Sırakaya, M. ve 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: 02.10.2018.]

12. BÖLÜM

ÇOCUKLARIN ÇEVRİM-İÇİ ORTAMLARDA KARŞILAŞTIKLARI RİSKLER VE GÜVENLİ İNTERNET KULLANIMI

Dr. Öğr. Üyesi Mustafa SIRAKAYA
Ahi Evran Üniversitesi

Prof. Dr. Süleyman Sadi SEFEROĞLU
Hacettepe Üniversitesi

Özet

İnternet'in her yıl katlanarak artan kullanıcı sayısında çocuk kullanıcılar önemli bir yer tutmaktadır. İnternet çocukların gelişimi için benzersiz fırsatlar sunmakla birlikte bazı riskler de içermektedir. İnternet'in bilginin yayılımı bakımından kontrolsüz bir alan olması ve sahte kimlik bilgilerinin kullanılabilmesi gibi durumlar çocukları çevrim-içi riskler bakımından hedef tahtasına oturtmaktadır. Bu çalışmayla, çocukların çevrim-içi ortamlarda karşılaştıkları risklerin incelenmesi, güvenli İnternet kullanımı ve dijital ebeveynlik kavramlarının irdelenmesi amaçlanmaktadır. Ayrıca çalışmanın sonunda güvenli İnternet kullanımı konusunda çocuklara ve ailelere yönelik önerilere yer verilmektedir.

İnternet teknolojilerinde sürekli olarak yaşanan gelişmeler, çevrim-içi ortamlarda karşılaşılan risklerde de değişmelerin ortaya çıkmasına ve çeşitlenmesine yol açmaktadır. Alanyazında bu risklerle ilgili çeşitli değerlendirmeler bulunmaktadır. Araştırmacılar tarafından derlenen çevrim-içi riskler çocuğun rolü ve risk kaynaklarına göre sınıflandırılmıştır. Çocuklar "pasif, etkileşen, gerçekleştiren ve aşırı kullanan" rollerinde "içerik kaynaklı, iletişim kaynaklı, ticari kaynaklı ve cinsel kaynaklı" risklerle karşılaşmaktadırlar.

Çevrim-içi ortamlarda çocukları bekleyen çok sayıda risk olmakla birlikte, "*siber zorbalık*" ve "*İnternet bağımlılığı*" en yaygın karşılaşılan riskler olarak değerlendirilmektedir. Siber zorbalık, bir elektronik iletişim aracı kullanılarak, kasıtlı ve tekrar eden biçimde karşıdakini rahatsız etmek ya da zarar vermek amacıyla yapılan davranışlar şeklinde tanımlanabilir. Teknolojinin sunduğu olanaklarla geleneksel zorbalığa göre daha kolay bir şekilde gerçekleştirilebilen siber zorbalık, özellikle son yıllarda çocuklar arasında yaygın olarak görülen bir durum şeklinde değerlendirilmektedir. Bireyin İnternet kullanımını kontrol edememesi, aşırı kullanımından dolayı iş, aile ve sosyal hayatında sorunlar yaşaması şeklinde tanımlanan İnternet bağımlılığı ise, çocuklarda fiziksel, sosyal ve psikolojik rahatsızlıklara neden olmaktadır. Öte yandan çocukların

İnternet'i doğru biçimde kullanmaları ve çevrim-içi risklerden korunmalarında ailelere önemli roller düşmektedir. Bu bağlamda ebeveynlerin yeterlik ve sorumluluk durumlarını güncel açıdan ele alan "*dijital ebeveynlik*" kavramı ortaya çıkmıştır. Dijital ebeveynlik, dijital dünyayı takip ederek olanak, fırsat, ihtiyaç ve tehlikelerin farkında olan, çocuğunu bu tehlikelerden koruyup olanakların kullanımı hakkında bilinçlendiren ebeveyn olarak tanımlanabilir.

Anahtar Sözcükler: Çevrim-içi riskler, dijital ebeveynlik, güvenli internet, internet bağımlılığı, siber zorbalık

Hazırlık Soruları

1. İnternet'in çocuklar üzerinde ne gibi olumsuz etkileri olabilir? Tartışınız.
2. Siber zorbalık nedir? Hangi tür davranışların siber zorbalık olabileceğini belirtiniz.
3. Dijital ebeveynlik kavramını tanımlayınız.
4. İnternet'in güvenli kullanımı konusunda neler yapılabileceğini açıklayınız.

Giriş

İnternet'in henüz yeni yeni tanınmaya başlandığı 1990'lı yılların alanyazını incelendiğinde İnternet'in hayatın önemli bir parçası olduğu vurgusunun yapıldığı görülmektedir. Günümüzde ise, özellikle gelişen mobil teknolojiler sayesinde, İnternet toplumun çok büyük bir kesimi tarafından günün her anında ulaşılması ve etkin biçimde kullanılması gereken bir araç olarak yaşamımızdaki yerini almış durumdadır. Bu duruma paralel olarak dünya genelinde ve ülkemizde İnternet kullanımı her yıl katlanarak artmaktadır. Türkiye İstatistik Kurumu (TÜİK) tarafından yapılan araştırmaların bulguları, İnternet kullanan bireylerin oranı 2015 yılında %55,9 iken 2016 yılında bu oranın %61,2'ye yükseldiğini göstermektedir (TÜİK, 2015; 2016). TÜİK'in 2017 yılı Ağustos ayı verilerine göre Türkiye'de İnternet kullanan bireylerin oranı %66,8'dir (TÜİK, 2017). Bu veriler Türkiye'de her geçen yıl İnternete erişen birey sayısının arttığını göstermektedir. Bu kullanıcılar arasında çocukların sayısında da her yıl düzenli bir artış meydana gelmektedir. Örneğin Radyo ve Televizyon Üst Kurulu (RTÜK) tarafından yapılan bir araştırmaya göre, Türkiye'deki çocukların %76,2'si İnternet kullanmaktadır (RTÜK, 2013). TÜİK'e göre de İnternet kullanmaya başlama yaşı ortalama 9'dur (TÜİK, 2013). Bu verilerden hareketle, İnternet'in nüfusla oranındaki artışla paralel olarak çocukların İnternet kullanım oranlarının da artmakta olduğu söylenebilir (Canbek & Sağıroğlu, 2007).

Çocuklar arasında İnternet kullanım oranlarının artışının dışında, araştırmalar çocukların İnternet kullanım yaşlarının da giderek düştüğünü, İnternet kullanım amaçlarının çeşitlendiğini ve daha bireyselleşen İnternet kullanımının gerçekleştiğini göstermektedir (Holloway, Green & Livingstone, 2013; RTÜK, 2013; TÜİK, 2013). İnternet'in çocukların bilişsel gelişimi için sunacağı fırsatlar dikkate alındığında, bu artan ve çeşitlenen İnternet kullanımı desteklenmesi gereken bir durum gibi algılanabilir. Ancak İnternet özellikle çocuklar için bazı riskleri de barındırmaktadır. Bu risklerin ortaya çıkmasında İnternetin karakteristik özellikleri önemli rol oynamaktadır. İnternet bilginin yayılımı ve paylaşımı konusunda kontrolsüz bir alandır. Özellikle Web 2.0 teknolojisi İnternet'i en önemli bilgi paylaşım ortamı haline getirmiştir. Örneğin, kullanıcılar herhangi bir teknik beceriye sahip olmadan İnternet'te kolayca paylaşım

yapabilmektedirler. Ayrıca isteyen kullanıcılar kolayca bir web sitesi sahibi olabilmektedirler. Bu durum İnternet'te her türlü bilginin kontrolsüz biçimde çoğalmasına neden olmuştur. Ayrıca kullanıcılar İnternet üzerinden diğer kullanıcılarla birebir iletişim kurarken, kendilerini olduklarından farklı yaş, cinsiyet vb. gibi fiziksel özelliklerle ve sahte kimlik bilgileriyle tanıtabilmektedirler. İnternet üzerinde açılan hesaplarda kimlik doğrulaması gibi bir durum gerekmemektedir. Bu nedenle, sahte isimlerle ya da başka kimselerin kimlik bilgileri kullanılarak hesapların oluşturulması mümkündür. Kötü niyetli kullanıcılar bu durumları kendi lehlerine kullanabilmekte ve bu süreçte özellikle de çocukları hedef olarak seçebilmektedirler.

