

# Ortaokul Öğrencilerine Yönelik Bilgi Güvenliği ve Etik Farkındalığı Ölçeği'nin Geliştirilmesi ve Uygulaması\*

## Development and Application of Information Security and Ethical Awareness Scale for Middle School Students

Ahmet Yılmaz, Ahmet Berk Ustun

### Yazar Bilgileri

**Ahmet Yılmaz**   
Öğretmen, Millî Eğitim  
Bakanlığı,  
[ahmetyilmazar@gmail.com](mailto:ahmetyilmazar@gmail.com)

**Ahmet Berk Ustun**   
Doç. Dr., Bartın Üniversitesi,  
Bilgisayar Teknolojisi ve Bilişim  
Sistemleri,  
[ustun.ab@gmail.com](mailto:ustun.ab@gmail.com)

### ÖZ

Bu çalışmanın ana amacı ortaokul öğrencilerinin bilgi güvenliği ve etik farkındalık düzeylerini ölçmeye yönelik ölçek geliştirmek, ikincil amacı ise öğrencilerin bilgi güvenliği ve etik farkındalık düzeylerini belirlemektir. İlk aşamada, ortaokul öğrencilerin bilgi güvenliği ve etik farkındalıklarını ölçmek için ölçek geliştirilmiştir. Bilgi Güvenliği ve Etik Farkındalığı Ölçeği, ilgili alanyazın kapsamında hazırlanarak uzman görüşleri doğrultusunda düzenlenmiş ve 621 öğrenciye uygulanmıştır. Açımlayıcı Faktör Analizi sonucunda "Kullanıcı Güvenliği", "Veri Güvenliği" ve "Etik" olmak üzere ölçeğin üç alt boyut ve 17 maddeden oluştuğu belirlenmiştir. Ölçeğin yapısı Doğrulayıcı Faktör Analizi ile doğrulanmış ve Cronbach alfa güvenirlik katsayısı .896 olarak bulunmuştur. Araştırmanın ikinci aşamasında, 921 ortaokul öğrencisine Bilgi Güvenliği ve Etik Farkındalığı Ölçeği ve kişisel bilgi formu uygulanmıştır. Betimsel istatistikler kullanılarak öğrencilerin bilgi güvenliği ve etik farkındalık düzeyleri analiz edilmiştir. Sonuçlar, öğrencilerin kullanıcı güvenliği ve etik farkındalıklarının yüksek, veri güvenliği farkındalıklarının ise orta düzeyde olduğunu göstermiştir. Sınıf seviyeleri açısından 5. ve 6. sınıf öğrencilerinin farkındalıklarının daha yüksek olduğu belirlenmiştir. Anne ve baba eğitim düzeylerinin öğrencilerin bilgi güvenliği ve etik farkındalık alt boyutlarını etkilediği sonucuna ulaşılmıştır.

### Makale Bilgileri

#### Anahtar Kelimeler

Bilgi güvenliği farkındalığı  
Bilgi güvenliği  
Etik  
Ölçek geliştirme  
Ortaokul

#### Keywords

Information security awareness  
Information security  
Ethics  
Scale development  
Middle school

#### Makale Geçmişi

Geliş: 20.12.2024  
Kabul: 25.06.25

### ABSTRACT

The main purpose of this study is to develop a scale to measure the level of middle school students' information security and ethical awareness and the secondary purpose is to determine the level of their information security and ethical awareness. In the first stage, a scale was developed to measure the middle school students' information security and ethical awareness. The Information Security and Ethics Awareness Scale was prepared within the scope of the relevant literature, organized in line with expert opinions and applied to 621 students. As a result of the exploratory factor analysis, the scale consisted of three sub-dimensions including "User Security", "Data Security", and "Ethics", and 17 items. The structure of the scale was confirmed by confirmatory factor analysis and Cronbach's alpha reliability coefficient was found to be .896. In the second stage of the study, 921 secondary school students were administered the Information Security and Ethics Awareness Scale and personal information form. Students' information security and ethical awareness levels were analysed using descriptive statistics. The results showed that students' user security and ethical awareness were high, while their data security awareness was at a medium level. In terms of grade levels, it was determined that the awareness of 5<sup>th</sup> and 6<sup>th</sup> grade students was higher. It was concluded that mother and father education levels affected students' information security and ethical awareness sub-dimensions.

\* Bu çalışma ikinci yazar danışmanlığında, birinci yazar tarafından hazırlanan yüksek lisans tezinden üretilmiştir.

### Makale Türü

Araştırma

### Önerilen Atıf

Yılmaz, A. & Ustun, A. B. (2025). Ortaokul öğrencilerine yönelik Bilgi Güvenliği ve Etik Farkındalığı Ölçeği'nin geliştirilmesi ve uygulaması. *TEBD*, 23(2), 2182-2210. <https://doi.org/10.37217/tebd.1604704>

## Giriş

### Bilgi Güvenliği ve Bilgi Güvenliği Farkındalığı

Bilgi ve iletişim teknolojilerinin gelişimi, bilgi birikiminde hızlı bir artışa yol açarak toplumsal değişimi tetiklemiştir (Akgün ve Ustun, 2023). Bilgiye erişimin kolaylaşması, bireylerin teknoloji ile bilgi arasında sağlıklı bir denge kurmasını zorunlu hâle getirmiştir (Karaoğlu-Yılmaz vd., 2024). Bu bağlamda, bilgiyi üretebilen, paylaşabilen, yönetebilen ve kullanabilen bireyler yetiştirme gerekliliği ortaya çıkmıştır. Ancak gelişen teknolojiyle birlikte bilgi güvenliği riskleri de ortaya çıkmıştır (İsmagilova vd., 2020). Bilginin güvenliğini sağlamak, üretim ve kullanım kadar önem kazanmıştır. Bu durum, eğitim politikalarının çağın ihtiyaçlarına uygun şekilde düzenlenmesini ve öğrenme süreçlerinde yeni yaklaşımlar bulunmasını gerektirmektedir. Bu şekilde bilgi güvenliği konusunda bilinçli bireylerin yetiştirilmesini sağlayacaktır.

Bilgi güvenliği, bilgilerin erişilebilirliğini, bütünlüğünü ve gizliliğini korumayı hedefleyen bir disiplindir (Whitman ve Mattord, 2016). Bu güvenlik, üç ana bileşen üzerine kuruludur; gizlilik, bütünlük ve erişilebilirlik. Bu bileşenlerden herhangi birinde yaşanacak sorun, güvenlik zafiyetine yol açabilir (Kara, 2018). Bilgi güvenliğinin temel hedefleri, yetkisiz erişimi ve kötü niyetli müdahaleleri önlemektir. Kullanıcı bilincini artırmak, güvenli şifreler kullanmak, güvenilir kaynaklardan dosya indirmek gibi önlemler bu sürecin bir parçasıdır. Bilgi güvenliğine yönelik tehditler arasında teknik arızalar, doğal afetler, insan hataları ve kötü amaçlı yazılımlar yer alır (Güldüren, 2015). İnsan faktörü, bilgi güvenliğinin en zayıf halkası olarak kabul edilmektedir ve bu nedenle bireylere bilgi güvenliği konusunda eğitim verilmesi büyük önem taşır (Wagner ve Brooke, 2007). Bilgi güvenliği farkındalığı ise bireylerin siber tehditler ve dolandırıcılıklara karşı güvenlik önlemleri almasını sağlar ve kurumlar açısından da önemlidir (Vural ve Sağiroğlu, 2010).

### Bilgi Güvenliğine Yönelik Tehditler

Bilgi, günümüz ve geleceğin şekillenmesinde büyük bir rol oynamaktadır. Bu nedenle, bilginin korunması ve doğru kullanılması hayati bir sorumluluk taşır. Eğitim, savunma, ulaşım ve ticaret gibi pek çok alanda bilginin güvenliği ve doğru şekilde yönetimi kritik önemdedir. Ancak bilginin korunması önemli bir sorun olarak karşımıza çıkmaktadır (Yılmaz, 2015). Bilgi güvenliğine yönelik tehditler doğal afetler, prosedür eksiklikleri, insan hataları ve zararlı yazılımlar kaynaklı olabilir (Öztezcan, 2017).

Doğal afetler, geçmişte olduğu gibi günümüzde de deprem, sel, yangın ve savaş gibi çeşitli biçimlerde yaşanmaktadır. İnsanlar ve devletler bu afetlere karşı önlemler alsa da tamamen durdurmaları mümkün olmamaktadır. Bu nedenle, doğal afetlerin gelecekte her an meydana gelebileceği gerçeği unutulmamalıdır. Doğal afetlerin bilgi kaynakları ve depolama birimlerine zarar verebileceği göz önünde bulundurulmalı, bu risklere karşı yönetim stratejileri geliştirilmelidir. Bilgi ve

belgelerin saklandığı yerlerin risk değerlendirmelerinin gerçekçi senaryolarla yapılması büyük önem taşır.

Bilginin üretimden depolanmasına ve kullanımına kadar çeşitli yöntemler ve teknikler uygulanmaktadır. Bu süreçler, idari ve yönetim kademesi tarafından belirlenen prosedürlerle düzenlenir. Kurumsallaşma eksikliği, görev ve yetki tanımlarının net olmaması, yetersiz personele aşırı sorumluluk verilmesi gibi durumlar, prosedür kaynaklı tehditlere yol açar. Ayrıca verilerin uygun şekilde depolanmaması, yedekleme eksiklikleri ve teknolojik altyapının düzenli bakımının yapılmaması da bilgi güvenliği açısından riskler oluşturur (Vural ve Sağiroğlu, 2010).

Bilgi güvenliğinin en zayıf halkası insan faktörüdür (Maleki vd., 2016). Kullanıcının yeterli eğitim almaması, bilgi güvenliğini ciddiye almaması, sistemde zafiyet ve tehditlere yol açar. Her ne kadar üst düzey teknolojik güvenlik önlemleri alınsa da insan hatası siber tehditlere davetiye çıkarır. Bu sebeple bilgi güvenliği ve etik üzerine bilinçli olmak oldukça önemlidir. Eğitim ve farkındalık programları, bireylerin siber tehditleri tanımalarına ve bilinçli hareket etme alışkanlıkları kazanmalarına yardımcı olur (Herath ve Rao, 2009). Ayrıca dolandırıcılık, kredi kartı sahtekarlığı, yalan haber gibi suçlarla mücadelede de insan faktörüne dikkat edilmelidir.

Sanal ortam, doğruluktan uzak ve etik dışı davranışların yaygın olduğu bir alan olabilir. Özellikle kötü niyetli yazılımlar ve dolandırıcılık yöntemleri, kullanıcıları hedef alarak kişisel ve finansal bilgileri ele geçirmeye çalışır. Bu tür tehditler arasında bilgisayar virüsleri, kimlik avı, sosyal mühendislik, casus yazılımlar, arka kapılar, istenmeyen e-postalar, solucanlar, klavye dinleme sistemleri, kök kullanıcı takımları, Truva atları ve botnet saldırıları yer alır. Bilgisayar virüsleri, bilgisayar sistemlerine zarar verebilen kötü niyetli programlardır.

Virüsler genellikle kullanıcıların izni olmadan yayılır ve sistemlerde veri kaybı, çökme gibi problemlere yol açar (Aycok, 2006). Bu tür yazılımlardan korunmak için güvenlik programlarının kullanılması ve yazılımların güvenilir kaynaklardan indirilmesi önemlidir (Szor, 2005). Kimlik avı, kötü niyetli kişilerin, sahte e-postalar ve web siteleri aracılığıyla kullanıcıların kişisel bilgilerini çalmaya çalıştığı bir dolandırıcılık yöntemidir. Genellikle bu tür saldırılarda kullanıcıların güvenilir olduğunu düşündükleri siteler veya hizmetlerden gelen sahte mesajlar ile kişisel bilgilerini girmeleri sağlanır. Bu saldırılardan korunmak için kullanıcıların dikkatli olmaları, şüpheli mesajları incelemeleri ve sadece güvenilir kaynaklardan gelen talepleri dikkate almaları gerekir. Sosyal mühendislik, insanları manipüle ederek bilgi çalmayı amaçlayan bir saldırı yöntemidir (Hadnagy, 2011). Saldırganlar, genellikle güven oluşturarak hedef kişileri kandırır ve hassas bilgileri ele geçirir. Bu tür saldırılardan korunmak için kişisel bilgileri paylaşmaktan kaçınmak, güvenilir olmayan kişilere şüpheyle yaklaşmak ve güvenlik farkındalığı eğitimleri almak önemlidir. Casus yazılımlar (spyware), kullanıcıların haberi olmadan bilgisayarlara yerleşir ve kişisel bilgileri toplar (Christodorescu vd., 2005). Bu yazılımlar genellikle

kullanıcıların aktivitelerini izler ve kötü amaçlar için kullanır (Cai vd., 2018). Casus yazılımlardan korunmak için güvenilir güvenlik yazılımları kullanılmalı ve bilgisayarlar düzenli olarak taranmalıdır (Bhatia vd., 2017).

Arka kapılar (backdoor), yazılım sistemlerine gizlice yerleştirilen ve yetkisiz erişime olanak sağlayan güvenlik açıklarıdır (Kaufman vd., 2002). Kötü niyetli kişilerin sistemleri kontrol etmesini veya verileri çalmasını sağlar (Biryukov vd., 2013). Bu tür saldırılardan korunmak için güvenlik yazılımlarını güncel tutmak ve sistemlerdeki açıkları düzenli olarak kontrol etmek gerekir. İstenmeyen e-postalar (spam), genellikle reklam amacıyla veya kötü niyetli yazılımlar yaymak için toplu olarak gönderilir (Feng vd., 2004). Bu istenmeyen e-postalar, kullanıcıların e-posta kutularını doldurarak zaman kaybına yol açabilir ve ciddi güvenlik tehditleri oluşturabilir (Krombholz vd., 2015). Kullanıcılar, spam filtreleri kullanarak bu tür e-postalardan korunabilirler. Bilgisayar solucanları (worm), ağlar üzerinden yayılarak diğer bilgisayarlara bulaşan kötü niyetli yazılımlardır (Moore vd., 2003). Solucanlar, sistem kaynaklarını tüketerek ağ performansının düşmesine ve sistem çökmesine sebebiyet verebilir. Güvenlik yazılımlarını güncel tutarak ve ağ trafiğini izleyerek bu tür tehditlerden korunmak mümkündür. Klavye dinleme sistemleri (keylogger), kullanıcının tuş vuruşlarını kaydeden yazılımlardır. Bu yazılımlar, özellikle şifre ve kredi kartı bilgilerini ele geçirmek için kullanılır (Filiol, 2011). Keyloggerlardan korunmak için güçlü güvenlik yazılımları kullanılmalı ve güvenilir olmayan kaynaklardan yazılım indirilmemelidir.

