamlı bir fark yoktur. İlköğretim ve lise öğrencileri örneğinde çalışan Tekerek ve Tekerek (2013) öğrenim kademesine göre bilgi güvenliği farkındalığını incelediğinde, lisede öğrenim gören öğrencilerin ilköğretim öğrencilerine göre anlamlı şekilde daha yüksek farkındalığa sahip olduğunu belirlemiştir. Yani öğrenim kademesine göre öğrencilerde gözlemlenen farkındalık değişimi, öğretmenlerde söz konusu olmamıştır. Öte yandan benzer çalışmaların öğretmen adayları ve kıdemli öğretmenler arası karşılaştırmalarla yinelenmesi, öğrenim kademesi değişkeninin etkisini daha iyi görmeyi kolaylaştırabilir.

Araştırma sonuçlarına göre öğretmenlerin dijital veri güvenliği farkındalıklarının fark

göstermediği diğer bir bağımsız değişken mesleki deneyimdir. Şöyle ki, öğretmenlerin meslekte geçirdiği yılların az ya da çok olması farkındalıklarında anlamlı fark oluşturmamaktadır. Alanyazında farklı sonuçlara ulaşan çalışmalar da bulunmaktadır. Mart (2012) yaş değişkenini incelemiş ve 25-34 yaş arasındaki öğretmenlerin bilgi güvenliği konusunda yeterli kaldıklarını ve bunun için farkındalık eğitimlerine gereksinim duyduklarını belirtmiştir. Tutum bağlamında bir değerlendirme yapan Oktay ve Çakır (2012) ilköğretim öğretmenlerinden 0-9 yıl arasında mesleki deneyime sahip olanların teknolojiye karşı tutumlarının diğerlerinden daha yüksek olduğu sonucuna ulaşmıştır. Bu bağlamda daha geniş örneklerle yeni araştırmalar gerçekleştirmekte ve mesleki deneyim değişkenini yeniden irdelemekte yarar vardır.

Öğrenim durumu dikkate alındığında da durum aynıdır. Öğretmenlerin dijital veri güvenliği farkındalıkları öğrenim durumlarına göre değişmemektedir. Bu sonucu destekleyen Mart'ın (2012) çalışmasında katılımcıların eğitim durumlarının bilgi güvenliği farkındalıkları üzerinde anlamlı bir etkisi olmadığı bulunmuştur. Oktay ve Çakır (2012) ise bu sonuçlardan farklı olarak ön lisans mezunu öğretmenlerin teknolojiye karşı tutumlarının, hem lisans hem de yüksek lisans mezunu öğretmenlerden daha düşük olduğunu bulmuştur. Bu bağlamda öğrenim durumunun etkisini daha iyi görebilmek için dijital veri güvenliği farkındalığına odaklanan ve temsil gücü yüksek örneklerle gerçekleştirilmiş yeni çalışmalara gereksinim duyulmaktadır.

Araştırmada günlük bilgisayar kullanım süreleri incelendiğinde; günde 3 saatten fazla bilgisayar kullanan öğretmenlerin 1-2 saat bilgisayar kullananlardan, günde 1-2 saat bilgisayar kullananların da hiç kullanmayanlardan dijital veri güvenliği farkındalıklarının daha yüksek

olduğu belirlenmiştir. Bir başka deyişle günlük bilgisayar kullanım süresi arttıkça dijital veri güvenliği farkındalığı da artmaktadır. Alanyazında farklı sonuçlara ulaşan araştırmalar da yer almaktadır. Örneğin, Mart (2012) katılımcıların bilgi güvenliği farkındalıklarının bilgisayar kullanım sürelerine bağlı olarak anlamlı bir şekilde değişmediği sonucuna ulaşmıştır.

Günlük İnternet kullanım süreleri incelendiğinde ise, günde 3 saatten çok İnternet kullanan öğretmenlerin hem günde 1-2 saat İnternet kullananlardan, hem de hiç kullanmayanlardan dijital veri güvenliği konusunda daha yüksek farkındalıkları olduğu görülmüştür. Mart'ın (2012) çalışmasında ise bu araştırmanın sonucundan farklı olarak katılımcıların bilgi güvenliği farkındalıklarının İnternet kullanım sürelerine bağlı olarak anlamlı bir şekilde değişmediği ortaya konmuştur. Bu araştırma ile Mart'ın (2012) çalışması birlikte ele alındığında günlük bilgisayar ve İnternet kullanım sürelerine ilişkin iki zıt bulgu ile karşılaşmaktadır. Bu da söz konusu değişkeni dikkate alan yeni araştırmalar gerçekleştirilmeden güçlü çıkarımlardan kaçınılması gerektiğini göstermektedir.