Çevrim-içi ortamların güvenli kullanımıyla ilgili olarak ihtiyaç duyulan okuryazarlık deneyimine (bilgi ve becerilerine) sahip olmayan çocuklar çevrim-içi riskler bakımından savunmasız durumda kalmaktadırlar (Valcke, Bonte, Wever & Rots, 2010). Çocuklar örneğin, siber zorbalık, İnternet bağımlılığı ve mahremiyet ihlalleri gibi çeşitli çevrim-içi risklere maruz kalabilmektedirler. Türkiye'nin de parçası olduğu "EU Kids Online" başlıklı araştırmanın sonuçlarına göre çocukların %25'i çeşitli çevrim-içi risklere maruz kalmaktadırlar (Kaşıkçı, Çağıltay, Karakuş, Kurşun & Ogan, 2014). Bu çalışmanın verileri, birçok sosyal paylaşım sitesinde kayıt için 13 yaş ve üstü olma şartı aranmasına rağmen, araştırmaya katılan 13 yaş altındaki çocukların yaklaşık 3'te birinin sosyal ağları kullandığını göstermektedir. Öte yandan çocukların %46'sının sosyal ağ sitesindeki kişisel bilgilerini herkes tarafından görülebilecek şekilde ayarladığı, %19'unun adres, %8'inin ise telefon bilgilerini sosyal ağlar üzerinde paylaştığı belirlenmiştir. Bu çalışmanın verilerine göre çocukların %11'i cinsel içerikli fotoğraf gördüğünü belirtirken, %11,5'i cinsel içerikli mesaj aldığını belirtmektedir. Araştırma sonucunda çocukların ve ebeveynlerin çevrim-içi riskler konusunda kendilerine güvenmelerine rağmen, İnternet becerileri konusunda yeterli düzeyde bilgi sahibi olmadıkları anlaşılmıştır. Araştırma sonuçları ayrıca Avrupa ülkeleri arasında en düşük İnternet okuryazarlığının Türkiye'deki çocuklarda olduğunu göstermektedir. Bu veriler ülkemizde çocukların çevrim-içi riskler bakımından karşı karşıya oldukları tehlikeyi göz önüne sermektedir. Nitekim ülkemizde yürütülen çeşitli çalışmalarda da çocukların karşılaştıkları çevrim-içi risklere dikkat çekilmektedir (Akbıyık & Kestel, 2016; Arıcak vd., 2008; Ayas & Horzum, 2012; Gökçearslan & Seferoğlu, 2016; Karahisar, 2014; Kaşıkçı vd., 2014; Kayri, Tanhan & Tanrıverdi, 2014; Peker, 2013; Sezer, Şahin & Aktürk, 2013; Topçu, Erdur-Baker & Çapa-Aydın, 2008). Öte yandan, çevrim-içi ortamda hızlı bir dönüşüm yaşanmaktadır. Her geçen gün yeni teknolojiler geliştirilmekte ve bu ortamlarda yeni araç ve uygulamalar kullanıma sunulmaktadır. Bu nedenle de çevrim-içi ortamlarda çocukların ve gençlerin karşılaştıkları risklerin sürekli olarak incelenmesine ihtiyaç duyulduğu söylenebilir.

Çalışmanın Amacı

Bu çalışmanın amacı, çocukların çevrim-içi ortamlarda karşılaştıkları riskleri ve bu bağlamda dijital ebeveynlik kavramını incelemektir. Çalışmada ayrıca güvenli İnternet konusu irdelenerek çocuklara ve ailelere yönelik önerilerde bulunulacaktır. Bu amaca ulaşmada aşağıdaki sorulara yanıt aranmıştır:

1. Çocukların çevrim-içi ortamlarda karşılaştıkları riskler nelerdir?
2. En sık karşılaşılan çevrim-içi risklerden siber zorbalık ve İnternet bağımlılığı nedir?
3. Çocukların çevrim-içi risklere karşı korunmasında ailelere düşen sorumluluk ve yeterlikler (dijital ebeveynlik) nelerdir?
4. Güvenli İnternet kullanımı nedir? Güvenli İnternet için dikkat edilmesi gerekenler nelerdir?

Çevrim-içi Riskler

Çevrim-içi riskler, bireyleri bilişsel, sosyal ve psikolojik olarak olumsuz etkileyen çevrim-içi durumlar olarak tanımlanabilir. Alanyazında çevrim-içi risklerin farklı şekillerde sınıflandırıldığı görülmektedir. Örneğin Livingstone ve Haddon (2008) bu riskleri, "içerik riskleri, bağlantılı kişi riskleri, ticari riskler ve gizlilik riskleri" olmak üzere 4 ana başlık altında toplamaktadır (Bkz. Şekil 1). İçerik risklerinde yasadışı içerikler, yanlış bilgiler, müstehcen/şiddet/ırkçı/nefret içerikli materyaller ve zorlayıcı (intihar, uyuşturucu vb.) içerikler gibi riskler bulunmaktadır. Bağlantılı kişi risklerinde yabancılarla bağlantı kurma ve siber zorbalığa maruz kalma riskleri yer almaktadır. Yasadışı kumar oynama, istenmeyen reklamlara maruz kalma ve korsan yazılım gibi durumlar ise ticari riskler başlığında yer almaktadır. Özel bilgilerin farkında olmadan paylaşılması ya da gizli bilgilerin başkaları tarafından ele geçirilmesi (hack) gibi riskler de gizlilik risklerini oluşturmaktadır.

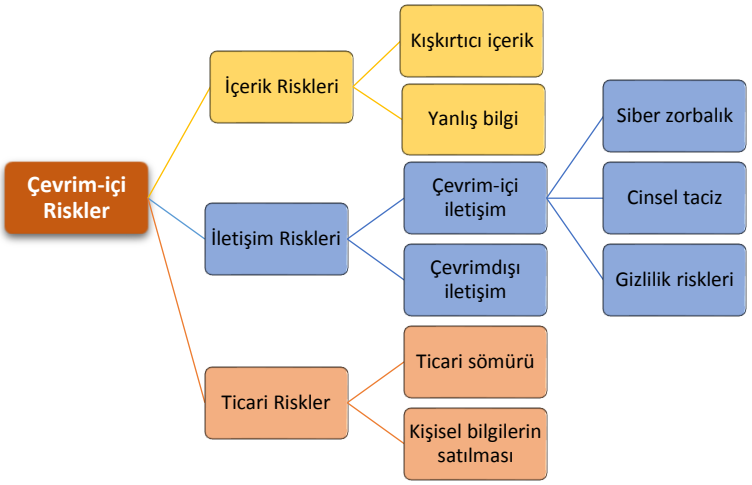
Şekil 1: Çevrim-içi Risklerle İlgili Bir Sınıflandırma (Livingstone & Haddon, 2008)

Livingstone, Mascheroni ve Staksrud (2015) çevrim-içi risklere çocukların aldığı rol boyutunu eklemişlerdir (Bkz. Tablo 1). Buna göre çocuklar "alıcı" rolünde içerik risklerine, "katılımcı" rolünde bağlantı risklerine ve "aktör" rolünde gerçekleştirme risklerine maruz kalmaktadırlar. Bu rollerin her biri "saldırganlık, cinsellik, değerler ve ticari" kategorilerinde değerlendirilmektedir. Böylelikle çocuğun oynadığı rol ve risk içeriğine göre 12 farklı risk kategorisi oluşmaktadır.

Tablo 1: Çocukların Üstlendikleri Rollere göre Çevrim-içi Riskler (Livingstone, Mascheroni & Staksrud, 2015)

	İçerik (Çocuk alıcı rolünde)	Bağlantı (Çocuk katılımcı rolünde)	Gerçekleştirme (Çocuk aktör rolünde)
Saldırganlık	Şiddetli / ürkütücü içerik	Gizlice izleme, taciz	Siber zorbalık
Cinsellik	Pornografik içerik	Yabancılarla iletişimde cinsel taciz	Müstehcen içerik, cinsel taciz
Değerler	Irkçı / nefret uyandıran içerik	İdeolojik propaganda	Zararlı içerik oluşturma
Ticari	Saklı (gizli) pazarlama	Kişisel bilgilerin kötüye kullanılması	Kumar oynama, korsan yazılım kullanma

De Moore vd.(2008 akt: Valcke, De Wever, Van Keer & Schellens, 2011) ise çevrim-içi riskleri, "içerik riskleri, iletişim riskleri ve ticari riskler" olmak üzere 3 kategoride listelemektedir (Bkz. Şekil 2). *İçerik riskleri*, "kışkırtıcı içerik ve yanlış bilgi" olarak ele alınmıştır. Kışkırtıcı içerik, "cinsel, ırkçı, nefret uyandıran metin ve görselleri" kapsamaktadır. Yanlış bilgi ise çocuğun doğru olduğunu düşündüğü "yönlendirici bilgiler"dir. *İletişim riskleri* çevrim-içi ve çevrimdışı olarak sınıflandırılmaktadır. Siber zorbalık, cinsel taciz ve gizlilik riskleri çevrim-içi iletişimde karşılaşılan risklerdir. Çevrim-içi ortamlarda tanışılan kişilerle yüz yüze görüşme ise çevrimdışı riski oluşturmaktadır. *Ticari riskler* ise, "çocukların yanlış yönlendirmelerle ticari olarak sömürülmesi ve kişisel bilgilerin toplanarak ticari amaçla satılması" olarak tanımlanabilir.



