

Türkiye’de İnternet Kanunu’nda Güncelleme İhtiyacı:

Tepkisel Müdahaleden Önleyici
Düzenlemelere



Enstitü Sosyal | Analiz No: 9

Türkiye’de İnternet Kanunu’nda Güncelleme İhtiyacı:

**Tepkisel Müdahaleden Önleyici
Düzenlemelere**

Muhammet Talha Kaan & Fatma Betül Ercan

Yazarlar

Muhammet Talha Kaan
Fatma Betül Ercan

Editör

Amine Ertürk

Grafik Tasarım

Betül Berra Kurt

Türkiye’de İnternet Kanunu’nda Güncelleme İhtiyacı:

Tepkisel Müdahaleden Önleyici Düzenlemelere

COPYRIGHT © 2026

Bu yayının tüm hakları Enstitü Sosyale aittir. Enstitü Sosyalın izni olmaksızın yayının tümünün veya bir kısmının elektronik veya mekanik (fotokopi, kayıt ve bilgi depolama vd.) yollarla basımı, yayımı, çoğaltılması veya dağıtımı yapılamaz. Kaynak göstermek suretiyle alıntı yapılabilir.

ISBN: 978-625-93766-9-1

NUN Eğitim ve Kültür Vakfı Yayınları

Sertifika No.: 79696

Baskı: Turkuvaz Haberleşme ve Yayıncılık A.Ş.

Güzeltepe Mah. Mareşal Fevzi Çakmak Cad. B Blok No: 29/1/1 Eyüpsultan, İstanbul

Tel: 0212 354 30 00

Sertifika No.: 46403

NUN Eğitim ve Kültür Vakfı Yayınları

Enstitü Sosyal | Analiz No. 9

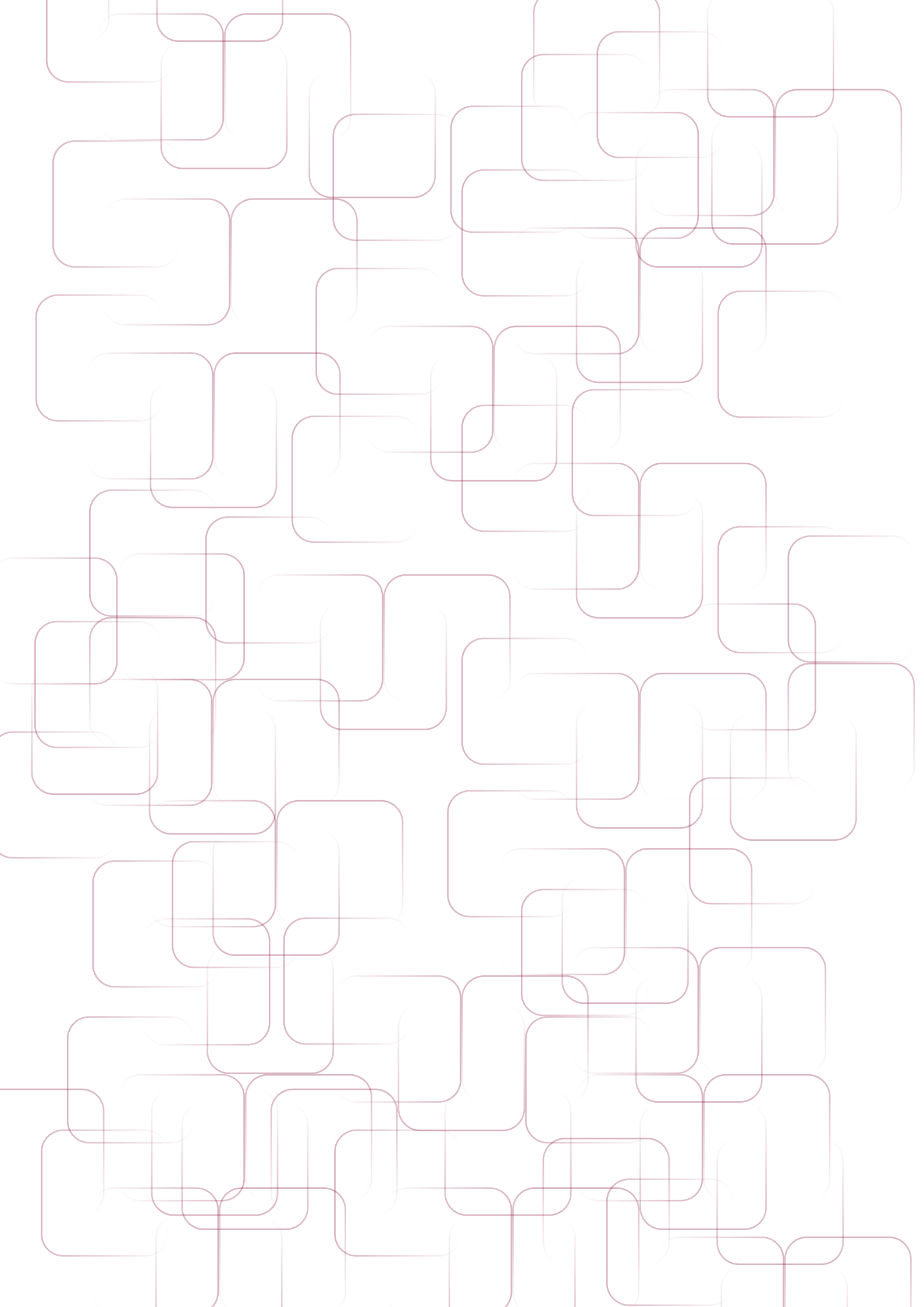
1. Baskı: Mart 2026

Burhaniye Mah. Hacı Reşit Paşa Sok. No:18 Üsküdar, İstanbul/TÜRKİYE

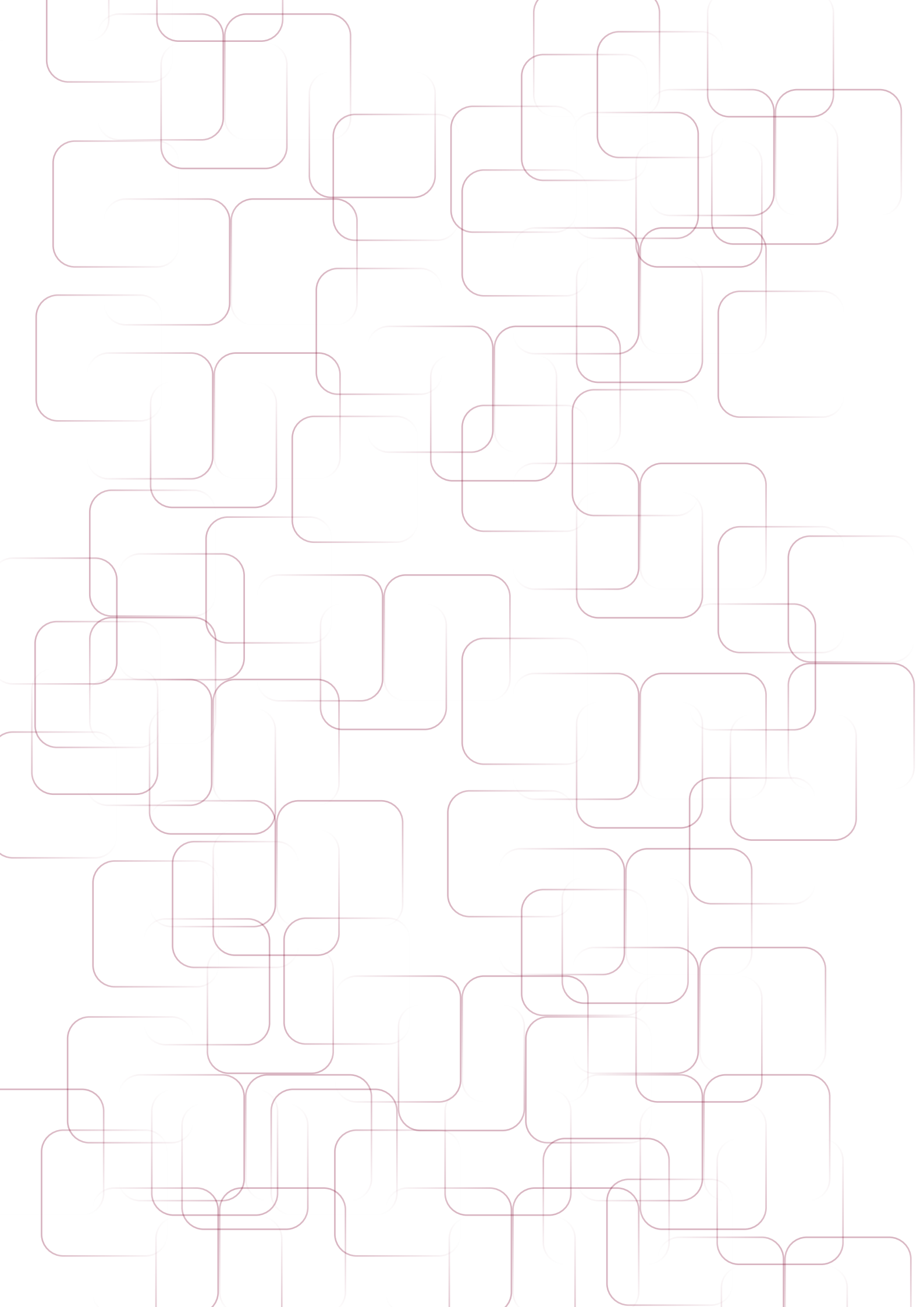
Tel: 0216 422 00 22 | <https://www.enstitusosyal.org> | info@enstitusosyal.org

■ İÇİNDEKİLER

Giriş	7
1. Değişiklik Önerisinin Paradigması ve Stratejik Öncelikleri	13
2. Dijital Platform Yükümlülüklerinin Yeniden Tanımlanması	19
3. Çocukların Dijital Ortamda Korunması	23
4. Sonuç	27
5. Politika Önerileri.....	31
Kaynakça	53
Yazarlar Hakkında.....	57



GİRİŞ



GİRİŞ

Kamuoyunda “İnternet Kanunu” olarak bilinen ve 2007 yılında yürürlüğe giren 5651 sayılı Kanun, kabul edildiği dönemin teknolojik, toplumsal ve hukuki koşullarına göre şekillenmiştir. Bu Kanun’un aradan geçen süre içinde dijital ekosistemin geçirdiği dönüşümle birlikte günümüzün ihtiyaçlarına uygun olarak güncellenmesi zorunlu hâle gelmiştir. Türkiye, nüfusuna oranla dijital platformların kullanım oranı bakımından dünyada önde gelen ülkeler arasında yer almaktadır. Bu nedenle dijital ortamların ve platformların yükümlülüklerinin düzenlenmesi Türkiye açısından mevzuat düzenlemesine ek olarak toplumsal refah, çocukların korunması ve kamu düzeni bakımından da stratejik bir gerekliliktir. Son dönemde 16 yaş altındaki çocukların sosyal medya ve akıllı telefon kullanımının sınırlandırılmasına ilişkin kamuoyunda ve politika yapıcılar nezdinde yoğunlaşan tartışmalar da, mevcut mevzuatın yetersizliğini ve İnternet Kanunu’nun kapsamlı biçimde güncellenmesi ihtiyacını görünür kılmaktadır.

Enstitü Sosyal, 5651 sayılı Kanun’u değerlendirmek üzere geniş katılımlı çalıştaylar düzenlemiş ve farklı uzmanlıklara sahip profesyoneller ile konu üzerinde derinlikli müzakereler yürütmüştür. Bu çerçevede çalışmanın çıkış noktası, mevzuat değişikliğine ek olarak, dijital düzenlemeye ilişkin paradigmanın bütünüyle yeniden düşünülmesidir. Bu yaklaşım, sembolik olarak Kanun’un adının “**Dijital Hizmetlerin ve Ortamların Düzenlenmesi Hakkında Kanun**” olarak değiştirilmesi önerisinde somutlaşmaktadır. Mevcut başlık olan “**İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun**” düzenlemeyi ağırlıklı olarak suç odaklı ve reaktif bir çerçeve içine yerleştirmektedir. Oysa dijital ekosistem düzenlemesi, artık yapay zekâ, algoritmik

şeffaflık, çocuk güvenliği ve dijital haklar gibi çok daha geniş bir alanı kapsamaktadır. Bu nedenle önerilen başlık, suçla mücadele yerine dijital ortamların bütüncül biçimde düzenlenmesini öne çıkaran proaktif bir yaklaşımı ifade etmekte ve “internet” yerine “dijital hizmetler ve ortamlar” kavramını kullanarak gelecekte ortaya çıkabilecek yeni teknolojileri de kapsayabilecek bir terminoloji benimsemektedir. Daha da önemlisi, bu Kanun’un dijital alana ilişkin tüm süreçlerde istisnai değil, birincil düzenleme olması ve dijital ortamdaki bütün meselelerin bu Kanun çatısı altında ele alınması hedeflenmektedir.

Bu analizin normatif dayanaklarından biri, Dijital Dünyada Çocuk Hakları Sözleşmesi’dir (Enstitü Sosyal, 2025a). Sözleşmenin her bir maddesi, Türkiye’de güncel ve kapsamlı bir internet kanununu gerekli kılmaktadır; zira çocukların dijital ortamda karşılaştıkları riskler, hak ihlalleri ve belirsizlikler, mevcut mevzuatla yeterince karşılanamamaktadır. Birleşmiş Milletler Çocuk Hakları Sözleşmesi, çocukların dijital ortamdaki varlıkları açısından da yorumlanabilmekle birlikte, bu alana özgü hakları, sorumlulukları ve sorumluları açık biçimde belirlememektedir. Bu belirsizliği gidermesi bakımından Dijital Dünyada Çocuk Hakları Sözleşmesi, önemli dayanaklardan biridir.

Bunun yanında, dijital kullanımın yaygınlaşması mevcut Kanun’un kapsamadığı yeni uygulamalar ve sorunlar üretmiştir. Enstitü Sosyal araştırmacıları tarafından hazırlanan Dijital Çağda Ailenin Dönüşümü raporunda da belirtildiği gibi toplumsal dönüşüm ile dijital mecraların kullanım biçimlerinin birlikte değişmesi, mevcut hukuki çerçevenin ihtiyaçlara cevap verememesine yol açmıştır (Enstitü Sosyal, 2025b). Bu durumu en çarpıcı biçimde gösteren örneklerden biri, dijital kumar bağımlılığındaki hızlı artıştır. Türkiye’de

Dijital Kumar raporu (Enstitü Sosyal, 2025c), dijital mecraların denetimsiz kullanımının bireyleri nasıl sömürüye açık hâle getirdiğini ortaya koymaktadır. Bugün her köşe başında görülen bahis ve kumar reklamları, mevcut düzenleme boşluklarını kullanarak insanları bir bağımlılık döngüsüne çekmekte; bu sorunla başa çıkabilmek için dijital platformların daha güçlü biçimde sorumlu tutulması zorunlu görünmektedir.

Benzer sorunlar farklı alanlarda da gözlemlenmekle birlikte, öncelikle çocuklar ve yaşlılar dijital ortamdaki denetimsizlikten en fazla etkilenen kesimlerdir. Henüz bilişsel ve psikososyal gelişimini tamamlamamış çocuklar ve gençler, algoritmaların manipülatif etkisine, siber zorbalığa, bağımlılık yapıcı tasarım kalıplarına ve ahlaki değerleri aşındıran içeriklere karşı daha savunmasızdır. Dijital okuryazarlığı sınırlı olan yaşlı nüfus ve diğer hassas gruplar ise dijital dolandırıcılık, finansal istismar ve manipülasyon girişimlerinin birincil hedefi olmuştur.

Çocukların oynadıkları oyunların içeriklerinin yeterince denetlenmemesi de bu sorunların somut bir örneğidir. Türkiye’de Avrupa merkezli PEGI derecelendirme sistemi kullanılıyor gibi görünse de, bu sistemin kültürel ve sosyolojik bağlamı yeterince dikkate almadığı tartışılmaktadır. Ayrıca bu derecelendirme sistemi ile oyunlara getirilen yaş sınırlamalarının bağlayıcı ve etkin yaptırımlarla desteklenmediği görülmektedir. Bu da Türkiye’nin ihtiyaçlarına uygun bir sistemin ve denetimin gerekliliğini açıkça ortaya koymaktadır.

Yapay zekâ teknolojilerinin yaygınlaşması, dijital ortamların düzenlenmesini aciliyet kazanan ve öncelik verilmesi gereken bir konuya dönüştürmüştür. *Deepfake* içeriklerin denetimsiz biçimde üretilmesi, yapay zekâ destekli içeriklerle toplumun manipüle edilebilmesi ve yanlış bilginin hızla yayılması, mevcut mevzuatın bu yeni risklere hızlı ve doğru bir yanıt veremediğini göstermektedir. Bu nedenle dijital ortamların düzenlenmesi kamu düzeni, millî güvenlik ve demokratik

süreçlerin korunması açısından kritik bir zorunluluktur.

Teknolojik paradigmanın köklü bir dönüşüm geçirdiği 21. yüzyılda, dijital ortamlar fiziksel sınırları aşan, geleneksel hukuk normlarını zorlayan ve devletlerin egemenlik alanlarını etkileyen yeni bir “siber uzay” gerçekliği yaratmıştır. Mevcut hukuki düzenlemelerin bu yeni gerçekliğin yarattığı çok boyutlu tehditler karşısında yetersiz kalması, devletin bu alandaki konumunu edilgen bir izleyici olmaktan çıkararak aktif bir düzenleyiciye dönüştürmesini gerektirmektedir.