Kök kullanıcı takımları (rootkitler), bilgisayar sistemine gizlice yerleşerek yetkisiz erişim sağlayan kötü niyetli yazılımlardır. Bu yazılımlar, kullanıcının bilgisi olmadan sistemde değişiklik yapabilir ve yetkisiz kişilerin sisteme erişimine olanak tanır (Anwar vd., 2019). Güvenlik açıklarını tespit ederek ve sistemleri düzenli olarak tarayarak kök kullanıcı takımlarından korunmak mümkündür. Truva atları, zararlı yazılımların, güvenilir bir program gibi görünerek bilgisayarlara sızmasıdır (Janczewski ve Colarik, 2004). Truva atları, kullanıcıların bilgilerini çalabilir, aktivitelerini izleyebilir ve sistem kontrolünü ele geçirebilir. Bu tür yazılımlardan korunmak için yalnızca güvenilir kaynaklardan program indirilmesi ve güvenlik yazılımlarının güncel tutulması gereklidir. Botnetler, bilgisayar korsanlarının büyük ölçekli saldırılar düzenlemek için kullandıkları bir ağıdır. Zombi bilgisayarlar üzerinden gerçekleştirilen bu saldırılar, spam e-postalar yaymak veya dağıtılmış hizmet reddi saldırıları (DDoS) gerçekleştirmek gibi amaçlarla kullanılır. Botnetlerden korunmak için ağ trafiği izlenmeli ve güvenlik yazılımları güncel tutulmalıdır.

### **Etik ve Etik Farkındalığı**

Etik, bireylerin ve toplumların doğru ile yanlış ayırt ederek ahlaki değerlendirmeler yapmasını ve bu doğrultuda bireylerin davranışlarını düzene sokmasını sağlayan çalışma alanıdır (Rosenstand, 2011). Etik, insanların eylemlerini ahlaki standartlara göre değerlendirme sürecini içerir ve çeşitli felsefi yaklaşımlarla incelenir. Ahlaki kavramlar, değerler, normlar ve ilkeler bu çalışmaların temel

unsurlarıdır (Beauchamp ve Childress, 2013). Etik farkındalığı ise özellikle bilişim ve teknoloji kullanımında bireylerin ahlaki sorumluluklarını ve etik değerlerini gözetmelerini ifade eder. Bu farkındalık, bireylerin etik çerçevede kararlar almasını ve davranışlarına yansıtmasını sağlar. Etik farkındalığı gelişmiş bireylerin, yanlış davranışlardan kaçınmaları ve doğru kabul edilen eylemleri yapmaları beklenir (Schwartz, 2017). Bu sayede etik olmayan davranışların azalması, toplumda ahlaki ve etik değerlerin ön plana çıkmasını sağlar. Etik farkındalığı artırılmış bireyler, zamanla etik bilince sahip toplumlar yaratır ve bu bireyler, sağlıklı bir toplum yapısının temel taşı oluşturur. Etik olmayan davranışların sadece cezalandırılması değil, etik davranışların eğitim yoluyla bireylere aktarılması da son derece önemlidir. Bu şekilde etik değerler, toplumun geneline yayılır ve bireylerin günlük hayatlarındaki karar ve davranışlarına yansır.

### **Bilişim Etiği**

Bilişim etiği, hızla gelişen teknoloji dünyasında teknoloji ve etik arasındaki dengeyi sağlamak amacıyla sürekli araştırma ve tartışma konusu olan bir disiplindir. Bilişim etiği, bilişim sistemlerinin ve bilgisayar teknolojilerinin kullanımından kaynaklanan ahlaki ve etik sorunları kapsar (Johnson, 2009). Bu sorunlar arasında veri güvenliği, özel hayatın gizliliği, siber zorbalık, yapay zekâ etiği, sansür gibi konular yer alır. Bilişim etiği ile teknoloji geliştiricileri ve kullanıcıların karşılaştığı etik problemleri ele alınır ve bilgi teknolojilerinin insan haklarına, özgürlüklere ve sosyal adalete uygun bir şekilde kullanılmasını sağlar. Alanyazın incelendiğinde genel olarak karşılaşılan bilişim teknolojilerinde etik sorunlar şu şekilde sıralanabilir; ifade özgürlüğü, sayısal uçurum, güvenlik ve kalite, mahremiyet, siber zorbalık, fikri mülkiyet, doğruluk, lisans anlaşması, telif hakları ve patent (Himma ve Tavani, 2008; Johnson, 2009; Mason, 1986).

Bilişim etiğinde en önemli konulardan biri mahremiyettir. Mahremiyet, bireylerin kişisel bilgilerinin gizliliğini koruma hakkıdır ve bu hakkın ihlali etik bir sorun olarak kabul edilir (Moor, 2008). Kullanıcı verilerinin izinsiz toplanması ve kötüye kullanılması, mahremiyetin zedelenmesine ve bilgi teknolojilerine olan güvenin azalmasına yol açar. Bu nedenle, mahremiyetin korunabilmesi için yüksek güvenlik önlemleri alarak kullanıcı verilerinin korunması amacıyla etik yönergelerin uygulanması gerekmektedir (Floridi, 2013). Kullanıcıların izni alınarak etik kurallar çerçevesinde kullanıcıların mahremiyeti korunarak bilgi toplanabilir (Tavani, 2007). Siber zorbalık da önemli bir etik sorundur. Siber zorbalık, bilişim teknolojileri aracılığıyla kişi veya toplulukları hedef alan saldırgan davranışları içerir (Wang vd., 2019). Sosyal medya ve mesajlaşma uygulamaları üzerinden tehdit, hakaret, iftira gibi davranışlar siber zorbalık kapsamına girer (Kowalski ve Limber, 2012). Özellikle gençler arasında daha yaygın olan bu sorun hem psikolojik hem de mahremiyet yönünden mağduriyetlere yol açar. Siber zorbalığın önlenmesi ve özellikle genç bireylerin bilinçlenmesi için etik farkındalığına yönelik eğitim çalışmalarının yaygınlaştırılması büyük önem taşır (Kowalski ve Limber, 2012). Lisans anlaşmaları, telif

hakları, fikri mülkiyet ve patentler de bilişim teknolojileri alanında sıkça karşılaşılan etik sorunlardır (McKeon, 2011). Dijital içeriklerin izinsiz kopyalanması, çoğaltılması ve paylaşılması gibi eylemler etik ihlaller arasında yer alır. Fikri mülkiyet, yenilikçi ve özgün eserlerin korunması için hukuki bir mekanizma sağlar ve bu hakların ihlali, etik açıdan ciddi sorunlara yol açar. Telif hakları, eserin sahibine yasal haklar tanırken lisans anlaşmaları eserin kullanım şartlarını belirler. Patentler ise yenilikçi fikirlerin korunmasını teşvik eder.

Güvenlik ve kalite, bilişim etiğinde birbirine bağlı kavramlardır. Güvenlik, dijital verilerin korunması ve sistemlerin yetkisiz erişimlere karşı güvence altına alınması anlamına gelir (Johnson, 2009). Kalite ise bilişim sistemlerinin ve verilerin düzgün işlemesi ve kullanıcı beklentilerini karşılamasıdır (McNurlin ve Sprague, 2006). Güvenlik ihlalleri, kullanıcıların zarar görmesine ve kalite standartlarının düşmesine neden olabilir. Bu nedenle, veri güvenliği ve hizmet kalitesi, bilişim etiğinde önemli bir yer tutar. Doğruluk, bilişim teknolojileri aracılığıyla aktarılan bilgilerin gerçek ve güvenilir olmasını ifade eder (Floridi, 2013). Yanıltıcı ve sahte haberler, yanlış bilgiler, etik açıdan büyük problemler yaratır. Özellikle sosyal medya ve internet ortamında bu tür sorunlarla sıkça karşılaşmaktadır. Bilginin doğruluğunu sağlamak, etik bir zorunluluk olarak kabul edilir. Bireylerin fikir ve düşüncelerini özgür bir biçimde ifade etme hakkına ifade özgürlüğü denir (Johnson, 2009). Bilişim teknolojileri, ifade özgürlüğü için önemli bir platform sağlar. Ancak bu özgürlük, nefret söylemi, hakaret ve yanıltıcı bilgilerin yayılması gibi etik sorunlara da yol açabilir. İfade özgürlüğünün etik sınırlarla düzenlenmesi, toplumun genel yararı için önemlidir. Sayısal uçurum, toplumun bazı kesimlerinin bilgi ve iletişim teknolojilerine erişim açısından diğerlerine göre geri kalmasına neden olan bir sorundur (Selwyn, 2003). Bu durum, özellikle sosyo-ekonomik düzeyi düşük bölgelerde daha belirgindir. Sayısal uçurumun azaltılması, toplumun tüm kesimlerinin bilişim teknolojilerinden eşit şekilde faydalanmasını sağlar ve bu da uygun politikalar ve dijital becerilerin yaygınlaştırılmasıyla mümkündür (Norris ve Pernia, 2019). Sonuç olarak bilişim etiği, teknolojinin sorumlu ve adil bir şekilde kullanılmasını sağlamaya yönelik önemli bir alandır. Mahremiyetin korunması, siber zorbalığın önlenmesi, fikri mülkiyet haklarının korunması, güvenlik ve kalite standartlarının sağlanması gibi konular bilişim etiğinin temel unsurlarıdır. Etik farkındalığın artırılması ve bilişim teknolojilerinin toplumsal yarar doğrultusunda kullanılması, bilişim etiğinin en önemli hedeflerindendir.

### **Araştırmanın Amacı**

Bilgi teknolojilerinin gelişmesi ve bu teknolojilere bağlantılı uygulamalarla bilgi güvenliği ve bu konudaki farkındalığın önemini artırmıştır (Çetinkaya vd., 2017). Bu bağlamda, bilgiyi oluşturan ve koruyan sistemlerin en zayıf halkası genellikle insan faktörü olduğu için kullanıcı farkındalığı kritik bir rol oynamaktadır (Güldüren, 2015). Günümüzde bilgisayar ve mobil teknolojilerin kullanım oranları hızla artmakta ve bu teknolojileri kullananların yaş aralığı gittikçe küçülmektedir. Bilgi güvenliği

farkındalığı üzerine yapılan çalışmaların büyük bir kısmı iş hayatındaki bireyler, akademisyenler, öğretmenler, lisans öğrencileri ve lise öğrencilerine odaklanmıştır (Akıncan, 2022; Güldüren vd., 2016; Hacımustafaoğlu, 2019; Kapanoğlu, 2016; Karaoğlu-Yılmaz vd., 2014; Karaoğlu-Yılmaz ve Çavuş-Ezin, 2017; Mart, 2012; Talan ve Aktürk, 2021; Tekerek ve Tekerek, 2013; Tekin ve Polat, 2016; Topal ve Akgün, 2015; Van De Mortel, 2021; Vilander, 2021; Zhen vd., 2022). Ancak ortaokul öğrencilerine yönelik bu alandaki çalışmalar sınırlıdır. Yapılan çalışmalar da incelendiğinde ortaokul öğrencilerine yönelik yapılan çalışmalarda yetişkinler için tasarlanan bilgi güvenliği farkındalığı ölçekleri ve anketlerin kullanıldığı görülmektedir. Örneğin, Özen-Serter (2021) lise öğrencileri için geliştirilen ölçeği ortaokul öğrencilerine uyarlamıştır. Bununla birlikte öğrencilerin etik bilincini geliştirmeye yönelik araştırmalar bulunsa da bu bilincin temellerinin atıldığı ortaokul seviyesindeki gruplarda etik farkındalığına yönelik çalışmaların sınırlı şekilde ele alındığı gözlemlenmiştir (Fidan, 2016).

Öğrencilerin bilgi güvenliği konusundaki eksikliklerinin giderilmesi, karşılaşılabilecekleri tehlikelerin önlenmesi ve öğretim programlarının bu doğrultuda yapılandırılması gerektiği alanyazında vurgulanmaktadır (Seferoğlu vd., 2018). Bu durumda ortaokul öğrencilerinin teknoloji kullanımı sırasında karşılaştıkları tehditlere karşı farkındalık seviyeleri ve etik bilincinin yeterliliği ölçülmesi gerekmektedir. Fakat öğrencilerin bilgi güvenliği ve etik farkındalığı düzeylerini ölçmeye yönelik alanyazında güvenilir ve geçerli ölçme aracının geliştirilme ihtiyacı mevcuttur. Bu bağlamda yapılacak çalışmanın ana amacı ortaokul düzeyindeki öğrencilerin bilgi güvenliği ve etik farkındalığı düzeylerini ölçmeye yönelik bir ölçek geliştirmektir. Ayrıca geliştirilen ölçek aracılığıyla öğrencilerin bilgi güvenliği ve etik farkındalık düzeyleri belirlenerek sınıf seviyesi ve ebeveynlerin eğitim düzeyine göre öğrencilerin bilgi güvenliği ve etik farkındalık düzeylerinin farklılık gösterip göstermediğinin araştırılması çalışmanın ikincil amacıdır.

