Orta Doğu ve Orta Asya Kafkaslar Araştırma ve Uygulama Merkezi Dergisi (ODAK)

DİJİTAL DÜNYA'NIN TEHDİTLERİ : SİBER ZORBALIK VE SİBER İSTİSMAR

ÖZET

Günümüzün dijital çağında, internetin ve sosyal medyanın yaygın kullanımı, bireylerin iletişim, bilgi edinme ve sosyal etkileşim yollarını kökten değiştirmiştir. Ancak, bu dönüşümle birlikte yeni tehditler de ortaya çıkmıştır. Siber zorbalık ve istismar, özellikle gençler arasında ciddi psikolojik ve sosyal sorunlara yol açan önemli problemler olarak karşımıza çıkmaktadır. Bu makale, siber zorbalık ve istismarın bireyler üzerindeki etkilerini, yanlış yönlendirmelerin ve yanıltıcı bilgilerin bu süreçlerdeki rolünü incelemektedir.

Siber zorbalık, bir kişinin dijital platformlarda sürekli olarak tacize veya zorbalığa maruz kalması olarak tanımlanabilir. Bu tür davranışlar, mağdurların kendilerine olan güvenlerini zedeleyebilir, depresyon, anksiyete ve hatta intihar gibi ciddi sonuçlara yol açabilir. Ayrıca, siber istismar, özellikle çocuklar ve gençler arasında giderek artan bir tehdittir ve mağdurların yaşam boyu sürebilecek travmalar yaşamasına neden olabilir.

Yanlış yönlendirme ve yanıltıcı bilgiler, siber zorbalık ve istismarın yayılmasını kolaylaştıran unsurlar arasındadır. Yanıltıcı içerikler, mağdurları hedef gösterme, yanlış bilgi yayma ve toplum içinde itibarlarını zedeleme amacıyla kullanılmaktadır. Bu durum, mağdurların sosyal ilişkilerini ve psikolojik sağlıklarını olumsuz yönde etkileyerek daha geniş çapta toplumsal sorunlara yol açmaktadır.

Bu makale, siber zorbalık ve istismarın bireyler üzerindeki etkilerini akademik literatür ve vaka analizleri üzerinden değerlendirerek, bu tür sorunların önlenmesi ve mağdurların korunması için öneriler sunmaktadır. Dijital dünyada güvenli bir ortam sağlamak için alınması gereken önlemler ve farkındalık yaratma stratejileri, makalenin ana odak noktalarından biridir.

ABSTRACT

In today's digital age, the widespread use of the internet and social media has fundamentally transformed the ways individuals communicate, gather information, and engage socially. However, along with this transformation, new threats have emerged. Cyberbullying and abuse, particularly among young people, have become significant issues leading to serious psychological and social problems. This article examines the impacts of cyberbullying and abuse on individuals, highlighting the role of misdirection and misleading information in these processes.

Cyberbullying can be defined as the continuous harassment or bullying of a person on digital platforms. Such behaviors can undermine victims' self-confidence, leading to depression, anxiety, and even severe outcomes like suicide. Additionally, cyber abuse, especially among children and adolescents, is an increasingly prevalent threat that can cause lifelong trauma for the victims.

Misdirection and misleading information are among the factors that facilitate the spread of cyberbullying and abuse. Deceptive content is used to target victims, spread false information, and

[ORCİD : 0000-0002-8626-6146] [DergiPark : @bbmnr] [E-Posta: bmnrpltci@gmail.com]

damage their reputation within society. This situation adversely affects victims' social relationships and psychological health, leading to broader societal issues.

This article evaluates the impacts of cyberbullying and abuse on individuals through academic literature and case analyses, offering recommendations for preventing such issues and protecting victims. Ensuring a safe environment in the digital world and creating awareness strategies are key focal points of this article.

