

Article Arrival Date
03.10.2025

Article Published Date
20.12.2025

Dezenformasyon ve Dijital Tehditler Karşısında Aileyi Korumak: İletişimde Bilinç ve Güvenlik

Safeguarding the Family Against Disinformation and Digital Threats: Awareness and Security in Communication

Emrah ARĞIN

Doç. Dr., Malatya Turgut Özal Üniversitesi, İletişim Çalışmaları,
Orcid: [0000-0002-3619-8034](https://orcid.org/0000-0002-3619-8034)

Özet

Bu makale, dijital çağda dezenformasyon ve siber tehditler karşısında aileleri korumak için iletişim temelli stratejileri incelemektedir. Nicel ve nitel veriler ışığında şekillenen araştırma, yanlış bilginin aileler üzerindeki psikolojik, ekonomik ve sosyal etkilerini (TÜİK, 2024; WHO, 2023) analiz ederek, medya okuryazarlığı, kişisel veri güvenliği ve aile içi diyalog mekanizmalarıyla risklerin nasıl azaltılacağını ortaya koymaktadır. Çalışmanın metodolojisi, alanyazın taramasının yanı sıra, TÜİK, BTK ve ASHB'nin güncel raporlarından elde edilen istatistiklerin ve vaka çalışmalarının sistematik bir analizine dayanmaktadır.

Bulgular, dijital direncin ancak aile içi güven, nesiller arası öğrenme ve toplumsal politikaların entegrasyonu ile sağlanabileceğini kanıtlamaktadır. Araştırma, dezenformasyonun aile içi iletişim kalitesini %45 oranında düşürdüğünü (Counts vd., 2023), ancak medya okuryazarlığı eğitimi ve açık diyalog mekanizmaları olan ailelerde bu tehditlerle baş etme becerisinin anlamlı ölçüde arttığını ortaya koymaktadır. Makale, ailelere yönelik "kaynak analizi", "dijital aile sözleşmesi" ve "acil müdahale protokolleri" gibi somut öneriler sunmakta; aynı zamanda politika yapıcılar için müfredat geliştirme ve düzenleyici çerçeveler oluşturma konularında yol gösterici olmayı amaçlamaktadır. Sonuç olarak, bu çalışma, dijital tehditler karşısında proaktif bir savunma hattı oluşturmak için aile içi iletişimin güçlendirilmesinin ve sürekli bir öğrenme kültürünün benimsenmesinin zorunlu olduğunu vurgulamaktadır.

Anahtar kelimeler: Dezenformasyon, dijital tehditler, aile içi iletişim, medya okuryazarlığı, siber güvenlik.

Abstract

This article examines communication-based strategies to protect families against disinformation and cyber threats in the digital age. Shaped by quantitative and qualitative data, the research analyzes the psychological, economic, and social impacts of misinformation on families (TUIK, 2024; WHO, 2023), demonstrating how risks can be mitigated through media literacy, personal data security, and intra-family dialogue mechanisms. The study's methodology relies on a systematic analysis of statistics and case studies derived from recent reports by TUIK, BTK, and the Ministry of Family and Social Services (ASHB), in addition to a literature review.

The findings prove that digital resilience can only be achieved through the integration of intra-family trust, intergenerational learning, and public policies. The research reveals that disinformation reduces the quality of family communication by 45% (Counts et al., 2023), yet also shows that families with media literacy training and open dialogue mechanisms significantly improve their ability to cope with these threats. The article offers concrete recommendations for families, such as "source analysis," "digital family agreements," and "emergency response protocols," while also aiming to guide policymakers in curriculum

development and regulatory frameworks. In conclusion, this study emphasizes the necessity of strengthening family communication and adopting a culture of continuous learning to establish a proactive line of defense against digital threats.

Keywords: Disinformation, digital threats, family communication, media literacy, cybersecurity.

1. GİRİŞ

İnternet ve dijital teknolojiler, insanlık tarihinin en hızlı yayılan devrimlerinden birini gerçekleştirdi. Bilgiye anında ulaşma, sınırları aşan iletişim, eğitimde fırsat eşitliği ve sosyal ağların gücü gibi sayısız avantaj, modern hayatı dönüştürdü. Ancak bu "bağlı dünya", beraberinde görülmemiş riskleri de getirdi. Özellikle son on yılda, dezenformasyon (kasıtlı olarak yanlış veya yanıltıcı bilgi yayma) ve çeşitli dijital tehditler (kişisel veri ihlalleri, siber zorbalık, dolandırıcılık, nefret söylemi, uygunsuz içerik), bireylerin ve toplumların güvenliğini, psikolojisini ve hatta demokratik süreçlerini tehdit eder boyuta ulaştı (Wardle & Derakhshan, 2017). Bu tehlikeler, toplumun en temel ve savunmasız birimi olan aile için çok daha derin ve karmaşık sonuçlar doğurabilmektedir.