Şekil 2: Çevrim-içi Riskler (De Moore vd., 2008 akt: Valcke vd., 2011)

Yukarıda verilen çevrim-içi risklerle ilgili modeller birbirleriyle çeşitli benzerlikler ve farklılıklar içermektedirler. İnternet teknolojilerinin sürekli gelişmesi, çevrim-içi ortamlarda bulunan risklerin değişmesine ve çeşitlenmesine yol açmaktadır. Bu nedenle çocukların karşı karşıya olduğu çevrim-içi riskleri güncel olarak ele alan bir sınıflamanın yararlı olacağı düşünülmektedir. Tablo 2'de araştırmacılar tarafından derlenen çevrim-içi riskler verilmiştir.

Tablo 2: Çocukların Çevrim-İçi Ortamlarda Karşılaştıkları Risklerle İlgili Bir Sınıflama

Risk Kategorileri / **Çocuğun Rolü**	**İçerikten Kaynaklanan Riskler**	**İletişimden Kaynaklanan Riskler**	**Ticari Kaynaklı Riskler**	**Cinsellik Kaynaklı Riskler**
Pasif	Yanlış, şiddet içeren, ideolojik, ırkçı, yönlendirici içerik	Kişisel bilgilerin sanal ortamlarda paylaşılması	İstenmeyen reklamlar, Gizli pazarlama yöntemleri	Uygunsuz müstehcen içeriğe maruz kalma
Etkileşen	Yanlış, şiddet içeren, ideolojik, ırkçı, yönlendirici iletişim	Siber zorbalığa maruz kalma, Siber tacize uğrama	Kişisel bilgilerin toplanması, Siber dolandırıcılık	Cinsel tacize uğrama
Gerçekleştiren	Uygunsuz içerikler üretme	Siber zorba olma	Telif haklarını ihlal, Kumar oynama	Uygunsuz müstehcen içerik oluşturma
Aşırı Kullanan	İnternet bağımlılığı, Çevrim-içi (dijital) oyun bağımlılığı, Sosyal medya bağımlılığı, Akıllı telefon bağımlılığı, Teknoloji bağımlılığı			

Tablo 2 incelendiğinde çocukların çevrim-içi riskler bakımından 4 farklı rolde yer aldıkları görülmektedir. *Pasif* rolde, risk kaynakları bakımından alıcı ya da izleyici durumundadır. *Etkileşen* rolünde risk kaynaklarıyla karşılıklı olarak yürütülen süreçlerde bulunan riskler söz konusudur. Etkileşen rolünde çocuk genellikle, karşı taraf tarafından başlatılan iletişim sürecinde mağdur olmaktadır. *Gerçekleştiren* rolünde ise, riski oluşturan çocuktur ve çoğunlukla iletişim sürecini çocuk başlatır. *Aşırı kullanan* rolü, çocuğun bütün risk kaynaklarından etkilenebileceği bir potansiyele sahip olduğu durumdur. Çocuk ciddi mağduriyetler yaşadığı halde sınırlandıramadığı İnternet'in aşırı kullanımından kaynaklı risklerle karşılaşabilir. Bu aşamada çocuklar İnternet bağımlılığı, çevrim-içi (dijital) oyun bağımlılığı, sosyal medya bağımlılığı, akıllı telefon bağımlılığı ve teknoloji bağımlılığı gibi farklı isimlerle adlandırılan bağımlılık türleriyle karşı karşıya kalmaktadırlar.

İçerik Kaynaklı Riskler: İnternet günümüzde her türlü bilgiye erişebildiğimiz, dünyanın en büyük bilgi kaynağı durumundadır. Sosyal ağların kullanımının yaygınlaşması, İnternet üzerinde bilgi paylaşımı yapmanın ve hatta web sayfası hazırlamanın teknik bilgi ve beceri gerektirmemesi gibi durumlar, İnternet üzerindeki bilginin büyük bir hızla artmasını sağlamıştır. Avantaj gibi görünen bu durum aynı zamanda zararlı içeriklerin de kolayca üretilmesinin ve yayınlanmasının önünü açmıştır. İnternet üzerinde; "ürkütücü, nefret uyandıran, şiddet içerikli, terör propagandası yapan, ırkçı söylemler içeren, kullanıcısını depresyon, intihar vb. durumlara sürükleyebilen, ideolojik, müstehcen ve yanlış bilgilendirici (trol)" içerikler bulunmaktadır. Çocuklar İnternet'te gezinirken bu tür içeriklerle istemsiz olarak karşılaşabilmektedirler. Çocukların zararlı içeriklerden korunmak için gerekli yeterliklere sahip olmadıkları dikkate alındığında, yetişkin kullanıcılara göre daha büyük risk altında oldukları söylenebilir. Ülkemizde yapılan çalışmalar çocukların İnternet'te "şiddet öğeleri, cinsel içerik, terör propagandası, yasaklı madde kullanımı" (Akbıyık & Kestel, 2016; Çelen, Çelik & Seferoğlu, 2011; Gökçearslan & Seferoğlu, 2016; Karahisar, 2014; Kaşıkçı vd., 2014) gibi uygunsuz içeriklerle karşılaştığını göstermektedir.

İletişimden Kaynaklanan Riskler: İnternet insanlar arasındaki fiziksel engelleri ortadan kaldırarak, iletişim kavramının sınırlarını genişletmiştir. Oluşan bu esnek ve kontrolsüz ortam çocuklar için ciddi iletişim riskleri içermektedir. İletişim risklerinden en masum gibi görüneni çocukların adres, telefon gibi kişisel bilgilerini İnternet üzerinden başkalarının görebileceği şekilde paylaşmalarıdır. Bu konuyla ilgili çalışmaların bulguları çocukların çevrim-içi ortamlarda tanımadıkları kişilerle sohbet ettiklerini (Karahisar, 2014) ve çevrim-içi arkadaş edindiklerini göstermektedir (Gökçearslan & Seferoğlu, 2016; Kaşıkçı vd., 2014; Kayri, Tanhan & Tanrıverdi, 2014). İşte bu etkileşimleri yaşayan çocuklar, karşılıklı iletişim kurdukları ortamlarda, tanımadıkları kişiler tarafından siber zorbalığa veya siber tacize maruz kalabilmektedirler.

Ticari Kaynaklı Riskler: İnternet, reklam ve pazarlama amacıyla kullanılabilecek en etkili kitle iletişim aracı olarak değerlendirilebilir. Diğer kitle iletişim araçlarında olduğu gibi bir kontrol mekanizmasının olmaması ve daha ucuz seçeneklere sahip olması İnternet'i pazarlama açısından cazip hale getirmektedir. Bu durum kullanıcıların istenmeyen ya da uygunsuz reklamlara maruz kalmalarına neden olabilmektedir. Gizli pazarlama yöntemleriyle kullanıcıların rızası dışında ürün ya da hizmet satılması ve dolandırıcılık da çevrim-içi ortamlarda sıklıkla karşılaşılan riskler arasında yer almaktadır. Çocuklar müzik dinleme, film izleme, oyun oynama gibi amaçlarla telif haklarını ihlal edebilmektedirler. Bu ortamlarda kullanılan korsan yazılımlar, indirilen

bilgisayardan kişisel bilgilerin, belge ve görüntülerin gizlice alınarak başkalarıyla paylaşılması gibi riskleri de barındırmaktadır.

Cinsel Kaynaklı Riskler: Cinsel istismar çevrim-içi ortamlarda çocukların maruz kaldığı risklerin başında gelmektedir. İnternet üzerindeki reklam ve içeriklerin denetimi genellikle söz konusu olmadığından çocukların istem dışı olarak bu cinsel içeriklerle karşılaşması söz konusu olabilmektedir Kaşıkçı vd. (2014) çocukların yaklaşık %13'nün İnternette gezinirken cinsel içeriklerle karşılaştığını belirtmektedir. Ayrıca sosyal ağlar, arkadaş edindirme siteleri, çevrim-içi oyunlar, çevrim-içi mesajlaşma ortamları sahte kimlik bilgileriyle çocukları taciz ve istismar etmek isteyen kişilerin kullanımına açıktır. Yine Kaşıkçı vd.'nin (2014) araştırmasında, çocukların %12'sinin cinsel içerikli mesajlar aldığı ve %4'ünün cinsel içerikli mesaj yolladığı ortaya çıkmıştır.