Anahtar Kelimeler : Siber Zorbalık, Dijital İstismar, Yanlış Bilgilendirme, Psikolojik Etki, Çevrimiçi Güvenlik

Keys : Cyberbullying, Digital Abuse, Misinformation, Psychological Impact, Online Safety

GİRİŞ

Siber zorbalık ve istismar, internetin ve sosyal medyanın yaygınlaşmasıyla birlikte özellikle gençler ve çocuklar arasında giderek artan ciddi sorunlar haline gelmiştir. Bu iki kavram sıklıkla birbiriyle ilişkilendirilse de, aralarındaki nüansları anlamak ve tamamlayıcı öğeleri analiz etmek büyük önem taşımaktadır.

Siber zorbalık, bir bireyin veya grubun, dijital platformlar aracılığıyla başka bir bireye veya gruba kasıtlı ve sürekli olarak zarar verici davranışlarda bulunmasıdır. Bu tür davranışlar, sosyal medya, kısa mesajlar, e-postalar ve diğer çevrimiçi ortamlar üzerinden gerçekleştirilebilir. Siber zorbalık, mağdurlarda ciddi psikolojik sorunlara yol açabilir ve hatta intihar düşüncelerine neden olabilir.

Öte yandan, siber istismar, çevrimiçi ortamlarda bir bireyin cinsel, duygusal veya psikolojik istismara maruz kalması durumudur. Siber istismar, çocuk pornografisi yayma, cinsel taciz ve kişisel verilerin izinsiz paylaşılması gibi çeşitli davranışları içerebilir. Siber istismar mağdurları, yaşadıkları deneyimlerin etkisiyle uzun süreli travmalar yaşayabilirler.

Siber zorbalık ve istismar, bireylerin dijital ortamlarda güvende kalmasını sağlamak amacıyla ciddiyetle ele alınması gereken konulardır. Eğitim kurumları, ebeveynler ve yasal otoriteler, bu tür davranışların önlenmesi ve mağdurların korunması için iş birliği yapmalıdır. Türkiye'de ise bu durum daha da önemlidir çünkü bilinçli internet kullanımı ülke genelinde yetersiz bir seviyededir.

Bu bağlamda, ebeveynlere büyük sorumluluklar düşmektedir ve eğitimcilerin de bu konuda bilgilendirilmesi ve gerekli önlemleri alması oldukça elzemdir. İlerleyen bölümlerde, bu konular detaylı bir şekilde ele alınacaktır. Siber zorbalık, genellikle bir kişi veya grup tarafından başka bir kişiye karşı internet üzerinden yapılan kasıtlı, zarar verici davranışlar zinciri olarak tanımlanır; ancak, siber zorbalığın birçok farklı formu bulunmaktadır.

Siber Zorbalık ve İstismar Detayları

Siber zorbalık, geleneksel (fiziksel) zorbalığın aksine, sanal bir ortamda gerçekleşir ve mağdurların sürekli bir tehdit altında hissetmelerine neden olabilir. Siber zorbalık, çeşitli şekillerde ortaya çıkar. Sözlü zorbalık, internette veya diğer dijital iletişim platformlarında hakaret edici, tehditkâr veya alay edici yorumlar yapılmasını içerir. Mağdura yönelik doğrudan mesajlar, sosyal medya gönderileri veya yorumlar şeklinde olabilir. Sosyal zorbalık, mağdurun sosyal çevresi içinde izolasyona veya dışlanmaya maruz bırakılması amacıyla yapılan eylemleri kapsar. Bu, dedikodu yayma, yanlış bilgi yayma veya bir kişinin çevrimiçi itibarını kasıtlı olarak zarar vermek için yapılan eylemleri içerebilir.

Görsel zorbalık, mağdurun izni olmadan kişisel fotoğrafların veya videoların paylaşılmasını içerir. Utandırıcı, zarar verici veya kişisel mahremiyeti ihlal edici içerikler bu kategoriye girer. Kimlik hırsızlığı

ve sahtekârlık, bir kişinin kimliğini çalarak veya sahte bir profil oluşturarak internet üzerinde zarar verici eylemlerde bulunmayı kapsar. Bu tür eylemler, mağdurun itibarına zarar vermek, yanlış bilgi yaymak veya başkalarını kandırmak amacıyla yapılabilir.

