Z KUŞAĞININ SOSYAL AĞLARDA KARŞI KARŞIYA OLDUĞU TEHLİKELER VE ONLARI BU TEHLİKELERDEN KORUMAYA YÖNELİK ÖNERİLER

THE THREATS Z GENERATION FACE ON SOCIAL MEDIA AND SUGGESTIONS TO PROTECT THEM FROM THESE THREATS

Hatice Gökçe BİLGİÇ*, Süleyman Sadi SEFEROĞLU**

Özet: Son yıllarda gelişen İnternet teknolojileri ve artan İnternet erişimi ile beraber sosyal ağların kullanımı da hızla yaygınlaşmaktadır. Günümüzde özellikle gençler, mobil telefonlar üzerinden artan İnternet erişimi ile her an her yerden sosyal ağlardaki varlıklarını sürdürebilir durumdadırlar. Gençler tarafından yoğun ilgi gören bu sosyal ağlara örnek olarak Facebook, Twitter, Instagram, Messenger, Youtube, Pinterest ve Blogger gibi ortamlar verilebilir. Gençler bu ortamları bilgiye erişmek, arkadaşları ile sosyal paylaşımda bulunmak, diğer insanların paylaşımlarını takip etmek, oyun oynamak, video vb. içerikleri izlemek, eğer varsa okul ve öğretmen paylaşımlarını takip etmek ve müzik dinlemek gibi amaçlarla yaygın bir şekilde kullanmaktadırlar. Sınırsız bir kitlenin yer aldığı sanal dünyada gençler hiç tanımadıkları kişi veya gruplarla da bağlantı kurabilmekte ve kendilerine ait kişisel bilgileri güven duydukları bu kişilerle rahatlıkla paylaşabilmektedirler.

Sosyal ağlar farklı yaş gruplarından, farklı sosyo-ekonomik düzeylerden, farklı kültürel ortamlardan, farklı eğitim seviyelerinden ve farklı psikolojik yapılardan birçok insanın aktif olarak yer aldığı kozmopolit bir sanal dünya olarak değerlendirilebilir. Gençler, bu farklı yapıları içinde barındıran sanal dünyanın ve özellikle sosyal ağ ortamlarının en geniş kullanıcı kitlesini oluşturmaktadırlar. Kullanıcılarına çok sayıda fırsat sunan bu sanal yapılar, birtakım olumsuzlukları ve tehlikeleri de barındırmaktadırlar. Başka bir ifadeyle sosyal ağların iletişim konusundaki esnek yapısı nedeniyle, bu ağlardaki varlığını yoğun bir şekilde sürdüren gençler birtakım tehdit ve risklerle karşı karşıya kalabilmektedirler.

Kitabın bu bölümünde sosyal ağ ortamlarının gençler için oluşturdukları riskler incelenerek, gençlerin bu risklerden korunması konusunda çeşitli öneriler sunulmaktadır. Bu bağlamda, öncelikle Türkiye'de ile çeşitli diğer ülkelerde İnternet ve sosyal ağ kullanımı, gençlerin sosyal ağları kullanım amaç ve durumları, gençlerin bu ortamlarda karşılaşabilecekleri tehditler ve bu tehditlerin onların hayatı üzerindeki olumsuz etkileri incelenmiştir. Ayrıca bu tehditlerin önlenmesi ile gençlerin kendilerini bu tehlikelerden korumalarına yönelik öneriler ele alınmıştır. Gençlerin sosyal ağ ortamlarındaki tehlikelerden korunmasına yönelik öneriler; hem gençlerin kendi öz-denetimleri doğrultusunda dikkat etmeleri gerekenler hem de ebeveyn ve öğretmenlerin yapabilecekleri bağlamında gruplandırılarak sunulmuştur. Kitap bölümünün sonunda sosyal ağlarda yaşanan sanal zorbalık ile savaşmaya yönelik geliştirilen yeni teknolojiler tanıtılmıştır.

Anahtar Sözcükler: Sosyal ağlar, sanal dünya, sosyal ağlarda tehlike, güvenlik önlemleri, dijital gençlik.

Abstract:In recent years, with the development of Internet technologies, use of social networks have become widespread rapidly. Today, especially youths are living in social networks by the increasing use of Internet through mobile phones. Facebook, Twitter, Instagram, Messenger, Youtube, Pinterest and Blogger can be shown as instances of social networks that youths are intensively interested in. These social network environments are being used as to reach information, to share with their friends, to follow others, to play game, to watch video and similar content, to follow posts made by school or teachers, to listen to music, and etc. In the virtual world, in which there exists mass of people, youths might be connected with people that they do not know before, and share their personal private information with those easily since they find them trustworthy.

Social networks can be considered as a cosmopolitian virtual world in which people from different age groups, different socio-economic levels, different cultural backgrounds, different educational levels and different psychological situations exist. Youths are the most pervasive population of this virtual world. Thus, although these virtual worlds especially social networks provide many opportunities for youths, they might also confront them with some negative consequences and threats.

*Dr. Öğr. Üyesi, Ondokuz Mayıs Üniversitesi, Eğitim Fakültesi, Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü, Samsun. e-Posta: gokce.dogan@omu.edu.tr

** Prof. Dr., Hacettepe Üniversitesi, Eğitim Fakültesi, Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü, 06800, Beytepe-Ankara. e-Posta: sadi@hacettepe.edu.tr

Focus of this chapter is to examine the threats of social network environments for youths including z-generation and to provide recommendations in order to protect them from these threats. In this context, firstly, use of Internet and social networks in Turkey and in other countries, youths' purposes and cases of social network use, threats that youths might face in these environments and the negative effects of these threats on youths are examined. Moreover, recommendations to prevent these threats and to protect youth generations from these threats are investigated. These recommendations are provided for both young people themselves, and their parents and teachers on what could be done. In addition to these, in the final part of the chapter, information about some new technologies that might be used in fighting cyberbullying in social networks, are provided.

Keywords: Social networks, virtual world, threats in social networks, security issues, digital generations.

GİRİŞ

Bilgi ve iletişim teknolojilerinde yaşanan gelişmeler bilgiye erişmek, bilgiyi sunmak, günlük ihtiyaçlarımızı gidermek, alışveriş yapmak, iletişimde bulunmak, araştırma yapmak, ürün geliştirmek, paylaşımda bulunmak gibi etkinliklerimizin birçoğunun gerçekleşme biçiminde değişikliğe yol açmıştır (Canbek & Sağıroğlu, 2007; Cohen-Almagor, 2018; Fallows, 2004; Kowalski, Limber, & McCord (inPress); Tuncer & Dikmen, 2016). Özellikle teknolojinin içine doğmuş olan ve Z kuşağı olarak adlandırılan yeni nesil için bu etkinliklerin günümüz teknolojileri kullanılmaksızın gerçekleştirilmesi olanaksız bir hal almıştır. Bu nesil doğdukları ilk günden itibaren bir şekilde teknoloji ile yüz yüze gelmiş, ilerleyen yaşlarda da oyun oynamak, bilgiye erişmek ve arkadaşları ile iletişime geçmek gibi temel ihtiyaçlarının karşılanmasında teknolojiyi hayatlarının merkezine yerleştirmiştir. Özellikle mobil cihazların kullanımının yaygınlaşması ve mobil cihazlardan İnternet erişiminin artmasıyla birlikte sosyal ağların kullanımının giderek yaygınlaştığı görülmektedir. Günümüzde gençler arkadaşlarıyla haberleşmek, paylaşımda bulunmak, başkalarının paylaşımlarını takip etmek gibi kişisel iletişim boyutundaki birçok amacı sosyal ağ ortamları aracılığıyla gerçekleştirmektedirler (Durak & Seferoğlu, 2016b). Öyle ki artık insan-insan etkileşiminin yüz yüze etkileşimden yavaş yavaş uzaklaşan ve çoğunlukla bir bilgisayar veya benzeri teknolojik araçtaki arayüz üzerinden gerçekleşen boyutunun tartışıldığı görülmektedir (Çağıltay, 2017). Teknolojilerin sunduğu kolaylıklarla birlikte hızla değişen iletişim alışkanlıkları bireyleri diğer insanlara yabancılaşma ve daha bireysel düşünme, kendi çıkarlarını ön plana alma, başkasının haklarını önemsememe gibi tavır ve davranışlar sergilemeye itebilir. Bu durum da İnternet ortamında istenmeyen, etik dışı iletişim biçimlerinin ortaya çıkmasına sebep olabilir (Çelen & Seferoğlu, 2016). Örneğin gençler sanal ortamdakilere göre gerçek hayatta kurulan arkadaşlıklara daha fazla güven duymaktadır. Ayrıca sanal ortamda daha az anlaşılır olduklarını düşünen gençler gerçek ortamda kendilerini daha rahat hissedebilmektedir. Bu durum gençlerin sanal yalnızlık duygusu içinde olduğuna işaret edebilir. Öte yandan gençlerin birçoğu; sanal ortamdaki diğer kullanıcılarla pek fazla ortak yönleri olmasa da, sanal ortamda arkadaşlıklar kurabilmekte, kendilerini diğer insanlarla uyum içinde hissetme eğilimi gösterebilmektedir. Bu durum her geçen gün kullanıcı sayısı ve popülerliği artan sosyal ağ ortamlarında güvenli iletişim ve etkileşim konusunda ikilem yaşayan gençlerin yönlendirilmesi gerekliğini gündeme getirmektedir (Çelen, Çelik & Seferoğlu, 2017).

Bunların ötesinde artık yeni İnternet çağı insanları için bilgisayar donanımlarının, yazılımlarının ve iletişim seçeneklerinin sunduğu avantajlar ile birlikte çevrim-dışı hayatlarına ek olarak sanal bir hayatın oluştuğu ileri sürülmektedir (Cohen-Almagor, 2018). Bu yenilik ve değişimlerin sonucu olarak, teknoloji dünyası gençler için sunduğu avantajlarla beraber odaklanılması gereken yeni risk ve tehditleri de ortaya çıkarmaktadır.

Sosyal ağlardaki birincil tehlike gençler tarafından paylaşılan kişisel bilgi ve içeriklerin kötü niyetli kişiler tarafından ele geçirilmesidir. Bu tehlikenin de büyük ölçüde gençlerin tanımadıkları kişilerle iletişime geçmeleri durumunda yaşandığı görülmektedir. Bu bağlamda, örneğin bu ortamlardaki gençleri kandırmak, onları yanlış yönlendirmek veya onları farklı yollarla istismar etmek amacıyla çok sayıda sahte hesabın oluşturulduğu görülmektedir (Tuncer & Dikmen, 2016). Bu hesaplardaki kimlikler çoğunlukla gerçek kimlikleri temsil etmemektedir. Bu sahte kimliklerle sosyal ağ ortamlarında gençlerle arkadaşlıklar kurulabilmekte ve onların güvenleri kazanılmaktadır. Daha sonra da ele geçirilen kişisel bilgi ve içeriklerle onları zor duruma sokacak ve hatta onları rehin alabilecek senaryolar devreye sokulabilmektedir. Gençler bu süreçte doğal olarak korku ve endişe yaşamaktadırlar. Bu durumdaki kişiler örneğin kendilerine yapılan tehdit ve şantajlar doğrultusunda birtakım yönlendirmelere uymak zorunda kalabilmekte ve istemedikleri davranış ve eylemler için zorlanabilmektedirler (BBC, 2017a; GüvenliWeb Oyun, 2018a).