Kısaca, çocukların çevrim-içi ortamlarda karşılaştıkları risk kaynaklarının 4 başlık altında incelenmesi mümkündür. Çevrim-içi ortamlarda yaşanan sorunlar konusunda yürütülen çalışmalarda "İnternet bağımlılığı, sanal zorbalık (İnternet'teki şiddet), İnternet'teki çocuk istismarı (çocuk pornografisi ve pedofili), sanal taciz, nefret söylemi, sanal yalnızlık, trolcülük, zararlı yazılımlar ve çeşitli diğer bağımlılıklar" gibi konu başlıklarıyla karşılaşıldığı görülmektedir (Akbıyık & Kestel, 2016; Arıcak vd., 2008; Ayas & Horzum, 2012; Çelen, Çelik & Seferoğlu, 2017; Doğan, Çınar & Seferoğlu, 2017; Kaşıkçı vd., 2014). Bu çalışma kapsamında alanyazında üzerinde yoğun olarak durulan sorunlardan olan, çocukların en çok mağdur oldukları "siber zorbalık ve İnternet bağımlılığı" ayrıntılı olarak ele alınmaktadır.

Siber Zorbalık

Özellikle mobil teknolojilerdeki gelişmeler ve kullanımın giderek yaygınlaşması, "orantısız güç kullanarak karşıdaki bireye zarar verme amacı taşıyan ve zaman içinde de tekrar eden saldırgan davranışlar" şeklinde tanımlanan geleneksel zorbalık davranışlarının sanal ortamlarda da yaşanması sonucunu doğurmuştur. Siber zorbalık bilgi ve iletişim teknolojilerini kullanarak başkalarına zarar vermek amacıyla yapılan davranışlar olarak tanımlanabilir (Agaston, Kowalski & Limber 2007; Keser & Kavuk, 2015). Yani teknoloji aracılığıyla saldırgan ve zorba davranışların gösterilmesine siber zorbalık denmektedir (Piotrowski, 2012). Kısaca siber zorbalık, bir elektronik iletişim aracı kullanılarak, kasıtlı ve tekrar eden biçimde karşıdakini rahatsız etmek ya da zarar vermek amacıyla yapılan davranışlar şeklinde tanımlanabilir. Tanım bakımından geleneksel zorbalıkla benzer gibi gözükse de siber zorbalığın elektronik iletişim cihazları üzerinden yapılması pek çok sınırlılığı ortadan kaldırmaktadır. Bu durum ne yazık ki zorba için işleri kolaylaştırırken, mağdur için durumu daha da içinden çıkılmaz bir hale getirebilmektedir. Bu bağlamda geleneksel zorbalıkla siber zorbalık arasında bir karşılaştırma yapıldığında (Durak & Seferoğlu, 2016) mağdur açısından durumun vahameti daha iyi anlaşılabilir (Bkz. Tablo 3).

Tablo 3: Geleneksel Zorbalıktan Siber Zorbalığa Değişen Özellikler (Durak & Seferoğlu, 2016)

Geleneksel Zorbalık	Siber Zorbalık
Sadece yüz yüze zamanlarda gerçekleşebilir.	Günün her anı gerçekleşebilir.
Zorbanın tespiti kolaydır.	Zorbanın tespit edilmesi zordur.
Mağdur için güvenli alanlar ya da kaçış imkânı vardır.	Güvenli alan yoktur, kaçış zordur.
İzleyicilerle sınırlıdır.	Coğrafi sınır yoktur.
Mağdur ile zorba arasında güç dengesizliği vardır.	Çevrim-içi ortamlarda zorbalık materyali çok hızlı yayılacağından, güç dengesizliği oluşturur.
Genellikle okulla sınırlıdır.	Zorbalık herhangi bir anda herhangi bir yerde gerçekleşebilir.

Tablo 3'te görüldüğü gibi yüz yüze ortamlarda yapılan zorbalık davranışları sanal ortamlarda daha kolay bir şekilde yapılabilmektedir. Sanal ortamlardaki işleyişlerin ve erişimlerin gerçek hayata göre daha hızlı olması, takip işinin ve kontrolün daha zor olması, zaman ve mekân sınırlarının ortadan kalkması ve karşıdaki kişinin gerçek kişi gibi algılanmayışı gibi durumlar siber zorbalık davranışlarının yaygın olarak görülmesine neden olabilmektedir. Siber zorbalar sanal ortamların sağladığı gizlilik şemsiyesi altında gerçek kimliklerini de saklayarak rahat hareket edebilmektedirler. Zorbalar, sahte kimlik bilgileri kullanmalarının yakalanmalarını önleyeceğini düşünmektedirler. Sanal ortamlarda gösterilen zorba davranışlar kısa zamanda çok sayıda kişi tarafından görüleceği için yaşanan mağduriyetlerin etkisi de geleneksel zorbalığa göre daha fazla olmaktadır. Ayrıca siber zorbanın mağdur üzerinde oluşturduğu zararı gerçek ortamda gözlemlememesi siber zorbalık davranışlarının küçümsenmesine neden olmaktadır. Ancak siber zorbalığın mağdurların sosyal ve psikolojik hayatlarında ciddi zararlara neden olduğu bilinmektedir (Akbıyık & Kestel, 2016; Ayas & Horzum, 2012; Çelen, Çelik & Seferoğlu, 2016; Durak & Seferoğlu, 2016; Li, 2007). Elektronik iletişim araçlarının kullanılıyor olması siber zorbalıkta kullanılan yöntem, ortam ve araçları geleneksel zorbalığa göre farklılaştırmaktadır. Siber zorbalık, bilgisayar, cep telefonu, akıllı telefon, tablet gibi araçlarla, e-posta yollama, mesaj gönderme, sesli arama, görüntülü arama, çeşitli ortamlarda paylaşım yapma gibi farklı yöntemler kullanılarak yapılabilmektedir. Bir kişi ya da grubu sanal yollarla tehdit etmek, hesabını ele geçirmek, taciz etmek, küçük düşürmek, isim takmak, ifşa etmek, alay etmek, hakaret etmek, dedikodu yapmak, başkaları adına sahte hesap açmak gibi davranışlar siber zorbalığa örnek olarak verilebilir (Bkz. Şekil 3).

Şekil 3: Siber Zorbalık Örnekleri

Yapılan araştırmalar sadece yetişkinlerin değil çocukların da siber zorbalığa maruz kaldığını ya da siber zorbalık yapabildiğini göstermektedir (Akbıyık & Kestel, 2016; Arıcak vd., 2008; Ayas & Horzum, 2012; Çelen, Çelik & Seferoğlu, 2016; Kavuk & Keser, 2016; Peker, 2013; Sezer, Şahin & Aktürk, 2013; Topçu, Erdur-Baker & Çapa-Aydın, 2008). Ülkemizde yapılan çalışmaların sonuçları çocuklar ve gençler arasında siber zorbalığın yaygın olduğunu ortaya koymaktadır. Ortaokul ve lise öğrencilerinin siber zorbalık durumlarını araştırdıkları çalışmalarında Arıcak vd. (2008) katılımcıların %40'ının hakarete uğradığını, %41'inin tehdit edildiğini, %26'sının ise dedikodusunun yapıldığını belirtmekledirler. Siber zorba olma bakımından, %24'ünün yüz yüze iletişimde söylemeyeceği şeyleri sanal ortamlarda söylediğini, %16'sının kendisini başkası gibi tanıttığını ve %5'inin başkalarına ait fotoğrafları izinsiz olarak kullandığı gerçeği ortaya çıkmıştır. Ayas ve Horzum (2012) tarafından yapılan çalışmada siber zorbalık bakımından ortaokul öğrencilerinin %18'nin mağdur, %11'nin ise sanal zorba olduğu anlaşılmıştır. Araştırmada, yaş arttıkça yapılan sanal zorbalık oranı artarken, daha düşük yaştaki çocuklarda sanal mağdur olma oranının arttığı sonucuna ulaşılmıştır. Akbıyık ve Kestel (2016) çocukların sanal zorbalığa en çok sosyal ağlar, çevrim-içi oyunlar ve mesajlaşma servislerinde maruz kaldığını belirtmektedir. Bu araştırmanın sonuçlarına göre, aşağılanma, tehdit, kişisel bilgi ve resimlerin ele geçirilmesi sık rastlanan siber zorbalık türleri arasında yer almaktadır. Öte yandan mağdur olan öğrencilerin siber zorbalıkla başa çıkma konusunda yeterli bilgiye sahip olmadıkları ve bu nedenle bu durumu ebeveyn ve öğretmenleriyle paylaşamadıkları anlaşılmıştır. Bu durumla kendi başlarına mücadele etmeye çalışmaları çocukların, öfke, tedirginlik, korku gibi olumsuz duygular yaşamalarına neden olmakta, okula devamsızlık, akademik başarıda düşüş ve sosyal hayatın olumsuz etkilenmesi gibi sonuçlar ortaya çıkabilmektedir. Aşırı şekilde siber zorbalığa maruz kalmanın mağdurda intiharı düşünmeye neden olmaya kadar ilerlemesi siber zorbalığın varabileceği tehlikenin boyutlarını göstermektedir. Siber zorbalığa maruz kalan çocukların bu durumla nasıl başa çıkabileceklerini bilmeleri onların siber sağlıkları açısından önem arz etmektedir. Ancak ülkemizde yürütülen çalışmalar çocuklarımızın ve ebeveynlerin bu yeterliklere sahip olmadığını göstermektedir (Canbek & Sağıroğlu 2007; Kaşıkçı vd., 2014). Siber zorbalığa uğrayan çocuklar genellikle durumu kimseyle paylaşmamaktadırlar. Hatta en az başvurulan yöntemin anne, baba ve öğretmen gibi yetişkinlerin haberdar edilmesi olduğu görülmektedir (Arıcak vd., 2008; Ayas & Horzum, 2012; Kavuk & Keser, 2016; Li, 2007; Sezer, Şahin & Aktürk, 2013; Topçu, Erdur-Baker & Çapa-Aydın, 2008). Öte yandan teknolojik araç kullanımlarına kısıtlama ya da yasak getirilebileceği düşüncesi veya korkusu çocukların çevrim-içi ortamlarda yaşadıkları sorunları bir yetişkinle paylaşmamaları sonucunu doğurabilmektedir (Kavuk & Keser, 2016). Bu durum siber zorbalıkla ilgili önleyici tedbirlerin alınmasına engel olmaktadır.

