



TÜRKİYE BİLİŞİM DERNEĞİ İCRA KURULU

DİJİTAL EGEMENLİK VE DİJİTAL GÜVENLİĞE DOĞRU TÜRKİYE İÇİN YOL HARİTASI

Temmuz 2026

**TÜRKİYE BİLİŞİM DERNEĞİ
İCRA KURULU
DİJİTAL EGEMENLİK VE DİJİTAL
GÜVENLİĞE DOĞRU
TÜRKİYE İÇİN YOL HARİTASI**



Temmuz 2026

YAYIN NO: 2026/07-1 2025-2027 İcra Kurulu – • Dijital ve Çevrim içi Platformlar: Dijital Dönüşüm ve Dijitalleşme Süreçleri Çalışma Grubu Raporu

Rapor içeriği Çalışma Grubu içinde yapılan çalışmalar ve araştırmalarından oluşturulmuştur.
Bu yayın 0050 adet basılmıştır.

Rapora Katkı Verenler ve Çalışma Grubu Üyeleri

Dijital ve Çevrim İçi Platformlar Çalışma Grubu çalışmalarına, sivil toplum kuruluşlarının temsilcileri ile kamu ve özel sektör temsilcileri katkı vermişlerdir. Bu raporun içeriğinde ve hazırlanmasında katkılarını sunan katılımcılar aşağıda yer almaktadır.

Çalışma Grubunun oluşumuna imkân ve olanak sağlayan saygıdeğer TBD İcra Kurulu Başkanı **Abdullah Raşit Gülhan** ve Yardımcısı **Ahmet Pekel** Beyefendilere teşekkür ederiz.

Abdullah Raşit Gülhan - TBD İcra Kurulu Başkanı

Ahmet Pekel - TBD İcra Kurulu Başkan Yardımcısı

Murat Özkarabekir - TBD İcra Kurulu Üyesi ve Çalışma Grubu Koordinatörü

Rapora Katkı Sunan Yazar ve Editörler (Soyadına göre sıralanmıştır)

Raporun oluşmasında araştırmaları ve yazıları ile önemli katkılar sağlayan yazar ve editörler;

Rifat Bayathoğlu (Genel editör ve danışman, tüketici odaklı regülasyon ve mevzuat)

Av. Halil Murat Berberer (Hukuksal danışman, regülasyonlar ve mevzuat)

Vehbi Çelikbaş (Platform ekonomileri ve mevzuat ile global uyum analizi)

Dr. Merve Ayyüce Kızrak (Yapay Zekâ ve Algoritmalar uzmanı, genel danışman)

Murat Özkarabekir (Rapor Genel Yazar ve Koordinatörü)

Haluk Hasan Şendoğdu (Şeffaflık, raporlama, hesap verilebilirlik, denetim, yaptırımlar)

Kerem Yazıcı (Yapay Zekâ ve Dijital Platformlar yorum ve öneriler)

Diğer Çalışma Grubu Üyeleri (Soyadına göre sıralanmıştır)

TBD yöneticileri, bölüm yazarlar ve editörler dışında çalışmalara katkı veren, görüş ve önerilerini paylaşan diğer çalışma grubu üyeleri aşağıda yer almaktadır.

Gonca Elibol (Editorial ve kamusal bakış ve öneriler)

Demet Türdü (Dijital dönüşüm odaklı görüş ve öneriler)

Berkay Yücel (YZ uzmanı, Analiz raporu: Algoritmik sistemler ve global düzenlemeler)

İÇİNDEKİLER

Rapora Katkı Verenler ve Çalışma Grubu Üyeleri	iv
İÇİNDEKİLER	v
SUNUŞ	xii
TEŞEKKÜR	xiii
ÖNSÖZ	xvii
BÖLÜM 1: TANIMLAR VE KAVRAMSAL ÇERÇEVE	1
1.1. Dijital, Çevrim İçi ve Sosyal Medya	3
1.2. Platform ve Servis Tipolojileri (Sınıflandırmaları)	4
1.3. Platformlaşma ve Ekosistemin Yapısal Dinamikleri	5
1.4. Platform Gücü ve Politik Ekonomi: Yapısal Riskler	6
1.5. Uluslararası Tanımlardan Seçkiler	7
1.6. Dijital Platformların Akademik ve Fonksiyonel Tanımı	11
BÖLÜM 2: ŞEFFAFLIK VE RAPORLAMA	14
2.1. Dijital Platformlarda Yeni Güven Mimarisi ve Türkiye Perspektifi	15
2.2. Genel Tanımlar	18
2.2.1. Arama Motorları	18
2.2.2. Sosyal Ağlar	22
2.2.3. E-Ticaret	24
2.3. Şeffaflık (Algoritmik Öngörülebilirlik, Bilgilendirme ve Güven İnşası)	26
2.3.1. Arama Motorları: İndeksleme, Otorite ve Bilgiye Erişim	28
2.3.2. Sosyal Ağlar: Etkileşim Ekonomisi ve Psikolojik Etkiler	29
2.3.3. E-Ticaret Platformları: Fiyatlandırma ve Güvenli Ticaret	30
2.4. Reklam ve Gelir Modellerinin Beyanı	30
2.4.1. Gelir Kaynakları ve Veri İlişkisi	31
2.4.2. Politik ve Kamusal Reklam Arşivleri: Demokratik Denetim	31
2.4.3. Dezenformasyonla Mücadele ve Finansal Şeffaflık	32

2.5. Raporlama (Operasyonel Veri Setleri, İstatistiksel Beyan ve Denetlenebilirlik)	33
2.5.1. İçerik Moderasyonu ve Operasyonel Raporlama	34
2.5.2. Şikâyet ve İtiraz Mekanizmalarının Raporlanması	35
2.5.3. Reklam Arşivi ve Ekonomik Veri Raporlaması	36
2.5.4. Raporlama Standartları ve Veri Kalitesi (Standardization)	36
2.5.5. Operasyonel Şeffaflıktan Sayısal Hesap Verebilirliğe	38
2.6. Hesap Verebilirlik (Risk Yönetimi, Bağımsız Denetim ve Kurumsal Sorumluluk)	39
2.6.1. Risk Temelli Öz-Değerlendirme (Self-Assessment), Önleyici Hesap Verebilirlik	40
2.6.2. Bağımsız Denetim (Independent Auditing) ve Dış Gözetim	41
2.6.3. E-Ticaret ve Sosyal Ağlarda Spesifik Hesap Verebilirlik Modelleri	41
2.6.4. Kurumsal Hesap Verebilirlik Yapısı: Uyum Görevlileri ve Regülatif İletişim	42
2.6.5. Sorumluluk Rejimi ve Denetlenebilir Platform Ekosistemi	44
2.7. Türkiye Perspektifinde Şeffaflık, Raporlama ve Hesap Verebilirlik	45
2.7.1. Türkiye’de Şeffaflık: Algoritmalar ve Reklam Modelleri	46
2.7.2. Raporlama Yükümlülükleri: Sayısal Veriler ve Yerellik	46
2.7.3. Hesap Verebilirlik: Temsilcilikten Denetlenebilirliğe	47
2.7.4. Tartışma: Harmonizasyon ve Gelecek Projeksiyonu	47
BÖLÜM 3: İÇERİK YÖNETİŞİMİ VE KULLANICI KORUNMASI	49
3.1. Dijital Platformlar Mevzuat Reformu ve Küresel Uyum Stratejisi	50
3.2. Neden Bu Reform Gerekli?	51
3.3. Vizyon ve Stratejik Çerçeve	52
3.4. Temel Reform Alanları ve Küresel Referanslar	53
3.4.1. Bildir-ve-Aksiyon (Notice-and-Action) Reformu	54
3.4.2. Stratejik Öneri: Standart Dijital Bildirim Protokolü	55
3.4.3. Güvenilir Bildirici (Trusted Flaggers)	56
3.4.4. Gerekçeli Karar ve Şeffaflık	58
3.5. Kullanıcı Hakları ve Şikâyet Yönetimi	60
3.5.1. Mahkeme Dışı Çözüm	61
3.5.2. Dijital Uyuşmazlık Yönetimi ve Yetkilendirme Mekanizması	61

