

Gönderim Tarihi: 17.12.2024

Kabul Tarihi: 02.05.2025

BİRLEŞMİŞ MİLLETLER ÇOCUK HAKLARINA DAİR SÖZLEŞME VE TÜRK CEZA KANUNU ÇERÇEVESİNDE ÇOCUĞUN DİJİTAL SÖMÜRÜSÜ

The United Nations Convention on the Rights of the Child and Digital
Exploitation of the Child within the Framework of the Turkish Penal Code

Siğnem BAĞCI

Bil. Uzm.; MEB

bagcisignem@gmail.com

ORCID ID: 0000-0002-9696-3930

Mehmet BOZTEPE

Dr.; İçişleri Bakanlığı

mboztepe@msn.com

ORCID ID: 0000-0002-9739-993X

Çalışmanın Türü: Araştırma

Öz:

Dijital dünya, günümüzde milyonlarca insanın günlük yaşamının ayrılmaz bir parçası haline gelmiştir. Çevrimiçi aktivitelerin, iletişimi kolaylaştırma, güncel olaylar hakkında hızlı bilgi akışını sağlama, toplumsal bir bilinç yaratabilme, bireylerin farklı kültürlerden gelen bilgilere ve deneyimlere kolayca erişebilmesi gibi imkanlar sağlayarak topluma faydalı etkileri göz önüne alınsa da, özellikle çocuklar üzerinde olumsuz etkileri göz ardı edilemez. Çocukların gelişimi ve ruh sağlığı üzerindeki tehlikelere ek olarak hak ihlali de bu olumsuz etkilerden biridir. Çocuk hakları açısından, Birleşmiş Milletler Çocuk Haklarına Dair Sözleşme ve Türk Ceza Kanunu çerçevesinde çocukların dijital platformlarda güvenliğinin sağlanması önemlidir. Bu makalede, dijital dünyada çocuk haklarının ihlali üzerinde durulmuş ve çocukların dijital platformlarda karşılaştığı riskler ile bunlardan korunma yolları tartışılmıştır. Bu risklerle başa çıkmak için ebeveynler, eğitimciler ve toplumun ortak bir çaba içinde olması gerekmektedir. Nitel, betimleyici ve doküman analizine dayalı bir literatür çalışması olan bu makalede, sosyal medyada çocukların verilerinin paylaşılmasının tehlikeli sonuçları, çocuk hakları çerçevesinde tartışılacak ve bu konuda ebeveynlerin, eğitimcilerin ve toplumun sorumlulukları ele alınmıştır.

Anahtar Kelimeler: Çocuk hakları, kişisel veriler, sosyal medya, çocuk istismarı, veri gizliliği

Abstract:

The digital environment has become a pervasive and indispensable element of contemporary life, shaping not only modes of communication but also access to information, cultural exchange, and social interaction. Despite its transformative potential, the digital realm presents significant challenges — particularly for children — whose cognitive, emotional, and social development renders them uniquely vulnerable. Among the most pressing concerns are infringements upon children's rights, which manifest through data exploitation, exposure to inappropriate content, and digital surveillance. Within the normative frameworks established by the United Nations Convention on the Rights of the Child and the Turkish Penal Code, safeguarding children's well-being in online spaces emerges as an ethical and legal imperative. This

article critically examines the multifaceted risks encountered by children in digital contexts, the nature and scope of rights violations, and proposes a multidimensional approach to protection that necessitates active engagement from caregivers, educators, policymakers, and civil society. This article, which constitutes a literature review grounded in qualitative, descriptive, and document analysis methods, examines the potential risks associated with the sharing of children's data on social media within the framework of children's rights. Additionally, it explores the responsibilities of parents, educators, and society regarding this issue.

Keywords: Children's rights, personal data, social media, child abuse, data privacy

1. GİRİŞ

Sosyal medya, günümüzde milyonlarca insanın günlük yaşamının ayrılmaz bir parçası haline gelmiştir. İnsanların birbirleriyle bağlantı kurmasını, bilgi alışverişi yapmalarını ve kültürel deneyimleri paylaşmalarını sağlaması yönüyle toplum üzerinde derin bir etkiye sahiptir. Bu etki oldukça çeşitlidir ve birçok farklı boyutta görülebilmektedir. İletişimi kolaylaştıran yönüyle, dünya genelindeki insanları bir araya getirebilmekte ve güncel olaylar hakkında hızlı ve geniş kapsamlı bilgi akışını sağlamaktadır. Toplumsal değişim ve aktivizmi desteklemek için güçlü bir araç olması nedeniyle sosyal medya üzerinden toplumsal bir bilinç yaratılabilmektedir. Bireylerin farklı kültürlerden gelen bilgilere ve deneyimlere kolayca erişmesiyle toplumdaki kültürel anlayışın artırılması, hoşgörüyü destekleme gibi etkiler gözlemlenmektedir.

Ancak, bu dijital platformların olumlu birçok işlev ve etkisinin yanı sıra olumsuz yansımaları üzerine endişeler bulunmaktadır. Sosyal medyanın kullanımı, bireylerin duygusal ve psikolojik sağlığı üzerinde olumsuz etki yaratabilmektedir. Sosyal medyada görülen mükemmeliyetçilik, karşılaştırma ve sosyal onay arayışı gibi unsurlar, bazı insanlarda stres, endişe ve düşük özsaygı gibi sorunlarla karşılaşılmasını sağlamaktadır (Fardouly vd., 2015). Sosyal medyanın aşırı kullanımı, depresyon, anksiyete ve düşük özsaygı gibi zihinsel sağlık sorunlarıyla ilişkilendirilmiştir (Twenge ve Campbell, 2018). Bazı araştırmalar, sosyal medya kullanımının yüz yüze etkileşimleri azaltabileceğini ve kişiler arasındaki ilişkileri zayıflatabileceğini, iş ve okul performansını olumsuz yönde etkileyerek zaman yönetimi sorunlarına neden olabileceğini göstermektedir (Rosen vd., 2013; Kross vd., 2013). Sosyal medyada uzun süreli aktif durumda olmanın kısa dönemli dikkat ve odaklanma yeteneklerini azaltabileceği dolayısıyla bilişsel işlevleri olumsuz yönde etkileyebileceği belirtilmektedir (Alloway ve Alloway, 2012). Bu gibi birçok olumsuz etkinin en önemlilerinden biri de, sosyal medya platformlarında kişisel veri paylaşımının yol açacağı mahremiyet ihlalleri ile kişisel güvenliği tehlikeye atabilmesidir (Dwyer vd.,

2007).

Dijital çağın çocuk haklarını geliştirip güçlendirme veya zayıflatması konusunda tartışmalar sürmektedir. Mevcut tartışmalar çocukların çevrimiçi mahremiyet hakları, bilgi ve ifade özgürlüğü, cinsel saldırılardan korunma hakları ve internetin çeşitli biçimlerde aracılık ettiği ve güçlendirdiği saldırgan tehditler üzerinde yoğunlaşmaktadır. Bilgi paylaşımı ve gizlilik konusunda giderek artan endişeler, özellikle çocukların verilerinin paylaşılması konusunda önemli bir tartışma noktası haline gelmiştir.

2. ARAŞTIRMA YÖNTEMİ

Bu çalışma, nitel araştırma yöntemlerinden literatür taraması tekniğine dayanmaktadır. Araştırmada, çocukların dijital dünyadaki hak ihlallerine ilişkin mevcut bilgi birikiminin derinlemesine incelenmesi amaçlanmıştır. Bu doğrultuda, Birleşmiş Milletler Çocuk Haklarına Dair Sözleşme, Türk Ceza Kanunu, Kişisel Verilerin Korunması Kanunu (KVKK) gibi ulusal ve uluslararası mevzuatlar ile konuya ilişkin akademik yayınlar incelenmiştir. Literatürde yer alan kuramsal ve yasal çerçeveler analiz edilerek çocukların dijital ortamlarda maruz kaldığı riskler ve hak ihlalleri üzerine kavramsal bir değerlendirme sunulmuştur. Çalışma, özgün veri toplama süreçleri (anket, görüşme, saha araştırması vb.) içermemekte olup, eldeki bilgilerin derlenmesi ve yorumlanması üzerine yapılmıştır.

2.1. Araştırmanın Sınırlılıkları

Bu çalışmanın bazı sınırlılıkları bulunmaktadır. Öncelikle, araştırma ampirik veri içermemekte, yalnızca mevcut literatür, mevzuat ve ikincil kaynaklar üzerinden yürütülmektedir. Bu durum, elde edilen sonuçların uygulama düzeyinde test edilmesini ve genellenmesini zorlaştırmaktadır. Ayrıca, çalışmanın büyük oranda Türkiye bağlamında ele alınmış olması, farklı kültürel, hukuki ve dijital ortamlarda geçerliliğini sınırlayabilir. İncelenen literatürün bir kısmı görece eski tarihli olup, dijital teknolojilerdeki hızlı değişim göz önüne alındığında bazı bulguların güncelliği zaman içinde azalabilir. Bu bağlamda, çalışmanın bulguları, kavramsal bir çerçeve sunmakla birlikte, geniş çaplı ampirik araştırmalarla desteklenmeye ihtiyaç duymaktadır.