Araştırmada son olarak katılımcıların sahip oldukları bilişim cihazlarına göre dijital veri güvenliği farkındalıkları incelenmiştir. Buna göre; kişisel bilgisayarı, tablet bilgisayarı veya akıllı telefonu olan öğretmenlerin bu cihazlara sahip olmayanlara göre farkındalıklarının daha yüksek olduğu görülmüştür. Alanyazında tutum konusuna odaklanan çalışmalar, paralel sonuçlar ortaya koymuştur. Örneğin, Çelik ve Bindak'ın (2005) araştırmasında bilgisayarı olan öğretmenlerin bilgisayara yönelik olumlu tutumları, olmayanlara göre daha yüksek bulunmuştur. Belli teknolojilere sahip olmanın gerek bu teknolojilere ilişkin tutum, gerekse farkındalık üzerinde etkili olması beklenen bir durumdur.

Öğretmenlerin dijital veri güvenliği farkındalıklarını yordayan değişkenler genel olarak incelendiğinde; branş, görev yapılan öğrenim kademesi, mesleki deneyim ve öğrenim durumu değişkenlerinin anlamlı bir fark oluşturmadığı bulunmuştur. Buna karşın cinsiyet, günlük bilgisayar kullanım süresi, günlük İnternet kullanım süresi ile kişisel bilgisayar, tablet bilgisayar veya akıllı telefon gibi bilişim cihazlarına sahip olmanın dijital veri güvenliği farkındalığını olumlu etkilediği sonucuna ulaşılmıştır. Araştırma sonuçları göstermektedir ki, öğretmenlerin dijital veri güvenliği farkındalıklarını etkileyen değişkenler; meslekleri ile ilgili özellikleri değil, bilişim cihazlarına sahip olma durumları ve bu teknolojileri kullanma süreleridir.

Dijital veri güvenliğine yönelik tehditlerin ortadan kaldırılmasında en kritik unsur insandır. Bu konuda yaşanan sorunların tamamen ortadan kaldırılabilmesi ya da en aza indirilebilmesi için özellikle okullarda ve toplum genelinde dijital veri güvenliği farkındalık eğitimleri verilmeli, bilinçlendirme çalışmaları yapılmalı ve farkındalığı arttıracak projeler yapılandırılmalıdır. Bu konuda, devlete ve özel sektöre, sivil toplum kuruluşlarına, yazılı ve görsel basına, üniversitelere ve okullara büyük sorumluluklar düşmektedir. Bireylerde dijital veri güvenliği farkındalığı yaratabilmek için küçük yaşlardan itibaren eğitim verilmelidir. Bilişim Teknolojileri dersi öğretim programına ve ders kitaplarına konu ile ilgili içerik eklenmelidir. Öğretmenlerde ve eğitim yöneticilerinde hizmet içi eğitim seminerleri ile farkındalık bilinci oluşturulmalıdır. Bu seminerlerde özellikle veri güvenliği ile ilgili bilişim teknolojileri alanına özgü kavramlara ağırlık verilmelidir. Bu sayede toplumun geleceğinin şekillenmesinde önemli bir role sahip olan öğretmenler; hem öğrencilerine yol gösterebilecek, hem de kendilerine ait dijital verilerin güvenliğini sağlayabilecektir.

Sonuç olarak dijital veri güvenliği, bilişim teknolojilerini kullanan her bireyin bilmesi ve dikkat etmesi gereken bir konudur. Kötü niyetli kişiler tarafından verilerin kolaylıkla ele geçirilip kullanılabilmesi dikkate alınrsa, ülkemizdeki kişi, kurum ve kuruluşların bu konuda gereken hassasiyeti göstermeleri, gerekli önlemleri almaları, yeni yaklaşımları yakından takip ediyor olmaları gerekmektedir. Yapılacak yasal düzenlemeler ile pek çok dijital veri güvenliği sorununun önüne geçebilmek müm-

kündür. İleride yapılacak araştırmalarda dijital veri güvenliği farkındalığına etkisi olabilecek farklı değişkenler irdelenebilir. Farklı örneklemelerden elde edilecek sonuçlar bu araştırmanın sonuçları ile karşılaştırılabilir. Son olarak, dijital veri güvenliği farkındalığına ilişkin göstergeler bağlamında bu çalışmada ortaya çıkan tablo dikkate alınarak eksiklik gözlemlenen konulara göre uygun farkındalık artırma etkinlikleri düzenlenebilir.

