NEVŞEHİR HACI BEKTAŞ VELİ ÜNİVERSİTESİ
Ara, bul.

Sosyal Bilimler Enstitüsü Dergisi
Cilt: 13 Sayı: 3 Eylül 2023
E-ISSN: 2149-3871

DİJİTAL ŞİDDETLE MÜCADELE YÖNTEMLERİNE DAİR BİR ARAŞTIRMA1

AN INVESTIGATION ON METHODS OF COMBATING DIGITAL VIOLENCE

Hatice OĞUZ ÖZGÜR
Isparta Uygulamalı Bilimler Üniversitesi
Uluborlu Selahattin Karasoy MYO
Terapi ve Rehabilitasyon Bölümü
haticeoguz@isparta.edu.tr
ORCID: 0000-0001-5901-3488

Metin ÖZKUL
Süleyman Demirel Üniversitesi
Fen Edebiyat Fakültesi
Sosyoloji Bölümü
metinozkul@sdu.edu.tr
ORCID: 0000-0003-2511-9780

Geliş Tarihi:
03.04.2023

Kabul Tarihi:
24.07.2023

Yayın Tarihi:
25.09.2023

Anahtar Kelimeler
Dijital şiddetle mücadele, Dijital güvenlik, Risk toplumu, Karma yöntem.

Keywords
Combating digital violence, Digital security, Risk society, Mixed method.

ÖZ

Araştırma, çağdaş risk toplumlarının gelişen imkân ve koşullarının ortaya çıkardığı yepyeni bir şiddet türü olarak kabul edilen dijital şiddet olgusuna odaklanmaktadır. Dijital şiddet, geleneksel sosyal bağlantıların kopması nedeniyle modern toplumun geliştirdiği yeni temas alanlarında insanların kendilerini ifade etmelerinin birçok yolundan biri olarak görülmektedir. Karma yöntemle gerçekleştirilen bu araştırmada, dijital şiddeti fail ya da mağdur olarak tecrübe eden bireylerin deneyimlerinin yapılandırılmış ve yarı-yapılandırılmış formlar kullanılarak sorgulanması ve bu deneyimlerin nedenlerine ve etkilerine ışık tutulması amaçlamıştır. Bireylerin dijital şiddeti en sık yaşadıkları dijital platformlar ve bu şiddet davranışlarının niteliği belirlenirken, bu davranışların önlenmesine yönelik öneriler de bu kapsamda toplanmıştır. Katılımcılar, dijital şiddetin önlenmesi ve dijital güvenliğin sağlanması için kullanıcıların kişisel bilgilerini çevrimiçi ortamda paylaşmaktan kaçınmaları, şiddet eylemlerini ilgili platform yetkililerine bildirmeleri ve gerekirse polise başvurmaları gibi önerilerde bulunmuşlardır. Ayrıca, bu tür eylemler için cezai yaptırımların artırılmasını ve sivil toplum kuruluşları, üniversiteler ve diğer kurumların bu tür şiddet eylemleri konusunda farkındalık yaratmayı destekleyen uygulamaları teşvik etmesini önermişlerdir. Araştırma, yaşadığımız risk toplumunda yeni bir deneyim olan dijital şiddet hakkındaki bilgi birikimine katkıda bulunması ve dijital şiddet sorununa çözüm önerileri sunması bakımından önemli görülmektedir.

ABSTRACT

The research focuses on the phenomenon of digital violence, which is considered as a brand-new type of violence emerging from the developing opportunities and conditions of contemporary risk societies. Digital violence is seen as one of the many ways for people to express themselves in the new contact areas developed by modern society due to the breakdown of traditional social connections. In this mixed-method study, it was aimed to investigate the experiences of individuals who experienced digital violence as perpetrators or victims by using structured and semi-structured forms and to shed light on the causes and effects of these experiences. While determining the digital platforms where individuals experience digital violence most frequently and the nature of these violent behaviors, suggestions for preventing these behaviors were also collected in this context. In order to prevent digital violence and ensure digital security, participants suggested that users should refrain from sharing their personal information online, report acts of violence to the relevant platform authorities and contact the police if necessary. They also suggested that criminal sanctions for such acts should be increased, and that civil society organizations, universities and other institutions should promote practices that support raising awareness about such acts of violence.

DOI: https://doi.org/10.30783/nevsosbilen.1276460
Atıf/Cite as: Oğuz Özgür, H. & Özkul, M. (2023). Dijital şiddetle mücadele yöntemlerine dair bir araştırma. *Nevşehir Hacı Bektaş Veli Üniversitesi SBE Dergisi, 13*(3), 1541-1560.

[1] Bu araştırma, Süleyman Demirel Üniversitesi, Sosyal Bilimler Enstitüsü, Sosyoloji Anabilim Dalı'nda Hatice Oğuz Özgür tarafından Prof. Dr. Metin Özkul danışmanlığında yürütülerek tamamlanan "*Risk toplumu bağlamında kuşaklararası boyutta şiddetin değişen yüzü: Dijital şiddet*" isimli doktora çalışmasının verilerinin bir kısmı kullanılarak üretilmiştir. Süleyman Demirel Üniversitesi Üniversite Etik Kurulu 11.11.2020 tarihli ve 98/12 sayılı kararına göre etik kurul izni alınmıştır.

Giriş

İnsanlık, kendi tarihsel yaşamı boyunca sayısız tehlike, risk ve tehditle karşı karşıya kalmıştır. İnsanları etkileyen bu riskler, tehlikeler ve tehditler zaman içinde gelişmelerle birlikte ortadan kalkmak yerine bir kısmı varlığını korumaya devam ederken, bir kısmının da niteliğinin yanında oluşturucu ve taşıyıcı araçsallıkları değişmiştir. Ayrıca araçsallıkların ya da teknolojilerin gelişimi ve çeşitlenmesinin getirdiği yeni birçok risk alanları da oluşmuştur. İnsanlık tarihinin ilk aşamalarındaki tehlikeler hayatta kalma ve temel ihtiyaçlara yönelik iken günümüzün tehlikeleri bunların yanı sıra çeşitli alanlarda toplumsallaşma talepleriyle bağlantılıdır (Lupton, 1999; Klinke & Renn, 2002). Şiddet olgusu da toplumsal değişimle birlikte niteliği ve araçsallıkları değişen ve toplumsal yaşamda riskleri artıran tehlikelerden biridir. Şiddet, en başından beri insanlığın sürdüre geldiği bir eylemdir ama dijital şiddet, modern toplum[2] insanının değişen toplumsal koşullarda geleneksel bağlarından kopmasından kaynaklı oluşturduğu yeni etkileşim alanlarında kendisini ifade etmesinin, varlığını somutlaştırmasının çeşitli biçimlerinden biridir.

Bu çalışma, insanlığın toplumsal yaşamı açısından günümüzde ulaştığı ve *risk toplumu* olarak da adlandırılan yeni sosyal çevrede şiddet olgusunun; öngörülemezlik, yalnızlık ve güvensizlik bağlamında çeşitli riskleri beraberinde getiren *bireyselleşmenin*; dijital medyada birlikte deneyimlenmesinin temel nedeni olduğu düşüncesini irdelemektedir. Sonuç olarak dijital alanda güvenliği tehlikeye atan endişelerden biri de şiddetin yeni türü olarak adlandırılan dijital şiddettir. Dijital alan, bu özelliğinin bir sonucu olarak geçmişte var olan çeşitli tehlikelerden ve risklerden etkilenip şekillenen yeni toplumsal alanlardan biridir. Diğer bir deyişle bu bağlamda dijital güvenlik, geçmişten günümüze varlığını sürdüren risk, tehlike ve tehditlerin oluşturdukları korkunun yeniden ortaya çıktığı alanlardan biridir.

Modernleşme, sosyal etkileşimlerin yeniden yapılandırılması için oluşturduğu dinamik imkanlarla yeni yaşam tarzları yaratmaktadır. Geleneksel ilişkilerin yerini giderek artan bir şekilde yeni ağlar aracılığıyla ve çeşitli ilgi alanlarını dikkate alarak kurulan ilişkiler almaktadır. Bu yeni tür etkileşimlerin destekleyici yapıları da teknoloji sayesinde mümkün olmaktadır. Oldukça farklı yaşam tarzlarında yetişen insanlar, teknolojinin sağladığı imkanlar sayesinde etkileşime girmekte ve hatta gittikçe artan bir yoğunlukta birbirlerini yönlendirme potansiyeline sahip olmaktadırlar. Aile dışındaki geleneksel toplumsal bağlar, ilişkilerin genişleyen ve kayganlaşan yapısıyla neredeyse büyük ölçüde ortadan kalkmaktadır. Hatta birçok durumda bile aile bağları tercih edilmemektedir (Beck, 2011). Toplumun yarattığı yüksek riskli ortamda bireyler, teknolojik olarak gelişmiş dijital alanda sosyal varlıklarını sürdürmek için geleneksel bağlarını yavaş yavaş koparırken yeni bağlantılar kurmaktadırlar (Kurt, 2012). Fiziksel dünyada kendilerini ifade etmek için kullandıkları davranışları da giderek artan bir şekilde dijital alana aktarmaktadırlar. Toplumun risklerine uyum sağlamak zorunda olan bireylerin dijital ortama taşıdığı ve kullandığı ya da içinde karşılaştığı faaliyetlerden biri de çeşitli görünümleriyle, şiddet içerikli eylemlerdir.

Modern toplumda, toplumsal olan hemen her şeyin değişimine yol açan faktör bilimsel bilgi ve onun pratik hayata yönelik araçsallaştırılmasını ifade eden teknolojidir. Modern toplum deneyimleri göstermektedir ki araçsallaştırılan bilginin kullanımı insanlık yararına olabildiği gibi zararına da olabilmektedir. Bu zarar verici özelliklerin bir kısmı öngörülebilirken bir kısmı ise hayatın akışı içerisinde deneyimlenen çeşitli ilişkilerde ve etkinliklerde fark edilmektedir. İnsanlık yararına geliştirilen internet teknolojisinin ve dijital araçların kullanımıyla birlikte ortaya çıkmaya başlayan dijital şiddet de bunun en somut örneklerindendir.

Temelde dijital şiddeti oluşturan durum, iletişim ya da bilgi paylaşımı benzeri amaçlarla üretilmiş ağ teknolojisinin amaç dışı kullanımı, kötü niyete alet edilmesi gibi sebeplerdir. Bununla birlikte internetin sağladığı kimliğin gizlenebilmesi, dijital şiddeti teşvik eden hatta saldırının şiddetini artıran unsurdur. Zira gizlilik faile gerçek hayatta yapamayacağı şekilde hareket etme şansı vermektedir (Aksaray, 2011; Türk & Şenyuva, 2021). Ayrıca bilişim teknolojileriyle yapılabilecek faaliyetlerin çok fazla olması, dijital alanla ilgili toplumsal ve yasal denetimlerin yeterli olmaması dijital şiddet davranışlarının yaygınlaşmasına zemin hazırlamaktadır. Dijital şiddet; çevrimiçi cinsel taciz, virüs veya kötü amaçlı yazılım içeren mesajlar gönderme, başkalarının görüntülerini veya videolarını izinleri olmadan çevrimiçi olarak yayınlama, kişisel verileri çalma, verileri silme veya değiştirme, yanlış

[2]Modernleşmeye dair açıklama yapan kuramcılar *risk toplumu, imal edilmiş belirsizlikler, müphemlik, risk kültürü, kaygı çağı* vb. adlandırmalarla modernleşme süreciyle birlikte toplumsal alanda meydana gelen değişimlerin potansiyel olumsuzluklarını açıklamaktadırlar (Ritzer & Stepnisky, 2014). Modernleşme ve küreselleşmeyle birlikte toplumsal ve bireysel fırsatların büyümesi, farklılaşması ve yayılması ile risk, belirsizlik, korku gibi değişkenlerin artması, farklılaşması ve yayılması risk toplumu hakkında açıklamalar yapan bilim insanlarının esasen vurguladıkları şeylerdir. Daha da önemlisi, bu güçler süreç içerisinde kontrolden çıkmaya başlamıştır (Beck, 2011).

bilgi yayma ve dolandırıcılık gibi faillerin diğer kişilerin görüntülerini kullanarak veya sosyal medyada kimliklerini gizleyerek gerçekleştirdikleri, psiko-sosyal taciz ve istismar dâhil olmak üzere daha birçok çeşitteki şiddeti kapsamaktadır (Türk & Şenyuva, 2021; Erbiçer, 2020; Šimandl & Vaníček, 2017).

Bu çalışmada karma yöntemle tasarlanmış saha araştırmasından elde edilen veriler ve ilgili literatür bilgisi dikkate alınarak söz konusu dijital şiddet olgusuyla mücadeleye yönelik öneriler sunulmaktadır. Bu önerilerin etkili olmasına yönelik beklentilerin gerçekleştirilmesinde; bireylerin dijital araç/uygulamalara yönelik tutumları, çeşitli dijital platformların kurucuları/yöneticileri, alanla ilgili mevzuatın oluşturulması, toplumsal otorite kabul edilebilecek kurumların iş birliği vs. önemli görülmektedir (Baltazar vd., 2009; Çolak, 2019). Çalışma, içinde yaşanılan risk toplumunun aktörleri için yeni bir deneyim olan dijital şiddetin tanınırlığının artırılmasında literatüre sunduğu katkı bakımından önemli görülmektedir. Ayrıca çalışmanın pratikteki önemi de dijital şiddet olgusuyla ilgili çözüm önerileri sunuyor olmasıdır.