Bu bağlamda dijital hizmet sağlayıcıları ve sosyal ağ platformları, karmaşık kullanıcı sözleşmeleri aracılığıyla bireylerin en mahrem kişisel verilerini toplamakta; bu verileri büyük veri madenciliği ile işleyerek insanların bilgilerini ticari birer meta hâline getirebilmektedir. Vatandaşların eğilimleri, tüketim alışkanlıkları, psikolojik zaafı ve biyometrik verileri küresel teknoloji şirketlerinin kâr maksimizasyonu hedefi doğrultusunda profillenmekte ve üçüncü taraflara pazarlanabilmektedir (Kosinski, Stillwell, & Graepel, 2013). 2018’de ortaya çıkan Cambridge Analytica davası bunun önemli bir örneğidir (Cadwalladr & Graham-Harrison, 2018). Bu dava, Facebook aracılığıyla elde edilen veriler kullanılarak seçim süreçlerine yapılan müdahalenin ve bu süreçte yürürlükte olan yasal mevzuatın etkisini görünür kılmıştır. Facebook 2019 yılında, ABD’de veri ihlali davası sonucunda 5 milyar dolar para cezası alırken, İngiltere’de yürütülen soruşturmada Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR - General Data Protection Regulation) henüz yürürlükte olmadığı için 1998 tarihli Veri Koruma Yasası’nın (Data Protection Act, 1998) izin verdiği en yüksek miktar olan 500.000 sterlin ceza almıştır (Federal Trade Commission, 2019; United Kingdom Parliament, 2019). Bu vaka mevzuat düzenlemelerinin hem ihlal ortaya çıkmadan alınacak önlemlerin, hem de cezai süreçlerin şirketlerin ticari kapasitelerine uygunluğunun önemini ortaya koymaktadır. Dahası, bu şirketlerin sahip olduğu veri, teknik

kapasite ve mali kaynaklar, güncel teknolojilere dair bilgiyi çoğu zaman devletlerden daha ileriye taşıyarak belirgin bir bilgi asimetrisi yaratmaktadır. Bu asimetrinin dengelenebilmesi için platformların veriyi nasıl kullandıklarını ayrıntılı biçimde gösteren şeffaflık raporları yayımlaması ve sivil toplum, akademi ve uzman kuruluşların denetleyici rolünün güçlendirilmesi kritik önemdedir.

Bu tablonun en önemli boyutlarından biri, verinin depolandığı sunucuların büyük ölçüde yurt dışında bulunmasıdır. Ulusal verinin ülke sınırları dışına çıkarılması hem kişisel verilerin korunması konusunda hem de ulusal güvenlik anlamında sorun teşkil etmektedir. Yargı mercilerinin suç teşkil eden eylemlere ilişkin dijital delillere erişiminin yabancı şirketlerin inisiyatifine bırakılması ve adli yardımlaşma süreçlerinin tıkanması, Türkiye Cumhuriyeti'nin yargı yetkisini zaman zaman sınırlandırmaktadır. Bu nedenle verinin millileştirilmesi ve sunucuların yurt içinde bulunması bir tercih değil, egemenlik hakkının gereğidir.

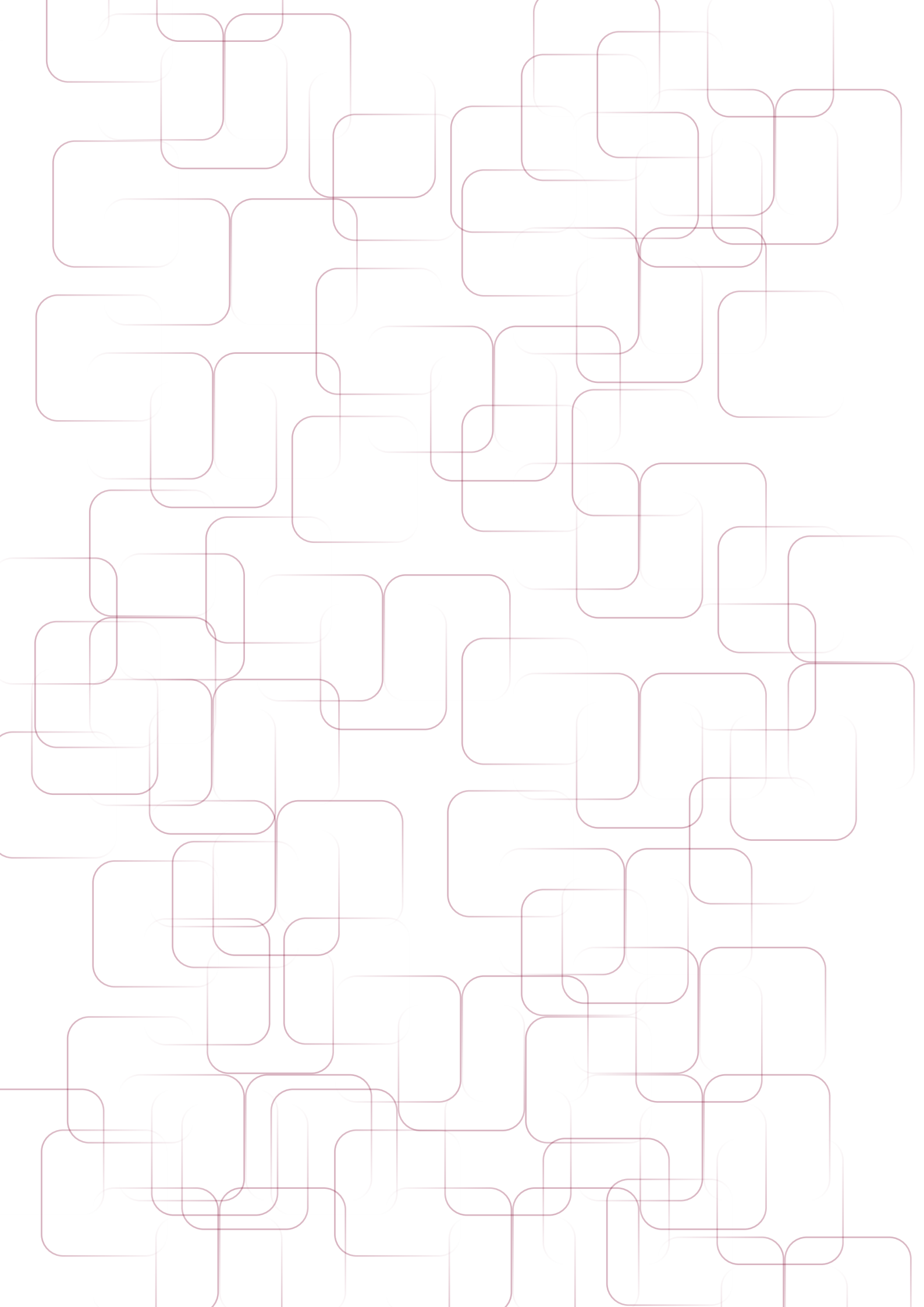
Dijital ortamlar, “mutlak anonimlik” algısının sağladığı sorumsuzluk hâli nedeniyle suç ve suçlu için güvenli bir alan hâline gelmiştir. İstatistikler, dijital mecralarda işlenen hakaret, tehdit, şantaj, dolandırıcılık, dezenformasyon ve terör propagandası suçlarında belirgin bir artış olduğunu göstermektedir. Bilişim suç dosya sayısı 2018 yılında 2.242 iken, bu sayı 2024 yılına geldiğimizde yedi kattan fazla artarak 16.358'e çıkmıştır (M. B. Kaya, 2022; Adalet İstatistikleri, 2025). Buna karşılık mevcut yasal çerçevede dijital hizmet sağlayıcıları için öngörülen idari para cezalarının, trilyon dolarlık bütçelere sahip küresel teknoloji şirketleri karşısında caydırıcı olmadığı açıktır.

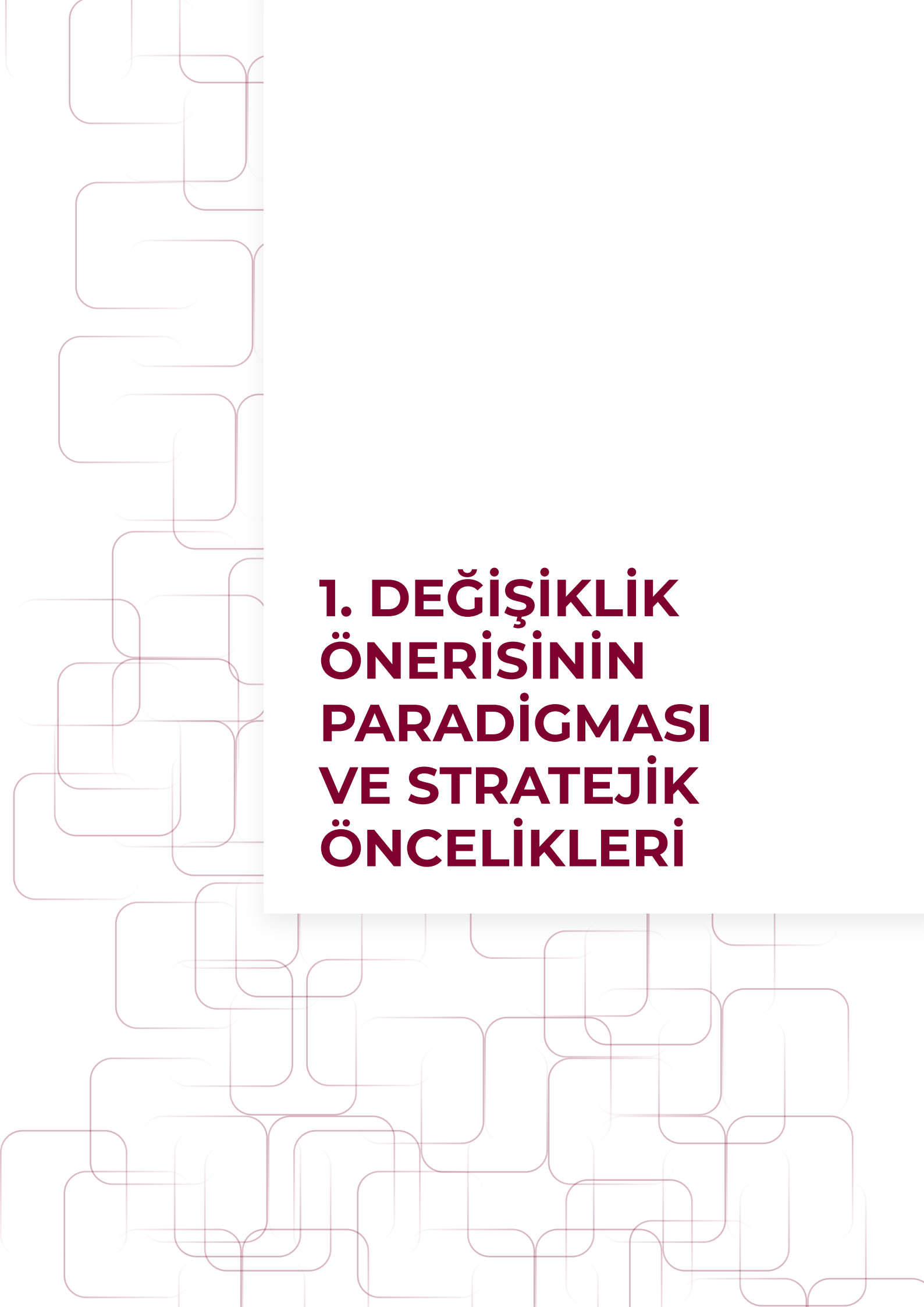
Bu nedenle bu analiz üç temel eksen üzerinde şekillenmektedir. Birinci ve öncelikli eksen, Kanun'un paradigmasının değişimidir; zira 5651 sayılı Kanun'un benimsediği suç odaklı, reaktif ve engelleme merkezli yaklaşımın yerini, risk temelli ve önleyici düzenlemeye, platform sorumluluğunun genişletilmesine, çocuklar için merkezi bir koruma rejimine, algoritmik şeffaflık ve hesap verebilirliğe ve çok paydaşlı katılıma dayanan yeni bir düzenleyici modele bırakması gerekmektedir. Analizin birinci bölümünde, Kanun'un mevcut paradigmasının sınırları ile yeni önerilen paradigmanın temel ilkeleri ve öncelik verilen alanları ele alınacaktır.

İkinci eksen, dijital teknoloji şirketlerinin yükümlülüklerinin genişletilmesidir; üçüncü eksen ise çocukların dijital haklarının korunmasıdır. İnternet Kanunu'nda yapılacak değişiklikler bakımından belirleyici başlıklar da esasen bu üç eksen etrafında şekillenmektedir.

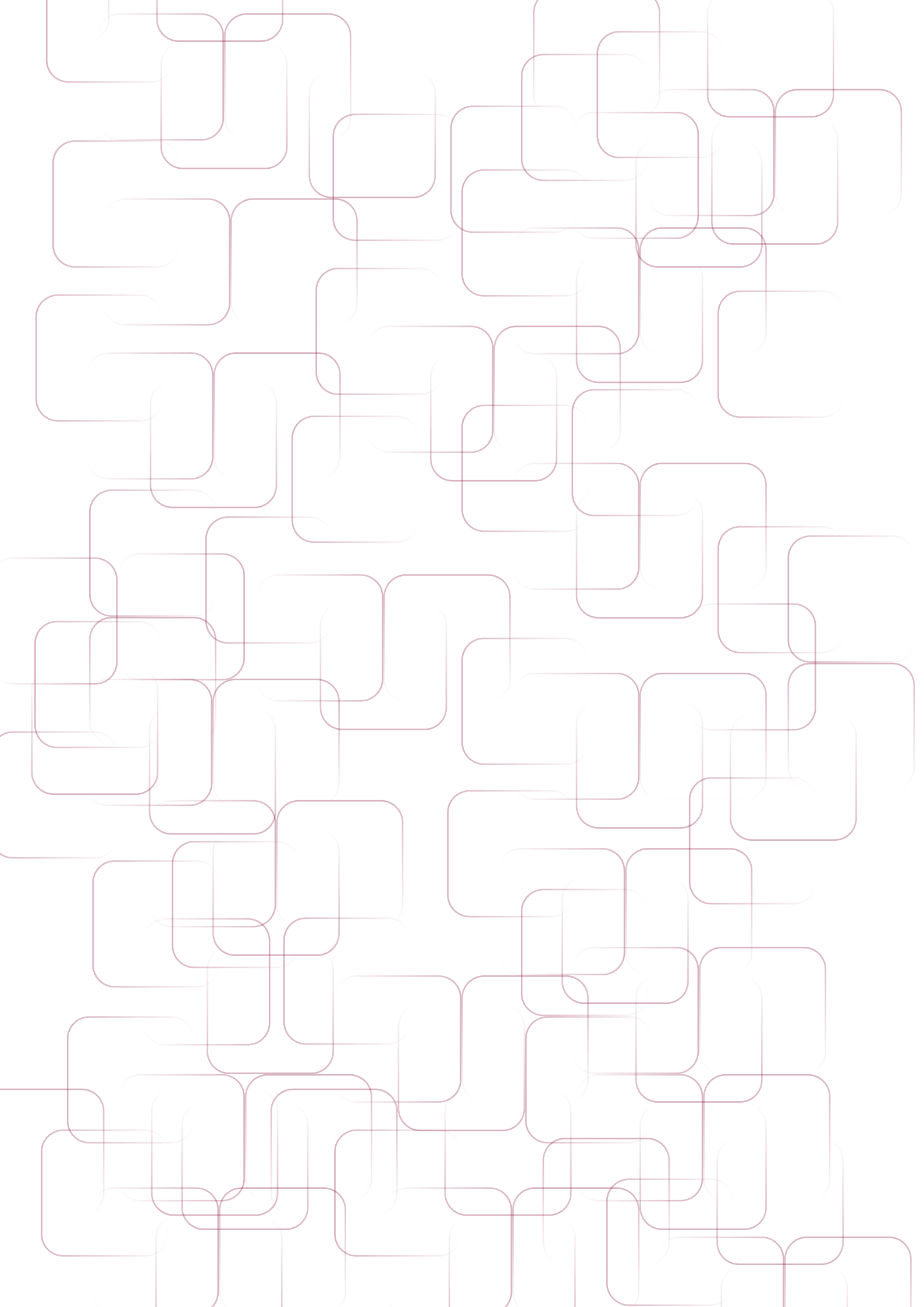
Aynı zamanda yeni düzenleyici çerçevenin; içerik sağlayıcıları, yer sağlayıcıları, erişim sağlayıcıları, sosyal ağ sağlayıcıları, arama motorları, çevrim içi pazar yerleri ve VPN hizmet sağlayıcılarını kapsayacak biçimde geniş ve bütüncül olması gerekmektedir.

Bu doğrultuda analiz boyunca, önce Kanun'un paradigmasına ilişkin dönüşüm önerileri ortaya konulacak; ardından platformların yükümlülüklerinin artırılması, hak ihlallerinin önlenmesi ve özellikle çocukların dijital ortamda daha etkin biçimde korunması yönünde mevzuat ve uygulama değişiklikleri tartışılacaktır. Analizin sonunda ise bahsedilen değişiklikleri içeren Kanun maddelerine dair önerilerle ilgili karşılaştırmalı bir tablo sunulacaktır (Tablo 3).





1. DEĞİŞİKLİK ÖNERİSİNİN PARADİGMASI VE STRATEJİK ÖNCELİKLERİ



DEĞİŞİKLİK ÖNERİSİNİN PARADİGMASI VE STRATEJİK ÖNCELİKLERİ

1.1. Paradigma Değişiklikleri

Mevcut 5651 sayılı Kanun, kabul edildiği dönemin koşulları gereği ağırlıklı olarak suçla mücadele odaklı, reaktif ve erişim engellemeye dayalı bir yaklaşım üzerine inşa edilmiştir. Dijital ekosistemin geldiği aşama ise bu yaklaşımın yetersiz kaldığını göstermekte ve köklü bir paradigma değişimini zorunlu kılmaktadır. Bu çerçevede eski yaklaşım ile önerilen yeni yaklaşım arasındaki temel farklar tabloda olduğu gibi özetlenebilir.

Bu değişim, Kanun'un yalnızca suçların bastırılmasına odaklanan bir araç olmaktan çıkıp dijital ekosistemi düzenleyen, riskleri yöneten ve hakları koruyan bir çerçeveye dönüşmesini hedeflemektedir.

orantılı sorumluluklar yükleyen bir düzenleyici yapı öngörmektedir. Bu çerçevede Kanun'un stratejik öncelikleri; çocukların korunması, algoritmik şeffaflık ve hesap verebilirliğin sağlanması, caydırıcı ve orantılı yaptırım mekanizmalarının oluşturulması, dijital uyumsuzluklarda hızlı ve ihtisaslaşmış bir yargılamanın tesis edilmesi, platform temsilciliğinin etkinleştirilmesi, bot hesap ve dezenformasyonlarla mücadele edilmesi, sivil toplumun denetim süreçlerine katılımını güçlendiren güvenilir işaretçi sisteminin kurulması ve VPN hizmetlerinin düzenlenmesi etrafında şekillenmektedir. Bu öncelikler birlikte ele alındığında, Kanun'un suç odaklı bir metin olmaktan çıkıp dijital ortamı bütüncül biçimde düzenleyen bir çerçeveye dönüşmesini hedeflemektedir.