3. BİRLEŞMİŞ MİLLETLER ÇOCUK HAKLARINA DAİR SÖZLEŞME

Birleşmiş Milletler Çocuk Haklarına Dair Sözleşme (BMÇHS), çocukların temel haklarını korumayı ve geliştirmeyi amaçlayan uluslararası bir belgedir. Bu sözleşme, çocukların yaşam, gelişim, korunma ve katılım

haklarını güvence altına alır. Birleşmiş Milletler Genel Kurulu tarafından 20 Kasım 1989 tarihinde imza onay ve katılıma açılan Çocuk Hakları Sözleşmesi, 2 Eylül 1990 tarihinde yürürlüğe girmiştir. Birleşmiş Milletler Çocuk Hakları Sözleşmesi'ne göre 18 yaşına kadar her insan çocuk sayılır ve çocukları ilgilendiren tüm faaliyetlerde çocuğun yüksek yararı dikkate alınır. Sözleşmeye taraf devletlerin kabul ettiği temel hak, çocuğun yaşama hakkıdır. Sözleşme uyarınca taraf devletler, çocuğun korunması ile ilgili gerekli tüm önlemleri almaktan, çocuğun güvenliği ve bakımından sorumlu kurum ve kişileri destekleme ve denetlemekten sorumludur.

Türkiye dahil olmak üzere 196 ülkenin taraf olduğu sözleşme, en fazla ülkenin onayladığı insan hakları belgesidir. Türkiye, 14 Aralık 1994 tarihinde Birleşmiş Milletler Çocuk Haklarına Dair Sözleşme'yi imzalayarak ve 14 Eylül 1995 tarihinde de onaylayarak kabul etmiştir. Bu adım, Türkiye'nin çocukların haklarını korumaya ve geliştirmeye olan taahhüdünü uluslararası alanda resmileştirmiştir. Sözleşme, Türkiye'nin çocukların yaşam hakkını, eğitim hakkını, sağlık hakkını, ayrımcılık yapmama hakkını, isyan hakkını, özel yaşamın gizliliği hakkını ve daha pek çok temel hakkını güvence altına almasını gerektirmektedir.

Birleşmiş Milletler Çocuk Haklarına Dair Sözleşme Genel Yorum No.13 (2011) incelendiğinde bilgi ve iletişim teknolojileri aracılığıyla şiddet içeren alanların aşağıdaki şekilde sıralandığı görülmektedir (IV/31):

- Bilişim teknolojileri ve internet vasıtasıyla üretilen işitsel ve görsel materyaller üzerinden çocukların cinsel istismarı,
- Çocukların düzmece video ve fotoğraflarının ahlaka aykırı şekilde üretimi,
- Çocuklarla alay eden materyallerin hazırlanması, gösterilmesi, alınması, alınmasına izin verilmesi, reklam edilmesi veya elde bulundurulması,
- Çocukların, saldırgan, nefret ve şiddet içeren, ırkçı, pornografik, yanlış sürükleyici zararlı bilgilerle, reklamlarla ve ilanlarla karşılaşması,
- İnternet üzerinden başka çocuklarla temasa geçen çocukların, kötü şakalara, tacize veya zorbalığa maruz kalması, kişisel bilgilerini ve/veya cinsel içerikli görüntülerini vermek ya da tanımadıkları yabancılarla dış dünyada buluşmak için ikna edilmeleri veya zorlanmaları,
- Çocukların kendilerinin taciz ve zorbalık eylemlerinde bulunmaları, uygunsuz cinsel içerikli materyaller hazırlayıp paylaşmaları,

- Psikolojik gelişimlerini olumsuz yönde etkileyecek oyunlar oynamaları, yasa dışı materyalleri indirmeleri,
- Yanlış yönlendirme ve bilgilendirmelerde bulunmaları, kumar oynamaları, bilgisayar korsanlığı yapmaları, terör içerikli eylemlere girmeleri.

Birleşmiş Milletler Çocuk Haklarına Dair Sözleşme Genel Yorum No.14 (2013) uyarınca, Taraf Devletlerin Yükümlülüklerinin Mahiyeti ve Kapsamı başlığı altında “Kitle iletişim araçlarını, sosyal medyayı ve çocukları da işin içine katan ve çocukların hak sahipleri olarak tanımlanmasını amaçlayan iletişim programları aracılığıyla çocuğun yüksek yararının değerlendirilmesi ve birinci planda dikkate alınması hakkının gerçekleşmesini engelleyen tüm olumsuz tutum ve algılara karşı mücadele edilmesi.” maddesi yer almaktadır. Birleşmiş Milletler Çocuk Haklarına Dair Sözleşme Genel Yorum No.15 (2013), Kitle İletişimi ve Sosyal Medya başlığı altında “Sözleşme’nin 17. Maddesi, kitle iletişim araçlarına sahip kuruluşların sorumluluklarını belirlemektedir. Sağlık açısından bakıldığında bu sorumluluklar genişletilerek aşağıdakileri de kapsayacak duruma getirilebilir: çocuklar arasında sağlığı ve sağlıklı yaşam tarzlarını yaygınlaştırma; sağlığın geliştirilmesine yönelik reklam ve ilanlara ücretsiz yer ayrılması; çocukların ve ergenlerin özel yaşamlarının gizliliğini gözetme; bilgiye erişimi arttırma; çocuk ve genel sağlık açısından zararlı iletişim programlarından ve materyallerinden kaçınma ve sağlık alanındaki sorunların insanlar için damgalanma nedeni olmasına izin vermeme.” ifadelerine yer vermiştir.

Türk Ceza Kanunu’nun hükümleri arasında da çocukların dijital platformlarda sömürülmesini önlemeyi amaçlayarak, çocukların güvenliğini korumaya yönelik ifadelere rastlanmaktadır. Bu hükümler aşağıda sıralanmaktadır.

- Türk Ceza Kanunu’nun 105/A maddesi, çocukların güvenliğini tehdit eden davranışları düzenler. Bu maddeye göre, çocukları tehlikeye sokan veya çocuklara zarar veren dijital veya fiziksel eylemler suç teşkil eder.
- Türk Ceza Kanunu’nun 103/A maddesi, çocuklara karşı kötü muamele suçlarını düzenler. Bu maddeye göre, çocukları cinsel içerikli mesajlarla taciz etmek, tehdit etmek veya rahatsız etmek suç teşkil eder. Çocukların dijital platformlarda ticari amaçlarla istismar edilmesi de, bu hüküm altında değerlendirilebilir.
- Türk Ceza Kanunu’nun 226. maddesi, çocuk pornografisi suçunu düzenler. Bu maddeye göre, çocukların cinsel istismarını içeren

materyalleri üretmek, bulundurmak, yaymak veya ticaretini yapmak suçtur. İnternet üzerinden çocuk pornografisinin yayılması da bu suç kapsamında değerlendirilir.

- Türk Ceza Kanunu'nun 105. maddesi, çocuklara karşı internet üzerinden cinsel saldırı ve taciz suçlarını düzenler. Bu maddeye göre, çocuklara karşı cinsel içerikli mesajlar göndermek, çocukların cinsel istismarını içeren materyalleri paylaşmak veya çocukları cinsel amaçlı olarak ikna etmek suç teşkil eder.
- Türk Ceza Kanunu'nun 103. maddesi, çocuklara karşı cinsel istismar suçlarını düzenler. Bu maddeye göre, cinsel amaçlı olarak çocukların cinsel bedenini kullanmak, izinsiz görüntü veya ses kaydı almak veya yaymak gibi eylemler suç teşkil eder. Bu hükümler, çocukların dijital platformlarda istismarını önlemeyi amaçlar.
- Çocuk İşçiliğinin Önlenmesine Dair Kanun (ÇİÖK): Türk Ceza Kanunu'ndan ziyade, çocuk işçiliğinin önlenmesine dair daha kapsamlı düzenlemeler içeren özel bir kanundur. Bu kanun, çocuk işçiliğini önlemek ve çocukların eğitimlerine zarar gelmemesini sağlamak amacıyla çeşitli düzenlemeler getirir. Dijital ortamda çocukların ticari amaçla istismar edilmesi bu kanun kapsamında ele alınabilir.

4. DİJİTAL ORTAMDA ÇOCUKLARIN KİŞİSEL VERİLERİ

Bilgi işlem çağında, yüksek düzeyde sosyal medya kullanımı ve sensör gömülü fiziksel ortamlar (kapalı devre televizyon [CCTV] kameraları, trafik akışı monitörleri ve drone'larla donatılmış halka açık alanlar dahil), insanların davranışları ve bedenleri hakkındaki dijital veriler, kendileri ve başkaları tarafından durmaksızın üretilmektedir. 'Dijital gözetleme' terimi, çevrim-içi ayak izinin anlık veya geçmişe dönük görüntülenmesi, işlenmesi ve listelenmesi olarak tanımlanabilmektedir (Chadwick & Howard, 2010; Marx, 2003; Raley, 2013; Van Dijck, 2014). Dijital gözetleme, bireylerin kendi kendini takip eden cihazlar ve yazılımlar kullanarak gönüllü olarak seçilmiş olabileceği gibi (Albrechtslund ve Lauritsen, 2013; Lupton, 2016a, 2016b), veri sahibi kişi yada kişilerin bilgi ve isteği dışında da gerçekleşebilmektedir. Bu kişisel verilerin dijital veri ekonomisinin bir parçası haline gelme eğiliminde olmaları, çeşitli kişi ve kurumlar tarafından, verilerin ait olduğu kişilerin genellikle bilmediği şekillerde kullanılabilmesi için yalnızca bir kez toplanmaları yeterlidir (Kitchin, 2014; Lupton, 2015, 2016).