Kimliğe bürünme, failin başka bir kişiymiş gibi davranarak onun kimliğini ele geçirmesi eylemidir. Bu tür davranışlar, özellikle siber ortamda, failin mağdur gibi hareket ederek mağdurun itibarına zarar verebilecek söylemlerde bulunmasını veya eylemlerde bulunmasını içerebilir. Örneğin, bir sosyal medya platformunda, özellikle geniş kitlelere ulaşabilen bir hesaba izinsiz erişim sağlayarak dezenformasyon yaymak, kimliğe bürünmenin tipik bir örneğidir. Bu tür eylemler, mağdurun kişisel ve profesyonel hayatında ciddi sonuçlara yol açabilir. Mağdurun sosyal çevresi, iş ilişkileri ve toplumdaki saygınlığı, gerçekte kendisinin yapmadığı eylemler veya söylemler nedeniyle zarar görebilir. Bu durum, sadece bireysel itibar kaybıyla sınırlı kalmayıp, aynı zamanda maddi zararlara veya hukuki sorunlara da neden olabilir.

Siber taciz, failin kurbanı hedef almak ve takip etmek amacıyla elektronik iletişim araçlarını kullanmasıyla gerçekleşen çevrimiçi bir taciz türüdür. Bu tür, genellikle mağdur için inandırıcı güvenlik tehditleri içerdiğinden, diğer siber zorbalık türlerine kıyasla daha tehlikeli olarak kabul edilir. Siber tacizciler, tehditkâr veya taciz edici nitelikte tekrarlanan mesajlar göndererek ya da mağdurun kimliğine bürünerek ve üçüncü şahısları mağdura yönelik benzer eylemlerde bulunmaya teşvik ederek hareket edebilir. Bu davranış biçimi, kurbanın yerini belirleme, spam yoluyla taciz, cinsel şantaj gibi elektronik takip yöntemlerinin bir kombinasyonunu içerebilir.

Doxing, mağdurun ev adresi, telefon numarası, tam adı gibi kişisel bilgilerinin izinsiz bir şekilde ifşa edilmesi ve kamuoyu ile paylaşılması eylemidir. Genellikle, bu tür eylemler, bireyin mahremiyetinin ihlali ve ciddi güvenlik sorunlarına yol açabilir. Doxing vakaları, mağdurların güvenliğini tehdit eden ciddi eylemlerdir ve yalnızca mağdurun çevrimiçi güvenliğini değil, fiziksel güvenliğini de riske atabilir. Botlar, doğrudan şahıs ya da grupları hedef alabilen ve genellikle sosyal medya üzerinden gerçekleşen bir takım siber saldırı yöntemleridir. Botlar, çeşitli yazılımlar ile yapılır ve API dediğimiz uzantılar ile sosyal medya araçlarına entegre edilebilir.

Bir kişiyi veya grubu, ırk, din, cinsiyet, cinsel yönelim, engellilik durumu veya diğer kişisel özellikler nedeniyle hedef almak hakaret ve alay olarak tanımlanabilir. Bu tür zorbalık, nefret söylemi içerebilir ve mağdurlar üzerinde ciddi psikolojik etkilere neden olabilir. İstenmeyen e-posta (spam), tekrar eden iletişim eylemleri ve birden fazla hesap oluşturarak bir hedefe toplu mesaj gönderme olarak tanımlanabilir. Bu durum, özellikle kişisel ilişkilerde yaşanan ayrılıklar sonrasında ortaya çıkabilir. Takıntılı bir partner, alıcı tarafından engellenmiş olsa bile, eski mesajlarını birden fazla platform üzerinden göndermeye devam edebilir.