Yöntem

Dijital şiddet deneyimlerinin sosyolojik faktörlere bağlı olarak bireyden bireye nasıl farklılaştığını ele alan bu araştırmada, "Dijital şiddet deneyimi bireylerin toplumsal ilişkilere yükledikleri anlamları ve toplumsal ilişki kurma biçimlerini etkilemekte midir?", "Bireylerin interneti ve sosyal medya uygulamalarını kullanma amaçlarına/beklentilerine göre dijital şiddet deneyimleri değişmekte midir?" gibi soruları aydınlatmaya odaklanılmıştır. Bu sorular çerçevesinde, dijital şiddet deneyiminin bireylerin toplumsal ilişki kurma biçimleri ve dijital platformlardaki koşulları, beklentileri ve amaçlarıyla ilişkili olduğu varsayılmaktadır. Bu sorular ve varsayımlardan hareketle araştırma, karma yöntemin ilkeleriyle tasarlanmıştır. Bu araştırmada, veri toplama süreci iki evrede gerçekleştirilmiştir. Öncelikle, saha çalışmasına nicel yönelimli aşama ile başlanıp arkasından daha özel sonuçlara ulaşmak için nitel yönelimli aşamaya geçilmiştir. Dolayısıyla bu araştırmada her iki veri türü de eşit önceliğe ya da değere sahiptir. Her iki yönteme ait tekniğe de araştırmayı güçlendirmek ve araştırma sonuçlarının genellenebilirliğini arttırmak amacıyla başvurulmuştur.

Verilerin elde edilmesinde yapılandırılmış anket formu ve yarı-yapılandırılmış derinlemesine görüşme formu kullanılmıştır. Örneklem, rastlantısal örnekleme tekniğiyle seçilmiş bireylerden oluşmaktadır. Bu kapsamda Türkiye genelinde araştırmaya katılmaya gönüllü 18-90 yaş arası 500[3] katılımcı ile görüşülmüştür. Örneklemin güvenirlik düzeyi yaklaşık olarak %98'dir (Raosoft Sample Size Calculator, 2004). Derinlemesine görüşme yapılan 20[4] birey ise amaçlı örnekleme tekniğiyle nicel verilerin elde edildiği katılımcılardan yine gönüllülük esasına dayalı olarak seçilmiştir; burada belirleyici olan kriter, dijital şiddeti mağdur ya da fail olarak deneyimlemiş olmaktır. Veriler, Kasım 2020-Şubat 2021 zaman aralığında çevrimiçi ortamda (Skype, FaceTime, WhatsApp, BİP, Facebook Messenger vb.) ve yüz yüze görüşmelerle elde edilmiştir. Ayrıca bu verileri betimlemeye yardımcı olması amacıyla, görüşmeler sürecinde katılımcıların dijital şiddet deneyimlerine yönelik tepkilerine dair sınırlı gözlemlerde[5] bulunulmuştur.

---

[3]Evrenimiz TÜİK'in Adrese Dayalı Nüfus Kayıt Sistemi'nden elde edilen "Cinsiyete ve yaş grubuna göre nüfus, (1950-2020)" verilerine göre yaklaşık 64.546.125 kişiden oluşmaktadır. Bu sayı Türkiye'de yaşayan 15-85+ yaş arasındaki kişileri temsil etmektedir. Bu değer 500.000'den yukarı olduğu için örneklem hesaplama işlemi sırasında "sonsuz" ya da "bilinmiyor" kabul edilmektedir. Evrenin bilinmediği durumlarda örneklem şu formülle hesaplanmaktadır: $N = \frac{Z^2\eta(1-\eta)}{(p-\eta)^2}$ (Bal, 2015).

[4]Nitel araştırmada, "vurgu genellikle belirli bağlamlardaki anlamların analizi üzerinedir" (Robinson, 1998) ve örneklemin temsili olması amaçlanmamaktadır. Nitel araştırmalarda genel bir kural olarak örneklem sayısı 50'nin altında olması gerekmektedir. Bu durumun üç önemli nedeni bulunmaktadır. Birincisi, her yeni görüşmede çok az yeni verinin geldiği nokta ortaya çıkmaktadır. Bu durum veri doygunluğu olarak ifade edilmektedir. İkincisi, nitel araştırmalarda insidans veya prevalans oranlarının önemsenmemesidir. Üçüncüsü, nitel araştırmaların sağladığı bilgi türünün ayrıntılar açısından zengin olmasıdır. Bu nedenle, her veri toplama biriminden yüzlerce bilgi ortaya çıkmaktadır. Verileri toplama ve analiz etmede sorun yaşanmaması için örneklem büyüklüğünün küçük bir ölçekte tutulması gerekir (Ritchie vd. 2003). Bunlardan dolayı derinlemesine görüşmelerde katılımcı sayısı araştırma süreci sırasında netleştirilmiştir; verilerin doygunluğa ulaştığı, anlatı ayrıntılarının dikkat çekiciliğini ve farklılığını kaybettiği aşamada görüşmeler sonlandırılmıştır.

[5]Araştırmanın saha uygulamasının yapıldığı zaman aralığında pandeminin hâkim olması sebebiyle katılımcılarla yoğun biçimde yüz yüze gelinememiştir. Bu sebeple burada kastettiğimiz 'sınırlı gözlem'; katılımcıların nicel sorulara verdikleri cevaplarla nitel sorulara verdikleri cevaplar dikkate alınarak, dijital şiddet deneyimlerine yönelik sergiledikleri beden dili, cevapların tutarlılığı, samimiyet, ses tonlamaları, endişe, şaşkınlık vb. tepkilerini yansıtan tavırlarıyla ilgili yapmaya çalıştığımız anlamlandırmalardır.

Nicel verilerin analizi sürecinde araştırmanın soru ve hipotezleri göz önünde bulundurularak çeşitli istatistiki işlemlerle (çapraz tablolama, ki-kare vs.) bağımlı (dijital araç/uygulamaları kullanım pratiği, dijital şiddet deneyimi) ve bağımsız (sosyo-demografik özellikler) değişkenler arasındaki korelasyon açıklanmaya çalışılmıştır. Nitel veriler de tematik betimsel bir analizle kodlanarak anlamlandırılmıştır. Katılımcıların anlatıları, 'dijital şiddeti tanımlama', 'dijital şiddet deneyimi', 'dijital şiddet ve toplumsallaşma koşulları' ve 'dijital şiddet ve sosyal ilişkiler' olmak üzere dört tema altında çözümlenmiştir.

Nihai olarak da nicel ve nitel veriler, birbirini destekleyici biçimde ilişkilendirilerek araştırmanın temel amacı doğrultusunda değerlendirmelerde bulunulmuştur.

Bulgular

Dijital şiddet deneyiminin sebep ve sonuçlarının sosyolojik dayanaklarla aydınlatılmasının amaçlandığı saha çalışmasında, katılımcıların dijital şiddetle en sık karşılaştıkları dijital platformlar ve bu şiddet davranışlarının içeriği tespit edilirken, dijital şiddet davranışlarıyla mücadeleye ilişkin öneriler de üretilmiştir. Bu çalışmada, özel olarak dijital şiddet karşısında verilen tepkiler ve bu şiddet türünün önlenmesine yönelik verilere yoğunlaşılmıştır.[6] Bundan dolayı yalnızca bu hususla ilişkili veriler üzerinden değerlendirmeler yapılmıştır.

Araştırmaya katılanların sosyo-demografik özellikleri şöyledir: Katılımcıların, yaş dağılımları 18-90 yaş arasında değişmektedir; %60'ı kadın, %40'ı ise erkektir; %21,4'ünün eğitim düzeyi ilkokul, %13,8'inin lise, %18'inin önlisans, %29'unun lisans, %15,2'sinin lisansüstüdür, %2,6'sı ise okuma-yazma bilmemektedir; %48'i bekâr, %52'si evlidir; %24'ü düşük gelir grubunda, %69,8'i orta gelir grubunda, %6,2'si yüksek gelir grubundadır.

Katılımcıların %75,8'i günlük hayatlarında aktif şekilde internet kullanırken, %24,2'si interneti aktif kullanmamaktadır. En sık kullandıkları dijital araç cep telefonu (%89,6), masaüstü (%11,6) ve dizüstü bilgisayar (%30,2), tablet (%5,4), akıllı saat (%3,6) olarak değişmektedir.

Katılımcıların dijital şiddet değişkenine dair deneyimleri ve bununla ilişkilendirilen diğer değişkenlerle ilgili veriler şöyledir:

Araştırmaya katılan bireylerin %88,7'si dijital şiddetin ne olduğunu bilmektedir. Bu veriye göre katılımcıların genel olarak dijital şiddetin farkında oldukları belirtilebilir. Katılımcıların yaklaşık %31'i dijital şiddet deneyimini mağdur, fail ya da tanık olarak yaşamışlardır. Katılımcılar günlük hayatlarında sıklıkla kullandıkları sosyal medya platformlarında ve web sitelerinde [sosyal ağ uygulamaları (%67,1), video siteleri (%15,6), haber siteleri (%11,8), e-posta siteleri (%11,5), oyun uygulamaları/siteleri (%10,6), saldırgan web siteleri veya bloglar (%10), sohbet odası uygulamaları/siteleri (%10), kısa mesaj uygulamaları (%9,1)] dijital şiddetle karşılaşmaktadır. Bundan dolayı, katılımcıların %79,4'ü dijital araçları kullanırken kişisel güvenlikleri konusunda endişe duymaktadır.

Katılımcılar en çok hakaret/küfür içeren mesajlardan/gönderilerden (%79,1), dolandırıcılıktan (%74,7) ve taciz içeren mesajlardan/gönderilerden (%74,1) oluşan dijital şiddet davranışlarından rahatsızlık duymaktadır. Bu veriler örneklem grubu tarafından en çok deneyimlenen dijital şiddet davranışlarıyla da uyumludur.

Katılımcıların %37,7'si dijital araç/uygulamalar aracılığıyla çirkin sözlere ya da tehdide maruz bırakılmıştır; %36,4'ünün bilgisayar, tablet veya akıllı cep telefonuna virüs, solucan, truva atı (trojan), casus yazılım, reklam yazılımı benzeri zararlı yazılım gönderilmiştir; %30,6'sı dijital araçlar/uygulamalar üzerinden dolandırılmış/maddi zarara uğratılmıştır; %28,2'sinin dijital araçlarda/uygulamalarda var olan hesapları/profilleri çalınmış ya da erişimleri engellenmiştir; %25,3'ü sanal tacize uğramıştır; %20,3'ü birileriyle herhangi bir konuda fikirlerinin uyuşmamasından dolayı dijital araçlar/uygulamalar üzerinden reddedilmiş/grup dışında bırakılmıştır; %15'i dijital araçlar/uygulamalar üzerinden tehdit edilme veya küçük düşürülme amacıyla haksız söylemlere, görüntülere maruz kalmıştır.

Ayrıca katılımcıların %32,2'si birilerini, herhangi bir konuda fikirleri uyuşmadığı için dijital araçlar/uygulamalar üzerinden reddederek grup dışında bırakmıştır; %8,2'si dijital araçlar/uygulamalar aracılığıyla herhangi birine çirkin adlarla hitap etme veya herhangi birini tehdit etme davranışında bulunmuştur; %5'i herhangi birinin dijital

[6]Bu metinde, kelime sınırlamasından dolayı araştırmadan elde edilen veriler oldukça sınırlı biçimde aktarılmıştır. Kapsamlı okuma için: Oğuz Özgür, H. (2022). *Risk toplumu bağlamında kuşaklararası boyutta şiddetin değişen yüzü: Dijital şiddet* (Tez No: 763761) [Doktora Tezi, Süleyman Demirel Üniversitesi]. Ulusal Tez Merkezi.

araçlarda/uygulamalarda var olan hesaplarını/profillerini çalarak erişimlerini engellemiştir; %2,1'i herhangi birilerini kasıtlı olarak küçük düşürmek, kırmak amacıyla dijital araçlar/uygulamalar üzerinden haksız söylemler, görüntüler vb. yayınlamıştır; %1,3'ü herhangi birine sanal taciz uygulamıştır; %0,05'i dijital araçlar/uygulamalar üzerinden herhangi birine bilgisayar virüsleri, solucanları, truva atı (trojan), casus yazılım, adware (reklam yazılımı) benzeri zararlı yazılımlar göndermiştir; %0,3'ü herhangi birini dijital araçlar/uygulamalar üzerinden dolandırarak maddi zarara uğratmıştır.