1.2. Önerinin Stratejik Öncelikleri

Önerilen değişiklikler dijital ekosistemde ortaya çıkan riskleri yönetebilen, hakları koruyan ve platformlara toplumsal etkisiyle

Öncelik 1: Çocukların Korunması

Mevcut Kanun, çocuk korumasını ağırlıklı olarak "çocukların cinsel istismarı" suçu üzerinden ele almaktadır. Yeni düzenlemelerle birlikte çocuk koruması çok boyutlu bir çerçevede düşünülmelidir:

Tablo 1. Mevcut ile önerilen Kanun'un yaklaşımının karşılaştırılması

Mevcut Yaklaşım	Önerilen Yaklaşım
Suç odaklı, reaktif	Risk temelli, önleyici
Engelleme ağırlıklı	Çok katmanlı müdahale
Platform pasifliği	Platform sorumluluğu
Sabit para cezaları	Ciro bazlı yaptırımlar
Genel düzenleme	Orantılı, kademelendirilmiş yükümlülükler
Çocuk koruma sınırı	Çocuk merkezli tasarım
Algoritmalar görünmez	Algoritmik şeffaflık zorunlu
Yabancı platformlara sınırlı erişim	Tam tüzel kişilik zorunluluğu

Çocuklara Yönelik Riskler:

- Cinsel istismar ve istismara hazırlama süreci (*grooming*)
- Siber zorbalık
- Psikolojik manipülasyon
- Ekonomik sömürü (dijital oyunlarda harcama teşvikleri)
- Dijital bağımlılık
- Veri gizliliği ihlalleri
- Uygun olmayan içeriğe maruz kalma

Önerilen Koruma Mekanizmaları:

- e-Devlet ya da benzeri sistemler vasıtasıyla teknik yaş doğrulama sistemleri
- Türkiye özelinde tasarlanacak pedagojik sınıflandırmalar doğrultusunda yaş gruplarına göre farklılaştırılmış koruma (0-15, 15 yaşını doldurmuş, 15-18)
- Varsayılan güvenlik ayarları (*privacy by design*)
- Çocuklar için kişiselleştirilmiş reklam yasağı
- Konum bilgisi toplama yasağı
- Tüm platformlarda aile denetim mekanizmalarının zorunlu hâle getirilmesi; arkadaş ekleme gibi etkileşimli fonksiyonlarda ebeveyn onayı aranması ve etkinlik izleme sistemlerinin oluşturulması
- Çocuk kullanıcılar için dijital platformlarda çevrim içi mesajlaşma uygulamalarının kısıtlanması

Öncelik 2: Algoritmik Şeffaflık ve Hesap Verebilirlik

Büyük ölçekli platformların algoritmik sistemleri, içerik yayılımını, kullanıcı davranışlarını ve kamusal algıyı şekillendirme kapasitesine sahiptir. Bu güç, şeffaflık ve hesap verebilirlik mekanizmaları ile dengelenmelidir:

Algoritmik Sorumluluk İlkeleri:

- Öneri algoritmalarının parametrelerinin açıklanması
- Algoritmik benimseme durumunda müteselsil sorumluluk

- Bağımsız algoritma denetimi mekanizmaları
- Kullanıcılara algoritmik tercihleri güncelleme seçeneği

Öncelik 3: Etkili Yaptırım Sistemleri

Mevcut sabit meblağlı para cezaları, özellikle küresel gelire sahip büyük platformlar için caydırıcı değildir.

Önerilen Yaptırım Sistemi:

- Büyük ölçekli platformlar için ciro bazlı cezalar (küresel ciro üzerinden)
- Küçük ve orta ölçekli hizmet sağlayıcılar için sabit meblağlı cezaların güncel şartlar doğrultusunda yeniden düzenlenmesi
- Kademeli yaptırım sistemi (uyarı → para cezası → reklam yasağı → bant genişliği daraltma)
- Dijital varlık ve gelirlerin dondurulması yetkisi (en ağır ihlallerde ve devletin egemenliğine aykırı durumlarda)
- Yönetici sorumluluğu ve müteselsil sorumluluk

Yükümlülükler, hizmet sağlayıcıların büyüklüğü, toplumsal etkisi ve risk profili ile orantılı olmalıdır. Türkiye’den erişim sayısı baz alınarak yapılacak planlama ile yükümlülükler şu şekilde sınıflandırılabilir:

- Büyük Ölçekli Platformlar (aylık 5 milyon üzerinde erişim): En kapsamlı yükümlülükler
- Orta Ölçekli Platformlar (100.000 - 5 milyon arası erişim): Temel yükümlülükler
- Küçük Ölçekli Platformlar (100.000 altı erişim): Minimum yükümlülükler

Kademeli Yaptırım Mekanizması:

1. Uyarı: İlk ihlalde yazılı uyarı
2. İdari Para Cezası: Tekrarlayan ihlallerde artan oranlı para cezası
3. Reklam Yasağı: Ciddi ihlallerde Türkiye’de reklam verme yasağı
4. Bant Genişliği Daraltma: Yükümlülüklerin

- yerine getirilmemesi hâlinde kademeli daraltma
5. Dijital Varlık Dondurma: En ağır ihlallerde Türkiye'deki dijital varlıkların dondurulması

Tablo 2. Platformların ihlal düzeyine göre almaları önerilen cezalar

İhlal Düzeyi	Ceza Oranı (Küresel Ciro Üzerinden)
Hafif ihlaller	Binde 1-5 veya güncel şartlarla orantılı sabit meblağlar
Orta ihlaller	Binde 5-10 veya güncel şartlarla orantılı sabit meblağlar
Ağır ihlaller	Yüzde 1-5
Çok ağır ihlaller	Yüzde 5-10

Öncelik 4: Hızlı ve İhtisaslaşmış Yargılama

Dijital ortamların hızı ile yargı süreçlerinin uyumsuzluğu ciddi sorunlara yol açmaktadır.

Önerilen Yapılanma:

- Bilişim ihtisas mahkemelerinin kurulması
- Hızlı itiraz mekanizmaları (24 saat içinde karar)
- Acil durumlarda 4 saat içinde geçici tedbir
- Hâkim ve savcılara dijital hukuk eğitimi

Öncelik 5: Platform Temsilciliğinin Etkinleştirilmesi

Mevcut temsilcilik sistemi uygulamada işlevsiz kalmıştır.

Yeni Temsilcilik Modeli:

- Tam yetkili ve tam sorumlu tüzel kişilik zorunluluğu

- Türkiye'de ikamet eden yöneticiler
- Türkçe konuşan ve kullanıcılar tarafından ulaşılabilir canlı destek mekanizması
- Kullanıcı şikayetlerine 72 saat içinde yanıt zorunluluğu

Öncelik 6: Bot Hesap ve Dezenformasyon ile Mücadele

Bot hesaplar kamu düzenini ve demokratik süreçleri tehdit etmektedir.

Önerilen Tedbirler:

- Bot tespit ve işaretleme sistemleri zorunluluğu
- Meşru botlar için "otomatik hesap" ibaresi zorunluluğu
- Sahte etkileşim üretimine yeni yaptırımlar

Öncelik 7: Güvenilir İşaretçi (Trusted Flagger) Sistemi

Sivil toplumun denetim süreçlerine katılımı güçlendirilmelidir.

Sistem Özellikleri:

- Uzman sivil oluşumlara (STK'lar, düşünce kuruluşları vs.) güvenilir işaretçi statüsü
- İşaretlenen içeriklere öncelikli değerlendirme
- Yıllık performans değerlendirmesi
- Kötü niyetli bildirimde statü iptali

Güvenilir işaretçi sistemi kapsamında STK'lar bu görevi belirli bir süre gönüllülük esaslı yürütebilir; ancak yapının sürekliliği için bir teşvik ve fonlama mekanizmasının kurulması zorunludur. Kamu yararına çalışan kuruluşlara (örneğin Kızılay, Yeşilay) yapılan bağışların vergi matrahından indirilebilmesine benzer şekilde, güvenilir işaretçi statüsündeki kuruluşlara sağlanacak mali desteklerin de vergi teşviki kapsamına alınması hâlinde, hem bireylerin hem de şirketlerin bu alana kaynak aktarmasının önü açılacak; sistem kurumsal kapasite ve uzmanlık bakımından sürdürülebilir hâle gelecektir.

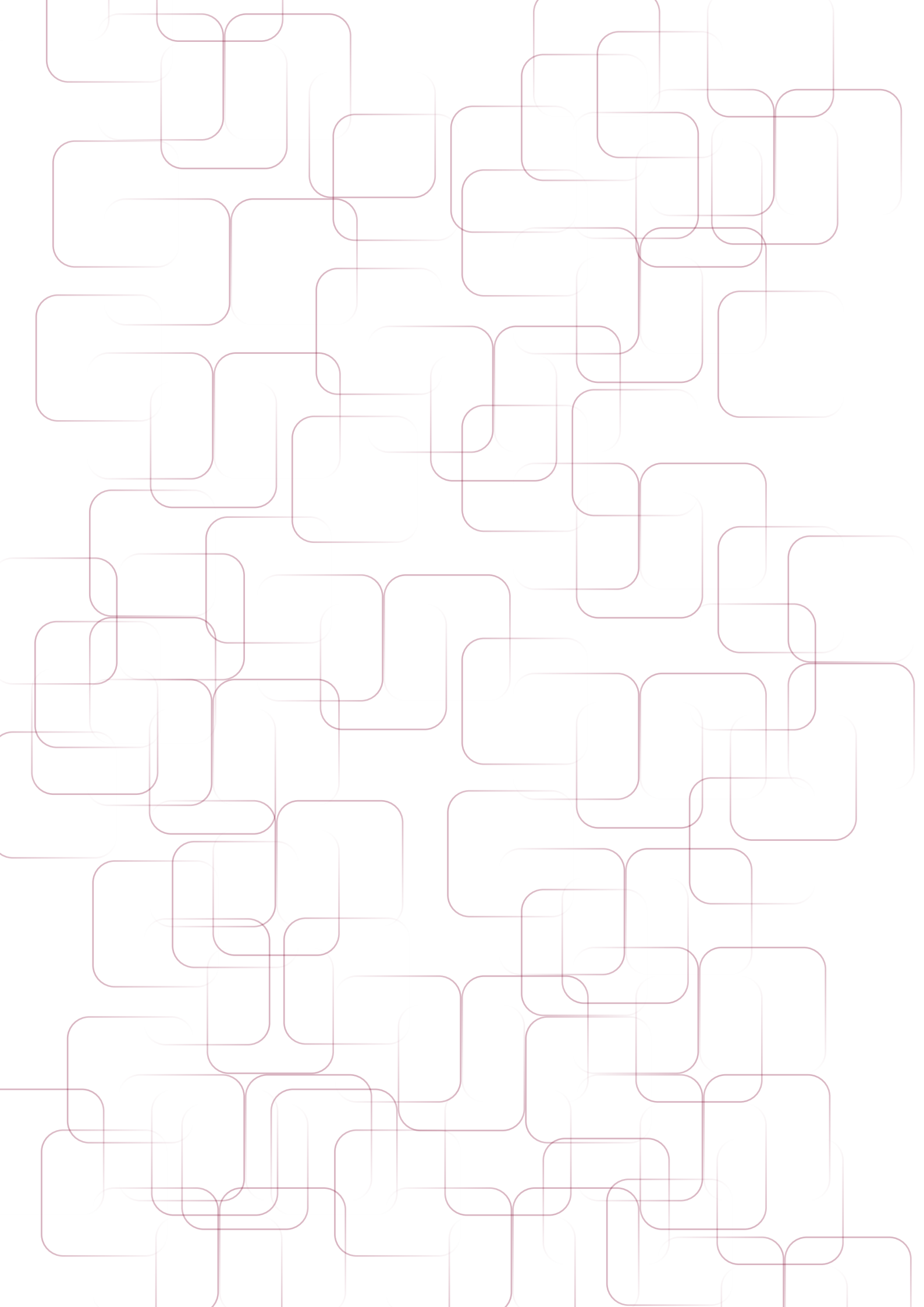
Öncelik 8: VPN Hizmetlerinin Düzenlenmesi

VPN hizmetlerinin meşru kullanımı korunurken, kötüye kullanımın önlenmesi gerekmektedir.

Düzenleme Çerçevesi:

- Lisanslama zorunluluğu
- Trafik bilgisi saklama yükümlülüğü
- Türkiye temsilciliği (belirli kullanıcı eşiği üstünde)
- Meşru kullanım alanlarının korunması

2. DİJİTAL PLATFORM YÜKÜMLÜLÜKLERİNİN YENİDEN TANIMLANMASI



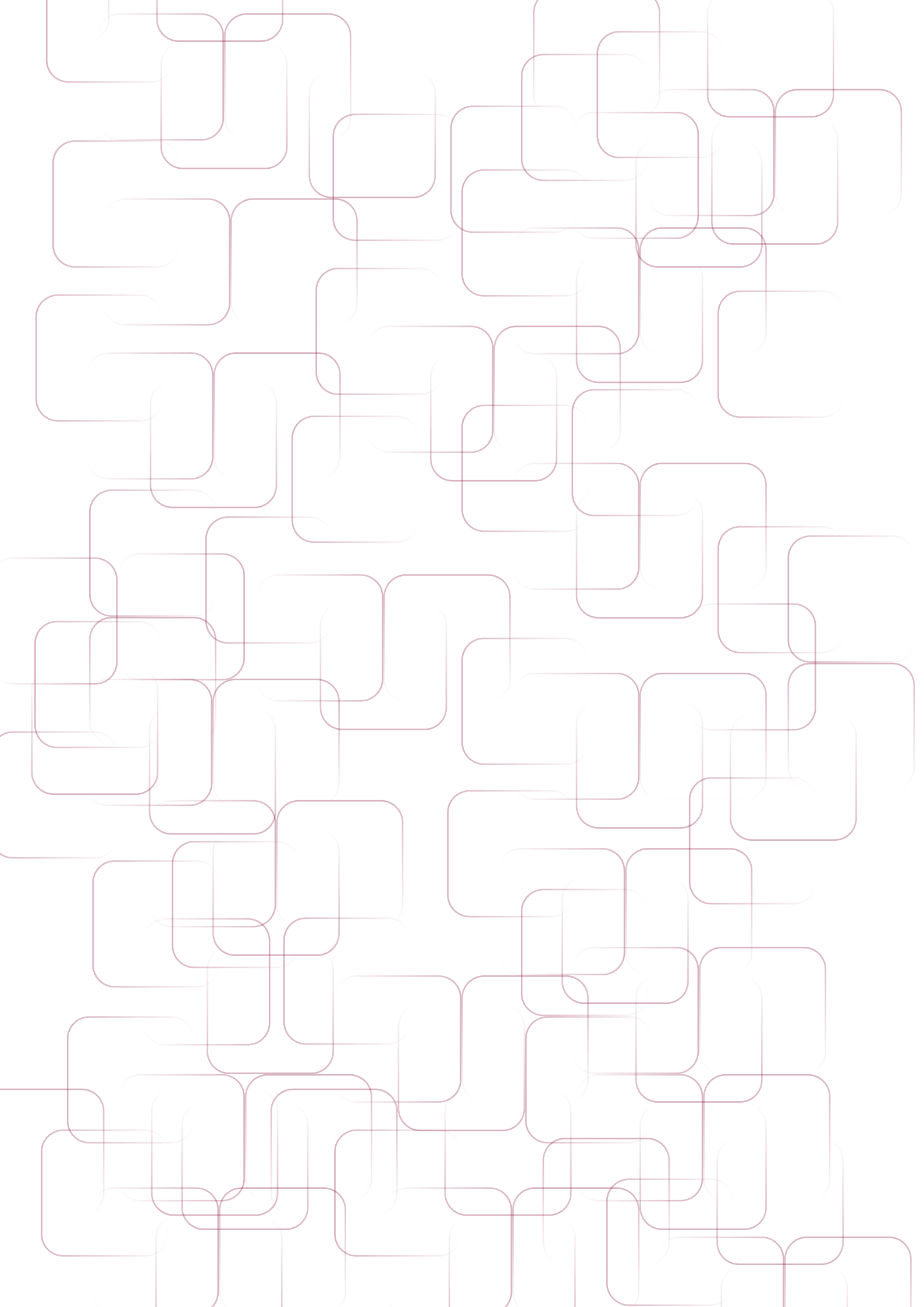
DİJİTAL PLATFORM YÜKÜMLÜLÜKLERİNİN YENİDEN TANIMLANMASI

Bu analizin ikinci eksenini, dijital platformların ve diğer dijital hizmet sağlayıcılarının yükümlülüklerinin kapsamlı biçimde yeniden tanımlanmasıdır. Önerilen değişiklikler, platformları pasif aracı konumundan çıkararak toplumsal etkileriyle orantılı sorumluluk üstlenen aktörler hâline getirmeyi hedeflemektedir.