İnternet Bağımlılığı

Çocukların ve gençlerin çevrim-içi ortamlarda yaşadıkları bir diğer sorun "İnternet bağımlılığı" olarak bilinen bağımlılık türüdür. İnternet zaman ve mekân gibi sınırlamaları ortadan kaldırarak, toplumların sosyal, kültürel, teknolojik ve bilimsel açıdan ilerlemesine ciddi katkılar sağlamaktadır. Bireysel anlamda ise, günlük hayatın rutin işlerinin kolayca yapılması, kişisel gelişim, eğitim olanakları gibi konularda hayatımızı kolaylaştırmaktadır. Ancak İnternet'in hızla yaygınlaşması birtakım olumsuz durumların da yaşanmasına sebep olmuştur (Gökçearslan & Seferoğlu, 2016). İnternet kullanımını sınırlandırma konusunda sorun yaşayan bireylerin tıpkı alkol ve uyuşturucu madde bağımlıları gibi olumsuz sonuçlarla karşılaştığı görülmektedir. İnternet bağımlılığı olarak ifade edilen bu durum, bireyin İnternet kullanımını kontrol edememesi, aşırı kullanımından dolayı iş, aile ve sosyal hayatında sorunlar yaşaması şeklinde tanımlanabilir (Young, 1996).

İlk defa doksanlı yıllarda tartışılmaya başlanan İnternet bağımlılığı zaman içerisinde, "patolojik İnternet kullanımı, problemli İnternet kullanımı, aşırı İnternet kullanımı, İnternet bağlılığı" gibi farklı kavramlar adı altında tartışılmaya devam etmiştir. Ülkemizde de İnternet'in yaygınlaşmaya başladığı 2000'li yıllardan itibaren İnternet kullanımıyla ilgili sorunların tartışılmaya başlandığı görülmektedir. İnternet ve mobil teknolojilerde yaşanan gelişim ve mobil cihazların yaygınlaşması, çocukların da İnternet kullanımıyla ilgili sorunlar yaşamasına neden olmuştur.

İnternet çocukların araştırma yapma, karar verme, eleştirel düşünme, problem çözme gibi niteliklerini geliştirme konusunda gerekli altyapıyı sunmasına rağmen zararlı kullanımı konusunda da ciddi riskler barındırmaktadır. Nitekim ulusal alanyazın, çocuklarımızın İnternet bağımlılığı bakımından önemli sayılacak düzeyde risk grubunda olduğunu göstermektedir (Çam & Nur, 2015; Gökçearslan & Günbatar, 2012; Gökçearslan & Seferoğlu, 2016; Kılınç & Doğan, 2014; Kıran, 2009; Müezzin, 2017; Taylan & Işık, 2015). Günümüzde İnternet'in çocuklar arasında yaygın biçimde kullanılması ve gelecekte bu kullanım oranının daha da artabileceği gerçeği, çocukların İnternet bağımlılığı bakımından taşıdıkları riski göstermektedir.

Aşırı İnternet kullanımı çocuklarda fiziksel, psikolojik, sosyal birçok sorunun yaşanmasına neden olabilmektedir. Çocuklarda aşırı İnternet kullanımına bağlı olarak görülen sorunlardan bazıları aşağıdaki şekilde özetlenebilir (Bkz. Şekil 4):

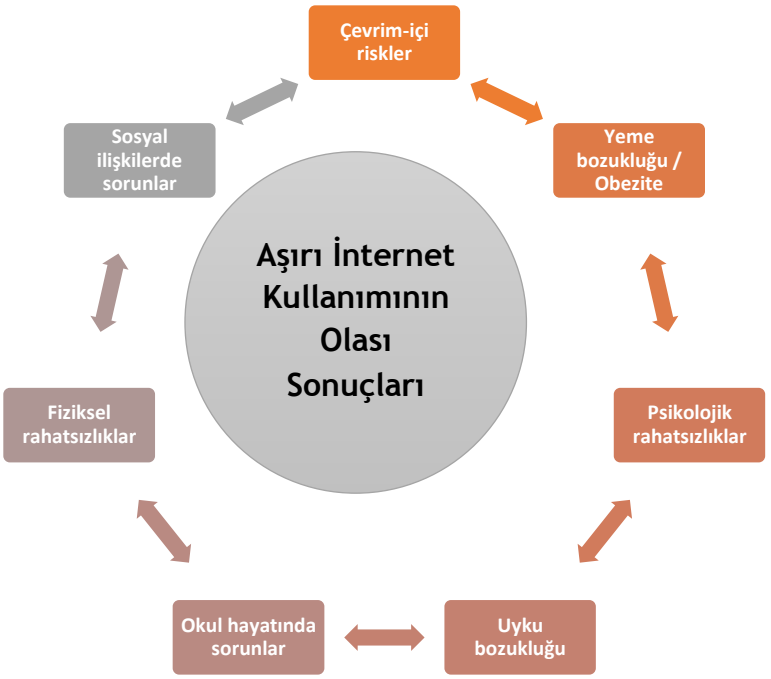
- İnternet kullanımı için bilgisayar ya da mobil cihaz başında geçirilen uzun süreler, gelişim döneminde bulunan çocuklarda fiziksel rahatsızlıkların görülmesine neden olabilir. Görme bozuklukları, eklem yerlerinde ağrı gibi rahatsızlıklar en çok görülen fiziksel bozukluklar arasındadır.

- İnternet kullanımını sonlandıramama çocukların yemek öğünlerini atlamalarına ya da düzensiz yemek yemeleri gibi beslenme sorunlarına neden olabilmektedir.

- Günlük İnternet kullanım süresinin sınırlandırılamaması, çocukların gece geç saatlere kadar İnternet başında olmalarıyla sonuçlanmaktadır. Gece geç uyuma, sabah uyanamama, düzensiz uyku gelişim dönemindeki çocuklar için önemli bir sorundur.

- İnternet başında uzun süreler hareketsiz kalarak vakit geçirmek ve düzensiz beslenme çocuklarda obezite riskini artırmaktadır.

- İnternet başında geçirilen sürenin artması, yüz yüze iletişimde geçirilen sürenin azalmasına neden olmaktadır. Bu durum çocukların aile bireyleri ve arkadaşlarıyla olan iletişimini olumsuz etkilemekte ve çocukların giderek yalnızlaşmasıyla sonuçlanmaktadır.
- İnternet kullanım süresini azaltmayı istemeye rağmen azaltamama, ailelerin bu konuda baskı uygulaması gibi durumlar çocuklarda huzursuzluk, gerginlik, saldırganlık gibi psikolojik olumsuzlukların yaşanmasına neden olmaktadır. İnternet kullanımını azaltamama çocukların suçluluk duygusuna kapılmasına neden olmaktadır.
- Çocukların okul başarısında düşüş yaşanması ve okula devamsızlık yapılması aşırı İnternet kullanımının neden olduğu durumlar arasında yer almaktadır.
- İnternet kontrolü zor ve sınırları esnek olan bir ortamdır. Çocuklar İnternet'te gerçek dünyadakinden çok daha tehlikeli durumlarla karşılaşabilirler. Çevrim-içi ortamlarda kurulacak arkadaşlıklar çocuklar için ciddi riskler taşımaktadır.