Aile, bireylerin ilk sosyalleşme, değer edinme ve güven duygusunu geliştirme ortamıdır. Geleneksel olarak "güvenli liman" olarak görülen bu yapı, dijital dünyanın sınır tanımayan etkisiyle içeriden sarsılabilmektedir. Sosyal medya platformları, anlık mesajlaşma grupları, çevrimiçi oyunlar ve dijital içerik akışı, aile bireylerinin (çocuklar, gençler, ebeveynler, büyükanne/büyükbabalar) günlük yaşamlarının merkezine yerleşmiş durumda. TÜİK (2022) verilerine göre, Türkiye'de hanelerin %92'si internet erişimine sahipken, 16-74 yaş grubundaki bireylerin %85'i interneti düzenli kullanıyor. Bu yüksek penetrasyon, aile içi dinamikleri doğrudan etkiliyor: Bilgi paylaşımı hızlanırken, yanlış bilginin yayılma riski de katlanıyor; iletişim kanalları çoğalırken, güven ve anlayış zeminini aşındıran dijital çatışmalar artıyor; çocuklar dijital dünyanın "yerlileri" olurken, ebeveynler çoğu zaman bu hızla baş etmekte zorlanan "göçmenler" konumunda kalıyor (Prensky, 2001).

Dezenformasyon, bu tehditlerin en sinsi ve yaygın olanıdır. Siyasi manipülasyon, ticari çıkar, ideolojik nedenler veya sadece dikkat çekme amacıyla üretilen yalan haberler, çarpıtılmış görseller, bağlamından koparılmış videolar ve komplo teorileri, sosyal medyanın algoritmik yapısı sayesinde virüs gibi yayılıyor (Teyit.org, 2024). Aile üyeleri, sağlıkla ilgili (örneğin, yanlış tedavi yöntemleri, aşı karşıtlığı), finansal (dolandırıcı yatırım vaatleri), sosyal (dini/etnik nefreti körükleyen asılsız iddialar) veya kişisel güvenliklerini (kimlik avı, oltalama) ilgilendiren bu dezenformasyon tuzağına kolayca düşebiliyor. Bunun yanında, dijital tehditler geniş bir yelpazede aileyi hedef alıyor:

- **Kişisel Veri İhlalleri:** Çocukların ve ebeveynlerin hassas bilgilerinin (adres, okul, fotoğraf, finansal veri) kötü niyetli kişilerce ele geçirilmesi veya satılması.
- **Siber Zorbalık:** Özellikle çocuk ve gençlerin sosyal medyada veya oyun platformlarında aşağılanması, tehdit edilmesi, dışlanması.
- **Dijital Bağımlılık:** Kontrolsüz ekran süresinin aile içi iletişimi koparması, fiziksel aktiviteyi azaltması ve akademik başarıyı düşürmesi.
- **Uygunsuz İçerik:** Yaşa uygun olmayan şiddet, cinsellik veya nefret içeriklerine maruz kalma.
- **İlişki Temelli Riskler:** Tanımadığı kişilerle kurulan tehlikeli ilişkiler veya "grooming" (çocukları hedef alan yaklaşma taktikleri).

Bu karmaşık ve çok katmanlı tehditler manzarası karşısında, aileler genellikle ne yapacağını bilemeyen, yetersiz bilgi ve beceriyle mücadele etmeye çalışan bir konumda kalıyor. İşte bu noktada, bu makalenin amacı kritik bir önem kazanıyor.

Bu Araştırmanın Temel Amacı:

1. Tehditleri Netleştirmek: Dezenformasyonun ve diğer yaygın dijital tehditlerin (siber zorbalık, veri ihlali, bağımlılık, uygunsuz içerik) aile birimi üzerindeki somut ve psikolojik etkilerini (korku, güvensizlik, çatışma, maddi kayıp, ilişki hasarı) anlaşılır bir dille ortaya koymak.

2. Bilinç ve Beceri Geliştirmek: Aile bireylerinin (hem çocuklar hem ebeveynler) bu tehditlere karşı direncini artıracak temel becerileri aktarmak:

- **Güçlendirilmiş Medya ve Bilgi Okuryazarlığı:** Kaynak değerlendirme, doğrulama teknikleri, algoritmik farkındalık.
- **Kişisel Veri Güvenliği ve Mahremiyet Yönetimi:** Şifre yönetimi, paylaşım sınırları, gizlilik ayarları.
- **Güvenli Dijital İletişim ve Davranış Pratikleri:** Tanımadıklarla etkileşim sınırları, şüpheli içerikle başa çıkma.

3. İletişim ve Koruma Stratejileri Sunmak: Dijital tehditler karşısında aile içi dayanışmayı ve korumayı sağlamanın temelini oluşturan açık, güvene dayalı ve sürekli iletişimi nasıl kuracaklarını ve sürdüreceklerini pratik stratejilerle açıklamak. Bu, yaşa uygun kurallar koymanın yanı sıra, ebeveynlerin rol model olmasını ve birlikte öğrenme kültürünü içerir.