Bu veri toplama ve işleme ortamında, çocukların sıklıkla hak mağduriyetine maruz kaldıkları görülmektedir. Dijital teknolojilerin ortaya

çıkışı ve gelişmesiyle çocuklar daha önce hiç olmadığı kadar izlenmeye açık hale gelmiştir. Çocuğun izlenmesi ve kişisel verilerinin toplanması doğum öncesine bile tarihlenebilmektedir. Ebeveynler arasında ultrason görüntülerini, fetüsün gelişimini, hareketlerini, hatta kalp atışlarını çeşitli uygulamalarla paylaşmak, doğum anını fotoğraf ve videolarla YouTube, Facebook, Instagram ve hamilelikle ilgili 1000'den fazla uygulama gibi halka açık dijital ortama yüklemek oldukça popüler hale gelmiştir (Leaver, 2016; Lupton, 2013; Lupton ve Thomas, 2015). Bebeğin doğumundan sonra da uyku ve beslenme düzeni, gelişimi, büyümesi ve sağlığı gibi konulardaki bilgiler ebeveynler için geliştirilen uygulamalarla izlenebilmekte, sensörlü ve kameralı bebek bakım eşyaları ve oyuncaklar yoluyla, bebeğin kalp ve solunum hızı, uyku sırasındaki vücut pozisyonu, cilt sıcaklığı gibi biyometrik verilerini kaydederek ebeveynlerin telefonlarına anlık olarak gönderilebilmektedir. Ebeveynlerin doğumdan itibaren bebeğinin çok sayıda dijital fotoğraf ve videosunu çekerek sosyal medya sitelerinde paylaşması, bebeğin doğumundan önce bebek adına sosyal medya profili oluşturulmasına kadar varmaktadır (Ammari vd., 2015; Holloway vd., 2013). 2010 yılında AVG Teknoloji'nin yaptığı araştırmaya göre çocukların henüz 6 aylıkken dijital kimlik kazandıkları belirlenmiştir (AVG Technologies, 2010). Benzer araştırmalar çocukların mobil dijital cihazları, özellikle de akıllı telefonlar, tablet ve bilgisayarları bebeklik döneminde kullanmaya başladıklarını göstermektedir (Holloway vd., 2013). Çocukların büyümesiyle gelişim, sağlık ve fiziksel aktiviteleri yine uygulamalar üzerinden izlenmeye devam etmektedir. Bebeğin tek başına hareket edebilir hale gelmesiyle saat ve bileklik gibi giyilebilir dijital cihazlarla tanışan bir çocuğun dakikada 1000 ölçümü alınabilmektedir. Çocukların coğrafi konum, yaş, cinsiyet ve uygulamayı kullanma tarzı dahil olmak üzere kişisel verilerini rutin olarak toplamakta olan uygulama ve cihazlar, konuşma tanıma yazılımı ve Wi-Fi ile donatılma gibi özelliklerle etkileşimi teşvik etmektedir (Timms, 2015). Oyuncakların tehlikesi ise "My Friend Carla" isimli oyuncak bebek üzerine yapılan tartışmalar ile anlaşılabilir. "My Friend Carla" adlı oyuncak bebeğin, çocukların kişisel gizliliğini ihlal etme ve güvenlik riski oluşturma tehlikesi nedeniyle yasaklanması istenmiştir. Bu oyuncak bebek, internet bağlantısı üzerinden çocuklarla etkileşim kurabilen bir yapay zeka ürünüdür. "My Friend Carla" adlı oyuncak bebek, çocukların seslerini tanıyabilen, konuşabilen ve hatta sohbet edebilen bir yapay zeka özelliğine sahip olması nedeniyle oyuncakların internet üzerinden çocukların seslerini ve konuşmalarını kaydedebileceği, bu bilgileri yetkisiz kişilerle paylaşabileceği veya kötü niyetli amaçlarla kullanabileceği endişesi yaratmış ve yasaklanma talepleri ortaya çıkmıştır.

Sosyal medyada çocukların kişisel verilerini paylaşan ebeveynler üzerine pek çok araştırma mevcuttur. Çocuklarının fotoğraflarını sosyal medyada yayınlayan annelerin yalnızlık hissini aşmak, dijital ortamda bir gruba ait olmak, günlük tutmak, motivasyon hissini yaşamak gibi amaçlarla hareket ettiği görülmektedir (Parmaksız, 2012). Bunun yanı sıra ebeveynlerin ticari kaygıyla, diğer ebeveynlerle bilgi paylaşımı amacıyla veya sadece hoş vakit geçirmek için çocuklarının görüntülerini sosyal medya üzerinden paylaştığı belirlenmiştir (Erişir ve Erişir, 2018). İngiltere’de 2000 ebeveynin katılımıyla yapılan bir araştırmaya göre ise ebeveynler çocukları ile ilgili yılda yaklaşık 195 fotoğraf paylaşmakta ve paylaşımlarının gizliliği konusunda endişe duymamaktadır (Aktaran Çimke vd., 2018: 264). Dolayısıyla anne babaların sosyal medyada çocuklarının verilerini paylaşımlarının tehlikeleri konusunda bilinçlendirilmesi gerekmektedir.

Çocukların okula başlamasıyla eğitimsel ilerlemelerinin ve sonuçlarının yazılım kullanılarak izlenmesi, alışlageldik bir durum haline gelmiştir. Veri kümelerini eğitim politikasına katkıda bulunmak için kullanmak amacıyla geliştirilmiş ve ayrıntılı veriler içeren yazılımlarla çocuğun tüm eğitim hayatının, zihinsel, sosyal becerileri ve ruh sağlıkları da dahil olmak üzere izlenmesi mümkündür (Simon, 2014). Okulların sosyal medya kullanımıyla çocuğun okulu ve giriş çıkış saatleri gibi bilgiler de kamu erişimine açıktır. Dolayısıyla çocukların bedeni, zihinsel aktiviteleri, yaşam tarzları iyi niyetli ya da art niyetli kişi ve kurumlar tarafından tehlikeli boyutta görüntülenebilir ve gözlemlenebilir hale gelmiştir.

4.1. Çocukların Kişisel Verilerini Dijital Ortamlarda Paylaşmanın Risk ve Olumsuzlukları

Birçok yetişkin, çocuklarının fotoğraflarını ve kişisel bilgilerini sosyal medya platformlarında paylaşmanın zararsız olduğunu, aksine iletişim ve bilgi paylaşımı ile çocuğun gelişimi için faydalı olabileceğini düşünebilmektedir. Ancak çocuk verilerinin ebeveynler, öğretmenler ve kurumlar tarafından sosyal medyada kontrolsüzce paylaşılması çocukların mahremiyetini ve güvenliğini koruma noktasında ciddi hak ihlallerine ve risklere yol açabilir. Özellikle çocukların kimlik avı ve diğer çevrimiçi tehlikelere karşı savunmasız oldukları ve bu paylaşımların istenmeyen kişilerin hedefi haline gelmelerine neden olabileceği unutulmamalıdır. Çocukların itibar kaybı, ticari yönden istismar, kimlik hırsızlığı, siber saldırılara açık hale gelme gibi olumsuzluklarla karşı karşıya gelmesi sosyal medya platformlarının güvenlik açıkları düşünüldüğünde oldukça büyük bir olasılıktır (Macenaite, 2017). Kişisel verilerinin paylaşımı için çocuğun rızasını alma vurgulanan bir kavram olsa da çocukların bu verilerin ne

şekilde kullanılacağını ve kişisel verilerinin işlenmesiyle meydana gelebilecek riskleri ve tehlikelerini tam olarak öngörmesi mümkün olmayacaktır.

Çocuk verilerinin sosyal medya platformlarında kontrolsüzce paylaşımının tehlikeleri birçok farklı boyutta karşımıza çıkabilmektedir. Bu makalede boyutlar gizlilik ihlali, çevrimiçi taciz ve zorbalık, kimlik hırsızlığı ve dolandırıcılık, psikolojik etkiler ve uzun vadeli etkiler olarak ele alınacaktır.

4.1.1. Gizlilik İhlali:

Kişisel verilerin gizlilik ihlali, bir bireyin kişisel bilgilerinin izinsiz veya hukuka aykırı bir şekilde toplanması, işlenmesi, kullanılması veya ifşa edilmesi durumunu ifade etmektedir. Bir kişinin gizliliğinin ihlal edilmesi genellikle kişinin rızası olmadan gerçekleşir. Bu durum, hem bireyin kişisel haklarını hem de güvenliğini tehdit eder ve çeşitli olumsuz sonuçlara yol açabilir. Kişisel verilerin gizlilik ihlali, birçok ülkede yasal düzenlemelerle korunmaktadır. Türkiye'de kişisel verilerin gizliliği ve korunmasıyla ilgili temel yasa, 6698 sayılı "Kişisel Verilerin Korunması Kanunu"dur. Bu kanun, 7 Nisan 2016 tarihinde kabul edilmiş ve 7 Nisan 2018 tarihinde yürürlüğe girmiştir. Kişisel Verilerin Korunması Kanunu (KVKK), Türkiye'deki kişisel verilerin işlenmesi, korunması ve kullanılmasına ilişkin esasları düzenlemektedir. KVKK'nın temel hedefleri:

- Kişisel verilerin işlenmesi sırasında bireylerin haklarını korumak ve gizliliğini sağlamak,
- Kişisel verilerin hukuka uygun, adil ve dürüst bir şekilde işlenmesini sağlamak,
- Kişisel verilerin korunması için gerekli güvenlik önlemlerini almak ve veri ihlallerini önlemek,
- Kişisel verilerin toplanması ve kullanılmasında açık rıza ilkesini teşvik etmektir.