Dijital şiddeti mağdur olarak deneyimlemiş bireylerin, dijital araçları ve interneti kullanım amaçları birbirinden farklı olmakla birlikte genel olarak; sosyal medya uygulamalarını kullanmayı, film, dizi, belgesel vb. izlemeyi, belirli konularda araştırma yapmak ya da eğitim amacını, haber okumayı-gündemi takip etmeyi kapsadığı görülmektedir. Dijital şiddet uygulayanların (fail) internet kullanım amaçları incelendiğinde de çoğunluğa ait yoğunluğun benzer yönde olduğu tespit edilmiştir. Ayrıca yine dijital şiddet mağduru katılımcıların dijital araçları ve interneti kullanım amaçlarına uygun olarak internet kullanım zamanlarını genellikle, sosyal paylaşım siteleri, arkadaşlık siteleri, film, dizi, belgesel vb. izleme siteleri, bilim içerikli siteler, haber siteleri gibi yerlerde değerlendirdikleri görülmüştür. Dijital şiddet uygulayanların ise internet kullanım zamanlarının önemli kısmını geçirdikleri sitelerin sosyal paylaşım içerikli siteler olduğu görülmektedir.

Bireylerin sosyal medya uygulamalarında bulunan profillerinde neler paylaştıkları ile dijital şiddet deneyimleri ilişkilendirilmeye çalışıldığında; dijital şiddet mağdurlarının da, faillerinin de paylaşımlarının günlük duygu ve deneyimlerini yansıtan kişisel görseller ya da metinler olduğu gözlenmektedir. Ayrıca gerçek hayattaki problemlerini sürekli veya bazen çeşitli sosyal medya platformlarında paylaşanların çoğunluğunun dijital şiddete maruz kaldığı da dikkat çekicidir.

Katılımcıların internet kullanım süreleri arttıkça, internet kullanım alışkanlıklarının getirdiği sorunların da arttığı gözlemlenmektedir. Örneğin, yüz yüze iletişimi sınırlandırdığı ve bundan dolayı sosyal etkileşimlerini kısıtladığını ifade eden (%43,9) katılımcılardan, %1,1'i interneti günlük ortalama yarım saat civarında kullanırken, %19,3'ü günde ortalama 3-5 saat kullanmaktadır. Benzer biçimde internetin bağımlılık yaptığını belirten (%53,9) katılımcıların %0,6'sı interneti günlük ortalama yarım saat civarında kullanırken, %22,1'i günde ortalama 3-5 saat kullanmaktadır. Bireylerin internet kullanım süreleri arttıkça dijital şiddete maruz kalma durumlarının da arttığı gözlenmektedir. Örneğin, bir grup katılımcıdan interneti günde 1-2 saat aktif kullananların dijital şiddete maruz kalmış olma yoğunluğu %8,3 iken, interneti neredeyse tüm gün aktif kullananların dijital şiddete maruz kalmış olma yoğunluğu %31,6'dır. Dijital şiddet uygulayan bireylerin interneti günlük kullanım sürelerine bakıldığında benzer sonuçların olduğu görülmektedir; örneğin, bir grup katılımcıdan internet erişimi günlük 1-2 saat gibi görece kısa bir süre olanların dijital şiddete başvurma yoğunluğu %11,8 iken, nerdeyse tüm gün internete erişimi olanların dijital şiddete başvurma yoğunluğu %25'tir. Bu problemlerin ve güvenlik sorunlarının yarattığı baskı sebebiyle interneti günlük yaşamında aktif olarak kullanan katılımcıların %34,3'ü kendisini internet ortamında özgür hissetmemektedir, %47,8'i de kısmen özgür hissetmektedir.

Bunlara ek olarak, interneti günlük yaşamlarında aktif şekilde düzenli kullananların, internet kullanım alışkanlıklarının sosyal etkileşimlerine etkisi incelendiğinde, %52,2'sinin internet kullanım alışkanlıklarının sosyal etkileşimlerini etkilemediği, %15,6'sının genellikle olumsuz etkilediği, %32,2'sinin genellikle olumlu etkilediği görülmektedir. Sanal ortamda etkileşime geçtikleri bireylerle iş, duygusal (aşk) içerikli, arkadaşlık, siyasi fikir paylaşımı gibi çeşitli niteliklerde ilişki kuranlar içerisinde, dijital şiddete maruz kalanların çoğunluğu (%54) arkadaşlık ilişkisi kuranlardır. Ayrıca sanal ortamda etkileşime geçtikleri kişilerle hiç ilişki kurmayanların dahi önemli kısmı (%23) dijital şiddete maruz kalabilmektedir. Dijital şiddet uygulayanların çoğunluğu (%60) yine sanal ortamdaki kişilerle arkadaşlık ilişkisi kuranlardır. Sanal ortamdakilerle çeşitli ilişkiler kurmayanların, dijital şiddet uygulayanlar içerisindeki yoğunluğu görece azdır. Sosyal medya uygulamaları aracılığıyla tanıştığı kimselere güvenen bireylerin önemli çoğunluğunun dijital şiddete maruz kaldığı gözlenmektedir. Dijital şiddet uygulayanların %46,7'si sosyal medya aracılığıyla tanıştıkları kimselere güven duymamaktadır. Burada göz ardı edilmemesi gereken husus, bireylerin sanal ortamda etkileşime geçtikleri kimselerle çeşitli ilişkiler kursalar da kurmasalar da sanal ortamdaki kimselere güven duysalar da duymasalar da dijital şiddeti mağdur ya da fail olarak deneyimleme ihtimallerinin bulunmasıdır.

Dijital şiddeti deneyimlemiş katılımcılardan bazıları kim tarafından, ne tür bir dijital şiddet davranışına maruz bırakıldıklarını ve bunun sonucunda nasıl tepki verdiklerini veya kime, ne tür bir dijital şiddet uyguladıklarını ve

karşılığında nasıl bir tepki aldıklarını derinlemesine görüşmelerde ayrıntılı biçimde ifade etmişlerdir. Bu veriler içerisinde şunlar dikkat çekicidir:

Katılımcıların çoğunluğu tanımadıkları bireylerce dijital şiddete maruz bırakılmıştır. Örneğin, 561.G'nin anlatımı şöyledir: *"…Twitter da takip isteğini kabul ettiğim bir hesap, önce benimle konuşmaya çalıştı. Tanımadığım için çok konuşmak istemedim. Ardından fotoğraflarımı çalıp yüzümü çıplak kadın fotoğraflarının üstüne koydular ve beni tehdit ettiler, para istediler...*" 231.G kodlu katılımcı ise tanımadıkları kişilerce dolandırıldığını şöyle anlatmıştır: "*Oyun tanıtımı yapan siteler para vermem karşılığında oyunlarda fazladan can hakkı vereceklerini söylediler. Ve maalesef dolandırıldım*…"

Birkaç katılımcı ise eski sevgilisi/eşi/arkadaşı tarafından dijital şiddete maruz bırakıldığını ifade etmiştir. 350.G'nin anlatımı şöyledir: "*Eski erkek arkadaşım tarafından hakkımda tweet atılarak tehdit edilmiştim. Beni bulup döveceğini, zarar vereceğini söyledi*…" Dijital şiddet mağduru olan katılımcıların çoğunluğu sosyal medya platformlarındaki gönderileri/etkileşimleri üzerinden ya da çevrimiçi oyun oynama etkinlikleri sırasında hakarete, ısrarlı takibe, cinsel tacize, şantaja, kişisel verilerin izinsiz biçimde yayılmasına maruz bırakılmıştır. Ayrıca bir kısım katılımcı da aktarılan anlatılarda da görüldüğü üzere dolandırıcılığa maruz kaldığını belirtmiştir.

Dijital şiddet eyleminde bulunduğunu ifade eden katılımcılar ise bu davranışı çoğunlukla tanımadıkları kişilerin sosyal medya platformlarındaki gönderilerine hakaret ve küfürle karşılık vererek, bu platformlarda izin almadan kişilerin verilerini paylaşarak ve kişiyi linç ederek gerçekleştirdiklerini belirtmişlerdir. Örneğin 543.G uyguladığı dijital şiddeti şöyle anlatmaktadır: "…*Online bir oyunda tanımadığım bir takım arkadaşı salak gibi oynadığı için ona küfrettim*…" 247.G ise nasıl faile dönüştüğünü şöyle ifade etmiştir: "*Facebook'ta parti konusunda anlaşmazlık yaşadığım kişilerle karşılıklı küfürleştik. Benim savunduğum parti hakkında onlar küfretti, ben de biraz bu konuda hassas davranırım, sonuçta savunduğum bir ideoloji var, bir şekilde bu parti onu yansıtıyor*…"

Katılımcıların, internet ortamında diğer bireylerle kurdukları ilişkilerin içerikleri ve bu ilişkiler sonucunda dijital şiddet deneyimi yaşayıp yaşamadıklarına dair cevapları incelediğinde; sosyal medya uygulamaları aracılığıyla arkadaşlık ilişkileri kuran, duygusal ilişki kuran veya siyasal fikir paylaşımları üzerinden ilişki kuran bazı katılımcıların dijital şiddet deneyimi yaşadıkları görülmektedir. Dahası bu deneyim, gündelik yaşamdaki ilişkilerine genel olarak olumsuz biçimde yansımaktadır. 763. G'nin deneyimine dair ifadesi şöyledir: "*Genellikle arkadaşlık ilişkisi* kuruyorum. *Bir dönem bir arkadaşımın sevgili olma talebini reddetmem sonucu yine rahatsız edici mesajlara maruz kalmıştım...*" 421.G'nin deneyimlediği dijital şiddet olayından sonra davranışı şöyledir: "*Bu rahatsız edici deneyimin ardından hesabımın gizlilik ayarlarını güncelledim ve mümkün mertebe tanımadığım kişi ya da kişilerle ilişki kurmadım*…" 561.G'nin ifadesinde de olası ilişkilere karşı güveninin kırıldığı görülmektedir: "*İlişki kurmak isteyenlere karşı tavrım çok değişti. Güven problemim tavan yaptı. Erkek kadın fark etmez, sanal dünyada kimseye güvenmiyorum*…"

Katılımcıların ifadelerine göre dijital şiddet deneyimleriyle ilgili tepkileri de faili engelleme, çevrimdışı olma, tepkisiz kalma/görmezden gelme, aynı yöntemle intikam alma, güvenlik birimlerine şikâyette bulunma gibi davranışlardan oluşmaktadır.

Katılımcılar kendi deneyimleri doğrultusunda dijital şiddetle mücadele ve dijital güvenliğin sağlanmasına yönelik şu önerilerde bulunmuşlardır: ilgili platforma şikâyet edilmeli (%72,6), polise bildirilmeli (%71,8), özel bilgileri paylaşmamalı (%63,9), şiddet uygulayanı engellemeli (%53,3), aile bireylerine ya da arkadaşlara anlatılmalı (%52), görüntüyü/profili izlemeyi durdurmalı (%26,4), kullanıcı bilgileri değiştirilmeli (%13,5), çevrim dışı kalınmalı (%10), tehditle yüzleşmeli (%6,3), misilleme yapılmalı/intikam alınmalı (%1,6). Bu önerilerin dışında, katılımcılardan hiçbir şey yapılmamasını (%1,3) da belirtenler olmuştur. Görüldüğü üzere katılımcıların önerileri genellikle kullanıcı tutumları üzerinedir.

Dijital şiddeti deneyimlemiş katılımcılarla yapılan bir kısım derinlemesine görüşmelerde, dijital şiddetle mücadele konusunda nasıl bir yol izlenmesi gerektiği ve ne tür tedbirlerin alınması gerektiği ile ilgili görüşleri istenmiştir. Bazı katılımcıların anlatılardan örnekler şöyledir: 247.G: "*İlgili kurumlar denetimle ilgili kurallar koymalı, insanlar daha bilinçli davranmalı.*" 350.G: "*Caydırıcı hukuki yaptırımlarla ve anonim hesapların kaldırılmasıyla. Tabi bunu yaparken kişisel bilgilerin güvenliği de sağlanmalı*…" 372.G: "*Herkesin sosyal medyayı kullanma amacı sınırlılıkları insan hakları gibi konularda bilgilendirilmesi önemli olabilir.*" 383.G: *"…Dijital şiddetin engellenebilmesi için global düzeyde tüm devletlerin yasal boyutta caydırıcı cezalara tabii tutmasıyla gerçekleşebilir. Her ne kadar caydırıcı kurallar getirilse bile bu işi profesyonel yapanlar çoğu zaman yakalanmadan devam edebiliyorlar bu yüzden tamamen engellenebileceğini düşünmüyorum ama diğer taraftan tüm bireyler teknoloji ve dijital alanlar konusunda bilgilendirilse, dijital şiddet eğiliminde bir nebze azalma gözlemlenebilir.*"

İfadelerde; hukuksal düzenlemelerin yapılması gerektiğine, cezai işlemlerin uygulanması gerektiğine, kullanıcıların bilinçlendirilmesi gerektiğine ve bu yönde farkındalığın artırılmasını destekleyici uygulamaların/etkinliklerin STK'lar, üniversiteler, diğer eğitim kurumları ve ilgili kamu kurumlarınca yaygınlaştırılması gerektiğine yönelik çeşitli söylemler yer almaktadır. Bakıldığında bu söylemler elde edilen nicel verileri de destekler niteliktedir.

Tartışma

Çalışmanın bu aşamasında, dijital şiddeti mağdur ya da fail olarak deneyimlemiş bireylerin bu şiddet türünden korunmak amacıyla sergiledikleri davranışlar ve mücadele önerileri incelenmiştir. Söz konusu davranışlar ve öneriler literatür bilgisiyle de kıyaslanarak dijital şiddetle ilgili kapsayıcı nitelikte çözüm yöntemleri geliştirilmeye çalışılmıştır.