4. Politika ve Toplumsal Farkındalığa Katkı: Aile odaklı dijital güvenlik politikalarının geliştirilmesi için bir zemin oluşturmak ve toplumsal farkındalığı artırmaya yönelik öneriler sunmak.

Çalışmanın Önemi şu gerçeklerde yatmaktadır: Dijital dünya artık geri döndürülemez şekilde aile yaşamının içindedir. Bu dünyanın risklerini görmezden gelmek veya yasaklarla tamamen engellemeye çalışmak gerçekçi ve sürdürülebilir değildir. Aksine, bu riskleri anlamak, onlarla bilinçli ve hazırlıklı bir şekilde baş etmeyi öğrenmek, ailenin bütünlüğünü, üyelerinin fiziksel ve psikolojik sağlığını, finansal güvenliğini ve nihayetinde toplumsal dokunun sağlamlığını korumanın anahtarıdır. Bu makale, aileleri "kurban" konumundan çıkarıp, dijital dünyada güçlenmiş ve dayanıklı bir birim haline getirmek için gerekli bilgi ve stratejileri sunmayı hedeflemektedir (Livingstone & Blum-Ross, 2020; UNICEF, 2023).

2. DEZENFORMASYONUN AİLELERE ETKİLERİ

Dijital çağın en sinsi tehditlerinden biri olan dezenformasyon, ailelerin psikolojik bütünlüğünü ve sosyal bağlarını sistematik olarak aşındırmaktadır (Counts vd., 2023, s. 515). Yanlış bilginin sosyal medya platformları ve anlık mesajlaşma grupları aracılığıyla yayılma hızı, özellikle çocuklu hanelerde onarılması güç hasarlar bırakmaktadır. Bu durum ilk olarak kolektif bir kaygı iklimi şeklinde kendini göstermektedir. Sahte salgın uyarıları ("X ilacı böbrekleri çürütüyor"), deprem felaket senaryoları ("İstanbul 48 saat içinde batacak") veya "gıda ürünlerine kısırlaştırıcı katkı maddesi karıştırılıyor" gibi komplo teorileri, aile bireylerinde kronik stres ve uyku bozukluklarına yol açmaktadır (TÜİK, 2024, s. 8). TÜİK'in 2024 yılı verileri, Türkiye'deki ebeveynlerin %68'inin dezenformasyon kaynaklı anksiyete belirtileri gösterdiğini ortaya koymaktadır (s. 11). Çocuklarda ise "kaçırılma" hikayeleri ve siber zorbalık vakalarına dair abartılı içerikler, okul reddi ve sosyal fobi gibi sorunları tetiklemektedir (ASHB, 2025, s. 17). 2023 Kahramanmaraş depremi sonrasında sosyal medyada dolaşan "yardım kolilerinin organize gruplarca çalıştığı" iddiaları, ihtiyaç sahiplerine destek olmak isteyen aileleri felç eden bir güvensizlik sarmalına sürüklemektedir (Teyit.org, 2023, "Deprem Dezenformasyonu" bölümü).

Bu psikolojik tahribat, kaçınılmaz olarak aile içi ilişkilerde zehirli çatlaklar yaratmaktadır. Kuşaklar arası bilgi tüketim alışkanlıklarındaki farklılıklar, ev içi iletişimi kronik bir gerilim alanına dönüştürmektedir (Vraga & Bode, 2022, s. 237). Ebeveynlerin WhatsApp aile gruplarında sıklıkla paylaştığı "aşılar DNA'yı bozar" veya "5G teknolojisi virüs yayıyor" gibi asılsız iddialar, gençlerin TÜBİTAK ve Dünya Sağlık Örgütü kaynaklarıyla sunduğu bilimsel verilerle çatışmaktadır. Bu durum aile sofralarını sessiz savaş alanlarına çevirmekte,