Çocuğun kişisel verilerini korumak, ailenin ve yetişkinlerin sorumluluğundadır. Çocukların güvenliğini sağlamak için çeşitli önlemler almak önemlidir. Çocuğun kendisi, ebeveynleri, öğretmenleri ve sosyal çevresinde yer alan diğer kişiler tarafından dijital dünyaya bırakılan verileri, çocuk hakkında kötü niyetli kişi ve kurumlar tarafından ulaşılabilecek birçok bilgiyi içermektedir. Bu bilgiler kimlik, görüntü, konum gibi kişisel olabileceği gibi, karakter özellikleri, sosyal çevreleri, duyguları, iletişim biçimleri, ilgi ve ihtiyaçları gibi bilgiler de olabilmektedir. Çocuğun karakter özellikleri, ilgi ve ihtiyaçları, hobileri gibi özel yaşamına dair bilgiler

istismarcılar tarafından çocukla iletişime geçme ve çocuklar tarafından güven kazanma amacıyla sıklıkla kullanılmaktadır. Okul, ev, kurs gibi konum bilgilerinin paylaşımı ise çocukları fiziksel olarak ulaşılma ve yakınlık kurulmaya açık hale getirmektedir (Morgan, 2018).

Yalnızca bireyler tarafından değil internet şirketlerinin veri ihlalleri veya veri sızıntısı da yaygın olarak karşımıza çıkmaktadır. Kötü niyetli siber saldırılar sonucu hackleme olayları düzenli olarak gerçekleşmesiyle yetişkin ve çocuklar hakkında çok özel ayrıntılar elde edilmektedir (McCarthy, 2013; Rosenzweig, 2012). 2020 yılında ortaya çıkan ve TikTok'un kullanıcı verilerini Çin hükümeti ile paylaşmakla suçlandığı dava bu duruma örnek gösterilebilir.

TikTok'un, çocukların kişisel verilerini topladığı ve bu verileri izinsiz olarak paylaştığı iddialarıyla Federal Ticaret Komisyonu (FTC) tarafından soruşturma altına alındığı bilinmektedir. Bu dava ile özellikle ABD'de, TikTok'un sahibi olan Çin merkezli ByteDance şirketinin, kullanıcıların kişisel verilerini Çin hükümetiyle paylaşabileceği endişesiyle birçok tartışma ve soru işareti ortaya çıkmıştır.

4.1.2. Çevrimiçi Taciz ve Zorbalık

Çocukların çevrimiçi taciz ve zorbalığa uğrama tehlikesi, internetin anonim ve geniş kapsamlı yapısı nedeniyle önemli bir endişe kaynağıdır. İnternet, çocukların sosyal ilişkilerini geliştirmeleri, eğlenmeleri ve öğrenmeleri için faydalı bir ortam sunsa da, aynı zamanda zararlı içeriklere ve kötü niyetli kişilere maruz bırakma riskini taşımaktadır. Çocuklar dijital ortamdaki fotoğraf ve bilgileri sayesinde, çevrimiçi tacizcilerin ve zorbaların hedefi haline gelebilmektedir. Bu kişiler, çocuğun kişisel bilgilerini ve fotoğraflarını kullanarak taciz edebilir, zorbalık yapabilir veya istismar edebilir (Livingstone ve Smith, 2014).

Siber zorbalık, diğer çocuklar tarafından alay edilme, tehdit edilme veya aşağılanma şeklinde olabileceği gibi sosyal medya hesabına kötü niyetli mesajlar gönderilmesi veya sansasyonel içeriklerin paylaşılması gibi durumlar ile de örneklendirilebilir. Tacizciler, çocuklarla sanal platformlarda iletişim kurarak kişisel bilgilerini toplayabilmekte, manipüle ve istismar edebilmektedir. Örneğin, bir çocuğun, kendisine güven duymasını sağlayarak kişisel bilgilerini paylaşmasını sağlayan bir tacizci, çocuğu istismar etmek için bu bilgileri kullanabilir. Çocuklar, internet üzerinde tanımadıkları kişilerle yanlış sonuçlar doğurabilecek arkadaşlıklar kurabilmektedir. Bu arkadaşlıklar, çocukların güvenliklerini tehdit edebilir ve istenmeyen durumlarla karşılaşmasına yol açabilir.

4.1.3. Kimlik Hırsızlığı ve Dolandırıcılık

İnternet, çocukların kişisel ve finansal bilgilerini ele geçirmek isteyen kötü niyetli kişiler için birçok fırsat sunmaktadır. İnternetin yaygınlaşması ve çocukların dijital ortamlarda daha fazla zaman geçirmesi, bu tehlikenin artmasına neden olmuştur. Kimlik hırsızlığı, çocukların adı, adresi, telefon numarası, doğum tarihi gibi hassas bilgilerinin çalınması ve bir kişinin kişisel bilgilerinin izinsiz şekilde ele geçirilip kullanılması anlamına gelir. Örneğin, ebeveynlerin sosyal ağlara yüklediği çocuklarına dair video ve fotoğrafların, üçüncü kişiler tarafından kendi sosyal medya hesaplarında kendi çocuklarının görüntüleri gibi paylaşılması rastlanan bir durumdur (Aktaran: Yavuz, 2020). İnternet üzerinden yapılan dolandırıcılık ise, çocukların güvenlik açıklarını kullanarak kandırılmasını, sahte web siteleri veya uygulamalar aracılığıyla maddi zarara uğratılmasını veya istismar edilmesini içerebilmektedir (Højgaard, 2003). Yetişkinler şirketlerin kişisel ayrıntılarını nasıl istismar ettiği ve istihdama, sigortaya, sosyal yardıma, özel tekliflere ve krediye erişim kararlarında kullanılmak üzere ayrıntılı profiller oluşturmak için bunları nasıl kullandıklarına dair genellikle çok az bilgiye sahiptir. (Crawford ve Schultz, 2014). Verileştirme yoluyla, çocukların bedenleri ve davranışları hakkındaki bilgiler, insan bedeninin ticari olarak sömürüldüğü dijital bir veri modu olan biyosermaye biçimine dönüştürülmektedir (Lupton, 2016). Verilerin toplanması ve ticari kuruluşlar tarafından işlenmesi, mahremiyet ve gizlilikle ilgili çeşitli tehlikelere fırsat verebilir. Hedefli reklamcılık, profil çıkarma, reklam ve pazarlama amacıyla toplanan ve işlenen veriler, çocukların mahremiyet hakkına hukuka aykırı veya keyfi müdahalelere yol açabilmektedir. Bu durum onların gelecekteki yaşamlarını da etkilemeye devam edebilecek olumsuz sonuçlar doğurabilir. Elde edilen verilerin, sahte hesaplar açmak, kredi kartı bilgilerine erişmek veya diğer dolandırıcılık faaliyetlerinde kullanılması sıklıkla karşılaşılan bir sorundur. Eğitim ortamlarında ise veri gösterge tablolarının ve diğer veri görselleştirme biçimlerinin kullanılması, çocuklar hakkındaki verileri, yükseltmeler ve kişiselleştirilmiş özelliklerle bir değer biçimine, sınıfları küçük dijital ekonomilere ve kişisel bilgilerin paylaşıldığı hesaplama alanlarına dönüştürmektedir. Çocukların internet üzerinden kimlik hırsızlığı ve dolandırıcılık tehlikesine maruz kalma olasılığını artıran bazı faktörler aşağıdaki şekilde örneklendirilebilir:

- Sahte Web Siteleri ve Uygulamalar: Sahte bir oyun veya uygulama indiren bir çocuk, kişisel bilgilerini veya ebeveynlerinin kredi kartı bilgilerini girerek dolandırıcılık faaliyetlerine maruz kalabilir.