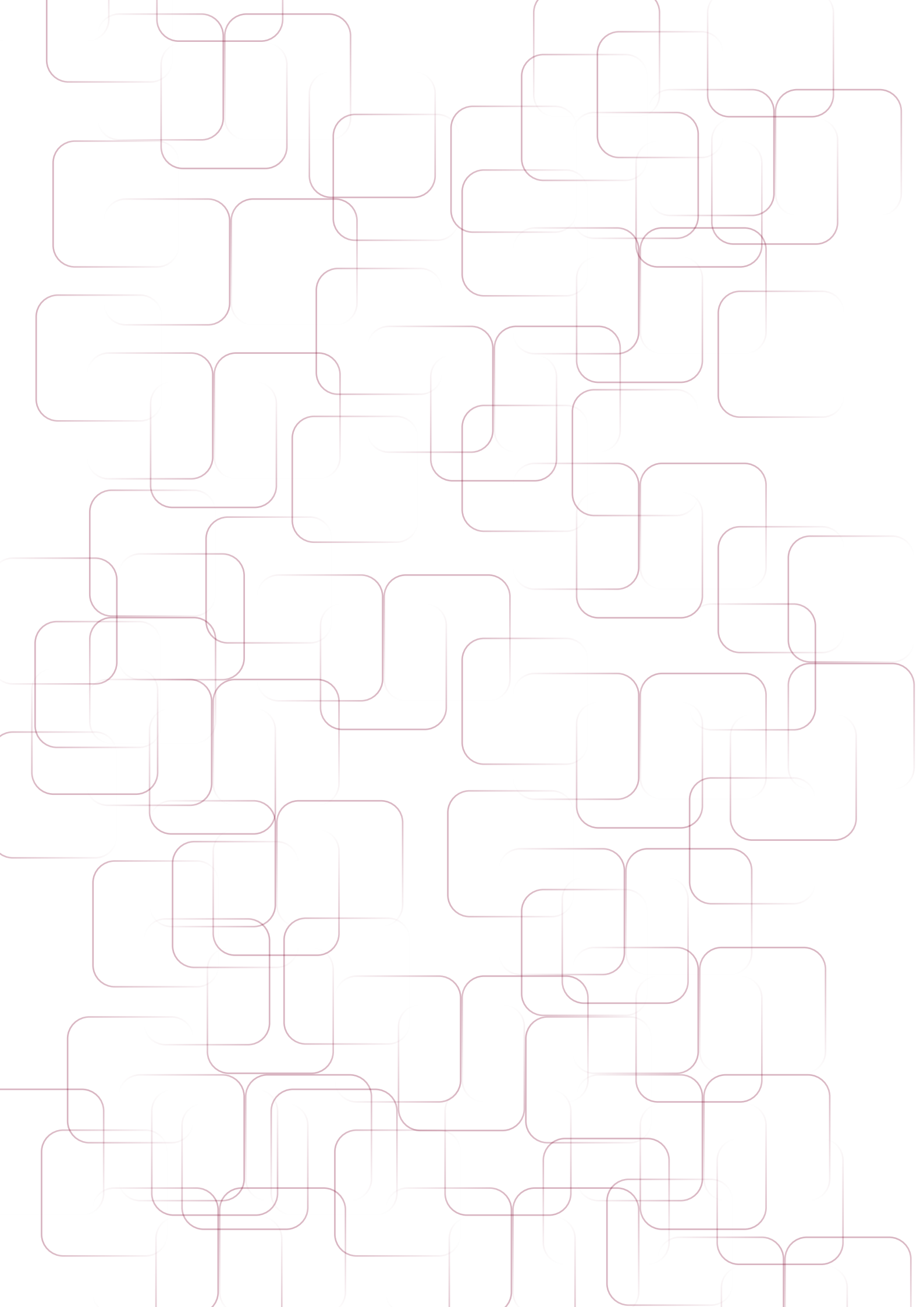
Bu çerçevede amaç maddesinde dijital hizmetlerin düzenlenmesi, şeffaflık ve hesap verebilirlik ilkelerinin açıkça tanımlanması; tanımlar bölümünde algoritmik şeffaflık, algoritmik benimseme, bot hesap, sentetik içerik ve büyük ölçekli platform gibi kavramların mevzuata dâhil edilmesi; bilgilendirme ve temsil yükümlülüğünde ciro bazlı yaptırımların benimsenmesi ve 7/24 Türkçe canlı destek zorunluluğunun getirilmesi öngörülmektedir. Platformun, içeriği algoritmik olarak öne çıkarması veya yayılımını artırması hâlinde müteselsil sorumluluk öngörülmekte; ayrıca öneri sistemlerinin şeffaf ve denetlenebilir olması ile zararlı içeriklerin yayılımını engelleyici proaktif tedbirler alması

zorunlu tutulmaktadır. Erişim sağlayıcılarına yönelik düzenlemeler, yalnızca engelleme ve log tutma yükümlülüklerinin ötesine geçerek şeffaflık raporları yayımlama ve çocuklara yönelik varsayılan güvenli internet profili sunma gibi altyapı düzeyinde sorumluluklar getirmektedir. Yargılama süreçlerinde bilişim ihtisas mahkemeleri, hızlı tedbir ve itiraz mekanizmaları öngörülmekte; temsilcilik rejiminde ise büyük ölçekli platformların Türkiye’de tam yetkili ve tam sorumlu tüzel kişilik kurması zorunlu kılınmaktadır.

Buna ek olarak VPN hizmetlerinin lisanslanması ve denetlenmesi, bot hesaplarla mücadele, güvenilir işaretçi sistemi, sentetik içerik ve *deepfake* düzenlemesi ile dijital hizmet sağlayıcılarının periyodik şeffaflık raporu yayımlama yükümlülüğü getirilmekte; böylece platformların veri işleme pratikleri, algoritmik işleyişleri ve ticari modelleri kamu denetimine açılmaktadır. Bütün bu düzenlemeler, platformların ekonomik gücüyle orantılı, risk temelli ve hesap verebilir bir sorumluluk rejimi inşa etmeyi amaçlamaktadır.



3. OCUKLARIN DİJİTAL ORTAMDA KORUNMASI



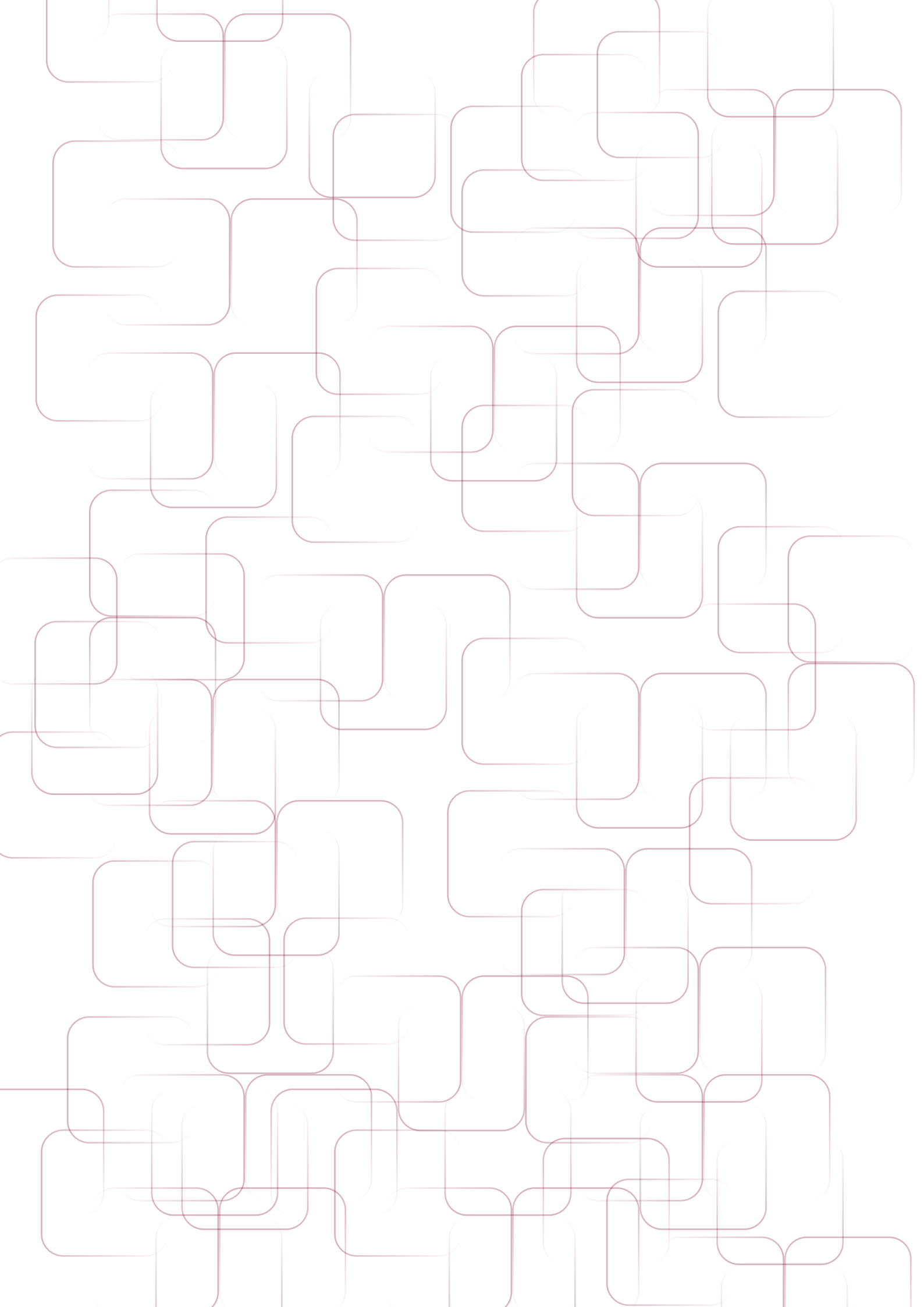
ÇOCUKLARIN DİJİTAL ORTAMDA KORUNMASI

Bu analizin üçüncü eksen, çocukların dijital ortamlarda çok boyutlu biçimde korunmasını merkezine alan bir hukuki yapının kurulmasıdır. Önerilen değişiklikler, çocuk korumasını yalnızca cinsel istismar suçu ekseninden çıkararak psikolojik, sosyal, ekonomik ve dijital riskleri de kapsayan bütüncül bir çerçeveye taşımaktadır. Bu sebeple amaç maddesinde “çocuğun gözetilmesi”nin Kanun’un kurucu ilkelerinden biri hâline getirilmesi önem taşımaktadır. Tanımlar bölümünde ise dijital istismar, siber zorbalık ve dijital bağımlılık gibi kavramların açıkça tanımlanması, olası hak ihlallerinin tespitini ve müdahaleyi mümkün kılacaktır. Erişim sağlayıcılarına, on beş yaş altı çocuklar için varsayılan güvenli internet profili sunma, yaş gruplarına göre farklılaştırılmış filtreleme sağlama ve ebeveyn denetim araçlarını ücretsiz kılma yükümlülükleri getirilmesi de bu noktada önemlidir.

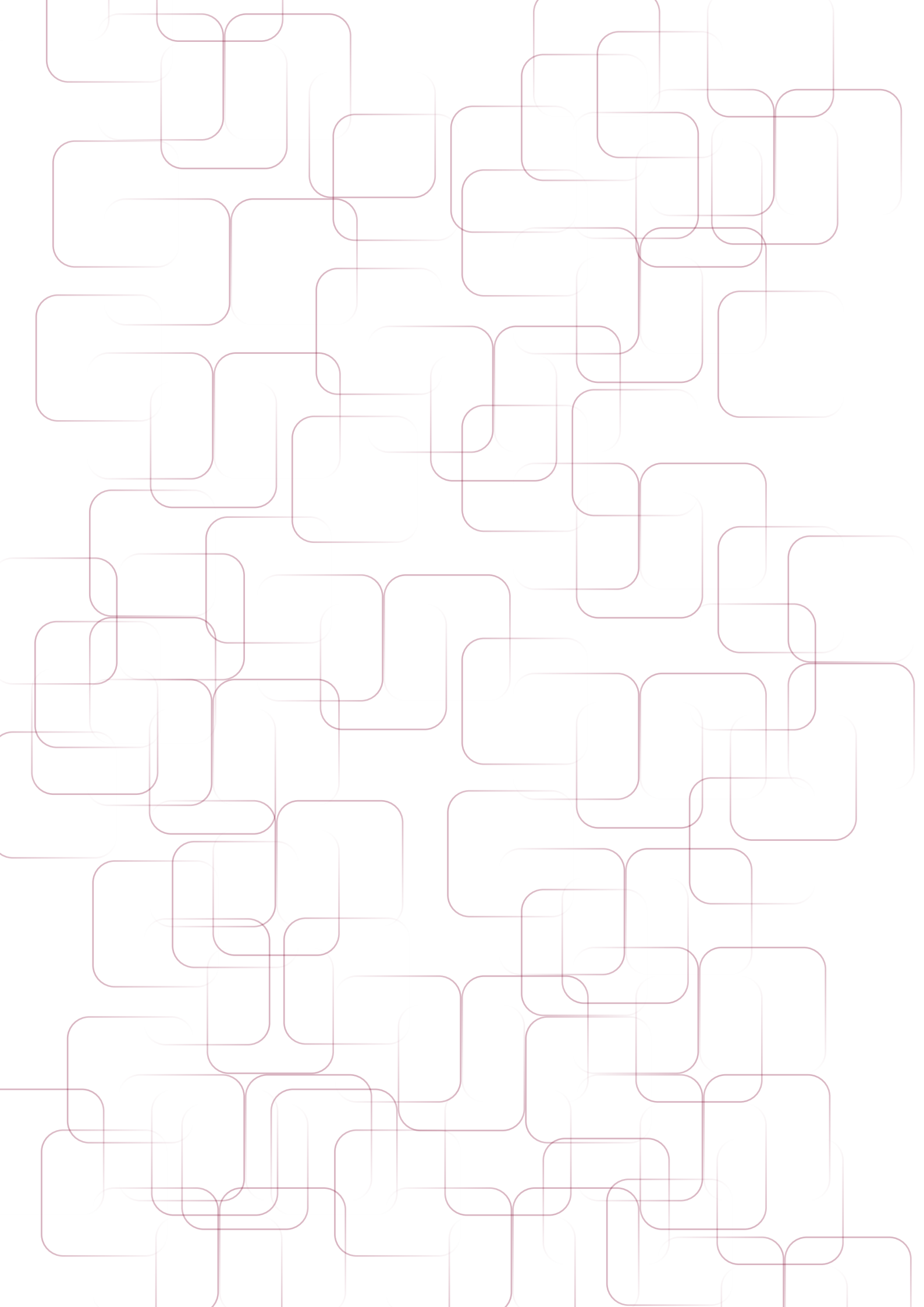
Çocuklara yönelik dijital hizmet sunan platformların Tablo 3’te önerilen Ek Madde 6’da olduğu gibi “*privacy by design*” yaklaşımını benimsemesi gerekmektedir (Tablo 3). Bu yaklaşım baştan itibaren çocukların gözetilmesi ilkesiyle uyumlu olarak tasarlanmış platformlarla olası ihlallerin önüne geçilmesi bakımından önem arz etmektedir. Buna ek olarak yine çocukların fiziksel duygusal ve zihinsel gelişimlerine uygun içeriklerle

muhatap olabilmesi için yaş kısıtlamalarını beyana dayalı yöntemlerle sürdürmek yerine teknik yaş doğrulama sistemleri elzemdir. Yaş doğrulama sistemlerinin oluşturulabilmesi on beş yaş altı çocukların sosyal medya platformlarına erişimiyle ilgili boşlukların tamamlanması için de ön koşullardan birisidir. Dijital Dünyada Çocuk Hakları Sözleşmesi’nde de bahsedildiği üzere çocukların verisinin özel nitelikli veri kapsamına alınması çocukların gözetilmesi ilkesiyle doğrudan uyumlu bir adım olacaktır. Böylelikle platformların çocuklara kişiselleştirilmiş reklam göstermesi, konum verisi toplaması, davranışsal profillemeye yapması ve üçüncü taraflarla veri paylaşmasının önüne geçilebilir; oyunlar ve video platformları için pedagojik temelli içerik sınıflandırma ve filtreleme zorunluluğu getirilebilir. Ayrıca çocuklara yönelik istismarı tespit edecek proaktif izleme sistemleri, etkili siber zorbalık raporlama mekanizmaları ve güvenilir işaretçiler tarafından bağımsız değerlendirme süreçleri de çocukların korunmasında önemli başlıklardandır.

Bütün bu düzenlemeler, çocukların dijital ortamda güvenli biçimde var olabilesini sağlarken ailelerin ve kamu otoritelerinin koruyucu rolünü güçlendiren, gelişimsel farklılıkları gözetken ve risk temelli bir çocuk koruma yaklaşımı oluşturmayı hedeflemektedir.



4. SONUÇ



SONUÇ

Buraya kadar olan değerlendirmeler, 2007 yılında yürürlüğe giren 5651 sayılı Kanun'un günümüzün dijital gerçekleri karşısında kapsamlı biçimde güncellenmesi gerektiğini açıkça göstermektedir. Türkiye'nin dijital platform kullanımında küresel ölçekte öne çıkması, dijital ortamların düzenlenmesini teknik bir mevzuat meselesinin ötesine taşıyarak toplumsal refah, çocukların korunması, kamu düzeni ve ulusal güvenlik bakımından kaçınılmaz bir gereklilik olarak ortaya koymaktadır. Özellikle 15 yaş altı çocukların sosyal medya ve akıllı telefon kullanımına ilişkin tartışmalar, algoritmik manipülasyon riski ve dijital içeriklerin yetersiz denetimi, mevcut hukuki çerçevenin sınırlılıklarını ortaya çıkarmakta ve İnternet Kanunu'nun kapsamlı biçimde güncellenmesini zorunlu kılmaktadır.