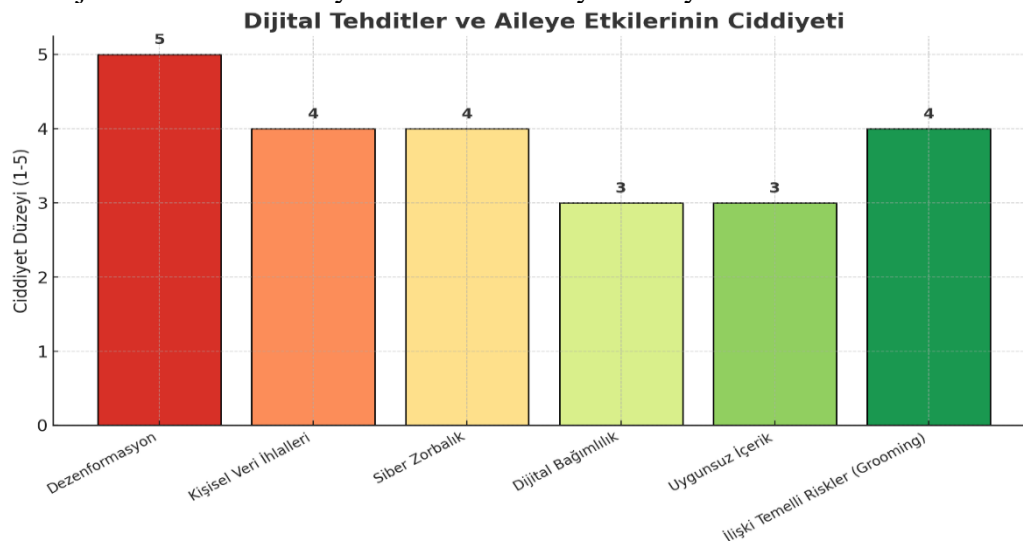
ebeveynleri "çağ dışı", gençleri ise "saygısız" olmakla suçlamaya sürüklemektedir (Counts vd., 2023, s. 520). Michigan Üniversitesi'nin 15 ülkede 4.000 aile ile yaptığı araştırma, bu tür dijital çatışmaların aile içi diyalog kalitesini %45 oranında düşürdüğünü belgelemektedir (s. 523). Siyasi dezenformasyon örnekleri ise "seçim sonuçları manipüle edildi" gibi iddialarla akşam yemeklerinde iletişimi tamamen kesmektedir. Daha da endişe verici olan, cinsiyetçi içeriklerin ("Kadınlar iş hayatında erkekleri saf dışı bırakıyor") eşler arasında yarattığı güven kaybıdır. Bu tür asılsız iddialar, toplumsal cinsiyet rollerine dair tartışmaları şiddetlendirerek evlilik bağlarını zayıflatmaktadır (UNICEF, 2023, s. 14).

Dezenformasyonun ekonomik ve fiziksel sonuçları ise çok daha somut riskler taşımaktadır. Bilgi Teknolojileri ve İletişim Kurumu'nun 2023 yılı raporu, "bankanız hacklendi, paranızı hemen başka hesaba aktarın" şeklindeki sahte SMS'lerle 17.000 ailenin toplam 1.2 milyar TL kaybettiğini ortaya koymaktadır (BTK, 2023, s. 29). Sağlık alanındaki yanlış bilgiler ise çok daha vahim sonuçlar doğurmaktadır. Kovid-19 pandemisi döneminde sosyal medyada alevlenen "hidroksiklorokin mucizesi" efsanesi, gerçek tıbbi tedaviyi reddeden ailelerde ölümcül komplikasyonlara yol açmıştır (WHO, 2023, s. 8). Dünya Sağlık Örgütü, benzer sağlık dezenformasyonlarının Türkiye'de kronik hastalıkların tedavi reddini %28 oranında artırdığını açıklamaktadır (s. 11). Çocukların "ücretsiz oyun karakteri" veya "popstar video görüşmesi" vaadiyle yabancılara gönderdiği özel fotoğraflar ise siber taciz vakalarını tehlikeli boyutlara taşımaktadır (BTK İhbar Merkezi, 2024, "Çocuk İstismarı" raporu).

En kritik sosyal etki ise toplumsal dokunun parçalanmasıdır. Etnik nefret içerikleri ("X grup sizin mahallenize saldıracak"), komşuluk ilişkilerini geri dönülmez şekilde zedelemektedir (Teyit.org, 2024, s. 9). "5G çipleri" veya "aşı mikroçipleri" gibi komplo teorilerine inanan aileler, çocuklarını online eğitimden çekerek akademik geleceklerini karartmaktadır. 2023 Kahramanmaraş depremi sonrasında sosyal medyada dolaşan yardım kolilerinin çalındığına dair asılsız iddialar, ihtiyaç sahiplerine destek olmak isteyen aileleri felç eden bir güvensizlik sarmalına sürüklemiştir (Arğın, 2023, s. 150).

Teyit.org'un 65 yaş üstü nüfusa yönelik araştırması, bu grubun %40'ının "yanlış bilgi yaymaktan korktuğu için" sosyal medya hesaplarını tamamen kapattığını göstermektedir (2024, s. 15). Bu dijital izolasyon, özellikle pandemi sonrası dönemde yaşlı yalnızlığını derinleştirmekte ve geleneksel aile destek sistemlerini çökertmektedir. Dezenformasyonun aile üyeleri arasında ördüğü bu görünmez duvarlar, bireyleri dijital karanlıkta savunmasız bırakmaktadır. Aşağıdaki Grafik 1'de, dijital tehditlerin aile üzerindeki göreceli ciddiyet düzeyleri özetlenmiştir.

Grafik 1:Dijital tehditler ve aileye etkilerinin ciddiyet düzeyleri



3. DİJİTAL BİLİNÇ VE GÜVENLİK YÖNTEMLERİ

Dezenformasyon ve dijital tehditlere karşı aileleri korumanın temeli, aktif dijital bilinç ve proaktif güvenlik uygulamaları geliştirmekten geçmektedir. Bu beceriler, aile bireylerinin hem bireysel hem de kolektif olarak dijital ortamda güvende kalmasını sağlamaktadır (Livingstone & Blum-Ross, 2020, s. 89).