Saha araştırmasından elde edilen verilere göre araştırmaya katılanların azımsanamayacak bir kısmı günlük yaşamında dijital araçları/uygulamaları kullanımları sürecinde, çevrimiçi olunan herhangi bir zamanda en az bir kez dijital şiddeti mağdur ya da fail olarak deneyimlemiştir. Literatürde dijital şiddeti konu alan araştırmalarda da interneti günlük yaşamında kullanan bireylerin dijital şiddetle karşılaşabildiği, bu durumun özellikle de genç bireyler arasında yaygın bir sorun olduğu ifade edilmektedir (Erdur-Baker & Kavşut, 2007; Arıcak vd., 2008; Ayas, 2011; Türk & Şenyuva, 2021). Örneğin, Türkiye genelinde yapılmış bir araştırmaya göre çevrimiçi olan her beş bireyden biri dijital şiddetle karşılaşmaktadır (Şener & Abınık, 2021). Başka bir araştırmada ise 12-17 yaşlarındaki öğrencilerin yaklaşık %37'sinin dijital şiddete maruz kaldığı; ayrıca %23'ünün de çevrimiçi ortamda başka birine olumsuz ifadeler kullandığı tespit edilmiştir (Akkoyunlu, 2020). Ulusal Suç Önleme Merkezi, i-SAFE Inc., Siber Zorbalık Araştırma Merkezi ve Amerikan Osteopatik Derneği tarafından rapor edilen istatistiklere göre çevrimiçi olan her üç gençten biri sanal ortamda tehdit edilmiştir; sosyal medyayı kullanan gençlerin %88'i herhangi bir sosyal ağ sitesinde dijital şiddet davranışlarına tanık olduklarını bildirmişlerdir (www.guardchild.com).

Bireylerin, dijital araçları/uygulamaları ve interneti kullanım alışkanlıklarına göre dijital şiddetle karşılaştıkları ortamlar da değişmektedir (Cebecioğlu & Altıparmak, 2017). Bu çalışma özelinde bireyler günlük yaşamlarında en çok sosyal medya uygulamalarını kullanmaktadır ve dijital şiddetle de en çok bu platformlarda karşılaşmaktadır. Dijital şiddet, sosyal ağların artan kullanımı ve sağladıkları ek katılım seçenekleri nedeniyle her geçen gün daha önemli bir sorun haline gelmektedir (Livingstone vd., 2011; Özmen, 2018). Literatürde de bu verileri destekleyen çalışmalar bulunmaktadır. Örneğin Şener ve Abınık'ın (2021) araştırmasında dijital şiddetle en yoğun karşılaşılan platformlar Instagram (%53), Facebook (%35) ve Twitter (%19)'dır. Bunları Whatsapp (%15), telefon aramaları (%11) ve mesaj uygulamaları (%6) takip etmektedir. Dijital şiddetin iletişim psikolojisi bağlamında incelendiği bir araştırmada da söz konusu platformlara ek olarak Youtube uygulamasının da dijital şiddet sergileme amacıyla yoğunlukla kullanıldığı aktarılmıştır (Gezginci, 2022).

Eldeki verilere göre bireyler çevrimiçi ortamda en çok hakaret/küfür içeren saldırgan dile ve zararlı yazılımlara maruz kalmışlardır. Bununla birlikte önemli bir kısmı da dolandırıcılık, kandırma faaliyetlerine ve tacize maruz kalmıştır. Dijital şiddet uyguladığını belirtenlerin ise en çok uyguladığı davranış fikir uyuşmazlığı gibi sebeplerden dolayı karşıdakini hariç bırakma/ayrımcılık uygulama ya da reddederek grup dışında bırakmadır. Birini tekrar tekrar internette takip etmek, onun resim, video veya ses kayıtlarını izinsiz almak, bunları internette yayınlamak veya bunlarla kişiyi tehdit etmek, maddi veya manevi olarak üzmek ve zayıflatmak "dijital şiddet" teşkil eden davranışlardandır (Tamer & Vatanartıran, 2014; Özmen, 2018; Aytekin, 2022;). Radyo ve Televizyon Üst Kurulu'nun çocukların yeni medya tüketim alışkanlıkları ve siber zorbalıkla ilgili araştırmasına göre, siber zorbalık olarak da bilinen dijital şiddet, internette endişe yaratan risklerin %34,8'iyle ilk sırada yer almaktadır. Bu kapsamda, katılımcıların %32,8'inin sosyal medya üzerinden olumsuz yorumlar (hakaret, küfür, aşağılama ifadeleri vb.) aldıkları, %16,7'sinin sanal tacize uğradığı (cinsel içerikli görüntüler, sesler vb.), %16,2'sinin fotoğraf veya video gibi gönderilerinin izinsiz paylaşıldığı tespit edilmiştir (RTÜK, 2018). Türkiye genelinde dijital şiddetin araştırıldığı diğer bir araştırmada bireylerin %50'sinin hakaret, küfür ve tehdide maruz kaldığı, %39'unun yazılı, sesli veya görüntülü taciz mesajları aldığı, %35'inin biri tarafından sürekli takip edildiği (stalklanmak/ısrarlı takip edilmek), %16'sının adına sahte hesaplar oluşturularak dolandırıldığı/kandırıldığı tespit edilmiştir (Şener & Abınık, 2021). Ergenlerle yapılan bir araştırmada ise bireylerin en fazla "ara sıra" maruz kaldıkları dijital şiddet

davranışları ve e-posta adreslerinin ele geçirilerek zarar görme (%19,7) ve kasıtlı olarak virüs veya zararlı yazılım gönderme (%5,9), internet veya telefon yoluyla tehdit edilmedir (%19,7). Bu araştırmaya göre bireylerin en fazla "ara sıra" uyguladıkları dijital şiddet davranışları çevrimiçi sohbet odasını veya oyunu terk etmeye zorlamadır (%2,6) (Tamer & Vatanartıran, 2014).

Verilerin de yansıttığına göre bireylerin çoğunluğu, söz konusu dijital şiddet davranışlarını tanımadıkları kimselere uygulamaktadır; dijital şiddete maruz kalanların çoğunluğu da tanımadıkları kimselerce mağdur edilmektedir (Williams & Guerra, 2007; Kowalski & Limber, 2007; Wolak vd., 2007; Mishna vd., 2009). Literatürde farklı örneklem gruplarıyla gerçekleştirilen çalışmalarda ise bu konuda farklılık olduğu görülmektedir. Aksaray'ın (2011) çalışmasına göre, dijital şiddet mağdurlarının yalnızca %40-50'ye yakını kendilerine şiddet uygulayanı tanımaktadır. İnsani Gelişme Vakfı'nca yapılan araştırmada şiddetle karşılaşanların yalnızca %34'ü bu davranışın yakın çevrelerinden, tanıdıklarından geldiğini belirtmişlerdir (İNGEV, 2019). Türkiye genelinde yapılan dijital şiddet araştırmasında dijital şiddete maruz kalan her dört kişiden üçü, bunun tanımadığı biri tarafından gerçekleştirildiğini belirtmiştir; hatta bu oran kadınlarda daha yüksektir (Şener ve Abınık, 2021). İlköğretim öğrencileri ile yapılan bir araştırmada da mağdurların %35'inin kendisine şiddet uygulayanı tanımadığı tespit edilmiştir (Dehue vd., 2007). Ancak sosyal medyada kadınlara yönelik dijital şiddeti konu alan bir çalışmada üniversite öğrencisi 18 kadınla yapılan yüz yüze görüşmelerde, kadınların 4'ünün hiç tanımadıkları kişiler tarafından dijital şiddet eylemlerine maruz bırakıldıkları belirlenmiştir (Yıldırım, 2019). 12-17 yaş arası ergenlerin dahil edildiği farklı bir araştırmada, çevrimiçi zorbalık mağdurlarının üçte ikisi faili tanıdığını ifade etmiştir (Juvonen & Gross, 2008). OFCOM araştırması, 12-15 yaş arasındaki çocukların %9'unun tanımadıkları birinden cinsel mesajlar aldığını ortaya koymuştur (OFCOM, 2018). Kanada'da yapılmış bir çalışmaya göre ise katılımcıların %32'si tanıdığı okul arkadaşlarınca, %11'i okulundan tanımadığı kişilerce, %16'sı da hem tanıdığı hem tanımadığı okul arkadaşlarınca dijital şiddet davranışlarına maruz bırakılmışlardır (Sharriff, 2005).

Araştırmada dikkat çekilmek istenilen bir diğer konu da "dijital güvenlik"tir. Katılımcıların önemli çoğunluğu dijital alanda kendilerini güvende hissetmemektedir. Özellikle de dijital şiddet davranışlarıyla karşılaşanlar sanal alandaki güvenliklerinden endişe duymaktadır. Sosyal ağlarda dijital şiddet uygulamaları üzerine yapılan bir araştırmada, kadınların %57,3'ünün ve erkeklerin %55,9'unun dijital araçları/uygulamaları kullanırken kişisel güvenliklerinden endişe duydukları tespit edilmiştir. Buna göre, yanıt verenlerin yarısından fazlası kişisel güvenlikleri konusunda endişelidir (Cebecioğlu & Altıparmak, 2017). Bir başka araştırmada bireylerin %69,8'inin internet ortamında gezinirken kendilerini kısmen ya da tamamen güvende hissetmedikleri tespit edilmiştir (Barındık, 2021). Öz'ün (2014) araştırmasında da bireylerin sosyal medya uygulamalarını kullanırken özellikle kişisel güvenliklerinden endişe duydukları, ancak yine de kendileri hakkında birçok kişisel bilgiyi yayınlamaya devam ettikleri belirtilmiştir.

Bireylerin dijital şiddet davranışlarıyla karşılaştıklarında verdikleri tepkilere bakıldığında çoğunluğun öncelikle faili engelleme, çevrimdışı olma ya da tepkisiz kalma gibi kaçınma/saklanma davranışlarında bulundukları görülmektedir. Türkiye genelinde dijital şiddetin araştırıldığı bir çalışmada dijital şiddetle karşılaşan bireylerin ilk olarak yaptıkları davranışın da bloklama/engelleme (%65) olduğu tespit edilmiştir. Buna ek olarak ikinci sırada verilen tepkiler arasında uygulama/platform içinde şikâyet etme (%39) yer almaktadır. Ayrıca tepkiler arasında yaşanılan durumu yakın çevreye anlatma/yakın çevreden yardım alma (%15), ekran görüntüsü alma (%14), güvenlik ayarlarını kontrol etme (%14) ve hukuki yollara başvurma veya polise bildirme (%7) de yer almaktadır. Ayrıca dijital şiddetle karşılaştığı halde hiçbir şey yapmamayı da tercih eden (%14) bireyler olduğu gözlenmiştir (Şener & Abınık, 2021). Barındık'ın (2021) çalışmasında, bireylerin dijital şiddete maruz kaldıklarında neler yaptıklarına yönelik eylemlere bakıldığında çoğunlukla kişileri engelledikleri (%20,6), mesajları sildikleri (%15,0), sosyal medya hesaplarını gizledikleri (%14,8) ve kişileri sosyal medya uygulamaları üzerinden şikâyet ettikleri (%14,5) tespit edilmiştir. Ayrıca psikiyatriste/psikoloğa başvurma (%1,5) ve polise/savcılığa/mahkemeye başvurma (%1,1) ise en az başvurulan yöntem olarak tespit edilirken, hiçbir şey yapmama oranı da %2,9 olarak elde edilmiştir. Üniversite öğrencileriyle yapılan farklı bir araştırmada, çoğunluğun çevrimiçi şiddete maruz kaldıktan sonra kullandığı programı kaldırmayı ve tüm bilgilerini gizlemeyi tercih ettiği tespit edilmiştir. Siber suçlar birimine/polise şikâyet etmek de yoğunlukla verilen tepkiler arasında yer almaktadır. Yine bu çalışmada da %19'a yakın bir kesim hiçbir şey yapmamayı tercih ettiğini belirtmiştir (Cebecioğlu & Altıparmak, 2017). Siber zorbalığı araştırmak için nitel bir yaklaşımın kullanıldığı çalışmada, katılımcıların zorbalığa yönelik tepkilerinin; sosyal medyada yasaklama veya şikâyet etme ve konuyu aileleri ve arkadaşlarıyla tartışmayı içerdiği bulunmuştur

(Yıldızaç & Demir, 2021). Ergenlerle yapılmış çeşitli araştırmalarda gençlerin çevrimiçi ortamdaki şiddet eylemlerini durdurmak için yetişkinlere ve ebeveynlere haber vermenin dışında, sohbet odalarından kaçınma, tanınmayan kişilerle konuşmama (Li, 2006), istenmeyen mesajı ve rahatsız eden kişiyi durdurma, taciz edene bunu durdurmasını söyleme, kullanıcı adını değiştirme (Arıcak vd., 2008), e-posta adreslerini veya telefon numaralarını değiştirme, suç içeren mesajları kanıt amaçlı saklama, güvenlik güçlerine haber verme (Smith vd., 2008; Aytekin, 2022), şifrelerini kimseyle paylaşmama (Juvonen & Gross, 2008) gibi kendi kendilerine de çeşitli yöntemlere başvurdukları tespit edilmiştir (Aksaray, 2011).