Gençlerin sosyal ağ ortamlarında karşılaştıkları bu tehditler sonrasında depresyona girdikleri ve kendilerini çıkmazda hissederek hayatlarını sonlandırmaya niyetlenmeleri gibi çok ciddi sonuçları bile yaşayabildikleri görülmektedir (BBC, 2017a; GüvenliWeb Oyun, 2018a). Özellikle son dönemlerde gizli bağlantılar üzerinden oyun ortamı adı altında farklı istismar alanlarına dahil edilen gençlerin, bu oyunların

hedefleri doğrultusunda yapılan yönlendirmelerle hayatlarına son verdikleriyle ilgili çok sayıda habere rastlanmaktadır. Bu yüzden bu tehditlere maruz kalan gençlerin hem alınabilecek önlemler konusunda yönlendirilmelerinin hem de karşılaştıkları tehdit ve şantajlar karşısında gerekli kanallara başvurmaları konusunda bilinçlendirilmelerinin çok önemli olduğu söylenebilir (Tuncer & Dikmen, 2016).

Bu bölümde gençleri bu ortamlardaki risk ve güvenlik tehditlerinden koruma yollarını planlamadan önce öncelikli olarak Dünya çapında ve ulusal çapta yapılan araştırmaların sonuçları temel alınarak İnternet ve sosyal ağ kullanım durumlarının incelenmesi amaçlanmaktadır. Bu bağlamda ayrıca gençlerin bu ortamları kullanım durumlarıyla ilişkili olası risk ve tehditler irdelenmekte ve son olarak bu risk ve tehditlerden korunma yolları sunulmaktadır.

Ulusal ve Uluslararası Düzeyde İnternet ve Sosyal Ağ Kullanım Durumları

Bireylerin İnternet ve sosyal ağ kullanımlarının incelendiği ulusal ve uluslararası çalışmalarda internet kullanımı, mobil cihazlardan İnternete erişim ve giderek artan sosyal ağ kullanım oranlarıyla ilgili çarpıcı veriler göze çarpmaktadır. Örneğin We Are Social ve Hootsuite her yıl düzenli olarak dünya çapında internet ve sosyal medya/ağ kullanım istatistikleri hazırlamakta ve bu verileri kamuoyuyla paylaşmaktadır. Gençlerin sosyal ağ kullanım durumlarını incelemeden önce İnternet ve sosyal ağ kullanım oranlarıyla ilgili verilerin incelenmesinin önemli olduğu düşünülmektedir. Bu inceleme dünya genelindeki ve Türkiye'deki genel eğilimleri görebilmek açısından önemlidir.

Dünya çapında gerçekleştirilen araştırma sonuçlarına göre 2018 yılı itibariyle 7.593 milyar olan dünya nüfusunun %53'ü (4.021 milyar) İnternet kullanıcısı iken %42'si de (3.196 milyar) aktif sosyal medya kullanıcısıdır. 2017 yılı verileri ile 2018 yılı verileri karşılaştırıldığında İnternet kullanıcı sayısının %7 (248 milyon) ve aktif sosyal medya kullanıcı sayısının ise %13 artış gösterdiği anlaşılmaktadır. Dünya'daki sosyal medya kullanıcılarının %93'ünün sosyal medya erişimini akıllı telefon veya tablet gibi mobil cihazlar üzerinden sağlaması ise (We Are Social, 2018) artan mobil cihaz kullanımı ile beraber sosyal medya kullanımının da yaygınlaşmasına bir kanıt olarak gösterilebilir.

Aynı araştırma kapsamında Türkiye ile ilgili veriler incelendiğinde ise Türkiye'de ülke bazında nüfusun %67'sinin İnternet kullanıcısı, %63'ünün ise aktif sosyal medya kullanıcısı olduğu görülmektedir. Bu oranlar Dünya geneline ait oranların (%53 ve %42) üzerinde yer almaktadır (We Are Social, 2018). TUİK (2018b) tarafından yapılan "Hanehalkı Bilişim Teknolojileri Kullanım Araştırması" sonuçlarına göre ise son üç ay içinde bireylerin yaş grubuna göre İnternet kullanımı oranlarının 16-24 yaş aralığındaki kişilerde %90,4, 25-34 yaş aralığında %90,1, 35-44 yaş aralığında %80 ve %45-54 yaş aralığında %61,5 olduğu görülmektedir. We Are Social (2018) verilerine göre Türkiye'de herhangi bir cihazdan erişim ile sosyal medyada geçirilen zamanın günlük ortalama 2 saat 48 dakika olduğu belirtilmektedir. Buna ek olarak, Türkiye aktif Instagram kullanıcıları sıralamasında 33 milyon (%42) kullanıcı ile dünya sıralamasında 5. sırada yer almaktadır. Bu da ülke olarak sosyal ağ ortamlarına olan ilgimizin bir göstergesi olarak değerlendirilebilir.

Öte yandan TUİK (2018a) tarafından 16-74 yaş arası bireylerle gerçekleştirilen "son üç ay içinde İnternet kullanımı" başlıklı çalışmada bireylerin interneti kişisel amaçlarla kullanımlarıyla ilgili olarak aşağıdaki dikkat çekici oranlar ortaya çıkmıştır:

- Katılımcıların %84'ü sosyal medya üzerinde profil oluşturma, mesaj gönderme veya fotoğraf vb. içerik paylaşımında bulunmuştur.
- Katılımcıların %35'i oyun oynamış veya oyun indirmiştir.
- Katılımcıların % 78'i YouTube gibi paylaşım sitelerinde video izlemiştir.
- Katılımcıların %45'i e-posta gönderme veya alma işlemleri gerçekleştirmiştir.

Böylece hem Türkiye'de hem de çeşitli diğer ülkelerde İnternet kullanıcılarının büyük bir çoğunluğunun artan İnternet kullanımıyla birlikte sosyal ağ ortamlarına yoğun ilgi gösterdiği görülmektedir. Dünya çapında İnternet ve sosyal ağ kullanımının incelendiği araştırma sonuçlarında sosyal ağ kullanımıyla ilgili verilere bakıldığında sırasıyla Facebook, Youtube ve WhatsApp'ın öne çıktığı anlaşılmaktadır. Bu sosyal ağ ortamlarının bazılarının aktif kullanıcı profilleri incelendiğinde ise yoğun bir genç kullanıcı kitlesi ortaya çıkmaktadır. Örneğin, Facebook kullanıcılarının %8'inin 13-17, %29'unun 18-24 ve %29'unun da 25-34 yaşları arasında olduğu görülmektedir (We Are Social, 2018). Instagram kullanıcılarının ise %7'sinin 13-17 yaş, %31'inin 18-24 yaş ve %30'unun 25-34 yaş aralığında olduğu bulunmuştur.

Bu araştırmalara ek olarak TUİK tarafından 2013 yılında 06-15 yaş grubu çocuklarda bilişim teknolojileri ve medya kullanım durumunu ortaya çıkarmayı amaçlayan bir araştırma yapılmıştır. Bu araştırmanın verilerine bakıldığında Türkiye'de bilgisayar kullanımına ortalama 8 yaşında, İnternet kullanımına ortalama 9 yaşında ve cep telefonu kullanımına ise ortalama 10 yaşında başlandığı görülmektedir. Verilere göre

çocukların %60,5'i bilgisayar, %50,8'i İnternet ve %24'ü cep telefonu kullanmaktadır. Bunlara ek olarak çocukların %24,4'ünün kendi kullanımına ait bilgisayarları bulunmaktadır (TUİK, 2013). Çocukların İnternet'i kullanım amaçları incelendiğinde ise %84,4'ünün İnternet'i ödev yapmak ve öğrenmek, %79,5'inin oyun oynamak, %56,7'sinin bilgi aramak ve %53,5'nin ise sosyal medya ağlarını takip etmek amacıyla kullandığı bulunmuştur. Bu verilerin 2013 yılı araştırma sonuçlarına ait olduğu düşünülürse de geçen yıllar içerisindeki artan mobil cihaz kullanımı ve mobil İnternet erişimi ile gelinen noktanın boyutları düşündürücü olabilmektedir.

Çevrim-içi etkinliklerin gençler arasında hızla yaygınlaşması, gelişen dijital dünyanın gençlere sosyal normlarla boğuşabilme, ilgilerini keşfetme, teknik becerilerini geliştirme ve kendini ifade etmenin farklı yollarını tecrübe etme gibi olanaklar sunması ile açıklanmaktadır (Ito vd., 2008). Gençler dijital dünyada en çok sosyal ağ ortamlarında ortaya çıkmaktadır (O'Keeffe, Clarke-Pearson & Council on Communications and Media, 2011). Ito vd.'nin araştırmasının verilerine göre gençlerin büyük bir çoğunluğu sosyal ağları öncelikli olarak okul veya spor gibi tanıdık ortamlardaki arkadaşları ile olan iletişim ağını genişletmek için kullanmaktadır. Mobil telefonlar veya anlık mesajlaşma platformları gençlere her zaman özel bir iletişim ağı kurma olanağı sunmaktadır. Gençler sosyal ağlarda herkese açık olabilen ortamlarda da iletişimde bulunabilmektedirler. Böylece arkadaşlar arasında halihazırda çevrimdışı olarak devam eden iletişim ağı günümüz dijital dünyasında gençlerin büyük bir çoğunluğu tarafından sosyal ağlar gibi dijital platformlara taşınmış olmaktadır.

Öte yandan gençlerin bir kısmı bu ortamları ilgi alanlarına yönelik keşifler yapmak amacıyla da kullanmaktadır. Çevrim-içi platformlar üzerinde gençler özel ilgi alanlarına yönelik bilgilere erişmek amacıyla daha önceden tanışmadıkları insanlarla iletişime geçebilmektedirler (Ito vd., 2008). Böylece İnternet insanlar arasındaki fiziksel engelleri ortadan kaldırırken sunduğu iletişim imkânları ile beraber sınırları genişletmektedir. Ancak bu genişleme ile gençler ve çocuklar için esnek ve kontrolsüz bir iletişim ortamı meydana gelmektedir (Sırakaya & Seferoğlu, 2018). İşte bu noktada gençlerin karşı karşıya kalabilecekleri birtakım risk ve tehditler söz konusu olabilmektedir. Sosyal ağların bu çerçevede kullanımı gençlere sınırlı alanlarının dışındaki insanlara erişme, kendi ürettikleri içerikleri herkese açık olarak paylaşma ve yeni bir çeşit görünürlük ya da ün kazanma imkânı sunmaktadır.