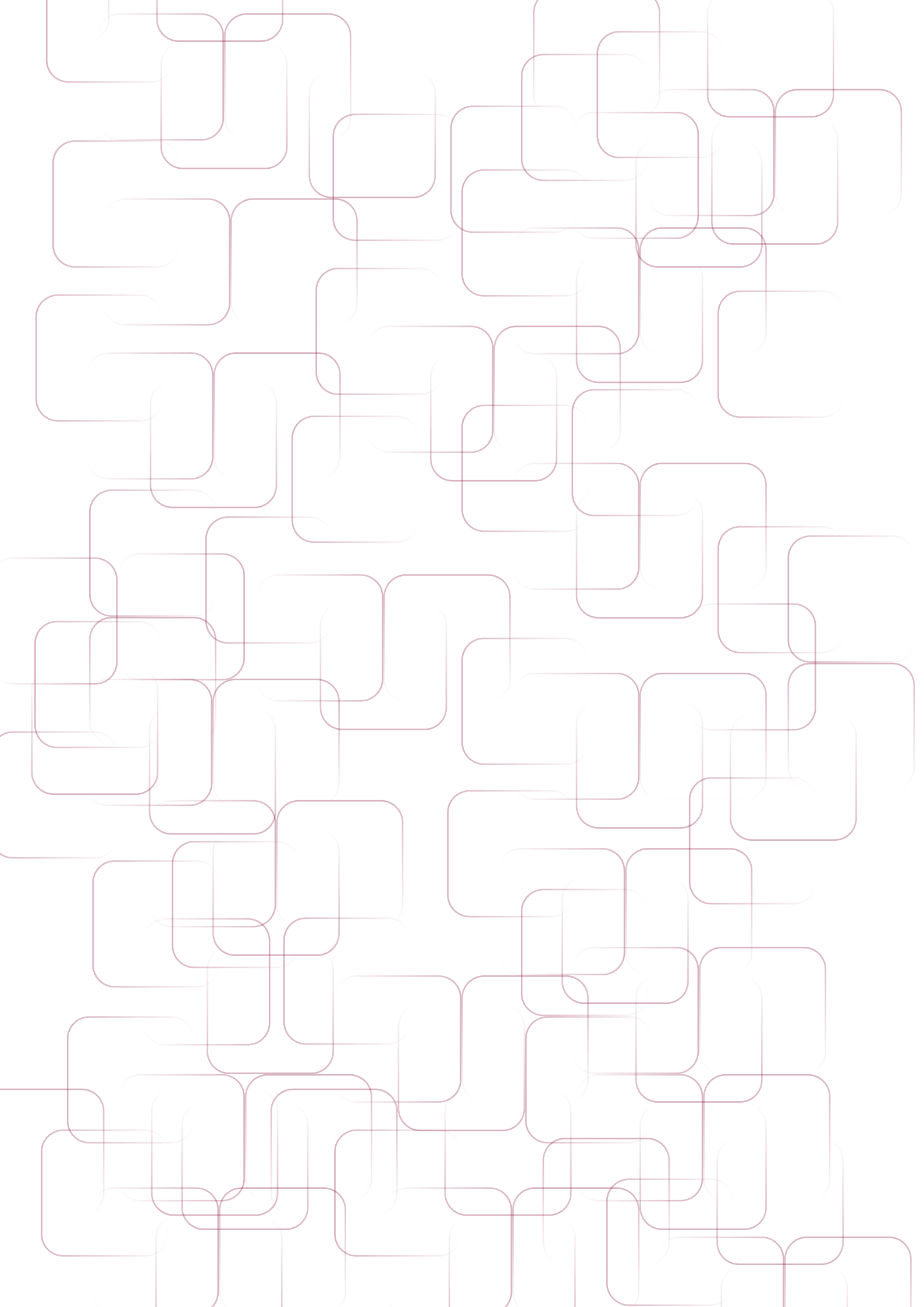
Bu ihtiyaç, dijital düzenlemeye ilişkin paradigmanın bütünüyle yeniden düşünülmesini gerektirmektedir. Bu yaklaşım, Kanun'un adının "Dijital Hizmetlerin ve Ortamların Düzenlenmesi Hakkında Kanun" olarak değiştirilmesi önerisinde somutlaşmaktadır. Mevcut başlık suç odaklı ve reaktif bir çerçeve sunarken, önerilen başlık yapay zekâ, algoritmik şeffaflık, dijital haklar

ve çocuk güvenliği gibi alanları kapsayan proaktif ve bütüncül bir düzenleme anlayışını yansıtmaktadır. Kanun'un dijital alandaki tüm süreçlerde istisnai değil, birincil düzenleme olması hedeflenmektedir.

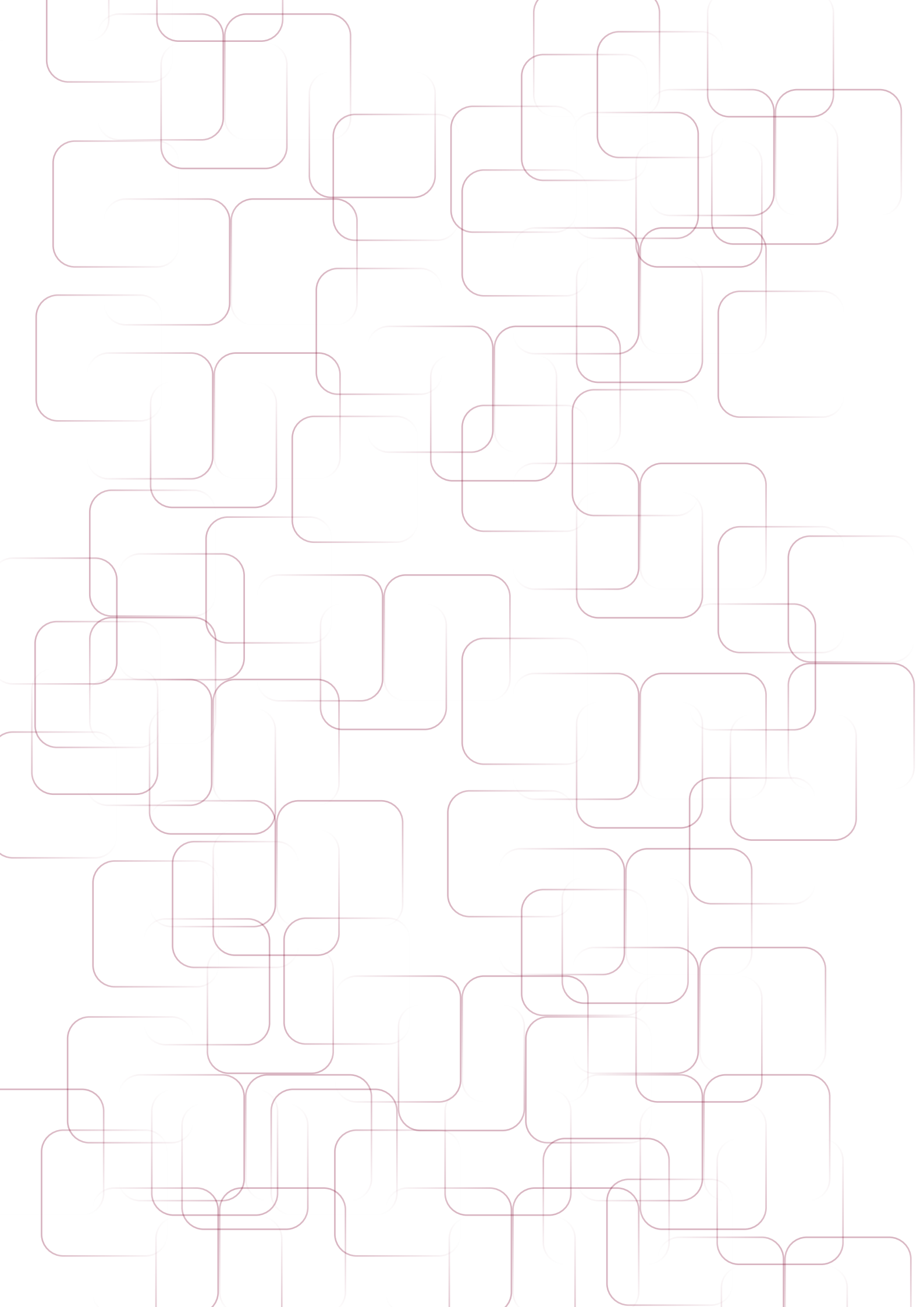
Dijital kullanımın yaygınlaşması, yapay zekâ, *deepfake*, algoritmik manipülasyon ve dezenformasyon gibi yeni riskler üretmiş; özellikle çocuklar açısından yeni kırılganlıklar yaratmıştır. Bu durum, mevcut İnternet Kanunu'nun günümüzün dijital gerçeklerine yanıt veremediğini ortaya koymaktadır.

Dijital düzenleme ihtiyacı üç temel eksen etrafında şekillenmektedir: (i) 5651 sayılı Kanun'un suç odaklı ve reaktif yapısından risk temelli ve önleyici bir modele geçiş, (ii) dijital platformların yükümlülüklerinin genişletilmesi ve (iii) çocukların dijital ortamda çok boyutlu korunması.

Sonuç olarak önerilen çerçeve, dijital ortamı daha güvenli, hesap verebilir ve adil kılarken, ifade özgürlüğünü, çocukların korunmasını ve kamusal çıkarı dengeli biçimde gözeten bütüncül bir düzenleyici modeli hedeflemektedir. Bu amaçla, Türkiye'nin dijital ekosistemine uygun yeni ve kapsamlı bir mevzuatın oluşturulması zorunludur.



5. POLİTİKA ÖNERİLERİ



POLİTİKA ÖNERİLERİ

5.1. Genel Öneriler

- Dijital suçların, çevrim içi istismarın, siber zorbalığın ve kişilik hakları ihlallerinin teknik niteliği gözetilerek hızlı, uzmanlaşmış ve tutarlı biçimde yargılanabilmesi için Bilişim İhtisas Mahkemeleri kurulmalıdır; bu mahkemeler dijital hukuk alanında özel eğitim almış hâkim ve savcılar ile teknik bilirkişi birimleri ile desteklenmelidir.
- Bilişim İhtisas Mahkemelerinin görev alanı; dijital ortamda işlenen suçlar, çevrim içi kişilik hakları ihlalleri, siber zorbalık davaları, dijital dolandırıcılık, çevrim içi telif ihlalleri ve platform sorumluluğu davaları gibi dijital ortamla ilişkili tüm yargılamaları kapsayacak şekilde belirlenmelidir.
- Dijital bağımlılık, siber zorbalık ve çocukların dijital ortamda korunmasına ilişkin dağınık yetkileri bütüncül biçimde yönetecek bir Dijital Güvenlik Koordinasyon Kurulu oluşturulmalı; kurul politika geliştirme, uygulama takibi ve kriz yönetimi işlevlerini birlikte yürütmelidir.
- Dijital Güvenlik Koordinasyon Kurulu, Bilgi Teknolojileri ve İletişim Kurumu Başkanlığı (BTK) uhdesinde; Aile ve Sosyal Hizmetler, Millî Eğitim, Sağlık ve İçişleri Bakanlıkları temsilcileri ile sivil toplum ve akademi temsilcilerinden oluşacak şekilde yapılandırılmalıdır.
- Dijital güvenlik, çocuk hakları ve medya okuryazarlığı alanlarında faaliyet gösteren sivil toplum kuruluşları ve düşünce kuruluşlarının politika yapım süreçlerine sistematik ve kurumsal katılımı sağlanarak ticari yapıların karşısında güçlü bir kamu-sivil toplum iş birliği oluşturulmalıdır.
- Düzenleyici kararlar alınmadan önce ilgili paydaşların görüşleri alınmalı ve bu görüşlerin nasıl değerlendirildiği karar gerekçelerinde açıkça gösterilmelidir.
- Bağımsız sivil toplum kuruluşlarının düzenli izleme ve değerlendirme raporları hazırlaması teşvik edilmeli ve bu raporlar politika geliştirme süreçlerinde dikkate alınmalıdır.
- Kanun'un adı, dijital düzenlemenin kapsamını ve proaktif yaklaşımını yansıtabilecek biçimde **"Dijital Hizmetlerin ve Ortamların Düzenlenmesi Hakkında Kanun"** olarak değiştirilmelidir.

5.2. Maddelere İlişkin Öneriler

Madde 1 (Amaç ve Kapsam)

- Kanun'un felsefesi "suçla mücadele" dar çerçevesinden çıkarılarak "dijital hizmetlerin bütüncül biçimde düzenlenmesi"ne genişletilmelidir.
- Kanun'un temel ilkeleri (dijital haklar, çocuğun gözetilmesi, kamu düzeni, algoritmik şeffaflık, risk temelli düzenleme, ifade özgürlüğü-güvenlik dengesi) açıkça yazılmalıdır.
- Kanun'da dijital haklar; çevrim içi mahremiyet, kişisel verilerin korunması, dijital kimlik güvenliği, algoritmik karar süreçlerinde şeffaflık talep etme ve dijital hizmetlere erişim hakkını kapsayacak şekilde tanımlanmalıdır.
- Dijital Dünyada Çocuk Hakları Sözleşmesi'nde temel bir ilke olarak benimsenen "çocuğun gözetilmesi", dijital ortamlara ilişkin tüm düzenlemelerin merkezine yerleştirilmelidir.

- Yapay zekâ ve algoritmik sistemlere karşı “şeffaflık” ilkesi Kanun’un kurucu unsuru hâline getirilmelidir.
- Alınacak tüm tedbirlerde ölçülülük ilkesi açık bir anayasal çerçeve olarak vurgulanmalı, temel hak ve özgürlükler güvence altına alınmalıdır.
- Dijital düzenlemede, ihlal gerçekleşikten sonra devreye giren reaktif yaptırımlardan ziyade, risklerin önceden tespit edilmesine ve zarar doğmadan engellenmesine dayanan risk temelli ve önleyici bir düzenleme yaklaşımı esas alınmalıdır.
- Dijital platformların yapılanmasından, algoritmik işleyişine ve içerik denetim süreçlerine kadar uzanan tüm aşamalarda, zarar doğmadan önce riski azaltmayı hedefleyen önleyici tedbirler hukuki bir yükümlülük hâline getirilmelidir.

Madde 2 (Tanımlar)

- Yapay zekâ ile üretilen içerik, *deepfake*, algoritmik yönlendirme ile çocuklara özgü dijital risk ve koruma alanları mevzuatta açık, işlevsel ve uygulanabilir biçimde tanımlanmalıdır.
- Tanımlar, farklı kurum ve mahkemelerde yeknesak uygulamayı mümkün kılacak biçimde uygulayıcılar için hukuki belirlilik sağlayan açık, net ve işlevsel hükümler hâlinde düzenlenmeli; aynı zamanda yükümlülük altındaki tüm aktörlerin hak, yetki ve sorumluluklarının kapsamını ortaya koyarak hukuki sınırları belirginleştirmelidir.

Madde 3 (Bilgilendirme ve Temsil Yükümlülüğü / Yaptırımlar)

- Sabit meblağlı cezalar yerine, büyük ölçekli platformlar için platformun ekonomik gücüyle orantılı, %1–%6 aralığında kademeli oranlara dayanan küresel ciro bazlı bir yaptırım sistemi benimsenmeli; küçük ölçekli sağlayıcılar bakımından ise güncellenmiş sabit meblağlı cezalar korunmalıdır.
- Platformlar, müşteri hizmetlerini bot hesaplarla sınırlı tutmamalıdır. Gerçek ve erişilebilir canlı destek (telefon, e-posta vb.) sunmakla yükümlü kılınmalı ve hak ihlallerine ilişkin başvuruların en geç 72 saat içinde değerlendirilmesi zorunlu olmalıdır.

Madde 4 (Algoritmik Benimseme ve Sorumluluk)

- İçerik sağlayıcı sorumluluğunu düzenleyen 4. maddede yer alan “içeriğin benimsenmesi” hâlinin kapsamı, platformun hangi koşullarda yayımlanan içeriği fiilen sahiplendiği kabul edileceğini gösterecek şekilde açık, objektif ve ölçülebilir kriterlerle tanımlanmalıdır; böylece platformların, algoritmik olarak öne çıkardıkları, teşvik ettikleri veya yayılımını güçlendirdikleri içerikten sorumlu tutulmaları sağlanmalıdır.
- Algoritmik benimseme hâlinde, platformlara içerik sağlayıcıyla birlikte müteselsil sorumluluk yüklenmelidir.
- Zarar gören kişilerin, kimliği belirsiz hesaplar yerine doğrudan ilgili platforma karşı hukuki yollara başvurabilmesi açıkça güvence altına alınmalıdır.
- Kullanıcıların kendilerine sunulan içeriklerin hangi algoritmik kriterlere göre seçildiğini anlayabilmeleri ve bu kararlara etkili biçimde itiraz edebilmeleri için algoritmik şeffaflık yükümlülüğü zorunlu kılınmalıdır.

Madde 6 (Erişim Sağlayıcılarının Yükümlülükleri)

- Çocuklar için varsayılan güvenli internet profili zorunlu hâle getirilmeli, “güvenli internet” uygulaması opsiyonel olmaktan çıkarılarak internetin korumalı şekilde sunulması esas kabul edilmeli, filtrelerin kaldırılması ancak bilinçli tercih üzerine mümkün olmalıdır.
- Erişim engelleme kararlarına ilişkin ayrıntılı şeffaflık raporları düzenli olarak yayımlanmalıdır. Bu raporlar, kararların gerekçelerini görünür kılarak hesap verebilirliği güçlendirecek ve kamuoyunun dijital riskleri daha iyi kavramasına katkı sağlayacaktır.

Madde 8 ve 8/A (İçerik Çıkarma ve Erişim Engelleme)

- Dijital içeriklere ilişkin karar süreçleri, dijital ortamın hızına uygun biçimde hızlandırılmalıdır. Viral içeriklerde hâlihazırda 48 saate varan sürenin uzunluğu dikkate alınarak acil geçici tedbir mekanizmaları oluşturulmalıdır. Alınan kararlara yönelik itirazların ise en geç 7 gün içinde sonuçlandırılması zorunlu kılınmalıdır.

Madde 9 (Kişilik Haklarının Korunması)

- Madde 9'un iptaliyle ortaya çıkan hukuki boşluk giderilmeli ve kişilik haklarının çevrim içi ortamda korunmasına ilişkin açık, işlevsel ve uygulanabilir bir düzenleme yeniden tesis edilmelidir.
- Kişilik hakları ihlallerine ilişkin uyuşmazlıklarda önce ilgili platforma başvuru, ardından yargı yoluna gidilmesi zorunlu kılınmalı ve platformların başvurulara en geç 24 saat içinde gerekçeli yanıt vermesi güvence altına alınmalıdır. Bu sistem platformları daha etkin sorumluluk almaya teşvik ederken gereksiz yargı yükünü azaltacaktır.

Madde 10 (Kurumun Görevleri)

- Bilgi Teknolojileri ve İletişim Kurumunun (BTK) görev alanı dijital ekosistemdeki gelişmelere paralel olarak genişletilmelidir. Yapay zekâ, dijital bağımlılık ve sivil toplum koordinasyonu açıkça kurumsal görevler arasına alınmalıdır. Kurumun dijital riskleri proaktif biçimde yönetmesi güvence altına alınmalıdır.

Ek Madde 4 (Temsilcilik ve Tüzel Kişilik)

- Mevcut temsilcilik sisteminin işlevsizliği nedeniyle model değişikliğine gidilmeli; büyük ölçekli platformların Türkiye’de tam yetkili ve tam sorumlu bir tüzel kişilik kurmaları zorunlu kılınmalıdır.

Önerilen Ek Madde 5 (VPN Düzenlemesi)

- VPN hizmetleri mevzuatta açık ve kapsamlı biçimde düzenlenmelidir. Güvenlik ve gizlilik gibi meşru kullanım amaçları korunurken yasa dışı içeriklere erişim ve siber suçlarda VPN kullanımının önüne geçecek mekanizmalar oluşturulmalı ve bu düzenleme Türkiye'nin dijital egemenliğini güçlendirecek şekilde tasarlanmalıdır.