### Kaynakça

- Acar, N. V. (2004). *Ne kadar farkındayım: Gestalt terapi (2. Baskı)*. Ankara: Babil Yayınevi.
- American Psychological Association (APA). (2010). *Publication manual of the American Psychological Association (6. Baskı)*. Washington DC: Author.
- Arıtürk, M. (2015). Bilgi farkındalığı ve bilgi güvenliğinin karşılaştırılması. XVII. Akademik Bilişim Konferansı, 4-6 Şubat 2015, Anadolu Üniversitesi, Eskişehir.
- Bartlett, J. E., Kotrlik, J. W. ve Higgins, C. C. (2001). Organizational research: Determining appropriate sample size in survey research. *Information Technology, Learning, and Performance Journal*, 19(1), 43-50.
- Büyüköztürk, Ş. (2011). *Sosyal bilimler için veri analizi el kitabı (14. Baskı)*. Ankara: Pegem Akademi.
- Canbek, G. ve Sağıroğlu, Ş. (2006). Bilgi, bilgi güvenliği ve süreçleri üzerine bir inceleme. *Politeknik Dergisi*, 9(3), 165-174.
- Chou, C. ve Peng, H. (2011). Promoting awareness of Internet safety in Taiwan in-service teacher education: A ten-year experience. *Internet and Higher Education*, 14, 44-53.
- Cohen, J. W. (1988). *Statistical power analysis for the behavioral sciences (2. baskı)*. Hillsdale, NJ: Lawrence Erlbaum Associates.
- Çavuş, N. ve Erçağ, E. (2016). The scale for the self-efficacy and perceptions in the safe use of the Internet for teachers: The validity and reliability studies. *British Journal of Educational Technology*, 47(1), 76-90.
- Çelik, H. C. ve Bindak, R. (2005). İlköğretim okullarında görev yapan öğretmenlerin bilgisayara yönelik tutumlarının çeşitli değişkenlere göre incelenmesi. *İnönü Üniversitesi, Eğitim Fakültesi Dergisi*, 6(10), 27-38.
- FATİH Projesi. (2012). *Proje hakkında*. <http://fatihprojesi.meb.gov.tr/tr/icerikincele.php?id=6> adresinden 17.12.2013 tarihinde edinilmiştir.



- Gökmen, Ö. F. ve Akgün, Ö. E. (2015). Bilgisayar ve Öğretim Teknolojileri Eğitimi öğretmen adaylarının bilişim güvenliği eğitimi verebilmeye yönelik yeterlilik algılarının incelenmesi. *İlköğretim Online*, 14(4), 1208-1221.
- Henkoğlu, T. ve Yılmaz, B. (2013). Avrupa Birliği (AB) bilgi güvenliği politikaları. *Türk Kütüphaneciliği*, 27(3), 451-471.
- Huck, S. W. (2008). *Reading statistics and research* (5. baskı). Boston: Pearson.
- Huck, S. W. (2012). *Reading statistics and research* (6. baskı). Boston: Pearson.
- İnci, Ş. (2002). *Türk Milli Eğitiminde eğitim teknolojisi politikaları ve uygulamaları*. Yayınlanmış Yüksek Lisans Tezi, Yüzüncü Yıl Üniversitesi, Sosyal Bilimler Enstitüsü, Van.
- Kağıtçıbaşı, Ç. (1999). *İnsan ve İnsanlar* (10. Baskı). İstanbul: Evrim Yayınları.
- Karakoç, M. (2011). Bilişim suçlarına genel bakış, bilişim suçlarını önleme çalışmaları ve güvenli internet kullanımı. *Suç ve Önleme Sempozyumu*, Bursa.
- Kaşıkçı, D. N., Çağiltay, K., Karakuş, T., Kurşun, E. ve Ogan, C. (2014). Türkiye ve Avrupa'daki çocukların İnternet alışkanlıkları ve güvenli İnternet kullanımı. *Eğitim ve Bilim*, 39(171), 230-243.
- Keser, H. ve Güldüren, C. (2015). Bilgi güvenliği farkındalık ölçeği (BGFÖ) geliştirme. *Kastamonu Eğitim Dergisi*, 23(3), 1167-1184.
- Kocamustafaogulları, M. (2013). *Bilgi güvenliği farkındalığı ve uygulama seviyesi değerlendirmek için bilgi güvenliği prototip uygulaması*. Yayınlanmamış Yüksek Lisans Tezi, Çankaya Üniversitesi, Fen Bilimleri Enstitüsü, Ankara.
- Krejcie, R. V. ve Morgan, D. W. (1970). Determining sample size for research activities. *Educational and Psychological Measurement*, 30(3), 607-610.
- Kruger, H., Drevin, L. ve Steyn, T. (2010). A vocabulary test to assess information security awareness. *Information Management & Computer Security*, 18(5), 316-327.
- Little, R. J. A. ve Rubin, D. R. (2002). *Statistical analysis with missing data* (2. baskı). New York: Wiley.
- Mart, İ. (2012). *Bilişim kültüründe bilgi güvenliği farkındalığı*. Yayınlanmamış Yüksek Lisans Tezi, Kahramanmaraş Sütçü İmam Üniversitesi, Fen Bilimleri Enstitüsü, Kahramanmaraş.
- MEB. (2002). *MLO modeli* (3. Baskı). Ankara: EARGED Yayınları.
- MEB. (2009). *e-Okul kullanım kılavuzu*. <http://e-okul.meb.gov.tr> adresinden 15.12.2013 tarihinde edinilmiştir.
- MEB Bilgi İşlem Dairesi Başkanlığı. (2012). *Bilgi ve sistem güvenliği yönergesi*. [http://bigb.meb.gov.tr/meb\\_iys\\_dosyalar/2012\\_06/18113300\\_yonerge.pdf](http://bigb.meb.gov.tr/meb_iys_dosyalar/2012_06/18113300_yonerge.pdf) adresinden 17 Mart 2014 tarihinde edinilmiştir.
- Oktay, S. ve Çakır, R. (2012). İlköğretim öğretmenlerinin teknoloji kullanımları ve teknolojiye yönelik tutumları arasındaki ilişkinin incelenmesi. *X. Ulusal Fen Bilimleri ve Matematik Eğitimi Kongresi*, 27-30 Haziran 2012, Niğde.