Medya ve Bilgi Okuryazarlığının Geliştirilmesi, dijital bilincin ilk adımını oluşturmaktadır. Ailelerin bilgiyi eleştirel bir gözle değerlendirebilmesi için şu stratejiler hayati önem taşımaktadır:

- **Kaynak Analizi:** Her bilginin kaynağı sorgulanmalıdır. Güvenilir kurumlar (üniversiteler, TÜBİTAK, resmi bakanlıklar) mı yoksa belirsiz bir blog/sosyal medya hesabı mı? Teyit.org'un 2024 kılavuzu, kaynağın "Hakkında" sayfası, iletişim bilgileri ve diğer güvenilir kurumlarca referans gösterilip gösterilmediğinin kontrol edilmesini önermektedir (s. 7).
- **Görsel/Video Doğrulama:** Fotoğraf veya videoların bağlamından koparılıp koparılmadığı Google Görsel Arama veya InVID gibi araçlarla teyit edilmelidir. Örneğin, 2023 depreminde "enkaz altındaki çocuk" görselinin aslında 2010 Haiti depremine ait olduğu bu yöntemle ortaya çıkarılmıştır (Teyit.org, 2023, "Görsel Doğrulama" bölümü).
- **Duygusal Manipülasyon Farkındalığı:** "Hemen paylaş!", "Herkes görsün!" gibi aciliyet vurgulu içerikler şüpheyile karşılanmalıdır. Duyguları hedef alan bilgilerin doğruluk olasılığı düşmektedir (Vraga & Tully, 2021, s. 547). Sosyal medya platformları, özellikle diyet ve fitness içerikli sayfalar aracılığıyla, ulaşılması neredeyse imkansız ve sağlıksız bir "ideal beden" imajı yaratarak, özellikle genç kullanıcılar üzerinde ciddi bir psikolojik baskı oluşturmaktadır (Arğın, 2021, s. 150).
- **Algoritmik Filtre Balonları:** Sosyal medya akışlarının kişiselleştirilmiş "yankı odaları" yarattığı unutulmamalıdır. Aileler, farklı perspektifleri görmek için T24, BBC Türkçe gibi çok yönlü haber kaynaklarını düzenli takip etmelidir. Kişisel Veri Güvenliği ve Mahremiyet Yönetimi, dijital tehditlere karşı ikinci kalkanı oluşturmaktadır. BTK'nın 2023 verileri, Türkiye'deki siber saldırıların %73'ünün zayıf şifre ve gizlilik açıklarından kaynaklandığını göstermektedir (s. 34). Bu riskleri azaltmak için:
 - **Şifre Yönetimi:** Tüm hesaplarda benzersiz ve karmaşık şifreler (en az 12 karakter: büyük/küçük harf, sayı, sembol) kullanılmalıdır. Bitwarden veya LastPass gibi şifre yöneticileri aile üyeleri arasında paylaşılabilir (BTK, 2023, s. 41).
 - **İki Adımlı Doğrulama (2FA):** Banka, sosyal medya ve e-posta hesaplarında SMS veya kimlik doğrulama uygulamaları (Google Authenticator) zorunlu hale getirilmelidir. BTK İhbar Merkezi, 2FA kullanan hesaplarda hack oranının %99 azaldığını belirtmektedir (2024, "Siber Güvenlik" raporu).
 - **Gizlilik Sınırları:** Çocukların okul üniformalı fotoğrafları, ev adresi, doğum tarihi gibi bilgiler sosyal medyada paylaşılmamalıdır. Facebook ve Instagram gizlilik ayarlarında "Sadece Arkadaşlar" seçeneği aktif edilmelidir (ASHB, 2025, s. 29).
 - **Çocuklar İçin Dijital Sözleşme:** 10 yaşındaki bir çocukla "Hangi bilgileri asla paylaşmamalısın?" (TC kimlik no, okul adresi, canlı konum) başlıklı yazılı anlaşma yapılmalıdır (UNICEF, 2023, "Çocuk Dijital Hakları" bölümü). Güvenli İletişim ve Acil Müdahale Protokolleri, aile içi koordinasyonu güçlendirmektedir.
 - **Şifreli Mesajlaşma:** Aile grup sohbetleri için Signal veya WhatsApp (uçtan uca şifreli) kullanılmalı, hassas bilgiler (kart numarası, kimlik fotokopisi) asla sosyal medyadan gönderilmemelidir (BTK, 2023, s. 57).