3.6. Karanlık Tasarım (Dark Patterns) ve Erişilebilirlik	62
3.7. AB-CSAM Işığında Türkiye’de Çocuk Koruma Mekanizmaları	64
3.8. Seçim Dürüstlüğü ve Reklam Şeffaflığı:	66
3.9. Bağımsız Denetim ve Yeni Yönetişim Modeli	68
3.9.1. Bağımsız Dijital Hizmetler Koordinatörü:	69
3.9.2. Birlikte Düzenleme (Co-Regulation):	69
3.9.3. Asimetrik Regülasyon ve Kademeli Sorumluluk Modeli:	70
3.10. Stratejik Sonuç: Küresel Rekabetçilik ve Uyum	70
BÖLÜM 4: DİJİTAL PLATFORM EKONOMİSİNDE REKLAM, GELİR, P2B VE ŞEFFAFLIK	72
4.1. Dijital Platform Ekonomisi: Stratejik Mimari ve Gelir Modelleri	73
4.1.1. Ekosistemin Yapısı ve Değer Zinciri	74
4.1.2. Gelir Modelleri, Yapısal Riskler ve Politika Tasarımı	77
4.1.3. Türkiye’de Yapısal Görünüm ve Risk Analizi	79
4.1.4. Stratejik Politika Önerileri ve KPI Mekanizması	79
4.2. Hedefli Reklamcılık ve Profilleme: Veri Yönetişi ve Koruma	80
4.2.1. Kavramsal ve Teknik Altyapı	82
4.2.2. AB Karşılaştırmalı Düzenleme Tablosu	82
4.2.3. Risk Odaklı Politika Tasarımı	83
4.2.4. İzleme ve KPI Mekanizması	84
4.3. Manipülatif Tasarım Kalıpları (Dark Patterns) ve Dijital Adalet	84
4.3.1. Kavramsal Tanımlama ve Uygulama Biçimleri	85
4.3.2. Dinamik Fiyatlandırma ve Algoritmik Gizli Anlaşmalar (Collusion)	86
4.3.3. Düzenleyici Çerçeve: AB ve Türkiye Karşılaştırması	87
4.4. Gelir Modelleri ve Platform Ekonomisi	88
4.4.1. Politika Önerileri, KPI ve İzleme	89
4.5. Tüketicilere Sunulan Ticari Bilginin Şeffaflığı	89
4.5.1. E-Ticaret, P2B İlişkileri ve Self-Preferencing (Kendine Öncelik)	90
4.5.2. Self-Preferencing ve DMA Yaklaşımı	91
4.6. Platform Yönetişiminin Politik Ekonomisi: Jeopolitik Dinamikler ve Güç Dengesi	92

4.7. Bütünleşik Denetim, Yaptırımlar ve Politika Önerileri	94
BÖLÜM 5: YAPAY ZEKÂ VE ALGORİTMİK SİSTEMLER	95
5.1. Özet	96
5.2. Kavramsal Temeller: Platformlarda Algoritmik Sistemler Ne Anlama Gelir?	98
5.3. Platform YZ Sistemlerinde Temel Risk Alanları	99
5.4. Yönetişim Boyutları ve Uluslararası Çerçeveler	102
5.5. Kurumsal ve Örgütsel Sorumluluklar	104
5.6. Politika ve Düzenleme Değerlendirmeleri	105
5.7. İyi Uygulama Örnekleri ve Öneriler	107
5.8. Öncelikli öneriler	108
BÖLÜM 6: SİBER GÜVENLİK VE SİBER (Operasyonel) DAYANIKLILIK	112
6.1. Giriş ve Amaç	113
6.2. Koordine Yapay Davranışlar ve Platform Bütünlüğü	114
6.3. Operasyonel (Siber) Dayanıklılık ve Olaylara Müdahale	117
6.3.1. Asgari Teknik Standartlar ve DORA Uyumu	118
6.3.2. Yedeklilik ve Afet Yönetimi (DR)	119
6.4. Stratejik Analiz ve Yeni Nesil Siber Güvenlik Yol Haritası	120
6.4.1. Algoritmik Hesap Verilebilirlik ve Sistemik Risk	121
6.4.2. Koordine Yapay Davranışlar (CIB) ve Bilgi Bütünlüğü	121
6.4.3. Operasyonel Dayanıklılık ve Kritik Hizmet Standartları	121
6.4.4. Dijital Egemenlik ve Bulut Jeopolitiği	122
6.4.5. Şeffaflık, Etik Tasarım ve Bağımsız Denetim	122
BÖLÜM 7: DENETİM, YAPTIRIMLAR VE HUKUKİ ÇÖZÜM MEKANİZMALARI	126
7.1. Giriş	127
7.1.1. Kapsam ve Metodoloji: Platform Ekonomisinde Regülasyonun Evrimi	128
7.2. Stratejik Paydaş Analizi ve Perspektifler	129
7.2.1. Hizmet Sağlayıcılar: Uyum Maliyetleri ve Operasyonel Öngörülebilirlik	129
7.2.2. Hizmet Alanlar (Kullanıcılar): Hak Arama Yolları ve Dijital Esenlik	130
7.2.3. Ekonomi ve Rekabet: Yarışılabilirlik (Contestability) ve İnovasyon	130

7.2.4 Hukuk ve Güvenlik: Siber Dayanıklılık ve Algoritmik Hesap Verebilirlik	131
7.3. Yetkili Denetim Otoritesi: Kurumsal Yapı ve Yetkiler	131
7.3.1. Otorite Bağımsızlığı ve Veri Odaklı Denetim	132
7.3.2. Kurumlar Arası Eşgüdüm Modelleri	132
7.4. Uluslararası Mevzuat Analizi ve Karşılaştırmalı Hukuk	134
7.4.1. Avrupa Birliği Dijital Müktesebatı: Çok Katmanlı Denetim Mimarisi	134
7.4.2. Birleşik Krallık (İngiltere) Yaklaşımı: Online Safety Act (OSA)	136
7.4.3. Kanada Modeli: Bill C-27 ve Dijital Şart (Digital Charter)	136
7.4.4. OECD Bakış Açısı	136
7.4.5. Karşılaştırmalı Analiz ve Akademik Perspektifler	137
7.5. Platform Özelinde Uygulama Stratejileri	138
7.5.1. Arama Motorları: Algoritmik Tarafsızlık ve Veri İndeksleme Denetimi	138
7.5.2. Sosyal Ağlar: Algoritmik Kürasyon, Dezenformasyon ve Çocuk Koruma	139
7.5.3. E-Ticaret Platformları: Veri Çifte Rolü ve Hibrit Pazar Yönetimi	140
7.5.4. Denetim Stratejileri ve Teknik Uygulama	142
7.6. Yaptırım Rejimi ve Caydırıcılık: Etkin Uygulama Mekanizmaları	143
7.6.1. Kademeli Para Cezaları ve Ekonomik Caydırıcılık Teorisi	143
7.6.2. Davranışsal Tedbirler: Süreç ve Tasarım Odaklı Müdahaleler	144
7.6.3. Yapısal Tedbirler	144
7.7. Hukuki Çözüm Mekanizmaları	145
7.7.1. İdari İtiraz Yolları ve Yargısal Denetim (Judicial Review)	146
7.7.2. Alternatif Uyuşmazlık Çözüm (Alternative Dispute Resolution) Yolları	146
7.7.3. Kolektif Hak Arama (Sınıf Davaları) ve Tazminat Hakları	147
7.7.4. Algoritmik Kararlara Karşı "İnsan Müdahalesi" ve İtiraz Hakkı	148
7.8. Türkiye İçin Geleceğe Hazır Regülasyon Tasarımı	149
7.8.1. Kurumsal Mimari Önerisi: "Dijital Ekosistem Düzenleme Kurulu"	149
7.8.2. Geleceğe Hazır (Future-Proof) Regülasyon Prensipleri	150
7.8.3. Türkiye İçin Öneriler	151
BÖLÜM 8: PAYDAŞ KATILIMI VE GÖZDEN GEÇİRME	153
TÜRKİYE BİLİŞİM DERNEĞİ İCRA KURULU-SEKTÖR ÇALIŞMA GRUBU	

8.1. Katılımcı Yönetişim Modeli: Çok Paydaşlı Danışma Kurulu	154
8.1.1. Operasyonel Çalışma Prensipleri ve Tematik Gruplar	155
8.1.2. Şeffaflık ve Hesap Verilebilirlik	156
8.2. Periyodik Gözden Geçirme ve Etki Değerlendirme Mekanizması	156
8.2.1. Düzenli Değerlendirme Döngüsü (2–3 Yıl)	156
8.2.2. Veri Odaklı Denetim ve Raporlama	157
8.2.3. Düzenleyici Adaptasyon: Teknolojik Değişimlere Göre Güncelleme Protokolleri	157
8.3. Uluslararası İyi Uygulamalarla Sürekli Uyum Stratejisi	158
8.3.1. Dinamik Mevzuat Takibi	158
8.3.2. Küresel İşbirliği ve Standart Birliği	159
8.4. Uygulama Yol Haritası ve Eylem Planı	159
8.4.1. Faz 1: Kurumsal Yapılanma ve Kapasite İnşası (0–6 Ay)	159
8.4.2. Faz 2: Pilot Uygulama ve İlk Etki Analizi (6–18 Ay)	160
8.4.3. Faz 3: Tam Uyum, Sürekli Gözden Geçirme ve Sürdürülebilirlik (18–36 Ay)	160
8.5. Politika Önerileri ve Sonuç	161
8.5.1. Regülatörler İçin Politika Önerileri (Kamu Sektörü)	161
8.5.2. Platformlar İçin Stratejik Öneriler (Özel Sektör)	162
8.5.3. Arama Motorları için Politika Önerileri	163
8.5.4. Sosyal Ağlar için Politika Önerileri	163
8.5.5. E-Ticaret Politika Önerileri	164
ANALİZ: ALGORİTMİK SİSTEMLER VE GLOBAL BAZI DÜZENLEMELER	170
Kavramsal Çerçeve	170
Uluslararası Yönetişim ve Düzenleme Yaklaşımları	172
Türkiye Açısından Değerlendirme	178
SONUÇ: Yeni Bir Dijital Mutabakata Doğru	180
EK: İNGİLİZCE TERİMLERİN TÜRKÇE KARŞILIĞI	183
ŞEKİL LİSTESİ	188
TABLO LİSTESİ	189
KAYNAKÇA	190
TÜRKİYE BİLİŞİM DERNEĞİ İCRA KURULU-SEKTÖR ÇALIŞMA GRUBU	

SUNUŞ

Kenan Nurhan Altınsaat
Türkiye Bilişim Derneği
Genel Başkanı

Çağdaş, refah düzeyi yüksek bir Türkiye özleminin gerçekleşmesi yolunda, Türkiye Bilişim Derneği (TBD) 55 yıldır yılmadan ve büyük bir özveriyle çalışmaktadır. 1994 yılında Kamu Yararına Çalışan Dernek statüsünü kazanan TBD, 13 bini aşkın üyesi, 15 şehrimize yaygınlaşan şube/temsilcilik yapılanması ve üniversitelerdeki TBD genç örgütlenmesiyle bilişim sektörüne önemli katkılar vermeye devam etmektedir.