Siber Zorbalık ve İstismar Yaygınlığı

Türkiye genelinde, öğrencilerin yaklaşık %12'si sözlü siber zorbalığa maruz kaldığını belirtirken, %10.5'i de sözlü siber zorbalık eyleminde bulunduğunu ifade etmiştir. Özellikle İstanbul ilinde, siber zorbalık mağduru olanların oranı %20'ye yaklaşırken, siber zorbalık yapanların oranı %15'i geçmektedir. Bu durum, siber zorbalığın çocuk ve gençler arasında yaygın bir sorun olduğunu ve önemli bir müdahale gerektirdiğini göstermektedir. Dünya çapında ise UNICEF'in yaptığı uyarı, 15-24 yaş arasındaki gençlerin %70,6'sının internette şiddet, siber zorbalık ve dijital taciz gibi tehlikelere maruz kaldığını göstermektedir. Bu veri, gençlerin çevrimiçi ortamlarda karşılaştıkları risklerin boyutunu ve bu konudaki acil müdahale ihtiyacını ortaya koymaktadır. Kuruluş, çocuklara ve gençlere yönelik çevrimiçi şiddetin önlenmesi amacıyla kararlı adımlar atılması çağrısında bulunmaktadır.

Siber zorbalığın yaygınlığı ve etkisi üzerine yapılan kapsamlı çalışmalar, yaş, cinsiyet ve sosyo-ekonomik durum gibi çeşitli faktörlere göre değişen karmaşık bir manzara ortaya koymaktadır. 2023 yılında Siber Zorbalık Araştırma Merkezi tarafından yapılan kapsamlı bir çalışma, Amerika Birleşik Devletleri'nde 13 ila 17 yaş arasındaki 5,005 ortaokul ve lise öğrencisini kapsayan ulusal temsili bir örneklemi inceledi. Bu çalışma, katılımcıların yaklaşık %55'inin hayatlarının bir noktasında siber zorbalığa maruz kaldığını, yaklaşık %27'sinin ise son 30 günde siber zorbalığa uğradığını buldu. Bildirilen siber zorbalık türleri arasında çevrimiçi yapılan kötü veya incitici yorumlar, grup sohbetlerinden dışlanma, çevrimiçi yayılan dedikodular ve çevrimiçi rezil edilme veya aşağılanma yer almaktadır. İlginç bir şekilde, çalışma cinsiyet farklılıklarını da vurgulayarak, ergen kızların yaşamları boyunca siber zorbalık deneyimlerinin erkeklere kıyasla daha yüksek olduğunu ortaya koymuştur.

Security.org tarafından 2024'te öne çıkarılan bir diğer çalışma, çeşitli sosyal medya platformlarında siber zorbalığa dair bilgiler sunarak, her yaştan çocuğun savunmasız olduğunu ve yaşları büyüdükçe risklerin arttığını belirtti. Bu araştırma, özellikle COVID-19 pandemisi sırasında artan ekran süresi ve çevrimiçi aktivite nedeniyle siber zorbalık olaylarında önemli bir artış olduğunu ifade etmektedir. Sosyal ağlar arasında, çocukların YouTube, Snapchat, TikTok ve Facebook'ta siber zorbalığa uğrama olasılıklarının en yüksek olduğu tespit edilmiştir. Ayrıca, yıllık geliri 75,000 doların altında olan hanelerin çocuklarının, daha yüksek gelirli hanelerin çocuklarına kıyasla siber zorbalığa uğrama olasılığının iki kat daha fazla olduğu belirlenmiştir.

Pew Araştırma Merkezi'nin 2022 yılında ABD'deki ergenler üzerinde yürüttüğü anket, siber zorbalığın genellikle fiziksel görünüş, cinsiyet, ırk veya etnik köken gibi sebeplerle yapıldığını ortaya koymuştur. Siyah ergenlerin, Hispanik veya Beyaz ergenlere kıyasla ırk veya etnik kökenlerinden dolayı çevrimiçi tacize uğrama ihtimalinin yaklaşık iki kat daha fazla olduğu belirlenmiştir. Bu anket ayrıca, birçok ergenin siber zorbalığı ciddi bir sorun olarak gördüğünü ve algıların demografik gruplara göre değiştiğini açıklamaktadır.