Ailede, okulda, kurumlarda ve sosyal ağlarda alınacak önlemler, dijital araçların/uygulamaların ve internetin güvenli kullanımına ve dijital şiddetin önlenmesine yönelik çözümlere ulaşılmasına yardımcı olabilecektir. Zira kişisel verilerin güvenliği zaten teknolojik olarak yazılım çözümlerinin kullanılması, kullanıcıların hukuki yollarla izlenmesi, teknik çözümlerin kullanılması ve mevzuat desteği ile sağlanmaktadır. Aileler, eğitim kurumları, sosyal ağ hizmeti veren şirketler, sivil toplum kuruluşları ve devlet kurumları bu konuda iş birliği yapmak suretiyle dijital şiddete yönelik daha köklü çözümler üretebilir (Baltazar vd., 2009).

Elde edilen verilere göre katılımcıların dijital şiddet karşısında öncelikli verdikleri tepkiler ve bununla mücadele etmek amacıyla önerdikleri fikirler kısmen örtüşmektedir. Şiddetle mücadele konusunda en çok önerdikleri durum "ilgili platforma şikâyet etme/polise bildirme"dir, ikinci sırada en çok önerilen durum da "kişisel bilgilerin çevrim içi ortamda paylaşılmaması" gerektiğidir. Dijital şiddetin önlenmesini konu alan araştırmalarda dijital araç/uygulamaları ve interneti kullanan bireylerin tutumları ve uygulanabilecek caydırıcı faktörler üzerine öneriler yer almaktadır (Erdoğan & Bahtiyar, 2014; Çolak, 2019). Bunlardan bazıları şöyledir:

Öncelikle, insanların çevrimiçi oldukları her anda, dijital şiddete maruz kalabilecekleri göz önüne alındığında, bu sorunun ortadan kaldırılabilmesi için toplumun her bireyinin şiddet konusunda bilinçlenmesi ve bu konuda bilgi sahibi olmasının çok önemli olduğu vurgulanmaktadır (Türk & Şenyuva, 2021). Bununla birlikte akılda tutulması gereken önemli bir nokta da dijital dünyada kullanılabilecek hiçbir güvenlik aracının, yazılımın veya donanımın tüketicilere risksiz bir çevrimiçi deneyim garanti etmeyeceğidir (Jalali vd., 2019). Çünkü kullanıcı faktörü; üretmek, dağıtmak, iletişim kurmak, etkileşimde bulunmak ve farklı hizmetlerden yararlanmak için çok önemlidir. İlişkili araştırmalara göre ağ, araç ve uygulama kullanıcıları, mevcut ve artan çevrimiçi tehditlerin farkında olmaları ve internet teknolojilerini kullanmak için gerekli bilgi ve becerilere sahip olmaları halinde son derece güvenli çevrimiçi deneyimler yaşayabileceklerine işaret etmektedir (De Bruijn & Janssen, 2017; Çolak, 2019).

Yiğit ve Seferoğlu (2017) siber zorbalıkla ilişkili faktörleri inceleyerek olası çözüm önerileri geliştirdikleri çalışmalarında literatürdeki çeşitli araştırmaları da dikkate alarak "empati tabanlı müdahaleler" (Topçu & Erdur-Baker, 2012; Casas vd., 2013; Doane, Pearson & Kelley, 2014; Del Rey vd., 2016; Schultze vd., 2016; Lee & Shin, 2017), "öfke kontrolü" (Batmaz & Ayas, 2013; Baroncelli & Ciucci, 2014; Den Hamer & Konjin, 2016;), "değerler eğitimi" (Dilmaç & Aydoğan, 2010; Peker & İskender,2015), "siber zorbalık müdahale programları" (Gradinger vd., 2016; Del Rey vd., 2016; Cross vd., 2016), "medya kullanım eğitimi" (Casas vd., 2013; Kokkinos vd., 2014; Den Hamer & Konjin, 2016; Festl, 2016; Lee & Shin, 2017), "okul içi müdahaleler" (Kärnä vd., 2011; Kowalski & Limber, 2013; Yenilmez & Seferoğlu, 2013) ve "aile içi müdahaleler" (Fanti vd., 2012; Hemphill & Heerde, 2014; Tabak & Köymen, 2014; Wright, 2017) gibi başlıkların ön plana çıkmakta olduğunu vurgulamışlardır.

Dijital şiddet mağdurluğu ve failliği ilişkisi üzerinde sosyal sorumluluğa sahip olmanın etkisinin incelendiği araştırmada, dijital şiddet mağduriyeti ile dijital şiddet suçu arasında anlamlı bir pozitif ilişki, dijital şiddet mağduriyeti ile sosyal sorumluluk arasında anlamlı bir negatif ilişki ve sosyal sorumluluk ile dijital şiddet suçu arasında anlamlı bir negatif ilişki tespit edilmiştir. Bundan dolayı sosyal sorumluluğa sahip olma durumunun geliştirilmesinin dijital şiddetle mücadelede işlevsel olabileceğini savunulmaktadır (Zhan vd., 2022; Uluçay ve Melek, 2017).

Bireyleri dijital şiddetin hedefi haline getiren durumlardan biri kişisel verilerin dijital ortamda bilinçsizce paylaşılmasıdır. Söz konusu kişisel veriler; güvenlik şifreleri, demografik özellikler, fotoğraflar, videolar, önemli belgeler, konum/adres bilgisi, iletişim bilgileri, banka hesap bilgileri gibi çeşitli verilerden oluşmaktadır. Bu sebepten dolayı bireylerin dijital araç/uygulamaları kullanırken kişisel verilerini paylaşmamaları gerektiği, kişisel verilerinin gizliliğini sağlamaları gerektiği, en azından güvenlik seviyesi düşük olan platformlara bilgilerini kaydetmemeleri gerektiği önerisi dijital şiddetle ilgili çalışmalarda ısrarla güvenlik önlemi olarak ısrarla

vurgulanmaktadır (Özel Eğitim ve Rehberlik Hizmetleri Genel Müdürlüğü, 2019; guvenliweb.org, 2017; Ceyhan vd., 2015; Erdur-Baker & Kavşut, 2007; Youn, 2005).

Dijital alandaki suçlara yönelik caydırıcı hükümlerin yer aldığı yasal metinlerin oluşturulması ve yürürlüğe konulması da önemli mücadele yöntemlerinden biri olarak görülmektedir (Cebecioğlu & Altıpatmak, 2017; CCIP). Bu düzenlemeler, halen Amerika Birleşik Devletleri (Megan Meier Cyberbullying Prevention Act), Kanada (The Cyberbullying Prevention Act), İngiltere, Avustralya gibi ülkelerde yürürlükte olan hukuki düzenlemelerdir. Ayrıca bu ülkelerde resmî kurumların ve sivil toplum kuruluşlarının iş birliği yaparak siber suçlara yönelik mücadele yürüttüğü bilinmektedir (Baştürk Akca vd., 2014; Yetim, 2015). Ülkemizde doğrudan dijital şiddeti konu alan bir yasal düzenleme söz konusu olmasa da 1982 Anayasası'ndaki çeşitli maddelerde (Özel hayatın gizliliği 20. Madde, Haberleşme hürriyeti 22. Madde, Düşünce ve kanaat hürriyeti 25. Madde, Düşünceyi açıklama ve yayma hürriyeti 26.Madde, vs.) ve Türk Ceza Kanunu'ndaki çeşitli maddelerde (Tehdit 106. Madde, Kişilerin huzur ve sükûnunu bozma 123. Madde, Hakaret 125. Madde, Haberleşmenin gizliliğini ihlal 132. Madde, Kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması 133. Madde, Özel hayatın gizliliğini ihlal 134. Madde, Kişisel verilerin kaydedilmesi 135. Madde, vd.) dijital şiddetin türlerini de kapsayıcı müdahaleler yer almaktadır (Türk Ceza Kanunu; Barındık, 2021; Türk & Şenyuva, 2021). Ayrıca 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'da da içerik sağlayıcıların, konum sağlayıcıların, erişim sağlayıcıların ve toplu kullanım sağlayıcıların niyet ve erişim açısından görev ve hesap verebilirlikleri ile internet ortamında içerik kullanılarak işlenen bazı suçların durdurulmasına ilişkin usul ve esasların düzenlendiği açıktır (5651 Sayılı Kanun; Barındık, 2021). Mevzuat düzenlemeleriyle birlikte şiddet mağdurları haklarını arayabilmekte, failler ise suç içeren eylemlerinden dolayı cezalandırılabilmektelerdir. Böylece dijital şiddete yönelik motivasyonlara dair caydırıcı bir ortam oluşturulabilmektedir. Bu aşamada, bireylerin haklarının ve yükümlülüklerinin neler olduğu ve çevrimiçi şiddetle mücadeleye nasıl katılabilecekleri hakkında ilgili düzenleyici çerçevelerin yanı sıra gelişmiş bilgi ve destek sistemlerine olan ihtiyacı da akılda tutmak önemlidir (Türk & Şenyuva, 2021; Barındık, 2021).

Ceyhan, Demiryürek ve Kandemir'in (2015) çalışmaları, sosyal ağ kullanım hedefleri, güvenlik ön koşulları, sosyal ağlardaki güvenlik tehditleri ve bu sorunlardan nasıl kaçınılacağına dair açıklamalar içermektedir. Çalışmanın bir sonucu olarak, bu bağlamda sosyal ağlarda bilgi güvenliği ve mahremiyetin sağlanmasıyla ilgili çeşitli tehlikeler not edilmiştir. Bu tehlikelerden en sık görüleni e-dolandırıcılık ve kimlik hırsızlığıdır. Kurumsal adların sahte kullanımı, piyango dolandırıcılıkları, profil klonlama, sahte güvenlik yazılımı dolandırıcılıkları, üçüncü taraf uygulama riskleri, yanlış/hatalı ürün satışları, kötü bağlantı istekleri, spam ve tehlikeli kötü amaçlı yazılımların tümü, kimlik avı ve e-dolandırıcılık tekniklerine örnektir. Çocukları ve gençleri bu risklerden korumak için bir takım yasal boşlukların kapatılması ve devletin, eğitim kurumlarının ve vatandaşların iş birliği yapması önerilmiştir. Ayrıca çalışmada kişisel verilerin paylaşımında dikkatli olunması gerektiği, hesap erişimlerinde güçlü parolaların kullanılması gerektiği, özellikle çocukların ebeveyn denetiminde interneti kullanmalarına önem verilmesi gerektiği, ülkemizde ücretsiz olarak verilen "Güvenli İnternet Hizmeti"nden faydalanılması gerektiği dijital şiddetten korunmayla ilgili tedbirler olarak detaylı biçimde sıralanmıştır. Bunlara ek olarak sanal ortamda diğer bireylerin varlığına saygılı davranılması gerektiği, zarar verici davranışlardan kaçınılması gerektiği de dijital şiddetin oluşmasını önleyici "temel" bir öneri olarak vurgulanmaktadır.

Çolak (2019), üniversite öğrencilerinin dijital güvenlik öz yeterliliklerini incelediği araştırmasında eğitim-öğretim kurumları, sivil toplum kuruluşları, araştırmacılar ve eğitmenler için uygulamaya ve araştırmaya yönelik dijital şiddetle mücadele ve güvenlikle ilgili şöyle önerilerde bulunmuştur: Kullanıcıların dijital uygulamalarda alınabilecek güvenlik önlemleri ve bunları almamaları durumunda karşılaşabilecekleri çevrimiçi riskler konusunda eğitim faaliyetleri ile farkındalıkları artırılmalıdır. Bu eğitimlerin etkinliği değerlendirilmeli ve düzenli olarak güncellenmelidir. Kişilerin kimlerle, ne zaman ve nasıl kullanılacağını öngöremedikleri bilgileri paylaşmalarını engellemek için bilgi ve iletişim teknolojilerinin güvenli kullanımı konusunda önceden eğitim almaları sağlanmalıdır. Buna ek olarak, kişilerin internet teknolojilerini ilk kullanmaya başladıkları yaş veya şu anda en sık kullandıkları sosyal medya platformları, çevrimiçi çok oyunculu oyunlar vb. veya bilgi ve dosya alışverişinin yapıldığı platformlarda kimlik hırsızlığı gibi ileride tehdit oluşturabilecek tehditlere karşı korunmak için atılabilecek adımlarla önlem almak mümkündür. Ayrıca literatürde sıklıkla vurgulanan çevrimiçi risklerin yeniden/yenilenerek ortaya çıkmasına yanıt olarak güvenli internet teknolojilerini devreye almak için yeni bilgi

ve becerilerin öğrenilmesi gerekli olabilir. Sonuç olarak söz konusu tehlikelerin güncellenmesine karşın alınabilecek önlemler ve mücadele yöntemleri de güncellenmelidir.

Çocukları ve gençleri kapsayan dijital şiddet üzerine yapılan araştırmalar, aile ve eğitim müdahalelerinin bunu durdurmanın en başarılı yolları olduğunu göstermiştir. Bir çocuk, zamanının büyük bir bölümünü evde ve okulda geçirdiğinden, bu iki ortamla ortaklaşa yapılacak çalışmaların dijital şiddet konusunun ele alınmasında faydalı olacağı öne sürülmektedir (Beale & Hall, 2007; Erdur-Baker & Kavşut, 2007; Mishna vd., 2009; Özdemir & Akar, 2011; Aksaray, 2011; Özmen, 2018; Türk & Şenyuva, 2021; Penezoğlu-Yıldırım & Ulukol, 2022;).

