TAAD Yıl 14 . Sayı 53 . Ocak 2023
ISSN 1309-6826
DOI: 10.54049/taad.1231771 Araştırma Makalesi/Research Article

DİJİTAL DÜNYADA ÇEVRİMİÇİ RİSKLER, BİLİŞİM SUÇLARI VE MAĞDUR ÇOCUK

Online Risks in The Digital World, Cyber Crimes and Child Victims

Pelin ÖZKAYA*

Özet

Çocuk, dünyada tehlikeye maruz kalmaya en müsait birey kuşkusuz. Tarihin tüm devirlerinde kaçırılan, öldürülen veya istismara uğrayan çocuklarla ilgili çok sayıda olayla karşılaşmaktayız. İnternetin olmadığı veya henüz evlere bu kadar yerleşmediği yıllarda, onları korumak fiziki alanlarla sınırlıydı. Dikkatli bir gözetim ve uzun demir parmaklıklı binalar güvenliği büyük ölçüde sağlıyordu ancak internetle birlikte tüm fiziki sınırlar ortadan kalkarak gözetim imkanı zorlaştı. Dünya'nın herhangi bir yerindeki herhangi bir kişi bir tık uzağımızda, hatta bazı zamanlarda evimizin içinde... Dahası, bilgisayarlar, cep telefonları ve tabletlerle o kişileri evimize kendimiz davet ediyoruz. Saldırganların giriş kapısı olarak kullandığı bu sistemler, çocukla ilgili kişisel verileri tehlikeye atarak gizlilik ihlaline neden olurken, istismar, kaçırma ve sömürü gibi fiillerin oluşumunu da tetiklemektedir. Dijital oyunlar sözü geçen tehlikeler için sosyal platformlarla birlikte en müsait alanları oluşturur. Bu mecralar çocukları kandırmak, manipüle etmek veya tehdit ya da şantajla sanal teması fiziki temasa dönüştürmek için kullanıldığı kadar, siber zorbalık, takip ve taciz eylemleri için de ideal araçlardır. Ailelerine veya öğretmenlerine yaşadıkları durumları anlatamayan veya hukuki olarak nereye başvurması gerektiğinin bilicinde olmayan çocuklar için sonucu telafi edilemeyen mağduriyetler doğmaktadır. Çocukları siber dünyanın tehditlerinden korumak için alınması gereken önlemler konusunda devlete büyük oranda iş düşmekle birlikte, temel eğitimin ve bilinçlendirmenin ailede başlayarak okulda devam ettiği unutulmamalıdır. Bu kapsamda bu makalede, çocukların dijital ortamda maruz kaldığı çeşitli tehlikeler anlatılarak hukuki çerçeve çizilecek ve alınması gereken tedbirlerden söz edilecektir.

Anahtar Kelimeler: Siber Suç, Bilişim Hukuku, Kişisel Veri, Çocuk Güvenliği, Adli Bilişim, Dijital Oyun, Siber Zorbalık

Abstract

The child is undoubtedly the most vulnerable individual in the world to be exposed to danger. We encounter many incidents of children who have been kidnapped, killed or abused in all periods of history. In the years when the internet did not exist or was not yet settled in homes, protecting them was limited to physical spaces. Careful surveillance and buildings with long iron bars provided security to large extent, but with the internet, all physical borders disappeared

➢ *Bu makale Etik Kurul İznine tabi değildir/This article is not subject to Ethics Committee Permission.*
➢ *Makale Geliş Tarihi/Article Received Date: 27.12.2021*
➢ *Yayın Kurulu Kabul Tarihi/Editorial Board Acceptance Date: 21.12.2022*

* Serbest Avukat, Ankara Barosu, Ankara Üniversitesi Adli Bilişim MSc., Hacettepe Üniversitesi Adli Bilimler Doktora Öğrencisi, avpelinozkaya@gmail.com, https://orcid.org/0000-0002-5429-2729

and surveillance became difficult. Any person anywhere in the world is just a click away, sometimes even inside our home... Moreover, we invite those people to our home ourselves with computers, mobile phones and tablets. These systems, which are used by the attackers as a gateway, cause a violation of privacy by jeopardizing the personal data of the child, while triggering the occurrence of acts such as abuse, kidnapping and exploitation. Digital games, together with social platforms, create the most suitable areas for the aforementioned dangers. These platforms are ideal tools for acts of cyberbullying, stalking and harassment, as well as being used to deceive, manipulate or turn virtual contact into physical contact with threats or blackmail. Unrecoverable grievances arise for children who cannot tell their families or teachers about the situations they are experiencing or are not aware of where to apply legally. Although the state has a lot of work to do about the measures to be taken to protect children from the threats of the cyber world, it should not be forgotten that basic education and awareness-raising starts in the family and continues at school. In this context, in this article, various dangers that children are exposed to in the digital environment will be explained, a legal framework will be drawn and the precautions to be taken will be mentioned.

Key Words: Cyber Crime, IT Law, Personal Data, Child Safety, Forensic Informatics, Digital Game, Cyber Bullying

GİRİŞ

Çocukların bizzat kendileri tarafından veya aileleri vasıtasıyla dijital dünyayla kurdukları ilk temas, fayda ve fırsatla birlikte pek çok tehlikeyi de beraberinde getirir. İnternet dünyaya ve bilgilere açılan büyük bir kapı olmuştur ve kuşkusuz ki çocukların eğitimleri ve gelişimleri için büyük fırsatlar sunmaktadır, ancak madalyonun diğer yüzü daha karanlık bir dünyayı yansıtıyor olabilir.

İnternet kendi içinde barındırdığı riskler bakımından birkaç gruba ayrılarak çocukların dijital dünyadaki varlıkları için tehdit oluşturur. Örneğin; internet bağımlılığı, asosyallik, kişilik bozuklukları ve obezite gibi "Kullanım Riskleri" en temel risk unsurudur. Şiddet, ırkçılık, ayrımcılık, nefret, cinsellik, pornografi, intihar, kendi kendine zarar verme gibi birçok uygunsuz içerikle karşılaşmaları "İçerikle İlgili Riskler"i oluştururken, bu karşılaşmalardan sonra geliştirdikleri olumsuz davranışlar (başka çocuklara şiddet uygulamak, nefret söylemleri gerçekleştirmek, ırkçı provokasyonda bulunmak, kendi oluşturduğu cinsel görüntülerini internette yaymak, intihara teşebbüs vb.) ise "Davranışla İlgili Riskler"[1] grubuna girmektedir. Mahremiyete müdahale, cinsel tehlike ve siber zorbalık "Çevrimiçi Temas Riskleri"nin parçasıyken, çevrimiçi başlayıp zamanla fiziksel temasa dönüşen "Çevrimdışı Temas Riskleri" de diğer bir risk unsurudur. Suçlularla sanal dünyada gerçekleşen çevrimiçi iletişim bugün adına "Bilişim Suçu" dediğimiz suçların bir ayağını oluştururken, fiziki alana geçişle birlikte çevrimdışı temas ile gerçekleşen suç tipleri ise, ikinci ayağını oluşturmaktadır.

[1] UNICEF, 'Dijital bir Dünyada Çocuklar' (2017) Dünya Çocuklarının Durumu Raporu s.22 <https://www.unicef.org/turkey/raporlar/d%C3%BCnya-%C3%A7ocuklar%C4%B1n%C4%B1n-durumu-2017-dijital-bir-d%C3%BCnyada-%C3%A7ocuklar> Erişim Tarihi: 23.12.2021.

I. BİLİŞİM SUÇLARI

Bilişim Suçu veya Siber Suç, elektronik sistemleri, ağları, web sitelerini ve verileri hedeflemek veya bir suçun işlenmesini kolaylaştırmak için bilgi ve iletişim teknolojileri (BİT ing. *ICT – Information and Communication Technologies*) kullanılarak işlenen, yasaları ihlal eden eylemler olarak tanımlanabilir ve tanımda da yer aldığı üzere temelde iki kategoriye ayrılır. Eğer siber saldırganlar tarafından bir bilişim sisteminin işleyişi hedef alınıyor veya içindeki bilgiler (kişisel veriler, ticari sırlar vb.) ele geçirilmeye çalışılıyorsa burada "Doğrudan Bilişim Suçları" söz konusu olmaktadır. Bilişim teknolojilerinin araç olarak kullanılması yoluyla gerçekleşen klasik suçlarda ise amaç bilişim sisteminin çalışmasını engellemek veya içindeki bilgileri ele geçirmek olmadığından, "Dolaylı Bilişim Suçları" işlenmekte olup, ihlal edilen ilgili kanun maddeleri işlerlik kazanmaktadır.

Birleşmiş Milletler Çocuk Haklarına Dair Sözleşme Genel Yorum No.13 uyarınca[2], bilgi ve iletişim teknolojileri aracılığıyla şiddet içeren alanlar şu şekilde sıralanmıştır (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, yanlışa 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.

Bahsi geçen bu fiiller, bilişim teknolojilerinin araç olarak kullanıldığı senaryolar bakımından açıklayıcı örneklerdir. Her biri fiziki olarak gerçekleşebil-

---

[2] Birleşmiş Milletler Çocuk Haklarına Dair Sözleşme Genel Yorum No. 13. [2011] <http://humanistburo.org/dosyalar/humdosya/BM%20CHK%20Genel%20Yorum%20No13%20-%20Cocuga%20Karsi%20Siddet.pdf≥ Erişim Tarihi: 22.12.2021

mekle birlikte, internetin ve elektronik cihazların devreye girmesiyle işlenmeleri daha da kolaylaşmakta ve etki alanları daha da genişlemektedir. Özellikle Türk Ceza Kanunu (TCK)'nda düzenlenmeleri bakımından "Dolaylı Bilişim Suçları" kapsamına giren fiiller: md.84 "İntihara Yönlendirme", md.103 "Çocukların Cinsel İstismarı", md.104 "Reşit Olmayanla Cinsel İlişki", md.141 ve 142 "Hırsızlık", md.226 "Müstehcenlik" maddeleriyle karşımıza çıkmakla birlikte, bilişim sistemleri vasıtasıyla kaçırılan çocukların dahil olduğu md.77 "İnsanlığa Karşı Suçlar", md.79 "Göçmen Kaçakçılığı", md.80 "İnsan Ticareti", md.90 "İnsan Üzerinde Deney", md.227 "Fuhuş", md.229 "Dilencilik" vb. maddeleri de söz konusu olabilmektedir.

Bilişim suçları bakımından en yaygın görünen suç tipi 'Çocuk İstismarı'nın görünüm şekillerinden biri olan 'Çocuk Pornografisi' TCK'da özel olarak düzenlenmiş bir suç tipi olmamakla beraber, Türkiye'nin kabul ettiği 2004 yılında yürürlüğe giren "Avrupa Konseyi Siber Suçlar Sözleşmesi"[3] ile hüküm altına alınmıştır. 9. Maddede düzenlenen bu suçta;

- *"Cinsel davranışta bulunan reşit olmayan bir kişi,*
- *Cinsel davranışta bulunan reşit olmayan bir kişi gibi gözüken kişi,*
- *Cinsel davranışta bulunan reşit olmayan bir kişiyi tasvir eden gerçekçi resimler"*

bulunduğu kabul edilmektedir. Suçun bilişim teknolojileri vasıtalarıyla işlenişi işe şu şekilde tanımlanmıştır:

- *"Başka bir bilgisayar sistemi ile dağıtılması amaçlı, çocuk pornografisi üretimi,*
- *Bir bilgisayar sistemi vasıtasıyla çocuk pornografisinin elde edilmesinin sağlanması,*
- *Bir bilgisayar sistemi ile çocuk pornosunun dağıtımı, iletilmesi veya aktarılması,*
- *Kendi veya başka bir kişi için, bir bilgisayar sistemi ile çocuk pornosunun temin edilmesi,*
- *Bir bilgisayar veri depolama ortamında veya bir bilgisayar sisteminde çocuk pornografisi bulundurmak".*

Diğer bir düzenleme, 2002 yılında Türkiye'nin onayladığı "Çocuk Haklarına Dair Sözleşmeye Ek Çocuk Satışı, Çocuk Fahişeliği ve Çocuk Pornografisi ile İlgili İhtiyari Protokol[4] "dür. Bu protokol, '1999 Viyana Uluslararası İnter-

[3] The Council of Europe Convention on Cybercrime [2004] ETS 185

[4] Çocuk Haklarına Dair Sözleşmeye Ek Çocuk Satışı, Çocuk Fahişeliği ve Çocuk Pornografisi ile İlgili İhtiyari Protokol. Yürürlük Tarihi: 18.01.2002 <https://www5.tbmm.gov.tr/kanunlar/k4755.html> Erişim Tarihi: 22.12.2021

net Üzerinde Çocuk Pornografisiyle Mücadele Konferansı (ICCCPI - *International Conference on Combating Child Pornography on The Internet*)'nın, sonuç kararının düzenlenmiş halidir. Söz konusu kararda, çocuk pornografisinin üretiminin, dağıtımının, ithalatının, ihracatının, kasıtlı zilyetliğinin ve reklamının internette ve diğer gelişen teknolojiler üzerinde artan erişilebilirliği vurgulanmış ve tüm dünyada suç olarak kabul edilmesi için çağrıda bulunulmuştur.