- Sosyal Medya ve İletişim Uygulamaları: Çocuklar, sosyal medya platformlarında veya iletişim uygulamalarında kişisel bilgilerini paylaşırken dikkatli olmalıdırlar. Kimlik hırsızları ve dolandırıcılar, sosyal medya aracılığıyla çocukları manipüle ederek kişisel bilgilerini veya ailelerinin finansal bilgilerini çalmaya çalışabilirler.
- Bilgisayar Virüsleri ve Zararlı Yazılımlar: Çocukların, zararlı web sitelerine veya e-posta eklerine girişleri ile bilgisayar virüsleri veya zararlı yazılımlar, bilgisayarı ele geçirerek kişisel bilgilerini çalabilir veya kötü niyetli faaliyetlerde bulunabilir.
- Phishing Saldırıları: Çocuklar, sahte e-postalar veya mesajlar aracılığıyla yapılan phishing saldırılarına maruz kalabilirler. Bu saldırılar, çocukları kişisel bilgilerini paylaşmaya veya sahte web sitelerine yönlendirmeye teşvik edebilir.
- Sosyal Mühendislik: Sosyal mühendislik, dolandırıcıların çocukları manipüle etmek için kullanabilecekleri bir tekniktir. Örneğin, bir dolandırıcı, çocuğu güven kazanarak kişisel bilgilerini veya ailelerinin finansal bilgilerini ifşa etmeye ikna edebilir.
- Oyun ve Sanal Dünya Dolandırıcılığı: Çocuklar, çevrimiçi oyunlar ve sanal dünyalar aracılığıyla dolandırıcılık tehlikesiyle karşılaşabilirler. Örneğin, bir çocuğun oyun içi karakterini veya eşyalarını çalmak için sahte bir takas teklifi sunulabilir.

Bu örnekler, çocukların internet üzerinden kimlik hırsızlığı ve dolandırıcılık tehlikesine maruz kalabilecekleri çeşitli senaryoları göstermektedir. Bu nedenle, çocukların çevrimiçi etkinliklerini düzenli olarak izlemek, çocukları ve aileleri güvenli internet kullanımı konusunda bilinçlendirmek tehlikeleri önlemek noktasında önemli olacaktır.

4.1.4. Psikolojik Etkiler

Çocukların kişisel verilerinin gizliliğinin ihlal edilmesi, yalnızca sosyolojik ve ekonomik açıdan değil, psikolojik açıdan da pek çok olumsuz sonuç doğurmaktadır. Kişisel verilerinin gizliliğinin ihlal edilmesi, çocuklarda güvensizlik duygusunun artmasına, mahremiyetlerinin ihlal edildiği hissine kapılmalarına ve intihara varan psikolojik travmalara yol açabilmektedir. Bu nedenle, çocukların çevrimiçi ortamlarda kişisel verilerinin gizliliğinin korunması, güvenli internet kullanımı konusunda eğitim almaları ve duygusal ihtiyaçlarının karşılanması kilit rol oynamaktadır.

Livingstone vd. (2014), tarafından yapılan bir çalışma, çocukların çevrimiçi ortamlarda maruz kaldıkları risklerin, stres, endişe ve güvensizlik

duygularına neden olduğunu ortaya koymuştur. Milosevic vd. (2019), yaptıkları araştırmada, çocukların maruz kaldığı bu ihlalin, çocukların kendine güveni, sosyal etkileşimleri ve duygusal refahı üzerinde olumsuz etkilere sahip olabileceğini öne sürmektedir. Araştırmacılar, çocukların kişisel verilerinin gizliliğinin ihlal edilmesinin, çocukların çevrimiçi etkinliklere katılımını ve deneyimlerini olumsuz şekilde etkileyebileceğini vurgulamaktadır. Bunun yanı sıra paylaşılan medya içerikleriyle kendisini başkalarıyla kıyaslayarak, kendini değersiz hissetme gibi olumsuzlukların gelişmesi olağan görülmektedir. Çocukların tanımadığı insanlarla etkileşime geçmesine ortam sağlaması ve gerçekten kopuk sanal bir kimlik oluşturmaya fırsat vermesi gibi özellikleriyle dijital dünya, istismara ve hayattan soyutlanmaya neden olduğu gerekçesiyle kısmen zararlıdır (Tüzün, 2002). Çevrimiçi taciz veya zorbalık durumu ise tıpkı gerçek yaşamda yaşanan taciz ve zorbalık gibi, çocuğun psikolojik sağlığına zarar verebilmektedir. Berson vd. (2017) tarafından yürütülen bir araştırmada, çocukların kişisel verilerinin gizliliğinin ihlal edilmesinin, sosyal izolasyon ve duygusal zorlanma gibi sonuçlara yol açabileceği ortaya koyulmuştur. Araştırmaya göre çocuklar, kişisel bilgilerinin istenmeyen kişilerle paylaşılması sonucu çevrimiçi ortamlarda güvenliklerini sorgulayabilirler ve bu da sosyal etkileşimlerini olumsuz yönde etkileyebilir.

4.1.5. Uzun Vadeli Etkiler

Çocukların kişisel verilerinin gizliliğinin ihlal edilmesinin uzun vadeli etkileri hakkında sınırlı sayıda araştırma bulunmaktadır ancak sosyal medyada paylaşılan bilgilerin gelecekteki iş fırsatlarını etkileyebileceği fikri, birçok araştırma ve uzman görüşü tarafından desteklenmektedir. İşverenlerin, adayların çevrimiçi profillerini dikkatlice inceledikleri ve adayların geçmiş davranışlarına ve paylaşımlarına önem verdikleri bir gerçektir. Olumsuz veya uygunsuz içeriklerin, adayların gelecekteki kariyerlerini etkileyebileceğine dair birçok kanıt bulunmaktadır.

CareerBuilder'ın (2018) yaptığı bir araştırma, işverenlerin %70'inin iş başvuru sahiplerinin çevrimiçi profillerini araştırdıklarını ve bu profillerin işe alım kararlarını etkilediğini belirtmektedir. Araştırmaya katılan işverenlerin %57'si, çevrimiçi profillerde olumsuz içeriklerin bulunması durumunda adayları işe almama eğiliminde olduklarını ifade etmiştir. CareerBuilder ve Harris Poll tarafından 2019 yılında yapılan bir araştırma ise, işverenlerin %48'inin iş başvuru sahiplerinin çevrimiçi profillerini incelediğini ve bu profillerin işe alım sürecini etkilediğini göstermektedir. Aynı araştırma, işverenlerin %70'inin adayların çevrimiçi profillerinde olumsuz içerikler bulunması durumunda onları işe almamaya karar

verebileceklerini ortaya koymaktadır. Yine LendEDU'nun (2018) yaptığı bir ankete katılan işverenlerin %70'inin, iş başvuru sahiplerinin çevrimiçi profillerini araştırdıklarını ve bu profillerin işe alım kararlarını etkilediğini, işverenlerin %57'sinin çevrimiçi profillerde olumsuz içeriklerin bulunması durumunda adayları işe almama eğiliminde olduklarını belirtmiştir. Bu araştırmalar, işverenlerin adayların çevrimiçi profillerini incelediklerini ve bu profillerin işe alım kararlarını etkilediğini göstermektedir. İleriki yıllarda teknolojik gelişmelerle çocukların dijital ayak izinin görüntülenebilme ihtimalinin büyüklüğü göz önüne alındığında, olumsuz veya uygunsuz içeriklerin, çocukların gelecekteki kariyerlerini olumsuz etkileyebileceği konusunda genel bir farkındalık bulunmaktadır.

Birleşmiş Milletler Çocuk Hakları Sözleşmesi 'nin 16. Maddesi; *“Hiç- bir çocuğun özel yaşantısına, aile, konut ve iletişimine keyfi ya da haksız bir biçimde müdahale yapılamayacağı gibi, onur ve itibarına da haksız olarak saldırılamaz. Çocuğun bu tür müdahale ve saldırılara karşı yasa tarafından korunmaya hakkı vardır.”* ifadesiyle çocuğun özel yaşamına karşı her türlü saldırıya karşı çocuğu koruma altına almaktadır. Türkiye Cumhuriyeti Anayasası'nın 20. Maddesinde de aynı düzenlemenin yer aldığı ve *“Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir”* hükmüyle özel hayatın gizliliği kapsamında kişisel verilerin korunması kavramını da ele almaktadır.

4.2. Çocukların Gizliliği ve Güvenliği:

Çocukların sosyal medyada kişisel verilerinin gizliliği ve güvenliği, çocukların dijital dünyada güvenli bir şekilde büyümeleri ve gelişmeleri için kritik bir konudur. Bu nedenle, ebeveynlerin, eğitimcilerin, sosyal medya platformlarının ve yasal düzenleyicilerin çocukların bu konudaki bilinç düzeyini artırmak ve güvenli bir çevrimiçi ortam sağlamak için işbirliği yapmaları büyük önem taşımaktadır. Ebeveynlerin çocuklarının çevrimiçi aktivitelerini izlemesinin yanı sıra ebeveynler ve eğitimciler tarafından çocuklara dijital güvenlik konusunda eğitim verilmesi çocukların kişisel verilerinin güvenliğini sağlamak için önemli adımlardır. Çocuklara, kişisel verilerinin ne olduğunu, neden önemli olduğunu ve nasıl korunması gerektiğini anlatmak ve farkındalık yaratmak, güvenli internet kullanımı konusunda bilinçli bireyler olmalarına yardımcı olacaktır. UNICEF'in yaptığı bir araştırma, ebeveyn denetiminin ve çocukların dijital okuryazarlık

seviyesinin, çocukların sosyal medyada kişisel verilerinin gizliliği ve güvenliği konusunda önemli bir rol oynadığını göstermektedir (UNICEF, 2017).