TBD olarak, 2026 yılında birbirini tamamlayan ve birlikte değer üreten bütünün parçaları olacak şekilde seçilen konular ile ülkemizin hızlı kalkınması, geleceğin güçlü bir şekilde inşa edilmesi maksadıyla sektörel ÇG oluşturulmuştur. Bu sayede hazırlanacak raporlar ile sektörel değerlendirme yapmaktan öte ülkemizin kalkınması için bütüncül bir bakış açısı sunulması hedeflenmiştir. Bu hedefe ulaşmak ve en doğru sonuca yaklaşabilmek maksadıyla 9 (dokuz) farklı ama birbiri ile örtüşen/birbirini tamamlayan ÇG oluşturulmuş, ortak akıl katkısı alabilmek için de 13 (on üç) ayrı çalıştay icra edilmiştir.

Çalışma gruplarımız tarafından hazırlanan raporlar; dünya genelindeki gelişmelerin yanı sıra Türkiye'nin mevcut durumunu tarafsız ve doğru verilerle inceleyen, karar vericiler, sektör temsilcileri, akademi ve tüm paydaşlar için; güçlü ve ileride olduğumuz konuların belirtildiği, kritik kırılma noktaları taşıyan noktaların tespit edildiği ve gecikmeden atılması gereken adımları öneren stratejik bir doküman olarak görüşlerinize sunulmaktadır.

Çevrimiçi Platformlar: Dijital Dönüşüm ve Dijitalleşme Süreçleri Çalışma Grubumuz tarafından yoğun bir çalışma dönemi sonucunda büyük bir emekle hazırlanan **“DİJİTAL EGEMENLİK VE DİJİTAL GÜVENLİĞE DOĞRU TÜRKİYE İÇİN YOL HARİTASI”** raporumuz yukarıda ifade ettiğim prensip doğrultusunda hazırlanmış çok önemli bir **stratejik belge** ve karar vericiler için çok değerli bir **yardımcı yayın** olma özelliği taşımaktadır.

Ortak akıl, yoğun emek ve özveri ile hazırlanan raporumuza katkıları nedeniyle süreç içerisinde İcra Kurulu Başkanımız olan Sayın **Abdullah Raşit Gülhan** ve daha sonra İcra Kurulu Başkan Yardımcısı olarak süreci devam ettiren **Ahmet Pekel**, Çalışma Grubu Başkanımız Sayın **Murat Özkarabekir** Beyefendilere ve raporun hazırlanmasına katkı veren tüm **ÇG üyelerimize** teşekkürlerimi sunuyorum.

Kamu, özel sektör, akademi dünyası ve diğer STK'larımıza önemli katkılar vereceğine inandığım bu önemli strateji belgesinin yaşayan bir doküman olacağını, siz değerli karar verici ve sektör temsilcilerimizin görüş önerileri ile geliştirilme çalışmaları yapılacağını belirtir, faydalı olması umut ve dileğiyle saygılar sunarım.

TEŞEKKÜR

Abdullah Raşit Gülhan
TBD İcra Kurulu Başkanı

Yirmi birinci yüzyılda sayısal teknolojiler; ekonomik büyümenin, toplumsal refahın ve ulusal güvenliğin temel belirleyicileri arasında en önemli, en üst noktada yer almaktadır. Bu nedenle ülkeler açısından dijitalleşme artık bir tercih değil, stratejik bir zorunluluktur. Bugünün ve yakın geleceğin dünyasında rekabet; ucuz iş gücü, coğrafi avantaj ya da geleneksel üretim kapasitesi üzerinden değil, veri, algoritma, altyapı ve teknoloji geliştirme yetkinliği ve çok iyi yetişmiş insan gücü üzerinden tanımlanmaktadır.

Küresel ölçekte Avrupa Birliği, OECD, Dünya Bankası ve Dünya Ekonomik Forumu ve benzeri uluslararası yapılar; veri ekonomisini, yapay zekâyı, siber güvenliği ve sayısal altyapıları ekonomik rekabetin ve sayısal egemenliğin temel unsurları olarak konumlandırmaktadır. Bu gelişmeler, tüm ülkeler için dijital dönüşümün yalnızca teknolojik bir süreç olmadığını; aynı zamanda ekonomik, politik ve stratejik ve hatta neredeyse ülkelerin köleleşmemeye karşı savaşımının bir yeniden yapılanma süreci olduğunu açıkça ortaya koymaktadır.

Türkiye'nin bu yeni küresel düzende güçlü bir konum elde edebilmesi; sahip olduğu potansiyeli doğru stratejilerle desteklemesine, eksiklerini yahut hatalarını gerçekçi bir şekilde tespit etmesine ve bunları düzeltmek ve tamamlamak için zamanında eylem almasına bağlıdır. Aksi halde, hızla şekillenen sayısal doğal çevrede (ekosistem) geç kalmanın maliyeti yalnızca ekonomik değil, aynı zamanda yapısal bir bağımlılık tehlikesi ile karşı karşıya kalınacaktır.

Bu birikim ve sorumluluk çerçevesinde, Türkiye Bilişim Derneği 2025–2027 dönemi İcra Kurulu ve Kurulumuza bağlı olan TBD İcra Sektör Kurulu tarafından, Türkiye'nin dijital geleceğine yön verecek kritik alanlarda derinlemesine analizler yapmak ve somut öneriler geliştirmek amacıyla bugüne kadar **on üç çalıştay** düzenlenmiş ve ayrıca aşağıda sıralanan **dokuz çalışma grubu** oluşturulmuştur:

- Akıllı Kentler
- Birlikte Çalışabilirlik: Standartlar ve Yasal Düzenlemeler
- Bulut Bilişim ve Veri Merkezleri
- Çevrimiçi Platformlar: Dijital Dönüşüm ve Dijitalleşme Süreçleri
- Siber Güvenlik: Güvenli İletişim, Blokzincir, Kripto Paralar ve Nitelikli İşgücü
- Sürdürülebilirlik: İklim Değişikliği, Tarım ve Hayvancılıkta Bilişim Teknolojileri
- Telekomünikasyon: GSM, Fiber ve Uydu Haberleşme
- Yapay Zekâ: Yapay Zekâ Etiği, Veri Bilimi ve Karar Destek Sistemleri
- Yenilikçi Projeler: Girişimcilik, Ar-Ge ve Ür-Ge

Çalışma gruplarımız tarafından hazırlanan raporlar; dünya genelindeki gelişmelerin yanı sıra Türkiye'nin mevcut durumunu tarafsız ve doğru verilerle inceleyen, eksiklikleri açık bir şekilde ortaya koyan ve uygulanabilir öneriler sunan kapsamlı bir değerlendirmeler ortaya koymaktadır. Çalışma Grubu Raporlarının karar vericiler, sektör temsilcileri, akademi ve tüm paydaşlar için yol gösterici bir kaynak (referans) belge olacaktır. Bu nedenle elinizdeki raporlar, bir durum tespiti çalışması olmanın ötesindedir. Bu raporların;

- Türkiye'nin nerede ileri gittiğini (ki bu sürdürülebilir kılmasının sağlanması dışında müdahale gerektirmez) nerede geri kaldığını açık biçimde ortaya koyan,
- Hangi alanlarda kritik kırılmalıklar taşıdığını gösteren,
- Gecikmeden atılması gereken adımları somut olarak tanımlayan,

strateji/politika belirleyicilere yol gösterici bir doküman olması amaçlanmıştır.