Şahin ve arkadaşları (2010), lise öğrencilerinin siber zorbalık davranışları ve maruz kalma senaryolarına ilişkin düşünceleri üzerine yaptıkları çalışmada, siber zorbalığın çocuk ve gençlerin gelişimi üzerindeki zararlı etkilerinden kaçınmak için konuyla ilgili araştırmalar yapılarak farklı adımlar atılması gerektiğini belirtmişlerdir. Bu çalışmada ve ilgili diğer çalışmalarda velilere, öğretim elemanlarına, okul yetkililerine ve öğrencilere teknoloji kullanımı ile ilgili bilgi verilmesi gerektiği açıkça belirtilmiştir. Özellikle öğrenciler, çevrimiçi ortamda kendilerini bekleyen tehlikelerin farkında olmalıdır. Dijital güvenliğe zarar veren davranışlar konusunda okul rehberlik servisi ile öğretmenlerin, ebeveynlerin, okul yöneticilerinin ve öğrencilerin iş birliği yapması önemli bulunarak, Bilgi İletişim Teknolojileri'ni bilinçli kullanma ve medya okur-yazarlığına dair eğitimler verilmesi (Barındık, 2021; Özmen, 2018; Narin & Ünal, 2016), okul rehberlik servislerinin dijital şiddet eylemlerinde bulunan ve bu davranışlara maruz kalan gençlere ilişkin psiko-eğitimsel programlar hazırlayarak sorunların çözümüne katkı sağlaması, zorbalık kapsamında yapılan davranışların yasal sorumlulukları hakkında bilgi verilmesi şeklinde önerilerde bulunulmaktadır (Agatston vd., 2007; Şahin vd., 2010; Akca vd., 2014; Eroğlu, 2014; Beyazıt vd., 2017; Bayhan, 2020; Yıldızaç & Demir, 2021; Gürkan vd., 2022).

İnsanların kendilerini çevrimiçi tehditlerden korumak için ihtiyaç duyduğu bilgi ve yetenekler, yalnızca teknolojiden anlayan/teknolojiyi bilen olmanın ötesine geçmektedir. Yani, dijital araçlara virüsten koruma yazılımı yüklemek, işletim sistemlerini güncellemek, kötü amaçlı yazılımları taramak ve kaldırmak çevrimiçi tehlikeleri veya çevrimiçiyken tehlikeli davranışlarda bulunmayı önlemek için yeterli değildir. Bununla birlikte karşılaşılan bilgiyi doğrulamak, kişisel bilgi paylaşımının hangi durumlarda ne kadar gerekli olduğunu anlamak gibi farklı ölçüm ve yöntemleri okumak için medya veya dijital okuryazarlık ve dijital güvenlik becerilerine sahip olmak da önemli bir gerekliliktir (Calvani vd., 2012; Çolak, 2019).

Gençlere ve çocuklara uygulanacak medya okuryazarlığı eğitimlerinin yanı sıra ebeveyn kontrolü/denetimi internet güvenliğinin sağlanmasında temel bileşenlerden biri olarak kabul edilmektedir. İnternet erişiminin çoğu evde bir bilgisayar aracılığıyla sağlandığı için ailenin interneti güvenli bir şekilde nasıl kullanacağını anlaması gerekir (Livingstone & Helsper, 2008; Aoyama vd., 2012; Tamer & Vatanartıran, 2014; Kaşıkçı vd., 2014; Faccio vd., 2014; Altundağ, 2016; You & Lim, 2016). Ek olarak, internet servis sağlayıcıları ve dijital araç/uygulama satan işletmeler, müşterilerine internet güvenliği konusunda gerekli yazılımları ve eğitim kaynaklarını sağlamalıdır. Servis sağlayıcılar ve bilgisayar/dijital iletişim aracı üreticileri, ailelere kullanımı basit ve gelişmiş bilgi okuryazarlığı gerektirmeyen ücretsiz filtreleme, kısıtlama ve kontrol yazılımları temin etmelidir. Bu, ayrıca ebeveyn kontrolünü de kolaylaştıracaktır. Ayrıca son zamanlarda güvenli internet kullanımını teşvik eden birçok web sitesi geliştirilmiştir ve bunların iletişim yöntemleriyle başarılı bir şekilde tanıtılması, kullanımlarının yaygınlaştırılması son derece önemlidir (Kaşıkcı vd., 2014). Bu uygulamalar hem çocukların hem yetişkinlerin interneti ve dijital araçları daha güvenli kullanmalarını kolaylaştıracaktır.

Sonuç

Sebep ve sonuçlarıyla çok yönlü ve türleri olan bir olgu olarak karşımızda duran şiddet, çağımızın teknolojik gelişmeleriyle yeni bir alan ve yeni bir tür daha edinmiştir. İletişim veya bilgi paylaşımı araçlarının dijitalleşmesinin bir sonucu olarak şiddet de dijital hale gelmiştir. İnternet erişimi olan kişiler, şiddet içeren davranışlarıyla başka bir kişiye veya bir grup insana doğrudan zarar vermek için sosyal medya platformlarını ve akıllı telefonlar, tabletler ve dizüstü bilgisayarlar gibi çevrimiçi bilgi işlem cihazlarını kullanma kapasitesine sahiptir. Bu imkân da şiddetin yeni bir biçimi olan ve literatürde siber zorbalık, dijital zorbalık, siber tartaklama, internet zorbalığı, çevrimiçi zorbalık, yeni şiddet, çevrimiçi şiddet, siber şiddet gibi farklı isimlerle de tanınan dijital şiddet olgusunun, diğer şiddet biçimlerinin yanına eklenmesine yol açmıştır.

Günlük etkileşimlerini sürdürmek, mesleğini icra etmek, sosyalleşme ihtiyacını karşılamak, serbest zamanını değerlendirmek gibi çok çeşitli nedenlerle internet teknolojisini kullanan bireyler, kendi faydalarına çaba sarf ederken beklemedikleri bir anda dijital şiddete uğrama riskiyle karşı karşıya kalmaktadırlar. Bu risk, nitelikleri sınırlı ya da belirlenmiş psikolojik ya da sosyo-kültürel özelliklere sahip bireyler için değil, interneti kullanan, çevrim içi olan herkes için geçerlidir.

Araştırmada, interneti ve dijital araçları günlük yaşamında sıklıkla kullanan bireylerin, bu araçların sunduğu imkânları kötü amaçlar için kullanan ya da bu imkânları kötü amaçlar için kullananların hedefi olan bireyler üzerinden elde edilen veriler incelenerek dijital şiddete yönelik çözüm ve mücadele önerileri geliştirilmeye çalışılmıştır. Bu kapsamda, sahadan elde edilen nicel ve nitel verilerden ve literatür bilgisinden hareketle hem internet ve dijital araç/uygulama kullanıcılarını hem dijital mecranın yönetici aktörlerini hem de kamu yönetiminden sorumlu kurumsal aktörleri kapsayan şu önerilerde bulunma gereği duyulmuştur:

-Öncelikle bireylerin şiddet olgusuna yönelik farkındalıkları geliştirilmelidir. İnterneti, dijital araç ve uygulamaları kullanan bireyler, dijital alan güvenliğini bozan davranışlarla ilgili çeşitli kanallar (internet reklamları, yazılı-sesli-görüntülü medya yayınları vb.) aracılığıyla bilgilendirilmeli ve bu tür davranışlara yönelik olası motivasyonun engellenmesi sağlanmalıdır.

-Dijital şiddetin çeşitli görünümleriyle ilgili somut örneklerin haber ve bilgilendirme kaynaklarında açıklanması/görünür hale getirilmesi ve bunların oluşturacağı olası zararlar ve faillerin karşılaşacakları çeşitli yaptırımların sembol, söylem ve spot sloganlar halinde sunulması, bireylerin bu konudaki bilinç seviyelerini yükseltecektir.

-Örgün ve yaygın eğitim süreçlerinde medya okur-yazarlığı bilgisinin, güvenli internet kullanımının bireylere öğretilmesine yönelik çalışmalar yapılmalıdır ve var olan çalışmalar sürdürülebilir hale getirilmelidir. Burada çalışmaların her yaştan, cinsiyetten, sınıftan vs. bireyi kapsayıcı biçimde; ilgi, beceri, amaç gibi faktörler göz önüne alınarak planlanması önemlidir.

-Özellikle de gençlerin ve çocukların dijital şiddet hakkında bilgilendirilmeleri, ailelerin ve okulun bu kapsamda iş birliği içinde hareket etmeleri, çocukların ebeveynleri denetiminde interneti ve dijital araçları kullanmaları "şiddete erken müdahale" kapsamında değerlendirilmelidir.

-Dijital şiddeti deneyimleyen katılımcıların genellikle tanınamayan kişiler tarafından ya da sanal (gerçek olmayan, hayal ürünü, taklit, vb.) kimliğe sahip profiller tarafından mağdur edildikleri verisi göz önünde bulundurularak, dijital uygulamalarda bu gibi anonim profillerin oluşturulmasını önleyici sistemler platform yetkililerince geliştirilmelidir. Ayrıca dijital uygulamaların ya da ağların güvenlik parametrelerinin arttırılması (güvenli şifreleme, ağa erişim, vb.) sağlanmalıdır.

-Dijital araç/uygulamaların amacına uygun biçimde kullanımı için teşvik edici politikalar oluşturulmalıdır. Örneğin kişisel verilerin çevrimiçi ortamda paylaşılmaması, güvenli görünmeyen bağlantılara tıklanmaması vb. gibi davranışlarla dijital araç/uygulamaları ve interneti kullanım alışkanlıkları güvenli hale getirilmelidir.

-Dijital alanda işlenen suçlara ve güvenliği bozucu eylemlere yönelik yasal metinlerin ve tanımlamaların oluşturulması, mevzuattaki eksikliklerin tamamlanması ve caydırıcılığın arttırılması sağlanmalıdır. Ayrıca bireylerin yasal hak ve sorumluluklarıyla ilgili ve olası mağduriyet durumunda nasıl bir hukuki yol izlemeleri gerektiği konusunda bilgilendirilmeleri çeşitli kanallarca sağlanmalıdır.

-Dijital bilgi-iletişim araçlarını temin eden ve internet servisi sağlayan kurumlar, müşterilerine dijital güvenlikle ilgili yazılım, materyal ve diğer bilgileri ücretsiz sağlamalıdır.

-Gelişen teknolojiyle her an yenilenen dijital tehditlere yönelik alınabilecek önlemler de güncellenmelidir.

-Teknolojinin ve sağladığı imkanların kötüye kullanılmasının nedenleri hakkında bilgi toplayarak, güvenli bir çevrimiçi ortam yaratmak için sürdürülebilir stratejiler geliştirilmelidir.

-Dijital şiddet olgusu neden ve sonuçlarıyla kapsamlı biçimde nicel ve nitel farklı yöntemlerle, farklı perspektiflerle araştırılmalıdır, böylece planlanacak önlemler daha somut verilerle oluşturulabilecektir.

-Dijital şiddetin de kökeni olan şiddet kültürünün (ayrımcılık, istismar, taciz, darp, dolandırıcılık, vs.) önlenmesine yönelik sistematik faaliyetler yürütülmelidir.

Dijital araçların ve internetin, bireysel ve toplumsal yaşantılarımızda önemli rol oynadığı gerçeğinden hareketle; bunlar ve benzeri önlemlerin bir an önce uygulamaya koyulması; bununla ilgili üniversitelerin, diğer eğitim

kurumlarının, sivil toplum kuruluşlarının, yerel yönetimlerin, ilgili bakanlıkların ve alt kurumların iş birlikleri dahilinde var olan uygulamaların geliştirilmesi dijital güvenlik için zaruri görülmektedir.

Kaynakça

Agatston, P.W., Kowalski R. & Limber, S. (2007). Students' perspectives on cyberbullying. *Journal of Adolescent Health,* (41), 59-60. https://doi.org/10.1016/j.jadohealth.2007.09.003

Akça, E. B., Sayımer, İ., Salı, J. B., & Başak, B. E. (2014). Okulda siber zorbalığın nedenleri, türleri ve medya okuryazarlığı eğitiminin önleyici çalışmalardaki yeri. *Elektronik Mesleki Gelişim ve Araştırmalar Dergisi*, 2(2), 17-30.

Akkoyunlu, A. (2020). *Siber zorbalık ile ilgili 11 gerçek*. https://bitdefender.com.tr/siber-zorbalik-ile-ilgili-11-gercek/.

Aksaray, S. (2011). Siber zorbalık. *Çukurova Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 20(2), 405-432.

Altundağ, Y. (2016). Lise öğrencilerinde sanal zorbalık ve problemli internet kullanımı ilişkisi. *Online Journal of Technology Addiction & Cyberbullying,* 3(1), 27-43.

Aoyama, I., Utsumi, S., & Hasegawa, M. (2012). Cyberbullying in Japan: Cases, government reports, adolescent relational aggression, and parental monitoring roles. Q. Li, D. Cross, & P. K. Smith (Eds.), *Cyberbullying in the global playground: Research from international perspectives* (pp. 183-201). Wiley Blackwell. https://doi.org/10.1002/9781119954484.ch9.