- Öğretmen Yetiştirme ve Geliştirme Genel Müdürlüğü. (2013). *Geliştirilen ve güncellenen standart kriterlere uygun olarak hazırlanan örnek hizmet içi eğitim programları*. [http://hedb.meb.gov.tr/net/\\_standart\\_program/](http://hedb.meb.gov.tr/net/_standart_program/) adresinden 17.12.2013 tarihinde edinilmiştir.
- Özenç, K. (2007). Bilgi ve iletişim teknolojilerinde kişisel ve kurumsal bilgi güvenliğinin sağlanması. *Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı*, 13-14 Aralık 2007, Ankara.
- Prensky, M. (2001). Digital natives, digital immigrants, Part 1. *On The Horizon* 9(5). 04 Şubat 2015 tarihinde <http://www.marcprensky.com/writing/Prensky%20-%20Digital%20Natives,%20Digital%20Immigrants%20-%20Part1.pdf> adresinden alınmıştır.
- Schmidt, A. H. (2004). *Building a mosaic of security for a better world, security matters*. USA: Aspatore Books.
- Symantec. (2013). *İnternet security threat report*. [http://www.symantec.com/content/en/us/enterprise/other\\_resources/b-istr\\_main\\_report\\_v18\\_2012\\_21291018.en-us.pdf](http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf) adresinden 22.12.2013 tarihinde edinilmiştir.
- Şahinaslan, Ö., Şahinaslan, E., Borandağ, E. ve Şahinaslan, A. M. (2013). Güvenli bir toplum için son kullanıcı siber güvenliği. *XV. Akademik Bilişim Konferansı*, 23-25 Ocak 2013, Akdeniz Üniversitesi, Antalya.
- Tekerek, M. (2008). Bilgi güvenliği yönetimi. *KSÜ Fen ve Mühendislik Dergisi*, 11(1), 132.
- Tekerek, M. ve Tekerek, A. (2013). A research on students' information security awareness. *Turkish Journal of Education*, 2(3), 61-70.
- Wagner, A. E. ve Brooke, C. (2007). Wasting time: The mission impossible with respect to technology-oriented security approaches electronic. *Journal of Business Research Methods*, 5(2), 117-124.
- Yavanoğlu, U., Sağıroğlu, Ş. ve Çolak, İ. (2012). Sosyal ağlarda bilgi güvenliği tehditleri ve alınması gereken önlemler. *Politeknik Dergisi*, 15(1), 15-27.
- Yılmaz, E. (2015). *Öğretmenlerin dijital veri güvenliği farkındalığı*. Yayınlanmamış Doktora Tezi, Anadolu Üniversitesi, Eğitim Bilimleri Enstitüsü, Eskişehir.
- Yılmaz, F. G. K., Yılmaz, R. ve Sezer, B. (2014). Üniversite öğrencilerinin güvenli bilgi ve iletişim teknolojisi kullanım davranışları ve bilgi güvenliği eğitimine genel bir bakış. *Bartın Üniversitesi Eğitim Fakültesi Dergisi*, 3(1), 176-199.