Müstehcenlik suçunda ise, bir çocuğa müstehcen söz, yazı veya görüntü içeren materyalleri vermek, göstermek ya da dinletmek; bunların içeriklerini çocukların girebileceği veya görebileceği yerlerde sergilemek, müstehcen söz, yazı veya görüntüleri basın ve yayın yolu ile yayınlamak veya yayınlanmasına aracılık etmek (…) suç kapsamındadır (TCK md.226).

Gerek cinsel istismar gerekse müstehcenlik suçlarının bilişim sistemleri vasıtasıyla işlenmesi hali nitelikli ve ağırlaştırıcı hal olarak düzenlenmelidir, çünkü internet doğası gereği sınır aşan özelliklidir ve görüntülerin bir yerden başka bir yere iletilmesi son derece hızlı olmakla birlikte, verilerin gerçek anlamda ve tamamıyla yok edilmesi ise mümkün değildir.

Bilişim teknolojileri aracılığıyla maruz kalınan diğer fiiller ise;

- Siber taciz (***Cyberharassment***): Bir kişi veya bir grup tarafından tehditkar ve saldırgan davranışlarla, başka bir kişinin, bilişim sistemleri ve internet kullanılarak çevrimiçi ortamda rahatsız edilmesi veya korkutulmasıdır[5]. Suçluların bizzat kendileri kısa mesaj, e-posta, sosyal medya platformları aracılığıyla taciz edici mesajlar ve tehditler göndermekte[6] veya üçüncü bir kişinin gerçekleştirdiği saldırıları kışkırtmaktadır. Diğer bir görünümü ise, mağdur kişilerin ailesi, arkadaşları, işverenleri veya öğretmenleri ile elektronik iletişime geçmeleri şeklindedir.
- Siber takip (***Cyberstalking***): Tıpkı fiziki bir eylemde olduğu gibi, saldırganlar hedef olarak belirledikleri kişilerin yerlerini tespit etmekte, bu kişileri elektronik araçlar kullanarak araştırmakta ve sonraki süreçte de taciz, tehdit veya korkutma yöntemleriyle rahatsız etmektedir. Saldırganlar bilişim sistemleri ve internet vasıtasıyla kurbanları ile ilgili çok çeşitli bilgiler edinebilmekte, bu bilgileri fiziki olarak erişim sağlamak ve yakın ilişki kurmak için kullanmaktadır.

---

5 Carsten Maple, Emma Short, Antony Brown, 'Cyberstalking in The United Kingdom: An Analysis of The ECHO Pilot Survey' (2011) National Centre for Cyberstalking Research: University of Bedfordshire <https://www.researchgate.net/publication/292157398_Cyberstalking_in_the_United_Kingdom_an_analysis_of_the_ECHO_Pilot_Survey_National_Centre_for_Cyberstalking_Research_University_of_Bedfordshire> Erişim Tarihi: 16.12.2021.

6 Michele L Ybarra, Dorothy L Espelage , Kimberly J Mitchell, 'The Co-occurrence of Internet Harassment and Unwanted Sexual Solicitation Victimization and Perpetration: Associations with Psychosocial Indicators' (2007) 41(32) Journal of Adolescent Health 31–S41.

- Siber zorbalık (***Cyberbullying***): Bir veya birkaç kişiye yönelik tekrarlı ve kasıtlı şekilde, zarar vermek, incitmek veya utandırmak amacıyla bilişim sistemleri vasıtasıyla, ses görüntü veya yazı göndermek, yayınlamak, küfür veya hakaret etmek, dalga geçmek, küçük düşürmek, dedikodu yapmak vb. eylemlerdir. Bunlar; sohbet odaları, web siteleri, sosyal medya platformları gibi ortamlarda gerçekleşebilmekte, mağdur duruma düşen kişilerde utanç, küçük düşme, aşağılanma, dışlanma şeklinde kendini göstererek, intihara varan etkilerle sonuçlanabilmektedir. Siber zorbanın kimliği bu süreçte açıkça bilinebildiği gibi, sahte hesaplar veya takma adlar kullanıldığı durumlarda tespit edilemeyebilir, kişi okul içinden veya dışından, arkadaş çevresinden hatta aile bireylerinden biri bile olabilir[7].
- Zararlı çevrimiçi içeriğe maruz kalma: Bir çocuğun kasıtlı olarak veya yanlışlıkla, yasadışı olmasa bile olumsuz yönde etkileme özelliğine sahip, yazılı, görsel veya sesli materyallerle karşılaşması halidir. Bu materyaller; ırksal veya etnik nefreti destekleyen web siteleri, şiddet içeren video oyunları, çevrimiçi pornografi, dolandırmaya veya kimlikleri çalmaya çalışan ticari siteler ve cinsel malzeme satış siteleri gibi gelişimlerine psikolojik veya cinsel yönden zararlı olabilecek içerikleri içerir[8] [9]. İçerikler, pop-up reklamlar veya spam e-postalar şeklinde yanlışlıkla gönderilebileceği gibi, sosyal medya hesabı, e-posta adresi ya da telefon numarası bilinen mağdura kasıtlı olarak da gönderilebilir. Zararlı içeriklerle karşılaşan çocuklar, içeriğin onları olumsuz yönde etkileyip etkilemeyeceğini kavrayamadan ve kendilerini mevcut olumsuzluktan uzaklaştıramadan içerikten etkilenebilmektedir. Hatta bazen bu etkilenme olumsuz şekilde olmak yerine, onların merakını tetikleyerek daha fazla materyale veya bilgiye ulaşma isteği ve gayreti şeklinde de kendini gösterebilmektedir[10].

---

7 Ethel Quayle, Linda Jonsson, Lars Lööf, 'Online Behaviour Related to Child Sexual Abuse Interviews with Affected Young People' (2012) Council of the Baltic Sea States, Stockholm: Robert Project. 31-118. Erişim Tarihi: 16.12.2021. https://childrenatrisk.cbss.org/wp-content/uploads/2020/12/Interviews_with_affected_young_people.pdf

8 Children's Internet Protection Act (CIPA) [2000] Pub. L. 106-554 art. 1711, 1721.

9 CIPA, 'Study of Technology Protection Measures in Section 1703' (2003). Department Of Commerce National Telecommunications and Information Administration. <https://www.ntia.doc.gov/files/ntia/publications/cipareport08142003.pdf> Erişim Tarihi: 16.12.2021

10 United Nations Office on Drugs and Crime (UNODC) Vienna, 'Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children'. (2015). <https://www.unodc.org/documents/organized-crime/cybercrime/Study_on_the_Effects.pdf> Erişim Tarihi: 16.12.2021

Siber taciz, siber istismar ve siber şiddet; zorbalık ve tehditler dâhil olmak üzere, siber agresifliği, intihar eylemlerinin teşvik edilmesini, çocuğun kendisinin cinsel içerikli görüntü ve mesajları rıza dışı üretmesini, paylaşmasını ve kendi kendisine zarar vermesini içerirken, internet ve sosyal platformların farklı açılardan başka riskleri de vardır. Çocukların cinsel içerikli mesajları isteyerek gönderme veya kendi müstehcen görüntülerini cep telefonuyla oluşturma ile internet üzerinden iletme ve paylaşma eylemleri "***Sexting***" olarak adlandırılmakta[11] [12], bu tür materyaller reşit olmayan çocuklar tarafından oluşturulduğu için "kendi ürettiği çocuk pornografisi" olarak kabul edilmektedir[13,14]. Diğer bir durum olarak, şiddet yanlısı aşırıcı olarak tanımlanan çeteler ile, terörist eylemler gerçekleştirmek üzerine oluşturulmuş gruplar için, çocukların ve gençlerin bu ve benzeri eylemlerle ilgilenmeye başlamalarını ya da söz konusu örgütlere katılmalarını sağlamak için bu mecralar yeni yöntemler sunabilir[15].

Yukarıda bahsi geçen çevrimiçi tehditler direkt olarak bir kanun maddesiyle düzenlenmiş olmamakla birlikte, ihlal ettikleri haklar bakımından diğer kanunları ilgilendirmektedir. Bunlardan birkaçını örnek olarak göstermek gerekirse:

- Siber taciz fiili için: TCK md.105 "Cinsel Taciz" suçu,
- Siber takip fiili için: TCK md.123 "Kişilerin Huzur ve Sükununu Bozma" suçu
- Özel görüntü ve yazışmaları ifşa fiili için: TCK md.132 "Haberleşmenin Gizliliğini İhlal" suçu
- Nefret söylemi için: TCK md.125 "Hakaret", md.216 "Halkı Kin ve Düşmanlığa Tahrik veya Aşağılama" suçu
- İnternet üzerinden ayrıntılı bilgi toplama, yayma, kullanma, kişi adı-

---

11 Jessica Ringrose, Rosalind Gill, Sonia Livingstone, Laura Harvey, 'A Qualitative Study of Children, Young People and 'Sexting': A Report Prepared for the NSPCC'' (2012). <https://www.researchgate.net/publication/265741962_A_qualitative_study_of_children_young_people_and_'sexting'_a_report_prepared_for_the_NSPCC> Erişim Tarihi: 16.12.2021

12 Amanda Lenhart, 'Teens and Sexting: How and Why Minor Teens are Sending Sexually Suggestive Nude or Nearly Nude Images via Text Messaging', (2009). Pew Research Centre Report. <https://www.pewresearch.org/internet/2009/12/15/teens-and-sexting/> Erişim Tarihi: 16.12.2021

13 Mary Graw Leary, 'Self-Produced Child Pornography: The Appropriate Societal Response to Juvenile Self-Sexual Exploitation', (2008) 15(1) Virginia Journal of Social Policy and the Law p.4

14 Mary Graw Leary, 'Sexting or Self-Produced Child Pornography? The Dialogue Continues – Structured Prosecutorial Discretion within a Multidisciplinary Response', (2010) 17(3) Virginia Journal of Social Policy and the Law Spring 486-566. p.488

15 Birleşmiş Milletler Çocuk Haklarına Dair Sözleşme Genel Yorum 25 [2021] <https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CRC%2fC%2fGC%2f25&Lang=eN> Erişim Tarihi: 16.12.2021

na sahte hesap açma için: TCK md.136 "Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme" suçu

- Gizlilik ihlali için: TCK md.134 "Özel Hayatın Gizliliğini İhlal" suçu, md.135,136,137,138 Kişisel Veri Suçları
- Tehdit suçu için: TCK md.106
- Şantaj suçu için: TCK md.107

Maddeleri uygulanabilecektir. Söz konusu fiiller aynı zamanda, temel hak ve özgürlükler bakımından aşağıdaki hükümlerin ihlaline sebebiyet verecektir:

- Anayasa md.17; Kişinin Dokunulmazlığı, Maddi Ve Manevi Varlığı
- Anayasa md.20; Özel Hayatın Gizliliği
- Anayasa md.22; Haberleşme Hürriyeti
- Avrupa İnsan Hakları Sözleşmesi md.8; Özel Hayata Ve Aile Hayatına Saygı Hakkı

5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun" uyarınca, kullanıcılarına internet ortamına erişim olanağı sağlayan TTNet, Kablonet, Turkcell, Vodafone gibi "Erişim Sağlayıcı (İnternet Servis Sağlayıcı – ISS (ing. ISP)"lar, kendileri aracılığıyla erişilen bilgilerin içeriklerinin hukuka aykırı olup olmadığını ve sorumluluğu gerektirip gerektirmediğini kontrol etmekle yükümlü değildir (md.6/2) ancak, herhangi bir kullanıcısının yayınladığı hukuka aykırı içerikten haberdar edilmesi halinde erişimi engellemek zorundadır (md.6/1-a). Bununla birlikte, "Telekomünikasyon Hizmetleri Yönetmeliği Ek md.3 İnternet Servis Sağlayıcılığıyla İlgili Yetki Belgelerine İlişkin Genel Hükümler"de yer alan Özel Şartlarda[16];

- *"İSS'ler, kullanıcılarının İnternet üzerindeki yetkisiz ve rahatsız edici girişimlerine meydan vermeme, gerek kendi tespit ettiği, gerekse diğer kullanıcı ve işletmeciler tarafından tespit edilip kendisine bildirilen bu tür girişimleri engelleme,*
- *İSS'ler Kurum'ca talep edilmesi halinde; kullanıcı sayısı, kullanıcı kimlikleri, sisteme bağlı kalınan süre ve iletilen bilgi miktarları ile ilgili trafik bilgileri verme"*

yükümlülükleri altındadır.