Önerilen Ek Madde 6 (Çocukların Dijital Ortamda Korunması)

- Çocukların dijital ortamda korunması yalnızca cinsel istismar riskiyle sınırlandırılmamalı; kapsamlı ve çok boyutlu bir koruma yaklaşımı benimsenmelidir.
- Çocukların maruz kaldığı psikolojik, sosyal ve ekonomik nitelikteki dijital riskler de açıkça düzenleme kapsamına alınmalıdır.
- Çocukların verisi, özel nitelikli veri kapsamına alınmalıdır.
- Beyana dayalı yaş doğrulama uygulamaları terk edilmeli ve bunların yerine güvenilir, denetlenebilir teknik yaş doğrulama yöntemleri zorunlu kılınmalıdır; bu çerçevede 0–15 ve 15–18 yaş grupları gibi farklı yaş kategorileri için risk düzeyine göre kademelendirilmiş ve farklılaştırılmış koruma mekanizmaları oluşturulmalıdır.
- Dijital oyunlardaki bağımlılık riskleri ile *loot box* ve benzeri şans temelli mekanizmalar, çocukların korunmasını önceleyen özel düzenlemelere tabi tutulmalıdır.

Önerilen Ek Madde 7 (Bot Hesaplar)

- Platformlar, bot hesapları etkin biçimde tespit edecek teknik sistemleri kurmakla yükümlü kılınmalı; bot hesapların kamuoyu manipülasyonu, dezenformasyon ve seçim süreçlerine müdahale amacıyla kullanılmasının önüne geçecek önleyici mekanizmalar oluşturulmalıdır.
- Bot tespiti dijital kamusal alanın sağlığı açısından zorunlu kabul edilmeli; buna karşılık haber, hava durumu, kamu hizmetleri ve müşteri hizmetleri gibi meşru amaçlarla kullanılan otomatik hesapların faaliyetleri korunmalıdır.

Önerilen Ek Madde 8 (Güvenilir İşaretçi - *Trusted Flagger*)

- AB Dijital Hizmetler Yasası (DSA) modeline benzer bir “güvenilir işaretçi” sistemi kurulmalı; uzman sivil kuruluşların zararlı içeriklerin tespiti ve bildirimine katkısı kurumsal mekanizmalarla güçlendirilerek kamu–sivil toplum iş birliği sistematik hâle getirilmelidir.
- Güvenilir işaretçi sisteminin işleyişi ve etkisi, kötüye kullanım risklerini önleyecek şekilde düzenli olarak yıllık performans değerlendirmesine tabi tutulmalıdır.

Önerilen Ek Madde 9 (Sentetik İçerik - *Deepfake*)

- Yapay zekâ ile üretilen içerikler açık ve görünür biçimde işaretlenmeli; özellikle mahremiyet hakkına aykırı cinsel içerikli ve dolandırıcılık amaçlı *deepfake* içerikler açıkça yasaklanmalıdır.
- Sanat, eğitim ve haber amaçlı meşru kullanımlar için istisnalar öngörülürken, platformlar zararlı sentetik içerikleri tespit edebilecek etkili *deepfake* tespit sistemlerini kurmak ve işletmekle yükümlü kılınmalıdır.

Önerilen Ek Madde 10 (Şeffaflık ve Raporlama)

- Dijital platformların veri kullanımına ilişkin bilgi asimetrisi giderilmeli; platformlar yılda en az iki kez, sade ve anlaşılır dille yazılmış kapsamlı şeffaflık raporları yayımlamakla yükümlü kılınmalıdır.
- Bu raporlarda kişisel verilerin hangi amaçlarla işlendiği, hangi ülkelere aktarıldığı ve ticari algoritmaların genel işleyiş mantığı açıklanmalı; böylece vatandaşların ve ilgili kurumların verilerin yolculuğunu takip edebilmesi sağlanmalıdır.

Tablo 3. Politika Önerileri Kapsamında 5651 Sayılı Kanun'da Yapılması Teklif Edilen Değişikliklerle İlgili Karşılaştırmalı Tablo

MADDE 1 - AMAÇ VE KAPSAM	
MEVCUT DÜZENLEME	ÖNERİLEN DÜZENLEME
Amaç ve Kapsam MADDE 1- (1) Bu Kanunun amaç ve kapsamı; içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcıların yükümlülük ve sorumlulukları ile internet ortamında işlenen belirli suçlarla içerik, yer ve erişim sağlayıcıları üzerinden mücadeleye ilişkin esas ve usûlleri düzenlemektir.	Amaç ve Kapsam MADDE 1- (1) Bu Kanunun amacı; dijital ortamda sunulan hizmetlerin düzenlenmesi, içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı, sosyal ağ sağlayıcı ve toplu kullanım sağlayıcıların yükümlülük ve sorumlulukları ile dijital ortamda işlenen suçlara karşı etkili mücadele yöntemlerinin belirlenmesine ilişkin esas ve usulleri düzenlemektir. (2) Bu Kanunun temel ilkeleri şunlardır: a) Dijital hakların korunması ve kullanıcı güvenliği, b) Çocukların gözetilmesi ve dijital ortamlarda korunması, c) Kamu düzeni, halk sağlığı ve genel güvenlik, d) Algoritmik şeffaflık ve hesap verebilirlik, e) Proaktif önleme ve risk temelli düzenleme, f) İfade özgürlüğü ile güvenlik arasında adil denge, (3) Bu Kanun, dijital ortamın dinamik yapısını dikkate alarak önleyici ve denetleyici tedbirlerin alınmasını ve dijital ekosistemin sürdürülebilir ve güvenli gelişimini amaçlar. (4) Bu Kanun kapsamında alınacak tedbirlerde, temel hak ve özgürlüklerin korunması, demokratik toplum düzeninin gerekleri ve ölçülülük ilkesi gözetilir.

MADDE 2 - TANIMLAR

MEVCUT DÜZENLEME	ÖNERİLEN DÜZENLEME
(Mevcut tanımlar korunarak yeni bentler önerilmektedir.)	ş) Dijital istismar: Aileye, kırılgan bireylere ve çocuklara yönelik olarak dijital ortamda gerçekleştirilen cinsel, psikolojik, ekonomik veya sosyal nitelikteki her türlü istismar eylemlerini, t) Siber Zorbalık: Bilişim sistemleri ve dijital araçlar kullanılarak, bir birey veya gruba karşı sistematik, tekrarlayıcı ve kasıtlı şekilde gerçekleştirilen psikolojik, sosyal veya ekonomik zarar verme, korkutma, sindirme, itibar zedeleme, dışlama veya taciz etme amacı taşıyan her türlü eylemi, u) Algoritmik Şeffaflık: Dijital hizmet sağlayıcıların, kullanıcılara sundukları içeriğin sıralanması, öne çıkarılması, gizlenmesi veya tavsiye edilmesinde kullandıkları temel parametrelerin, karar mekanizmalarının ve önceliklendirme kriterlerinin açık, anlaşılır, erişilebilir ve denetlenebilir şekilde sunulmasını, ü) Bot Hesap: Bir gerçek kişi tarafından doğrudan ve anlık olarak yönetilmeyen; yazılım, yapay zekâ veya algoritmalar aracılığıyla otomatik veya yarı otomatik şekilde işlem yapan, içerik üreten, paylaşan veya etkileşimde bulunan sosyal ağ hesabını, v) Çocuk: On sekiz yaşını doldurmamış gerçek kişiyi, y) Dijital Bağımlılık: Dijital teknoloji, oyun veya çevrim içi platform kullanımının birey tarafından kontrol edilememesi, kullanımın diğer yaşam alanlarına öncelik kazanması ve ortaya çıkan fiziksel, psikolojik, sosyal ya da akademik/mesleki olumsuz sonuçlara rağmen sürdürülmesinin sonucu olarak işlevselliğe belirgin ve süreklilik gösteren bozulmayı, z) Sentetik İçerik: Yapay zeka, <i>deepfake</i> teknolojisi veya benzeri yöntemlerle üretilen, manipüle edilen veya değiştirilen ve gerçekmiş izlenimi veren ses, görüntü, video veya metinleri, aa) Varsayılan güvenlik (<i>privacy by design</i>): Dijital hizmetlerin tasarım aşamasından itibaren güvenlik ve gizlilik ilkelerinin merkeze alınmasını gerektiren yaklaşımı, bb) Büyük ölçekli platform: Türkiye’den aylık erişimi beş milyonu aşan sosyal ağ sağlayıcı veya yer sağlayıcıları, cc) Algoritmik benimseme: Sosyal ağ sağlayıcı veya yer sağlayıcının, algoritmik sistemler aracılığıyla belirli içerikleri öne çıkarması, görünür kılması, önerme listelerine dâhil etmesi veya yayılımını desteklemesi yoluyla içeriği sahiplenmesini, çç) Güvenilir işaretçi (<i>Trusted Flag</i>): Kurum (BTK) tarafından yetkilendirilen ve dijital güvenlik, çocuk hakları veya medya okuryazarlığı alanlarında uzmanlaşmış sivil toplum kuruluşları veya akademik kurumları, yetkilendirilen ve dijital güvenlik, çocuk hakları veya medya okuryazarlığı alanlarında uzmanlaşmış sivil toplum kuruluşları veya akademik kurumları,

MADDE 3 - BİLGİLENDİRME YÜKÜMLÜLÜĞÜ

MEVCUT DÜZENLEME	ÖNERİLEN DÜZENLEME
Bilgilendirme yükümlülüğü MADDE 3- (2) Yukarıdaki fıkarda belirtilen yükümlülüğü yerine getirmeyen içerik, yer veya erişim sağlayıcısına Başkan tarafından iki bin Türk lirasından elli bin Türk lirasına kadar idarî para cezası verilir.	Bilgilendirme yükümlülüğü MADDE 3- (2) Yukarıdaki fıkarda belirtilen yükümlülüğü yerine getirmeyen içerik, yer veya erişim sağlayıcısına Başkanlık tarafından idarî para cezası verilir. İdari para cezasının miktarı: a) Büyük ölçekli platformlar için: Bir önceki mali yıla ait küresel cirosunun yüzde birine kadar b) Diğer sağlayıcılar için: ... Türk lirasına kadar, olarak belirlenir. (6) Büyük ölçekli platformlar, kullanıcıların hak ihlallerine ilişkin başvurularını en geç yetmiş iki saat içinde değerlendirecek etkili mekanizmalar kurmak, 7/24 erişilebilir iletişim kanalları sağlamak ve şeffaf şikayet prosedürleri oluşturmakla yükümlüdür. Yükümlülükleri yerine getirmeyen büyük ölçekli platformlara, Başkanlık tarafından bir önceki takvim yılı küresel cirosunun yüzde biri ile yüzde beşine kadar idari para cezası verilir.

MADDE 4 - İÇERİK SAĞLAYICININ SORUMLULUĞU

MEVCUT DÜZENLEME

İçerik sağlayıcının sorumluluğu

MADDE 4- (2) İçerik sağlayıcı, bağlantı sağladığı başkasına ait içerikten sorumlu değildir. Ancak, sunuş biçiminden, bağlantı sağladığı içeriği benimsediği ve kullanıcının söz konusu içeriğe ulaşmasını amaçladığı açıkça belli ise genel hükümlere göre sorumludur.

ÖNERİLEN DÜZENLEME

İçerik ve Algoritmik Sorumluluk

MADDE 4- (2) İçerik sağlayıcı, bağlantı sağladığı başkasına ait içerikten sorumlu değildir. Ancak, sunuş biçiminden, bağlantı sağladığı içeriği benimsediği ve kullanıcının söz konusu içeriğe ulaşmasını amaçladığı açıkça belli ise genel hükümlere göre sorumludur.

(3) Sosyal ağ sağlayıcı veya yer sağlayıcı, algoritmik sistemler aracılığıyla başkasına ait içeriği öne çıkarması, öneri listelerine dâhil etmesi, görünürlüğünü artırması veya yayılımını desteklemesi hâlinde algoritmik benimseme gerçekleşmiş sayılır ve bu içerikten müteselsil olarak sorumlu tutulur.

(4) Üçüncü fıkra kapsamındaki sorumluluk, platformun algoritmik tercihlerinin kamuoyu oluşturma, toplumsal algıyı şekillendirme veya kullanıcı davranışlarını yönlendirme etkisi dikkate alınarak değerlendirilir.

(5) Algoritmik öneri ve sıralama sistemlerinin çalışma prensipleri, kullanılan parametreler ve karar mekanizmaları şeffaf, anlaşılır ve denetlenebilir biçimde kullanıcılara sunulmalıdır.

(6) Platformlar, algoritmik sistemlerinin zararlı içeriklerin yayılımını engellemek veya sınırlandırmak üzere proaktif tedbirler almakla yükümlüdür.

MADDE 6 - ERIŞİM SAĞLAYICININ YÜKÜMLÜLÜKLERİ

MEVCUT DÜZENLEME	ÖNERİLEN DÜZENLEME
Erişim sağlayıcının yükümlülükleri (Mevcut fıkralar korunarak yenileri önerilmektedir.)	Erişim Sağlayıcının Yükümlülükleri MADDE 6- (4) Erişim sağlayıcılar, çocukların internet kullanımına yönelik olarak aşağıdaki tedbirleri almakla yükümlüdür: a) On beş yaş altı çocuklar için varsayılan olarak güvenli internet profili sunmak, b) Yaş gruplarına göre farklılaştırılmış içerik filtreleme seçenekleri sağlamak, c) Ebeveyn denetim araçlarını ücretsiz ve erişilebilir kılmak, d) Çocuklara özgü siber güvenlik eğitim materyalleri sunmak. (5) Erişim sağlayıcılar, erişim engelleme kararlarına ilişkin olarak altı aylık dönemlerle şeffaflık raporu yayımlar. Bu raporlarda en az şu bilgiler yer alır: a) Hangi içeriklerin hangi gerekçelerle engellendiği (kategorik bazda), b) Toplam erişim engelleme kararı sayısı ve karar mercii, c) Kullanıcı itirazları ve sonuçları, d) Engelleme sürelerine ilişkin istatistikler. (6) Dördüncü ve beşinci fıkralardaki yükümlülükleri yerine getirmeyen erişim sağlayıcılara ... Türk lirasına kadar idari para cezası verilir.

MADDE 8 VE 8/A - İÇERİĞİN ÇIKARILMASI VE ERİŞİMİN ENGELLENMESİ
Yeni Fıkra Eklmeleri Önerisi

MEVCUT DÜZENLEME	ÖNERİLEN DÜZENLEME
Erişimin engellenmesi kararı... MADDE 8- (2) ...kararı, soruşturma evresinde hâkim, kovuşturma evresinde ise mahkeme tarafından verilir...	Erişimin Engellenmesi ve İhtisas Yargılaması MADDE 8- (2) Bu Kanun kapsamındaki suçlara, tedbirlere ve idari yaptırımlara ilişkin kararlar, Hâkimler ve Savcılar Kurulu tarafından belirlenen Bilişim İhtisas Mahkemeleri tarafından yirmi dört saat içerisinde verilir. İhtisas mahkemesi bulunmayan yerlerde, bu sıfatla görevlendirilen Sulh Ceza Hakimlikleri yetkilidir. (Ek Fıkra) İçerik çıkarma ve erişim engelleme kararlarına karşı yapılacak itirazlar, Bilişim İhtisas Mahkemeleri tarafından yedi gün içinde karara bağlanır. (Ek Fıkra) Acil hâllerde ve telafisi güç zararlara yol açacak durumlarda, mahkeme tarafından başvurudan itibaren dört saat içinde geçici tedbir kararı verilebilir. (Ek Cümle) Bilişim İhtisas Mahkemeleri, dijital suçlar, çevrim içi istismar, siber zorbalık, kişilik hakları ihlalleri ve dijital dolandırıcılık vakalarının teknik bilgiye sahip yargı mensupları tarafından ele alınmasını sağlamak üzere kurulur. İhtisas mahkemeleri, bünyelerinde bilişim uzmanı, pedagog ve psikologlardan oluşan teknik bilirkişi ofisleri bulundurur ve 7/24 nöbet esasına göre çalışır.
Gecikmesinde sakınca bulunan hâllerde... MADDE 8/A- (1) ...Başkan tarafından internet ortamında yer alan yayınlara ilgili olarak içeriğin çıkarılması ve/veya erişimin engellenmesi kararı verilebilir.	Hızlı Karar ve Güvenilir İhbarcı Mekanizması MADDE 8/A- (1) ...Başkanlık tarafından resen veya Kurumca (BTK) yetkilendirilmiş Güvenilir İşaretçi statüsündeki çocuk koruma kuruluşları, üniversiteler veya ilgili sivil toplum kuruluşlarının doğrulanmış bildirimleri üzerine, öncelikli inceleme yapılarak içeriğin çıkarılması ve/veya erişimin engellenmesi kararı verilebilir. (Ek Fıkra) Başkan, Kurumun yapay zekâ destekli otomatik içerik analiz sistemlerini kullanarak tespit ettiği, çocuk istismarı, yasa dışı bahis, yasaklı madde satışı ve terör propagandası içeren yayınlara, yargı kararı beklenmeksizin anlık erişim engelleme uygulama yetkisine sahiptir.

MADDE 9 - KİŞİLİK HAKLARININ KORUNMASI (YENİDEN DÜZENLENMESİ)

MEVCUT DURUM

Anayasa Mahkemesinin 11/10/2023 tarihli ve E.: 2020/76; K.: 2023/172 sayılı Kararı ile iptal edilmiştir.

İPTAL EDİLEN MADDE YERİNE ÖNERİLEN MADDE

1. İnternet ortamında yapılan yayın içeriği nedeniyle kişilik haklarının ihlal edildiğini iddia eden kişiler, içerik sağlayıcıya veya yer sağlayıcıya başvurarak içeriğin yayından çıkarılmasını veya düzeltilmesini talep edebilir.
2. Birinci fıkra kapsamındaki başvuruya yirmi dört saat içinde olumlu veya gerekçe göstererek olumsuz yanıt verilmesi zorunludur.
3. Başvuruya olumlu yanıt verilmemesi veya olumsuz yanıt verilmesi hâlinde, kişi Bilişim İhtisas Mahkemesine başvurabilir. Mahkeme, başvuruyu yedi gün içinde karara bağlar.
4. Acil hâllerde ve telafisi güç zararlara yol açacak durumlarda, mahkeme tarafından dört saat içinde geçici tedbir kararı verilebilir.
5. Mahkeme kararının gereğini yerine getirmeyen içerik veya yer sağlayıcılara, Başkanlık tarafından ... Türk lirasına kadar idari para cezası verilir. Büyük ölçekli platformlar için, küresel cirolarının yüzde biri ile **yüzde beşine kadar idari para cezası verilir.**

MADDE 10 - İDARİ YAPI VE GÖREVLER

ÖNERİLEN DÜZENLEME

YENİ BENT EKLEME ÖNERİSİ

(Ek Fıkra) (h) Yapay zekâ destekli içerik üretimi, sentetik medya ve *deepfake* teknolojilerinin tespiti ve düzenlenmesine yönelik çalışmalar yapmak; bu alanlarda standartlar belirlemek ve denetim mekanizmaları kurmak,

(Ek Fıkra) (ı) Dijital bağımlılık, siber zorbalık ve çocukların dijital korunması alanlarında kurumlar arası koordinasyonu sağlamak üzere özel kurullar oluşturmak,

(Ek Fıkra) (i) Güvenilir işaretçi sistemi kapsamında sivil toplum kuruluşlarını yetkilendirmek ve denetlemek,

(Ek Fıkra) (j) Dijital okuryazarlık ve bilinçli internet kullanımı konularında farkındalık çalışmaları yapmak ve desteklemek.