### Yöntem

Araştırma yöntemi olarak bu çalışmada tarama modeli benimsenmiştir. Tarama modelinin amacı, insan topluluklarının, kurumların, nesnelerin ve olayların doğasını ve özelliklerini tanımlayarak bunları net ve açık bir biçimde ortaya koymaktır (Büyüköztürk vd., 2020; McMillian ve Schumacher, 2001).

### Çalışma Grubu

Araştırmanın örneklemini 2022-2023 eğitim-öğretim yılında 5, 6, 7 ve 8. sınıflarda okuyan ortaokul öğrencileri oluşturmaktadır. Ölçek geliştirme çalışmalarında örneklem büyüklüğü konusunda farklı görüşler bulunsa da genel kabul gören görüş, örneklem büyüklüğünün ölçek maddelerinin 5 ila 10 katı kadar olması gerektiğidir (Kass ve Tinsley, 1979; Kline, 1994; Tavşancıl, 2005). Ayrıca bazı araştırmacılar 200 katılımcının yeterli olduğunu söylerken (Guilford, 1954; Kline, 1994) Çokluk vd. (2014) faktör analizi yapabilmek için 300 ve üzeri katılımcı ile yapılan çalışmaların daha güvenilir

sonuçlar sağlayacağına dikkat çekmektedirler. Özellikle ölçek maddelerinin her biri için en az 10 katılımcı bulunmasının ölçek geliştirme aşamasında yapılacak analizlerin duyarlılığını artıracığı vurgulanmaktadır (Field, 2009; Kline, 1994). Ölçeğin geliştirilme sürecinde yapılan analizlerin duyarlılığını arttırmak için fazla katılımcı sayısına ulaşmakla sağlanabilir. Bu bağlamda ölçek geliştirme sürecinde 621 öğrenciden veri toplanmıştır. Çalışmaya katılan öğrencilerin cinsiyet ve sınıf düzeyine yönelik betimsel verileri Tablo 1’de verilmiştir.

**Tablo 1.** Öğrencilerin Cinsiyet ve Sınıf Düzeyine Göre Değişimleri

|          | Sınıf Düzeyi |      |     |      |     |      |     |      |        |      |
|----------|--------------|------|-----|------|-----|------|-----|------|--------|------|
|          | 5            |      | 6   |      | 7   |      | 8   |      | Toplam |      |
| Cinsiyet | n            | %    | n   | %    | n   | %    | n   | %    | n      | %    |
| Kız      | 89           | 14,3 | 92  | 14,8 | 55  | 8,8  | 72  | 11,6 | 308    | 49,6 |
| Erkek    | 107          | 17,2 | 76  | 12,2 | 67  | 10,8 | 63  | 10,2 | 313    | 50,4 |
| Toplam   | 196          | 31,6 | 168 | 27,1 | 122 | 19,6 | 135 | 21,7 | 621    | 100  |

Tablo 1 incelendiğinde çalışmaya katılan kız öğrencilerin sayısı 308 öğrenci (%49,6), erkek öğrencilerin sayısı 313 öğrenciden (%50,4) oluştuğu anlaşılmaktadır. Öğrencilerin sınıf seviyelerine göre dağılımlarına bakıldığında %21,7’sinin (135 öğrenci) 8. sınıf, %19,6’sının (122 öğrenci) 7. sınıf %27,1’inin (168 öğrenci) 6. sınıf ve %31,6’sının (196 öğrenci) 5. sınıf öğrencilerinden oluştuğu anlaşılmaktadır.

Çalışmanın ikincil amacı doğrultusunda öğrencilerin bilgi güvenliği ve etik farkındalık düzeyini belirleyerek öğrencilerin farkındalık düzeyinin sınıf seviyesi, anne ve baba eğitim durumuna göre farklılaşıp farklılaşmadığının belirlenebilmesi amacıyla 921 ortaokul öğrencisine BGEFÖ uygulanmıştır.

### **Bilgi Güvenliği ve Etik Farkındalığı Ölçeği’nin Geliştirilmesi Süreci**

Ölçek geliştirme çalışmaları deneysel veya kuramsal süreçlerle gerçekleştirilir. Deneysel süreçte, alanyazın veya uzman görüşü doğrultusunda aday ölçek formu oluşturulur ve hedef gruba benzer özelliklerdeki bir örneklem üzerinde pilot uygulama yapılır. Bu süreçte maddelerin psikometrik özellikleri incelenir ve uygun görülen maddelerle ölçek oluşturulur. Bu çalışmada Karasar (2009) ve Balcı (2018) tarafından önerilen yol haritası takip edilmiştir. İlk olarak madde havuzu oluşturulmuş, uzman görüşleri alınmış, pilot deneme yapılmış ve faktör analizi ile güvenilirlik hesaplamaları gerçekleştirilmiştir. Bilgi Güvenliği ve Etik Farkındalığı Ölçeği (BGEFÖ) geliştirilirken bilgi güvenliği ve etik üzerine yapılan çalışmalar ve mevcut ölçekler incelenmiştir. Ayrıca Millî Eğitim Bakanlığının Bilişim Teknolojileri ve Yazılım ders içerikleri ve Kişisel Verilerin Korunumu Kanunundaki hassas noktalar dikkate alınmıştır.

Alanyazın taraması ve ortaokul düzeyinde verilen ders içerikleri incelenerek bilgi güvenliği ve etik konularına yönelik ortaokul öğrencilerinden beklenen davranışlara göre 37 maddelik bir madde havuzu oluşturulmuştur. Bilişim teknolojisi alanında beş uzman akademisyenin görüşleriyle maddeler gözden geçirilmiştir. Maddelerin amaca uygunluğu ve dil açısından açık ve anlaşılır olup olmadığı incelenerek maddelerde gerekli düzenlemeler gerçekleştirilmiştir. Ölçek, 5’li Likert tipi derecelendirme

sistemiyle tasarlanmıştır. Ölçeğin en önemli geçerlik ölçütleri olan yapı, uygulama ve kapsam geçerliği değerlendirilmiştir (Karasar, 2009).

### Verilerin Toplanması ve Analizi

Açımlayıcı Faktör Analizi (AFA) ve Doğrulayıcı Faktör Analizi (DFA) farklı örneklem gruplarından elde edilen verilerle ölçek geliştirme çalışmalarında yapılmalıdır (Çakmak vd., 2014). Ancak faktör analizi her veri seti için uygun olmayabilir. Verilerin faktör analizi için uygunluğunu test etmek için Bartlett küresellik ve Kaiser-Meyer-Olkin (KMO) testi kullanılır. KMO değerinin 0,60'ın üzerinde olması beklenirken Bartlett testi değişkenler arasındaki ilişkileri inceleyerek sonuçların anlamlılığını ve puanların normal dağılıma uygunluğunu gösterir (Büyüköztürk, 2015). Bu koşullar sağlandığında faktör analizi uygulanabilir.

Bilgi Güvenliği ve Etik Farkındalık Ölçeği'nin (BGEFÖ) güvenirlik ve geçerlik çalışmaları için 621 ortaokul öğrencisi üzerinde uygulama yapılmıştır. Bu 621 öğrenci, 421 öğrenci AFA için ve 200 öğrenci DFA için olmak üzere iki alt gruba ayrılmıştır. Uzman görüşlerine göre ölçeğin kapsam geçerliği değerlendirilmiş ve geçerliliği sağlanmıştır. Yapı geçerliğini incelemek amacıyla elde edilen veriler üzerinde faktör analizi yapılmış ve ölçeğin psikometrik özellikleri belirlenmiştir.

Araştırmanın ikincil amacı doğrultusunda alt sorularını yanıtlamak için ortaokul öğrencilerinin bilgi güvenliği ve etik farkındalık düzeylerini belirlemeye yönelik BGEFÖ'den alınan puanlar üzerinden istatistiki hesaplar yapılmıştır. Öğrencilerin bilgi güvenliği ve etik farkındalığı düzeylerinde sınıf düzeylerine ve ebeveynlerinin eğitim durumlarına göre anlamlı farklılık olup olmadığını incelemek için parametrik testlerden tek yönlü varyans analizi (ANOVA) kullanılmıştır. Veri analizleri için anlamlılık düzeyi  $p=.05$  olarak belirlenmiştir.

### Bulgular

Verilerin faktör analizine uygunluğunu görmek için ölçek geliştirme çalışmalarında, Kaiser-Meyer-Olkin (KMO) ve Bartlett küresellik testi kullanılır. KMO katsayısı, örneklem büyüklüğünün yeterliliğini değerlendirir ve 0-1 aralığında bir değer alır. Yüksek KMO değeri, ölçek maddelerinin diğer maddelerle iyi ilişkilendirildiğini gösterir (Field, 2009). Hutcheson ve Sofroniou (1999), KMO değerlerini 0,5-0,7 aralığında vasat, 0,7-0,8 arasında iyi, 0,8-0,9 arasında çok iyi, 0,9 üzerindeyse mükemmel olarak nitelendirmiştir. 0,6'nın üzerindeki KMO değerleri faktör analizi için genellikle kabul edilebilir olarak görülür (Huck, 2012). Bartlett küresellik testi, ölçek maddeleri arasındaki ilişkileri kısmi korelasyonlara dayalı olarak değerlendirir (Büyüköztürk, 2015). Ölçek verileri üzerinden elde edilen ki-kare istatistiğinin anlamlı çıkması ve Bartlett testinin anlamlı sonuç vermesi, veri matrisinin faktör analizi için uygun olduğunu ve normallik varsayımının karşılandığını gösterir. BGEFÖ'nün AFA uygunluğunu görmek için KMO katsayısı ve Bartlett küresellik testi uygulanmıştır. KMO ve Bartlett testi sonuçları Tablo 2'de sunulmuştur.

**Tablo 2.** Barlett Küresellik ve KMO Testleri Sonuçları

|                                     |                   |          |
|-------------------------------------|-------------------|----------|
| <b>KMO Örneklem Yeterliği Testi</b> |                   | .932     |
|                                     | Kare ( $\chi^2$ ) | 3792,329 |
| <b>Barlett Küresellik Testi</b>     |                   | 136      |
|                                     |                   | .000     |

Tablo 2'ye göre, BGEFÖ için KMO hesaplanmış ve katsayısı .932 bulunmuştur. Kaiser (1974), Tavşancıl (2005) ve Çokluk vd.'ne (2014) göre KMO katsayısının .90 ve üzeri değerler mükemmel olarak kabul edilir. Ayrıca Bartlett Küresellik Testi'nin sonucu [ $\chi^2=3792,329$ ;  $df=136$ ;  $p=.000$ ] .01 anlamlılık düzeyinde anlamlı bulunmuştur. Bu sonuçlar, faktör analizi için verilerin uygun olduğunu göstermektedir.

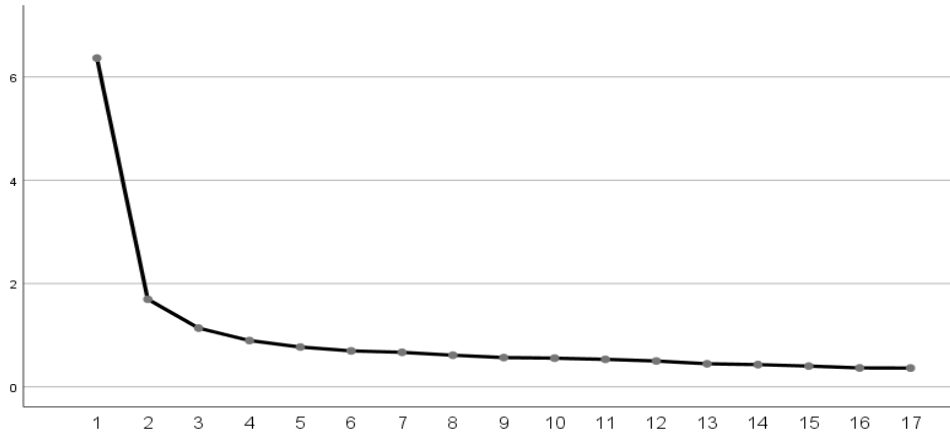
### Açımlayıcı Faktör Analizi

Açımlayıcı Faktör Analizi (AFA), ölçeğin yapısını keşfetmek, maddeler arasındaki ilişkileri ve hangi maddelerin hangi faktörlerle ilişkili olduğunu belirlemek için yapılır (Fabrigar vd., 1999). AFA, korelasyon veya kovaryans matrisine dayalı olarak ilişkili değişkenleri birleştirir ve gizil değişkenler ortaya çıkarır (Özdamar, 2013; Tabachnick ve Fidell, 2015). Bu analiz, faktörlerin varyansını, toplam varyansın ne kadarını açıkladığını ve maddelerin faktör yüklerini belirler (Field, 2009). BGEFÖ faktör yapısını incelemek ve maddelerin uygunluğunu tespit etmek amacıyla da AFA yapılmıştır. AFA'nın önemli bir işlevi, ölçeğin madde havuzunda yer alan gereksiz veya çelişkili maddeleri belirleyip ölçekten çıkarmaktır. Düşük faktör yüküne sahip ve faktörle ilişkisi olmayan maddeler analizle atılabilir (Costello ve Osborne, 2005). Bu adımlar, ölçeğin tutarlılığını artırarak geçerlilik ve güvenilirliği sağlar (Fabrigar vd., 1999). Maddelerin ayıklanması, ölçeğin daha sağlam ve teorik olarak tutarlı bir yapıya kavuşmasına yardımcı olur.

Ortaokul öğrencilerinin bilgi güvenliği ve etik farkındalığını ölçen ölçeğin faktör yapısını belirlemek için yapılan AFA, maddelerin uygunluğuna karar verirken faktör yük değerinin .30 alt sınırı kullanılmıştır. Alanyazına göre, faktör yük değerleri .30 ile .60 arasında (Kline, 1994) veya .30 üzerinde olmalıdır (Stevens, 2002). Ölçekte yer alacak faktörlerin belirlenmesinde öz değer önemli bir kriterdir; öz değeri 1 veya daha büyük olan faktörler temel kabul edilir (Kaiser, 1960). Bu sebeple faktör sayısı belirlenirken öz değerlerin 1'den büyük olmasına dikkat edilmesi gerekmektedir (Thompson, 2008). Ayrıca faktörlerin açıkladığı toplam varyans oranının %50 veya üzeri olması, ölçeğin geçerliliği için yeterli kabul edilir (Güriş ve Astar, 2015). AFA kapsamında faktör öz değerlerine ait çizgi grafiği Şekil 1'de verilmiştir.