Sosyal Ağlarda Gençleri Bekleyen Riskler ve Güvenlik Tehditleri

Sosyal ağ ortamları ve bu ortamlarla ilişkili teknolojilerin kullanıcılarına sunduğu birçok yararı olmasına rağmen, bunların kullanımı ile ilişkili ciddi tehlikeler de söz konusudur (Cohen-Almagor, 2018; Durak & Seferoğlu, 2016a; GüvenliWeb, 2017; Picazo-Vela, Gutierrez-Martinez & Luna-Reyes, 2012). Sosyal ağ ortamlarının kullanımı yeni nesil çocuk ve ergen grupları arasındaki en yaygın etkinliklerden birisi olarak ortaya çıkmaktadır. Facebook, Twitter, Instagram ve Snapchat gibi sosyal ağ ortamlarının gençler arasında artan popülaritesi sanal zorbalığa maruz kalma ihtimallerinde de artışa neden olmuştur (Cohen-Almagor, 2018). Öte yandan, yeni kuşağın büyük bir çoğunluğunun sosyal ve duygusal gelişiminin İnternet üzerinde veya mobil telefonlar üzerinde oluştuğu ileri sürülmektedir (O'Keeffe vd., 2011). Bu yüzden çocukların ve gençlerin sosyal ağ ortamlarının barındırdığı olası risk ve güvenlik tehlikelerinden korunması, bu gençlerin sosyal, duygusal ve hatta fiziksel gelişimleriyle ilgili olarak oluşabilecek zararların da en aza indirilmesi açısından büyük öneme sahiptir (Yildiz-Durak, 2018).

Günümüz toplumunda ergenlik öncesindeki ya da ergenlik dönemindeki yeni nesil için en temel riskler "teknolojinin uygunsuz ve yersiz kullanımı, gizlilik ve mahremiyet eksikliği, çok fazla miktarda kişisel bilgi paylaşımı, dijital okuryazarlık konusundaki yetersizlik ve deneyimsizlik ile sosyal olarak uygun olmayan kullanım" (O'Keeffe vd., 2011; Picazo-Vela vd., 2012) şeklinde listelenebilir. Gençlerin sanal ortamların doğru kullanımı konusunda yeterli bilgiye sahip olmayışları ve bu bağlamda yanlış olarak değerlendirilebilecek olan davranışları öncelikli olarak gizlilik ve mahremiyet sorunlarına yol açmaktadır.

Öte yandan çevrim-içi ortamlarda dijital ayakizi bırakmayla ilgili farkındalık düzeyinin düşük oluşu gençler için önemli risklerden bir diğeri olarak ortaya çıkmaktadır. Dijital kimlik kavramı çağımızın önemli kavramları arasında yer almaktadır (Durak, 2016). Bireyler sosyal ağ ortamlarını kullanmak, bu ortamlarda profil oluşturmak ve yönetmek için temsili kimlikler oluşturmaktadırlar. Bu kimlikler üzerinden kullanıcıların çevrim-içi ortamlardaki dolaşımları sırasında bütün yaşananlarla ilgili kayıtlar oluşturulmaktadır. Çevrim-içi ortamda gerçekleştirilen bütün işlemlerin kayıtlarının oluşturulup depolanması işlemi alanyazında "dijital ayakizi" olarak tanımlanmaktadır. Gençler için sosyal ağ ortamlarının en büyük tehlikelerinden birisi bırakılan dijital ayakizi ve bunun geleceğe yönelik olası sonuçlarıdır. Bu bağlamda ilerleyen yıllarda bu ortamların kullanıcılarının mesleki hayatının, geçmişte bilgisizlik veya deneyimsizlikten kaynaklanan nedenlerle gerçekleştirilen birtakım fare tıklamaları sonucunda tehlikeye atılması ihtimalinin olduğu ileri sürülebilir (O'Keeffe vd., 2011).

Sanal dünyada çocukların ve gençlerin karşı karşıya oldukları başka bir tehlike de sanal zorbalıktır. Sanal ortamlarda yaşanan sanal zorbalıklar "siber zorbalık" veya "elektronik zorbalık" olarak da bilinmektedir. Bu bölümde sosyal ağ ortamlarında yaşanan zorbalık olayları sanal zorbalık olarak isimlendirilecektir. Sanal zorbalık sanal dünyada yaşanan zorbalık biçimi olarak ifade edilebilir. Sanal zorbalık kavramını doğru anlayabilmek için öncelikle geleneksel zorbalık kavramının incelenmesinde yarar bulunmaktadır. Zorba kavramı TDK Güncel Sözlükte "gücüne güvenerek hükmü altında bulunanlara söz hakkı ve davranış özgürlüğü tanımayan kimse" olarak, zorbalık ise "zorbaca davranışta bulunma" şeklinde tanımlanmaktadır (TDK, 2018). Böylece gücüne güvenen kişilerin kendinden daha güçsüz konumda olan kişilere uyguladığı her türlü kötü davranış ve zorlama hareketi zorbalığa örnek olarak verilebilir.

Geleneksel zorbalık kavramı bir bireye bireysel veya grup olarak uygulanan, tekrarlayıcı nitelikte eylem ya da davranışların oluşturduğu saldırganlık şeklinde de tanımlanmaktadır (Durak & Seferoğlu, 2016a; Olweus, 1996; Whitney & Smith, 1993). Sanal zorbalık da bu zorbalığın sanal dünyadaki yeni formu olarak gösterilmektedir. Sanal zorbalık ayrıca, Samsung ve Bilgi Teknolojileri ve İletişim Kurumu (BTK) işbirliğinde gerçekleştirilen "Siber Zorba Olma" başlıklı etkinlikte "bilgi ve iletişim teknolojileri aracılığıyla bir bireyin ya da bir grubun diğerlerine yönelik düşmanlık, korkutma, tehdit, sindirme, taciz amaçlı yazılı veya görsel iletileri kasıtlı ve düzenli bir şekilde göndermesi" olarak tanımlanmıştır (Samsung, 2017).

Sanal zorbalığın değişen yüzü ile beraber artan tehlikenin ortaya konulması amacıyla Tablo 1'de geleneksel zorbalıktan sanal zorbalığa geçişte değişen özellikler sunulmuştur. Geleneksel zorbalıkta mağdur tarafın sadece yüz yüze ortamlarda zorbalığa maruz kalması hem zamansal hem de mekânsal olarak kaçış noktaları sağlamaktadır. Ancak sanal zorbalıkta sanal dünyanın sınırsız yapısı dolayısıyla mağdurun herhangi bir yerde ve zamanda zorbalıkla karşı karşıya kalabildiği görülmektedir. Geleneksel zorbalıkta zorbalığa şahit olan kitle sınırlı iken, sanal zorbalıkta sanal dünyanın herkese açık bir ortam olması nedeniyle bu tür zorbalıklara sınırsız bir kitle şahit olabilmektedir. Başka bir ifadeyle, sanal zorbalığın zaman, mekân ve kitle gibi konulardaki sınırsızlığı mağdurun çok daha ciddi bir durum ile karşı karşıya kalması anlamına gelebilmektedir.

Tablo 1. Geleneksel Zorbalıktan Sanal Zorbalığa Değişen Özellikler (Durak & Seferoğlu, 2016a)

Geleneksel Zorbalık	**Sanal Zorbalık**
Yüz yüze ortamlarda gerçekleşebilir.	Elektronik araçlarla çevrim-içi olarak herhangi bir zamanda gerçekleşebilir.
Zorba kolay tespit edilebilir.	Zorbanın tespiti kolay değildir.
Zorbalıktan kaçış imkânı ya da güvenli alanlar vardır.	Güvenli alan yoktur ve kaçış zordur.
İzleyici kitle sınırlıdır.	İzleyici kitlenin coğrafi bir alan sınırlılığı yoktur.
Kurban ile zorba arasında güç dengesizliği vardır.	Kurban ile zorba arasında güç dengesizliği vardır. Ancak çevrim-içi ortamda kullanılan elektronik içerikler daha hızlı yayıldığından etki değeri daha yüksektir.
Genellikle okul ile sınırlıdır.	Zorbalık herhangi bir yerde ve herhangi bir zamanda gerçekleşebilir.

Sanal zorbalık olarak karşılaşılan örnekler "Siber Zorma Olma" hareketi kapsamında geliştirilen Eğitici Kitapçıklarda (Akca, 2017a; Akca 2017b) aşağıdaki şekilde listelenmektedir:

- Bireylerin görüntülerini onların izinleri olmaksızın mobil cihazlar aracılığıyla çekip paylaşmak,
- Bireylerin görüntülerini onların onayları olmaksızın mobil cihazlar aracılığıyla çekip paylaşmak,
- Diğer kullanıcılara sosyal ağlar ya da sohbet odaları gibi çevrim-içi ortamlarda aşağılayıcı, alay edici, öfke dolu, kaba, cinsel taciz veya şiddet içeren mesajlar göndermek,
- Birinin kişisel bilgilerini o kişinin rızası ve haberi olmadan İnternet ortamında paylaşmak,
- Sosyal ağlarda birisi hakkında dedikodu yaymak ya da özel hayatıyla ilgili konuları açıklamak,
- Bir kişiye ilişkin karalayıcı, aşağılayıcı web sayfaları hazırlamak,
- Başkası adına sahte hesap açıp, onun kimliğine bürünmek,
- Bir kişinin çevrim-içi ortamdaki tüm hesaplarını ısrarlı bir biçimde takibe almak,

- Bir kişinin sosyal ağlardaki paylaşımlarına sürekli olumsuz yorumlar yapmak,
- Ortak tanıdıklarını etkileyerek hedef olan seçilen bireyi, arkadaş listelerinden silmelerini veya bloke etmelerini, yani sosyal olarak dışlamalarını sağlamak.

Kaspersky Lab (2016) tarafından yapılan bir çalışmada ise "İnternet veya mobil telefonlar gibi diğer teknolojilerle doğrudan veya doğrudan olmayan yollarla, sözlü, yazılı veya fiziksel öğelerle korkutmak, tehdit etmek, taciz etmek, utandırmak gibi amaçlar güderek güç ve etki gibi uygun olmayan davranışların sergilenmesi" olarak tanımlanan sanal zorbalığın Şekil 1'de gösterilen 10 formunun olduğu ileri sürülmektedir:

1. Dışlamak (Exclusion)

Sosyal medya ortamlarında kurulan sohbet ortamlarına birisini davet etmemek, yapılan paylaşımlarda herkesi etiketlerken onu etiketlememek gibi davranışlar ilgili kişinin o grubun dışında bırakılmasının amaçlandığı türden davranışlar olarak değerlendirilebilir.