Sosyal etkileşim amacıyla kullanıcılara internet ortamında metin, görüntü, ses ve konum gibi içerikleri oluşturmalarına, görüntülemelerine veya paylaşmalarına imkan sağlayan Facebook, Twitter, Youtube vb "Sosyal Ağ Sağlayıcı"lar 5651 sayılı Kanun'un Ek 4. Maddesi uyarınca; hukuka

[16] Telekomünikasyon Hizmetleri Yönetmeliği. RG 28.03.2001 / 24356.

aykırı içeriği yayından çıkarmak / kaldırmak / erişimin engellenmesini sağlamak yükümlülüğü altında olup, taleplere en geç 48 saat içinde cevap vermek zorundadır.

Kişilere belli bir yerde ve belli bir süre internet ortamı kullanım olanağı sağlayan oyun salonları, internet kafeler, kütüphaneler, okullar "Toplu Kullanım Sağlayıcı"lar olarak, konusu suç oluşturan içeriklere erişimin engellenmesi ve kullanıma ilişkin erişim kayıtlarının tutulması (5651 sk. md.7/2) ile ailenin ve çocukların korunması, suçun önlenmesi ve suçluların tespiti kapsamında gerekli tedbirleri almakla yükümlüdür (md.7/3).

İnternet ortamında yapılan yayın içeriği nedeniyle kişilik haklarının ihlal edildiğini iddia eden kişiler içerik sağlayıcısına, buna ulaşamaması hâlinde yer sağlayıcısına veya doğrudan sulh ceza hâkimine başvurarak içeriğin çıkarılmasını ve/veya erişimin engellenmesini de isteyebilir (5651 sk. md.9). Eğer özel hayatının gizliliğinin ihlali söz konusu ise, doğrudan Bilgi Teknolojileri ve İletişim Kurumu (BTK)'na başvurarak içeriğe erişimin engellenmesi tedbirinin uygulanmasını talep edebilir (md.9/A)

İnternet ortamında yapılan ve içeriği TCK'da yer alan aşağıdaki suçları oluşturduğu hususunda yeterli şüphe sebebi bulunan yayınlarla ilgili olarak içeriğin çıkarılmasına ve/veya erişimin engellenmesine karar verilir (5651 sk md.8/1):

- İntihara yönlendirme (md.84),
- Çocukların cinsel istismarı (md.103/1),
- Uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma (md.190),
- Sağlık için tehlikeli madde temini (md.194),
- Müstehcenlik (md.226),
- Fuhuş (md.227),
- Kumar oynanması için yer ve imkân sağlama (md.228).

Bilgi Teknolojileri ve İletişim Kurumu (BTK), 5651 sayılı kanun uyarınca 8. Maddede sayılan bu suçlarla ilgili içeriklerin web üzerinden ihbar edilebilmesi için "İnternet Bilgi İhbar Merkezi [17]"ni kurmuştur. Sitedeki bilgi ihbar formuna, ihbar edilecek sitenin adresi, ihlal içeriğinin detayları ve içerikle karşılaşma tarihi gibi bilgiler eklenerek gerekli ihbar yapılabilmektedir.

Çocukların cinsel istismarı suçuna ilişkin içerikleri oluşturan ve yayan kişilere ulaşmak için gereken bilgiler, soruşturma aşamasında Cumhuriyet savcısı, kovuşturma aşamasında yargılamanın yürütüldüğü mahkeme tarafından, yurtdışı kaynaklı sosyal ağ sağlayıcının Türkiye'deki temsilcisin-

[17] https://www.ihbarweb.org.tr/

den talep edilmektedir. Gereken bilgiler verilmediği takdirde, yurt dışı kaynaklı sosyal ağ sağlayıcının internet trafiği bant genişliğinin %90 oranında daraltılması talebiyle Ankara Sulh Ceza Hâkimliğine savcılık tarafından başvurulabilir (5651 sk. Ek Madde 4/5). Hukuka aykırılığı hâkim veya mahkeme kararı ile tespit edilen içerik sosyal ağ sağlayıcı tarafından çıkarılmaz veya erişim engellenmez ise, sosyal ağ sağlayıcı, doğan zararların tazmin edilmesinden sorumlu olacaktır (5651 sk. Ek Madde 4/14). Bununla birlikte sosyal ağ sağlayıcı, kişilerin can ve mal güvenliğini tehlikeye sokan içerikleri öğrendiği takdirde, bu içeriği ve içeriği oluşturana ilişkin bilgileri yetkili kolluk birimleriyle paylaşmak durumundadır (Ek Madde 4/16).

Hukuka aykırı olarak kişilik hakkına saldırılan kişi aynı zamanda hâkimden, saldırıda bulunanlara karşı korunmasını Türk Medeni Kanunu (TMK)'nun tazminat hükümleri kapsamında isteyebilir (TMK md.24); yani mağdur saldırı tehlikesinin önlenmesini, sürmekte olan saldırıya son verilmesini, sona ermiş olsa bile etkileri devam eden saldırının hukuka aykırılığının tespitini isteyebilir (TMK md.25).

Saldırganlar tarafından bilişim sistemlerinin ve içindeki verilerin direkt olarak hedef alındığı "Doğrudan Bilişim Suçları"nda ise teknik altyapı ile teknik bilginin kullanılması suretiyle bilişim sistemlerine yetkisiz erişim gerçekleşmesi neticesinde, gizlilik, bütünlük ve erişilebilirlik unsurlarından oluşan "Bilgi Güvenliği İlkeleri (CIA – *Confidentiality, Integrity, Availability*) "ne yönelik ihlaller söz konusu olmaktadır ve ilgili fiiller TCK'nın "Topluma Karşı Suçlar" başlıklı 3. Kısmının 10. Bölümü'nde yer alan maddelerle düzenlenmektedir:

- Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak girmek veya orada kalmaya devam etmek; bu fiil nedeniyle sistemin içerdiği verilerin yok olması veya değişmesi; bir bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakillerini, sisteme girmeksizin teknik araçlarla hukuka aykırı olarak izlemek "Bilişim sistemine girme" suçunu (TCK md.243);
- Bir bilişim sisteminin işleyişini engellemek veya bozmak; verileri bozmak, yok etmek, değiştirmek veya erişilmez kılmak, sisteme veri yerleştirmek, var olan verileri başka bir yere göndermek ise "Sistemi engelleme, bozma, verileri yok etme veya değiştirme" suçunu (TCK md.244) oluşturmaktadır.

Bu suçların ortaya çıktığı bilişim teknolojilerinin incelenmesi ve araştırılması, hukuk ve mühendislik biliminin birleşiminden oluşan multi-disipliner ve inter-disipliner bir bilim dalı olan "Adli Bilişim" teknikleri vasıtasıyla yapılmakta ve kovuşturmaya hazır hale getirilmektedir.

II. ADLİ BİLİŞİM İNCELEMELERİ

Bilişim sistemlerinin ve iletişim araçlarının kullanımı, suçluların kimliklerini gizleyerek faaliyetlerini sürdürmelerine olanak tanır. Sahte kimlikli e-posta adresleri ve sosyal medya hesapları kullanarak, halka açık kablosuz erişim noktaları vasıtasıyla internete bağlanmaları tespit edilmelerini zorlaştırmaktadır. Özellikle çocukların cinsel istismarı suçlarında, cep telefonları dikkat çekmeden görüntü kaydetmeyi kolaylaştırırken, internet, üretilen görüntülerin dağıtımında ve erişiminde oldukça etkin bir rol üstlenmektedir. Yine cep telefonları, suçluların çocuklara rahatça ulaşarak, hareketleri üzerinde daha fazla kontrol sahibi olmalarına ve GPS aracılığıyla hareketlerini takip edebilmelerine fırsat vermektedir. Bulut bilişimin yerleşik depolama imkanını ortadan kaldırması, söz konusu suç materyallerinin kolayca ve tespitsiz şekilde depolanmasına imkan sağlamaktadır. Özellikle Dark Web veya Deep Web üzerinden erişime sunulan suç materyallerinin ödemesinin kripto paralarla yapılması, suçluların tespitini zorlaştıran diğer bir unsurdur.

Bilişim suçlarında suçun ve suçlunun ispatında, klasik yöntemlerle elde edilen fiziki delillerin yanı sıra, esas olarak elektronik biçimde saklanan veya iletilen her türlü bilgi aranmaktadır. Elektronik/Dijital delil adı verilen bu bilgiler, elektronik aygıtların doğasından kaynaklanan maddi anlamda elle tutulamama özelliğine rağmen bilişim suçlarının ispatı açısından olmazsa olmaz araçlardır[18]. Bilişim sistemlerinin teknik özelliklerine uygun olarak delil türleri ile bunların depolandıkları alanlar farklılaşabilmektedir. Örneğin çocuk istismarının söz konusu olduğu bir olayda incelenecek cihazlar; bilgisayarlar, cep telefonları, fotoğraf makinesi, video kasetler, web kamera, e-posta, sosyal medya hesapları, taşınabilir depolama üniteler vb.,iken, bu cihazlardan incelenecek veriler; internet erişim kayıtları, sohbet kayıtları, kamera yazılımı, tarih ve saat bilgileri, resim ve video dosyaları, oyunlar, e-posta, adres defteri vb. olmaktadır[19]. Bilişim sistemine hukuka aykırı olarak girme suçunda; IP adresleri, kullanıcı kayıtları, şifreler, kaynak kodları, tarih ve saat bilgileri, çalıştırılabilir dosyalar, internet erişim bilgileri, sohbet kayıtları vb. alanlar incelenmekte, delilin özelliğine göre steganografi analizi, veri madenciliği gibi yöntemler uygulanmakta, görüntü ve DNA veri tabanlarından yardım alınabilmektedir.

Dijital deliller ilk etapta gözle görülemeyen, yapıları gereği hassas, değişmeye, bozulmaya ve yok olmaya müsait niteliktedir. Bu sebeple özel muameleye tabi olmak zorundadır ve ortaya çıkarılmaları için özel donanım ve yazılımlara ihtiyaç vardır[20]. Bu özel donanım ve yazılımlar sayesinde deliller insanlar tarafından algılanabilecek, hukuk tarafından anlamlandırılabilecek ve

---

18 Özkaya P, *Adli Bilişimde Özel Araştırma ve Soruşturma Yöntemleri* (1st edn, Seçkin Yayıncılık 2022) s.34

19 Türkay Henkoğlu, *Adli Bilişim* (2nd edn, Pusula Yayıncılık 2014) s.8

20 Pelin Özkaya, s.66

nihayetinde mahkemece niteliğine uygun şekilde değerlendirilebilecek hale gelmektedir. Bunların sağlanabilmesi ise, adli bilişim aşamalarının işlerlik kazanmasıyla mümkün olmaktadır.

Adli bilişimin ortaya çıkışıyla çok sayıda model geliştirilmiş olsa da, temelde bir adli bilişim süreci yaklaşık 5 aşamayla tanımlanabilir; olayın/suçun tespitiyle başlayan "Tanımlama ve Hazırlık Aşaması"; fiziki ve elektronik deliller ile cihazları "Koruma Aşaması"; uygun yazılım ve donanımlar kullanılarak delillerin eksiksiz ve bütün halde elde edildiği "Toplama Aşaması"; adli kopyaların alınıp, canlı analizlerin yapıldığı "Analiz Aşaması"; elde edilen delillerin mahkemeye sunumu için hazırlandığı "Raporlama ve Sunum Aşaması".

Adli bilişime ilişkin bu aşamalarda usul, Ceza Muhakemeleri Kanunu (CMK)'nun 134, 135 ve 140. Maddelerinde düzenlenmiştir. 134. Madde "Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve El Koyma" fiillerini kapsamakta olup, suça konu olduğu düşünülen bir elektronik cihazın incelenmesinde esas alınacak maddedir. Her ne kadar başlıkta 'bilgisayar' terimi geçse de, üzerinde depolama üniteleri bulunan elektronik cihazlar elektronik deliller ürettiğinden, bu madde diğer bilişim teknolojileriyle işlenen suçlarda da uygulama alanı bulacaktır. Fiziki arama ve el koyma faaliyetlerinden farklı olarak, "somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka surette delil elde etme imkânının bulunmaması" şartına bağlı olarak ve hakim kararıyla bir bilişim sistemi üzerinde arama, kopyalama ve el koyma faaliyeti gerçekleştirilmektedir.