Şekil 1'de AFA sonucunda BGEFÖ maddelerinin üç ana faktör olarak toplandığı tespit edilmiştir. Faktörlerin öz değerleri 1'den büyük olduğu ve toplamda ölçeğin %54,10'luk varyansını açıkladığı görülmüştür. Düşük faktör yüküne sahip maddeler ve birden fazla faktörde yakın yük değerine sahip maddeler ölçekten çıkarılmıştır. 0,30 yük değeri kriteri ve maddelerin kuramsal olarak

faktörle olan uygunluğu dikkate alınarak 20 madde ölçekten çıkarılmış, geriye kalan 17 madde 3 faktör altında toplanmıştır. Her faktörün öz değeri, varyans oranları ve faktör yük değerleri Tablo 3'te sunulmuştur.



Şekil 1. Faktör öz değerlerine ilişkin çizgi grafiği

**Tablo 3.** Bilgi Güvenliği ve Etik Farkındalığı Ölçeği Faktör Yükleri Matrisi

| Faktörler                            | Maddeler | Faktör Yük Değerleri |        |        |
|--------------------------------------|----------|----------------------|--------|--------|
|                                      |          | 1                    | 2      | 3      |
| Etik                                 | M31      | 0,794                |        |        |
|                                      | M32      | 0,738                |        |        |
|                                      | M33      | 0,729                |        |        |
|                                      | M28      | 0,724                |        |        |
|                                      | M35      | 0,721                |        |        |
|                                      | M34      | 0,704                |        |        |
|                                      | M36      | 0,674                |        |        |
|                                      | M30      | 0,670                |        |        |
|                                      | M29      | 0,667                |        |        |
| Veri Güvenliği                       | M27      |                      | 0,721  |        |
|                                      | M25      |                      | 0,689  |        |
|                                      | M19      |                      | 0,681  |        |
|                                      | M15      |                      | 0,636  |        |
|                                      | M20      |                      | 0,422  |        |
| Kullanıcı Güvenliği                  | M4       |                      |        | 0,834  |
|                                      | M17      |                      |        | 0,630  |
|                                      | M5       |                      |        | 0,611  |
| Öz Değer                             |          | 6,365                | 1,696  | 1,137  |
| Açıklanan Varyans                    |          | 28,614               | 14,525 | 10,961 |
| Açıklanan Toplam Varyans (%): 54,100 |          |                      |        |        |

Tablo 3 incelendiğinde BGEFÖ faktör yük değerlerinin .422 ile .834 aralığında olduğu görülmüştür. Birinci alt boyut dokuz madde içerirken faktör yükleri .667 ile .794 arasındadır. İkinci alt boyut beş madde içermekte olup faktör yükleri .422 ile .721 arasında, üçüncü alt boyut ise üç madde ile .611 ile .834 arası faktör yüklerine sahiptir. Faktörlerin öz değerleri sırasıyla 6,365, 1,696 ve 1,137 olarak hesaplanmış, toplam varyansın %54,10'unu açıklamışlardır. Alanyazın, uzman görüşleri ve madde içerikleri doğrultusunda alt boyutlar “Etik”, “Veri Güvenliği” ve “Kullanıcı Güvenliği” olarak

adlandırılmıştır. AFA sonrasında BGEFÖ için alt boyutlar arasındaki ilişkiye bakılmıştır. Korelasyon katsayılarına yönelik sonuçlar Tablo 4'te verilmiştir.

**Tablo 4.** Ölçeğin Alt Boyutları Arasındaki Korelasyon Katsayıları

| <i>Alt Boyutlar</i> |             |                       |                            |              |
|---------------------|-------------|-----------------------|----------------------------|--------------|
|                     | <i>Etik</i> | <i>Veri Güvenliği</i> | <i>Kullanıcı Güvenliği</i> | <i>BGEFÖ</i> |
| Etik                | 1           | 0,464**               | 0,461**                    | 0,895**      |
| Veri Güvenliği      |             | 1                     | 0,460**                    | 0,763**      |
| Kullanıcı Güvenliği |             |                       | 1                          | 0,700**      |
| <b>BGEFÖ</b>        |             |                       |                            | <b>1</b>     |

Tablo 4 göre, BGEFÖ'nün alt boyutlarının arasındaki korelasyon katsayılarının .460 ve .464 arasında değişmektedir. Alt boyutlar arasındaki ilişkiler .01 düzeyinde anlamlı bulunmuş ve bu ilişkilerin pozitif yönlü olduğu tespit edilmiştir. Alt boyutlar arasındaki korelasyon katsayılarının 0,3 ile 0,7 arasında olması, bu ilişkilerin orta düzeyde olduğunu göstermektedir. Etik alt boyutunun BGEFÖ ile korelasyonu 0,895, veri güvenliği alt boyutunun 0,763 ve kullanıcı güvenliği alt boyutunun korelasyonu ise 0,700'dür. Bu değerler, alt boyutlar ile BGEFÖ arasında doğrusal ve güçlü ilişkiler olduğunu ortaya koymaktadır.

#### Ölçme Aracının Güvenirliğinin Belirlenmesi

Ortaokul öğrencileri bilgi güvenliği ve etik farkındalığının belirlenmesi için geliştirilen BGEFÖ ve alt boyutlarına yönelik iç tutarlık katsayıları hesaplanmıştır. Tablo 5'te ölçek ve içerdiği alt boyutlarına yönelik elde edilen iç tutarlık katsayıları yer almaktadır.

**Tablo 5.** Öğrencilerin BGEFÖ Yönelik İç Tutarlılık Katsayıları

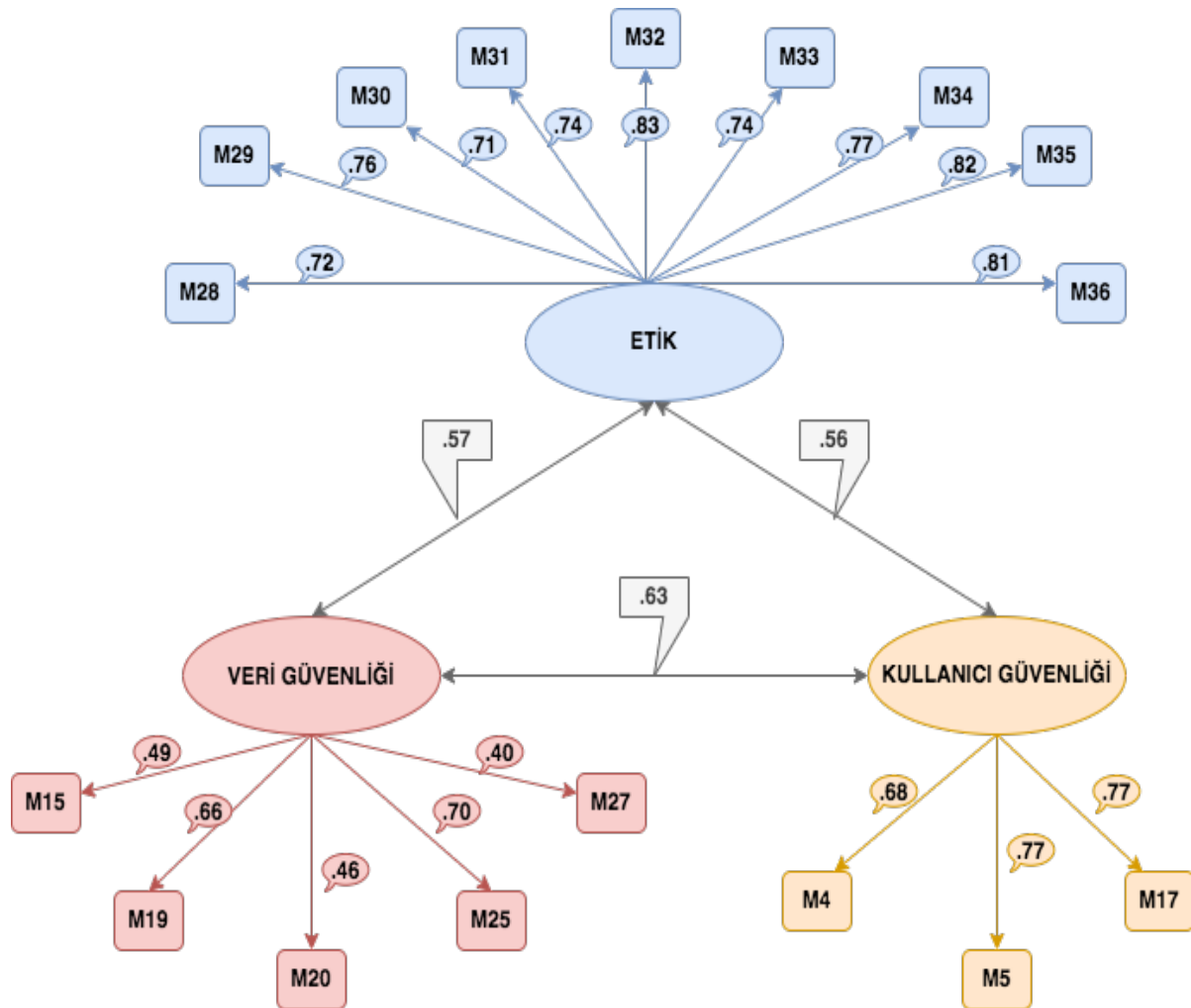
| <i>Alt Boyutlar</i> | <i>Madde Sayısı</i> | <i>Cronbach Alfa (α)</i> |
|---------------------|---------------------|--------------------------|
| Kullanıcı Güvenliği | 3                   | 0,687                    |
| Veri Güvenliği      | 5                   | 0,688                    |
| Etik                | 9                   | 0,912                    |
| <b>BGEFÖ</b>        | <b>17</b>           | <b>0,896</b>             |

Tablo 5 incelendiğinde ortaokul öğrencilerine yönelik geliştirilen BGEFÖ'nin genel iç tutarlılık katsayısının .896 olduğu görülmektedir. Büyüköztürk (2015) ve Nunnally (1978), güvenilirlik katsayısının .70 ve üzeri olmasını önerirken .60-.90 aralığında katsayıya sahip ölçme araçlarının oldukça güvenilir kabul edildiği belirtilmiştir (Özdamar, 2013; Tavşancıl, 2005). Ölçekte yer alan “veri güvenliği” ve “kullanıcı güvenliği” alt boyutlarına yönelik güvenilirlik katsayıları bu doğrultuda güvenilir olduğu tespit edilmiştir. “Etik” alt boyutuna ait güvenilirlik katsayısı ise .90'nın üzerinde olup yüksek güvenilirliğe sahip olduğu tespit edilmiştir. BGEFÖ'nün toplam güvenilirlik katsayısı, yüksek güvenilirlikte olduğu söylenebilir.

#### Doğrulamalı Faktör Analizi

AFA yapıldıktan sonra BGEFÖ modeli yapı geçerliğinin test etmek için Doğrulamalı Faktör Analizi (DFA) gerçekleştirilmiştir (Kline, 2000). Elde edilen verilerle gerçekleştirilen analizler

sonucunda modelin uyum iyiliği değerlendirilmiştir. DFA’da kullanılan uyum indeksleri arasında Normlaştırılmış uyum indeksi (NFI), İyilik uyum indeksi (GFI), Ki-Kare ( $\chi^2$ ) iyilik uyumu, Artık ortalamaların karekökü (RMR), Yaklaşık hataların ortalama karekökü (RMSEA), Düzenlenmiş iyilik uyum indeksi (AGFI), Karşılaştırmalı uyum indeksi (CFI), Standardize edilmiş anlık ortalamaların karekökü (SRMR) ve değerleri yer almıştır. Üç faktörlü BGEFÖ yapısının Doğrulamalı Faktör Analizi sonucunda, faktör yüklerinin AFA ile uyumlu olduğu görülmüş ve modelde herhangi bir modifikasyona ihtiyaç duyulmamıştır. Modelin uyum indeksleri sırasıyla  $\chi^2/sd=1,902$ ; CFI=0,957; GFI=0,928; AGFI=0,902; RMSEA=0,055 ve NFI=0,914 olarak bulunmuştur. DFA sonuçları Şekil 2’de sunulmuştur.



Şekil 2. BGEFÖ için DFA sonuçları

Alanyazındaki çeşitli kaynaklarda modele ilişkin kabul edilebilir ve iyi uyum değerleri üzerine farklı görüşler incelenmiştir. Bu görüşler ve geliştirilen ölçek modeli için elde edilen araştırma modelinin uyum değerleri Tablo 6’da sunulmuştur (Brown, 2006; Jöreskog ve Sorbom, 1993; Kline, 2011; Özdamar, 2013; Smith ve McMillan, 2001; Sümer, 2000; Tabacknick ve Fidell, 2015).