Bugün küresel ölçekte veri merkezi yatırımları ve bulut hizmetleri trilyon dolarlık bir ekonomik büyüklüğe ulaşırken; dijital platformlar ekonominin en hızlı büyüyen alanlarından biri haline gelmiştir. Siber güvenlik, devletlerin ulusal güvenlik politikalarının merkezine yerleşmiş; yapay zekâ ise üretimden sağlığa, finanstan kamu yönetimine kadar tüm alanları dönüştüren bir güç olarak öne çıkmıştır. Telekomünikasyon altyapıları, 5G ve ötesi teknolojilerle birlikte yeni nesil ekonomik faaliyetlerin temelini oluştururken; akıllı şehir uygulamaları ve sürdürülebilirlik odaklı çözümler, yaşam kalitesini ve kaynak verimliliğini yeniden tanımlamaktadır. Girişimcilik ekosistemleri ülkelerin rekabet gücünü belirlerken; birlikte çalışabilirlik ve standartlar, sayısal ekonominin görünmeyen ancak en belirleyici unsurlarından biri olarak öne çıkmaktadır.

Çalışma gruplarının konu başlıklarını ve kapsamalarını belirlerken ülkemizin hızlı kalkınması ve geleceğinin güçlü bir şekilde inşa edilmesine katkı sağlanacak seçimler yapılmasına en üst seviyede özen gösterildi. Ayrıca konuların birbirinden bağımsız olması değil; birbirini tamamlayan ve birlikte değer üreten bütünün parçaları olmasına özel bir önem verildi. Bu nedenle hazırlanan raporlar ile yalnızca sektörel değerlendirmeler sunmakla kalmamayı aynı zamanda ülkemizin hızla kalkınması için bütüncül bir bakış açısı sunmanın da hedeflendiğini ifade etmek yanlış olmayacaktır.

Kısaca, Türkiye açısından önümüzdeki sorun açıktır: Sayısal dönüşüm ya içeriden bizce yönetilecek ya da dışarıdan yönetilecek ve yönlendirilecektir. Dışarıdan yönetilmesi ile veriye ve insan kaynağına sahip olamayan ülkeler için **yeni nesil kölelik düzeninin çağdaş köleleri olması** ile sonuçlanacaktır. Bu çalışmaların amacı, yalnızca Türkiye'nin dijital dönüşümünü hızlandırmak olmayıp aynı zamanda sayısal dönüşüm sürecinin bizim tarafımızdan yönetilmesi ile bu dönüşümün yönünü **Türkiye'nin lehine çevirmektir**. Bu gelişmelerin ortak bir sonucu vardır: Dijitalleşme artık bir fırsat alanı değil, bir ayrışma mekanizmasıdır.

Günümüzde sayısal teknolojiler, ekonomik ve toplumsal dönüşümün en güçlü itici güçleri arasında yer almaktadır. Sayısal dönüşümü sayısal teknolojilerin kullanıldığı bir dönüşüm projesi olarak görmemek ulusların, kurumların ve bireylerin varoluş biçimini yeniden tanımlayan, tüm sosyolojiyi derinden etkileyen yapısal bir süreç olarak görmek gerekmektedir. 2024 yılında küresel dijital dönüşüm harcamaları 2,5 trilyon ABD dolarına ulaşmıştır. Bu rakamın 2027 yılında 3,9 trilyon ABD dolarına erişeceği öngörülmektedir. 2030 yılı itibarıyla ise pazar büyüklüğünün yaklaşık 5 trilyon ABD dolarına ulaşması beklenmektedir.

Çevrim içi platformlar; bireyleri, işletmeleri ve kamu kurumlarını bir araya getirerek bilgiye erişimi kolaylaştırmakta, hizmet sunumunu hızlandırmakta ve yeni iş modellerinin önünü açmaktadır. E-ticaret, fintek, eğitim teknolojileri ve akıllı şehir uygulamalarından sağlık platformlarına kadar uzanan geniş bir yelpazede faaliyet gösteren bu yapılar, artık modern ekonomilerin vazgeçilmez bileşenleri hâline gelmiştir. Kısaca çevrimiçi platformlar sayısal dönüşümü derinden etkileyen ve tetikleyen önemli bir etmen adeta dijital dönüşümün motoru haline gelmiştir. E-ticaret, e-devlet, uzaktan eğitim, sağlık teknolojileri, fintech ve akıllı üretim; hepsinin omurgasında güvenilir, ölçeklenebilir ve kapsayıcı dijital platformlar kullanıcı kolaylığını sağlaması ile sayısal dönüşümü yaygınlaştırmakta kullanıcılar ile yatmaktadır.

Dijital dönüşüm, yalnızca teknolojik bir yenilik süreci değil; aynı zamanda ülkelerin küresel rekabetteki konumlarını belirleyen stratejik bir kaldıraçtır. Dijital altyapısını güçlendiren ülkeler, verimlilik artışı, yatırım çekme kapasitesi ve ihracat potansiyeli bakımından ciddi avantajlar elde etmektedir. Bu çerçevede dijital dönüşüm; girişimcilik ekosistemlerini canlı tutmakta, yüksek katma değerli istihdam yaratmakta ve kamu hizmetlerinin daha etkin biçimde sunulmasına zemin hazırlamaktadır. Uluslararası platformlarla entegrasyon ise yerel aktörlere küresel pazarlara açılma fırsatı sunarak ülkelerin rekabet gücünü kalıcı biçimde artırmaktadır.

Dijitalleşme süreci ise bu dönüşümün somut ve ölçülebilir ayağını oluşturmaktadır. Kurumsal süreçlerin, kamu kayıtlarının ve ticari işlemlerin dijital ortama taşınması; şeffaflığı artırmakta, bürokratik engelleri azaltmakta ve vatandaş ile iş dünyası odaklı hizmet anlayışını güçlendirmektedir. Ancak dijitalleşmenin gerçek anlamda kapsayıcı olabilmesi için altyapı yatırımlarının yanı sıra dijital okuryazarlığın yaygınlaştırılması, veri güvenliğinin sağlanması ve uygun düzenleyici çerçevelerin oluşturulması da büyük önem taşımaktadır. Çalışma grubumuzun bu raporu, söz konusu süreçlere ilişkin kapsamlı bir değerlendirme sunmak ve politika yapıcılara yol gösterici bir kaynak oluşturmak amacıyla hazırlanmıştır.

Bütün bu olumlu gelişmelerin yanı sıra raporda bilgi güvenliği (siber güvenlik) konusu bireyler, tüzel kişiler (kamu ve özel) kısaca ülkeler açısından önemi de göz önünde tutularak özellikle ayrıntılı olarak incelenmiştir. Türkiye Bilişim Derneği olarak bu rapor ile ülkemizin geleceğine u, Dijital ekonominin yeni güç merkezleri artık ülkeler değil, platformlardır. Küresel ölçekte birkaç büyük dijital platform; ticaretten medyaya, reklamlardan lojistiğe kadar birçok sektörü yeniden tanımlamaktadır.

Dünya Ekonomik Forumu, platform ekonomisinin küresel ekonominin en hızlı büyüyen bileşeni olduğunu ortaya koyarken; Avrupa Birliği bu gücü dengelemek için Dijital Pazar düzenlemeleri geliştirmektedir.

Türkiye için kritik soru şudur:

Dijital platformların pazarı mı olacağız, yoksa platform üreten bir ülke mi olacağız?

KOBİ'lerin dijitalleşme oranı, yerli platformların ölçeklenme kapasitesi ve regülasyonların yönü, bu sorunun cevabını belirleyecektir.

Bu rapor, Türkiye'nin dijitalleşme sürecini hızlandırmak ve platform ekonomisinde güçlü bir aktör haline gelmesini sağlamanın zeminini oluşturmak ve kamuoyunu bilgilendirmek için hazırlanmıştır.

Elinizdeki bu kapsamlı rapor, **Çevrimiçi Platformlar: Dijital Dönüşüm ve Dijitalleşme Süreçleri Çalışma Grubumuz** tarafından yoğun bir çalışma dönemi sonucunda büyük bir emekle hazırlanmıştır. Raporun hazırlanmasında başta Çalışma Grubumuzun değerli başkanı sayın **Murat ÖZKARABEKİR** beyefendiye ve sayın **ÖZKARABEKİR** nezdinde raporun hazırlanmasına emek veren çalışma grubu üyelerine, her çalışma grubundaki çalışmaları yakından izleyen TBD İcra Kurulu Başkan Yardımcıları sayın **Ahmet PEKEL** beyefendiye ve sayın **Demet TÜRÜ** hanımefendiye içten teşekkürlerimi sunuyorum. Ortaya konulan bu ortak akıl ve kolektif çaba, Türkiye'nin dijital geleceğini şekillendirme, sürdürülebilir büyüme modelinin oluşturulması yolunda önemli bir adım teşkil etmektedir.