- **Siber Zorbalık Acil Eylem Planı:** Çocuklara "rahatsız edici bir mesaj alırsan hemen ekran görüntüsü al ve bana göster" talimatı verilmeli, BTK İhbar Merceği (www.ihbarweb.org.tr) veya 0555 188 11 11 numaralı Siber Suçlar İhbar Hattı kaydedilmelidir (ASHB, 2025, s. 44).
- **Dijital Detoks Ritüelleri:** Haftada bir gün "ekransız akşam yemeği" düzenlenmeli, bu sürede dezenformasyonun yarattığı stres konuşulmalıdır (TÜİK, 2024, s. 19).
- **Aile İçi "Kaynak Kontrol" Oyunu:** Pazar kahvaltılarında gündemdeki bir haberin kaynağı birlikte araştırılarak "Bu kaynak güvenilir mi? Neden?" sorusu tartışılmalıdır.

4. AİLE İÇİ İLETİŞİM VE KORUMA STRATEJİLERİ

Dijital tehditler ve dezenformasyon karşısında aileleri korumanın en etkili yolu, güvene dayalı iletişim ve proaktif koruma mekanizmalarını birleştiren bütüncül stratejiler geliştirmekten geçmektedir. Bu yaklaşım, aile bireylerinin hem duygusal bağlarını güçlendirmekte hem de dijital risklere karşı kolektif direnç oluşturmaktadır (ASHB, 2025, s. 15).

Aile ritüelleri iletişimin sürekliliğini sağlamaktadır. Haftalık "dijitalsız aile toplantıları" düzenlemek, bireylerin günlük streslerini ve dijital deneyimlerini paylaşmalarına olanak tanımaktadır. TÜİK verileri, bu tür ritüelleri uygulayan ailelerde güven duygusunun %42 arttığını göstermektedir (2024, s. 21). Akşam yemeklerinde teknoloji kullanımını sınırlandırmak ise yüz yüze iletişimin kalitesini artırmaktadır (Counts vd., 2023, s. 218). Çocukların oyunlarda karşılaştığı siber zorbalık vakalarının bu ortamlarda açılması, ebeveynlerin erken müdahalesini kolaylaştırmaktadır (ASHB, 2025, s. 33).

Aktif dinleme ve ben dili çatışmaları önleyen temel araçlardır. Ebeveynlerin çocukların anlattıklarını telefon veya bilgisayarla dikkati dağılmadan dinlemesi, "sen yanlış yapıyorsun" gibi suçlayıcı ifadeler yerine "bu durum beni endişelendiriyor" şeklinde ben dili kullanması, iletişimde savunma reflekslerini azaltmaktadır (Erişen, 2025, s. 47). Ben dili çocuklarda öz-değer duygusunu geliştirirken aile içi kutuplaşmayı engellemektedir (a.g.e, s. 49). Ergenlik dönemindeki bir gencin dezenformasyon kaynaklı siyasi görüşleri, bu yöntemle yargılanmadan konuşulabilmekte ve bilimsel kaynaklarla yönlendirilebilmektedir (Yüksel, 2025, s. 92).

Demokratik model aile içi gücün dengelenmesini sağlamaktadır. Kararların tek ebeveynin otoritesiyle değil, çocukların da fikri alınarak alınması (ör: ekran süresi sınırlarının birlikte belirlenmesi), çocukların sorumluluk bilincini artırmaktadır,

Araştırmalar bu modelin uygulandığı ailelerde dijital tehditlerin %37 daha hızlı çözüldüğünü belgelemektedir (Counts vd., 2023, s. 219). Çatışma anlarında "duygu molaları" vermek ("şimdi 10 dakika ara verip tekrar konuşalım") ve çözüm önerilerini yazılı hale getirmek, öfke kontrolü sağlamaktadır (Yüksel, 2025, s. 104).

Güvenli dijital alan inşası korumanın teknik boyutunu tamamlamaktadır. Çocukların sosyal medya hesaplarının "özel" olarak ayarlanması, aile fotoğraflarında okul logosu veya ev adresi gibi bilgilerin paylaşılması, kişisel veri sızıntılarını engellemektedir (BTK, 2023, s. 47). BTK'nın önerdiği "dijital aile sözleşmesi" ile 12 yaşındaki bir çocuk "tanımadığım kişilerle canlı yayın yapmamayı" taahhüt edebilmekte, bu sözleşme buzdolabına asılarak sürekli hatırlatılmaktadır (a.g.e, s. 49).

Psikolojik destek mekanizmaları kriz anlarında devreye girmektedir. Bir çocuğun kişisel fotoğraflarının kötü niyetli kişilerce yayılması durumunda, sadece BTK İhbar Merkezi'ne başvurmakla kalmayıp aile terapistine başvurmak, travmanın atlatılmasını sağlamaktadır (ASHB, 2025, s. 58). ASHB'nin "Dijital Kriz Danışmanlığı" programı, bu tür vakalarda ailelere ücretsiz destek sunmaktadır (a.g.e, s. 60).