Kişisel bilgilerin toplanması ve kullanılmasına yönelik bu yeni yollardan kaynaklanan veri gizliliği, potansiyel gizlilik zararları ve güvenlik sorunları, insan hakları açısından önemli sonuçlar doğurmaktadır (Solove, 2006). Araştırmalar, sosyal medya platformlarının çocukların kişisel verilerinin gizliliğini korumak için daha sıkı güvenlik politikaları uygulaması gerektiğini öne sürmektedir (Livingstone vd., 2017). Yasal düzenlemelerin çocukların çevrimiçi güvenliğini sağlamak için daha etkili olması ve sosyal medya platformlarının çocukların veri gizliliğini korumasını zorunlu kılması gerekmektedir. Ancak ebeveynler ve aileden sonra çocuğa en yakın yetişkin olarak eğitimcilerin de çocukların veri gizliliğini korumak adına dikkat edeceği bazı noktalar bulunmaktadır. Çocuk hakları alanında uzmanlaşmış bir uluslararası organizasyon olan Çocuk Hakları İzleme Grubu (CRIN), "Children's Privacy Online" başlıklı bir raporunda, çocukların çevrimiçi gizliliği konusunda ebeveynlerin ve yetişkinlerin rolünü vurgulamıştır.

Çocukların kullandığı ya da çocukların verilerinin paylaşıldığı cihazlarda ve uygulamalarda gizlilik ayarlarını doğru şekilde yapılandırmak veri gizliliğini korumak için doğru bir adım olacaktır. Ebeveynler, çocukların kişisel verilerini korumak için gizlilik ayarlarını düzenlemeli ve gerektiğinde kısıtlamalara gitmelidir. Finkelhor, D., Mitchell, K. J., & Wolak, J. (2000) tarafından yapılan çalışma, ebeveynlerin yalnızca %33'ünün çocuklarını bu tür risklerden korumak için filtreleme veya engelleme yazılımı kullandığını göstermektedir. Yabancılarla iletişim konusunda tanınmayan kişilerden gelen gönderilere yorum yapılmaması ve çevrimiçi iletişimin yalnızca yakın arkadaşlarla sınırlandırılması önerilmektedir.

Genel olarak uygulanan teknik gizlilik ayarlarını 'yalnızca arkadaşlar' olarak değiştirmektir. Daha kısıtlayıcı bir başka seçenek ise kişisel verileri yalnızca özel bir grup (örneğin yakından tanınan güvenilir insanlardan oluşan bir grup) ile paylaşmaktır. Bunun yanı sıra veri gizliliğini koruma yöntemi olarak, özellikle halka açık bilgisayarlarda veya halka açık Wi-Fi bölgelerinde kişisel hesaplardan doğru şekilde çıkış yapmak önemlidir. Ayrıca şifrenin asla ifşa edilmemesi ve çok zor bir şifre seçilmesi gizliliğin korunması için önerilmektedir (Vandoninck, S. ve d'Haenens, L., 2014). Ebeveynlerin dikkat etmesi gereken bir başka nokta ise çocuklarının kullandığı uygulamaların ve web sitelerinin güvenilir olduğundan emin

olmak, güvenlik açıkları veya veri sızıntıları olabilecek uygulamalardan kaçınmaktır.

Ebeveynler, çocukların çevrimiçi etkinliklerini düzenli olarak izleyerek gerektiğinde rehberlik ederken, iletişim kanallarını açık tutarak çocukların güvenlik endişelerini kendileriyle çekinmeden paylaşımlarını teşvik etmelidir. Çocukla çevrimiçi güvenlik konusunda etkileşime geçildiğinde teknoloji, internet, yeni çıkan tehlikeler ve gerekli önlemleri konularında güncel bilgilere sahip olmak doğru rehberlik açısından büyük öneme sahiptir. Bu önlemler çocukların kişisel verilerinin korunmasında ebeveynlerin çocuklarına internet ve teknoloji konusunda sağlıklı alışkanlıklar kazandırmalarına yardımcı olacaktır.

Sosyal medyada çocukların verilerinin paylaşılması konusunda sadece ebeveynlerin değil, toplumun da rolü büyüktür. Toplum olarak, çocukların dijital haklarına saygı gösterilmeli ve bu hakları korumak için gerekli adımların atılması gerekmektedir. Okullar, çocuklara dijital mahremiyet ve çevrimiçi güvenlik konularında eğitim vermeli ve bilinçlendirme kampanyaları düzenlemelidir. Ayrıca, sosyal medya platformları da çocukların verilerini korumak için daha sıkı güvenlik önlemleri almalı ve ebeveynlere bu konuda rehberlik sunmalıdır. Ancak bu şekilde, çocukların güvenli ve sağlıklı bir dijital ortamda büyümesi sağlanabilir.

5. DEĞERLENDİRME VE SONUÇ

Dijital dünya, çocukların da aktif bir şekilde yer aldığı modern çağın bir parçası haline gelmiş durumdadır. Dolayısıyla, dijital platformlar ve kişisel verilerin paylaşımının getirdiği riskler ve çocukların haklarının ihlali konusu gün geçtikçe daha fazla önem kazanmaktadır. Bu makalede, sosyal medyada çocuk haklarının ihlali üzerinde durulmuş, çocukların dijital dünyada karşılaştıkları tehlikeler ve güvende olmaları için alınması gereken önlemler tartışılmıştır.

Dijital platformlarında çocukların kişisel bilgileri sıklıkla paylaşılmakta ve bu bilgilerin nasıl kullanılacağı konusunda yeterli şeffaflık sağlanmamaktadır. Bu durum, çocukların gizliliğinin ihlal edilmesine ve kişisel verilerinin kötüye kullanılmasına yol açmaktadır. Sosyal medya platformlarında çocuklar çevrimiçi taciz ve zorbalığa maruz kalma riski altındadır. Anonimlik ve sınırsız erişim, çocukların bu tür kötü niyetli davranışlara karşı savunmasız hale gelmelerine neden olmaktadır. Çevrimiçi aktiviteler, çocukların zihinsel sağlığını olumsuz etkileyebilecek birçok faktörü içermektedir. Sürekli olarak idealize edilmiş yaşamların sergilendiği

platformlar, çocukların özsayıgılarını ve mutluluk algılarını olumsuz yönde etkileyebilmektedir. Ebeveynler, eğitimciler, diğer yetişkinler ve toplumun, bu risklerin üstesinden gelmek ve çocukları dijital dünyada güvende tutmak için ortak bir çaba içinde olmaları gerekmektedir. Sosyal medyada çocuğun fotoğraflarının ve bilgilerinin paylaşılması bir dizi soruna, ciddi hak ihlallerine ve risklere yol açabilir. Ebeveynler, yetişkinler ve kurumlar, çocukların kişisel verilerini sosyal medyada paylaşmadan önce dikkatli olmalı, çocuğun mahremiyetini ve güvenliğini korumak için gerekli önlemleri almalıdır. Bu önlemler arasında çocuğun rızasını almak, sadece gerekli bilgileri paylaşmak, çocuğun tanınmasını engellemek için fotoğrafları düzenlemek ve gizlilik ayarlarını kontrol etmek yer alabilir. Ayrıca çocukların çevrimiçi aktiviteleri yakından takip edilmeli ve güvenli bir çevre sağlamak için gerekli önlemler alınmalıdır.

Çocukların güvenli ve bilinçli internet kullanımı için dijital dünyadaki tehlikeleri öğrenmeleri gerekmektedir. Çocuklara, ebeveynlere ve eğitimciler, psikologlar, sosyal hizmet uzmanları gibi çocuklarla etkileşime giren tüm çalışanlara, kendi mesleki gelişimleri ve çocuklara rehberlik edebilmeleri için hizmetiçi eğitimler ve atölyeler düzenlenmelidir. İnternet üzerindeki riskleri tanıma ve onlara karşı nasıl korunacaklarını öğrenme konusundaki eğitimler hak ihlali, dijital suçlar ve veri güvenliği açısından önemli bir adım olacaktır.

Çocuklar, dijital dünyada kendilerini koruyacak yetişkin denetimine sahip olmayabilirler. Toplum genelinde, çocukların dijital dünyada güvende olmaları konusunda farkındalık artırılmalı ve desteklenmelidir. Bu nedenle, yasalar çocukların kişisel verilerinin korunmasını sağlanması, onları çevrimiçi tehlikelerden ve kötü niyetli kullanımdan korumak için kilit rol oynamaktadır. Yasalar, çocukların kişisel verilerinin izinsiz olarak toplanmasını veya paylaşılmasını engelleyerek bu özel yaşantıyı güvence altına almalıdır. Çocukların veri gizliliğini koruyan yasalar, dijital dünyada etik ve adil bir kullanımı teşvik etmeli, ebeveynlere ve topluma çocukların dijital dünyada güvenliğini sağlama ve kişisel verilerinin korunmasını sağlama konusunda sorumluluklarını hatırlatmalıdır. Her ülkenin çocuk verilerinin korunması konusunda farklı yasal düzenlemeleri olabilir, yerel yasalara ve çocuk haklarına uygun davranmak toplumun görevlerinden biridir. Çocukların veri gizliliğini koruyan yasalar, toplumun bu konuda bilinçlenmesine yardımcı olmaktadır. Bu bilinçlenme, çocukların dijital dünyada güvende olmaları için gereken önlemlerin alınmasını ve toplumun genelinde çocuk haklarına daha fazla önem verilmesini desteklemektedir.