**Tablo 6.** BGEFÖ için DFA Uyum İyiliği İndeksleri

| <i>Uyum İndeksleri</i> | <i>Araştırma Modelinin Değeri</i> | <i>Kabul Edilebilir Model Değerleri</i> | <i>İyi Model Değerleri</i> |
|------------------------|-----------------------------------|-----------------------------------------|----------------------------|
| $\chi^2 / sd$          | 1,902                             | $\leq 5$                                | $\leq 2,5-3$               |
| NFI                    | 0,914                             | $\geq 0,90$                             | $\geq 0,95$                |
| CFI                    | 0,957                             | $> 0,90$                                | $> 0,95$                   |
| RMR                    | 0,057                             | $\leq 0,08$                             | $\leq 0,05$                |
| GFI                    | 0,928                             | $> 0,90$                                | $> 0,95$                   |
| AGFI                   | 0,900                             | $< 0,90$                                | $< 0,90$                   |
| RMSEA                  | 0,055                             | $\leq 0,10$                             | $\leq 0,05$                |

Tablo 6 incelendiğinde DFA sonucunda elde edilen  $\chi^2/sd$ , CFI ve AGFI uyum indeks sonuçlarının iyi model sınırları içinde olduğu; RMR, NFI, GFI ve RMSEA uyum indeks sonuçlarının ise kabul edilebilecek düzeylerde olduğu belirlenmiştir. BGEFÖ için yapılan DFA sonuçlarına dayanarak modelin uyum indekslerinin alanyazındaki görüşlere ve kriterlere göre kabul edilebilir seviyede olduğu ifade edilebilir. Ayrıca analiz sonucunda ulaşılan ki-kare ( $\chi^2$ ) değerinin istatistiksel olarak anlamlı bulunması, modelin uygunluğunu gösteren diğer uyum indekslerini de desteklemektedir ( $\chi^2=214,901$ ;  $p=0,00$ ).

Araştırmanın ikincil amacı doğrultusunda öğrencilerin bilgi güvenliği ve etik farkındalığı düzeylerini belirlemek için BGEFÖ'den öğrencilerin elde ettikleri puanlarının betimsel istatistikleri yapılmıştır. BGEFÖ'den öğrencilerin elde ettikleri puanlar Tablo 7'de verilmiştir.

**Tablo 7.** Öğrencilerin BGEFÖ Puanlarına İlişkin Betimsel İstatistikleri

| <i>Faktör</i>       | <i>N</i>   | <i>Min</i> | <i>Max</i> | <i><math>\bar{X}</math></i> | <i><math>\bar{X} / Madde</math></i> | <i>ss</i>    |
|---------------------|------------|------------|------------|-----------------------------|-------------------------------------|--------------|
| Kullanıcı Güvenliği | 921        | 3          | 15         | 12,28                       | 4,09                                | 2,67         |
| Veri Güvenliği      | 921        | 5          | 25         | 17,38                       | 3,48                                | 3,89         |
| Etik                | 921        | 9          | 45         | 38,43                       | 4,27                                | 6,52         |
| <b>BGEFÖ</b>        | <b>921</b> | <b>17</b>  | <b>85</b>  | <b>68,09</b>                | <b>4,01</b>                         | <b>10,67</b> |

Tablo 7'de, BGEFÖ'den öğrencilerin elde ettikleri puanların ortalaması, madde sayısı ile bölündüğündeki sonuçlar verilmiştir. Bu inceleme sonucunda veri güvenliği faktörü ortalamasının (3,48) en düşük, etik faktörü ortalamasının (4,27) en yüksek olduğu belirlenmiştir. Ölçeğin genel ortalamasının ise 4,01 olduğu tespit edilmiştir. Bu bulgulara göre öğrencilerin veri güvenliğine ilişkin farkındalığının daha düşük, etik farkındalığının ise daha yüksek bulunduğu söylenebilir.

BGEFÖ'den öğrencilerin elde ettikleri puanın sınıf seviyeleri açısından anlamlı farklılaşım farkı olmadığını belirlemek amacıyla ANOVA analizi gerçekleştirilmiştir. Tablo 8'de BGEFÖ'den öğrencilerin elde ettikleri puanların sınıf seviyelerine göre ANOVA sonuçlarını sunmaktadır.

Tablo 8 incelendiğinde Kullanıcı Güvenliği faktöründen ortaokul öğrencilerinin elde ettikleri puanların sınıf düzeyinde anlamlı farklılaştığı tespit edilmiştir ( $F(3, 917)=5,189$ ;  $p \leq 0,05$ ). Scheffe testi yapılarak gruptaki anlamlı farklılaşmanın nerede olduğu belirlenmeye çalışılmıştır. 5. sınıfın

ortalamasının anlamlı olarak (5. sınıf=12,79), 6. sınıfın ortalamasından (6. sınıf=12,01) ve 7. sınıfın ortalamasından (7. sınıf=11,91) daha yüksek olarak gözlemlenmiştir.

**Tablo 8.** BGEFÖ'den Ortaokul Öğrencilerinin Elde Ettikleri Puanların Sınıf Düzeylerine Göre ANOVA

| Sonuçları           |              |          |           |           |          |          |                   |
|---------------------|--------------|----------|-----------|-----------|----------|----------|-------------------|
| <i>Faktör</i>       | <i>Sınıf</i> | <i>N</i> | $\bar{X}$ | <i>ss</i> | <i>F</i> | <i>p</i> | <i>Anlamlılık</i> |
| Kullanıcı Güvenliği | 5            | 244      | 12,79     | 2,66      | 5,189    | .001*    | 5>6<br>5>7        |
|                     | 6            | 261      | 12,01     | 2,62      |          |          |                   |
|                     | 7            | 190      | 11,91     | 2,63      |          |          |                   |
|                     | 8            | 226      | 12,34     | 2,68      |          |          |                   |
| Veri Güvenliği      | 5            | 244      | 18,72     | 3,93      | 14,795   | .000*    | 5>6<br>5>7<br>5>8 |
|                     | 6            | 261      | 17,14     | 3,46      |          |          |                   |
|                     | 7            | 190      | 16,60     | 3,86      |          |          |                   |
|                     | 8            | 226      | 16,82     | 3,98      |          |          |                   |
| Etik                | 5            | 244      | 40,00     | 5,73      | 9,540    | .000*    | 5>7<br>5>8        |
|                     | 6            | 261      | 38,77     | 5,93      |          |          |                   |
|                     | 7            | 190      | 37,25     | 6,98      |          |          |                   |
|                     | 8            | 226      | 37,30     | 7,15      |          |          |                   |
| BGEFÖ               | 5            | 244      | 71,52     | 10,37     | 13,725   | .000*    | 5>6<br>5>7<br>5>8 |
|                     | 6            | 261      | 67,94     | 9,15      |          |          |                   |
|                     | 7            | 190      | 65,76     | 10,88     |          |          |                   |
|                     | 8            | 226      | 66,48     | 11,54     |          |          |                   |

Veri Güvenliği faktöründen ortaokul öğrencilerinin elde ettikleri puanların sınıf düzeyinde anlamlı farklılaştığı tespit edilmiştir ( $F(3, 917)=14,795$ ;  $p \leq .05$ ). Scheffe testi yapılarak gruplardaki anlamlı farklılaşmanın nerede olduğu belirlenmeye çalışılmıştır. 5. sınıfın ortalamasının anlamlı olarak (5. sınıf=18,72), 6. sınıfın ortalaması (6. sınıf=17,14), 7. sınıfın ortalaması (7. sınıf=16,60) ve 8. sınıf ortalamasından (8. sınıf=16,82) daha yüksek olarak gözlemlenmiştir.

Etik faktöründen ortaokul öğrencilerinin aldıkları puanların sınıf düzeyinde anlamlı bir farklılık gösterdiği tespit edilmiştir ( $F(3, 917)=9,540$ ;  $p \leq .05$ ). Scheffe testi yapılarak gruplardaki anlamlı farklılaşmanın nerede olduğu belirlenmeye çalışılmıştır. 5. sınıfın ortalamasının anlamlı olarak (5. sınıf=40,00), 7. sınıfın ortalaması (7. sınıf=37,25) ve 8. sınıf ortalamasından (8. sınıf=37,30) daha yüksek olarak gözlemlenmiştir.

Ortaokul öğrencilerinin BGEFÖ'den elde ettikleri puanların sınıf düzeyinde anlamlı farklılaştığı tespit edilmiştir ( $F(3, 917)=13,725$ ;  $p \leq .05$ ). Scheffe testi yapılarak gruplardaki anlamlı farklılaşmanın nerede olduğu belirlenmeye çalışılmıştır. 5. sınıfın ortalamasının anlamlı olarak (5. sınıf=71,52), 6. sınıfın ortalamasından (6. sınıf=67,94), 7. sınıfın ortalamasından (7. sınıf=65,76) ve 8. sınıf ortalamasından (8. sınıf=66,48) daha yüksek olarak gözlemlenmiştir.

Öğrencilerin bilgi güvenliği ve etik farkındalık düzeylerinin anne ve baba eğitim düzeyine göre anlamlı farklılık gösterip göstermediğini belirlemek amacıyla ANOVA analizi yapılmıştır. Tablo 9, öğrencilerin BGEFÖ puanlarının anne eğitim durumuna göre ANOVA sonuçları sunulmuştur.

**Tablo 9.** BGEFÖ'den Ortaokul Öğrencilerinin Elde Ettikleri Puanların Anne Eğitim Durumuna Göre Sonuçları

| <i>Faktör</i>       | <i>Anne Eğitim Durumu</i> | <i>N</i> | <i><math>\bar{X}</math></i> | <i>ss</i> | <i>F</i> | <i>p</i> | <i>Anlamlılık</i> |
|---------------------|---------------------------|----------|-----------------------------|-----------|----------|----------|-------------------|
| Kullanıcı Güvenliği | İlkokul (A)               | 264      | 12,20                       | 2,76      | 2,336    | .072     | -                 |
|                     | Ortaokul (B)              | 310      | 12,03                       | 2,70      |          |          |                   |
|                     | Lise (C)                  | 222      | 12,47                       | 2,60      |          |          |                   |
|                     | Üniversite (D)            | 125      | 12,69                       | 2,41      |          |          |                   |
| Veri Güvenliği      | İlkokul (A)               | 264      | 17,18                       | 3,76      | .902     | .140     | -                 |
|                     | Ortaokul (B)              | 310      | 17,35                       | 4,09      |          |          |                   |
|                     | Lise (C)                  | 222      | 17,72                       | 3,70      |          |          |                   |
|                     | Üniversite (D)            | 125      | 17,19                       | 3,97      |          |          |                   |
| Etik                | İlkokul (A)               | 264      | 37,98                       | 6,78      | 7,000    | .000     | C > B<br>D > B    |
|                     | Ortaokul (B)              | 310      | 37,44                       | 6,86      |          |          |                   |
|                     | Lise (C)                  | 222      | 39,52                       | 5,86      |          |          |                   |
|                     | Üniversite (D)            | 125      | 39,85                       | 5,64      |          |          |                   |
| BGEFÖ               | İlkokul (A)               | 264      | 67,37                       | 10,95     | 4,609    | .003     | C > B             |
|                     | Ortaokul (B)              | 310      | 66,84                       | 11,58     |          |          |                   |
|                     | Lise (C)                  | 222      | 69,72                       | 9,48      |          |          |                   |
|                     | Üniversite (D)            | 125      | 69,74                       | 9,13      |          |          |                   |

Tablo 9 incelendiğinde öğrencilerinin Kullanıcı Güvenliği ( $F(3, 917)=2,336$ ;  $p \geq .05$ ) ve Veri Güvenliği ( $F(3, 917)=.902$ ;  $p \geq .05$ ) faktörlerinden elde ettikleri puanın anne eğitim durumuna göre anlamlı farklılaşmadığı tespit edilmiştir. Etik faktöründe ise anne eğitim durumuna göre öğrencilerin elde ettikleri puanların anlamlı farklılaştığı tespit edilmiştir ( $F(3, 917)=7,000$ ;  $p \leq .05$ ). Scheffe testi yapılarak gruplardaki anlamlı farklılaşmanın nerede olduğu belirlenmeye çalışılmıştır. Lise mezunu anne grup ortalamasının (lise=39,52) ve üniversite mezunu anne grup ortalamasının (üniversite=39,85) anlamlı olarak ortaokul mezunu anne eğitim grup ortalamasından (ortaokul=37,44) büyük olduğu belirlenmiştir. Ortaokul öğrencilerinin BGEFÖ'den anne eğitim durumuna göre elde ettikleri puanların anlamlı farklılaştığı tespit edilmiştir ( $F(3, 917)=4,609$ ;  $p \leq .05$ ). Scheffe testi ile hangi gruplar arasında anlamlı farklılığın bulunduğu belirlenmeye çalışılmıştır. Lise mezunu anne grup ortalamasının (lise=69,72) anlamlı olarak ortaokul mezunu anne grup ortalamasından (ortaokul=66,84) yüksek olduğu belirlenmiştir. Tablo 10, öğrencilerin BGEFÖ puanının baba eğitim durumuna göre ANOVA sonuçları sunulmuştur.