2. Taciz/Rahatsız Etmek (Harrassment)

Taciz eylemi sanal zorbalığın en tehlikeli boyutlarından birisidir. Taciz, kötü sözlerle ve cinsel içerikli mesajlarla kişinin rahatsız edilmesidir. Bu eylem gençler üzerinde ciddi olumsuz etkiler bırakmaktadır. Örneğin, bireyin kendine öz-saygısını ve güvenini yitirmesi gibi sonuçlar doğurabilmektedir.

3. Utandırmak/Küçük Düşürmek (Outing)

Bir bireyle ilgili özel bir bilginin ilgili kişinin izni alınmadan, bir ortamda onun küçük düşmesine veya utanmasına sebebiyet verecek şekilde diğer kişilerle paylaşılmasıdır.

4. Sinsice İzlemek (Cyberstalking)

Genellikle yetişkinlerin cinsel içerikli ve taciz amaçlı olarak gençleri izleyerek İnternet üzerinden iletişim kurması eylemi olarak tanımlanabilecek olan bu eylem türü çok ciddi sonuçları olabilecek en tehlikeli sanal zorbalık formlarından birisidir. Bu tür eylemlerin gençlerin hem fiziksel hem de ruh sağlığında ciddi sonuçları olabilir.

5. Bir Birey Adına Mesaj Göndermek (Fraping)

Bu sanal zorbalık eylemi bir kişinin sosyal medya hesabına giriş yaparak onun rolüne geçilmesi ve onun adına başkalarına mesajlar atılması eylemidir. Özellikle akranlar arasında yaygın olan ve eğlenceli olarak görülen sanal zorbalık formlarından birisidir.

6. Sahte Hesaplar Oluşturma (Fake Profiles)

Bu sanal zorbalık türü sahte hesaplar açarak kişilere bu sahte hesaplar üzerinden tehdit içerikli mesajların gönderilmesidir. Bazen sahte hesaplar yerine başkalarının e-posta adresleri ya da telefonları bu tehdit içerikli mesajların gönderimi için kullanılabilir.

7. Bir Birey Hakkında Kötü Mesajlar Göndermek (Dissing)

Bu eylem, bir bireyin saygınlığını yitirmesine sebep olacak şekilde kötü içerikli mesajların dağıtımını içerir. Mesajların ötesinde, kişiye ait özel fotoğraflar, videolar veya ekran görüntüleri ile içerikler de gönderilebilir.

8. Kandırmak/Hilekârlık (Trickery)

Bu eylem bir kişinin özel bilgilerini ve sırlarını ele geçirecek kadar güven kazanıp, kazanılan güven neticesinde elde edilen bilgilerin kamusal olarak herkesle paylaşılmasıdır.

9. Avlamak (Trolling)

Bu eylem özellikle çevrim-içi forumlarda veya sosyal ağ sitelerinde karşı tarafı kışkırtıcı ve provoke edici mesajlar göndererek onun da aynı şekilde tepki vermesini sağlamak üzere planlanan saldırı etkinliğidir. Genellikle kişilerin kendini tatmin etmek ve zevk almak amaçlı uyguladığı bir zorbalık formudur.

10. Oltalamak (Catfishing)

Bu sanal zorbalık türü bir kişinin özel hesabının ve bilgilerinin çalınarak bu hesap ve bilgilerinin aldatıcı sosyal ağ hesabı olarak kullanılmasıdır. Bu eylem türünde ele geçirilen hesaplardaki bilgi ve belgeler kullanılarak sahte hesaplar oluşturulmaktadır. Böylece kişinin kendi adıyla görüntülenen kişisel hesabı, içerdiği bilgi ve görsellerle birlikte başka kişileri kandırmak amaçlı bir sahte hesabın içeriğinde kullanıldığından kişinin kötü bir üne sahip olmasına neden olunabilmektedir.

Şekil 1. Siber/Sanal Zorbalığın 10 Formu

Günümüzde yaygın olarak karşılaşılan tehditlerden bir diğeri de dijital oyun ortamlarının kötüye kullanılmasıdır. Bu bağlamda bazı dijital oyunların ortaya çıkışı sözde dijital oyun akımı olarak adlandırılmıştır (GüvenliWeb Oyun, 2018b). Özellikle Mavi Balina oyunu ile ortaya çıkan bu tehdidin ciddi olumsuz sonuçları ortaya çıkmıştır. Sadece Türkiye'de bu oyunun 100'den fazla kurbanı olduğu ifade edilmektedir (BBC, 2017a). Mavi Balina oyununda yönetici konumunda olan bir kişinin gençlerin kişisel bilgilerini ele geçirdiği ve daha sonraki aşamalarda şantaj yaparak kişileri oyunda kalmaya zorladığı ifade edilmektedir. Bu oyunun 50 aşamadan oluştuğu ve oyunun her aşamasında kişilere çeşitli görevler verildiği belirtilmektedir. Oyunun en son aşamasında genellikle intihar etme görevi ile gençlerin hayatlarını sonlandırmalarına neden olduğu anlaşılmaktadır. BBC'nin bu konuyla ilgili haberine göre, Mavi Balina oyununa katılmış ama sonradan kurtulmuş olan Hindistanlı gençlerden biri oyuna dahil olma sürecinin WhatsApp mesajlaşma programı üzerinden kendisine yollanan bir bağlantı adresine tıklaması ile başladığını ifade etmiştir. Hindistanlı kurban ifadesinde Mavi Balina oyununun telefona indirilen bir uygulama olmadığını oyunun, kişilerin bir yönetici tarafından bir bağlantı aracılığıyla yönlendirilmesiyle oynandığını belirtiyor. Ayrıca burada esas önemli olanın yönetici tarafından verilen görevlerin gece yarısından sonra saat 02:00'de gerçekleştirilmesinin istenmesi ve ilk birkaç gün süresince istenen görevlerin de kişilerin kişisel bilgilerinin ve fotoğraflarının yönetici ile paylaşılması olduğudur. BBC'nin haberinde ayrıca Mavi balina oyunu içinde bulunan gençlerin bu süreçte genellikle insanlarla konuşmayı bıraktıkları ve odalarına kapandıkları, oyundan çok kez çıkmak istemelerine rağmen başarılı olamadıkları ifade edilmektedir. Benzer bir şekilde "Mariam" oyunu da Mariam isimli bir kızın kaybolması ve evine tekrar dönebilmek için oyunu oynayan kişiden yardım talebinde bulunması senaryosu ile gençlere yönelik tehdit içermektedir. Bu sözde oyun da gençlerden kişisel bilgilerini toplamakta ve gençler için özellikle mahremiyet noktasında ciddi tehlikeler ortaya koymaktadır. Bu sözde oyun ortamlarının ortak noktasının, hedef kitlesinin çocuklardan ve gençlerden oluşması ile çocukların ve gençlerin psikolojileri üzerindeki olumsuz etkileri olduğu anlaşılmaktadır (GüvenliWeb Oyun, 2018b). Bu bağlamda çocukların ve gençlerin İnterneti saplantılı ve bağımlı bir şekilde kullanmalarına sebep olabilecek dijital oyunlar ile İnternet bağımlılığı konularında çocukların erken yaşlardan itibaren bilgilendirilmeleri, bu bilinçlendirme sürecine ebeveynlerin de dahil edilmeleri önerilebilir (Çelik, Çelen & Seferoğlu, 2014).

Çocuklar ve gençler için bir diğer tehlike de reklamlardır. Birçok sosyal ağ sitesinde çoklu reklamlar yer almaktadır. Reklamların bir kısmı başlık çubuğu (banner) üzerindeki sabit reklamlar bir kısmı da davranışsal reklamlar olarak ortaya çıkmaktadır. Davranışsal reklamlar kullanıcının İnternet üzerindeki hareketlerini, arama

davranışlarını ve demografik bilgilerini kaydederek kişiye özel sunulan reklamları içermektedir. Bu reklamların ise satış amacından öte gençler üzerinde manipülasyon etkisinden söz edilmektedir (O'Keeffe vd., 2011).

İnternette pornografik öğe, düşmanlık, öfke ve şiddet içerikli yasa dışı öğelerin yer alması da bir diğer tehlike olarak ortaya çıkmaktadır. Gençler ve çocuklar istemsiz olarak bu öğelere maruz kalabilmektedirler (Canbek & Sağıroğlu, 2007). Bu unsurlar çocukların erişim sağladığı sitelerin reklam alanlarında, izledikleri bir videoda, bir dijital oyunda, tanımadıkları kişiler ya da kendi akranları tarafından gönderilen bağlantılar üzerinde bulunabilmektedir. Çocuklar ve gençler bu içeriklerle bazen bir video ya da oyun içerisinde karşılaşmakta, bazen de istemsiz olarak tıkladıkları bir bağlantı içerisinde bu içeriklere maruz kalabilmektedirler.

Sosyal ağ ortamlarında karşılaşılan bu sanal zorbalık örnekleri gençlerde depresyon, endişe, şiddetli yalnızlık duygu durumu veya trajedik olarak intihar gibi sonuçlarla neticelenebilmektedir (Hinduja & Patchin, 2010; O'Keeffe vd., 2011). Bu yüzden sosyal ağlardaki tehlikelerden korunma yollarının bilinmesi hem gençler hem de onlardan birinci derecede sorumlu olan ebeveynler ve öğretmenler için çok önemli bir durum olarak değerlendirilmektedir.

Sosyal Ağlardaki Tehlikelerden Korunma Yolları/Önerileri

Sosyal ağ ortamları çocuklar ve gençler için hem eğlence hem de iletişim olanağı sunan, her geçen gün yaygınlaşan ve etkisini giderek daha çok hissettiğimiz sanal ortamlardır. Bu yeni sanal ortamlar gençlerin sosyalleşme ve öğrenme gibi durumlarında değişikliğe neden olmakla beraber yeni birçok hususu da beraberinde getirmektedir. Gelişi güzel olarak düzenlenen İnternet etkinlikleri çocukları ve gençleri dolandırıcılar için hedef haline getirebilmektedir. Bu yüzden ebeveynler ve öğretmenler olarak doğası gereği bu ortamların çocuklar ve gençler için her zaman sağlıklı ortamlar olmadığının farkında olunmalıdır (O'Keeffe vd., 2011). Sanal ortamlarda gençlerin karşılaştıkları sorunlarla ilgili olarak alanyazında çeşitli önlemlerin alınması da önerilmektedir. Örneğin Yiğit ve Seferoğlu (2017) sanal zorbalıkla başa çıkmada hem okul içi hem de aile içi müdahalelerin önemli sonuçları olabileceğini belirtmektedir. Gençleri ve çocukları bu ortamlarda yaşanabilecek sorunlardan korumak için ebeveynlerin ve eğitim kurumlarının ortak çalışması bu bağlamda önemli görülmektedir (Ceyhan, Demiryürek & Kandemir, 2015). Başka bir ifadeyle sanal zorbalıkla etkin bir şekilde mücadele edilebilmesi için de mücadelenin "okul-öğrenci ve aile" üçgeninde gerçekleştirilmesi gerekmektedir (Akca, 2017b).