Şekil 4: Çocuklarda Aşırı İnternet Kullanımına Bağlı Görülen Sorunlar

Güvenli İnternet Kullanımı Ve Dijital Ebeveynlik

Güvenli İnternet aşırı olmayan kullanım süresinde, İnternet'in barındırdığı risklerden korunarak sunduğu sayısız imkândan yararlanmak olarak tanımlanabilir. Çocukların çevrim-içi ortamlarda istismar edilmesi İnternet'in güvenli biçimde kullanımını gündeme getirmiştir. Bu bağlamda ülkemizde de İnternet'in güvenli biçimde kullanılabilmesini sağlamak amacıyla yasal düzenlemeler ve çeşitli etkinlikler yürütülmektedir. Bilgi Teknolojileri ve İletişim Kurumu, bünyesinde faaliyet gösteren Güvenli Web (www.guvenliweb.org.tr), Güvenli Çocuk (www.guvenlicocuk.org.tr), Güvenli İnternet (www.guvenlinet.org.tr/tr), İnternet Yardım Merkezi (www.internetyardim.org.tr) ve İnternet Bilgi İhbar Merkezi (www.ihbarweb.org.tr) gibi İnternet siteleri aracılığıyla İnternet'in güvenli biçimde kullanımı için gerekli desteği sağlamaktadır.

Güvenli İnternet Hizmeti (www.guvenlinet.org.tr): Bu hizmet, İnternet'teki zararlı içeriklerden korunmak için İnternet hizmet sağlayıcıları tarafından ücretsiz olarak sunulan alternatif bir erişimdir. Güvenli İnternet Hizmetinde çocuk profili ve aile profili olmak üzere iki seçenek bulunmaktadır. Çocuk profilinde sadece güvenliği onaylanmış web sayfalarına erişim sağlanmaktadır. Çocukların ruhsal ve bedensel sağlıklarını olumsuz etkileyecek, yabancılarla doğrudan iletişime izin veren web sayfaları güvenli liste dışında tutulmaktadır. Çocuk profilinden daha geniş erişim imkanına sahip olan aile profilinde, yasaklı listedeki sitelere erişim engellenmektedir. Cinsel istismar, kumar, tehlikeli madde kullanımı, ırkçılık, korsan yazılım gibi içeriklere sahip siteler erişime kapalıdır. Oyun, sosyal medya ve sohbet sitelerinin erişimi ise ailelerin tercihine bırakılmaktadır.

Güvenli Web (www.guvenliweb.org.tr): Bu site İnternet'in güvenli biçimde kullanımı hakkında destekleyici ve bilinçlendirici bilgiler içermektedir. Ayrıca bu faaliyet kapsamında öğrencileri bilinçlendirmek için çeşitli etkinlikler düzenlenmektedir.

İnternet Yardım Merkezi (www.internetyardim.org.tr): Bu web alanında güvenli İnternet kullanımı için dikkat edilmesi gerekenler ve istenilmeyen durumlarla karşılaşıldığında yapılması gerekenler gibi konularla ilgili sorulara cevaplar yer almaktadır.

İnternet Bilgi İhbar Merkezi (www.ihbarweb.org.tr): Bu site aracılığıyla kullanıcılardan gelen ihbarlar doğrultusunda 5651 sayılı yasanın 8. maddesinde yer alan, intihara yönlendirme, çocuk istismarı, uyuşturucu madde kullanımı, sağlığa tehlikeli madde temini, müstehcenlik, fuhuş, kumar oynatma veya yer sağlama, Atatürk aleyhine suç işleme gibi içerikler barındıran sitelere erişim engellenmektedir.

Güvenli Çocuk (www.guvenlicocuk.org.tr): Bu alan, çocuklar için oyun, güncel haberler, eğlence içerikleri barındıran web sayfasıdır.

Güvenli İnternet kullanımıyla ilgili olarak gerekli yasal düzenlemeler yapılarak, bu konudaki mağduriyetlerin giderilmesi için adım atılmıştır. Türk Ceza Kanunu'nun 243, 244 ve 245. maddeleri bilişim vasıtasıyla işlenen suçlara düzenleme getirmiştir. Buna göre çevrim-içi ortamlarda yapılması bilişim suçu sayılan eylemlerden bazıları aşağıdaki şekilde listelenebilir (GüvenliWEB, 2018):

- Bilgisayar sabotajı,
- Bilgisayar yoluyla dolandırıcılık,
- Bilgisayar yoluyla sahtecilik,
- Bilgisayar yazılımının izinsiz kullanımı,
- Kişisel verilerin kötüye kullanılması,
- Sahte kişilik oluşturma ve kişilik taklidi,
- Terörist faaliyetler,
- Çocuk pornografisi,
- Bilgisayar korsanlığı (hacking),
- Yasadışı yayınlar,
- Tehdit, uyuşturucu, fuhuş gibi diğer suçlar.

Yapılan yasal düzenlemelerle çevrim-içi ortamlarda karşılaşılan risklerin suç olarak sayılması için gerekli zemin hazırlanmıştır. Ancak teknolojide yaşanan gelişmeler, kötü niyetli kişilerin farklı yollar ve araçlarla bilişim suçu işlemelerinin yolunu açabilmektedir. Bu nedenle konuyla ilgili birimlerin bilgi ve iletişim teknolojilerindeki gelişmeleri yakından takip ederek gerekli önlemlerin alınması konusunda sürekliliği sağlamaları önemlidir.

Çocukların bilgi ve eğlence kaynağı olarak İnternet'ten doğru biçimde faydalanmaları ve çevrim-içi risklerden korunmalarında ailelere önemli roller düşmektedir. Palfrey ve Gasser (2008) çocukların karşılaştığı çevrim-içi risklerin çözümünde en önemli paydaşın aile olduğunu belirtmektedir. Mobil teknolojilerde yaşanan gelişim, çocukların da doğrudan İnternet kullanıcısı olmalarının yolunu açmıştır. Bu durum ebeveynlerin yeterlik ve sorumluluklarını güncelleyerek dijital ebeveynlik kavramını ortaya çıkarmıştır.

Dijital ebeveynlik, dijital dünyayı takip ederek olanak, fırsat, ihtiyaç ve tehlikelerin farkında olan, çocuğunu bu tehlikelerden koruyup olanakların kullanımı hakkında bilinçlendiren ebeveyn olarak tanımlanabilir. Yurdakul, Dönmez, Yaman ve Odabaşı (2013) dijital ebeveynliği 5 ana başlık altında ele almışlardır. Bu ana başlıklar, "dijital okuryazarlık, farkında olma, kontrol, etik ve yenilikçilik" şeklindedir. *Dijital okuryazarlık* İnternet'te yer alan uygunsuz içerikleri tespit edebilecek teknoloji kullanım becerisine sahip olma olarak ele alınmıştır. Dijital okuryazar olan ebeveynlerden çevrim-içi ortamlarda bulunan fırsatlar ve risklerin *farkında olma*ları beklenmektedir. Ebeveynlerin çocuklarını dijital risklere karşı korumasında *kontrol* mekanizmasını işletmeleri gerekmektedir. Ancak bu kontrol mekanizması çocuğun çevrim-içi fırsatları kullanmasına engel olmamalıdır. Ebeveynler ayrıca çocuğa sadece gerçek yaşamda değil dijital ortamlarda da *etik* kuralların öğretiminden sorumludurlar. Bu nedenle ebeveynlerin kendilerinin de dijital etiğe sahip olması gerekmektedir. Dijital ebeveynlerin sahip olması gerek son özellik olarak, yeniliklere açık olma ve yenilikleri takip etme olan *yenilikçilik* belirtilmiştir.

Sonuç ve Öneriler

İnternet ortamındaki kullanıcı sayısı ve bu ortamda geçirilen sürenin giderek artması, gerçek ve sanal dünya arasındaki ayrımı giderek ortadan kaldırmaktadır. Yaşam şeklimizdeki bu değişim farkında olmadığımız pek çok riski de beraberinde getirmektedir. Çocukların İnternet kullanımı arttıkça İnternet'in sağladığı olanaklardan yararlanma oranlarıyla birlikte çevrim-içi risklere maruz kalma oranları da artmaktadır (Livingstone, Haddon, Görzig & Olafsson, 2011). Yukarıda bahsedilen bu riskler çocukların bilişsel ve psikolojik olarak önemli sorunlar yaşamalarına neden olabilir. Bu durumun önlenmesi ve güvenli İnternet kullanımı için çocuklara aşağıdaki önerilerde bulunulabilir:

- Kimlik bilgileri, kart bilgileri, ev adresi, okul adı, telefon numarası, ebeveynlerin kimlik, iş ve iletişim bilgileri gibi bilgiler size ait özel bilgilerdir. Bu bilgilerin sosyal ağlarda başkalarının görebileceği şekilde paylaşılması ya da bir mesajın içeriğinde birilerine gönderilmesi sizi ve ailenizi riske atar.

- Çevrim-içi hesaplarınızın ele geçirilmesini önlemek için şifrelerinizi kimseyle paylaşmayın. Ayrıca şifrelerinizi oluştururken başkaları tarafından tahmin edilmesi zor şifreler seçmeye dikkat edin.

- Bilgisayarınızda ve mobil cihazınızda virüslere karşı koruma sağlayacak güncel bir anti-virüs programı bulundurmayı ihmal etmeyin.

- Gerçek hayatta uymamız gereken kurallar olduğu gibi sanal ortamlarda da dikkat etmemiz gereken etik kurallar vardır. Kendinize yapılmasını istemediğiniz şeyleri başkasına yapmayın.