Ülkemizin değerli yöneticilerinin ve ilgililerinin dikkatlerine bu raporun hazırlanma zamanlamasının yaşamsal derecede önemli olduğunu arz etmek isteriz. Çünkü sayısal platform ekonomisinde geç kalanlar, kalıcı olarak bağımlı hale gelecek ve ülke olarak 3'üncü sınıf ülke veya yukarıda da ifade edildiği şekilde çağdaş köleler olacaklardır. Ancak, sadece bu rapora değil Çalışma Gruplarımız tarafından hazırlanan tüm raporlarda ülkenin geleceği için önemli bilgiler bulunacağını vurgulamak isterim. Önemli olan sorunların tespiti, çözümlerin bulunması ve sürdürülebilir yönetim ve büyüme yaklaşımı ile çağa ayak uyduracak adımların atılmasıdır. Sürdürülebilir olmayan bir büyüme modeli, **geleceği ipotek altına almak demektir**. Unutulmalıdır ki; **sayısallaşma bir teknoloji meselesi değil, bir güç meselesidir**. Dijital dönüşüm bir süreç değil, sürekli evrilen bir yolculuktur. Bu yolculukta başarı; **doğru zamanda doğru adımları atabilme kararlılığıyla** mümkün olacaktır. 13 Mayıs 2026

ÖNSÖZ

Dijital platformlar, internetin erken dönemlerinde yalnızca veri barındıran ve ileten "pasif teknik araçlar" olarak kabul ediliyorlardı lakin, günümüzde oldukça farklı bir duruma evrilmişlerdir. Algoritmik sıralama, yapay zekâ destekli sistemler ve büyük verilerle toplumsal yaşamı, ticareti ve pek çok sosyal süreçleri aktif olarak şekillendiren platformlar haline dönüşmüştür. Milyarlarla ifade edilebilecek sayıda insanın algılarını yönlendirmeye etki edebilen bu yapılar, dijital kamusal alanda önemli ve bir nevi kural koyucular haline gelmiştir.

Platformların bu güçleri, dijital ekosistemde, teknik altyapılar sunduğu ve karmaşık algoritmalar halindeki kapsamlı etkilerini anlamak ve buna uygun sistemleri oluşturmak küresel oyuncu olmanın gereğidir.

Dijital ve Çevrim İçi platformlar teknik yapılar olmanın ötesinde, bireysel ve toplumsal sosyo-ekonomik boyutta etki gücüne sahiptir.

Elinizdeki bu Rapor; Türkiye'nin dijital platform yönetiminde daha çok etken bir pazar haline gelmesi amacıyla ele alınmış olup, küresel standartlar (AB DSA/DMA, AI Act, NIS2 ve OECD ilkeleri) ile uyumlu ve yerel ülke gereklerine hitap eden vizyonda hazırlanmıştır.

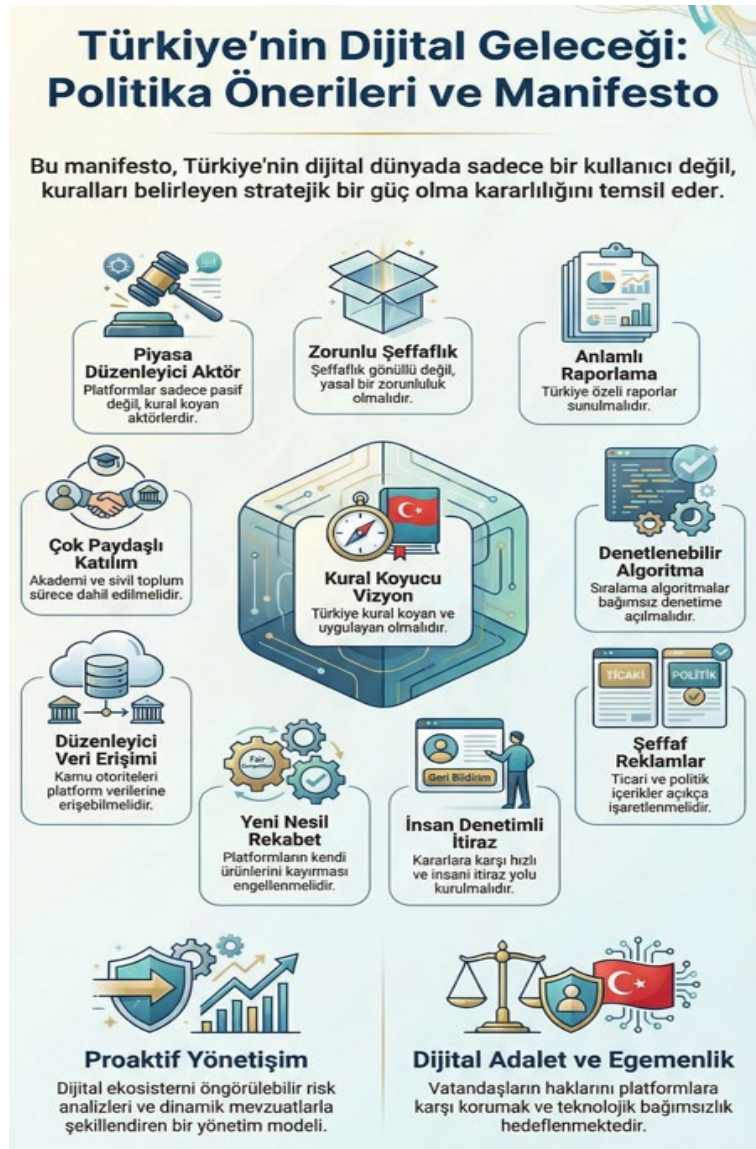
Stratejik odağımız Türkiye'nin dijital ve çevrim içi platformlar ekosisteminde daha etken, kendi standartlarını belirleyen, ekosistemde var olan teknoloji firmaları ile global regülasyonlara uyumlu nitelikte lider ülkeler arasında yer almasıdır.

Amacımız: Bu çalışmanın temel amacı; ‘Dijital ve Çevrim İçi Platformlar’ kapsamında yer alan Arama Motorları, Sosyal Ağlar ve E-Ticaret platformlarının yapılarını irdeleyerek farkındalık oluşturarak ülkemizin gelişimine katkı sağlayacak öneriler sunmaktır. Teknoloji, küresel regülasyonlar uyumu ve yerel düzenlemeler dahil olacak haliyle, sosyo-ekonomik boyutlarda, proaktif tekno-politikalar ile ekosistemin gelişmesine imkân verecek, inovasyonu teşvik edecek vizyonda geniş kapsamda ele alınmıştır. Bu çalışmaları yaparken uluslararası kabul görmüş regülasyonları (AB, OECD, İngiltere vb.) temel alarak ülkemiz mevcut regülasyonlar ile karşılaştırmalı analiz ettik. Temel hedef olarak, zararın oluşmasını bekleyip sonradan aksiyon alan "statik ve reaktif" uygulamalardan ziyade; algoritmik ve kurumsal tedbirlerle olası zararların oluşmasını önleyen "risk temelli ve proaktif" bir modele geçişin stratejik yol haritası sunulmaktadır.

Rapor Manifestosu: Türkiye İçin 10 Politika Önerisi Raporumuzun savunduğu vizyonu ve Türkiye'nin dijital geleceği için önerdiğimiz temel stratejiyi aşağıdaki 10 maddelik manifesto özetlemektedir:

1. Dijital platformlar, sadece aracılık işlevi olan pasif ağlar değildir; bilakis algoritmik süreçler ve kullanım şartları aracılığıyla **piyasa davranışlarını kendi ticari öncelikleri doğrultusunda şekillendirme gücü olan** dinamik teknolojik yapılardır.
2. Platformlardaki şeffaflık, gönüllü değil **zorunlu bir kamu yükümlülüğü** olmalıdır.
3. Ülke bazlı şeffaflık raporları ve standartları olmalıdır.

4. Algoritmik sıralama ve öneri sistemleri denetlenebilir hale gelmelidir.
5. Sponsorlu içerik ve ticari önceliklendirme açıkça etiketlenmelidir.
6. Etkin ve kolay erişilebilen insan denetimli itiraz mekanizmaları oluşturulmalıdır.
7. Rekabet hukuku, algoritmik piyasa gücünü içerecek şekilde yapılanmalıdır.
8. Tüketici ve satıcı verileri düzenleyici kurumlara erişilebilir olmalıdır.
9. Yetkilendirilmiş akademi ve sivil toplum kuruluşları sürece dahil edilmelidir.
10. Türkiye, dijital platform yönetişimi süreçlerinde uluslararası standartları takip eden bir konumdan ziyade, bu alandaki **standartları belirleyen ekosistemde proaktif rol** almalıdır.