**Tablo 10.** BGEFÖ'den Ortaokul Öğrencilerinin Aldığı Puanların Baba Eğitim Durumuna Göre Sonuçları

| <i>Faktör</i>       | <i>Baba Eğitim Durumu</i> | <i>N</i> | <i><math>\bar{X}</math></i> | <i>ss</i> | <i>F</i> | <i>p</i> | <i>Anlamlılık</i> |
|---------------------|---------------------------|----------|-----------------------------|-----------|----------|----------|-------------------|
| Kullanıcı Güvenliği | İlkokul (A)               | 190      | 11,94                       | 2,88      | 3,598    | .013     | D > A             |
|                     | Ortaokul (B)              | 246      | 12,03                       | 2,79      |          |          |                   |
|                     | Lise (C)                  | 299      | 12,43                       | 2,56      |          |          |                   |
|                     | Üniversite (D)            | 186      | 12,70                       | 2,35      |          |          |                   |
| Veri Güvenliği      | İlkokul (A)               | 190      | 17,19                       | 3,87      | 1,161    | .323     | -                 |
|                     | Ortaokul (B)              | 246      | 17,10                       | 3,94      |          |          |                   |
|                     | Lise (C)                  | 299      | 17,67                       | 3,76      |          |          |                   |
|                     | Üniversite (D)            | 186      | 17,43                       | 4,02      |          |          |                   |

|       |                |     |       |       |       |      |                |
|-------|----------------|-----|-------|-------|-------|------|----------------|
| Etik  | İlkokul (A)    | 190 | 38,21 | 6,15  | 7,944 | .000 | C > B<br>D > B |
|       | Ortaokul (B)   | 246 | 36,89 | 7,02  |       |      |                |
|       | Lise (C)       | 299 | 39,03 | 6,49  |       |      |                |
|       | Üniversite (D) | 186 | 39,68 | 5,82  |       |      |                |
| BGEFÖ | İlkokul (A)    | 190 | 67,35 | 10,33 | 6,049 | .000 | C > B<br>D > B |
|       | Ortaokul (B)   | 246 | 66,03 | 11,44 |       |      |                |
|       | Lise (C)       | 299 | 69,15 | 10,42 |       |      |                |
|       | Üniversite (D) | 186 | 69,82 | 9,89  |       |      |                |

Tablo 10 incelendiğinde Veri Güvenliği faktöründen ortaokul öğrencilerinin elde ettikleri puanın baba eğitim durumuna göre anlamlı farklılığın olmadığı belirlenmiştir ( $F(3, 917)=1,161$ ;  $p \geq .05$ ). Kullanıcı Güvenliği faktöründen öğrencilerin elde ettikleri puanın, baba eğitim durumuna göre anlamlı farklılığın olduğu belirlenmiştir ( $F(3, 917)=3,598$ ;  $p \leq .05$ ). Scheffe testi yapılarak gruplardaki anlamlı farklılaşmanın nerede olduğu belirlenmeye çalışılmıştır. Üniversite mezunu baba grubunda olanların ortalamasının (üniversite=12,70) anlamlı olarak ilkokul mezunu baba eğitim grubunda olanların ortalamasından (ilkokul=11,94) büyük olduğu belirlenmiştir. Ortaokul öğrencilerinin Etik faktöründen ettikleri puanın, baba eğitim durumuna göre anlamlı farklılaştığı bulunmuştur ( $F(3, 917)=7,944$ ;  $p \leq .05$ ). Scheffe testi yapılarak gruplardaki anlamlı farklılaşmanın nerede olduğu belirlenmeye çalışılmıştır. Lise mezunu baba grubunda olanların ortalamasının (lise=39,03) ve üniversite mezunu baba grubunda olanların ortalamasının (üniversite=39,68) anlamlı olarak ortaokul mezunu baba eğitim grubunda olanların ortalamasından (ortaokul=36,89) büyük olduğu belirlenmiştir. Öğrencilerin BGEFÖ'den elde ettikleri puanın baba eğitim durumuna göre anlamlı farklılığın olduğu bulunmuştur ( $F(3, 917)=6,049$ ;  $p \leq .05$ ). Scheffe testi yapılarak gruplardaki anlamlı farklılaşmanın nerede olduğu belirlenmeye çalışılmıştır. Lise mezunu baba grubunda olanların ortalamasının (lise=69,15) ve üniversite mezunu baba grubunda olanların ortalamasının (üniversite=69,82) anlamlı olarak ortaokul baba grubunda olanların ortalamasından (ortaokul=66,03) büyük olduğu belirlenmiştir.

### Tartışma ve Sonuç

Bilişim ve mobil teknolojilerin kullanımı artmakta, bu teknolojileri kullanan bireylerin yaşı ise giderek düşmektedir (Pekyürek vd., 2020). Bilişim teknolojilerindeki hızlı değişimlerle birlikte bilgi güvenliği ve farkındalığının önemi de artmıştır (Çetinkaya vd., 2017). İnsan faktörü, bilgi sistemlerinde en zayıf halka olarak kabul edildiğinden kullanıcı farkındalığı kritik öneme sahiptir (Güldüren, 2015). Alanyazındaki çalışmalar genellikle yetişkinler, akademisyenler, öğretmenler, lisans ve lise öğrencileri üzerine odaklanmışken ortaokul öğrencilerine yönelik sınırlı çalışmalar bulunmaktadır. Benzer şekilde etik farkındalığı üzerine yapılan çalışmalarında lise ve lisans düzeyinde öğrenciler ve meslek ve iş gruplarında yer alan yetişkinlere yönelik yoğunlaştığı görülmekte ve ortaokul öğrencilerine yönelik sınırlı çalışmalar bulunmaktadır. Ayrıca alanyazında ortaokul öğrencilerinin bilgi güvenliği ve etik farkındalığının birlikte ele alındığı bir ölçek bulunmamaktadır. Bu bağlamda bilgi güvenliği ve etik farkındalığını ortaokul öğrencileri için ölçmek için geçerli ve güvenilir bir ölçek geliştirilmiştir.

BGEFÖ'nün yapı geçerliliği için faktör analizi yöntemi kullanılmıştır. 621 öğrenci üzerinde uygulanan bu ölçeğin faktör analizine uygun olup olmadığını belirlemek için öncelikle KMO katsayısı hesaplanmış ve ardından Barlett küresellik testi uygulanmıştır. BGEFÖ için elde edilen KMO katsayısı ve Barlett küresellik testi sonuçları, faktör analizini yapmak için verilerin uygun olduğunu ortaya koymuştur.

Ölçeğin yapısını incelemek için Açımlayıcı Faktör Analizi uygulanmıştır. Bu analizde varimax dik döndürme yöntemi kullanılarak düşük faktör yüklerine sahip maddeler ölçekten çıkarılmıştır. Geriye kalan maddelerin faktör yüklerinin .422 ile .834 arasında değiştiği tespit edilmiştir. Analiz sonucunda dokuz madde Etik, beş madde Veri Güvenliği ve üç madde Kullanıcı Güvenliği olmak üzere ölçeğin üç faktörden oluştuğu belirlenmiştir. Bu üç faktör, toplam varyansın %54,100'ünü açıkladığı tespit edilmiştir. Oluşturulan bu üç boyutlu BGEFÖ'nün faktör yapısını doğrulamak için Doğrulamalı Faktör Analizi yapılmış ve sonuçları Açımlayıcı Faktör Analizi sonuçlarıyla uyumlu bulunmuştur.

Sonuçlar, BGEFÖ alt boyutlar arası korelasyon katsayılarının .460 ile .464 arasında değiştiğini ortaya koymuştur. Bununla birlikte bu alt boyutların iç tutarlılığı, Cronbach alfa kullanılarak değerlendirilmiştir. Nunnally (1978) ve Büyüköztürk (2015) tarafından önerilen ve yaygın olarak kabul gören bir ölçüt, güvenilirlik katsayılarının 0,70'i aşması gerektiğini belirtmektedir. Özdamar (2013) ise 0,60-0,90 arasındaki güvenilirlik katsayılarını oldukça güvenilir olarak tanımlamaktadır. BGEFÖ'nün güvenilirlik katsayısı .896 olarak belirlenmiş olup, bu değer oldukça güvenilir bir seviyede ve yüksek güvenilirlik sınırına oldukça yakındır. BGEFÖ için yapılan analizler ve elde edilen bulgular, ölçeğin ortaokul öğrencilerinin bilgi güvenliği ve etik farkındalık seviyelerini ölçmede geçerli ve güvenilir bir araç olduğunu göstermektedir.

Öğrencilerin veri güvenliğine yönelik farkındalığının en düşük, etik farkındalığına yönelik ise daha yüksek olduğu belirlenmiştir. Genel olarak ölçekten elde edilen puanlara bakıldığında, öğrencilerin bilgi güvenliği ve etik farkındalıklarının yüksek düzeyde olduğu, ancak veri güvenliği farkındalığının orta düzeyde kaldığı söylenebilir. Benzer bir şekilde Tekerek ve Tekerek (2013) tarafından çalışmayla bu bulgu paralellik göstermektedir. Ortaokul düzeyinde yapılan diğer çalışmalarda da (Beder ve Ergün, 2015; Özen-Serter, 2021), bilgi güvenliği farkındalığının genellikle düşük ve orta seviyelerde olduğu tespit edilmiştir. Lise, lisans ve yetişkin grupları üzerinde yapılan çalışmalarda ise (Dönmez, 2019; Hacımustafaoğlu, 2019; Karaoğlu-Yılmaz vd., 2017; Slusky ve Partow, 2012) bilgi güvenliği alt boyutlarında yüksek farkındalık, etik farkındalık alt boyutlarında ise orta ve düşük düzeylerde sonuçların çıktığı görülmektedir. BGEFÖ'den elde edilen bulgular ile önceki çalışmalar arasındaki bu farkın teknoloji kullanım yaşının hızla düşmesi ve özellikle pandemi döneminde öğrencilerin uzaktan eğitimle bilişim teknolojileri, mobil cihazlar ve iletişim sistemlerini daha yoğun kullanmalarıyla ilgili olabileceği düşünülmektedir.

Çalışma sonuçlarına göre öğrencilerin bilgi güvenliği ve etik farkındalığının yüksek olduğu, ancak veri güvenliği konusunda orta düzeyde oldukları tespit edilmiştir. Bu bulgu, Tekerek ve Tekerek (2013) tarafından yapılan çalışmanın sonuçlarıyla örtüşmektedir. Ortaokul düzeyinde Özen-Serter (2021) ile Beder ve Ergün (2015) tarafından gerçekleştirilen araştırmalarda, bilgi güvenliği farkındalığının düşük ve orta seviyelerde olduğu ortaya çıkmıştır. Lise, üniversite ve farklı yetişkin gruplarla yapılan çalışmalarda (Dönmez, 2019; Hacımustafaoğlu, 2019; Karaoğlu-Yılmaz vd., 2017; Slusky ve Partow, 2012), bilgi güvenliğiyle ilgili alt boyutlara yönelik yüksek farkındalık gösterilirken etik farkındalığa dair alt boyutlarda ise orta ve düşük seviyelerde kaldıkları görülmektedir.

5. sınıf öğrencilerinin etik farkındalığı, veri güvenliği ve kullanıcı güvenliği boyutlarına göre genel olarak ölçekten aldıkları puanlar diğer sınıf düzeylerine kıyasla daha yüksek çıkmıştır. Bireylerin eğitim düzeyleri arttıkça veya farklı bir değişle öğrencilerin sınıf seviyeleri yükseldikçe bilgi güvenliği farkındalığının artmayabileceği görüşüyle uyumlu olarak değerlendirilebilir (Van De Mortel, 2021). Ayrıca 5. sınıf öğrencilerinin bilgi güvenliği ve etik farkındalığının yüksek çıkması özellikle 5. ve 6. sınıflarda bilişim teknolojileri ve yazılım derslerinin programda yer alması, bu sınıf seviyesindeki öğrencilerin farkındalık düzeylerinin diğer sınıflara kıyasla daha yüksek olmasına katkı sağlamış olabilir. Bununla beraber çalışmada, anne eğitim durumuna göre öğrencilerin veri güvenliği ve kullanıcı güvenliği farkındalıklarının anlamlı bir fark göstermediği sonucuna ulaşılmıştır. Ancak etik farkındalığın anne eğitim düzeyi lise ve üniversite olan öğrencilerin, anne eğitim düzeyi ortaokul olan öğrencilerden anlamlı ölçüde farklı olduğu gözlemlenmiştir. Bu bulgu, anne eğitim düzeyiyle öğrencilerin bilgi güvenliği ve etik farkındalığının doğru orantılı bir şekilde arttığını göstermektedir. Baba eğitim durumunun etkilerine bakıldığında ise, veri güvenliği farkındalığı üzerinde anlamlı bir etki bulunamamıştır. Ancak kullanıcı güvenliği farkındalığında baba eğitim durumu üniversite olan öğrenciler ile ilkokul olanlar arasında anlamlı bir fark olduğu tespit edilmiştir. Aynı şekilde etik farkındalıkta baba eğitim düzeyi lise ve üniversite olan öğrencilerin, baba eğitim durumu ortaokul olanlara kıyasla daha yüksek farkındalık sergilediği sonucuna ulaşılmıştır. Öğrencilerin bilgi güvenliği ve etik farkındalıklarının baba eğitim düzeyi ile de paralel olarak arttığı sonucuna ulaşılmıştır. Bu bulgular, Özen-Serter'in (2021) çalışmasındaki sonuçlarla da benzerlik göstermektedir.

Bu araştırmada ortaokul öğrencilerinin bilgi güvenliği ve etik farkındalık düzeylerini ölçmeye yönelik geçerli ve güvenilir bir ölçek geliştirilmiş ve öğrencilerin farkındalık düzeyleri çeşitli değişkenler açısından incelenmiştir. Araştırma bulguları doğrultusunda öğrencilerin özellikle veri güvenliği farkındalık düzeylerinin diğer boyutlara göre daha düşük olduğu göz önüne alındığında, bilgi güvenliği ve etik konularına yönelik daha kapsamlı ve uygulamalı içeriklerin bilişim teknolojileri ve yazılım derslerine entegre edilmesi önerilmektedir. Bununla beraber 5. ve 6. sınıf öğrencilerinin daha yüksek farkındalığa sahip olmaları, bu yaş grubunun bilgi güvenliği ve etik konularında eğitim

açısından uygun bir dönem olduğunu ve öğrencilere farkındalık kazandırıcı etkinliklerin yapıldığını göstermektedir. Fakat farkındalık kazandırıcı etkinliklerin bu yaş gruplarından itibaren kademeli olarak başlatılmasıyla beraber öğrencilerin ileriki dönemlerde de yaş gruplarına uygun bilgi güvenliği ve etik konularında bilinçlendirilmesine yönelik etkinliklerin devamlı hâle getirilmesi önerilmektedir. Ayrıca araştırma sonuçlarına göre ebeveynlerin eğitim düzeyleri öğrencilerin farkındalıklarını etkilemektedir. Bu bağlamda, okullarda ailelere yönelik bilgi güvenliği ve dijital etik konularında bilgilendirme seminerleri ve rehberlik çalışmaları düzenlenmesi önerilmektedir.