135. Madde Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi üst başlığının altında, "İletişimin Tespiti, Dinlenmesi ve Kayda Alınması" fiillerini düzenleyerek, yine suç işlendiğine ilişkin somut delillere dayanan kuvvetli şüphe sebeplerinin varlığını ve başka suretle delil elde edilmesi imkânının bulunmaması durumlarını arayarak, hâkim kararına vurgu yapmaktadır. Bu madde özellikle içinde sayılan belli suçlar için uygulanabilmektedir.

140. Madde "Teknik Araçlarla İzleme" ise, yukardaki maddelerle uyumlu olarak, somut delillere dayanan kuvvetli şüphe sebeplerinin varlığını ve başka suretle delil elde edilememesi hâlini aramaktadır. Bu madde, şüpheli veya sanığın kamuya açık yerlerdeki faaliyetleri ile işyerinin teknik araçlarla izlenebileceği, ses veya görüntü kaydı alınabileceği durumları düzenleyerek, uygulama alanını yine sayılı suçlarla sınırlı bırakmıştır.

CMK 135. Madde; çocuğun konu olabileceği Göçmen Kaçakçılığı ve İnsan Ticareti (TCK md.79, 80) ile Organ veya Doku ticareti (TCK md.91), İşkence (TCK md.94, 95), Cinsel Saldırı (birinci fıkra hariç, TCK md.102), Çocukların Cinsel İstismarı (TCK md.103), Fuhuş (TCK md.227) fiillerini kapsarken, CMK 140. Madde; Göçmen Kaçakçılığı ve İnsan Ticareti, Organ veya Doku Ticareti ve Fuhuş suçlarında uygulanmaktadır.

İnternetin ve bilişim teknolojilerinin, işlenmesini oldukça kolaylaştırdığı bu suçlarda uluslararası işbirliği mekanizmasının işlerliği oldukça önemlidir. Siber suçlarda diğer suçlardan farklı olarak, fiziki alan sınırının olmaması, faille mağdurun farklı hukuk sistemlerine sahip farklı ülkelerde bulunmaları sonucunu doğurabilmektedir. Suç delillerinin elektronik yapılarından kaynaklanan kolay kaybolup değiştirilme özellikleri, kolluk kuvvetlerinin hızlı hareket etmesini gerektirecek durumlar olup, karşılıklı yardımı zorunlu kılmaktadır.

Adli bilişim incelemeleri sırasında elde edilen deliller içerisinde, mağdur konumdaki çocukların ve gençlerin çok sayıda kişisel verisi de ele geçirilmektedir. Veri koruma kanunları uyarınca koruma altında olan bu verilerin araştırmalar sırasında gizliliğinin sağlanması oldukça önem arz etmektedir. Diğer taraftan, virüs, solucan, Truva atı gibi zararlı yazılımlarla çocukların bilişim sistemlerine giren saldırganlar, onlara ait birçok kişisel veriyi de ele geçirebilmekte, bunları tehdit, şantaj veya manipülasyon unsuru olarak kullanabilmektedir. Bir diğer nemli nokta ise, kişisel verilerin çocukların kendileri veya aileleri tarafından sanal dünyaya bırakılma halidir.

III. KİŞİSEL VERİ GİZLİLİĞİ VE GÜVENLİĞİ

Çocuğun kendisi, ebeveynleri, akrabaları, hatta yabancı kişiler tarafından sanal dünyaya bırakılan bilgiler; kimlikleri, görüntüleri, konumları gibi kişisel verilerini içerdiği gibi, kişilik özellikleri, duyguları, iletişimleri, ilişkileri hakkında da bilgiler sağlayabilir. İstismarcıların çocuğun duygusal ve zayıf yönlerini öğrenerek ilgi alanlarını keşfetmelerine yardımcı olan bu bilgiler, onlarla iletişim kurarak güven kazanmalarına sebep olabilir, ev, okul, kurs gibi konum bilgilerinin paylaşımı onlara fiziki ulaşımı mümkün kılabilir. Diğer bir tehlike ise kimlik hırsızlığıdır.

Verilerin toplanması ile kamu kurumları 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 açabilir ve bu durum onların gelecekteki yaşamlarını da etkilemeye devam edebilecek olumsuz sonuçlar doğurabilir[21].

Birleşmiş Milletler Çocuk Hakları Sözleşmesi[22]'nin 16. Maddesi; "*Hiçbir çocuğun özel yaşantısına, aile, konut ve iletişimine keyfi ya da haksız bir biçimde müdahale yapılamayacağı gibi, onur ve itibarına da haksız olarak*

---

21 United Nations Office on Drugs and Crime (UNODC) Vienna, 'Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children' (2015). <https://www.unodc.org/documents/organized-crime/cybercrime/Study_on_the_Effects.pdf> Erişim Tarihi: 16.12.2021.

22 The United Nations Convention on the Rights of the Child, Kabul Tarihi: 20.11.1989, Genel Kurul Karar Sayısı: 44/25, Yürürlük Tarihi: 02.09.1990

saldırılamaz. Çocuğun bu tür müdahale ve saldırılara karşı yasa tarafından korunmaya hakkı vardır." demek suretiyle özel yaşamına yönelik gerçekleşecek her türlü müdahaleye karşı çocuğu koruma altına almıştır. Aynı düzenleme Türkiye Cumhuriyeti Anayasası'nın 20. Maddesinde de bulunmaktadır. 20. Madde ayrıca; "*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 işlenebili*r" hükmüyle kişisel verilerin korunmasını isteme hakkını özel hayatın gizliliği kapsamında değerlendirmiştir.

A. Çocuğun Açık Rızasının Sınırı

6698 sayılı Kişisel Verileri Koruma Kanunu (KVKK) da açık rıza olmaksızın kişisel verilerin işlenemeyeceğini ve aktarılamayacağını belirtmektedir (md.5/1, 8/1) ve açık rızayı "*belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza*" şeklinde tanımlamaktadır (md.3/1-a). Bununla birlikte çocukların açık rıza vermeleri ve açık rızalarının kanunen kabul edilebileceği yaş sınırı ile ilgili herhangi bir düzenleme bulunmamaktadır. Bu noktada 2018 yılında yürürlüğe giren Genel Veri Koruma Yönetmeliği (GDPR - *General Data Protection Regulation*) md.8/1'e bakıldığında yaş sınırının 16 olarak belirlendiği görülmektedir. İlgili madde; "*...Çocuğun en az 16 yaşında olması halinde, ilgili çocuğun kişisel verilerinin işlenmesi hukuka uygundur. Çocuğun 16 yaşından küçük olması halinde, söz konusu işleme faaliyeti, ancak rızanın çocuk üzerinde velayet hakkı bulunan kişi tarafından verilmesi veya onaylanması halinde ve verildiği veya onaylandığı ölçüde hukuka uygundur*" demek suretiyle belirlenmiş yaş sınırı altındaki çocuklar için rıza verme konusunda velileri yetkili kılmıştır. GDPR, üye devletlere 13 yaşından küçük olmamak kaydıyla, bu amaçlara yönelik olarak kanunla daha küçük bir yaş belirleyebilmeleri konusunda da esneklik tanımıştır.

4721 sayılı Türk Medeni Kanunu md.11 ve 5395 sayılı Çocuk Koruma Kanunu md.3/1 uyarınca 18 yaşını doldurmamış her birey çocuk olarak kabul edilmektedir. Yine TMK md.335 ergin olmayan çocuğun anne ve babasının velâyeti altında olduğunu, md.343 ise, velâyet altındaki çocuğun fiil ehliyetinin, vesayet altındaki kişinin ehliyeti gibi olduğunu söylemektedir. Dolayısıyla, vesayet altındaki küçüğün veya kısıtlının kişiliği ve malvarlığı ile ilgili bütün menfaatlerini korumak ve hukukî işlemlerde onu temsil etmek vasinin yükümlülüğündedir (TMK md.403). Bu düzenleme velilerin açık rıza vermeleri konusundaki GDPR düzenlemesiyle örtüşmektedir ve internetin tehlikelerini ve kişisel verilerin korunmasının önemini algılama konusunda yetersiz olan çocukları korumak açısından mantıklı bir düzenleme olduğu açıktır. Ço-

cukların, bilincin oluşmaya başladığı yaş sınırının altında iken kontrolsüz şekilde internette ürettiği verilerin aileleri tarafından kontrol edilmesi konusunda herhangi bir ihtilaf bulunmamaktadır ancak söz konusu çocuk verileri aileleri tarafından sanal aleme bırakıldığında durum ne olacaktır?

Günümüzde özellikle instagram üzerinde ailelerin bebekleri ve çocukları ile ilgili çok sayıda kişisel veriyi paylaştığı, hatta bazılarının bu paylaşımlardan gelir elde ettiği görülmektedir. Bu duruma ingilizcede 'paylaşma (*share*)' ve 'ebeveynlik (*parenting*)' kavramlarının birleşiminden oluşan bir kavram olan "***Sharenting*** (paylaşan ebeveynlik)" denilmektedir[23]. Paylaşımlar ailelerin kendi hesaplarından yapıldığı gibi, çocuk adına açılıp yönetilen hesaplar üzerinden de gerçekleşmektedir. En yaygın paylaşım türleri fotoğraf ve video olarak görülmekle birlikte, durumun sadece 'görünüm'le sınırlı kaldığı düşünülmemelidir. Çocuğun yüzü, sesi, konuşması, hareketleri biyolojik ve davranışsal biyometrik verileri oluştururken[24], paylaşılan sağlık raporları, test sonuçları, bilişsel durumları hassas sağlık verilerini oluşturmakta, okul, kurs, ev bildirimleri konum verilerini göstermektedir.

Türk hukukunda, ailelerin çocuğun gelecekteki bilinçli varlığından izinsiz şekilde yaptıkları bu veri paylaşımları için başvurulacak kanun yoluyla ilgili herhangi bir düzenleme bulunmamaktadır. BM Çocuk Hakları Hakkında Sözleşme md.3; çocuğun menfaatini esas alarak üstün yararını gözetmekte ve "… *Taraf Devletler, çocuğun ana-babasının, vasilerinin ya da kendisinden hukuken sorumlu olan diğer kişilerin hak ve ödevlerini de göz önünde tutarak, esenliği için gerekli bakım ve korumayı sağlamayı üstlenirler ve bu amaçla tüm uygun yasal ve idari önlemleri alırlar*" demek suretiyle çocuğun özel hayatına haksız ve keyfi her türlü müdahalenin yasak olduğunun altını çizmektedir (md.16). Bu vurgu, hem üçüncü kişilere hem de ebeveynlerine karşı çocuğun korunması gerektiğini belirtmesi bakımından önemlidir.

Çocuk Koruma Kanunu 5/1-a maddesi, çocukların eğitim ve gelişimleri ile yetiştirilmeleri konusunda, çocuğun bakımından sorumlu kişilere 'danışmanlık tedbirleri' almaları konusunu düzenleyerek, yukarda bahsi geçen sorumluluğa çözüm sunan bir vurgu yapmıştır. Aynı maddenin c bendinde ise; bakımdan sorumlu bu kişilerin görevlerini yerine getirmemesi durumunda çocuğun koruyucu aile hizmetlerinden yararlandırılması ya da özel veya resmî bakım yurdu gibi kurumlara yerleştirilmesine karar verilmesi düzenlenmektedir. Do-

---

[23] Hülya Ayhan ve Erdinç Öztürk, 'Dijital Dünyada Ebeveyn Olmanın Görünürde Normal Bir Yansıması Olarak Paylaşan Ebeveynlik (Sharenting): Geleneksel Bir Derleme' (2021) 18(2) Türkiye Klinikleri Adli Tıp ve Adli Bilimler Dergisi 165-77 doi: 10.5336/forensic.2021-82082

[24] Pelin Özkaya ve Refik Samet. 'Biyolojik Biyometrik Sistemler, Biyometrik Veriler, Hukuk ve Güvenlik' Siber Güvenlik ve Savunma - Biyometrik ve Kriptografik Uygulamalar, (1. Basım. 4.Bölüm Nobel Yayıncılık, 2020) 121-180, s.107

layısıyla çocuğun fiziksel ve zihinsel sağlığı ile güvenliğinin sağlanması ailenin temel görevleri kapsamında olduğundan, dijital dünya tehlikelerinin oluşturacağı tehditlerden koruyamayan veya bizzat bu tehditlere açık kapı bırakan ebeveynler için yaptırımlar söz konusu olabilecektir.