Psikoloji alanındaki bir başka kapsamlı inceleme, siber zorbalığın ergenler ve çocuklar arasında ciddi bir kamu sağlığı sorunu olarak kabul edildiğini ve küresel olarak etkileri olduğunu vurgulamaktadır. Bu inceleme, siber zorbalık araştırmalarının siber zorbalığın yaygınlık oranlarını ve risk faktörlerini çeşitli ülkelerde inceleyerek bu konunun karmaşıklığını ortaya çıkarmaya çalıştığını belirtmiştir. Ancak, siber zorbalık ölçümü ve metodolojilerindeki farklılıklar nedeniyle tutarlı sonuçlara varılamamaktadır. Siber zorbalığın ölçülmesindeki bu tutarsızlıklar, aynı ülkede, aynı zaman diliminde yapılan ölçümlerde sıklıkla karşılaşılan bir sorundur.

Frontiers in Psychology tarafından yapılan kapsamlı inceleme, siber zorbalığın küresel durumunu, risk faktörlerini ve dünya genelinde alınan önleyici önlemleri detaylı bir şekilde ele almıştır. Bu inceleme, 2015 ile 2019 yılları arasında yapılan çalışmaları gözden geçirerek siber zorbalığın yaygınlık oranlarının %6.0 ile %46.3 arasında değiştiğini ve siber zorbalığa maruz kalma oranlarının ise %13.99 ile %57.5 arasında değiştiğini bulmuştur. Sözel şiddet, en yaygın siber zorbalık türü olarak belirlenmiştir. Ayrıca, kişisel düzeyde yaş, cinsiyet, çevrimiçi davranış, ırk, sağlık durumu, geçmişte mağduriyet deneyimi ve dürtüsellik gibi değişkenlerin; durumsal düzeyde ise ebeveyn-çocuk ilişkisi, kişilerarası ilişkiler ve coğrafi konumun risk faktörleri olarak saptandığı belirtilmiştir. Koruyucu faktörler olarak ise empati ve duygusal zeka, ebeveyn-çocuk ilişkisi ve okul iklimi sıkça vurgulanmaktadır.

Sonuç olarak, siber zorbalık, farklı platformlarda aktif olan bireylerin yaş, cinsiyet, sosyo-ekonomik durum gibi çeşitli faktörlerden etkilenebilen çok yönlü bir sorundur. Mağdurlar üzerindeki etkileri dikkate alındığında, siber zorbalığın nedenlerinin karmaşıklığı ve etkilerinin çeşitliliği, önleme ve müdahalede çok yönlü ve kapsayıcı yaklaşımlar gerektirir.

Hangi Yöntemlerle, Nasıl Yapılıyor?

Siber zorbalık, sanal alemde gerçekleştiği için gerektiğinde sosyal mühendislik faktörlerini de kullanmaktadır. Belirttiğimiz siber zorbalık yöntemlerinde ilerlemeler sağlanırken genellikle sosyal mühendislik yöntemleri de kullanılır. Örneğin, sahte bir site yaparak doxing gerçekleştirildiğinde sosyal mühendisliğin bir alt dalı olan phishing yöntemi de kullanılabilir. Bir başka örnekle, mobil cihazlar üzerinde belirli kişileri hedef almak için geliştirilen yazılımlar veya herhangi bir API uzantısı ile hedeflere saldırı mümkün olabilir. Yine hoax (aldatmaca) yöntemiyle bireylere karşı siber zorbalık gerçekleştirilebilir.