Gelecek çalışmalara yönelik geliştirilen BGEFÖ farklı yaş gruplarında, farklı sosyoekonomik düzeylerdeki öğrencilerle ve çeşitli bölgesel örneklerle uygulanarak ölçeğin geçerlilik ve güvenilirliğinin desteklenmesi önerilmektedir. Bu bağlamda, farklı bölgesel ya da kültürel bağlamlarda yapılan karşılaştırmalı çalışmalar, öğrencilerin bilgi güvenliği ve etik farkındalık düzeylerinin sosyo-kültürel etkilerle nasıl şekillendiğini de ortaya koyabilir. Ayrıca bu çalışmada kullanılan ölçek, ileride yapılacak araştırmalarda internet kullanım süresi veya dijital oyun oynama sıklığı gibi farklı değişkenlerle ilişkilendirilerek derinlemesine analizler yapılabilir ve nitel araştırmalarla desteklenerek öğrencilerin bilgi güvenliği ve etik kavramlarına ilişkin algıları daha detaylı olarak incelenebilir. Bu bağlamda yürütülecek gelecekteki çalışmaların yalnızca öğrenci örneklem grubuyla sınırlı kalmayıp aynı zamanda öğrencilerin ebeveynlerini de kapsayacak şekilde genişletilmesi faydalı olacaktır. Özellikle ebeveynlerin dijital teknolojilere yönelik tutumları, çocuklarıyla bu konudaki iletişim düzeyleri ve dijital güvenlik konularında üstlendikleri rehberlik rolleri detaylı olarak incelenebilir. Bu tür bir yaklaşım, öğrencilerin bilgi güvenliği ve etik farkındalık düzeylerinin oluşumunda aile faktörünün etkisini daha kapsamlı bir biçimde ortaya koyarak alanyazına önemli katkılar sağlayabilecektir. Bunlara ek olarak oyun temelli öğrenme, senaryo temelli öğretim veya sanal ve artırılmış gerçeklik uygulamalarıyla desteklenen farklı öğretim yöntemlerinin bilgi güvenliği ve etik farkındalık üzerindeki etkisini değerlendirmek amacıyla deneysel araştırmalar yapılabilir.

### Kaynaklar

- Akgün, E. & Ustun, A. B. (2023). Mobil artırılmış gerçeklikle öğrenmeye yönelik içerik analizi. *Dokuz Eylül Üniversitesi Buca Eğitim Fakültesi Dergisi*(56), 362-383. <https://doi.org/10.53444/deubefd.1153240>
- Akıncan, E. (2022). *Ortaokul öğrencilerinin dijital okuryazarlık, dijital bağımlılık ve bilgi güvenliği farkındalık düzeylerinin incelenmesi*. (Yüksek Lisans Tezi). <https://tez.yok.gov.tr> sayfasından erişilmiştir.
- Anwar, M. S., Hussain, A., Javaid, A., Ali, M., & Khalid, A. (2019). State-of-the-art rootkit detection and removal techniques: A systematic literature review. *Computers & Electrical Engineering*, 74, 547-566.
- Aycock, J. (2006). *Computer viruses and malware*. Springer.

- Balcı, A. (2018). *Sosyal bilimlerde araştırma yöntem, teknik ve ilkeler*. Pegem Akademi.
- Beauchamp, T. L. & Childress, J. F. (2013). *Principles of biomedical ethics*. Oxford University.
- Beder, A. & Ergün, E. (2015). Ortaokul öğrencilerinin güvenli internet kullanım durumlarının belirlenmesi. *Journal of Educational Sciences & Practices*, 14(27), 23-41.
- Bhatia, S., Singh, R., & Bansal, D. (2017). Malware detection techniques: A brief review and comparison. *Procedia Computer Science*, 122, 478-485.
- Biryukov, A., Pustogarov, I., & Weinmann, R. P. (2013). Trawling for tor hidden services: Detection, measurement, deanonymization. *IEEE Symposium on Security and Privacy* içinde (s. 125-141). Berkeley.
- Brown, T. A. (2006). *Confirmatory factor analysis for applied research*. The Guilford.
- Büyüköztürk, Ş. (2015). *Sosyal bilimler için veri analizi el kitabı* (21. b.). Pegem Akademi.
- Büyüköztürk, Ş., Çakmak, E. B., Akgün, Ö. E., Karadeniz, Ş., & Demirel, F. (2020). *Eğitimde bilimsel araştırma yöntemleri* (29. b.). Pegem Akademi.
- Cai, L., Xing, X., Zhang, Y., Xu, X., & Guan, L. (2018). Detecting android malware through deceptive user interfaces. *IEEE Transactions on Dependable and Secure Computing*, 15(3), 438-451.
- Christodorescu, M., Jha, S., Seshia, S. A., Song, D., & Bryant, R. E. (2005). Semantics-aware malware detection. *IEEE symposium on security and privacy* içinde (s. 32-44). Oakland.
- Costello, A. B. & Osborne, J. W. (2005). Exploratory factor analysis: Four recommendations for getting the most from your analysis. *Practical Assessment, Research, and Evaluation*, 10(7), 1-9.
- Çakmak, E. K., Çebi, A., & Kan, A. (2014). E-öğrenme ortamlarına yönelik sosyal bulunuşluk ölçeği geliştirme çalışması. *Kuram ve Uygulamada Eğitim Bilimleri*, 14(2), 755-768.
- Çetinkaya, L., Güldüren, C., & Keser, H. (2017). Öğretmenler için Bilgi Güvenliği Farkındalık Ölçeği (BGFÖ) geliştirme çalışması. *Milli Eğitim Dergisi*, 46(216), 33-52.
- Çokluk, Ö., Şekercioğlu, G., & Büyüköztürk, Ş. (2014). *Sosyal bilimler için çok değişkenli istatistik: SPSS ve LISREL Uygulamaları*. Pegem Akademi.
- Dönmez, G. (2019). *Lise öğrencilerinin bilgi güvenliği farkındalığı ile dijital okuryazarlığı arasındaki ilişkinin incelenmesi*. (Yüksek Lisans Tezi). <https://tez.yok.gov.tr> sayfasından erişilmiştir.
- Fabrigar, L. R., Wegener, D. T., & MacCallum, R. C. (1999). Evaluating the use of exploratory factor analysis in psychological research. *Psychological Methods*, 4(3), 272-299.
- Feng, M., Gehrke, J., & Srikant, R. (2004). Spam: A review. *ACM SIGMOD Record*, 33(4), 22-37.

- Fidan, M. (2016). Bilişim etiği boyutlarına göre bilişim teknolojileri ve yazılım dersi öğretim programı kazanımlarının incelenmesi. *Kastamonu Eğitim Dergisi*, 24(4), 1641-1654.
- Field, A. (2009). *Discovering statistics using SPSS* (3. b.). Sage.
- Filiol, E. (2011). *Computer viruses and malware*. Science & Business Media.
- Floridi, L. (2013). *The ethics of information*. Oxford University.
- Guilford, J. P. (1954). *Psychometric methods* (2. b.). McGraw-Hill.
- Güldüren, C. (2015). Yükseköğretim kurumlarındaki öğretim elemanlarının bilgi güvenliği farkındalık düzeylerinin değerlendirilmesi. (Doktora Tezi). <https://tez.yok.gov.tr> sayfasından erişilmiştir.
- Güldüren, C., Çetinkaya, L., & Keser, H. (2016). Ortaöğretim Öğrencilerine Yönelik Bilgi Güvenliği Farkındalık Ölçeği (BGFÖ) geliştirme çalışması. *İlköğretim Online*, 15(2), 682-695.
- Güriş, S. & Astar, M. (2015). *Bilimsel araştırmalarda SPSS ile istatistik*. Der.
- Hacımustafaoğlu, R. (2019). Ortaöğretim öğrencilerinin bilgi güvenliği farkındalık düzeylerinin siber mağdur olma durumlarına etkisinin incelenmesi (Üsküdar örneği). (Yüksek Lisans Tezi). <https://tez.yok.gov.tr> sayfasından erişilmiştir.
- Hadnagy, C. (2011). *Social engineering: The art of human hacking*. John Wiley & Sons.
- Herath, T. & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, 18(2), 106-125.
- Himma, K. E. & Tavani, H. T. (2008). *The handbook of information and computer ethics*. Wiley Sons.
- Huck, S. W. (2012). *Reading statistics and research*. Pearson.
- Hutcheson, G. & Sofroniou, N. (1999). *The multivariate social scientist. Introductory statistics using generalized linear models*. Sage.
- Ismagilova, E., Slade, E., Rana, N. P., & Dwivedi, Y. K. (2020). The effect of characteristics of source credibility on consumer behaviour: A meta-analysis. *Journal of Retailing and Consumer Services*, 53, Article 1017362. <https://doi.org/10.1016/j>
- Janczewski, L. J. & Colarik, A. M. (2004). *Cyber warfare and cyber terrorism*. IGI Global.
- Johnson, D. G. (2009). *Computer ethics* (4. b.). Pearson Education.
- Jöreskog, K. G. & Sörbom, D. (1993). *LISREL 8: Structural equation modeling with the SIMPLIS command language*. Lawrence Erlbaum.
- Kaiser, H. F. (1960). The application of electronic computers to factor analysis. *Educational and Psychological Measurement*, 20(1), 141-151. <https://doi.org/10.1177/001316446002000116>
- Kaiser, H. F. (1974). An index of factorial simplicity. *Psychometrika*, 39, 31-36.

- Kapanoğlu, G. (2016). *Öğretmenlerin bilgi güvenliği farkındalığının incelenmesi*. (Yüksek Lisans Tezi). <https://tez.yok.gov.tr> sayfasından erişilmiştir.
- Kara, M. (2018). *Endüstriyel nesnelerin internetinde hızlı ve güvenli veri iletimi*. (Yüksek Lisans Tezi). <https://tez.yok.gov.tr> sayfasından erişilmiştir.
- Karaoğlu-Yılmaz, F. G., Ustun, A. B., Zhang, K., & Yılmaz, R. (2024). Smartphone addiction, nomophobia, depression, and social appearance anxiety among college students: A correlational study. *Journal of Rational-Emotive & Cognitive-Behavior Therapy*, 42(2), 305-321.
- Karaoğlu-Yılmaz, F. G. & Çavuş-Ezin, Ç. (2017). Ebeveynlerin bilgi güvenliği farkındalıklarının incelenmesi. *Eğitim Teknolojisi Kuram ve Uygulama*, 7(2), 41-57.
- Karaoğlu-Yılmaz, F. G., Yılmaz, R., & Sezer, B. (2014). Üniversite öğrencilerinin güvenli bilgi ve iletişim teknolojisi kullanım davranışları ve bilgi güvenliği eğitime genel bir bakış. *Bartın Üniversitesi Eğitim Fakültesi Dergisi*, 3(1), 176-199.
- Karasar, N. (2009). *Bilimsel araştırma yöntemi*. Nobel.
- Kass, R. A. & Tinsley, H. E. A. (1979). Factor analysis. *Journal of Leisure Research*, 11, 120-138.
- Kaufman, C., Perlman, R., & Speciner, M. (2002). *Network security: Private communication in a public world*. Prentice Hall.
- Kline, P. (1994). *An easy guide to factor analysis*. Routledge.
- Kline, P. (2000). *Handbook of psychological testing* (2. b.). Routledge.
- Kline, R. S. (2011). *Principles and practice of structural equation modeling*. The Guilford Press.
- Kowalski, R. M. & Limber, S. P. (2012). Psychological, physical and academic correlates of cyberbullying and traditional bullying. *Journal of Adolescent Health*, 53(1), 13-20.
- Krombholz, K., Hobel, H., & Huber, M. (2015). Advances in detecting spam, bots, and malware on Twitter. *IEEE Transactions on Dependable and Secure Computing*, 12(3), 337-349.
- Maleki, H. R., Shahgholian, A., & Lutfi, A. (2016). The role of human factor in information security. *Procedia Computer Science*, 102, 602-608.
- Mart, İ. (2012). *Bilişim kültüründe bilgi güvenliği farkındalığı*. (Yüksek Lisans Tezi). <https://tez.yok.gov.tr> sayfasından erişilmiştir.
- Mason, R. O. (1986). Four ethical issues of the information age. *MIS Quarterly*, 10(1), 5-12.
- McKeon, N. (2011). Ethical issues in intellectual property. *American Medical Association Journal of Ethics*, 13(2), 132-136.
- McMillan, J. H. & Schumacher, S. (2001). *Research in education: A conceptual introduction* (2. b.). Longman.
- McNurlin, B. & Sprague, R. (2006). *Information systems management in practice*. Prentice Hall.

- Moor, J. H. (2008). Why we need better ethics for emerging technologies. *Ethics and Information Technology*, 10(2-3), 93-104.
- Moore, D., Paxson, V., Savage, S., Shannon, C., Staniford, S., & Weaver, N. (2003). Inside the slammer worm. *IEEE Security & Privacy*, 1(4), 33-39.
- Norris, P. & Pernia, E. M. (2019). Digital divide and e-government: Evidence from the European Union. *Policy & Internet*, 11(1), 102-121.
- Nunnally, J. C. (1978). *Psychometric theory* (2. b.). McGraw-Hill.
- Özdamar, K. (2013). *Paket programlar ile istatistiksel veri analizi-1: SPSS-MINITAB*. Nisan.
- Özen-Serter, B. (2021). *Ortaokul öğrencilerinin bilgi güvenliği farkındalık düzeyinin belirlenmesi*. (Yüksek Lisans Tezi). <https://tez.yok.gov.tr> sayfasından erişilmiştir.
- Öztezcan, B. A. (2017). *Bilgi güvenliği farkındalığı üzerine bir araştırma: Marmara Üniversitesi örneği*. (Yüksek Lisans Tezi). <https://tez.yok.gov.tr> sayfasından erişilmiştir.
- Pekyürek, M. F., Sağlam, Z., & Ustun, A. B. (2020). MIT App Inventor ve Android Studio kullanılarak tasarlanmış mobil uygulamanın performans karşılaştırması. *Bilgi ve İletişim Teknolojileri Dergisi*, 2(2), 161-181.
- Rosenstand, N. (2011). *The moral of the story: An introduction to ethics*. McGraw-Hill.
- Schwartz, M. S. (2017). *Corporate social responsibility*. Routledge.
- Seferoğlu, S. S., Yıldız-Durak, H., Karaoğlu-Yılmaz, G., & Yılmaz, R. (2018). Bilgi güvenliği farkındalığı ve bilgi güvenliği politikalarıyla ilgili bir inceleme. B. Akkoyunlu, A. İşman & H. F. Odabaşı (Ed.), *Eğitim teknolojileri okumaları içinde* (s. 29-43). TOJET ve Sakarya Üniversitesi.
- Selwyn, N. (2003). Apart from technology: Understanding people's non-use of information and communication technologies in everyday life. *Technology in Society*, 25(1), 99-116.
- Slusky, L. & Partow, P. (2012). Students information security practices and awareness. *Journal of Information Privacy and Security*, 8(4), 3-26.
- Smith, T. D. & McMillan, B. F. (2001). *A primer of model fit indices in structural equation modeling*. The Annual Meeting of the Southwest Educational Research Association'da sunulmuş bildirisi, 1-3 Şubat, New Orleans, LA.
- Stevens, J. P. (2002). *Applied multivariate statistics for the social sciences* (4. b.). Lawrence Erlbaum.
- Sümer, N. (2000). Yapısal eşitlik modelleri: Temel kavramlar ve örnek uygulamalar. *Türk Psikoloji Yazıları*, 3(6), 49-74.
- Szor, P. (2005). *The art of computer virus research and defense*. Addison-Wesley Professional.