EK MADDE 4 - TEMSİLCİLİK VE TÜZEL KİŞİLİK YÜKÜMLÜLÜĞÜ

MEVCUT DÜZENLEME

Sosyal ağ sağlayıcı (Temsilci)

EK MADDE 4

(1)...yetkili en az bir kişiyi Türkiye’de temsilci olarak belirler... Temsilcinin gerçek kişi olması hâlinde bu kişinin Türkiye’de mukim ve Türk vatandaşı olması zorunludur.

ÖNERİLEN DÜZENLEME

Tam Yetkili Tüzel Kişilik ve Sorumluluk

EK MADDE 4

(1) Türkiye’den günlük erişimi bir milyondan fazla olan veya Türkiye’de aylık yüz bin kullanıcıya ulaşan yurt dışı kaynaklı sosyal ağ sağlayıcı ve büyük ölçekli yer sağlayıcılar:

- a) Türkiye’de yerleşik, tam yetkili ve tam sorumlu bir tüzel kişilik kurmak,
- b) Bu tüzel kişilik aracılığıyla hukuki, mali, teknik ve idari sorumlulukları üstlenmek,
- c) Tüzel kişiliğin yöneticilerinin Türkiye’de ikamet eden ve Türk vatandaşı olması veya Türkiye’de kalıcı oturma iznine sahip olması,
- d) Kullanıcı şikayetlerini değerlendirecek, yanıtlayacak ve çözüm üretecek Türkçe konuşan yeterli sayıda personel istihdam etmek ile yükümlüdür.

(2) Birinci fıkra kapsamındaki yükümlülüğü yerine getirmeyen platformlara uygulanan yaptırımlar şu şekilde kademeli olarak uygulanır:

- a) İlk bildirimden sonra otuz gün içinde yükümlülük yerine getirilmezse: ... Türk lirası idari para cezası,
- b) İkinci bildirimden sonra otuz gün içinde yükümlülük yerine getirilmezse: ... Türk lirası idari para cezası,
- c) İkinci cezadan sonra otuz gün içinde yükümlülük yerine getirilmezse: reklam yasağı,
- d) Reklam yasağından üç ay sonra: hâkim kararı ile internet trafiği bant genişliğinin yüzde elli daraltılması,
- e) Daraltmadan otuz gün sonra: hâkim kararı ile internet trafiği bant genişliğinin yüzde doksan daraltılması,

(3) Tüzel kişilik kurulan platformlar, Türk Ticaret Kanunu ve ilgili mevzuat hükümlerine tam olarak tabidir. Bu platformların Türkiye’deki tüzel kişilikleri, platformun tüm eylem ve işlemlerinden doğan hukuki ve mali sorumluluğu müteselsilen üstlenir.

(4) Kullanıcı sayısı eşğinin altında kalan ancak Türkiye’de milli güvenlik, ticari ya da sosyal alanlar gibi önemli alanlarda veri işleme ya da depolama faaliyet yürüten veya Türkiye pazarını hedefleyen platformlar için de Kurum (BTK) tarafından tüzel kişilik kurma yükümlülüğü getirilebilir.

ÖNERİLEN EK MADDE 5 - VPN HİZMETLERİNİN DÜZENLENMESİ**EK MADDE 5 - VPN hizmet sağlayıcıların lisanslanması ve denetimi**

(1) Türkiye’de VPN (*Virtual Private Network* - Sanal Özel Ağ) hizmeti sunan veya Türkiye kullanıcılarına yönelik VPN hizmeti sağlayan yerli ve yabancı tüm gerçek ve tüzel kişiler, Kurumdan (BTK) lisans almakla yükümlüdür.

(2) VPN hizmet sağlayıcıları:

- a) Hizmet sunduğu kullanıcılara ilişkin kayıt tutmak,
- b) Trafik bilgilerini bu Kanunun 6. maddesinde belirtilen sürelerde saklamak,
- c) Yetkili mercilerin talepleri doğrultusunda bilgi ve belge sunmak,
- d) Türkiye’de temsilcilik veya tüzel kişilik bulundurmak (aylık on bin veya daha fazla Türkiye kullanıcısı varsa) ile yükümlüdür.

(3) VPN hizmetlerinin meşru kullanım alanları korunur. İşletmeler, akademik kurumlar ve bireyler tarafından gizlilik, güvenlik ve kurumsal iletişim amaçlı VPN kullanımı serbesttir.

(4) Lisans almadan VPN hizmeti sunan sağlayıcılara erişim engellenir ve Başkanlık tarafından ... Türk lirasına kadar idari para cezası verilir.

(5) VPN hizmetlerinin yasa dışı içeriklere erişim, telif hakkı ihlali veya suç işleme amacıyla kullanılmasını kolaylaştırdığı tespit edilen durumlarda, Bilişim İhtisas Mahkemesi kararıyla ilgili VPN hizmetine erişim engellenebilir.

(6) VPN hizmet sağlayıcıların lisanslama, denetim ve yükümlülüklerine ilişkin usul ve esaslar Kurum (BTK) tarafından hazırlanan yönetmelikle düzenlenir.

ÖNERİLEN EK MADDE 6 - ÇOCUKLARIN DİJİTAL ORTAMLARDA KORUNMASI

MADDE 6/A - (1) Çocuklara yönelik dijital hizmet sunan platformlar, hizmetlerini tasarım aşamasından itibaren “varsayılan güvenlik” ilkesine uygun olarak geliştirmekle yükümlüdür. Çocuklar için özel koruma mekanizmaları ve sınırlandırılmış içerik erişimi zorunludur. Çocukların verisi özel nitelikli veri kapsamındadır.

(2) Yaş doğrulama:

- a) Platformlar, çocuk kullanıcılarını tespit etmek için beyana dayalı yöntemlerin ötesinde teknik ve algoritmik yaş doğrulama sistemleri kurmakla yükümlüdür.
- b) On beş yaşını doldurmamış çocuklar sosyal medya platformlarına üye olamaz ve erişemez.
- c) Yaş doğrulama süreçlerinde kişisel verilerin korunması ilkelerine uygun hareket edilir.

(3) Farklılaştırılmış koruma:

- a) On beş yaşını doldurmamış çocuklar güvenli olarak işaretlenmiş hizmetlere ve içeriklere erişebilir.
- b) On beş - on sekiz yaş arası çocuklar için ebeveyn denetim seçenekleri sunulur ve risk uyarı sistemleri ve internete güvenli etkileşim araçları sağlanır.

(4) Platformlar, çocuklara yönelik olarak:

- a) Kişiselleştirilmiş reklam gösteremez,
- b) Konum bilgisi toplayamaz (acil durum hizmetleri hariç),
- c) Davranışsal profillemeye yapamaz,
- d) Üçüncü taraflarla kişisel veri paylaşamaz.

(5) Dijital oyunlar, sosyal medya platformları ve video paylaşım siteleri, çocukların psikolojik, sosyal ve duygusal gelişim dinamiklerini dikkate alan içerik sınıflandırma, işaretleme ve filtreleme sistemleri kurmakla yükümlüdür.

(6) Dijital hizmetler, sosyal medya ve içerik platformları, oyunlar ve çocuklara mahsus sanal servisler çocukların erişimine sunulmadan önce güvenilir işaretçiler tarafından bağımsız değerlendirmeye tabi tutulur.

(7) Platformlar, çocuklara yönelik istismarı (cinsel, psikolojik, ekonomik, sosyal) tespit etmek için proaktif izleme sistemleri kurmakla ve tespit edilen vakaları derhal yetkili makamlara bildirmekle yükümlüdür.

(8) Siber zorbalık eylemlerinin tespiti ve önlenmesi için platformlar, kullanıcılara etkili bildirim mekanizmaları sunmak ve bildirilen içerikleri yirmi dört saat içinde değerlendirmekle yükümlüdür.

(9) Bu madde hükümlerine aykırı hareket eden platformlara, Başkanlık tarafından bir önceki takvim yılı Türkiye cirosunun yüzde ikisine kadar idari para cezası verilir.

ÖNERİLEN EK MADDE 7 - BOT HESAP VE OTOMATİK İÇERİK ÜRETİMİ

EK MADDE 7 - (1) Sosyal ağ sağlayıcılar ve yer sağlayıcılar, platformlarında bot hesapları tespit etmek, işaretlemek ve sınırlandırmak için etkili teknik ve algoritmik sistemler kurmakla yükümlüdür.

(2) Meşru amaçlarla kullanılan bot hesaplar açıkça bot olduğunu belirtmek ve kullanıcıları bu konuda bilgilendirmek zorundadır.

(3) Bot hesapların aşağıdaki faaliyetlerde bulunması yasaktır:

- a) Seçim ve referandum dönemlerinde karalama veya propaganda yapmak,
- b) Kamuoyunu yanıltıcı dezenformasyon yaymak,
- c) Sahte etkileşim (beğeni, yorum, paylaşım) üreterek içerik manipülasyonu yapmak,
- d) İçerik üreticileri ile koordineli biçimde kamuoyu algısını manipüle etmek,
- e) Kişi veya kurumları hedef alan kampanyaları yürütmek ya da destek olmak.

(4) Sosyal ağ sağlayıcılar:

- a) Bot hesap tespit ve temizleme faaliyetlerine ilişkin altı aylık raporlar yayımlar,
- b) Tespit edilen bot hesapları derhal askıya alır veya siler,
- c) Bot hesaplarla ilgili kullanıcı şikayetlerini en geç yetmiş iki saat içinde değerlendirir.

(5) Bu madde hükümlerine aykırı hareket eden platformlara, Başkanlık tarafından bir önceki takvim yılı küresel cirosunun binde beşinden yüzde ikisine kadar idari para cezası verilir.

(6) Bot hesap kullanarak üçüncü fıkrafta belirtilen yasaklanmış faaliyetlerde bulunan kişiler hakkında Cumhuriyet Başsavcılığına suç duyurusunda bulunulur.

ÖNERİLEN EK MADDE 8 - GÜVENİLİR İŞARETÇİ (TRUSTED FLAGGER) SİSTEMİ

EK MADDE 8 - (1) Kurum (BTK), dijital güvenlik, çocuk hakları, medya okuryazarlığı ve insan hakları alanlarında faaliyet gösteren sivil toplum kuruluşları, akademik kurumlar ve uzman kuruluşları “güvenilir işaretçi” statüsü vermeye yetkilidir.

(2) Güvenilir işaretçi statüsü verilen kuruluşlar:

- a) Hukuka aykırı içerikleri tespit edip işaretleme,
- b) İşaretlenen içeriklerin risk seviyesini belirleme,
- c) Platformlara ve Kuruma bildirimde bulunma,
- d) İçerik denetim süreçlerine danışmanlık sağlama, yetkilerine sahiptir.

(3) Güvenilir işaretçiler tarafından işaretlenen içerikler, Kurum ve platformlar tarafından öncelikli olarak değerlendirilir ve ilk incelemeye alınır.

(4) Güvenilir işaretçi olabilme kriterleri:

- a) En az üç yıldır ilgili alanda faaliyet gösteriyor olmak,
- b) Alan uzmanlığı, bağımsızlık ve tarafsızlık ilkelerine bağlı çalışmak,
- c) İçerik denetimi ve dijital hukuk konularında eğitimli personel istihdam etmek,
- d) Kurum tarafından belirlenen standartlara uymak.

(5) Güvenilir işaretçi statüsü, yıllık değerlendirmeye tabi tutulur. Yanlış işaretleme oranı yüksek olan veya kötü niyetli bildirimde bulunan kuruluşların statüsü iptal edilir.

(6) Platformlar, güvenilir işaretçilerden gelen bildirimlere dört saat içinde yanıt vermek ve gerekli tedbirleri almakla yükümlüdür.

(7) Güvenilir işaretçi sisteminin işleyişi, statü verme kriterleri ve değerlendirme süreçleri Kurum tarafından çıkarılacak yönetmelikle düzenlenir.

ÖNERİLEN EK MADDE 9 - SENTETİK İÇERİK VE DEEPFAKE DÜZENLEMESİ

EK MADDE 9 - (1) Yapay zekâ, *deepfake* teknolojisi veya benzeri yöntemlerle üretilen, manipüle edilen veya değiştirilen içerikler (sentetik içerik), bu nitelikleri açıkça belirtilmeksizin yayınlanamaz.

(2) Sentetik içerik üreticileri ve yayıncıları:

- a) İçeriğin sentetik olduğunu görsel veya işitsel bir uyarı ile belirtmek,
 - b) İçeriğin metadata bilgilerinde sentetik olduğunu işaretlemek,
 - c) Talep hâlinde içeriğin üretim yöntemi hakkında bilgi vermek,
- ile yükümlüdür.

(3) Aşağıdaki amaçlarla sentetik içerik üretilmesi ve yayılması yasaktır:

- a) Gerçek kişilerin rızası olmaksızın cinsel içerikli görüntü üretilmesi,
- b) Seçim dönemlerinde siyasi manipülasyon amacıyla kullanılması,
- c) Kişilik haklarının ihlali amacıyla kullanılması,
- d) Dolandırıcılık veya diğer suçların işlenmesi amacıyla kullanılması,
- e) Kamuoyunu yanıltıcı dezenformasyon yayılması.

(4) Platformlar, sentetik içerikleri tespit etmek için yapay zekâ tabanlı sistemler kurmak ve tespit edilen içerikleri işaretlemekle yükümlüdür.

(5) Bu madde hükümlerine aykırı hareket eden içerik sağlayıcılara, Başkanlık tarafından... Türk lirasına kadar idari para cezası verilir.

(6) Üçüncü fıkrafta belirtilen yasaklanmış amaçlarla sentetik içerik üreten veya yayan kişiler hakkında Cumhuriyet Başsavcılığına suç duyurusunda bulunulur.

(7) Sanat, eğitim ve haber amaçlı üretilen sentetik içerikler, bu amaçları açıkça belirtilmek ve işaretlenmek kaydıyla birinci ve ikinci fıkra yükümlülüklerinden muaf tutulabilir.

ÖNERİLEN EK MADDE 10 - DİJİTAL HİZMET SAĞLAYICILARININ ŞEFFAFLIK VE RAPORLAMA YÜKÜMLÜLÜĞÜ

EK MADDE 10 – (1) Türkiye'den günlük erişimi 100 binden fazla olan yurt içi veya yurt dışı kaynaklı sosyal ağ sağlayıcıları ile kullanıcı verisi işleyen diğer dijital hizmet sağlayıcıları; veri depolama mimarileri, veri işleme algoritmaları, kişisel verilerin anonimleştirilse dahi ticari amaçlarla kullanımı ve üçüncü taraflarla paylaşım metodlarına ilişkin şeffaflık raporunu her yılın ocak ve haziran aylarında olmak üzere altı ayda bir Kuruma bildirmek ve kendi internet sitelerinde kullanıcıların kolayca ulaşabileceği şekilde yayınlamakla yükümlüdür.

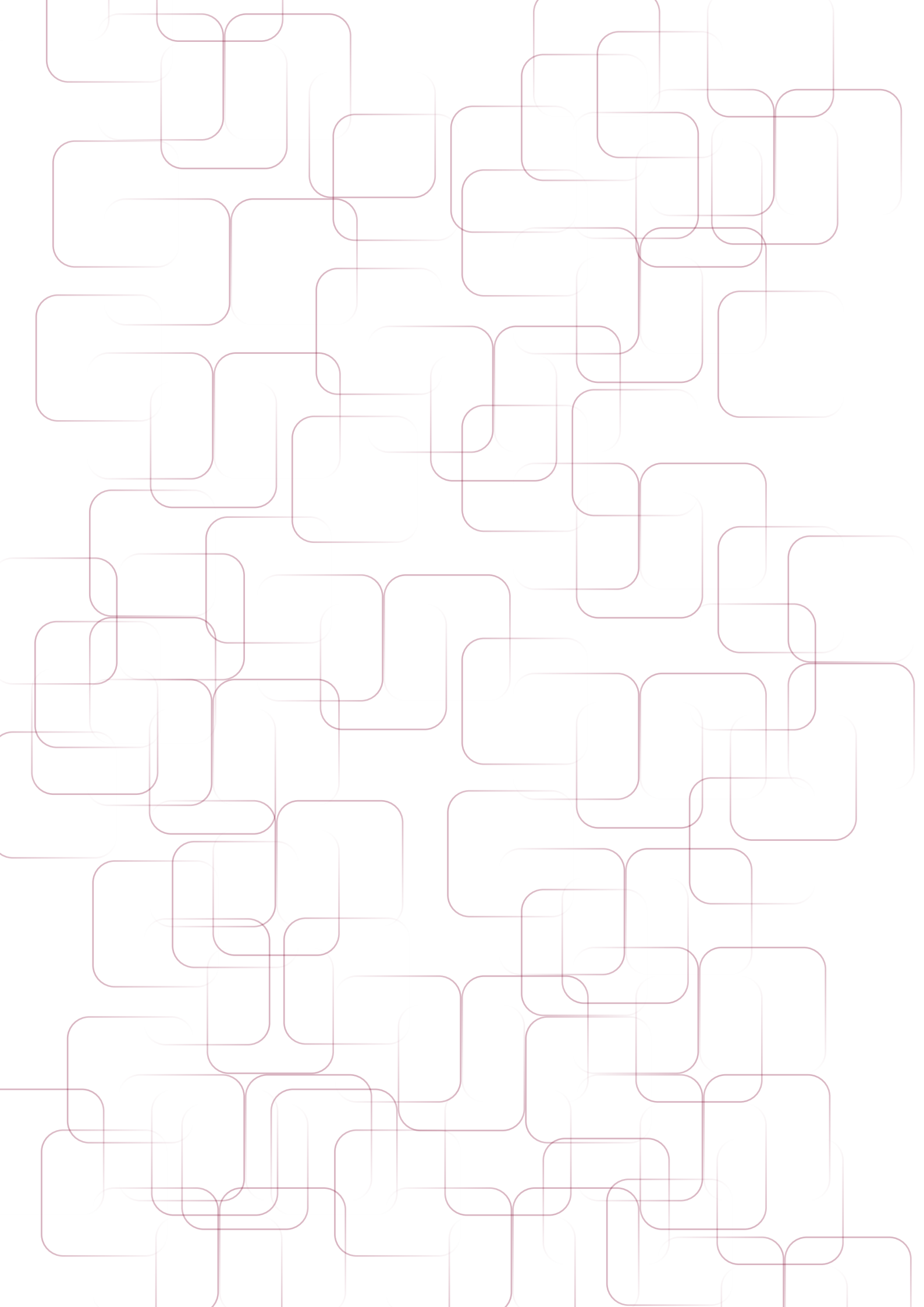
(2) Birinci fıkra uyarınca yayınlanacak olan raporda;

- a) Türkiye Cumhuriyeti vatandaşlarına ait verilerin hangi ülke veya ülkelerde depolandığı,
- b) Kullanıcı davranışlarını analiz etmek amacıyla kullanılan algoritmaların genel işleyiş prensipleri,
- c) Kişisel verilerin reklam hedeflemesi veya pazarlama stratejileri kapsamında nasıl ticari bir değere dönüştürüldüğü,
- ç) Kullanıcı sözleşmelerinde yer alan hükümlerin pratikteki uygulama metotları, hakkında, teknik terimlerden arındırılmış, açık, anlaşılır ve bilgi asimetrisini ortadan kaldırmaya elverişli Türkçe bilgilendirmelere yer verilmesi zorunludur. Bu raporun asgari standartları ve formatı Kurum tarafından belirlenir.