Arıcak, T., Siyahhan, S., Uzunhasanoğlu, A., Sarıbeyoğlu, S., Çıplak, S., Yılmaz, N., & Memmedov, C. (2008). Cyberbullying among Turkish adolescents. *CyberPsychology & Behavior,* 11(3), 253-262. https://doi.org/10.1089/cpb.2007.0016

Ayas, T. (2011, 3-5 Ekim). *Lise öğrencilerinin sanal zorba ve mağdur olma yaygınlığı*. [Sözlü sunum]. 11. Ulusal Psikolojik Danışma ve Rehberlik Kongresi, İzmir.

Aytekin, G. (2022). *Dijital şiddetin tezahürleri ve siber zorbalık*. https://www.guvenliweb.org.tr/blog-detay/dijital-siddetin-tezahurleri-ve-siber-zorbalik.

Bal, H. (2015). *Sosyolojide yöntem ve araştırma teknikleri*. Sentez Yayıncılık.

Baltazar, J., Costoya, J., Flores, R. (2009). *The Heart of KOOBFACE C&C and Social Network Propagation, A Trend Micro Threat Research.* https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2009/12/21185104/the_20heart_20of_20koobface_final_1_.pdf

Barındık, G. (2021). *Dijitalleşen medya ve yarattığı yeni şiddet alanı: Dijital şiddet* [Yüksek Lisans Tezi, Akdeniz Üniversitesi]. Ulusal Tez Merkezi.

Baroncelli, A., & Ciucci, E. (2014). Unique effects of different components of trait emotional intelligence in traditional bullying and cyberbullying. *Journal of Adolescence,* 37(6), 807-815. https://doi.org/10.1016/j.adolescence.2014.05.009

Baştürk Akca, E., Sayımer, İ., Balaban Salı, J., & Ergün Başak, B. (2014). Okulda siber zorbalığın nedenleri, türleri ve medya okuryazarlığı eğitiminin önleyici çalışmalardaki yeri. *Elektronik Mesleki Gelişim ve Araştırma Dergisi,* 2(Özel Sayı), 17-30.

Batmaz, M., & Ayas, T. (2013). İlköğretim ikinci kademedeki öğrencilerin psikolojik belirtilere göre sanal zorbalık düzeylerinin yordanması. *Sakarya University Journal of Education,* 3(1), 43-53.

Bayhan, V. (2020). Z kuşağı lise gençlerinde sosyal medya bağımlılığı ile siber zorbalık ve siber mağduriyet deneyimleri. *İlahiyat Akademi,* (12), 117-144.

Beale, A. V., & Hall, K. R. (2007). Cyberbullying: What School Administrators (and Parents) Can Do. *The Clearing House,* 81(1), 8-12. https://doi.org/10.3200/TCHS.81.1.8-12

Beck, U., (2011). *Risk toplumu: Başka bir modernliğe doğru.* (K. Özdoğan & B. Doğan. çev.). İthaki Yayınları.

Beyazıt, U., Şimşek, Ş., & Ayhan, A. B. (2017). An examination of the predictive factors of cyberbullying in adolescents. *Social Behavior and Personality: an International Journal*, 45(9), 1511-1522. https://doi.org/10.2224/sbp.6267

Calvani, A., Fini, A., Ranieri, M., & Picci, P. (2012). Are young generations in secondary school digitally competent? A study on Italian teenagers. *Computers & Education,* (58), 797-807. https://doi.org/10.1016/j.compedu.2011.10.004

Casas, J. A., Del Rey, R., & Ortega-Ruiz, R. (2013). Bullying and cyberbullying: Convergent and divergent predictor variables. *Computers in Human Behavior,* 29(3), 580-587. https://doi.org/10.1016/j.chb.2012.11.015

Cebecioğlu, G., & Altıparmak, İ. B. (2017). Dijital şiddet: sosyal paylaşım ağları üzerine bir araştırma, *Sakarya University Journal of Education,* 7(2), 423-431. https://doi.org/10.19126/suje.305282

Ceyhan, E. B., Demiryürek, E. & Kandemir, B. (2015). Sosyal ağlarda güncel güvenlik riskleri ve korunma yöntemleri. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi,* 1 (1), 1-10. https://doi.org/10.18640/ubgmd.192646

Cross, D., Shaw, T., Hadwen, K., Cardoso, P., Slee, P., Roberts, C., & Barnes, A. (2016). Longitudinal impact of the Cyber Friendly Schools program on adolescents' cyberbullying behavior. *Aggressive Behavior,* 42(2), 166-180. https://doi.org/10.1002/ab.21609

Çolak, C. (2019). *Üniversite öğrencilerinin dijital güvenlik öz yeterlikleri ve çevrimiçi risk alma eğilimlerinin incelenmesi* [Doktora Tezi, Anadolu Üniversitesi]. Ulusal Tez Merkezi.

De Bruijn, H., & Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. *Government Information Quarterly,* 34 (1), 1-7. https://doi.org/10.1016/j.giq.2017.02.007

Dehue, F., Bolman, C., & Völlink, T. (2008). Cyberbullying: Youngsters' experiences and parental perception. *Cyberpsychology and Behavior,* 11(2), 217-223. https://doi.org/10.1089/cpb.2007.0008

Del Rey, R., Lazuras, L., Casas, J. A., Barkoukis, V., Ortega-Ruiz, R., & Tsorbatzoudis, H. (2016). Does empathy predict (cyber) bullying perpetration, and how do age, gender and nationality affect this relationship?. *Learning and Individual Differences,* (45), 275-281. https://doi.org/10.1016/j.lindif.2015.11.021

Den Hamer, A. H., & Konijn, E. A. (2016). Can emotion regulation serve as a tool in combating cyberbullying?. *Personality and Individual Differences,* (102), 1-6. https://doi.org/10.1016/j.paid.2016.06.033

Dilmaç, B., & Aydoğan, D. (2010). Values as a predictor of cyber-bullying among secondary school students. *International Journal of Social Sciences*, 5(3), 185-188.

Doane, A. N., Pearson, M. R., & Kelley, M. L. (2014). Predictors of cyberbullying perpetration among college students: An application of the theory of reasoned action. *Computers in Human Behavior,* (36), 154-162. https://doi.org/10.1016/j.chb.2014.03.051

Erbiçer, E. S., (2020). Siber zorbalık ve siber mağduriyetin sosyal uyuma ve bazı demografik değişkenlere göre incelenmesi. *Pamukkale Üniversitesi Eğitim Fakültesi Dergisi,* (49), 190-222. https://doi.org/10.9779/pauefd.559831.

Erdoğan, G. & Bahtiyar, Ş. (2014, 5-7 Şubat). *Sosyal Ağlarda Güvenlik,* [Sözlü sunum]. XVI. Akademik Bilişim Konferansı. Mersin Üniversitesi. https://akademiksunum.com/index.jsp?modul=document&folder=36dd71d0b115e3b4ed01c3141d13100d35b5f289.

Erdur-Baker, Ö. & Kavşut, F. (2007). Akran zorbalığının yeni yüzü: Siber zorbalık. *Eurasian Journal of Educational Reserach,* (27), 31-42.

Eroğlu, Y. (2014). *Ergenlerde siber zorbalık ve mağduriyeti yordayan risk etmenlerini belirlemeye yönelik bütüncül bir model önerisi* [Doktora Tezi, Uludağ Üniversitesi]. Ulusal Tez Merkezi.

Faccio, E., Iudici, A., Costa, N., & Belloni, E. (2014). Cyberbullying and interventions programs in school and clinical setting. *Procedia-Social and Behavioral Sciences,* (122), 500-505. https://doi.org/10.1016/j.sbspro.2014.01.1382

Fanti, K. A., Demetriou, A. G., & Hawa, V. V. (2012). A longitudinal study of cyberbullying: Examining risk and protective factors. *European Journal of Developmental Psychology,* 9(2), 168-181. https://doi.org/10.1080/17405629.2011.643169

Festl, R. (2016). Perpetrators on the internet: Analyzing individual and structural explanation factors of cyberbullying in school context. *Computers in Human Behavior,* (59), 237-248. https://doi.org/10.1016/j.chb.2016.02.017

Gezginci, G. (2022). *İletişim psikolojisi açısından yeni medyada şiddet* [Doktora Tezi, İstanbul Üniversitesi]. Ulusal Tez Merkezi.

Gradinger, P., Yanagida, T., Strohmeier, D., & Spiel, C. (2016). Effectiveness and sustainability of the ViSC Social Competence Program to prevent cyberbullying and cyber-victimization: Class and individual level moderators. *Aggressive Behavior,* 42(2), 181-193. https://doi.org/10.1002/ab.21631

Guardchild, (2023). *Cyber Bullying Statistics.* https://www.guardchild.com/cyber-bullying-statistics/.

Gürkan, H., Atabay, E., & Gezgin, D. M., (2022). Lise öğrencileri arasında dijital şiddet: siber zorbalık, akıllı telefon bağımlılığı ve medya okuryazarlığı arasındaki ilişki. *Trakya Eğitim Dergisi,* 12(3), 1799-1820. https://doi.org/10.24315/tred.1115385

Güvenli Web. (2017). *Sosyal ağlarda güvenlik.* https://www.guvenliweb.org.tr/dokuman-detay/sosyal-aglarda-guvenlik.

Hemphill, S. A., & Heerde, J. A. (2014). Adolescent predictors of young adult cyberbullying perpetration and victimization among Australian youth. *Journal of Adolescent Health*, 55(4), 580-587. https://doi.org/10.1016/j.jadohealth.2014.04.014

İnsani Gelişme Vakfı (İNGEV). (2019). *Siber zorbalık araştırması.* https://ingev.org/basin-bultenleri/INGEV_Siber_Zorbalik_Basin_Bulteni_28082019.pdf.

İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun. https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5651.pdf.

Jalali, M. S., Kaiser, J. P., Siegel, M., & Madnick, S. (2019). The Internet of Things promises new benefits and risks: a systematic analysis of adoption dynamics of IoT products. *IEEE Security & Privacy,* 17(2), 39-48. DOI: 10.1109/MSEC.2018.2888780

Juvonen, J., & Gross, E. F. (2008). Extending the school grounds? Bullying experiences in cyberspace. *Journal of School Health,* 78(9), 496-505. https://doi.org/10.1111/j.1746-1561.2008.00335.x

Kadir Has Üniversitesi Siber Güvenlik ve Kritik Altyapı Koruma Uygulama ve Araştırma Merkezi (CCIP). *Dijital dünyada şiddet: siber zorbalık.* https://ccip.khas.edu.tr/post/29/dijital-dunyada-siddet-siber-zorbalik

Kärnä, A., Voeten, M., Little, T. D., Poskiparta, E., Kaljonen, A., & Salmivalli, C. (2011). A large-scale evaluation of the KiVa antibullying program: Grades 4–6. *Child Development*, 82(1), 311-330. https://doi.org/10.1111/j.1467-8624.2010.01557.x

Kaşıkçı, D. N., Çağıltay, K., Karakuş, T., Kurşun, E., & Ogan, C. (2014). Türkiye ve Avrupa'daki Çocukların İnternet Alışkanlıkları ve Güvenli İnternet Kullanımı, *Eğitim ve Bilim Dergisi,* 39(171), 230-243.

Klinke, A., & Renn, O. (2002). A new approach to risk evaluation and management: risk-based, precaution-based and discourse-based strategies. *Risk Analysis,* 22(6), 1071-1094. https://doi.org/10.1111/1539-6924.00274.

Kokkinos, C. M., Antoniadou, N., & Markos, A. (2014). Cyber-bullying: An investigation of the psychological profile of university student participants. *Journal of Applied Developmental Psychology,* 35(3), 204-214. https://doi.org/10.1016/j.appdev.2014.04.001

Kowalski, R.M., & Limber S.P. (2007). Electronic bullying among middle school students. *Journal of Adolescent Health,* (41), 22-30. https://doi.org/10.1016/j.jadohealth.2007.08.017

Kowalski, R. M., & Limber, S. P. (2013). Psychological, physical, and academic correlates of cyberbullying and traditional bullying. *Journal of Adolescent Health,* 53(1), 13-20. https://doi.org/10.1016/j.jadohealth.2012.09.018

Kurt, İ. (2012). Toplumsallaşma sürecinin 'toplumsanallaşma' bağlamındaki yolculuğu. *Bayburt Eğitim Fakültesi Dergisi,* 7(1), 1-10.

Lee, C., & Shin, N. (2017). Prevalence of cyberbullying and predictors of cyberbullying perpetration among Korean adolescents. *Computers in Human Behavior,* (68), 352-358. https://doi.org/10.1016/j.chb.2016.11.047

Li, Q. (2006). Cyberbullying in schools a research of gender differences. *School Psychology International,* 27(2), 157-170. https://doi.org/10.1177/0143034306064547

Livingstone, S., & Helsper, E. J. (2008) Parental mediation and children's Internet use. *Journal of Broadcasting and Electronic Media,* 52(4), 581-599. https://doi.org/10.1080/08838150802437396

Livingstone, S., Haddon, L., Görzig, A., & Ólafsson, K. (2011). *EU Kids Online final report: LSE*, https://eucpn.org/document/eu-kids-online-final-report.

Lupton, D. (1999). *Risk and sociocultural theory: new directions and perspectives*. Cambridge University Press.