ŞEKİL A: Dijital Manifesto (YZ ile hazırlanmıştır)

Kapsam ve Raporun Yapısı: Bu rapor, dijital ve çevrim içi platformları aşağıda özetlenen sekiz bölüm olarak ele almıştır:

1. **Bölüm 1 Tanımlar ve Kavramsal Çerçeve:** "Dijital", "çevrim içi", "sosyal medya", "çok büyük çevrim içi platform (VLOP)" ve "geçit bekçisi (gatekeeper)" gibi temel kavramların uluslararası kabul görmüş (DSA/DMA) tanımları.
2. **Bölüm 2 Şeffaflık ve Raporlama:** Platformların "kara kutu" yapısını açmayı hedefleyen çok katmanlı şeffaflık boyutları, veri kusması (data dumping) yerine "anlamlı raporlama" standartları ile bağımsız denetim mekanizmaları ve politik/kamusal reklam arşivleri.
3. **Bölüm 3 İçerik Yönetişi ve Kullanıcı Koruması:** Genel kapsamda yönetim modelleri, elektronik erişilir "Bildir-ve-Aksiyon" süreçleri, mahkeme dışı uyuşmazlık çözüm seçeneği (Alternative Dispute Resolution - ADR), Güvenilir/Yetkilendirilmiş işaretleyiciler (Trusted Flaggers) ile karanlık tasarımların (dark patterns) yasaklanması ve elzem olarak çocukların korunması.
4. **Bölüm 4 Dijital Platform Ekonomisinde Reklam, Gelir Modelleri, P2B İlişkileri ve Şeffaflık:** Platformdan İşletmeye (P2B) olan süreçlerdeki yapısal çıkar çatışmaları, e-ticaret platformlarının "kendine öncelik verme" (self-preferencing) sorunu, kilitlenme (lock-in) etkisi ve hedefli reklamcılıktaki veri yönetişimi.
5. **Bölüm 5 Yapay Zekâ (YZ) ve Algoritmik Sistemler:** Risk temelli yapay zekâ yönetişimi, algoritmik ayrımcılıkla mücadele, üretken YZ kaynaklı sentetik içeriklerin (deepfake) makine okunur şekilde işaretlenmesi ve algoritmik etki değerlendirmeleri vb. içermektedir.
6. **Bölüm 6 Siber Güvenlik ve Siber (Operasyonel) Dayanıklılık:** AB'nin NIS2 ve DORA standartları çerçevesinde hizmet sürekliliği, koordine yapay davranışlara (CIB) karşı altyapı güvenliği tesisi, çoklu bölge yedekleme mimarisi, tedarik zinciri güvenliği ve afet yönetimi.
7. **Bölüm 7 Denetim, Yaptırımlar ve Hukuki Çözüm Mekanizmaları:** Küresel ciro bazlı idari para cezaları, davranışsal ve yapısal tedbirler, çoklu kurum eşgüdümüne (DRCF modeli) dayalı denetim otoritesinin inşası ve kolektif hak arama (sınıf davaları) mekanizmaları.
8. **Bölüm 8 Paydaş Katılımı ve Gözden Geçirme:** Kamu, akademi, özel sektör ve sivil toplum dahil "Dijital Ekosistem Danışma Kurulu" modeli oluşturulması, "Uygula veya Açıkla" prensibi ile periyodik etki değerlendirmeleri yapılması ile dinamik regülasyon döngüsü.

Önemli kavram ve terimlerin referans alınan orijinal İngilizce kelimeleri ilgili metin içerisinde Türkçe karşılığı ile verilmiştir. Bazı kavram ve terimler farklı bölümlerde tekrarlanmış olmakla birlikte, ilişkili bölümün odağı kapsamında ele alınmış ve irdelenmiştir.

Gelecek Çalışma Alanları ve Tamamlayıcı Raporlama İhtiyacı

Son olarak; Dijital ve Çevrim İçi Platformlar Çalışma Grubu tarafından kaleme alınan bu Rapor, ekosistemin temel yönetim, şeffaflık ve adil rekabet sütunlarını inşa etmeyi amaçlamıştır. Ancak Türkiye'nin "Dijital Egemenlik" vizyonu kapsamında, ekosistemin çok boyutlu kapsamına istinaden bu raporda detaya inilmeyen ancak uzman kuruluşlarca oluşturulacak farklı çalışma görevlendirmelerinde ele alınacağı varsayılan stratejik başlıklar da bulunmaktadır.

Bu kapsamda, aşağıdaki başlıkların ayrı raporlar halinde derinlemesine ele alınması öngörülmüştür:

Dijital Vergilendirme: Mevcut vergi mevzuatının platform ekonomisi özelinde irdelenmesi ve gerekli olacak mevzuat ihtiyaçlarının belirlenmesi.

Finansal Platformlar: Bankacılık, ödeme sistemleri ve finansal teknolojiler (fintek) alanlarında kullanılan dijital platformların yapısal analizi ve düzenlemeler.

Telif ve Fikrî Mülkiyet: Haber, müzik ve diğer dijital sanat eserlerinin telif hakları ile telif gelirlerinin korunması amacıyla ele alınması.

Medya ve Dijital Reklamcılık: Basın ve yayın kuruluşlarının dijital mecralardaki asimetrik pozisyonu ve dijital reklamcılık ekosistemindeki gelir dağılımının ele alınması ve gerekli düzenlemelerin belirlenmesi.

Yatırım ve Fiyatlandırma: Bahse konu platformların Türkiye'deki yatırım alanları ve zorunlu yatırım yapılabilecek hususlar ve genel olarak fiyatlandırma konularının ele alınması.

Ayrıca belirtmek isteriz ki; bu rapor, Aralık 2025 ile Nisan 2026 döneminde, Dijital ve Çevrim İçi Platformlar Çalışma Grubu üyeleri tarafından tamamen gönüllülük esasına dayalı olarak titizlikle ele alınmış ve hazırlanmıştır.

BÖLÜM 1: TANIMLAR VE KAVRAMSAL ÇERÇEVE

Bölümün Amacı: Dijital ekosistemin hızla evrilen yapısal bileşenlerini ele alarak olası kavram karmaşasını gidermek, terminoloji bütünlüğü sağlamak ve rapor boyunca kullanılacak ortak bir tanım seti oluşturmaktır.

İçerik ve Kapsam:

- Dijital, Çevrim İçi ve Sosyal Medya kavramlarının izahı ve birbirinden ayrıştırılması.
- Arama motorları, uygulama mağazaları, pazar yerleri gibi platform ile servis tipolojilerinin sınıflandırılması.
- Platform kapitalizmi, veri asimetrisi, ağ etkileri ve kilitleme (lock-in) gibi ekosistemin yapısal güç dinamiklerinin analizi.
- Avrupa Birliği (DSA/DMA), OECD ve ABD mevzuatındaki yer alan ilgili kavram ve tanımlarının incelenmesi.

Temel Kavramlar: Dijital (Sayısal), Çevrim İçi, Dijital Medya, Çevrim İçi Medya, Sosyal Medya, Çevrim İçi (Online) Platform, Çok Büyük Çevrim İçi Platformlar (VLOPs), Arama Motorları, Çok Büyük Çevrim İçi Arama Motorları (VLOSEs), Dijital Medya ve Çevrim İçi Medya, Çevrim İçi Servisler, Geçit (Kapı) Bekçileri (Gatekeepers), Sosyal Medya ve Sosyal Ağlar, Çevrim içi piyasası, Çevrim İçi Seyahat ve Konaklama Platformu, İçerik Paylaşım Platformu, Uygulama (App) Mağazası, Chatbot (Sohbet Robotu), Agentic / Conversational AI (Eylemsel ve Diyalog bazlı Yapay Zekâ), Platformlaşma ve Ekosistemin Yapısal Dinamikleri, Platform Gücü ve Politik Ekonomi: Yapısal Riskler, Dijital Platformların Akademik ve Fonksiyonel Tanımı

“Dijital” ve “Çevrim İçi” ekosistemin dinamik ve hızla evrilen yapısı, teknik terminolojinin gündelik dile aktarılması sürecinde anlam farklılığına ve kavram karmaşasına neden olmaktadır. Hukuki, teknik ve işlevsel düzlemde belirgin nüanslara sahip olan bu terimlerin bazen birbirleri yerine kullanılması, yanlış çıkarımlara yol açabilmektedir. Bu nedenle raporun başlangıcında, kavramsal netliği sağlamak, terminolojik birliği tesis etmek ve tüm paydaşların aynı tanım seti üzerinde mutabık kalmasını temin etmek amacıyla ana tanımlar ele alınmıştır.

Türk Dil Kurumu (TDK) sözlüğüne göre önemli olan iki temel olgu şu şekilde ayrılmaktadır. (<https://sozluk.gov.tr/>)

Tanım: Bir kavramın niteliklerini eksiksiz olarak belirtme veya açıklama; tarif.

Kavram: Bir nesnenin veya düşüncenin zihindeki soyut ve genel tasarımı; mefhum, fehva, konsept, nosyon.

“Dijital” ile “Çevrim İçi” kelimeleriyle anlatılmak istenenin netleştirilmesi de yerinde olacaktır.

“Dijital” teknolojinin formatını (verinin saklanma ve işlenme biçimi) ifade ederken, “çevrim içi” bu verinin bir ağa (şebeke-network, internet şebekesi) bağlı olma durumunu belirtir.

TDK Uyum: TDK, “online” kelimesinin Türkçe karşılığı olarak “çevrim içi” (ayrı yazılır) kullanımını önermektedir.

Hukuki/Teknik Netlik: Dijital ve çevrim içi kavramları arasındaki temel fark, verinin varlık biçimi ile erişim yöntemi arasındaki ilişki ile açıklanabilir. Bir doküman dijital (sayısal) bir yapıda oluşturulmuş olsa bile, bu durum onun mutlaka çevrim içi olduğunu göstermez. Örneğin, bir kullanıcının yerel bilgisayarında kayıtlı olan bir PDF dosyası dijital bir formda olabilir; ancak herhangi bir ağa bağlı olmadığı için çevrim içi değildir. Söz konusu dijital içerik, bir internet platformuna yüklendiği ve üçüncü tarafların erişimine açıldığı andan itibaren hem dijital hem de çevrim içi olma niteliği kazanır.