- Tabachnick, B. G. & Fidell, L. S. (2015). *Çok değişkenli istatistiklerin kullanımı* (M. Baloğlu, Çev. Ed.). Nobel.
- Talan, T. & Aktürk, C. (2021). Ortaöğretim öğrencilerinin dijital okuryazarlık ve bilgi güvenliği farkındalığı seviyelerinin incelenmesi. *Kahramanmaraş Sütçü İmam Üniversitesi Sosyal Bilimler Dergisi*, 18(1), 158-180.
- Tavani, H. T. (2007). Informational privacy: Concepts, theories, and controversies. *Handbook of Information and Computer Ethics*, 310-335.
- Tavşancıl, E. (2005). *Tutumların ölçülmesi ve SPSS ile veri analizi*. Nobel.
- Tekerek, M. & Tekerek, A. (2013). Öğrencilerin bilgi güvenliği farkındalığı üzerine bir araştırma. *Turkish Journal of Education*, 2(3), 61-70.
- Tekin, A. & Polat, E. (2016). Ortaokul öğrenci velilerinin güvenli internet kullanımı farkındalığı. *Journal of Instructional Technologies and Teacher Education*, 5(2), 80-92.
- Thompson, B. (2008). *Foundations of behavioral statistics: An insight-based approach*. Guilford.
- Topal, M. & Akgün, Ö. E. (2015). Investigation of educational internet use self-efficacy perceptions of prospective teachers enrolled at a faculty of education: Sakarya University sample. *Kastamonu Education Journal*, 23(1), 343-364.
- Van De Mortel, K. (2021). *De Invloed Van Opleiding op information security awareness the influence of education on information security awareness*. (Yüksek Lisans Tezi). [https://research.ou.nl/ws/portalfiles/portal/41057432/Mortel\\_vd\\_K\\_IM9806\\_AF\\_BPMIT\\_scriptie\\_PURE.pdf](https://research.ou.nl/ws/portalfiles/portal/41057432/Mortel_vd_K_IM9806_AF_BPMIT_scriptie_PURE.pdf) sayfasından erişilmiştir.
- Vilander, J. (2021). *Bridging the knowing-doing gap: The role of attitude in information security awareness*. (Yüksek Lisans Tezi). <https://jyx.jyu.fi/bitstreams/555c8f8d-435f-4dbf-921d-6593b8240097/download> sayfasından erişilmiştir.
- Vural, Y. & Sağiroğlu, Ş. (2010). Veritabanı yönetim sistemleri güvenliği: Tehditler ve korunma yöntemleri. *Politeknik Dergisi*, 13(2), 71-81.
- Wagner, A. E. & 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.
- Wang, J., Niiya, M., & Mark, G. (2019). Cyberbullying: A socio-technological perspective. *Computers in Human Behavior*, 91, 277-282.
- Whitman, M. E. & Mattord, H. J. (2016). *Principles of Information Security*. Cengage Learning.
- Yılmaz, E. (2015). *Öğretmenlerin dijital veri güvenliği farkındalığı*. (Doktora Tezi). <https://tez.yok.gov.tr> sayfasından erişilmiştir.

Zhen, J., Dong, K., Xie, Z., & Chen, L. (2022). Factors influencing employees' information security awareness in the telework environment. *Electronics*, 11(21), 1-14.

### Extended Summary

The development of information technologies and the applications connected to these technologies has increased the importance of information security and awareness regarding this issue. (Çetinkaya et al., 2017). In this context, since the human factor is often the weakest link in the systems that create and protect information, user awareness plays a critical role (Güldüren, 2015). Today, the usage rates of computer and mobile technologies are rapidly increasing, and the age range of those using these technologies is becoming increasingly younger. A large portion of the studies conducted on information security awareness have focused on individuals in the business world, academics, teachers, undergraduate students, and high school students (Akıncan, 2022; Güldüren et al., 2016; Hacımustafaoğlu, 2019; Kapanoğlu, 2016; Karaoğlu-Yılmaz and Çavuş-Ezin, 2017; Karaoğlu-Yılmaz et al., 2014; Mart, 2012; Talan and Aktürk, 2021; Tekerek and Tekerek, 2013; Tekin and Polat, 2016; Topal and Akgün, 2015; Van De Mortel, 2021; Vilander, 2021; Zhen et al., 2022). However, studies in this area targeting middle school students are limited. When examining the existing studies, it is apparent that those conducted with middle school students often utilize information security awareness scales and surveys designed for adults. For example, Özen-Serter (2021) adapted a scale developed for high school students for use with middle school students. Furthermore, while there is research aimed at developing students' ethical awareness, it has been observed that studies addressing ethical awareness in middle school groups, where the foundations of this awareness are laid, are limited (Fidan, 2016).

The literature emphasizes the need to address students' shortcomings in information security, prevent potential dangers, and structure curricula accordingly (Seferoğlu et al., 2018). In this context, it is necessary to measure middle school students' awareness levels regarding the threats they face while using technology and the adequacy of their ethical awareness. However, there is a need in the literature for a reliable and valid measurement tool to assess the level of information security and ethical awareness of middle school students. In this regard, the main aim of this study is to develop a scale to measure the level of information security and ethical awareness of students at the middle school level. Additionally, a secondary aim of the study is to determine students' levels of information security and ethical awareness through the developed scale, and to investigate whether these levels differ based on grade level and the educational level of the parents.

Within the main aim of this study, a scale for information security and ethical awareness for middle school students was developed in the first phase, with the participation of 621 students. In the second phase, a survey model was used to determine whether middle school students' levels of information security and ethical awareness differ based on grade level and parental education. The

purpose of the survey model is to identify and clearly describe the nature and characteristics of human communities, institutions, objects, and events (Büyüköztürk et al., 2020; McMillian and Schumacher, 2001).

To examine the construct validity of the Information Security and Ethical Awareness Scale, factor analysis was conducted. To determine if the scale administered to 621 students was suitable for factor analysis, the KMO coefficient was calculated and the Bartlett's test of sphericity was applied. The KMO coefficient obtained for the scale (.932) and the results of the Bartlett's test of sphericity ( $\chi^2=3792.329$ ;  $df=136$ ;  $p=.000$ ) indicated that the data were suitable for factor analysis.

Exploratory factor analysis was conducted using the varimax rotation method, and items with low factor loadings were removed from the scale. The factor loadings of the remaining 17 items ranged from .422 to .834. It was determined that the scale consists of three factors: User Security (three items), Data Security (five items), and Ethics (nine items). These factors explain 54.100% of the total variance. To test the accuracy of the three-dimensional factor structure of the scale, confirmatory factor analysis was performed, and the results were found to be consistent with the exploratory factor analysis.

It was found that the correlation coefficients between the sub-dimensions of the scale ranged from 0.460 to 0.464. The reliability coefficient of the scale was determined to be 0.896, which was at a highly reliable level and very close to the high reliability limit. The analyses performed for the scale and the findings showed that the scale was a valid and reliable tool for measuring the information security and ethical awareness levels of middle school students.

Middle school students had the lowest awareness regarding the data security factor and higher awareness regarding the ethics factor. Overall, when examining the scores obtained from the scale, it can be said that students' information security and ethical awareness were at a high level, but their data security awareness remained at a moderate level. It was concluded that students' user security and data security awareness did not show a significant difference based on the mother's education level. However, it was observed that ethical awareness was significantly different for students whose mothers had a university or high school education compared to those whose mothers had a middle school education. This finding suggested that middle school students' information security and ethical awareness increased proportionally with the mother's level of education. When looking at the effects of the father's education level, no significant impact was found on data security awareness. However, a significant difference was found in user security awareness between students whose fathers had a university education and those whose fathers had a primary school education. Similarly, in ethical awareness, it was seen that students whose fathers had a high school or university education exhibited higher awareness compared to those whose fathers had a middle school education. It was concluded

that middle school students' information security and ethical awareness also increased in parallel with the father's level of education.

### Ekler

#### EK 1: Bilgi Güvenliği ve Etik Farkındalığı Ölçeği (BGEFÖ)

| <b>BİLGİ GÜVENLİĞİ VE ETİK FARKINDALIĞI<br/>ÖLÇEĞİ</b>                                                                                                                                                       | <b>Kesinlikle<br/>Katılmıyorum</b> | <b>Katılmıyorum</b> | <b>Kararsızım</b> | <b>Katılıyorum</b> | <b>Kesinlikle<br/>Katılıyorum</b> |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------|---------------------|-------------------|--------------------|-----------------------------------|
| Aşağıda sizlere yöneltilen ifadelere "Kesinlikle Katılmıyorum", "Katılmıyorum", "Kararsızım", "Katılıyorum" ve "Kesinlikle Katılıyorum" şeklindeki seçeneklerden yalnızca size en yakın olan birini seçiniz. |                                    |                     |                   |                    |                                   |
| 1.Bilgisayar, telefon ve tablet gibi cihazlarımın şifrelerini belirlerken başkalarının tahmin edemeyeceği şifreler belirlerim.                                                                               |                                    |                     |                   |                    |                                   |
| 2.Kendime ait cihazlarımda kullandığım şifrelerimi kimseyle paylaşmam.                                                                                                                                       |                                    |                     |                   |                    |                                   |
| 3.Kullanıcı şifrelerimi oluştururken tahmin edilmesi zor olacak şekilde belirlerim.                                                                                                                          |                                    |                     |                   |                    |                                   |
| 4. Verileri düzenli veya otomatik olarak yedeklerim.                                                                                                                                                         |                                    |                     |                   |                    |                                   |
| 5.USB bellekleri bilgisayarımdan çıkarırken donanımı güvenli kaldır seçeneğini kullanırım.                                                                                                                   |                                    |                     |                   |                    |                                   |
| 6.Okullarda bilgi güvenliği ile ilgili yeterince bilgilendirmeler yapıldığını düşünüyorum.                                                                                                                   |                                    |                     |                   |                    |                                   |
| 7.İndirdiğim dosyaları açmadan önce virüs taraması yaparım.                                                                                                                                                  |                                    |                     |                   |                    |                                   |
| 8.Kablosuz modem şifremi aralıklarla değiştiririm.                                                                                                                                                           |                                    |                     |                   |                    |                                   |
| 9.Başkalarının bilgilerini ve fotoğraflarını paylaşırken onlardan izin alırım.                                                                                                                               |                                    |                     |                   |                    |                                   |
| 10.Başkalarının bilgisayarını ve telefonunu izinsizce karıştırmam.                                                                                                                                           |                                    |                     |                   |                    |                                   |
| 11.Başkaları hakkında gerçek dışı paylaşımlarda bulunmam.                                                                                                                                                    |                                    |                     |                   |                    |                                   |
| 12.Sahibinin izni olmadan resim, video vb. içerikleri kullanmam.                                                                                                                                             |                                    |                     |                   |                    |                                   |
| 13.Arkadaşlarımın bilgisayar kullanırken yaptıkları işleri onlardan habersiz izlemem.                                                                                                                        |                                    |                     |                   |                    |                                   |
| 14.Diğer insanlar hakkında izinleri olmadan bilgi toplamam.                                                                                                                                                  |                                    |                     |                   |                    |                                   |
| 15.Başkalarına ait internet bağlantısını izni olmadan kullanmam.                                                                                                                                             |                                    |                     |                   |                    |                                   |
| 16.Doğruluğundan emin olmadığım bilgileri internet ortamında paylaşmaktan sakınırım.                                                                                                                         |                                    |                     |                   |                    |                                   |
| 17.Başkalarının şifrelerini ve üyelik bilgilerini kullanmam.                                                                                                                                                 |                                    |                     |                   |                    |                                   |

#### Araştırmacıların Katkı Oranı Beyanı

Bu çalışma birinci yazarın yüksek lisans tezinden üretilmiştir. Bu araştırmanın planlanması, yürütülmesi ve yazılı hâle getirilmesi birinci yazar tarafından ikinci yazar gözetiminde gerçekleştirilmiştir.

**Destek ve Teşekkür Beyanı**

Bu araştırmada herhangi bir kurum, kuruluş ya da kişiden destek alınmamıştır.

**Çatışma Beyanı**

Araştırmacıların araştırma ile ilgili diğer kişi ve kurumlarla herhangi bir kişisel veya finansal çıkar çatışması yoktur.

**Etik Kurul Beyanı**

Bu araştırma, Bartın Üniversitesi Etik Komisyonunun 07.03.2023 tarih ve E-23688910-050.01.04-230023177 sayılı onayı ile yürütülmüştür.