Megan Meier Cyberbullying Prevention Act. https://www.meganmeierfoundation.org/bullying-cyberbullying-laws.

Mishna, F., Saini, M., & Solomon,S. (2009) Ongoing and online: Children and youth's perceptions of cyberbullying. *Children and Youth Services Review,* 31(12), 1222-1228. https://doi.org/10.1016/j.childyouth.2009.05.004.

Narin, B., & Ünal, S. (2016). Siber zorbalık ile ilgili haberlerin Türkiye yazılı basınında çerçevelenişi. *Akdeniz İletişim Dergisi,* (26), 9-23. https://doi.org/10.31123/akil.438555

OFCOM. (2018). *Children and parents: Media use and attitudes report,* https://www.ofcom.org.uk/__data/assets/pdf_file/0024/134907/children-and-parents-media-use-and-attitudes-2018.pdf.

Öz, M. (2014). Sosyal medya kullanımı ve mahremiyet algısı: Facebook kullanıcılarının mahremiyet endişeleri ve farkındalıkları. *Journal of Yasar University,* 35(9), 6009-6260.

Özdemir, M., & Akar, F. (2011). Lise öğrencilerinin siber-zorbalığa ilişkin görüşlerinin bazı değişkenler bakımından incelenmesi. *Kuram ve Uygulamada Eğitim Yönetimi*, 4(4), 605- 626.

Özel Eğitim ve Rehberlik Genel Müdürlüğü, (2019). *Siber zorbalık.* https://orgm.meb.gov.tr/meb_iys_dosyalar/2019_12/26113055_SYBER_ZORBALIK.pdf.

Özmen, Ş. Y. (2018). Dijital şiddet, siber zorbalık ve yeni medya okuryazarlığı üzerine bir değerlendirme. *Journal of International Social Research,* 11(61). 958-966. http://dx.doi.org/10.17719/jisr.2018.2989

Penezoğlu Yıldırım, D. N., & Ulukol, B. (2022). Dijital oyunlar ve şiddet, *TRT Akademi*, 7(16), 1163-1170.

Peker, A., & İskender, M. (2015). İnsani değerler yönelimli psiko-eğitim programının siber zorbalık üzerine etkisi. *Atatürk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi,* 19(1), 11-22.

Radyo ve Televizyon Üst Kurulu (RTÜK), (2018). *Çocukların Yeni medya kullanım alışkanlıkları ve siber zorbalık 2018 araştırması, RTÜK Kamuoyu Yayın Araştırmaları ve Ölçme Dairesi Başkanlığı.*

https://www.rtuk.gov.tr/Media/FM/Birimler/Kamuoyu/cocuklarin-yeni-medya-kullanimlari-ve-siber-zorbalik.pdf.

Raosoft Sample Size Calculator, (2004). http://www.raosoft.com/samplesize.html.

Ritchie, J., Lewis, J., & Elam, G. (2003). Designing and selecting samples. In J. Ritchie, J. Lewis (Eds.), *Qualitative research practice A Guide for Social Science Students and Researchers*, (pp. 77-108), Sage.

Ritzer, G., & Stepnisky, J. (2014). *Sosyoloji kuramları.* (H. Hülür, çev.). De Ki Basım Yayım.

Robinson, G. (1998). *Methods and techniques in human geography*. J. Wiley.

Schultze-Krumbholz, A., Schultze, M., Zagorscak, P., Wölfer, R., & Scheithauer, H. (2016). Feeling cybervictims' pain: The effect of empathy training on cyberbullying. *Aggressive Behavior*, 42(2), 147-156. https://doi.org/10.1002/ab.21613

Shaheen, S. (2005). Cyber-Dilemmas in the new millennium: school obligations to provide student safety in a virtual school environment, *Mcgill Journal of Education,* 40(3). 457-477.

Šimandl, V., & Vaníček, J. (2017). The use of Inquiry Based Education in a Simulation Software Environment in Pre-Service ICT Teacher Training. *International Journal of Information and Communication Technologies in Education,* 4(1), 5-15. DOI: 10.1515/ijicte-2015-0001.

Smith, P. K., Madhavi, J., Carvalho, M., Fisher, S., Russel, S., & Tippett, N. (2008). Cyberbullying: Its nature and impact in secondary school pupils. *Journal of Child Psychology and Psychiatry,* 49(4), 376-385. https://doi.org/10.1111/j.1469-7610.2007.01846.x

Şahin, M., Sarı, S. V., Özer, Ö., & Er, S. H. (2010). Lise öğrencilerinin siber zorba davranışlarda bulunma ve maruz kalma durumlarına ilişkin görüşleri, *Süleyman Demirel Üniversitesi Fen Edebiyat Fakültesi Sosyal Bilimler Dergisi,* (21), 257-270.

Şener, G., & Abınık, N. (2021). *Türkiye'de dijital şiddet araştırması.* https://www.cybermagonline.com/turkiyede-dijital-siddet-arastirmasi.

Tabak, F. S., & Köymen, Ü. (2014). Student experiences with cyberbullying in northern Cyprus. *Procedia-Social and Behavioral Sciences,* (116), 5200-5209. https://doi.org/10.1016/j.sbspro.2014.01.1100

Tamer, N., & Vatanartıran, S. (2014), Ergenlerin Teknolojik Zorbalık Algıları. *Online Journal Of Technology Addiction & Cyberbullying,* 1(2), 1-20.

The Cyberbullying Prevention Act. https://web2.gov.mb.ca/bills/40-2/b214e.php.

Topçu, Ç., & Erdur-Baker, Ö. (2012). Affective and cognitive empathy as mediators of gender differences in cyber and traditional bullying. *School Psychology International,* 33(5), 550- 561. https://doi.org/10.1177/0143034312446882

Türk, B., & Şenyuva, G., (2021). Şiddet sarmalı içinden siber zorbalık: bir gözden geçirme. *IBAD Sosyal Bilimler Dergisi,* (10), 462-479. https://doi.org/10.21733/ibad.901032

Türk Ceza Kanunu. http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5237.pdf.

Uluçay, D. M., & Melek, G., (2017). Türkiye'deki okullarda siber zorbalık: bir literatür değerlendirmesi. *AJIT-e: Online Academic Journal of Information Technology.* http://dx.doi.org/10.1089/cpb.2005.8.1.

Williams, K. R., & Guerra, N.G. (2007). Prevelance and predictors of internet bullying. *Journal of Adolescent Health,* (41), 14-21. https://doi.org/10.1016/j.jadohealth.2007.08.018

Wolak ,J., Mitchell ,K.J., & Finkelhor, D. (2007). Does online harrasment constitute bullying? An exploration of online harrasment by known peers ond onlineonly contacts. *Journal of Adolescent Health,* (41), 51-58. https://doi.org/10.1016/j.jadohealth.2007.08.019

Wright, M. F. (2017). Parental mediation, cyberbullying, and cybertrolling: The role of gender. *Computers in Human Behavior,* (71), 189-195.

Yenilmez, Y., & Seferoglu, S. S. (2013). Sanal zorbalık ve öğretmenlerin farkındalık durumlarına bir bakış. *Eğitim ve Bilim,* 38(169), 420-432.

Yetim, S. (2015). Siber zorbalık, Türkiye ve ABD karşılaştırması (ABD V. Drew Dosyası*). Türkiye Barolar Birliği Dergisi,* 28 (120), 325-384.

Yıldırım, E. (2019). *Sosyal Medyada Kadınlara Yönelik Dijital Şiddet* [Yüksek Lisans Tezi, İstanbul Üniversitesi]. Ulusal Tez Merkezi.

Yıldızaç, B., & Demir, F. (2021). Siber zorbalık üzerine nitel bir araştırma. *Sosyal Sağlık Dergisi,* 1(1), 116-139.

Yiğit, M. F. & Seferoğlu, S. S. (2017). Siber zorbalıkla ilişkili faktörler ve olası çözüm önerileri üzerine bir inceleme, *Online Journal of Technology Addiction & Cyberbullying,* 4(2), 13-49.

You, S., & Lim, S. A. (2016). Longitudinal predictors of cyberbullying perpetration: Evidence from Korean middle school students. *Personality and Individual Differences,* (89), 172-176. https://doi.org/10.1016/j.paid.2015.10.019

Youn, S. (2005). Teenagers' perceptions of online privacy and coping behaviors: A risk-benefit appraisal approach, *Journal of Broadcasting and Electronic Media,* 49(1), 86-110. https://doi.org/10.1207/s15506878jobem4901_6

Zhan, J., Yang, Y., Lian, R. (2022). The relationship between cyberbullying victimization and cyberbullying perpetration: The role of social responsibility. *Digital Mental Health,* (13), 1-14. https://doi.org/10.3389/fpsyt.2022.995937.

EXTENDED SUMMARY

Digital violence has evolved into a phenomenon that affects all members of society as a social reality in the modern day as a result of the widespread use of the Internet and digital tools. The purpose of this study is to provide recommendations for preventing digital violence. A field study that was planned to use the mixed method principles was done. The literature was used to assist the interpretation of the data.

The data was gathered using a structured questionnaire and a semi-structured in-depth interview form. The sampling was chosen randomly. In this context, 500 participants from all around Turkey, ranging in age from 18 to 95, took part in the study. The sample has a 98% reliability level, on average. Individuals interviewed in-depth were determined by purposive sampling. Being a victim or offender of digital violence is the deciding factor in this case.

During the analysis of the quantitative data, the correlation between the dependent and independent variables was tried to be explained by various statistical procedures, taking into account the questions and hypotheses of the research. Qualitative data were also coded with a thematic descriptive analysis and made sense of.

This study specifically focuses on responses to digital violence and information on how to stop this kind of abuse. A total of 31% of the participants in the survey had experience with digital violence either as offenders, victims, or observers. On social media networks and websites, they often utilize in their everyday lives, participants come across digital violence [e-mail (11.5%), offensive websites or blogs (10%), text messaging apps (9.1%), video websites (15.6%), chat room apps/websites (10%), gaming apps/websites (10%), social network apps (67.1%), and news websites (11.8%)]. Because of this, 79.4% of the participants expressed fear about their personal safety online.

According to the information gathered from the multiple-choice question, the behaviors of digital violence, such as insulting/abusive messages and posts (79.1%), fraud (74.7%), and abusive messages and posts (74.1%), most concern the participants. The sample group's most prevalent digital violent behaviors and these results are both consistent. Some of the participants who have been the victims of digital violence went into great depth about who perpetrated it, what sort of violence they were subjected to, how it affected them, and what kind of response they got in return. These findings are noteworthy in the following ways:

Most of the participants had experience with digital violence from people they didn't know. A few people said that their ex-girlfriend, ex-wife, or acquaintance exposed them to digital violence. Through their postings or interactions on social media platforms or during online gaming activities, the majority of participants who are victims of digital violence have been subjected to insults, persistent stalking, sexual harassment, blackmail, and illegal publishing of personal data. Additionally, a few individuals said that they had experienced fraud.

Participants who admitted to engaging in digital violence said they often carried it out by lynching the victim, exposing their personal information without permission on social media networks, and abusing and cursing at the posts of strangers. Participants' responses to digital violence incidents, according to their remarks, include banning the offender, going offline, being indifferent or unresponsive, exacting revenge using the same technique, and reporting the incident to the security departments. In accordance with their own experiences, participants recommended the following strategies for preventing digital violence: complain on the appropriate platform (72.6%), law enforcement (71.8%), not divulge personal data (63.9%), stop the offender (53.3%), relatives or friends (52%), stop looking at the photo or profile (26.4%), altering user data (13.5%), remaining online (10%), face the danger (6.3%).

In addition to these recommendations, 1.3% of respondents said that nothing should be done. As is evident, participant ideas tend to focus on user sentiments. Participants who had experienced digital violence were questioned in some in-depth interviews about their opinions on how to address it and what steps may be made. There are several discourses in the assertions that legal regulations should be made, criminal prosecutions should be carried out, user awareness should be increased, and non-governmental organizations, universities, and pertinent public institutions should disseminate practices and activities that support raising user awareness in this regard. When examined, these discourses also lend credence to the collected quantitative evidence.

Numerous recommendations on preventing digital violence have been developed based on data from the literature and the field, and they address institutional actors in public administration as well as users of the internet and digital tools as well as managing actors in the digital media. Some of them include the following:

People should be made aware of digital violence when utilizing the internet and other digital technologies. Planned trainings should be held for this purpose at businesses, educational institutions, etc. It should be assured that legal texts and definitions for offenses committed online and activities that compromise security are developed, that gaps in the law are filled, and that deterrent is boosted. Digital applications and networks should also have more stringent security requirements (secure encryption, network access, etc.). By gathering data on the reasons why technology is misused and the opportunities it presents, long-lasting policies should be established to ensure a secure online environment. Actions need to be taken to stop the culture of violence, which also fuels digital violence (discrimination, abuse, harassment, assault, battery, etc.).

It is considered necessary to consider people's attitudes toward digital tools, the creators of various digital platforms, the enactment of relevant laws, the collaboration of organizations that might be regarded as social authorities, etc. Finally, this study is significant because it adds to the literature by raising awareness of digital violence, which is a novel experience for those who live in a high-risk environment. The study's practical value also stems from the fact that it provides remedies for the problem of digital violence.