Rapor boyunca kullanılan terimlerin doğru anlamlandırılması için “Dijital (Sayısal)” ve “Çevrim İçi” kavramları arasındaki farklılıkların belirlenmesi önemlidir:

Dijital (Sayısal): Verinin fiziksel olmayan, bilgisayar sistemleri tarafından işlenebilir formatını ifade eder. Örneğin, yerel bir diskte saklanan bir dosya dijitaldir, ancak bir ağa bağlı değildir.

Çevrim içi: Dijital bir varlığın veya servisin internet altyapısı üzerinden erişilebilir ve etkileşime açık olma durumudur.

Bu rapor, yalnızca dijital olan unsurları değil, dijital verinin internet ortamında bir platform aracılığıyla üçüncü tarafların erişimine sunulduğu “Dijital ve Çevrim İçi” ekosistemi de kapsamaktadır.

AB’nin Dijital Hizmetler Yasası (DSA) kapsamında aracı hizmetler katmanlı bir yapıya sahiptir. Bu yapı, dijital ekosistemde yer alan hukuki sorumluluk ve yükümlülüklerinin farklılaşmasını mümkün kılmaktadır. DSA, aracı hizmetleri “mere conduit” (yalnızca iletim sağlayan hizmetler), “caching” (geçici depolama), “hosting” (barındırma hizmetleri) ve bunların alt kümesi olarak “çevrim içi platformlar” şeklinde

sınıflandırmaktadır. Çevrim içi platformlar ise kullanıcı tarafından sağlanan içeriği kamuya ulaştırma işlevi üstlenen özel bir hosting türü olarak tanımlanır. Ayrıca, belirli ölçek ve etki eşiklerini aşan platformlar “Çok Büyük Çevrim İçi Platformlar (VLOP)” olarak ayrı bir kategoriye tabi tutulmakta olup, **sistemik risk** yönetimi, bağımsız denetim ve şeffaflık yükümlülüklerine tabi olmaktadır.

Sistemik Risk (Systemic Risk): DSA kapsamında tanımlandığı üzere; bir platformun tasarımının, algoritmasının veya kullanımının toplum geneli üzerinde (demokrasi, kamu sağlığı, temel haklar veya güvenlik) yaratabileceği yaygın ve derin etkilerdir. Denetim odak noktası, tekil ihlallerden ziyade bu risklerin yönetimidir.¹

1.1. Dijital, Çevrim İçi ve Sosyal Medya

Dijital ekosistemde sıklıkla birbirinin yerine kullanılan bu üç kavram, aslında hiyerarşik ve işlevsel açıdan belirgin kriterlerde birbirinden ayrılmaktadır:

- **Dijital Medya:** Elektronik cihazlar aracılığıyla işlenebilen, sayısal formatta (0 ve 1 tabanlı) oluşturulan ve depolanan her türlü veri biçimini (görüntü, ses, video vb.) kapsayan temel tanımdır. Bir verinin dijital olması, onun mutlaka bir ağa bağlı olmasını gerektirmez; mesela yerel bir sürücüde saklanan dosya dijitaldir, ancak henüz "çevrim içi" değildir.
- **Çevrim İçi Medya:** Dijital medyanın internet altyapısı üzerinden erişilebilir hale gelmiş durumudur. İnternet siteleri, bloglar ve çevrim içi yayın platformları gibi tüm internet tabanlı içerikleri kapsayan geniş bir çatı terimdir. Buradaki temel ayırıcı unsur, içeriğin bir ağ (network) üzerinden erişime sunulmuş olmasıdır.
- **Sosyal Medya:** Çevrim içi medyanın kullanıcı etkileşimine ve içerik üretimine dayalı bir alt bileşenidir. Bu platformlar, kullanıcıların sadece içerik tüketmesini değil, aynı zamanda içerik üretmesini, paylaşmasını ve diğer kullanıcılarla etkileşim kurulmasına olanak verir.

Kavramsal Hiyerarşi ve İlişki Notu:

Sosyal medya, çevrim içi medyanın etkileşim odaklı bir alt bileşeni konumundadır; ancak her çevrim içi medya ortamı sosyal medya niteliği taşımaz. Örneğin, kullanıcı etkileşimine kapalı olan kurumsal web siteleri veya tek yönlü bilgi aktarımı sağlayan haber portalları, çevrim içi medya kapsamında yer alırken, sosyal medya tanımının dışında kalmaktadır.

Benzer şekilde, dijital medya hem çevrim içi hem de sosyal medyanın temel bileşeni ve bir nevi hammaddesini oluşturmaktadır. Ancak bir içeriğin dijital formatta olması, onun otomatik olarak geniş

¹ Zuboff, S. (2019): *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs.

kitlelere ulaştığı anlamına gelmez. Dijital bir veri, bir ağ marifetiyle internet ortamına aktarılmadığı sürece çevrim içi bir statü kazanamayacağı gibi, sosyal bir nitelik de oluşturmaz.

1.2. Platform ve Servis Tipolojileri (Sınıflandırmaları)

Raporun bu kısmında, aşağıda yer alan terimlerin aynı kavramda anlaşılması ve terminolojik birlikteliğin sağlanması hedeflenmiştir.

Düzenleyici ve Stratejik Kavramlar

- **Çevrim İçi (Online) Platform:** İnternet aracılığıyla iki veya daha fazla kullanıcı grubunu (örneğin satıcılar ve alıcılar) bir araya getiren etkileşimli dijital yapılar.
- **Çok Büyük Çevrim İçi Platformlar (VLOPs):** Kullanıcı sayısı ve pazar etkisi bakımından belirli büyüklüğe sahip, sistemik risk taşıyan yapılar.
- **Arama Motorları:** İnternet üzerindeki içerikleri tarayan, veri dizini belleğine ekleyen ve kullanıcı sorgularına göre listeleyen sistemler.
- **Çok Büyük Çevrim İçi Arama Motorları (VLOSEs):** Global ölçekte pazar hakimiyetine sahip, büyük ölçekte veri trafiğini yöneten arama sistemleri.
- **Dijital Medya ve Çevrim İçi Medya:** Haber, eğlence ve verinin dijital kanallar üzerinden iletildiği yayıncılık ve içerik ağlarıdır.
- **Çevrim içi Servisler:** Bulut depolamadan e-posta hizmetlerine kadar internet üzerinden sunulan her türlü yazılımsal ve teknik hizmetler.
- **Geçit (Kapı) Bekçileri (Gatekeepers):** Çevrim içi arama motorları, uygulama mağazaları ve mesajlaşma servisleri gibi "temel platform hizmetleri" sunan, pazar üzerinde önemli etkisi olan çok büyük ölçekte veri trafiği içeren dijital platformlardır.

Sektörel ve Sosyal Odaklı Yapılar

- **Sosyal Medya ve Sosyal Ağlar:** Kullanıcıların içerik ürettiği, paylaştığı ve sosyal etkileşim kurduğu dijital topluluk mecraları.
- **Çevrim İçi Pazaryeri:** Birden fazla satıcının ürünlerini tek bir çatı altında sunduğu e-ticaret platformları.
- **Çevrim İçi Seyahat ve Konaklama Platformu:** Rezervasyon, uçuş ve konaklama hizmetlerini dijital ortamda birleştiren platformlar.
- **İçerik Paylaşım Platformu:** Video, ses veya görsel içeriklerin kullanıcılar tarafından yüklendiği ve kitlelere ulaştırıldığı ekosistemler.
- **Uygulama (App) Mağazası:** Mobil veya masaüstü yazılımların kullanıcılara ulaştırıldığı, güncellenmesinin ve satışının yapıldığı dijital mecralar.

Yapay Zekâ ve Etkileşim Teknolojileri

- **Chatbot (Sohbet Robotu):** Belirli kurallara veya algoritmalara dayalı, kullanıcı sorularına insan yerine makine olarak yanıt veren metin tabanlı uygulama arayüzleri.
- **Agentic / Conversational AI (Eylemsel ve Diyalog bazlı Yapay Zekâ):** Sadece yanıt vermekle kalmayan, makine muhakeme yeteneği ile karmaşık işlevleri yapabilme yeteneği olan, doğal dille insan benzeri etkileşim kuran gelişmiş sistemler.

1.3. Platformlaşma ve Ekosistemin Yapısal Dinamikleri

Dijital ve çevrim içi hizmetlerin tanımlanması, bu hizmetlerin içerdiği ekosistemin sosyo-ekonomik boyutunun anlaşılmasını gerekli hale getirmiştir. Dijital platformlar sadece teknolojik altyapılar değildir ve ekonomiyi yönlendirme gücüne sahip yapılara evrilmiş olup aşağıdaki yer alan kapsamda ele alınmaktadır:

Platform Kapitalizmi: Geleneksel ekonomik modellerden dijital ekosisteme geçişle birlikte platformlar, yalnızca alıcı ve satıcıyı buluşturan teknik araçlar olmanın dışında; kendi kurallarını koyan, algoritmik sistemler ve veri temelli gelir modelleri üzerinden piyasa oluşturucu hale (platform kapitalizmi) dönüşmüştür. Bu platformlaşma süreci, dijital platformları pasif aktarıcılar (hosting) yerine, algoritmik sıralama ve yapay zekâ destekli içerik marifetiyle, kullanıcı deneyimini ve ticari erişimi belirleyen aktif oyuncu konumuna getirmiştir.