Bu süreçte ayrıca İnternet erişiminin ve kullanımının artmasıyla birlikte İnternet ortamındaki riskleri önleme sürecinin dengeli olarak yürütülmesi gerekliliği gündeme gelmektedir. İnternet ortamındaki riskleri azaltırken uygulanabilecek yöntemler, genç kullanıcıların İnternetin sunduğu fırsatlardan faydalanabilme potansiyelini düşürmemelidir. Bu bağlamda İnternet kullanıcısı olan çocukların ve gençlerin belirli durumlarda mevcut risklerle mücadele edebilmeleri ve olası riskleri önleyebilmeleri için sürekli yapılacak bilinçlendirme çalışmalarının önemli olduğu söylenebilir (Çelen, Çelik & Seferoğlu, 2011).

Bu aşamada öncelikli olarak bilgi güvenliği kavramının önemi ortaya çıkmaktadır. Günümüz bilgi ve iletişim teknolojileri çağında gençlerin, öğretmenlerin ve ebeveynlerin İnternet ve sosyal ağ ortamlarındaki güvenlik sorunlarını aşabilmelerinde bilgi güvenliği farkındalıkları önem taşımaktadır. BTK İnternet Daire Başkanlığı (2018) bilgi güvenliğini "bir varlık türü olarak kabul edilen bilginin başkaları tarafından izinsiz ya da etkisiz bir şekilde erişilmesini, başkalarına verilmesini veya bu bilgilere kullanılamayacak şekilde hasar verilmesini önlemek ve bu varlık türünü korumak" olarak tanımlamıştır. Gençlerin, ebeveynlerin ve öğretmenlerin bilgi güvenliği konusundaki farkındalık düzeylerinin artırılması onların olası risk ve güvenlik tehditlerine karşı güvenliklerini sağlamalarında etkili olacak temel etkenlerden biri olarak değerlendirilebilir.

Bu bölümde sosyal ağ ortamlarının en yoğun kitlesini oluşturan gençlere yönelik olarak bu ortamlardaki olası risk ve tehditlerden korunabilmeleri için çeşitli öneriler sunulmaktadır. Ayrıca çocuklar ve gençler için hem rol model olmada hem de rehberlik sağlamada önemli etkileri bulunan ebeveyn ile öğretmenlere, çocuk ve gençlere doğru rehberliği sağlayarak gerekli önlemleri alabilmeleri için öneriler sunulmaktadır.

Genç Kullanıcılar için Öneriler

Gençler, bütün kullanıcılar gibi çevrim-içi ortamları kullanırken çeşitli risk ve tehditlerle karşı karşıya kalabilmektedirler. Gençleri sosyal ağ ortamlarındaki olası risk ve güvenlik tehditlerinden korumaya yönelik olarak, göz önünde bulundurulmasının önemli olduğu düşünülen aşağıdaki önerilerde (Akca, 2017a; BTKİnternet Daire Başkanlığı, 2018; Canbek & Sağıroğlu, 2007; Ceyhan vd., 2015; Güvenli Çocuk, 2018) bulunulabilir:

1. Kişisel bilgisayarlar, mobil telefonlar veya tabletler gibi kişisel cihazların öncelikli güvenliğini sağlamak için işletim sistemleri güncel tutulmalı ve bu cihazlar içerisinde güncel lisanslı antivirüs programları kullanılmalıdır.

2. Sosyal ağ ortamlarında kişisel bilgiler, konum bilgileri, nüfus cüzdanı, ehliyet, pasaport vb. resmi kimlik bilgileri, banka veya kredi kartı bilgileri ile her türlü kişisel kullanıcı adı ve şifre bilgilerinin paylaşılmaması konusunda dikkatli olunmalıdır.
3. Sosyal ağ ortamlarındaki arkadaş listesine sadece günlük hayatta birebir tanınan arkadaşlar eklenmelidir. Sanal ortamda dolandırıcılık amacıyla açılan çok sayıda sahte hesabın olduğu unutulmamalıdır.
4. Tanınmayan kişilere asla güvenilmemelidir. Bu kişilerden gelen teklifler, istekler dikkate alınmamalıdır. Ayrıca bu kişilerden gelen bağlantılara tıklamaktan da kaçınılmalıdır.
5. Yaşça büyük olan kişilerle kesinlikle özel iletişime geçilmemelidir.
6. Şüpheli içeriğe sahip İnternet sitelerine bağlanılmamalıdır.
7. Sosyal ağ ortamlarında ilgi çeken yarışma, ödül veya çekiliş gibi etkinliklere davet eden mesajlardaki yönergelerle ilgili olarak aile bireylerine danışılmadan herhangi bir işlem yapılmamalıdır. Bu kapsamda özellikle kişisel bilgilerin istendiği bir form (başvuru formu, çekiliş formu vb.) doldurulmalıdır.
8. Bilinmeyen kişilerden gelen e-posta mesajı, kısa mesaj, resim ve dosyalar kabul edilmemeli ve açılmamalıdır. Bu mesajlar veya dosyalar virüs içeriyor olabilir veya hoşa gitmeyecek içerikleri olabilir.
9. Kullanılan sosyal ağ ortamı ya da çevrim-içi platform güvenli şekilde kullanılmalıdır. Kullanılan ortamın gizlilik ve güvenlik ayarları "güvenli" konumda tutulmalıdır.
10. Herhangi bir sanal zorbalığa maruz kalındığında bu durum hemen güvenilen bir yetişkinle paylaşılmalıdır.
11. İnternet ortamında yaşanan tüm olumsuzluklara (taciz veya tehdit mesajları gibi) aile bireylerine danışılmadan herhangi bir tepki verilmemelidir.
12. Başkasını rahatsız edecek içeriklerin yayılmasına aracılık edilmemelidir.
13. İnternet ortamında kullanılan şifrelerin güvenliğine dikkat edilmelidir. Bu amaçla güçlü şifreler tercih edilmelidir.

Genç Kullanıcıların Ebeveynlerine Yönelik Uyarılar/Öneriler

Küçük yaşta çocukları olan ebeveynler için çevrim-içi ortamların kullanımıyla ilgili olarak aşağıdaki önerilerde (Akca, 2017b; BBC, 2017b; BTK İnternet Daire Başkanlığı, 2018; O'Keeffe vd., 2011; Sırakaya & Seferoğlu, 2018) bulunulabilir:

1. Çocukların İnternet kullanım süresine kısıtlama getirilmelidir. Özellikle küçük yaşlardaki çocukların anne ve babaları tarafından belirlenmiş olan zaman dilimlerinde ve belirlenmiş süre kadar İnternet'e erişim sağlamalarına izin verilmelidir. Böylece çocuğun öncelikli olarak İnternet erişiminin süre kontrolü sağlanmalı ve İnternet bağımlılığının önüne geçilmelidir.
2. Çocuklara yönelik tamamen yasaklayıcı, kısıtlayıcı önlemler almak yerine onların bilinçli kullanım ve içerik yönetimine teşvik edilmesinin önemli olduğu unutulmamalıdır.
3. Çocukların bilgisayar, cep telefonu ve diğer teknolojik araçları kullanımıyla ilgili olarak birtakım kurallar belirlenmelidir. Özellikle çocukların erişebilecekleri web siteleri konusunda kurallar konulması ve hangi web sitelerinin çocuklar açısından uygun olup olmadığı kararının çocukla paylaşılması önemlidir. Ayrıca uygun ve güvenli olduğuna karar verilen İnternet sitelerinin adreslerinin belirlenerek İnternet tarayıcısının "Sık Kullanılanlar" bölümüne kaydedilmesi sağlanabilir.
4. Teknolojik aletlere ve İnternet'teki etkinliklere erişim konusundaki kurallar çocuklarla tartışılarak ortak nihai kararlar doğrultusunda oluşturulmalıdır.
5. Çocukların İnternet sitelerindeki gezintileri takip edilmelidir. Ayrıca çocukların ebeveynlerin onayını almadan erişimde bulunduğu içerikler incelenmelidir.
6. Çocukların mobil cihaz(lar)ına indirdiği uygulamalar belirli aralıklarla kontrol edilerek takip edilmelidir.
7. Çocukların İnternet'e, ebeveynlerin gözetiminde evdeki ortak bir alanda girmesi sağlanmalıdır. Böylece çocuğun İnternet'teki dolaşımı esnasında yalnız kalmaması sağlanarak sürekli bir gözetimin yapılması kolaylaşacaktır.
8. Çocukların erişmek istediği web sitelerinin ya da sosyal ağ ortamlarının incelenerek çocuğun yaşına uygunluğu konusunda gerekli değerlendirmeler yapılmalıdır.