Bu konuda senaryo oluşturmak için birçok örnek verilebilir. Ancak net bir şekilde belirtilebilir ki sosyal mühendislik, siber zorbalıkta yaygınlıkla kullanılan bir faktördür. Bunun dışında, vatansever duyguları istismar ederek kendi kişisel çıkarları için kullanılabilecek siber zorbalık yöntemleri Türkiye'de oldukça yaygındır. Örneğin, bir hacker grubunun vatansever rolü ile gençleri etkileyerek kendi kişisel çıkarlarını gerçekleştirmesi ve bunu gençler üzerinden yapması da bir tür siber zorbalıktır. Burada kullanılan yöntemler arasında aldatma, duygu sömürüsü, manipülasyon, inandırma ve hatta şantaj gibi ileriye gidebilecek faktörler yer alabilir. Genellikle internet ortamında belirli bir oluşum vasıtasıyla hedeflere ulaşarak çeşitli analizler ile siber zorbalık karşı tarafa hissettirmeden yıllar boyunca sürebilmektedir. Basit bir web sitesi bile, içeriğine göre gençleri, çocukları ve hatta yetişkinleri manipüle etmek için bir siber zorbalık aracı olabilir.

Ayrıca, zararlı yazılımlar aracılığıyla gerçekleştirilen siber zorbalık eylemleri de bulunmaktadır. Çocuklar çoğu zaman bu tür davranışların farkında olmayabilir ve maruz kaldıkları zorbalığı tanımlayamayabilirler. Bu nedenle, ebeveynlerin ve eğitimcilerin çocukların çevrimiçi etkileşimlerini dikkatle gözlemlemeleri ve siber zorbalık belirtilerini tanıyabilmeleri çok önemlidir. Güvenli web ağ geçidi ve tehdit engelleme yazılımları gibi teknolojik çözümler, çocukları çevrimiçi tehditlerden korumak için kullanılabilir. Bu yazılımlar, zararlı içeriklerin engellenmesi ve çocukların güvenli bir çevrimiçi ortamda gezinmelerini sağlamak için tasarlanmıştır. Ebeveynlerin ve eğitimcilerin, çocukları siber zorbalık konusunda bilgilendirmeleri ve onlara güvenli internet kullanımı hakkında rehberlik etmeleri gerekmektedir. Aynı zamanda, siber zorbalığa maruz kalan çocuklara destek olmak ve gerekli müdahaleleri yapmak için iş birliği içinde çalışmaları önemlidir. Bu çok yönlü yaklaşım, siber zorbalığın önlenmesi ve çocukların dijital ortamlarda daha güvenli bir şekilde var olmalarını sağlamada kritik bir rol oynamaktadır.

Siber zorbalık ve sosyal mühendislik yöntemlerinin karmaşıklığı ve çeşitliliği, bu tür tehditlere karşı daha bilinçli ve proaktif yaklaşımlar geliştirilmesini zorunlu kılmaktadır. İnternet kullanımının artmasıyla birlikte, bu tür davranışların önlenmesi ve mağdurların korunması için hem teknolojik hem de eğitsel önlemlerin bir arada kullanılması gerekmektedir. Toplumun tüm kesimlerinin, özellikle gençlerin ve çocukların, dijital dünyada güvenli bir şekilde var olabilmeleri için farkındalık seviyelerinin artırılması ve siber zorbalığın olumsuz etkilerinin minimize edilmesi hedeflenmelidir. Bu amaç doğrultusunda, sürekli güncellenen eğitim programları, teknolojik çözümler ve toplumsal bilinçlendirme kampanyaları önemli birer araçtır. Siber zorbalık ve sosyal mühendisliğin etkilerini azaltmak ve güvenli dijital ortamlar oluşturmak için bütüncül ve sürdürülebilir stratejiler benimsenmelidir.

Korunma Yolları ve Bilinçlenme

Siber zorbalıkla mücadelede yalnızca teknik önlemler ve bilgilendirme yeterli değildir; ebeveynlerin çocuklarının çevrimiçi davranışlarını düzenli olarak gözlemlemeleri ve gerektiğinde müdahale etmeleri de kritik bir öneme sahiptir. Bu, ebeveynlerin çocuklarının sosyal medya kullanımını, çevrimiçi etkileşimlerini ve katıldıkları dijital platformları yakından takip etmeleri anlamına gelir. Ebeveynlerin,

çocuklarının çevrimiçi arkadaşlıklarını ve dijital dünyadaki aktivitelerini gözden geçirmeleri, potansiyel riskleri erken aşamada tespit etmelerine yardımcı olabilir.