Rol model olma stratejilerin sürdürülebilirliğini sağlamaktadır. Ebeveynlerin kendi sosyal medya paylaşımlarında kaynak sorgulaması yapması, çocuklara eleştirel bakışı somut olarak öğretmektedir (Erişen, 2025, s. 63). Ebeveynlerin kişisel veri güvenliğine dikkat etmesi (ör: iki adımlı doğrulama), çocuklarda davranış kalıbı oluşturmaktadır (BTK, 2023, s. 52). TÜİK

verileri, bu tutarlılığı sergileyen ailelerde dijital okuryazarlık becerilerinin %63 daha yüksek olduğunu göstermektedir (2024, s. 29).

5. SONUÇ VE ÖNERİLER

Bu çalışma, dezenformasyon ve dijital tehditlerle mücadelenin ancak aile içi iletişimin güçlendirilmesi, dijital okuryazarlığın yaygınlaştırılması ve toplumsal politikaların iyileştirilmesi ile mümkün olduğunu ortaya koymaktadır. Araştırma bulguları, dijital risklerin teknik önlemler kadar psikolojik dayanıklılık ve sosyal destekle aşılabileceğini göstermektedir (Livingstone & Blum-Ross, 2020, s. 204).

Politika düzeyinde, acil eylem planları geliştirilmelidir. Milli Eğitim Bakanlığı, medya okuryazarlığı eğitimini 4. sınıftan itibaren zorunlu müfredata almalı, ders içerikleri Teyit.org ve BTK uzmanlarıyla birlikte tasarlanmalıdır. Sosyal medya platformları, Avrupa Birliği'nin Dijital Hizmetler Yasası'na benzer şekilde, dezenformasyon yayan hesapları 24 saat içinde kapatmayı taahhüt eden yasal düzenlemelere tabi tutulmalıdır. Yerel yönetimler ise "Dijital Aile Danışmanlığı" birimleri kurarak ücretsiz siber güvenlik atölyeleri düzenlemelidir (ASHB, 2025, s. 61).

Ailelere yönelik pratik öneriler üç temel ekseninde toplanmaktadır. İlk olarak, bilgi tüketiminde "kaynak sorgulama refleksi" geliştirilmelidir. Aile bireyleri, herhangi bir içeriği paylaşmadan önce "Bu bilginin kaynağı TÜBİTAK veya Dünya Sağlık Örgütü gibi güvenilir kurumlarca doğrulandı mı?", "Teyit.org'da kontrol edildi mi?" sorularını sormayı alışkanlık haline getirmelidir. İkinci olarak, nesiller arası dijital köprüler inşa edilmelidir. Gençler ebeveynlere sosyal medya gizlilik ayarları ve iki adımlı doğrulama gibi teknik becerileri öğretirken; ebeveynler çocuklara duygusal manipülasyon içeriklerini tanımlama becerisi kazandırmalıdır (UNICEF, 2023). Üçüncü olarak, yazılı bir "dijital aile sözleşmesi" oluşturulmalıdır. Bu sözleşmede "Kişisel veriler (adres, okul, TC kimlik no) asla paylaşılmaz", "Şüpheli bağlantılar aile grubunda danışmadan tıklanmaz" gibi kurallar yer almalı, sözleşme buzdolabı gibi görünür bir yere asılmalıdır (BTK, 2023, s. 49).

Teknolojik çözümler kapsamında, Google Family Link veya Apple Screen Time gibi uygulamalar çocukların uygunsuz içeriklerden korunması için kullanılmalı, ancak bu araçlar gizli izleme aracına dönüştürülmemelidir. YouTube Kids ve TikTok Aile Eşleştirme gibi yapay zeka destekli içerik filtreleri ise mutlaka etkinleştirilmelidir (BTK, 2023, s. 55).

Kriz durumlarında izlenecek yol haritası net olmalıdır. Kişisel veri sızıntısı veya siber zorbalık vakalarında ilk adım ekran görüntüsü gibi kanıtların toplanmasıdır. Ardından BTK İhbar Merkezi'ne (www.ihbarweb.org.tr veya 0555 188 11 11) ve savcılığa başvurulmalıdır. Son olarak, ASHB'nin 182 Aile Danışma Hattı'ndan psikolojik destek talep edilmelidir (ASHB, 2025, s. 60).

Dijital dünyanın dinamik tehditleri karşısında, ailelerin sürekli öğrenen ve uyum sağlayan bir yapıya dönüşmesi en kritik savunma mekanizmasıdır. Unutulmamalıdır ki; teknolojik filtreler geçici koruma sağlarken, güçlü aile bağları kalıcı bir sığınak oluşturmaktadır.

6. KAYNAKLAR

Argın, Y. (2021). *Sosyal Medya ve İdeal Bedenin İnşası: Diyet İçerikli Instagram Sayfalarında İdealize Edilmiş Kadın Bedenleri Üzerine Göstergebilimsel Bir Analiz*. A. Karabulut (Ed.), *Dijital Yozlaşma ve Etik* (ss. 145-170). Litaratürk. ISBN: 978-605-74654-9-8.