Ülkemizde çocukların dijital dünyada mağduriyetini engellemek

amacıyla oluşturulan yasal hükümler olsa da rutin düzenlemeler ve güncellemeler ile etkililiğinin artırılması gerekmektedir. Çocukların kişisel verilerinin korunması için katı yasal düzenlemeler getirilmelidir. İnternet üzerindeki içeriklerin yaşa uygunluğu, çocukları zararlı içeriklerden korumak için içerik filtreleri ve aile kontrolü araçları gibi teknolojik önlemler teşvik edilebilir. Sosyal medya ve dijital içerik platformları, çocuk kullanıcılarına yönelik içerikleri filtreleyebilecek teknik altyapılar kurmalı ve çocuk verilerinin işlenmesi konusunda daha şeffaf olmalıdır. Ayrıca, çocuklara dair içeriklerin denetlenmesi için bağımsız denetim mekanizmaları oluşturulmalıdır. Çocukların rızası olmadan veri toplanması ve işlenmesi engellenmelidir. Ayrıca, çocukların kimlik bilgilerini korumak için çevrimiçi platformlarda gizlilik politikaları ve kullanım şartlarının açık ve anlaşılır olması sağlanmalıdır. Okullarda ve toplumda dijital okuryazarlık eğitimi yasalarla zorunlu hale getirilmelidir. Bu sayede çocuklar, çevrimiçi tehditleri tanıyabilir, güvenli internet kullanımı konusunda bilinçlenebilir ve dijital güvenlik önlemlerini öğrenebilirler. Çocuklar tarafından üretilen içeriklerin korunması için oluşturulan yasal düzenlemeler çocukların çevrimiçi ortamlarda güvenli bir şekilde içerik üretmelerini desteklerken, aynı zamanda çocukların içeriklerinin kötüye kullanılmasını ve istismarını engellemeyi amaçlamalıdır. Çocuk istismarı ve çevrimiçi taciz gibi suçları önlemek için yasal düzenlemelerle cezai yaptırımlar güçlendirilmelidir. Ayrıca, çocukları çevrimiçi tehlikelere karşı korumak amacıyla siber suç birimleri ve çocuk istismarıyla mücadele ekipleri gibi uzman ekiplerin oluşturulması teşvik edilebilir.

Dijital dünyanın çocuklar üzerindeki etkileri her geçen gün daha belirgin hale gelmektedir. Çocukların kişisel verilerinin izinsiz şekilde toplanması, dijital mecralarda teşhir edilmesi, psikososyal gelişimlerinin olumsuz etkilenmesi gibi riskler; sadece bireysel değil, aynı zamanda toplumsal sorumluluk alanı olarak da değerlendirilmelidir. Özellikle "sharenting" (ebeveynlerin çocukları hakkında dijital paylaşımlarda bulunması) gibi kavramlar, çocuk haklarının dijital ortamlarda ne denli ihlal edildiğini ortaya koymaktadır. Bu bağlamda, hem ulusal hem de uluslararası düzeyde çocukların dijital haklarının korunmasına yönelik bütüncül bir yaklaşım geliştirilmesi gerekmektedir. Bu doğrultuda, aşağıda belirtilen önerilerin çocukların dijital haklarının korunması adına önemli olduğu düşünülmektedir.

Okul öncesi dönemden itibaren çocuklara yaşlarına uygun biçimde dijital okuryazarlık ve kişisel veri bilinci kazandırılmalıdır. Aynı zamanda ebeveynler ve öğretmenler için sürekli eğitim programları düzenlenerek

farkındalık artırılmalıdır. Ebeveynler, çocuklarının dijital izlerini takip etmek yerine onlarla birlikte dijital sözleşmeler oluşturarak güvene dayalı bir dijital davranış çerçevesi belirlemelidir. Bu tür sözleşmeler, çocuğun dijital özerkliğini desteklerken, risklerden korunmasını da sağlayabilmektedir.

Bunun yanı sıra Türkiye’de yürürlükte olan 6698 sayılı KVKK kapsamı, çocuklara özel düzenlemeleri içerecek şekilde genişletilmeli; dijital platformlarda çocuklara ilişkin içeriklerin paylaşımına yönelik açık hükümler getirilmelidir. Hukuk, psikoloji, medya çalışmaları ve eğitim bilimleri alanlarında çalışan uzmanlar bir araya getirilerek çocukların dijital hakları konusunda kapsamlı politika önerileri hazırlanmalıdır. Çocukların ileriki yaşlarında kendi dijital geçmişlerini kontrol edebilmeleri adına, dijital “unutulma hakkı” konusunda hem yasal zemin hem de dijital araçlar geliştirilmelidir.

Sonuç olarak, dijital ortamda çocukların güvenliğinin sağlanması yalnızca bireysel farkındalıkla değil; kamusal politika, teknolojik sorumluluk ve etik duyarlılığın birleştiği çok aktörlü bir yaklaşım ile mümkün olacaktır. Bu süreçte devlet kurumları, akademik çevreler, sivil toplum ve dijital platformlar eşit düzeyde katkı sağlaması beklenmektedir.

6. SUMMARY

The digital world has become a part of the modern age, where children are actively involved. Therefore, the risks brought about by digital platforms and the sharing of personal data and the violation of children's rights are becoming more and more important. This article focuses on the violation of children's rights on social media, and discusses the dangers children face in the digital world and the precautions that need to be taken to keep them safe. Children's personal information is frequently shared on digital platforms, and sufficient transparency is not provided on how this information will be used. This leads to the violation of children's privacy and the misuse of their personal data. Children are at risk of online harassment and bullying on social media platforms. Anonymity and unlimited access make children vulnerable to such malicious behavior. Online activities include many factors that can negatively affect children's mental health. Platforms where idealized lives are constantly displayed can negatively affect children's self-esteem and perception of happiness. Parents, educators, other adults and society need to make a joint effort to overcome these risks and keep children safe in the digital world. Sharing children's photos on social media can lead to a number of problems, serious rights violations and risks. Parents, adults and institutions should be careful before sharing

children's personal data on social media and take the necessary precautions to protect the child's privacy and security. These precautions may include obtaining the child's consent, sharing only necessary information and editing photos to prevent the child from being recognized, and checking privacy settings. In addition, children's online activities should be closely monitored and the necessary precautions should be taken to provide a safe environment.

Children need to learn about the dangers in the digital world for safe and conscious internet use. In-service training and workshops should be organized for children, parents and all employees who interact with children, such as educators, psychologists and social workers, for their own professional development and to guide children. Training on recognizing the risks on the internet and learning how to protect against them will be an important step in terms of rights violations, digital crimes and data security.

Children may not have the adult supervision that will protect them in the digital world. Awareness should be raised and supported in society in general about children's safety in the digital world. Therefore, laws play a key role in ensuring the protection of children's personal data, protecting them from online dangers and malicious use. Laws should protect this privacy by preventing children's personal data from being collected or shared without permission. Laws protecting children's data privacy should encourage ethical and fair use in the digital world, reminding parents and society of their responsibilities in ensuring children's safety in the digital world and ensuring the protection of their personal data. Each country may have different legal regulations on the protection of children's data, and it is one of the duties of society to act in accordance with local laws and children's rights. Laws protecting children's data privacy help society to become more aware of this issue. This awareness supports the necessary measures to be taken for children to be safe in the digital world and to give more importance to children's rights in society in general.

Although there are legal provisions in our country to prevent children from being victimized in the digital world, their effectiveness needs to be increased with routine regulations and updates. Strict legal regulations should be introduced to protect children's personal data. Age-appropriate content on the internet, technological measures such as content filters and family control tools can be encouraged to protect children from harmful content. Data collection and processing without children's consent should be prevented. In addition, privacy policies and terms of use on online platforms should be ensured to be clear and understandable in order to protect children's identity information. Digital literacy education should be made

mandatory by law in schools and society. In this way, children can recognize online threats, become aware of safe internet use and learn digital security measures. Legal regulations created to protect content produced by children should support children in producing content safely in online environments, while also aiming to prevent the misuse and exploitation of children's content. Legal regulations and penal sanctions should be strengthened to prevent crimes such as child abuse and online harassment. In addition, the establishment of expert teams such as cybercrime units and child abuse prevention teams can be encouraged to protect children against online dangers.

The impact of the digital world on children is becoming increasingly evident. Risks such as the unauthorized collection of children's personal data, exposure in digital environments, and negative effects on psychosocial development should not only be considered individual concerns but also as societal responsibilities. Concepts such as "sharenting" (parents sharing digital content about their children) illustrate the extent to which children's rights are violated in digital spaces. In this context, a holistic approach to safeguarding children's digital rights must be developed at both the national and international levels.

In this regard, the following recommendations are considered crucial for the protection of children's digital rights. From the early childhood period, children should be taught age-appropriate digital literacy and personal data awareness. Simultaneously, continuous educational programs should be organized for parents and educators to raise awareness. Rather than tracking their children's digital footprints, parents should collaborate with them to create digital contracts that establish a secure digital behavior framework based on trust. Such contracts can support the child's digital autonomy while ensuring protection from risks.