9. Çocukların belirlenen etkinlikler doğrultusunda anne ve babasıyla İnternet ortamında beraber vakit geçirmesi sağlanmalıdır. Bu esnada da aktif kullanım içerisindeyken çocukla olası tehlikeler ve dikkat edilmesi gerekenler hakkında konuşulmalıdır. Böylece çocuğa nasihat vermenin ötesinde bir diyalog kurma şansı elde edilebilir. Bu diyalog süresince çocuk, ebeveynlerinin İnternetteki eylemlerini takip ederken yapılan öğütlerin hedefe ulaşması kolaylaşacaktır.
10. Çocukların İnternet'e eriştiği tüm cihazlarda ebeveyn kontrol ve koruma sistemi yazılımlarının kullanımına özen gösterilmelidir.
11. Filtreli alternatif bir İnternet erişim hizmeti sunan Güvenli İnternet Hizmeti (http://www.guvenlinet.org/) konusunda bilgi sahibi olunmalıdır. Güvenli İnternet Hizmeti İnternet servis sağlayıcıları tarafından sunulan merkezi bir filtreleme sistemi olarak 2011 yılından itibaren sunulmaktadır. Bu kapsamda aile ve çocuk profili gibi seçenekler bulunmaktadır.
12. Okuldaki öğretmenlerle ve diğer öğrencilerin ebeveynleri ile sürekli iletişim içerisinde olup gençler arasındaki yeni eğilimler ve/veya yaşanan sıkıntılı durumlardan haberdar olunmalıdır.
13. Çocuklara, şifrelerini ve kişisel diğer bilgilerini kimseyle paylaşmamaları gerektiği konusunda bilgi verilmelidir.
14. Çocuklara sosyal ağ ortamlarındaki paylaşımları konusunda uyarılar yapılmalıdır.
15. Çocuklarda bilgi mahremiyeti konusunda farkındalık oluşturulmalıdır. Bu bağlamda kişisel bilgileri başkaları ile paylaşmanın yol olacağı olası durumlar hakkında bilgi verilmeli ve bu tür durumlarla ilgili örnekler paylaşılmalıdır.
16. Okul sınırları içerisindeki bilgisayar veya İnternet erişimi konusunda öğretmenlerle ve okul yönetimiyle işbirliği yapılarak, bu konuda çeşitli kuralların konulması sağlanmalıdır.
17. Olumsuz içeriklerle karşılaşıldığında bu durum Bilgi Teknolojileri ve İletişim Kurumu tarafından oluşturulmuş ihbar hattı (https://www.ihbarweb.org.tr/) ile paylaşılmalıdır.
18. Çocukların akıllı telefon veya tablet gibi mobil cihazlarındaki ebeveyn kontrol seçenekleri hakkında bilgi sahibi olunmalı ve bu özellikler çocukların birebir erişim sağladıkları tüm mobil cihazlarda etkin hale getirilmelidir. Örneğin, Apple marka telefonlarda Web içerikleri engelleme, oyun merkezini sınırlama, uygunsuz içerikleri ve içerik derecelendirmelerini engelleme veya alım işlemlerini engelleme gibi farklı seçeneklerle ebeveyn kontrolüne yardımcı araçlar geliştirilmiştir (Apple, 2018b).
19. Sosyal ağ ortamlarının kullanımı konusunda çocuklara rol model olunmalıdır.
20. Ebeveynler tarafından sosyal ağ ortamlarında çocukların mahremiyetini göz ardı eden paylaşımlar yapılmamalıdır.
21. Çocuklarla güçlü bir iletişim kurulmalıdır. Çocuklara yaşadıkları olumsuz durumları paylaşabilecekleri bir güven ortamı sağlanmalıdır.
22. Çocukların sosyal ağlardaki sanal zorbalık olayları hakkında bilgi sahibi olmaları sağlanmalıdır. Sanal zorbalığa maruz kalan bazı çocukların genellikle yaşadıkları olayın sanal zorbalık olduğunun farkında olmamaları sebebiyle gerekli müdahaleleri yapamadıkları ve ihtiyaç duydukları yardımı alamadıkları unutulmamalıdır.
23. Sanal zorbalık belirtileriyle ilgili olarak bir farkındalık oluşturulmalıdır. Gençlerin ve çocukların yaşadıkları sanal zorbalık durumları bazı belirtilerle ortaya çıkabilmektedir (Şekil 2). Bu yüzden çocukların davranışları gözlenerek ruh halinde veya psikolojik durumunda oluşabilecek bir değişiklikle ilgili olarak farkındalık sahibi olunmalıdır. Böylece olası ciddi bir değişiklikte çocuğun çevresindekilerle görüşüp onun İnternet ortamındaki eylemleri daha dikkatli gözlenebilir.

Şekil 2. Sanal/Siber Zorbalığa Uğrayan Gençlerde ve Çocuklarda Ortaya Çıkan Belirtiler (Megan Meier Foundation, 2018)

Genç Kullanıcıların Öğretmenlerine Yönelik Uyarılar/Öneriler

Öğretmenler okulda çeşitli yaş ve gelişimleri açısından farklı düzeyde olan çocuklarla çalışmaktadırlar. Savunmasız durumdaki bu çocukların öğretmen desteğine her zaman ihtiyaçları olacaktır. Öğretmenlerin sanal zorbalığın ne olduğu, öğrenciler üzerinde ortaya çıkabilecek sonuçlarının neler olabileceği ve öğrencilerin karşılaşabileceği zorbalık olaylarına karşı dikkat edilmesi gerekenler hakkında fikir sahibi olmaları önemlidir (Ayas & Horzum, 2011). Bu bağlamda küçük yaştaki bu çocukların ve gençlerin çevrim-içi ortamları kullanımlarıyla ilgili olarak öğretmenlere yönelik aşağıdaki önerilerde (National Commission for Protection of Child Rights, 2018) bulunulabilir:

1. Öğrencilerin sınıf içindeki hareketleri dikkatle takip edilmeli ve öğrencilerde oluşabilecek değişikliklerle ilgili farkındalık geliştirilmelidir. Örneğin, başarılı bir öğrencinin derse yönelik azalan ilgisi, sınav notlarındaki düşüşler, davranışlarında gözlenebilecek huzursuzluklar vb. gibi durumlar takibi yapılması gereken durumlar olarak değerlendirilmelidir. Bu tür durumlarda problemin tespiti için ya da problem tespiti yapılan durumlarda da problemi çözmek amacıyla ilgili kişilerle işbirliği içerisinde gerekli önlemler alınmalıdır.
2. Ebeveynlerle işbirliği içinde bulunulmalıdır. Bu amaçla kullanmak üzere iletişim grupları kurulmalıdır.
3. Öğrenciler arasında oluşan "Mavi Balina", "Mariam" veya "Momo" gibi sözde oyun akımlarından haberdar olunmalı ve bu güncel tehlikeler konusunda ebeveynler bilgilendirilmelidir.
4. Öğrencilere İnternet okuryazarlığı temel becerisini kazandırmaya yönelik etkinlikler düzenlenmelidir.
5. Öğrenciler sosyal ağ ortamlarındaki olası risk ve güvenlik tehditleri konusunda bilgilendirilmeli ve zaman zaman bu bilgiler güncellenmelidir.
6. Ebeveynlerin İnternet dünyasının ve sosyal ağ ortamlarının ortaya çıkardığı olası risk ve güvenlik tehditleri konusundaki farkındalığını artırıcı etkinlikler düzenlenmelidir.
7. Öğrencilerle ilgili olarak gözlenen herhangi bir tehdit veya tehlike durumunda okul yönetimi ile derhal iletişime geçilmelidir.
8. Sınıf içerisinde içine kapanık, anti-sosyal davranışlar sergilediği gözlenen öğrencilerle birebir iletişim kurulmalıdır. Böylece bu öğrencilerin normal koşullarda farkına varılmayacak sıkıntılar yaşanmasının önüne geçilebilir.

Sosyal Ağlardaki Tehlikelere Karşı Geliştirilen Teknolojilere Örnekler

Gelişen bilgi ve iletişim teknolojilerinin bir ürünü olan sosyal ağ ortamlarında ortaya çıkan risk ve tehditlere karşı yine teknolojik gelişmelerle çeşitli tepkiler ve korunma yolları geliştirilmektedir. Bu tür teknolojilere Microsoft tarafından yapay zekâ ve makine öğrenmesi teknolojileri ile geliştirilmiş yüz tanıma sistemi ile çalışan Fotoğraf Eşleştirme yazılımı (Magid, 2018) örnek olarak verilebilir. Bu yazılım ile çocuk pornografisinin önüne geçmek için çocukların çıplak ya da cinsel içerikli fotoğraflarının kullanımının önlenmesi amaçlanmıştır. Geliştirilen yazılım ile, Facebook'a yüklendiğinde çocuk istismarı olduğu bilinmeyen çıplak çocuk fotoları taranmaktadır. Bu tarama sürecinde sorunlu olduğu düşünülenler önceliklendirilerek bir sıraya yerleştirilmektedir. Daha sonra bunlar şirketin konuyla ilgili uzmanları tarafından değerlendirilerek çocuk istismarıyla ilişkili görseller Facebook hesaplarından kaldırılmaktadır. Bu tarama işlemleri sayesinde Facebook ortamında toplam 8,7 milyon içeriğin kaldırıldığı belirtilmektedir. Bu içeriklerden %99'unun ise herhangi bir kullanıcı tarafından raporlanmasına gerek kalmadan tamamen bu teknolojinin kendi tarama çalışması sonucunda kaldırıldığı ileri sürülmektedir (Magid, 2018).

Benzer şekilde yapay zekâ teknolojisi ile çalışan fakat daha çok bireysel hizmet sunan bir diğer uygulama da Megan Meier vakfı, Identity Guard firması ve IBM şirketi işbirliğinde tarafından geliştirilmiştir. Megan Meier çocuğunu sanal zorbalığın neden olduğu bir intihar vakası sonucunda kaybetmiş bir annedir. Megan Meier vakfı ise bu olaydan sonra sanal zorbalıkla mücadele etmek üzere kurulmuştur. Bu vakıf tarafından öğrencileri, eğitimcileri ve ebeveynleri hedef alan birçok konferans, çalıştay ve eğitimler düzenlenmektedir. Vakıf bu konuda yaşanmışlığı olan ailelere ve bireylere ücretsiz danışmanlık hizmeti de sunmaktadır. Identity Guard firması ise kimlik hırsızlığına karşı bireysel antivirüs gibi yazılım hizmetleri sunan bir firmadır. Identity Guard firmasının Meier vakfına başlattığı danışmanlık hizmeti sonrasında iki kuruluş IBM'in desteğini alarak yeni bir teknoloji geliştirmişlerdir. Bu teknoloji ile bireylere gönderilen ve bireyler tarafından gönderilen mesajlar kategorize edilmekte ve karmaşık algoritmalar ile olası siber saldırı durumları tanımlanmaktadır. Bu yazılım tarafından siber zorbalık ihtimali algılandığında, bireyin ebeveynlerine tetikleyici bir uyarı gönderimi yapılmaktadır (Meier, 2018). Bu bağlamda teknolojinin kötü olmadığı ancak nasıl kullanıldığının önemli olduğu söylenebilir. Bu kuruluşların amacı da ebeveynleri, onların korkulu rüyaları haline gelen sanal dünyalar hakkında bilgilendirirken, çocuklarının da güvenli bir şekilde sanal dünyada yer almasını sağlamaktır.