## Extended Summary

Teachers were accustomed to studying with printed materials in the past. Nowadays, their information production and storage habits change in accordance with the advances in emerging information and communication technologies. As they are supposed to employ current information technologies in their instructional practices, the security of their digital data becomes more and more important. Data security can be described as the transmission of information from sender to receiver without any interference, seizure or change. While the concept was used to refer to the physical security of printed materials in the past, it now means the storage, protection and transmission of digital data through relevant digital platforms.

Several threats to digital data can be listed such as natural disasters, power outages, malfunction of camera and telephone switchboards, hardware problems, computer viruses and abuse of authorization. Among these threats, human problems carries the primary importance as most threats can be eliminated through awareness improvement and training. According the Internet Security Threat Report of Symantec (2013), threats to online security have grown and evolved about 42 % in comparison to the previous year. In addition, Turkey ranked among the most vulnerable settings in Europe in terms of spam e-mails (5<sup>th</sup>), phishing attacks (8<sup>th</sup>) and virus problems (5<sup>th</sup>).

Classroom teachers have significant roles in equipping students with the fundamentals of emerging practices and modeling the appropriate use of current information and communication technologies. Thus, empirical studies regarding the digital security awareness of teachers are needed. Regarding the priority of digital data security, the current study aimed to investigate the digital data security awareness of teachers, who are employed in different schools of the National Ministry of Education. The target population involved 12760 teachers in Balıkesir. Through cluster sampling, 1446 teachers from different educational clusters and 29 different schools were selected and sent the survey form. The response rate was 60.2 percent (n:870), and the number of valid questionnaires after the elimination of inappropriately filled ones was 837. This number was regarded as representative of the target population since a confidence level of 95 % and a confidence interval of 3.5 requires a sample size of 739 (Bartlett et al., 2001).

The survey included a personal information form and the Digital Data Security Awareness Scale which was developed by Yılmaz (2015). The scale was developed through extensive literature reviews, expert panels, pilot implementations with 79 teachers, an exploratory factor analysis with 529 teachers and a confirmatory factor analysis with 335 different teachers. Factor loadings ranged between .506 through .689. The internal consistency coefficient was quite high ( $\alpha=.945$ ). The single factor structure explained 36 percent of the total variance; and involved 32 Likert indicators which were rated as completely agree (5) through completely disagree (1).

Descriptive statistics based on the self-report measure indicated that participants' digital data security awareness levels were quite high. It should be noted that the findings were based on self-report. When individual items were evaluated with regard to their descriptive statistics, the highest levels of awareness were observed in terms of creating powerful passwords, selecting strong security questions and using antivirus software. On the other hand, the level of awareness was quite low in terms of firewalls and online security certificates.

After the skewness and kurtosis values were checked and non-linear transformations were conducted, further parametric tests were used to investigate the differences based on background variables. While the awareness levels varied with regard to gender, duration of daily computer and Internet use, and ownership of different digital technologies; it did not change with regard to teachers' branch, school type (i.e., primary, secondary, high), educational background (i.e., vocational, undergraduate, graduate) and experience. More specifically, the average of males with regard to digital data security awareness was significantly higher than that of females. Awareness averages increased in accordance with daily computer and internet use duration. Ownership of different digital technologies meant higher levels of awareness such as personal computer, tablets and smart phones.

Other similar studies in the field indicated that females outperform males in terms of digital data security awareness in populations of engineers, lawyers and medical staff. Student populations revealed the same pattern. However, the finding was different in the current study which involved teachers. Duration of daily computer and internet use and ownership of several digital technologies also predicted digital data security awareness. That is, more experience meant more awareness. On the other hand, teachers' branch, school type, educational background and experience was not influential on the level of awareness. In brief, predictor variables were mostly about technology experience rather than teacher-related issues. Further studies are needed to understand the contribution of each variable and other potential variables predicting digital data security awareness. Same instruments can be administered to pre-service teachers to see whether there is a difference between emerging teachers and experienced ones. The current findings may also be used to inform instructional designers who want to organize in-service training for teachers about digital data security awareness.