Aynı zamanda, ebeveynlerin çocuklarına sağlıklı çevrimiçi alışkanlıklar kazandırmaları gerekmektedir. Bu, belirli zaman dilimlerinde internet kullanımı, ekran süresinin sınırlandırılması ve dijital detox dönemlerinin teşvik edilmesi gibi uygulamaları içerebilir. Çocukların çevrimdışı aktiviteleri ve sosyal etkileşimleri de desteklenmeli, böylece dijital dünyaya bağımlılıklarının azaltılması hedeflenmelidir.

Ebeveynlerin, çocuklarının çevrimiçi ortamda karşılaşabilecekleri riskler konusunda farkındalık seviyelerini artırmak için düzenli olarak bilgilendirici oturumlar düzenlemeleri önemlidir. Bu oturumlar, siber zorbalıkla ilgili güncel gelişmeleri, yeni tehdit türlerini ve bunlarla başa çıkma stratejilerini kapsamalıdır. Ebeveynler, çocuklarına siber zorbalığın yalnızca bir kurban olarak değil, bir zorba olarak da karşılarına çıkabileceğini anlatmalı ve bu tür davranışların neden yanlış olduğunu detaylı bir şekilde açıklamalıdır.

Siber zorbalıkla mücadelede topluluk ve okul destek sistemlerinin de devreye girmesi gerekmektedir. Ebeveynler, çocuklarının okulları ile işbirliği yaparak, siber zorbalıkla mücadele politikalarının ve programlarının geliştirilmesine katkıda bulunabilirler. Okulların, öğrenciler arasında siber zorbalık farkındalığını artırmak ve bu tür davranışları önlemek için eğitim programları ve atölye çalışmaları düzenlemeleri teşvik edilmelidir. Ebeveynler, öğretmenler ve okul yöneticileri arasındaki düzenli iletişim ve işbirliği, siber zorbalık vakalarının erken tespit edilmesi ve hızlı müdahalelerde bulunulması açısından hayati önem taşır.

Siber zorbalıkla mücadelede yerel ve ulusal düzeydeki politikaların ve yasaların da etkin bir şekilde uygulanması gerekmektedir. Ebeveynler, bu yasal çerçeveler hakkında bilgi sahibi olmalı ve gerekli durumlarda yasal yollara başvurarak çocuklarını koruma altına almalıdır. Ayrıca, toplumun genelinde siber zorbalık konusunda farkındalığın artırılması amacıyla kamuoyu kampanyalarının düzenlenmesi önemlidir. Bu kampanyalar, siber zorbalığın olumsuz etkilerini vurgulayan, bilinçlendirici ve eğitici içeriklerle desteklenmelidir.

Sonuç olarak, siber zorbalıkla mücadele, ebeveynlerin teknik önlemler almasının yanı sıra çocuklarıyla sürekli ve açık bir iletişim kurmasını gerektiren çok yönlü bir süreçtir. Çocukların dijital dünyada karşılaşabilecekleri tehlikelerden korunabilmesi için, ebeveynlerin bilinçli, proaktif ve işbirliğine dayalı bir yaklaşım benimsemeleri gerekmektedir. Bu kapsamlı strateji, çocukların dijital ortamlarda güvenli bir şekilde var olmalarını sağlayacak ve siber zorbalığın olumsuz etkilerini minimize edecektir.

KAYNAKÇA

[1] Paltacı, B. M. (2024). Yanlış Yönlendirmeler ve Acı Sonuçlar: Siber Zorbalık ve İstismar. *Siber Güvenlik*

[2] Patchin, J. W., & Hinduja, S. (2010). *Siber Zorbalığın Önlenmesi ve Yanıt Verilmesi: Uzman Görüşleri.*

[3] Livingstone, S., & Smith, P. K. (2014). Yıllık Araştırma İncelemesi: *Çevrimiçi ve mobil teknolojileri kullanan çocukların maruz kaldığı zararlar: Dijital çağda cinsel ve agresif risklerin doğası, yaygınlığı ve yönetimi.*