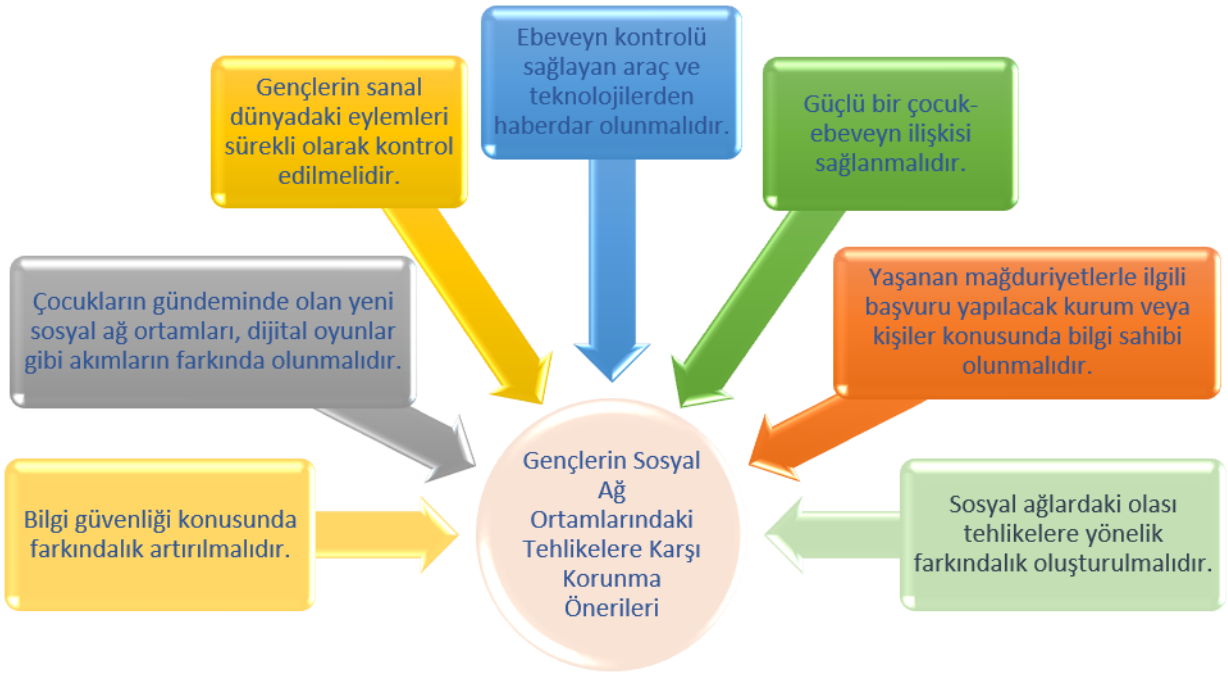
Güvenli İnternet Hizmeti ise Türkiye'de İnternet sağlayıcıları tarafından sunulan ve bir filtreleme sistemi ile İnternetteki zararlı içeriklere erişimi kontrol eden bir alt yapıdır (BTK, 2018). Bu hizmet herhangi bir kurulum gerektirmeyen ve bir SMS mesajı ile aboneliğin gerçekleştirilebildiği ücretsiz bir hizmettir. Bu hizmetin, "çocuk profili" ve "aile profili" olmak üzere iki tipi bulunmaktadır. Çocuk profili ile erişilebilecek siteler uzman kontrollerinden geçmiş belirli kriterlere göre onaylanmış siteler olarak ifade edilmektedir. Çocukların tanımadıkları kişilerle iletişime geçebilecekleri sohbet veya sosyal medya sitelerine erişimi engellenmektedir. Dijital oyun bağlamında ise sadece sabit içerikli oyunlar oynanabilmekte çevrim-içi olarak farklı kişilerle iletişim ağı ve dinamik görevler içeren oyunlara erişim sağlanamamaktadır. Aile profili ise çocuk profiline göre nispeten biraz daha esnek olabilecek, ebeveyn kontrolü ile sohbet, sosyal medya veya oyun sitelerine erişimin açılıp kapatabileceği şekilde yapılandırılmış bir profildir. Bu profilde müstehcenlik, şiddet, ırkçılık, kumar gibi yasadışı ve zararlı içerik barındırabileceği tespit edilmiş, Sağlık bakanlığınca zararlı olduğu açıklanan ürünlerin satışının yapıldığı sitelere erişim engellenmektedir. Başvuru esnasında çocuk ya da aile profillerinden biri seçilebilmektedir. Daha sonra istenildiğinde profil değişikliği yapılabilmekte veya profil sistemi tamamen devre dışı bırakılabilmektedir.

Sanal ortamda karşılaşılan sanal zorbalık durumlarına ilişkin çocukların ve gençlerin mağduriyetlerini önlemek amacıyla geliştirilen çeşitli mobil uygulamalar da bulunmaktadır. Bu uygulamalardan biri ücretsiz olarak erişilebilen "Bully Button" uygulamasıdır. IOS tabanlı bu mobil uygulama aracılığıyla sanal ortamda bir sanal zorbalık eylemine maruz kalan çocuklar bu eylemi kaydederek ebeveynleri ya da okul yöneticileri ile anında paylaşabilmektedir (Apple, 2018a). Çocukların güvenli İnternet kullanımını sağlamaya yönelik bir diğer mobil tabanlı uygulama örneği ise "Net Nanny" uygulamasıdır (Net Nanny, 2018). Android tabanlı bu uygulama ile ebeveynlerin çocukların İnternet ortamındaki etkinliklerini filtrelemeleri, izlemeleri ve kontrol etmeleri kolaylaşabilmektedir.

Günümüzde değişen bilgi ve iletişim teknolojileri, yaygınlaşan mobil cihazlardan İnternet erişimi, erken yaşta İnternet ile tanışma, sosyal ağ ortamlarında artan genç kullanıcı kitlesi ve sözde dijital oyun akımı ile ortaya çıkan sanal platformlar odaklanılması gereken birçok risk ve tehlikeyi meydana getirmektedir. Sanal zorbalık bu değişimin meydana getirdiği en önemli risk ve tehditlerden biri olarak gündeme gelmektedir. Özellikle de gençler ve çocuklar için ciddi riskler ve tehlikeler barındıran bu konu ile mücadelede yine teknoloji temelli yaklaşımlar kullanılmaya başlanmıştır. Yapay zekâ ve makine öğrenmesi gibi teknolojinin gözde konuları ile alternatif çözümler üretilmektedir. Bu bölümde sanal zorbalıkla mücadele sürecinde geliştirilen teknolojiler konusunda bir fikir oluşturmak için bazı örnek çalışmalar paylaşılmıştır. Böylece yapılabilecekler konusunda bir farkındalık oluşturulabileceği düşünülmüştür.

SONUÇ

Gelişen İnternet dünyası bir yandan günlük işlerimizin parmaklarımızın ucuyla çok hızlı bir şekilde halledilmesi, bilgiye hızlı erişim, iletişimde sınırsız imkânlar gibi avantajlar sunarken öte yandan da bu sınırsız dünya içerisindeki birçok risk ve güvenlik tehdidiyle karşı karşıya kalmamıza yol açmaktadır. Özellikle teknoloji çağının ortasında doğan ve Z nesli olarak bilinen genç grubu, yoğun bir teknoloji ve İnternet kullanımına maruz kalmaktadır. Bu nesil sosyal ağ ortamlarının da en aktif kullanıcı kitlesi olarak gündeme gelmektedir. Gençler sosyal ağ ortamlarını hem mevcut arkadaşlarıyla iletişim için hem de ilgi alanlarına göre farklı gruplara dâhil olarak tanımadıkları kişilerle iletişim için kullanmaktadır. Burada önemli olan gençlerde, bu tanımadıkları ortamlardaki risklere karşı kendilerini koruyabilecek seviyede farkındalıklarının oluşturulmasıdır. Eğer gençler, çevrim-içi ortamları kullanırken karşı karşıya kalabilecekleri risk ve tehditler hakkında bilgi sahibi olurlarsa bu risk ve tehlikelerden kendilerini tamamen veya en az düzeyde etkilenecek şekilde koruyabilirler. Bu süreçte ebeveyn ve öğretmenlere büyük sorumluluklar düşmektedir (Bkz. Şekil 3).



Şekil 3. Gençlerin Sosyal Ağ Ortamlardaki Tehlikelere Karşı Farkındalıklarının Artırılması ve Korunmasına Yönelik Öneriler

Bilgi güvenliği farkındalığı sosyal ağlarda yer alan daha geniş kapsamlı olarak da İnternet dünyasında yer alan herkes için en önemli konulardan birisidir. Bu konu güçlü şifre kullanımı, kişisel bilgilerin bilinmeyen kişilerle paylaşılmaması, güvenli hesap ayarları, gizlilik ve erişilebilirlik gibi konuların çatısını oluşturmaktadır. Sosyal ağlardaki tehlikelere karşı gerekli tedbirleri oluşturabilmek için temel bilgi güvenliği konularına hâkim olmak önemlidir. Bu bağlamda ebeveynler ve öğretmenler gençlerin çevrim-içi ortamları kullanmalarıyla ilgili farkındalıklarını artırarak onlara destek olmalıdırlar. Ayrıca çevrim-içi ortamları kullanmayla ilgili olarak onları gerekli bilgilerle donatmalıdırlar. Öte yandan gençlerin çevrim-içi ortamları kullanımları ve bu ortamda gerçekleştirdikleri eylemler takip edilmelidir. Böylece herhangi bir risk ve güvenlik tehdidiyle ilgili olarak, risk ve/veya tehdit amacına ulaşamadan müdahale şansı olabilecektir. Bu da her şeyden önce başarılı ve huzurlu bir toplumun ön koşulu olarak değerlendirilebilir.

KAYNAKLAR

Akca, E. B. (2017a). *Siber zorbalık nedir? Nasıl mücadele edilir? Gençler için eğitici kitapçık.* [Çevrim-içi: https://images.samsung.com/is/content/samsung/p5/tr/sosyal-sorumluluk/siber-zorba-olma/Siber_Zorba_Olma_Cocuk_Genc.pdf, Erişim tarihi: 05.10.2018.]

Akca, E. B. (2017b). *Siber zorbalık nedir? Nasıl mücadele edilir? Yetişkinler için eğitici kitapçık*. [Çevrim-içi: https://images.samsung.com/is/content/samsung/p5/tr/sosyal-sorumluluk/siber-zorba-olma/Siber_Zorba_Olma_Yetiskin.pdf, Erişim tarihi: 05.10.2018.]

Apple (2018a). Bully button for parents and kids. [Çevrim-içi: https://itunes.apple.com/us/app/bully-button-for-parents-and-kids/id1265818101?mt=8, Erişim Tarihi: 27.10.2018]

Apple (2018b). Çocuğunuzun iPhone, iPad veya İpod touch'ında ebeveyn denetimlerini kullanma. [Çevrim-içi: https://support.apple.com/tr-tr/HT201304, Erişim tarihi: 27.10.2018.]

Ayas, T., & Horzum, M.B. (2011). Exploring the teachers' cyber bullying perception in terms of various variables. *International Online Journal of Educational Sciences*, *3*(2), 619-640.

BBC (2017a). *İntihar oyunu Mavi Balina'dan kurtulanlar anlatıyor*. [Çevrim-içi: https://www.bbc.com/turkce/41281200, Erişim tarihi: 23.10.2018.]

BBC (2017b). *UNİCEF'ten anne babalara tavsiyeler: Çocuklarınızı intihar oyunu Mavi Balina'dan nasıl korursunuz?* [Çevrim-içi: http://www.bbc.com/turkce/haberler-41350844, Erişim tarihi: 25.04.2018.]

BTK (2018). *Güvenli İnternet hizmeti*. [Çevrim-içi: http://www.guvenlinet.org/guvenli-internet-hizmeti, Erişim tarihi: 23.10.2018.]

BTK İnternet Daire Başkanlığı (2018). *Bilgi teknolojileri ve İnternetin bilinçli, güvenli kullanımı.* [Çevrim-içi: http://www.guvenliweb.org.tr/dokuman-detay/bilgi-teknolojileri-ve-internetin-bilincli-guvenli-kullanimi-kitabi, Erişim tarihi: 15.10.2018.]