Bu açıdan bakıldığında TMK uyarınca mahkemeden velayetin kaldırılmasının istenebileceği (TMK md.348) sonucu çıkmaktadır. Elbette bu düzenlemelerin uygulanmasından önce, gelecekte karşılaşılacak çok sayıda tehlike göz önüne alındığında, çocukları koruyucu ve aileleri bilinçlendirici, sıkı yaptırımlı, kapsamlı ve açık düzenlemeler yapılması konusu ciddiye alınmalıdır. Çünkü teknolojik dünyanın içine doğan çocuklar için oluşturulan dijital kimlikler, yukarda da bahsi geçen suçlar ve hukuka aykırı fiiller bakımından suçlulara ve istismarcılara muazzam fırsatlar sunmaktadır.

B. Çocuk Verilerinin İşlenmesi – Örnek Olaylar

Video paylaşım sitesi TikTok, çocukların konum bilgisi, telefon numaraları ve biyometrik verileri dahil olmak üzere birçok kişisel verisini, yeterli uyarı, şeffaflık ve yasaların gerektirdiği gerekli izinler olmaksızın toplamakla ve, çocuklar ile ebeveynlerine bu verilerin nasıl ve nerede kullanıldığı, hangi üçüncü taraflara aktarıldığı konusunda gerekli bilgilendirmeleri yapmamakla suçlanmaktadır. Bu suçlamalar neticesinde birçok ülkenin veri koruma otoritesi tarafından soruşturulan şirket, farklı ülkeler tarafından para cezalarına mahkum edildi. Aynı sorun Google ve Youtube ile yaşandı, bu şirketler ebeveynlerin izni olmadan çocuklardan yasa dışı şekilde kişisel bilgiler topladığı ve bu verileri İngiltere ve Avrupa veri gizliliği yasalarını ihlal ederek reklamlar üzerinden kar elde etmek amacıyla kullandığı iddialarıyla davalık oldu.

Alman Federal Ağ Ajansı (Bundesnetzagentur), konuşabilen ve cevap verebilen "My Friend Carla" adlı oyuncak bebeğin yasaklanması ve imha edilmesi gerektiği konusunda aileleri uyarmıştı[25]. Uyarının nedeni, bilgisayar korsanlarının oyuncakla oynayan çocukları ve ailelerini yerleşik gizli mikrofonlar sayesinde dinlemesi veya diğer bir senaryo olarak bu cihazların üreticiler haricinde üçüncü şahıslar tarafından hacklenmesi neticesinde dinlenilmesi haliydi. Elektronik Gizlilik Bilgi Merkezi (EPIC - *Electronic Privacy Information Center*) ise bu akıllı oyuncağın kaydettiği görüşmeleri ebeveyn izni olmadan uzak bir sunucuya ileterek gizlilik kurallarını ihlal ettiğini belirtti.

Bir eğitim kurumu, aydınlatma yükümlülüğünü yerine getirmeden ve öğrenciler ile velilerinin açık rızasını almadan hukuka aykırı şekilde "CAS (*Cognitive Assessment System*) Uygulama ve Değerlendirme Testi"ni yapması ve

[25] Bundesnetzagentur, 'Bundesnetzagentur Removes Children's Doll "Cayla" from The Market', (2017). <https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/EN/2017/17022017_cayla.html?nn=404422> Erişim Tarihi: 16.12.2021

test sonucu elde edilen sağlık verilerini hukuka aykırı şekilde başka kişilerle paylaşması sebebiyle Kişisel Verileri Koruma Kurumu tarafından 50.000 TL idari para cezasına çarptırıldı. CAS testi nörolojik ve klinik değerlendirme yapan bir test olup, öğrencinin ilgi alanları, yetenekleri, zeka düzeyi, kişilik özellikleri, akademik başarısı gibi psikolojik özellikleri ile hiperaktivite, kaygı bozukluğu ve dikkat eksikliği gibi ruh sağlığına ilişkin özel nitelikli pek çok veriyi işlemektedir. Özel nitelikli kişisel veriler kanun uyarınca daha sıkı şartlarla koruma altına alınmış olduğundan Kurul, kararında veri sorumlusu okula bu şartları yerine getirmemesi sebebiyle, hukuka aykırı şekilde işlenen verilerin silinmesi, yok edilmesi vb talimatlar da vermiştir[26].

Diğer bir husus, uygulama ve oyun üreticilerinin, kişisel verilerin toplanması, işlenmesi, depolanması ve aktarılması konusunda, kullanıcı konumundaki çocukların anlayabileceği açıklıkta ve uygun dillerde açıklama ve bilgilendirmelerin yapılması konusundaki eksiklikleridir. Yine TikTok üzerinden gidersek, Hollanda Veri Koruma Otoritesi (DPA - *Dutch Data Protection Authority - Autoriteit Persoonsgegevens*), TikTok'un Hollandalı kullanıcılar için bilgilendirme metnini Flemenkçe sunmayarak, uygulamanın kişisel verileri nasıl topladığı, işlediği ve kullandığı konusunda yeterli bir açıklama sağlayamamasını gizlilik yasası ihlali olarak kabul etmiştir[27].

C. Veri Koruma Otorite Tavsiyeleri

Çocuklar genellikle fotoğraflarının, videolarının, bilgilerinin vb. kişisel verileri olduğundan, bu verilerin belirli amaçlar için toplandığından (reklam, uygulama içi deneyimler vb.) ve belli süreler boyunca saklanacağından habersizdir[28]. Hollanda Veri Koruma Otoritesi gibi İrlanda Veri Koruma Komisyonu (DPC - *Data Protection Commissioner*)[29] da kurumlara, çocukların kişisel verilerini işlediklerinde bu verilerle tam olarak ne yapacaklarını çocuklara açıklamak için, çocukların yaş aralığına uygun, açık, sade ve basit bir dil kullanmalarını önermektedir. Bu bilgilerin, çocukların site içinde aramalarını gerektirmeyecek şekilde erişmesi kolay ve görünür bir yerde gösterilmesi (ör-

---

26 Kişisel Verileri Koruma Kurulu, Karar Tarihi: 02.04.2020. Karar Sayısı: 2020/255.

27 Autoriteit Persoonsgegevens (AP), Karar Tarihi: 22.06.2021<https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boete_tiktok.pdf>

28 Sonia Livingstone, Mariya Stoilova ve Rishita Nandagiri, 'Children's Data and Privacy Online: Growing up in A Digital Age, An Evidence Review' (2019) London: London School of Economics and Political Science, <https://www.semanticscholar.org/paper/Children's-data-and-privacy-online%3A-growing-up-in-a-Livingstone-Stoilova/65e26c5308ab20efa9a2e2c4e976457fe18fade2> Erişim Tarihi: 24.12.2021

29 İreland Data Protection Commission (DPC) Children Front and Centre, 'Fundamentals for a Child-Oriented Approach to Data Processing', (2021) s.29. <https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf> Erişim Tarihi: 24.12.2021

neğin, yönlendirmeler, anında açılan pencereler veya fareyi üzerine getirdiğinde çıkan yazılar şeklinde[30]) gerektiği açıklanmıştır. Ayrıca, yalnızca üyelik sırasında değil, gizlilik ayarları değişmeden veya yeni bir çevrimiçi yayın yapmadan hemen önce olacak şekilde devamlılık arz ederek sunulması gerektiği de vurgulanmıştır. Eğer bu bilgilendirmenin yazılı şekilde yapılması amaçlanıyorsa, parlak renkler, büyük boy yazı tipleri, okunması kolay listeler vb. kullanılarak dikkat çekici şekilde sunulmalıdır. Metin haricinde görsel unsurlar kullanılarak yapılacaksa, resim, video, karikatür, çizgi film veya oyunlaştırma yöntemleri kullanılarak çocukların daha kolay kavramaları sağlanabilir. Çocukların/gençlerin bu süreçte kişisel verilerinin akıbeti ve gizlilik hususlarıyla ilgili bilgilenme konularında herhangi bir soruları olduğu takdirde, veri işleyen kuruluşlara doğrudan (örneğin, e-posta adresi, anlık sohbet, telefon vb.) ulaşma imkanı da sağlanmalı, bu imkanlar da onların kolayca ulaşabileceği görünür yerlerde yer almalıdır.

Kanada Gizlilik Komiserliği Ofisi (OPC - *Office of the Privacy Commissioner of Canada*) ailelere, çocuklarına dijital dünyadaki gizlilik ve mahremiyetlerini sağlama konularında eğitim verirken yararlanabilecekleri eğlenceli aktiviteler önermektedir[31]. Bu aktiviteler[32]:

- Yılanlar ve Merdivenler *(Privacy Snakes and Ladders)*: Yılan ve merdiven şeklindeki oyun tahtasında 1'den 50'ye kadar sayılar bulunan kareler vardır. Atılan zardan çıkan sayı kadar karelerde ilerlenir. Oyuncular güçlü şifre oluşturduklarında veya internette gördükleri kötü muameleyi bir yetişkine söylediklerinde merdiveni tırmanır; bir şifreyi veya kendisine ait olmayan bir resmi arkadaşlarıyla paylaştıklarında yılandan aşağı kayar.
- Noktaları Birleştirme *(Connect the Dots)*: Tamamlanmamış bir resimde 1'den 16'ya kadar numaralandırılmış noktalar vardır. Noktalar birleştirildiğinde resmin altında bir metin görünür ve ilgili kutucukların işaretlenmesi beklenir: "Çevrimiçi gizliliği iyi şekilde uygulamak için evinizde sahip olduğunuz kuralları kontrol edin":

- Çevrimiçi olarak bilgi/verinin nasıl paylaşılacağını öğrenmek için güvendiğimiz bir yetişkinle birlikte çalışacağız.
- Tıklamadan önce düşüneceğiz. Fotoğrafları, videoları ve yorumları kaldırmak bazen zor olabilir.
- İnsanlara çevrimiçi olduğumuzda nerede olduğumuzu söylemeyeceğiz.

---

30 Anna Morgan, 'The Transparency Challenge: Making Children Aware of Their Data Protection Rights and The Risks Online', (2018) s.3. <https://www.dataprotection.ie/sites/default/files/uploads/2019-02/TransparencyChallenge.pdf> Erişim Tarihi: 24.12.2021

31 Bknz: https://www.priv.gc.ca/en/about-the-opc/what-we-do/awareness-campaigns-and-events/privacy-education-for-kids/t-v/activ/index/

32 Bknz: https://www.priv.gc.ca/en/opc-news/news-and-announcements/2019/an_190826/

- İstemediğimiz bir şeyi internete koyarsak bir yetişkinden yardım isteyeceğiz.
- Ebeveynimize veya velimize sormadan oyun satın almayacağız.
- Ebeveyn veya veliye sormadan bir uygulamayı (ücretsiz olsa bile) indirmeyeceğiz.

***Şifreleri Öğrenme / Tableti Renklendirme*:** Çocukları boşlukları doldurarak sekiz karakterli güçlü ve benzersiz şifreler oluşturmaya zorlayan oyunda, şifrelerin iyi veya kötü şekilde koruduğunu tableti renklendirerek göstermelerini ve kilit resmi çizmelerini ister.

Kelime Arama: Çocukların "bilgisayar, göndermek, tıklamak, paylaşmak vb." kelimeleri bulmaları için bir bulmacayı taramalarını sağlayarak gizlilikle ilgili kelime dağarcığını genişletir.

Bunların haricinde "Boyama etkinliği", "2 resim arasındaki 13 farkı bulma", "Fotoğraftaki kişileri etiketleme" ve "Kriptografi alıştırması" etkinlikleri ile gizlilik sorunları hakkında farkındalığı artırmalarına ve mahremiyet risklerini azaltmalarına yardımcı olacak bilgiler sağlamaya çalışılır.

OPC bu etkinlikler aracılığıyla çocuklara "Çevrimiçi Gizliliğinizi Korumak İçin 5 İpucu" da önermiştir:

- Göndermeden önce düşünün! İnternette paylaştığınız fotoğrafları, yorumları, mesajları ve videoları, siz veya aileniz onları yayınlamadan önce düşünün.
- Gönderdiğiniz ve paylaştığınız şeylerin özel kalmayabileceğini ve insanların çevrimiçi olarak bunları kopyalayıp başkalarına gönderebileceğini unutmayın.
- Arkadaşlarınızın kim olduğunu bilin. Birini şahsen tanımıyorsanız, o kişinin gerçekte kim olduğundan emin olamazsınız.
- Gizliliğinizi parolalarla koruyun. Güçlü parolalar oluşturmayı öğrenin ve bunları başkalarıyla paylaşmayın.
- Arkadaşlarınıza saygı duyun. Siz veya bir ebeveyn paylaşmadan önce başka birinin fotoğrafını veya videosunu paylaşmanın uygun olup olmadığını sorun. İnternetteki diğer insanlar hakkında kötü şeyler söylemeyin.