Furthermore, the Turkish Personal Data Protection Law (KVKK) No. 6698, which is currently in effect, should be expanded to include specific regulations for children, and explicit provisions should be introduced regarding the sharing of content related to children on digital platforms. Experts from fields such as law, psychology, media studies, and educational sciences should collaborate to develop comprehensive policy recommendations concerning children's digital rights. In order to allow children to control their digital histories in the future, both legal frameworks and digital tools for the "right to be forgotten" should be developed.

In conclusion, ensuring children's safety in the digital environment requires not only individual awareness but also a multi-actor approach that combines public policy, technological responsibility, and ethical sensitivity. It is expected that state institutions, academic circles, civil society organizations, and digital platforms will all contribute equally to this process.

7. KAYNAKLAR

- Alloway, T. P., ve Alloway, R. G. (2012). The impact of engagement with social networking sites (SNSs) on cognitive skills. *Computers in Human Behavior*, 28(5), 1748–1754. <https://doi.org/10.1016/j.chb.2012.04.015>
- Chadwick, A., ve Howard, P. N. (Eds.). (2010). *Routledge Handbook of Internet Politics*. Taylor & Francis.
- Ammari, T., Kumar, P., Lampe, C., ve Schoenebeck, S. (2015). Managing children's online identities: How parents decide what to disclose about their children online. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (pp. 1895–1904). ACM. <https://doi.org/10.1145/2702123.2702325>
- AVG Technologies. (2010). *AVG Digital Diaries – A Look At How Technology Affects Us From Birth Onwards*. <https://www.avgdigitaldiaries.com/post/41940227757/avg-digital-diaries-a-look-at-how-technology>
- Berson, I. R., Berson, M. J., ve Ferron, J. M. (2017). The impact of privacy violations on children's cognitive and emotional processing of e-commerce websites. *Journal of Child Psychology and Psychiatry*, 58(10), 1125–1133.
- Çimke, S., Gürkan, D. Y., ve Polat, S. (2018). Sosyal medyada çocuk hakkı ihlali: Sharenting. *Güncel Pediatri*, 16(2), 261–267.
- Crawford, K., ve Schultz, J. (2014). Big data and due process: Toward a framework to redress predictive privacy harms. *Boston College Law Review*, 55(1), 93–128.
- Dwyer, C., Hiltz, S., ve Passerini, K. (2007). Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace. In *AMCIS 2007 Proceedings* (p. 339).
- Erişir, R. M., ve Erişir, D. (2018). Yeni medya ve çocuk: Instagram özelinde “sharenting” (“paylaşan babalık”) örneği. *Yeni Medya*, (4–5), 50–64.
- Fardouly, J., Diedrichs, P. C., Vartanian, L. R., ve Halliwell, E. (2015). Social comparisons on social media: The impact of Facebook on young women's body image concerns and mood. *Body Image*, 13, 38–45. <https://doi.org/10.1016/j.bodyim.2014.12.002>
- Finkelhor, D., Mitchell, K. J., ve Wolak, J. (2000). *Online victimization: A report on the nation's youth*. National Center for Missing & Exploited Children.
- Holloway, D., Green, L., & Livingstone, S. (2013). *Zero to eight: Young children and their internet use*. EU Kids Online. http://eprints.lse.ac.uk/52630/1/Zero_to_eight.pdf
- Højgaard, L. (2003). Children and the internet: Developmental implications of web

sites for young children. *European Early Childhood Education Research Journal*, 11(1), 39–52.

Kişisel Verilerin Korunması Kanunu, Kanun Numarası: 6698, Kabul Tarihi: 24.3.2016. Resmî Gazete: 07.04.2016 / 29677.

Kitchin, R. (2014). *The data revolution: Big data, open data, data infrastructures and their consequences*. SAGE.

Kross, E., Verduyn, P., Demiralp, E., Park, J., Lee, D. S., Lin, N., ... ve Ybarra, O. (2013). Facebook use predicts declines in subjective well-being in young adults. *PLOS ONE*, 8(8), e69841. <https://doi.org/10.1371/journal.pone.0069841>

Leaver, T. (2016). Born digital? Presence, privacy, and intimate surveillance. In J. Hartley & Q. Wang (Eds.), *Re-Orientation: Translingual, Transcultural, Transmedia* (pp. 149–160). Fudan University Press.

Lenhart, A. (2015). *Teens, social media & technology overview 2015*. Pew Research Center.

Livingstone, S., ve Smith, P. K. (2014). Annual research review: Harms experienced by child users of online and mobile technologies: The nature, prevalence and management of sexual and aggressive risks in the digital age. *Journal of Child Psychology and Psychiatry*, 55(6), 635–654.

Livingstone, S., Haddon, L., Görzig, A., ve Ólafsson, K. (2011). *Risks and safety on the internet: The perspective of European children*. EU Kids Online.

Livingstone, S., ve Third, A. (2017). Children and young people's rights in the digital age: An emerging agenda. *New Media & Society*, 19(5), 657–670.

Lupton, D. (2013). *The social worlds of the unborn*. Palgrave Macmillan.

Lupton, D. (2015). *Digital sociology*. Routledge.

Lupton, D. (2016). Personal data practices in the age of lively data. In J. Daniels, K. Gregory, & T. McMillan Cottom (Eds.), *Digital Sociologies* (pp. 335–350). Policy Press.

Marx, G. T. (2003). A tack in the shoe: Neutralizing and resisting the new surveillance. *Journal of Social Issues*, 59(2), 369–390. <https://doi.org/10.1111/1540-4560.00069>

Lupton, D., ve Thomas, G. M. (2015). Playing pregnancy: The ludification and gamification of expectant motherhood in smartphone apps. *M/C Journal*, 18(5). <http://journal.media-culture.org.au/index.php/mcjournal/article/view/1012>

Macenaite, M. (2017). From universal towards child-specific protection of the right to privacy online: Dilemmas in the EU General Data Protection Regulation. *New Media & Society*, 19(5), 765–779.

McCarthy, M. (2013). Experts warn on data security in health and fitness apps. *BMJ*, 347, f5600. <https://doi.org/10.1136/bmj.f5600>

Milosevic, T., ve Lwin, M. O. (2019). Privacy in the digital age: The impact of online surveillance on children's psychological well-being. *Cyberpsychology, Behavior, and Social Networking*, 22(4), 245–251.

Morgan, A. (2018). The transparency challenge: Making children aware of their data

- protection rights and the risks online. <https://www.dataprotection.ie/sites/default/files/uploads/2019-02/TransparencyChallenge.pdf>
- Parmaksız, Y. P. M. (2012). Digital opportunities for social transition: Blogosphere and motherhood in Turkey. *Fe Dergi*, 4(1), 123–134.
- Raley, R. (2013). Dataveillance and countervailance. In L. Gitelman (Ed.), “*Raw Data*” is an *Oxymoron* (pp. 121–145). MIT Press.
- Rosen, L. D., Whaling, K., Rab, S., Carrier, L. M., ve Cheever, N. A. (2013). Is Facebook creating “iDisorders”? The link between clinical symptoms of psychiatric disorders and technology use, attitudes and anxiety. *Computers in Human Behavior*, 29(3), 1243–1254. <https://doi.org/10.1016/j.chb.2012.11.012>
- Rosenzweig, P. (2012). Whither privacy? *Surveillance & Society*, 10(3–4), 344–347. <https://doi.org/10.24908/ss.v10i3/4.4325>
- Simon, S. (2014, June 5). Big brother: Meet the parents. *Politico*. <https://www.politico.com/story/2014/06/internet-data-mining-children-107461.html>
- Timms, P. (2015, November 27). Hello Barbie: Wi-Fi enabled doll labelled a bedroom security risk. *ABC News*. <https://www.abc.net.au/news/2015-11-27/wi-fi-enabled-hello-barbie-doll-raises-security-concerns/6981528>
- Twenge, J. M., ve Campbell, W. K. (2018). Associations between screen time and lower psychological well-being among children and adolescents: Evidence from a population-based study. *Preventive Medicine Reports*, 12, 271–283. <https://doi.org/10.1016/j.pmedr.2018.10.003>
- Tüzün, Ü. (2002). Gelişen iletişim araçlarının çocuk ve gençlerin etkileşimi üzerine etkisi. *Düşünen Adam Dergisi*, 15(1), 46–50.
- UNICEF. (2017). *The state of the world's children 2017: Children in a digital world*. <https://www.unicef.org/reports/state-worlds-children-2017>
- Van Dijck, J. (2014). Datafication, dataism and dataveillance: Big data between scientific paradigm and ideology. *Surveillance & Society*, 12(2), 197–208. <https://doi.org/10.24908/ss.v12i2.4776>
- Vandoninck, S., ve d’Haenens, L. (2014). Ways to avoid problematic situations and negative experiences: Children’s preventive measures online. *Communications*, 39(3), 261–282. <https://doi.org/10.1515/commun-2014-0116>
- Yavuz, C. (2020). Sosyal medya ebeveynliği ve çocukların unutulma hakkı. *İzmir Barosu Dergisi*, 85(1), 15–52.

Çatışma beyanı: Bu çalışma ile ilgili taraf olabilecek herhangi bir kişi ya da kurum ile finansal ilişki bulunmamaktadır.

Katkı Oranı Beyanı: Birinci yazarın katkı oranı %60, ikinci yazarın katkı oranı %40 olarak belirlenmiştir.