Canbek, G., & Sağıroğlu, Ş. (2007). Çocukların ve gençlerin bilgisayar ve internet güvenliği. *Politeknik Dergisi, 10*(1), 33-39. [Çevrim-içi: http://dergipark.gov.tr/download/article-file/384608, Erişim tarihi: 05.10.2018.]

Ceyhan, E. B., Demiryürek, E., & Kandemir, B. (2015). Sosyal ağlarda güncel güvenlik riskleri ve korunma yöntemleri. *Uluslar arası Bilgi Güvenliği Mühendisliği Dergisi, 1*(1), 1-10.

Cohen-Almagor, R. (2018). Social responsibility on the Internet: Addressing the challenge of cyberbullying. *Aggression and Violent Behavior*, 39, 42-52.

Çağıltay, K. (2017). *İnsan-Bilgisayar etkileşimi ve kullanılabilirlik mühendisliği*. Ankara: Seçkin Yayıncılık.

Çelen, F. K., Çelik, A., & Seferoğlu, S. S. (2017). *Çevrimiçi ortamlarda çocukları ve gençleri bekleyen riskler: Sanal ortam yalnızlığı üzerine bir değerlendirme*. 11th International Computer & Instructional Technologies Symposium (ICITS-2017). May 24-26, 2017, İnönü University, Malatya, Turkey.

Çelen, F. K., Çelik, A., & Seferoğlu, S. S. (2011). Çocukların İnternet kullanımları ve onları bekleyen çevrim-içi riskler. *XIII. Akademik Bilişim Konferansı (AB11) Bildirileri*, 645-652. İnönü Üniversitesi, Malatya. [Çevrim-içi: http://yunus.hacettepe.edu.tr/~sadi/yayin/AB11_Celen-Celik_Seferoglu_Cocuklar-Internet-Riskler.pdf, Erişim tarihi: 05.10.2018.]

Çelen, F. K., & Seferoğlu, S. S. (2016). Bilgi ve iletişim teknolojilerinin kullanımı ve etik olmayan davranışlar: Sorunlar, araştırmalar ve değerlendirmeler. *Bilgisayar ve Eğitim Araştırmaları Dergisi [Journal of Computer and Education Research], 4*(8), 124-151.

Çelik, A., Çelen, F. K., & Seferoğlu, S. S. (2014). Ortaokul öğrencilerinin İnternet bağımlılık düzeylerinin çeşitli değişkenler açısından incelenmesi. *XVI. Akademik Bilişim Konferansı (AB14) Bildirileri*, 373-382. Mersin Üniversitesi, Mersin. [Çevrim-içi: http://yunus.hacettepe.edu.tr/~sadi/yayin/AB14_Celik-Celen-Seferoglu_InternetBagimliligi.pdf, Erişim tarihi: 05.10.2018.]

Durak, H. (2016). İlköğretim ve ortaöğretim öğrencilerinin Facebook kullanımında dijital kimliklerinin incelenmesi üzerine bir araştırma. *Uluslararası Sosyal Araştırmalar Dergisi, 9*(44), 1-16.

Durak, H., & Seferoğlu, S. S. (2016a). Siber zorbalık: Eski bir toplumsal sorunla ilgili yeni tanımlamalar, bakışlar, değerlendirmeler. A. G. Baran & M. Çakır (Ed.), içinde *İnter-disipliner yaklaşımla gençliğin umudu toplumun beklentileri* (ss. 167-187). Hacettepe Üniversitesi Yayınları, Ankara.

Durak, H., & Seferoğlu, S. S. (2016b). Türkiye'de sosyal medya okuryazarlığı ve sosyal ağ kullanım örüntülerinin incelenmesi. *Uluslararası Sosyal Araştırmalar Dergisi*, *9*(46), 1-10.

Fallows, D. (2004). The Internet and daily life. Pew Internet & Amercan Life Project, Washington, D.C. [Çevrim-içi: http://www.pewinternet.org/2004/08/11/the-internet-and-daily-life/, Erişim Tarihi: 21.10.2018.]

Güvenli Çocuk (2018). *Kişisel verileri koru*. [Çevrim-içi: http://www.guvenlicocuk.org.tr/siber-cocuk/kisisel-verilerini-koru, Erişim tarihi: 29.09.2018.]

GüvenliWeb (2017). *Siber zorbalık*. [Çevrim-içi: http://www.guvenliweb.org.tr/dokuman-detay/siber-zorbalik, Erişim tarihi: 29.09.2018.]

GüvenliWeb Oyun (2018a). Dijital oyunlar ve bireyler üzerindeki etkileri. [Çevrim-içi: http://oyun.guvenliweb.org.tr/blog-detay/dijital-oyunlar-ve-bireyler-uzerindeki-etkileri, Erişim Tarihi: 28.10.2018.]

GüvenliWeb Oyun (2018b). *Sözde oyun akımına dikkat.* [Çevrim-içi: http://oyun.guvenliweb.org.tr/haber-detay/sozde-oyun-akimina-dikkat, Erişim tarihi: 28.10.2018.]

Hinduja, S., & Patchin, J. W. (2010). Bullying, cyberbullying, and suicide. *Archives of Suicide Research*, 14, 206-221. [Çevrim-içi: https://pdfs.semanticscholar.org/7a31/16377b5654dc1f8362dee85b7845f07b5850.pdf, Erişim tarihi: 13.10.2018.]

Ito, M., Horst, H., Bittani, M., Boyd, D., Herr-Stephenson, B., Lange, P.G., et. al. (2008). *Living and learning with new media: Summary of findings from the digital youth project*. The John D. and Catherine T. MacArthur Foundation Reports on Digital Media and Learning. [Çevrim-içi: http://digitalyouth.ischool.berkeley.edu/files/report/digitalyouth-WhitePaper.pdf, Erişim tarihi: 13.10.2018.]

Kaspersky Lab (2016). *10 Forms of cyberbullying.* [Çevrim-içi: https://kids.kaspersky.com/10-forms-of-cyberbullying/https://kids.kaspersky.com/10-forms-of-cyberbullying/, Erişim tarihi: 25.04.2018.]

Kowalski, R.M., Limber, S.P., & McCord, A. (In Press). A developmental approach to cyberbullying: Prevalence and protective factors. *Aggression and Violent Behavior, xxx*(xxxx) xxx-xxx. doi: https://doi.ord/10.1016/j.avb.2018.02.009.

Magid, L. (2018). *Facebook's new tech to counter child sex abuse images.* [Çevrim-içi: https://www.larrysworld.com/facebooks-new-tech-to-counter-child-sex-abuse-images/, Erişim tarihi: 21.10.2018.]

Megan Meier Foundation (2018). *Cyberbullying resources*. [Çevrim-içi: https://meganmeierfoundation.org/cyberbullying/, Erişim tarihi: 27.10.2018.]

Meier, T. (2018). *AI technology helps protect teens from cyberbullying.* [Çevrim-içi: https://www.ibm.com/blogs/client-voices/ai-technology-protect-teens-cyberbullying/, Erişim tarihi: 27.10.2018.]

National Commission for Protection of Child Rights (2018). *Blue whale challenge – What parents need to know.* [Çevrim-içi: http://ncpcr.gov.in/showfile.php?lid=1499, Erişim tarihi: 25.04.2018.]

Net Nanny (2018). *Features.* [Çevrim-içi: https://www.netnanny.com/features/, Erişim Tarihi: 25.10.2018.]

O'Keeffe, G. S., Clarke-Pearson, K., & Council on Communications and Media (2011). The impact of social media on children, adolescents, and families. *Journal of American Academy of Pediatrics, 127*(4), 800-804.

Olweus, D. (1996). *The revised Olweus bully/victim questionnaire*. Mimeo. Bergen, Norway: Research Center for Health Promotion, University of Bergen.

Picazo-Vela, S., Gutierrez-Martinez, I., & Luna-Reyes, L. F. (2012). Understanding risks, benefits, and strategic alternatives of social media applications in the public sector. *Government Information Quarterly*, 29, 504-511.

Samsung (2017). *Siber zorba olma*. [Çevrim-içi: https://www.samsung.com/tr/sosyal-sorumluluk/siber-zorba-olma/, Erişim tarihi: 25.10.2018.]

Sırakaya, M., & Seferoğlu, S.S. (2018). Çocukların çevrim-içi ortamlarda karşılaştıkları riskler ve güvenli internet kullanımı. B. Akkoyunlu, A. İşman ve H. F. Odabaşı (Ed.). *Eğitim teknolojileri okumaları 2018*, (12. Bölüm, ss. 185-202). TOJET ve Sakarya Üniversitesi, Adapazarı. [Çevrim-içi: http://yunus.hacettepe.edu.tr/~sadi/yayin/Kitap_ETO2018_Bolum12_185-202_Cevrimici-Riskler.pdf, Erişim tarihi: 05.10.2018.]

TDK (2018). Güncel Türkçe Sözlük. [Çevrim-içi: http://www.tdk.gov.tr/index.php?option=com_gts , Erişim Tarihi: 23.10.2018.]

TUİK (2013). *06-15 Yaş grubu çocuklarda bilişim teknolojileri kullanımı ve medya*. [Çevrim-içi: http://www.tuik.gov.tr/PreHaberBultenleri.do?id=15866, Erişim Tarihi: 20.10.2018.]

TUİK (2018a). *Son üç ay içinde İnternet kullanan bireylerin İnterneti kişisel kullanma amaçları, 2018*. [Çevrim-içi: http://www.tuik.gov.tr/PreTablo.do?alt_id=1028, Erişim tarihi: 12.10.2018.]

TUİK (2018b). *Son üç ay içinde bireylerin yaş grubuna ve cinsiyetine göre bilgisayar ve İnternet kulanım oranları, 2018*. [Çevrim-içi: http://www.tuik.gov.tr/PreTablo.do?alt_id=1028, Erişim tarihi: 20.10.2018.]

Tuncer, M., & Dikmen, M. (2016). *Sosyal ağlarda bekleyen yeni tehlike: Siber zorbalık. Re-discovery Learning with Digital Learners.* (ss. 94-102). Elazığ: Elektronik Kitap. [Çevrim-içi: https://openaccess.firat.edu.tr/xmlui/bitstream/handle/11508/9302/Sosyal%20A%C4%9Flarda%20Bekleyen%20Yeni%20Tehlike.pdf?sequence=1&isAllowed=y, Erişim tarihi: 15.07.2018.]

We Are Social (2018). *Global digital report 2018*. [Çevrim-içi: https://digitalreport.wearesocial.com/, Erişim tarihi: 12.10.2018.]

Whitney, I., & Smith, P. K. (1993). A survey of the nature and extent of bullying in junior/middle and secondary schools. *Educational Research*, 35, 3–25.

Yıldız Durak, H. (2018). Modeling of variables related to problematic internet usage and problematic social media usage in adolescents. *Current Psychology*, 1-13. doi: https://doi.org/10.1007/s12144-018-9840-8.

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.