Kişisel Verileri Koruma Kurumu ise, uygulama geliştiriciler için çocukların kişisel verileri konusunda bazı uyarılarda bulunmuştur[33]:

- 6698 sayılı KVKK'ya en yüksek uyumun sağlanması,

[33] Kişisel Verileri Koruma Kurumu, 'Çocukların Kişisel Verilerinin Korunması, Ürün ve Hizmet Geliştirenler Tarafından Dikkat Edilmesi Gerekenler Rehberi' <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/db0b3f30-c636-4fcb-930a-bf8f2e524de8.pdf> Erişim Tarihi: 17.12.2021

- Veri işleme faaliyetlerinde veri minimizasyonu ilkesine uygunluk,
- Çocuğun yaşını doğrulayacak sistemlerin kullanımı,
- Açık rıza ve bilgilendirme metinlerinin gerekli hallerde velayet/vesayet hakkı sahiplerinin iletişim bilgilerine gönderilmesi,
- Teknik ve idari tedbirlerin maksimum seviyede uygulanması,
- Çocukları kendi haklarının varlığı ve bu hakların kullanımı konularında bilgilendirme, bunlara uygun mekanizmalar geliştirme ve politikalar düzenleme,
- Çocukların algı düzeyine ve yaş aralığına uygun bilgilendirme metinleri hazırlama, daha kavrayıcı olması için bu metinleri görsel öğelerle destekleme.

Özellikle çevrimiçi oyunlar ve sosyal medya platformları açısından oluşabilecek tehlikelerin önüne geçmek için uygulama geliştiricilerin bahsi geçen konularda dikkatli olması ve sorumluluk alması oldukça önemlidir. Çünkü bu mecralar farklı nitelikli ama çocuklara ve gençlere zarar verme bakımından birbirinden aşağı kalmayacak pek çok ciddi tehlikeyle doludur.

IV. ÇEVRİMİÇİ OYUNLAR VE SOSYAL MEDYA

Çocuklarla temas kurulan en kolay platformlar, sosyal medya uygulamaları ile çevrimiçi (online) oyunlar olmaktadır. Bazı durumlarda anlayışlı bir yetişkin rolüyle, bazense başka bir çocukmuş gibi davranan kişiler çocuklarla iletişim kurarak güven kazanmakta, onları buluşmaya veya cinsel içerikli eylemlerde bulunmaya ya da özel görüntülerini yollamaya ikna etmektedir. Ailesiyle veya arkadaşlarıyla iletişim sorunları yaşayan çocuklar, yabancı biri de olsa kendilerini anlayan kişilere yakınlık duyma eğilimindedir. Bu durumun zararları hakkında bilgisi olmayan veya henüz anlama kapasitesi gelişmemiş çocuklar saldırganlara kendileriyle yakınlaşmaları için birçok fırsat vermektedir. Güven ilişkisi haricinde, kandırma, manipülasyon veya tehdit yöntemlerine başvurduklarında ise maruz kaldıkları duygusal baskılara direnemeyen çocuklar, her türlü bilgiyi, ev adreslerini ve okul bilgilerini verebilmekte, birçok olumsuz davranışa boyun eğebilmektedir.

İstismarcılarla iletişim haricinde farklı başka tehlikelere de sebebiyet veren bu platformlar, kendine veya başkasına zarar verme, öldürme, intihar etme, soygun-hırsızlık yapma gibi eylemler konusunda çocuk ve genç kullanıcıları yönlendirmede kullanılabilmektedir. Bu noktada gerçek hayatta yaşanmış birkaç örneği açıklamak faydalı olacaktır:

2008 yılında Galler'de gerçekleşen ve 25 gencin ölümüyle sonuçlanan "Bebo Vakası", sosyal paylaşım sitesiyle yayılan bir intihar dalgasıydı. "İnternet İntihar Tarikatı" adı verilen olayda, gençlerin hepsi kendini asarak intihar

etmişti[34]. Olayın gizemi hiçbir zaman gerçekten çözülemedi ancak ortak kanı, medyada yayınlanan haberlerin gençler üzerindeki olumsuz etkisi üzerineydi. İntihar haberlerinin servis edilişindeki 'heyecan', ölenleri sürekli gündemde ve ilgi odağı halinde tutarak 'ünlü' haline getiriyordu. Uzmanlar, çevresi tarafından dışlanan veya görmezden gelinen çocuklardaki ilgi çekme arayışını yansıtan bir olay olarak kabul etti.

Sonraki yıllarda ortaya çıkan "Mavi Balina - *Blue Whale* (2015)" ve "Momo Challenge (2017)" çevrimiçi oyunları nedeniyle dünyanın birçok ülkesinde intihar eden çocuk sayısındaki artış tehlikenin boyutunu daha geniş bir perspektiften gözler önüne sermektedir. WhatsApp üzerinden gönderilen bir link ile erişilebilen bu oyunlarda grup yöneticisi tarafından, belirli bir süre boyunca tamamlanması, belgelenmesi ve yayınlanması gereken görevler, seçilen oyunculara dağıtılmakta, oyuncuların ise bir kez başladıkları oyunu bırakmalarına izin verilmeyerek, şantaj ve siber zorbalıkla oyunu tamamlamaları için baskı yapılmaktadır. Oyuncuların korku içinde yaşamalarının amaçlandığı oyunlardaki, mezarlığa gece yarısı tek başına gitme, her gece korku filmi izleme gibi görece daha az zararlı ilk görevler, aşamalar ilerledikçe kendine zarar verme şeklinde şiddetini artırmakta ve son görev intihar ettirmeye yönelik olmaktadır. Oyun sebebiyle ölen çocukların arkalarında bıraktıkları notlar ve videolar ile, kurtulan çocukların ifadeleri dehşeti çarpıcı şekilde gözler önüne sermektedir.

Bazı oyunlarda ise karakter, mülk, silah gibi ekipmanların satın alınması için gerçek paranın kullanılması sistemi benimsenmektedir[35]. Bu durum, çocukların gerekli ekipmanları alabilmek için ailelerinin kredi kartlarını çalmaları şeklinde sonuçlandığı gibi, diğer oyuncuların hesaplarını ve karakterlerini çalma şeklinde de görülebilmektedir. 2007 yılında 17 yaşında bir çocuk (aynı yaş grubunda birkaç çocukla birlikte) 3D sosyal ağ sitesi "Habbo Hotel"den gerçek parayla satın alınan 4.000 avro değerindeki sanal mobilyayı çalmakla suçlandı. Habbo kullanıcıları, gerçek parayla satın aldıkları Habbo kredileri ile ödeme yaparak oyun oynayabilmekte, kendi karakterlerini oluşturabilmekte ve kendi odalarını dekore edebilmektedir. Oyun sahipleri, hırsızlık yapabilmenin tek yolunun, oyuncuların kullanıcı adı ve şifrelerini ele geçirip, oturum açarak mobilyaları almak olduğunu söylediler ve hırsızlık olayının bu şekilde gerçekleştiğini iddia ettiler. Aynı olay 2010 yılında tekrar yaşandı.

Özellikle Japonya'da ve Güney Kore'de yaygın olarak oynanan "Lineage II"-nin iki oyuncusu, diğer oyuncuların karakterlerini yenmek ve değerli eşyalarını

---

34 Rainer Kurz, 'Bridgend "Bebo Internet Suicide Cult" And Ritual Violence in Wales' (2017) 41(S1), 25th European Congress of Psychiatry of the in Florence. European Psychiatry 888-S889. doi:10.1016/j.eurpsy.2017.01.1803

35 Erıc J. Hayes, 'Playing it Safe: Avoiding Online Gaming Risks'. Cybersecurtiy&Infrastructure Security Agency (CISA). <https://www.cisa.gov/uscert/sites/default/files/publications/gaming.pdf> Erişim Tarihi: 19.12.2021

çalmak için web üzerinden çalışan bot yazılım kullandılar. İnsan oyuncu yerine bir yazılım tarafından kontrol edilen oyun karakteri yenilmezdi ve diğer oyuncuların onu yenmesi için karakterlerinin savaş özelliklerini geliştirmeleri gerekmekteydi. Bunun için ücretsiz araçlar sunan bir web sitesi oluşturdular ve bu sayede kullanıcı adı ve şifreler ele geçirildi. Çalınan sanal eşyalar daha sonra gerçek parayla değiştirildi. Toplamda, yaklaşık 1 milyon yen (yaklaşık 12.000 ABD Doları) kazandıkları ve 100'den fazla kişinin hesabını ele geçirdikleri iddia edildi.

Hırsızlık ve dolandırıcılık haricinde ölümle sonuçlanan bir olay ise; bir oyuncunun oyunda kullanılan bir silah yüzünden başka bir oyuncuyu öldürmesiyle gerçekleşti. Oyuncuların savaşçı, büyücü ve rahip rollerini üstlendiği bir fantezi dünyasında geçen "Legends of Mir 3" oyununda oyuncular seviye olarak geliştikçe daha güçlü silahları kullanabilir hale gelmekte ve milyonlarca dolarlık değere ulaşan bu oyun ekipmanları siteler üzerinden alınıp satılmaktadır. Bir oyuncu yüksek değere ulaşan "ejderha kılıcı"nı ödünç verdiği kişinin, bu kılıcı satarak gerçek paraya çevirdiğini öğrenince onu öldürdü ve ömür boyu hapse mahkum edildi. Bu olaydaki tarafların birer yetişkin olması, çocukların oyuncu olarak yer aldığı bu tip oyunlarda tehlikeyi ortadan kaldıran durumlar olmamakta ve bu büyük riskler çocukların her zaman yanı başında durmaktadır.

"The Sims" rol yapma oyunları içinde belki de en ünlü olanıdır. Oyuncu, görünüş, kişilik, duygu dünyaları, meslek, ilişki vb gibi konularda, kendi seçeceği özelliklere göre yarattığı karakteri bir evde yaşatabilmekte, işe veya okula gönderebilmekte, sosyalleştirebilmekte veya evlendirip yuva kurdurabilmektedir. Oyun teknolojiyle birlikte epey gelişti, önceleri çevrimdışı bir simülasyon oyunu şeklindeyken sonraları dünyanın birçok yerindeki çok sayıda gerçek insanın yönlendirebildiği, çevrimiçi olarak oynanabilme özelliği olan bir oyun halini aldı. Oyunun para birimi 'simolean'ın gerçek para birimi karşılığı bu oyunda da bulunmakta ve oyunda artık yasadışı olarak kabul edilebilecek aktiviteler de yer almaktadır. Elbette bu durum, yaşça küçük oyuncuların da bulunduğu bu ortamda, kötü örnek teşkil edici birçok unsur barındırırken, istismarcılar için de kimliklerini gizleyerek kalmaları için ideal bir ortam oluşturmaktadır. Tüm bu sebeplerle oyun 13 yaşından küçüklere yasaklanmıştır. Yazacağı yeni kitap için sanal hukuk sistemlerini ve oyun içinde sosyal kültürün gelişimini inceleme ve belgeleme amacıyla oyuna katılan Michigan Üniversitesi felsefe profesörü Peter Ludlow'un, oyunda seçtiği karakter bir gazete muhabiriydi. Bu meslek vesilesiyle mahallenin kötü adamı olan ve sanal bir genelev işleten Evangeline karakterinin gerçek hayatta 17 yaşında bir çocuk olduğunu ve müşterilerine para karşılığı siberseks hizmeti sunduğunu ortaya çıkardı[36]. Oyunun, çocukların psikolojik ve hatta fiziksel gelişimini olumsuz yönde etkileyici çok sayıda de-

36 Bknz: Evangeline Röportajı 'Alphaville Herald, Evangeline: Interview with a Child Cyber-Prostitute in TSO' (2003) <http://alphavilleherald.com/2003/12/evangeline_inte.html> Erişim Tarihi: 18.12.2021

tay barındırdığını da ifşa eden Ludlow'un oyun sahibi şirket tarafından hesabı sonlandırıldı[37].

Diğer bir oyun faciası, 'sanal uzayda tecavüz' adıyla bilinen olaya sahne olan "LambdaMOO" oyununda yaşandı. Oyunda, bir kullanıcı kendi karakterini istediği gibi yaratabilmekte, diğer karakterlerle etkileşime sokabilmekte ve odalar, mobilyalar dahil olmak üzere yeni nesneler oluşturabilmektedir. "Bungle" adında bir karakter, Voodoo bebeği alt programını kullanarak, diğer iki karakterin kontrolünü ele geçirdi ve bu karakterleri sadist tecavüz eylemlerinde kullandı[38].