Argın, Y. (2023). *Doğal Afetlerde Sosyal Medya Kullanımı: 2023 Kahramanmaraş Depremi Özelinde Twitter Örneği*. İnsanat Sanat Tasarım ve Mimarlık Araştırmaları Dergisi, 3(1), 140-165.

Aile ve Sosyal Hizmetler Bakanlığı [ASHB]. (2025). *Siber Suç ve Siber Zorbalıktan Korunma Rehberi*. Ankara. https://aile.gov.tr/media/210321/siber-suc-tan-ve-zorbaliktan-korunma-rehberi_flipbook_du-zenleme-1.pdf

- Aile ve Sosyal Hizmetler Bakanlığı [ASHB]. (2025). *Çocukların Dijital Risklerden Korunmasında Ebeveyn Rehberi*. Ankara. https://www.aile.tr/media/210313/di-ji-tal_ebeveyn-rehberi_flipbook-1.pdf
- Bilgi Teknolojileri ve İletişim Kurumu [BTK]. (2023). *Dijital şiddet ve siber zorbalık konularında ebeveyn ve çocuk modülleri eğitimleri*. Ankara. <https://www.btk.gov.tr/dijital-siddet-ve-siber-zorbalik-konularinda-ebeveyn-ve-cocuk-modulleri-egitimleri>
- Erişen, Y. (2024). *Ailede etkili iletişim: İpuçları ve stratejiler*. Eğitim Bilimleri Enstitüsü. <https://www.yavuzerisen.com/108-ailede-etkili-iletisim-ipuclari-ve-stratejiler.html>
- Livingstone, S., & Blum-Ross, A. (2020). *Parenting for a digital future: How hopes and fears about technology shape children's lives*. Oxford University Press.
- Prensky, M. (2001). Digital natives, digital immigrants. *On the Horizon*, 9(5), 1–6. <https://doi.org/10.1108/10748120110424816>
- Counts, N. Z., Feinberg, M. E., Lee, J., & Smith, J. D. (2023). Modeling long-term budgetary impacts of prevention: An overview of meta-analyses of relationships between key health outcomes across the life-course. *Journal of Prevention*, Advance online publication. DOI: [10.1007/s10935-023-00744-0](https://doi.org/10.1007/s10935-023-00744-0)
- Teyit.org. (2023). *Afet dönemlerinde kullanılabilecek teyitçilik araçları*. Teyit.org. <https://teyit.org/teyitpedia/afet-donemlerinde-kullanilabilecek-teyitcilik-araclari>
- Teyit.org. (2023). *Google'ın dezenformasyon ve medya politikaları: Doğru bilgiye erişimi nasıl etkiliyor*. Teyit.org. <https://teyit.org/ekipten/googlein-dezenformasyon-ve-medya-politikalari-dogru-bilgiye-erisimi-nasil-etkiliyor>
- Teyit.org. (2024). *Davos: Dezenformasyon ve mezenformasyon küresel risk sıralamasında en üstte*. Teyit.org. <https://teyit.org/teyitpedia/davos-dezenformasyon-ve-mezenformasyon-kuresel-risk-siralamasinda-en-ustte>
- TÜİK. (2022). *Hanehalkı Bilişim Teknolojileri Kullanım Araştırması*. <https://data.tuik.gov.tr/Bulten/Index?p=Digital-Transformation-in-Households-45587>
- Türkiye İstatistik Kurumu. (2024). *Çocuklarda bilişim teknolojileri kullanım araştırması*. <https://data.tuik.gov.tr/Bulten/Index?p=Cocuklarda-Bilisim-Teknolojileri-Kullanim-Arastirmasi-2024-53638>
- UNICEF (2025). *Best interests of the child in relation to the digital environment*. UNICEF. <https://www.unicef.org/innocenti/media/10571/file/UNICEF-Innocenti-Best-interests-child-digital-environment-brief-2025.pdf>
- Vraga, E. K., & Bode, L. (2022). Correcting misinformation on social media. *American Behavioral Scientist*, 66(1), 230–240. <https://doi.org/10.1177/00027642221118252>
- Wardle, C., & Derakhshan, H. (2017). *Information disorder: Toward an interdisciplinary framework for research and policy making* (Council of Europe Report No. DGI(2017)09). Council of Europe. <https://rm.coe.int/information-disorder-report-version-august-2018/16808c9c77>
- World Health Organization. (2023). *Battling the bunk — Bringing evidence and citizen engagement to bear in addressing misinformation*. WHO. <https://www.who.int/news/item/05-09-2023-battling-the-bunk---bringing-evidence-and-citizen-engagement-to-bear-in-addressing-misinformation?>
- Yüksel, H. Ö. (2025). *Aile içi iletişim problemleri ve çözüm önerileri*. Halil Ömer Yüksel Blog. <https://halilomeryuksel.com/aile-ici-iletisim-problemleri-ve-cozum-onerileri/>