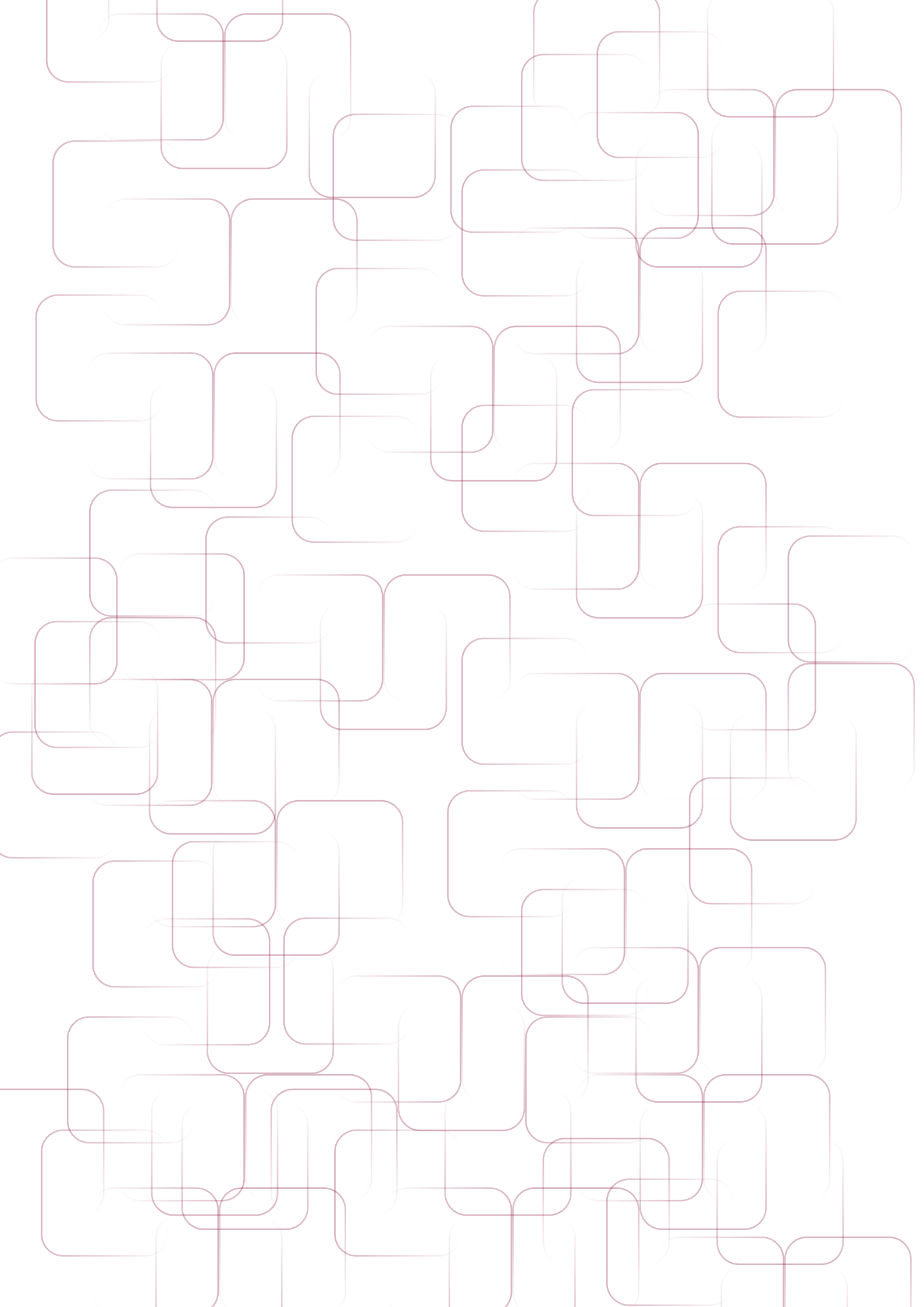
(3) Bu madde kapsamındaki raporlama yükümlülüğü, 6698 sayılı Kişisel Verilerin Korunması Kanunu uyarınca doğan yükümlülükleri ortadan kaldırmaz.

(4) Birinci ve ikinci fıkradaki yükümlülüklerini yerine getirmeyen dijital hizmet sağlayıcılarına Kurum Başkanı tarafından ihtarla bulunulur. İhtara rağmen otuz gün içinde raporlama yükümlülüğünü yerine getirmeyen sağlayıcıya ... Türk lirasına kadar idari para cezası verilir.

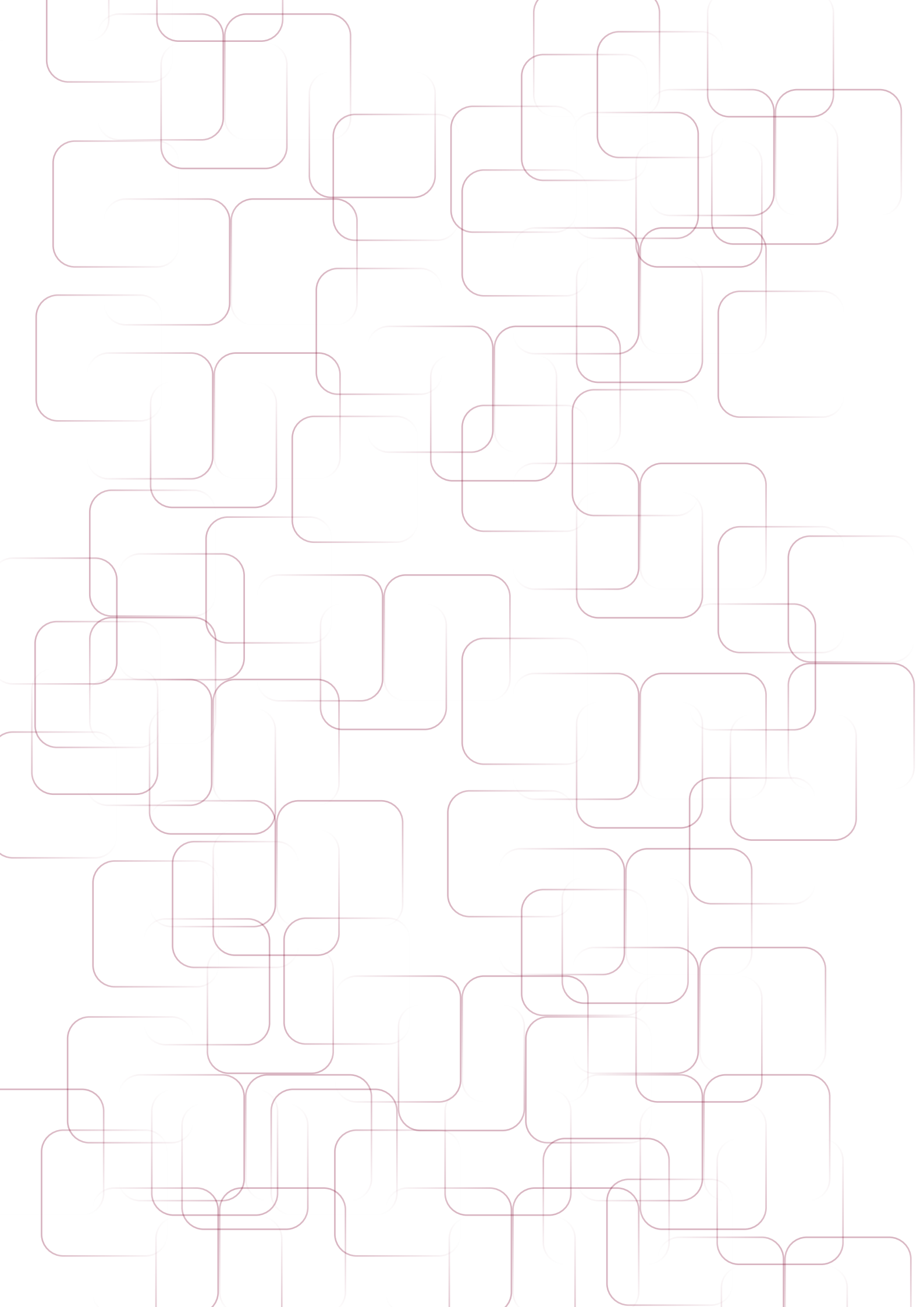
(5) İdari para cezasının tebliğinden itibaren otuz gün içinde yükümlülüğün yerine getirilmemesi hâlinde, Kurum Başkanı tarafından ilgili hizmet sağlayıcının internet trafiği bant genişliğinin **yüzde elli oranında** daraltılması için Sulh Ceza Hakimliğine başvurulur. Hakim kararının uygulanmasından itibaren otuz gün içinde yükümlülüğün yerine getirilmemesi hâlinde, bant genişliğinin **yüzde doksan oranında** daraltılması için Sulh Ceza Hakimliğine başvurulur.



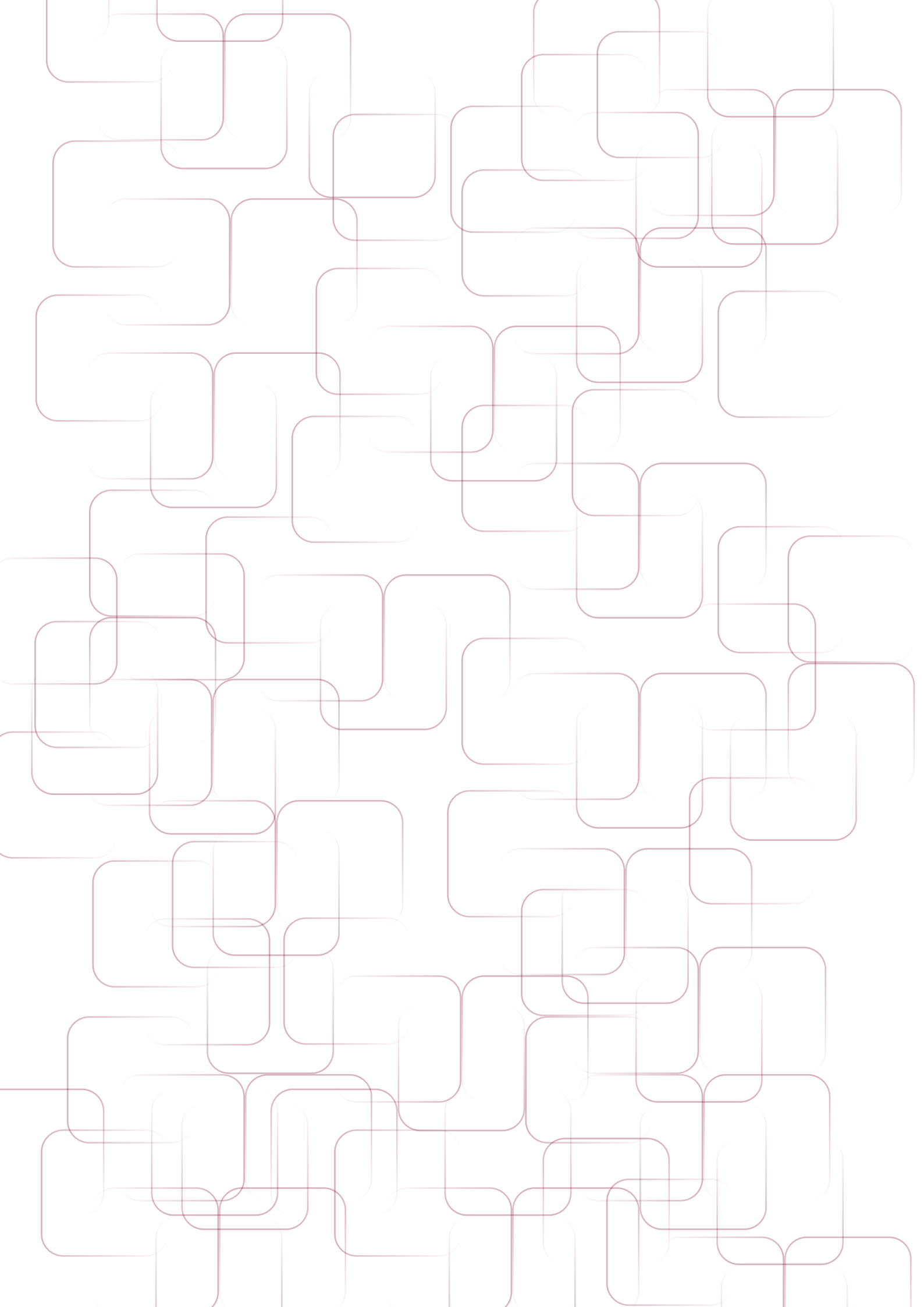
KAYNAKÇA



- Adalet Bakanlığı. (2025). *Adalet İstatistikleri 2024*. https://adlisicil.adalet.gov.tr/Resimler/SayfaDokuman/7042025092455Adalet_%C4%B0statistikleri_2024%20T%C3%BCrk%C3%A7e_Ingilizce.pdf
- Cadwalladr, C., & Graham-Harrison, E. (2018). *How Cambridge Analytica turned Facebook 'likes' into a lucrative political tool*. *The Guardian*. <https://www.theguardian.com/technology/2018/mar/17/facebook-cambridge-analytica-kogan-data-algorithm>
- Enstitü Sosyal. (2025a). *Dijital Dünyada Çocuk Hakları Sözleşmesi*. <https://enstitusosyal.org/imza>
- Enstitü Sosyal. (2025b). *Dijital Çağda Ailenin Dönüşümü: Yeni Nesil Bağlar ve Dinamikler*. <https://enstitusosyal.org/yayinlarimiz/arastirma-raporlari/dijital-cagda-ailenin-donusumu-yeni-nesil-baglar-ve-dinamikler>
- Enstitü Sosyal. (2025c). *Türkiye'de Dijital Kumar: Görünüm, Dinamikler ve Mücadele Stratejileri*. <https://enstitusosyal.org/yayinlarimiz/arastirma-raporlari/turkiye-de-dijital-kumar-gorunum-dinamikler-ve-mucadele-stratejileri>
- Federal Trade Commission. (2019). *FTC imposes \$5 billion penalty and sweeping new privacy restrictions on Facebook*. <https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook>
- Kaya, M. B. (2022). *Bilişim Suç İstatistikleri ve Türkiye'de Siber Güvenlik*. <https://mbkaya.com/bilisim-suc-istatistik-turkiye-siber-guvenlik/>
- Kosinski, M., Stillwell, D., & Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences of the United States of America*, 110(15), 5802–5805. <https://doi.org/10.1073/pnas.1218772110>
- United Kingdom Parliament. (2019). *Disinformation and "fake news": Final report* (HC 1791-I). <https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/179106.htm>



YAZARLAR HAKKINDA



YAZARLAR HAKKINDA

Muhammet Talha Kaan

Muhammet Talha Kaan, 2017 yılında Fatih Sultan Mehmet Vakıf Üniversitesi Hukuk Fakültesinden, 2018 yılında Anadolu Üniversitesi İktisat Fakültesinden mezun olmuştur. İbn Haldun Üniversitesi Uluslararası ve Mukayeseli Hukuk Programını "Hukuki Boyutuyla Slot Uygulamaları" başlıklı teziyle 2020 yılında tamamlamıştır. Hâlen Marmara Üniversitesi Kamu Hukuku Bölümünde doktora çalışmalarına devam etmektedir. 2021 yılından itibaren İbn Haldun Üniversitesi Hukuk Fakültesi İdare Hukuku Anabilim Dalında araştırma görevlisi olarak görev yapmaktadır. İdare hukuku, hava ve uzay hukuku, yapay zekâ hukuku ve bilişim hukuku ilgi alanları arasında yer almaktadır.

Fatma Betül Ercan

Boğaziçi Üniversitesi Psikoloji Bölümünde lisans eğitimini tamamlayan Fatma Betül Ercan, İstanbul Medipol Üniversitesinde nörobilim alanında yüksek lisans yapmıştır. Çeşitli sivil toplum kuruluşlarında psikososyal destek ve bağımlılıkla mücadele üzerine projelerde proje yöneticisi ve psikolog olarak görev almıştır. Hafıza, mikrobiyota ve Alzheimer konularında bilimsel çalışmaları vardır. Hâlen İstanbul Medipol Üniversitesinde nörobilim doktorasına devam etmektedir. Enstitü Sosyalde eğitim araştırmacısı olarak görev yapmaktadır.