Tüm bu örnek olaylar ve daha fazlası gösteriyor ki, sanal davranışın gerçek psikolojik ve fiziksel sonuçları olabilmekte, özellikle çocuklar üzerinde travmatik etkiyle sonuçlanabilmektedir. Çoğu ebeveynin çocuğunun oynadığı oyunlar veya üye olduğu sosyal platformlar hakkında herhangi bir bilgisi yoktur hatta meşgul ebeveynler için çocukları oyalamak açısından teşvik edilen uygulamalardır. Ancak görülüyor ki hırsızlıktan tecavüze hatta cinayete kadar korkunç etkileri bulunmaktadır. Dahası ülkeler, ne sanal soygunlar ne de sanal tecavüzler için hiçbir hukuki düzenlemeye sahip değildir ve bu olayların nasıl sonuçlanacağı tamamen belirsizdir, hukukun bu alanlara eğilmesi konusundaki aciliyet ise oldukça belirgindir. Ailelerin, bakıcıların ve eğitimcilerin, dijital dünyanın her bir noktasında daha dikkatli, daha bilinçli ve daha etkili duruş sergilemeleri hayati bir zorunluluk halini almıştır. Oyun ve uygulama geliştiricilerin ise üye kullanıcı davranışları üzerindeki denetim konularında daha keskin politikaları olmalı, yükümlülükleri ise daha katı kurallara bağlanmalıdır. Sanal dünyanın öngörülemez ve zamanında durdurulamaz özelliğinin gelecekte de katlanarak süreceğini düşünürsek her türlü senaryoya hazır olmak bariz bir zorunluluk olarak karşımızda durmaktadır.

V. DEĞERLENDİRME VE ÖNERİLER

Ebeveynlerin çocuklarının internette geçirdikleri zamanlarla ilgili daha fazla bilgi sahibi olması önemlidir. Çocuklar kişilik ve mahremiyet hakları olan bireyler olmakla birlikte, tehditleri ve tehlikeleri anlamaları konusunda yardıma ihtiyaçları vardır. İnternetten ve dijital dünyadan çocukları tamamen uzaklaştırmak mümkün olmadığı gibi sağlıklı bir çözüm de sunmayacaktır. Harcadıkları saat sayısını azaltmak veya en verimli şekilde kullanmalarını sağlamak daha faydalı sonuçlar verirken, birtakım tedbirlerle süreci doğru şekilde yürütmeye çalışmak daha anlamlı olacaktır. Sosyal medya hesaplarının arkadaş listelerinde sadece tanıdıkları kişilerin bulunması, kullanıcı adı ve soyadı yerine takma isim (*ni-*

---

37 Bknz: 'Line Between Virtual and Real Blurred in Online Game' (2005) Tampa Bay Times. <https://www.tampabay.com/archive/2004/02/16/line-between-virtual-and-real-blurred-in-online-game/>Erişim Tarihi: 18.12.2021

38 Chuck Huff, Deborah G. Johnson ve Keith W. Miller, 'Virtual Harms and Real Responsibility' (2003) 22(2) IEEE Technology and Society Magazine, 13.

ckname) kullanmaları, gizlilik ayarlarının düzenlenmesi ve güçlü parolalarla hesaplarını güvende tutmaları başlangıç için önemli tedbirlerdir. Çocukların hangi web sitelerini kullandığı ve hangi çevrimiçi oyunları oynadığı konusunda aileler bilgi toplamalı ve onları nasıl güvende tutacaklarına dair kendilerini eğitmelidir. Çocuklarla iletişimi iyi tutmak, onları dijital dünya ve riskleri hakkında bilgilendirmek, herhangi bir sorunla karşılaştıklarında destek olunacağına dair güven vermek öncelikli eylem planı olmalıdır.

Dijital okuryazarlığın önemi tam da burada kendini göstermektedir. Ailede başlayıp okulda devam eden bir bilgilendirme süreci sağlanması çok önemlidir çünkü çocuklar artık evde olduğu kadar okullarda da bilişim teknolojileriyle temas halindedir. En basit haliyle artık her çocuğun elinde akıllı telefon, tablet ve diğer dijital cihazlar bulunmakta ve bunlarla her yerden internete bağlanmaları mümkün olmaktadır. Çocukların ilk rol modelleri ebeveynleri olmakla birlikte, yaşları ilerledikçe öğretmenlerinden ve en çok da akranlarından etkilenmektedirler. Bu sebeple, özellikle okul döneminin erken sınıflarından itibaren onlara, çevrimiçi ortamda iletişim kurmanın usulleri, içerik paylaşmanın riskleri konularında bilgilendirmeler yapılmalı, mahremiyetin ve kişisel verilerin önemi, gizlilik ayarlarının kontrolünün yapılmasının yöntemleri öğretilmeli, siber zorbalık, takip, sömürü, pornografi gibi tehlikeler konusunda eğitimler verilmeli, bu hususların erken sınıflardan itibaren müfredata eklenmesi sağlanmalıdır. Elbette gösterilecek bu farkındalık faaliyetleri için önce ebeveynler, bakıcılar, öğretmenler ve eğiticiler gerekli eğitimleri almalı, uygulamaları tecrübe etmelidir.

Oyun ve uygulamalar açısından, bu platformlarda oluşturulan profillerden gerekli bilgileri toplayarak yeni hesaplar oluşturmak, içerikleri satmak veya mevcut finansal hesaplara erişmek kimlik hırsızlığı ile mümkün olurken, sosyal mühendislik[39] yöntemleri ile sahte yamalar veya zararlı yazılımlar bulunan eklentiler indirmeleri için çocuklar sahte web sitelerine yönlendirilebilir. Böylece kötü niyetli kişiler bilgisayarları uzaktan kontrol edilebilir ve çocukların çevrimiçi etkinliklerini izleyebilir. Oyun ve uygulama indirirken, satıcıların itibarlı olduğundan emin olmak ve bunları güvenilir sitelerden indirmek önemlidir. Sistemlerin güvenliğinin sağlanması, gizlilik ve mahremiyet protokolleri, uygulama ve üyelik kuralları ürün tasarımları sırasında ticari kaygılardan daha öncelikli olarak dikkate alınmalı, geliştiriciler için etik protokoller ve standartlar oluşturulmalıdır. Çocuklar ve gençler için tehdit oluşturacak içeriklerin ve materyallerin dolaşımını engelleyici önlemler alınması, diğer kullanıcıların faaliyetlerinin titiz denetlemelere tabi tutulması ve yargıya intikal eden olaylarda işbirliği konusunda daha istekli davranılması da önemli hususlardandır. Yaş

[39] Sosyal Mühendislik (*Social Engineering*): Bir siber saldırıyı gerçekleştirmek, gizli veya hassas bilgileri ifşa etmek için insan davranışlarından ve hatalarından yararlanarak, ikna ve güven yöntemleriyle manipüle etme sanatıdır. Saldırganlar kurbanları ile iletişime geçerek onların güven, aciliyet ve merak, korku gibi duygularına odaklanır.

doğrulama, filtreleme, izinli veya engelli listeler oluşturma ve ebeveynler için şifre koruma özellikleri bulunan uygulamalar geliştirme çocukların kontrolsüz mesailerine de çözüm sağlayabilir[40].

İnternetin rahatlığı ve ucuzluğu, bilişim teknolojilerinin doğasından kaynaklanan özellikler ile birleşince, bilişim suçları sınır ötesi nitelikli hale gelerek, saldırganların ve istismarcıların dünyanın herhangi bir yerindeki bilişim sistemine girmesine imkan sağlamaktadır. Elektronik cihazların hızlı şekilde alınıp satılması, suç delillerini yok etmek için bu cihazların kolaylıkla imha edilebilmesi, başkalarının cihazlarının ve sistemlerinin yaygın şekilde kullanılması bu süreci kolaylaştıran diğer etkenler olmaktadır. Dijital delillerin değişmeden ve bütün halde elde edilmesindeki zorluk ve elektronik verilerin tamamen yok edilmesindeki imkansızlık ise suçluların tespitinin ve yakalanmasının zorluğunu arttırmakta ve bu suçların soruşturulması, kovuşturulması ve hüküm verilmesi süreçlerinde özel düzenlemeleri zorunlu kılmaktadır. Bu suçların kıtaları aşan bağlantılar sağlaması sebebiyle ülkeler arası yardımlaşma kuralları konulmalı, yargılamalarda paralellik sağlanması açısından uluslararası hukuki düzenlemelere uygun ulusal kanunlar ile uluslararası standartlara uygun en iyi uygulama rehberleri *(best practices)* oluşturulmalıdır. Bilişim suçları, siber güvenlik ve adli bilişim kurallarına ilişkin düzenlemelerin ayrı kanunlar halinde ve bütün halde hazırlanması gelecekteki teknolojik gelişmeler de göz önüne alındığında, uygulayıcılar açısından hakkaniyetli ve hukuka uygun uygulamalar ve yargılamalar için hayati önem taşımaktadır. Hukukun, internet ve teknolojinin gelişim ve dönüşüm hızı karşısında geride kalması, çoğu fiilin cezasız kalmasına ve mağduriyetleri arttırmasına sebep olmaktadır. Örneğin, çocuk pornografisi, siber takip, siber taciz ve siber zorbalık gibi eylemlerle ilgili açık düzenlemeler yapılması bir ihtiyaçtır, çünkü bu fiillerin verdiği zararlar bariz şekilde önümüzde durmaktadır. Dahası, ceza kanunlarında yer alan ve çocukların konu olduğu suçların bilişim sistemleri vasıtasıyla işlenmesi halleri ağırlaştırıcı sebep sayılmalıdır. İnternet ortamında çocukların ve gençlerin gelişimlerini, psikolojilerini ve güvenliklerini zedeleyici yayınların ortadan kaldırılması veya erişimlerinin engellenmesi hususlarındaki düzenlemelerin de daha detaylı ve daha engelleyici olması sağlanmalıdır. Aynı durum çocuk kişisel verileriyle ilgili özel düzenlemeler açısından da geçerlidir. Veri koruma kanunları çocuklarla ilgili düzenlemeleri genişletmeli ve keskinleştirmeli, veri işleyen ve veri aktaranlara daha fazla yükümlülük yüklemelidir. Özellikle çocukların konu olduğu çevrimiçi suçların soruşturulmasında çocuk verilerinin anonimleştirilmesi/maskelenmesi çocukların en yüksek menfaatleri ışığında uygulanmalıdır, çünkü kişisel verilerin gizliliği her bireyin güvenliği için çok önemlidir ancak çocuklar için hayatidir.

---

[40] Kimberly J. Mitchell, David Finkelhor, Janis Wolak. The Exposure of Youth to Harmful Content on the Internet. A National Survey of Risk, Impact and Prevention" (2003) 34(3) Youth & Society 330-358 p.332 DOI:10.1177/0044118X02250123

SONUÇ

Teknoloji ve internetin ortaya çıktığı ilk yıllarda insan hayatını bu kadar etkileyeceği muhtemelen tahmin edilmemişti. Geldiğimiz noktadan geleceğe baktığımızda çok daha fazlasının olduğunu artık görebiliyoruz. Akıllı telefonlar yerini akıllı evlere, akıllı şebekelere ve akıllı şehirlere bırakıyor. Yapay zekanın ve nesnelerin internetinin yaygınlaştığı günümüzde gelecekteki planlarımızı tam otonom robotlar üzerine kurmaya başladık. Dahası, online oyunların evrimleşmesi, artırılmış gerçeklik, 3D teknoloji, VR ve AR gözlükler vasıtasıyla yaratılan "Metaverse" evreni hızlıca geliştiriliyor ve fiziki hayatın yerini yavaş yavaş almaya başladı bile. Çocuklar artık böyle bir dünyanın içine doğuyorlar. Doğum anlarından itibaren hayatlarının her anı ebeveynleri tarafından paylaşıldığından dijital kimlik sahibi oluyorlar ve bu durum hayatlarının her alanına sirayet ediyor. Onlar artık bu dünyanın doğal sakinleri konumunda ve bitmeyen merakları ile sürekli keşfetme ihtiyaçları daha fazlasına çekilmelerini sağlıyor. Dahası, her şeyin internete bağlanmış olması, eğitim, sosyalleşme, iletişim, bilgi, oyun, eğlence, film vb. birçok materyale erişim için de onları çevrimiçi kalmaya mecbur kılıyor. Bu durumun eğitim olanaklarına ve çeşitli hizmetlere erişim noktasında sayısız faydası olmasının yanında, ruhsal ve zihinsel gelişimlerine de birçok olumlu katkısı bulunmaktadır. Tüm bunlara rağmen teknolojinin kullanımı açısından zihinsel ve eylemsel açıdan hazır olsalar bile, zorluklar ve riskler konusunda psikolojik olarak savunmasızlar. Bu savunmasızlık hali, ebeveynler, bakıcılar ve öğretmenlerin farkındalık ve bilgi eksikliği ile birleşince failler için ideal ortamlar haline gelmekte ve çocukların bu ortamlarda hasarsız ve zarar görmeden kalmaları ise gittikçe zorlaşmaktadır.