- Sosyal ağlarda çok sayıda arkadaş sahibi olmak eğlenceli gibi görünebilir. Ancak tanımadığımız kişilerle arkadaşlık kurmanın önemli riskler içerebileceğini unutmayın.

- İnternet'te yapılan paylaşımlar geri alınamaz. Paylaşım yapmadan önce sizde yaratacağı uzun vadeli etkileri hesaplamaya çalışın.

- Müstehcen, tehditkâr, taciz içerikli, nefret söylemi vb. içeren bir mesaj aldığınızda bu mesaja cevap vermeyin. Mesajı göndereni engelleyin ve durumu güvendiğiniz bir yetişkinle (öğretmen, anne, baba gibi) mutlaka paylaşın.

- Tanımadığınız kişilerden gelen mesaj, e-posta vb. iletileri açmayın. Bu iletilerin içeriğinde gönderilen bağlantı, resim, dosya vb. ekler virüs içerebilir. Cihazınıza bulaştırılan bir virüs nedeniyle, cihazınızın çalışmaz hale gelmesi, bilgilerinizin çalınması, fidye istenmesi veya benzeri başka zararlara uğrayabilirsiniz.

- İnternet'te isteyen herkesin kasıtlı ya da kasıtsız olarak yanlış bilgi yayabileceğini unutmayın. Bu nedenle İnternet'ten edindiğiniz bilgilerin doğruluğunu farklı kaynaklardan teyit etmeden kullanmayın.

- Bilgisayara ya da mobil cihaza uygulama kurarken, uygulamanın sizden istediği erişim ve paylaşım izinlerine dikkat edin.

- Çevrim-içi ortamlardan alınan bilgi ve belgeleri kullanırken kaynak göstermeyi unutmayın.

- Bilgisayar ve İnternet kullanım süresini ebeveyn ve/veya öğretmeninizle birlikte belirleyin. Bu süreleri aşan kullanımlardan kaçının. Ayrıca bilgisayar ve İnternet'te 45 dakika vakit geçirdikten sonra mutlaka ara verin. Bu süreçte uzaktaki nesnelere bakmak gözü, gerilme hareketleri yapmak kasları ve eklemleri dinlendirecektir.

Çocukların İnternet'te karşılaşılabilecek risklerden korunması ve güvenli İnternet kullanımlarının sağlanmasında ailelere önemli görevler düşmektedir (Palfrey & Gasser, 2008). Güvenli İnternet kullanımı ve dijital ebeveynlik konusunda yürütülen çalışmalar ailelerin, dijital ebeveynliğin gerektirdiği, çevrim-içi ortamlarda çocukların karşılaşabilecekleri riskler konusunda yeterli bilgiye sahip olmadıklarını göstermektedir (Canbek & Sağıroğlu, 2007; 2014; Kaşıkçı vd., 2014). Çocukları kadar iyi derecede teknoloji kullanamayan ebeveynler, çocuklarını dijital risklerden korumak için yasaklayıcı ve kısıtlayıcı önlemler almaktadırlar. Günümüz ebeveynlerinden İnternet konusunda kısıtlayıcı ve yasaklayıcı olmak yerine, çocuklarına İnternet'i güvenli biçimde kullanmaları konusunda rehberlik etmeleri beklenmektedir (Mitchell, 2010). Bu bağlamda çocukların güvenli İnternet kullanımı konusunda ailelere verilebilecek tavsiyeler aşağıdaki şekilde özetlenebilir:

- Çocuğunuza teknoloji kullanımı imkânı sağlamak görevinizin bittiği değil aslında başladığı yerdir.

- İnternet'i etkin kullanmayı bilmeden çocuğunuzu İnternet'in zararlarından korumanız mümkün değildir. Bu nedenle yeniliklere açık olun ve takip etmeye çalışın.

- İnternet'in uygunsuz kullanımının neden olacağı sorunlar konusunda öncelikle siz bilgi sahibi olun. Karşılaşabilecekleri riskler konusunda açık ve dürüst olarak bilgi paylaşımı yapın.
- İnternet servis sağlayıcınızla iletişime geçerek, güvenli İnternet hizmetini ücretsiz olarak başlatın. Bu hizmete ek olarak İnternet'e bağlanılan cihaza filtreleme programları kurarak zararlı içeriklere erişimi engelleyebilirsiniz.
- İnternet kullanımı konusunda çocuğunuzla birlikte makul kurallar belirleyin ve bu kuralları ilk olarak siz uygulayın.
- Çocuğunuzun İnternet'e ailenin ortak kullanım alanlarında girmesini sağlayın.
- Çocuğunuz için doğal ortamda ilgisini çekecek etkinlikler planlayın. Başka bir ifadeyle çocuğunuzun sanal ortamda fazla zaman geçirmesini önleyecek aile içi etkinlikler düzenleyin.
- Çocuğunuza gizlilik ayarları hakkında bilgi verin. Çevrim-içi ortamlarda paylaşmaması gereken özel bilgileri ve sosyal ağlarda uygulaması gereken gizlilik ayarlarını gösterin.
- Bir sosyal ağa katılmak isteyen çocuğunuzun, ilgili sosyal ağa üyelik için gerekli yaş sınırı vb. koşulları taşıyıp taşımadığını kontrol edin. Ayrıca çocuğunuzun kullandığı sosyal ağlarda sizin de hesabınız olsun. Böylelikle çocuğun paylaşımları ve çevrim-içi arkadaşları hakkında bilgi sahibi olabilirsiniz.
- Sosyal ağlarınızda gizlilik ya da görünürlük ayarlarınızı kontrol edin ve güncel olarak denetleyin. Çocuğunuzla ilgili yapacağınız paylaşımları kimlerin görebileceğine dikkat edin.
- Çocuğunuzu çevrim-içi ortamlarda karşılaştığı olumsuz durumlar hakkında sizi bilgilendirmesi için cesaretlendirin.
- Uygunsuz içerik yayınlayan sitelere, hesaplara karşı duyarsız kalmayın. Uygun olmayan içeriklerle karşılaştığınızda web sayfası yöneticilerine, İnternet servis sağlayıcılara ya da resmi kurumlara konuyla ilgili şikâyetinizi iletin.
- Engelleyici ve yasaklayıcı tedbirlerden kaçının. Bilinçlendirici ve destekleyici tavır takının. Zararlı olanın İnternet'in kendisi değil, barındırdığı uygunsuz içerikler olduğunu unutmayın.

Yansıtma Soruları

1. İnternet bağımlılığı nedir? Aşırı İnternet kullanımının çocuklara zararları nelerdir?
2. Çocukların çevrim-içi ortamlarda karşılaştıkları riskler nelerdir?
3. Dijital ebeveynlerin sahip olması gereken özellikler nelerdir?
4. Güvenli İnternet kavramını tanımlayınız. Çocukların güvenli İnternet kullanımı için alınması gereken önlemleri tartışınız.

Kaynaklar

Agaston, P. W., Kowalski, R., & Limber, S. (2007). Students' perspectives on cyberbullying. *Journal of Adolescent Health, 41*, 59-60.

Akbıyık, C., & Kestel, M. (2016). Siber zorbalığın öğrencilerin akademik, sosyal ve duygusal durumları üzerindeki etkisinin incelenmesi. *Mersin Üniversitesi Eğitim Fakültesi Dergisi, 12*(3), 844-859.

Arıcak, O. T., Siyahhan, S., Uzunhasanoğlu, A., Sarıbeyoğlu, S., Çıplak, S., Yılmaz, N., & Memmedov, C. (2008). Cyberbullying among Turkish adolescents. *Cyberpsychology & Behaviour, 11*(3),253-261.

Ayas, T., & Horzum, M. B. (2012). İlköğretim öğrencilerinin sanal zorba ve mağdur olma durumu. *İlköğretim Online, 11*(2), 369-380.

Çam, H. H., & Nur, N. (2015). Adölesanlarda internet bağımlılığı prevalansı ile psikopatolojik semptomlar ve obezite arasındaki ilişkinin incelenmesi. *TAF Prev Med Bull, 14*(3), 181-189.

Canbek, G., & Sağıroğlu, Ş. (2007). Çocukların ve gençlerin bilgisayar ve İnternet güvenliği. *Politeknik Dergisi, 10*(1), 33-39.

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. 20.03.2018 tarihinde http://yunus.hacettepe.edu.tr/~sadi/yayin/AB11_Celen-Celik_Seferoglu_Cocuklar-Internet-Riskler.pdf, adresinden erişilmiştir.