Tüm bu nedenlerle, bu makalede çocukların sanal dünyada karşı karşıya kaldığı tehlikeler farklı kalemler halinde sıralanarak, gerek aileler ve eğitimciler, gerek sektörlerde faaliyet gösteren kişi ve kuruluşlar, gerekse devlet organları açısından yapılması gerekenlerle ilgili tavsiyelerde bulunularak hukuki çerçeve çizilmeye çalışılmıştır. Sağlıklı bir toplum, yarının büyükleri olacak bugünün çocuklarının fizyolojik ve psikolojik olarak zarar verici her türlü faktörden korunarak, güvenli ortamlarda büyümelerinin sağlanmasıyla oluşturulur. Çocuğun üstün yararı ilkesi her zaman ilk sırada tutularak, ortak güçlüklerin üstesinden gelmeyi amaçlayan koordinasyon çalışmaları, aileler, üniversiteler, özel sektör, sivil toplum örgütleri ve devletlerin elbirliği ile çalışması durumunda faydalı sonuçlar verecektir. Güçlü kanunlar ve detaylı rehberler, bilinçli ve eğitimli insanların çabalarıyla birleştiğinde, çocuklar ve gençler için daha güvenli ve daha huzurlu bir dünyanın yaratılması sağlanacak, devletlerin ortak eylemleri ve işbirliği ile sınır ötesi nitelikli bilişim suçlarıyla mücadelede de kıtalar üstü bir başarı sağlanacaktır.

KAYNAKÇA

Autoriteit Persoonsgegevens (AP) Karar Tarihi: 22.06.2021 <https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boete_tiktok.pdf>

Ayhan H ve Öztürk E, 'Dijital Dünyada Ebeveyn Olmanın Görünürde Normal Bir Yansıması Olarak Paylaşan Ebeveynlik (Sharenting): Geleneksel Bir Derleme' (2021) 18(2) Türkiye Klinikleri Adli Tıp ve Adli Bilimler Dergisi 165-77 doi: 10.5336/forensic.2021-82082

Birleşmiş Milletler Çocuk Haklarına Dair Sözleşme Genel Yorum No:13 (United Nations Committee on the Rights of the Child, Convention on the Rights of the Child, General Comment No. 13) Kabul Tarihi: 17.01. – 04.02.2011 <http://humanistburo.org/dosyalar/humdosya/BM%20CHK%20Genel%20Yorum%20No13%20-%20Cocuga%20Karsi%20Siddet.pdf> Erişim Tarihi: 22.12.2021

Birleşmiş Milletler Çocuk Haklarına Dair Sözleşme Genel Yorum No:25 (United Nations Committee on the Rights of the Child, Convention on the Rights of the Child, General Comment No. 25 on Children's Rights in Relation to The Digital Environment). Yayınlanma Tarihi: 24.03.2021. <https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CRC%2fC%2fGC%2f25&Lang=en> Erişim Tarihi: 16.12.2021

Bundesnetzagentur. 'Bundesnetzagentur Removes Children's Doll "Cayla" from The Market'. (2017). <https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/EN/2017/17022017_cayla.html?nn=404422> Erişim Tarihi: 16.12.2021

Ceza Muhakemesi Kanunu, Kanun Numarası : 5271, Kabul Tarihi : 4.12.2004, RG 17.12.2004/25673

Children's Internet Protection Act (CIPA). Kabul Tarihi: 21 Aralık 2000. Pub. L. 106-554 art. 1711, 1721 <http://ifea.net/cipa.html>

Children's Internet Protection Act (CIPA) 'Study of Technology Protection Measures in Section 1703' (2003). Department Of Commerce National Telecommunications and Information Administration. <https://www.ntia.doc.gov/files/ntia/publications/cipareport08142003.pdf> Erişim Tarihi: 16.12.2021

Çocuk Haklarına Dair Sözleşmeye Ek Çocuk Satışı, Çocuk Fahişeliği ve Çocuk Pornografisi ile İlgili İhtiyari Protokol. Yürürlük Tarihi: 18.01.2002. <https://www5.tbmm.gov.tr/kanunlar/k4755.html> Erişim Tarihi: 22.12.2021.

Çocuk Koruma Kanunu, Kanun Numarası : 5395, Kabul Tarihi : 03.07.2005, RG 15.07.2005/ 25876

General Data Protection Regulation – GDPR, Kabul Tarihi: 14.04.2016, Yürürlük Tarihi: 25.05.2018, 2016/679

Herald A, 'Evangeline: Interview with a Child Cyber-Prostitute in TSO' (2003) <http://alphavilleherald.com/2003/12/evangeline_inte.html> Erişim Tarihi: 18.12.2021

Hayes EJ, 'Playing It Safe: Avoiding Online Gaming Risks' Cybersecurtiy & Infrastructure Security Agency (CISA). <https://www.cisa.gov/uscert/sites/default/files/publications/gaming.pdf> Erişim Tarihi: 19.12.2021

Henkoğlu T, *Adli Bilişim* (2. Bası, Pusula Yayıncılık 2014).

Huff C, Johnson DG ve Miller KW, 'Virtual Harms and Real Responsibility' (2003) 22(2) IEEE Technology and Society Magazine, Summer 12-19.

Ireland Data Protection Commission (DPC) 'Fundamentals for a Child-Oriented Approach to Data Processing' (2021) Children Front and Centre. <https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf> Erişim Tarihi: 24.12.2021

İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, Kanun Numarası: 5651, Kabul Tarihi: 4.5.2007, RG 23.5.2007/26530

Kişisel Verilerin Korunması Kanunu, Kanun Numarası: 6698, Kabul Tarihi: 24.3.2016 RG 07.04.2016 / 29677

Kişisel Verileri Koruma Kurumu 'Çocukların Kişisel Verilerinin Korunması, Ürün ve Hizmet

Geliştirenler Tarafından Dikkat Edilmesi Gerekenler Rehberi' <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/db0b3f30-c636-4fcb-930a-bf-8f2e524de8.pdf> Erişim Tarihi: 17.12.2021

Kişisel Verileri Koruma Kurulu. Karar Tarihi: 02.04.2020. Karar Sayısı: 2020/255. <https://www.kvkk.gov.tr/Icerik/6894/2020-255> Erişim Tarihi: 16.12.2021

Kurz R, "Bridgend 'Bebo Internet Suicide Cult' and Ritual Violence in Wales" (2017) 41(S1), 25th European Congress of Psychiatry of the in Florence. European Psychiatry 888-889. doi:10.1016/j.eurpsy.2017.01.1803

Leary MG, 'Self-Produced Child Pornography: The Appropriate Societal Response to Juvenile Self-Sexual Exploitation' (2008) 15(1) Virginia Journal of Social Policy and the Law.

Leary MG, 'Sexting or Self-Produced Child Pornography? The Dialogue Continues – Structured Prosecutorial Discretion Within A Multidisciplinary Response' (2010) 17(3) Virginia Journal of Social Policy and the Law Spring, 486-566.

Lenhart A, 'Teens and Sexting: How and Why Minor Teens are Sending Sexually Suggestive Nude or Nearly Nude Images via Text Messaging' (2009) Pew Research Centre Report. <https://www.pewresearch.org/internet/2009/12/15/teens-and-sexting/> Erişim Tarihi: 16.12.2021

Livingstone S, Stoilova M ve Nandagiri R, 'Children's Data And Privacy Online: Growing Up in A Digital Age, An Evidence Review' (2019) London School of Economics and Political Science. <https://www.semanticscholar.org/paper/Children's-data-and-privacy-online%3A-growing-up-in-a-Livingstone-Stoilova/65e26c5308ab20efa9a2e2c4e976457fe18fade2> Erişim Tarihi: 24.12.2021

Maple C, Short E ve Brown A, 'Cyberstalking in The United Kingdom: An Analysis of The ECHO Pilot Survey' (2011) National Centre for Cyberstalking Research: University of Bedfordshire. <https://www.researchgate.net/publication/292157398_Cyberstalking_in_the_United_Kingdom_an_analysis_of_the_ECHO_Pilot_Survey_National_Centre_for_Cyberstalking_Research_University_of_Bedfordshire> Erişim Tarihi: 16.12.2021

Mitchell K, Finkelhor D ve Wolak J, 'The Exposure of Youth to Harmful Content on the Internet. A National Survey of Risk, Impact And Prevention' (2003) 34(3) Youth and Society 330-358 Doi:10.1177/0044118X02250123

Morgan A, 'The Transparency Challenge: Making Children Aware of Their Data Protection Rights and The Risks' Online (2018) <https://www.dataprotection.ie/sites/default/files/uploads/2019-02/TransparencyChallenge.pdf> Erişim Tarihi: 24.12.2021

Office of the Privacy Commissioner of Canada (OPC) 'Activity Sheets For Kids' <https://www.priv.gc.ca/en/about-the-opc/what-we-do/awareness-campaigns-and-events/privacy-education-for-kids/t-v/activ/index/> Erişim Tarihi: 24.12.2021

Özkaya P, *Adli Bilişimde Özel Araştırma ve Soruşturma Yöntemleri* (1. Bası, Seçkin Yayıncılık 2022).

Özkaya P ve Samet R, 'Biyolojik Biyometrik Sistemler, Biyometrik Veriler, Hukuk ve Güvenlik' Siber Güvenlik ve Savunma - Biyometrik ve Kriptografik Uygulamalar Kitabı (1. Basım. 4.Bölüm, Nobel Yayıncılık 2020) 121-180

Quayle E, Jonsson L ve Lööf L, 'Online Behaviour Related to Child Sexual Abuse Interviews with Affected Young People' (2012) Council of the Baltic Sea States, Stockholm: Robert Project. <https://childrenatrisk.cbss.org/wp-content/uploads/2020/12/Interviews_with_affected_young_people.pdf> Erişim Tarihi: 16.12.2021

Ringrose J, Gill R, Livingstone S ve Harvey L, "A Qualitative Study of Children, Young People and 'Sexting': A Report Prepared for the NSPCC" (2012).

<https://www.researchgate.net/publication/265741962_A_qualitative_study_of_children_young_people_and_'sexting'_a_report_prepared_for_the_NSPCC> Erişim Tarihi: 16.12.2021

Tampa Bay Times, 'Line Between Virtual and Real Blurred in Online Game' (2005) <https://www.tampabay.com/archive/2004/02/16/line-between-virtual-and-real-blurred-in-online-game/> Erişim Tarihi: 18.12.2021

Telekomünikasyon Hizmetleri Yönetmeliği. RG 28.03. 2001/ 24356. Erişim Tarihi: 22.12.2021.

The Council of Europe Convention on Cybercrime. Yürürlük Tarihi: 01.07.2004. ETS 185 <https://rm.coe.int/1680081561> Erişim Tarihi: 22.12.2021

The United Nations Convention on the Rights of the Child, Kabul Tarihi: 20.11.1989, Genel Kurul Karar Sayısı: 44/25, Yürürlük Tarihi: 02.09.1990

Türk Ceza Kanunu, Kanun Numarası: 5237, Kabul Tarihi: 26.9.2004, RG 12.10.2004/25611

Türkiye Cumhuriyeti Anayasası, Kabul Tarihi: 18.10.1982. RG 09.11.1982/17863

Türk Medeni Kanunu, Kanun Numarası : 4721, Kabul Tarihi : 22.11.2001, RG 08.12.2001/24607

UNICEF (Birleşmiş Milletler Çocuklara Yardım Fonu) 'Dijital bir Dünyada Çocuklar' (2017) Dünya Çocuklarının Durumu Raporu <https://www.unicef.org/turkey/raporlar/d%C3%BCnya-%C3%A7ocuklar%C4%B1n%C4%B1n-durumu-2017-dijital-bir-d%C3%BCnyada-%C3%A7ocuklar> Erişim Tarihi: 23.12.2021.

United Nations Office on Drugs and Crime (UNODC) Vienna, 'Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children'. (2015). <https://www.unodc.org/documents/organized-crime/cybercrime/Study_on_the_Effects.pdf> Erişim Tarihi: 16.12.2021

Ybarra ML, Espelage DL ve Mitchell KJ, 'The Co-Occurrence of Internet Harassment And Unwanted Sexual Solicitation Victimization And Perpetration: Associations With Psychosocial Indicators' (2007) 41(32) Journal of Adolescent Health 31–41 <http://unh.edu/ccrc/pdf/CV120b.pdf> Erişim Tarihi: 16.12.2021.