Çelen, F. K., Çelik, A., & Seferoğlu, S. S. (2016). Ortaokul öğrencilerinin sanal zorbalık ve internet saldırganlığı durumlarının çeşitli değişkenler açısından incelenmesi. *25. Ulusal Eğitim Bilimleri Kongresi (UEBK 2016) Bildiri Özetleri Kitabı, 27-28*. İstanbul Kültür Üniversitesi, Ulusal Eğitim Dernekleri Platformu-ULED ve Pegem Akademi, 21-24 Nisan 2016, Antalya. 20.03.2018 tarihinde http://yunus.hacettepe.edu.tr/~sadi/yayin/UEBK2016_BildiriOzeti_Celen-Celik-Seferoglu.pdf adresinden erişilmiştir.

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. 20.03.2018 tarihinde http://yunus.hacettepe.edu.tr/~sadi/yayin/ICITS2017_Celen-Celik-Seferoglu_Sanal-Ortam-Yalnizligi.pdf adresinden erişilmiştir.

Doğan, D., Çınar, M., & Seferoğlu, S. S. (2017). Sosyal medyanın karanlık yüzleri trollerle ilgili bir inceleme. H. F. Odabaşı, B. Akkoyunlu ve A. İşman (Ed). *Eğitim teknolojileri okumaları 2017*, (45. Bölüm, ss. 887-915). TOJET ve Sakarya Üniversitesi, Adapazarı. 20.03.2018 tarihinde http://yunus.hacettepe.edu.tr/~sadi/yayin/Kitap_ETO2017_Bolum45_887-915_Troller.pdf adresinden erişilmiştir.

Durak, H., & Seferoğlu, S. S. (2016). 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. 20.03.2018 tarihinde http://yunus.hacettepe.edu.tr/~sadi/yayin/Kitap_GencliginUmudu-2016_Durak-Seferoglu_SiberZorbalik_167-187.pdf, adresinden erişilmiştir.

Gökçearslan, Ş., & Günbatar, M. S. (2012). Ortaöğrenim öğrencilerinde internet bağımlılığı. *Eğitim Teknolojisi Kuram ve Uygulama, 2*(2), 10-24.

Gökçearslan, Ş., & Seferoğlu, S. S. (2016). Ortaokul öğrencilerinin internet kullanım biçimleri: Riskli davranışlar ve fırsatlar. *Kastamonu Eğitim Dergisi [Kastamonu Education Journal],*

24(1), 383-404. 20.03.2018 tarihinde http://yunus.hacettepe.edu.tr/~sadi/yayin/Gokcearslan-Seferoglu_Internet-Riskler_KSEF-2016-24.1.pdf adresinden erişilmiştir.

GüvenliWEB (2018). *İnternette hak hukuk ve sorumluluklar.* 10.03.2018 tarihinde http://www.guvenliweb.org.tr/dokuman-detay/internette-hak-hukuk-ve-sorumluluklar adresinden erişilmiştir .

Holloway,D., Green, L., & Livingstone, S. (2013). *Zero to eight. Young children and their Internet use*. LSE, London: EU Kids Online.

Karahisar, T. (2014). İnternet'te çocukları bekleyen riskler ve medya okuryazarlığı. *The Turkish Online Journal of Design, Art and Communication, 4*(4), 82-95

Kaşıkçı, D. N., Çağıltay, K., Karakuş, T., Kurşun, E., & Ogan, C. (2014). Türkiye ve Avrupa'daki çocukların internet alışkanlıkları ve güvenli internet kullanımı. *Eğitim ve Bilim, 39*(171), 230-243

Kavuk, M., & Keser, H. (2016). İlköğretim okullarında siber zorbalık. *Hacettepe Üniversitesi Eğitim Fakültesi Dergisi [Hacettepe University Journal of Education]*, *31*(3), 520-535.

Kayri, M., Tanhan, F., & Tanrıverdi, S. (2014). Ortaöğretim öğrencilerinde İnternet bağımlılığı ile algılanan sosyal destek arasındaki ilişkinin incelenmesi. *Online Journal of Technology Addiction & Cyberbullying, 1*(1), 1-27.

Keser, H., & Kavuk, M. (2015). Okulda siber zorbalık farkındalık anketinin geliştirilmesi. *Kastamonu Eğitim Dergisi, 23*(1), 17-30.

Kılınç, M., & Doğan, A. (2014). Ortaokul 7. ve 8. sınıf öğrencilerinin internet bağımlılığı ile biliş üstü farkındalıklarının çeşitli değişkenler açısından incelenmesi. *Turkish Studies-International Periodical for the Languages, Literature and History of Turkish or Turkic*, *9*(5), 1385-1396

Kıran, E. B. (2009). Çeşitli değişkenlere göre ergenlerde internet bağımlılığının yordanması. *Journal of New World Sciences Academy, 4*(4), 1331-1340.

Li, Q. (2007). New bottle but old wine: A research of cyberbullying in schools. *Computers in Human Behavior, 23*, 1777–1791.

Livingstone, S., & Haddon, L. (2008). Risky experiences for children online: Charting European research on children and the Internet. *Children & Society, 22*(4), 314-323.

Livingstone, S., Haddon, L., Görzig, A., & Olafsson, K. (2011). *EU Kids Online. Final report*. London: EU Kids Online: LSE.

Livingstone, S., Mascheroni, G., & Staksrud, E. (2015). *Developing a framework for researching children's online risks and opportunities in Europe*. London: London School of Economics and Political Science.

Mitchell, K. (2010). Remaining safe and avoiding dangers online: A social media Q&A with Kimberly Mitchell. *The Prevention Researcher*, *17*, 7-9

Müezzin, E. (2017). Lise öğrencilerinde internet bağımlılığının yoksunluk, kontrol güçlüğü, işlevsellikte bozulma ve sosyal izolasyon bağlamında incelenmesi. *Sakarya University Journal of Education, 7*(3), 541-551.

Palfrey, J., & Gasser, U. (2008). *Born digital: Understanding the first generation of digital natives*. New York: Basic Books.

Peker, A. (2013). Ortaokul öğrencilerinin siber zorba ve siber mağdur olma durumu. 5.*Uluslararası Risk Altında ve Korunması Gereken Çocuklar Sempozyumu*'nda sunulan bildiri. Antalya, Türkiye.

Piotrowski, C. (2012). From workplace bullying to cyberbullying: The enigma of e-harassment in modern organizations. *Organization Development Journal, 30*(4), 44.

RTÜK (2013). *Türkiye'de çocukların medya kullanma alışkanlıkları araştırması*. 20.03.2018 tarihinde https://www.rtuk.gov.tr/haberler/3787/18/turkiyede-cocuklarin-medya-kullanma-aliskanliklari-arastirmasi-sonuclandi.html adresinden erişilmiştir.

Sezer, M., Şahin, I., & Aktürk, A. O. (2013). Cyber bullying victimization of elementary school students and their reflections on the victimization. *International Journal of Social, Human Science and Engineering, 7*(12), 1989-1992.

Taylan, H. H., & Işık, M. (2015). Sakarya'da ortaokul ve lise öğrencilerinde internet bağımlılığı. *Turkish Studies-International Periodical for the Languages, Literature and History of Turkish or Turkic, 10*(6), 855-874

Topçu, Ç., Erdur-Baker, Ö., & Çapa-Aydın, Y. (2008). Examination of cyberbullying experiences among Turkish students from different school types. *Cyber Psychology & Behavior, 11*(6), 643-648.

TÜİK (2013). *06-15 yaş grubu çocuklarda bilişim teknolojileri kullanımı ve medya, 2013*. 20.03.2018 tarihinde http://www.tuik.gov.tr/PreHaberBultenleri.do?id=15866 adresinden erişilmiştir.

TÜİK (2015). *Hanehalkı bilişim teknolojileri kullanım araştırması, 2015*. 20.03.2018 tarihinde http://www.tuik.gov.tr/PreHaberBultenleri.do?id=18660 adresinden erişilmiştir.

TÜİK (2016). *Hanehalkı bilişim teknolojileri kullanım araştırması, 2016*. 20.03.2018 tarihinde http://www.tuik.gov.tr/PreHaberBultenleri.do?id=21779 adresinden erişilmiştir.

TÜİK (2017). *Hanehalkı bilişim teknolojileri kullanım araştırması, 2017*. 20.03.2018 tarihinde http://www.tuik.gov.tr/PreHaberBultenleri.do?id=24862 adresinden erişilmiştir.

Valcke, M., Bonte, S., De Wever, B., & Rots, I. (2010). Internet parenting styles and the impact on internet use of primary school children. *Computers & Education, 55*(2), 454-464.

Valcke, M., De Wever, B., Van Keer, H., & Schellens, T. (2011). Long-term study of safe Internet use of young children. *Computers & Education, 57*(1), 1292-130

Young, K. S. (1996). Internet addiction: The emergence of a new clinical disorder. *CyberPsychology and Behavior, 1*(3), 237-244

Yurdakul, I. K., Dönmez, O., Yaman, F., & Odabaşı, H. F. (2013). Dijital ebeveynlik ve değişen roller. *Gaziantep Üniversitesi Sosyal Bilimler Dergisi, 12*(4), 883-896.