Veri Asimetrisi: Platform ekonomisinin temel kaynaklarından biri, kullanıcılar ve işlem verileri üzerindeki kontrolden doğan veri asimetrisidir. Platformlar, pazar yerindeki ticari kullanıcıların (satıcıların) faaliyetlerinden elde ettikleri verileri kendi markalı ürünlerini (Private Label) geliştirmek veya algoritmalarını eğitmek için kullanabilirler. Lakin, ellerindeki bu verileri satıcılardan, düzenleyici kurumlardan veya bağımsız denetçilerden gizleyerek hem bilgi hem de haksız bir rekabet avantajı elde edebilmektedir.

Dijital Kamusal Alan ve Dönüşüm: Arama motorları ve sosyal ağlar, internetin erken dönemlerindeki statik web sayfaları işlevinden farklı olarak, dijital kamusal alanı aktif olarak yöneten ve/veya yönlendiren sosyo-teknik ekosistemler haline getirmiştir. Bu dönüşüm, platformları ticari şirketler olmanın ötesine, bilginin yayılım hızını, kamusal tartışmaları ve biçimlerini etki edip yönlendirebilen altyapı sağlayıcıları haline getirmiştir.

Ağ Etkileri ve Piyasa Yoğunlaşması: Dijital platform ekonomisi, ağ etkileri, ölçek ekonomisi ve büyük ölçekli veri avantajı ile karakterize edilmektedir. Bir platformun kullanıcı sayısı arttıkça, ticari kullanıcılar (satıcılar veya yayıncılar) için o platformda bulunmama maliyeti de artmaktadır. Bu ekonomik bağımlılık ve kilitleme etkisi (lock-in effect), dijital pazarın ve gelirlerin çok az sayıdaki büyük global şirketlerin elinde toplanmasına (piyasa yoğunlaşması) yol açarak yeni KOBİ'lerin veya girişimlerin pazara girişini zorlaştıran bir bariyer oluşturmaktadır.

Algoritmik Kapı (Eşik) Bekçiliği (Gatekeeping): Piyasada "geçit bekçisi" (gatekeeper) konumuna ulaşan devasa platformlar, algoritmik kararlarıyla hangi bilginin görünür olacağını, hangi satıcının gelir elde edeceğini ve rakiplerin pazara nasıl erişeceğini belirleme gücüne sahip algoritmik kapı bekçiliği işlevini üstlenmektedir. Bu geçit bekçisi rolü, platformların kendi hizmetlerini organik arama sonuçlarında veya uygulama mağazalarında haksız şekilde öne çıkarması (kendine öncelik verme / self-preferencing) riskini beraberinde getirmektedir.

1.4. Platform Gücü ve Politik Ekonomi: Yapısal Riskler

Dijital platformların teknik ve operasyonel tanımlarının ötesinde, modern ekonomiyi ve toplumsal düzeni etkileyen politik ve ekonomik boyutu da bulunmaktadır. Platformların piyasadaki "aracı" rollerinden çıkarak ekosistemin hakim konumuna gelmeleri, aşağıdaki kritik yapısal güç ve bağımlılık dinamiklerini ortaya çıkarmıştır:

Algoritmik Yönetişim Mimarisi Olarak Platformlar: Dijital platformlar, günümüzde yalnızca içerik barındıran teknik araçlar olmaktan çıkmış; dijital kamusal alanı şekillendiren, pazarın kurallarını koyan ve uygulayan "özel regülatörler" ve yönetim aktörleri haline dönüşmüştür. Literatürde "platform iktidarı" ve "algoritmik yönetim" olarak adlandırılan bu yapı, devlet dışı özel aktörlerin milyonlarca kullanıcının bilgiye erişimini, ticari faaliyetlerini ve ifade alanlarını kendi hizmet şartları üzerinden yönetmesi ve düzenlemesidir.

Veri Çıkarımı ve Dikkat Ekonomisi: (Attention Economy) Platform iş modellerinin merkezinde "dikkat ekonomisi" (attention economy) yer almaktadır. Bu modelde kullanıcılara sunulan "ücretsiz" hizmetler karşılığında, kullanıcıların platformda geçirdikleri süre ve ilgi bir veri hammadde haline dönüşmektedir. Kullanıcıların davranışsal verileri ve dijital izleri rıza dışı "davranışsal artık" olarak toplanmakta, profillenmekte ve hedefli reklamcılık gibi yöntemlerle ticari bir değere dönüştürülmektedir.

Algoritmik Görünürlük ve Gündem Belirleme: Platformların sahip olduğu algoritmik sıralama ve öneri sistemleri, hangi bilginin, ürünün veya siyasi/sosyal anlatının ne kadar görünür olacağına karar verecek bir editoryal güç oluşturmaktadır. Bu algoritmik görünürlük kontrolü kullanıcıları yankı odalarına (filtre balonları) hapsetme, dezenformasyonun yayılım hızını organik olmayan şekilde artırma (amplifikasyon) ve hatta arama motoru manipülasyonu (SEME) yoluyla kararsız seçmenlerin tercihlerini değiştirerek toplumsal/siyasal gündemi doğrudan belirleme gücüne sahiptir.

Altyapısal Güç ve Arayüz Gücü: Platformların pazar üzerindeki etkileri iki farklı katmanda işlemektedir. Bir yanda lojistik ağlar, ödeme sistemleri ve devasa veri sunucuları üzerinde kurulan "altyapısal güç", diğer yanda ise tüketicinin platformla etkileşime girdiği noktada devreye giren "arayüz gücü". Karanlık tasarımlar (dark patterns) ve manipülatif seçim mimarileri inşa ederek tüketicinin rasyonel karar verme yetisini yönlendirme etkisi vardır.

Kullanıcılar ve KOBİ'ler İçin Bağımlılık ve Kilitlenme (Lock-in) Riskleri. Platform ekonomisindeki asimetrik güç, dijital pazara erişmek isteyen yerel KOBİ'ler ve ticari kullanıcılar için tek taraflı bir ekonomik bağımlılık oluşturmaktadır. Yüksek komisyonlar ve zorlayıcı sözleşme şartlarına boyun eğmeye zorlayan "kilitlenme etkisine" (lock-in effect) neden olmaktadır.

1.5. Uluslararası Tanımlardan Seçkiler

Avrupa Birliği Dijital Hizmetler ve Dijital Pazarlar Yasası

Avrupa Birliği-AB'nin düzenleyici çerçevesinde, özellikle Dijital Hizmetler Yasası (DSA) ve Dijital Pazarlar Yasası (DMA) kapsamında, bu terimler şu şekilde tanımlanmaktadır:

Dijital Hizmetler: İnternet erişim sağlayıcıları, alan adı kayıt kuruluşları ve bulut barındırma gibi ağ altyapısı sağlayan tüm aracı hizmetleri kapsayan geniş bir kategoriye ait hizmetler.

Çevrim İçi Platformlar: Yalnızca bilgi depolamakla kalmayıp, kullanıcının isteği üzerine kamuya da yayılan belirli bir barındırma hizmeti türü. Örnekler arasında sosyal medya, pazar yerleri, uygulama mağazaları ve seyahat rezervasyon sistemleri yer almaktadır.

Dijital Hizmetler Yasası (DSA – Yönetmelik (AB) 2022/2065) ²

DSA kapsamındaki “Dijital Hizmetler”, kullanıcıları dijital ağlardaki içeriklere, diğer kullanıcılara veya hizmetlere bağlayan hizmetler de dahil olmak üzere çevrim içi aracı hizmetlerini kapsar; genel olarak AB’de sağlanan internet platformlarını, barındırma ve diğer çevrim içi hizmetleri içerir.

Dijital Pazarlar Yasası (DMA – Yönetmelik (AB) 2022/1925)³

Çok Büyük Çevrim İçi Platformlar (VLOP'lar), B'nin Dijital Pazarlar Yasası (DMA) uyarınca, ortalama aylık aktif hizmet alıcı sayısı 45 milyon veya daha çok olan ve Komisyon tarafından VLOP olarak tanımlanan çevrim içi platformlardır. 45 milyon eşiği, AB nüfusunun yaklaşık %10'una denk gelmektedir ve belirleme süreci, Resmî Gazete’de yayınlanan Komisyon kararlarıyla ilan edilmiştir. Komisyon, platform veya arama motorunun bir yıl boyunca aylık 45 milyon kullanıcı eşiğine ulaşmaması durumunda kararını iptal eder. VLOP statüsü yalnızca kullanıcı sayısı ile değil, Avrupa Komisyonu tarafından yapılan resmi ilan ile belirlenir. Bu platformlar sistemik risk değerlendirmesi, bağımsız denetim ve veri erişimi yükümlülükleri gibi önemli yükümlülüklerle tabidir.

Geçit Bekçileri (Dijital Platformlar / Temel Platform Hizmetleri), ‘Geçit bekçisi’, 3. Madde uyarınca belirlenmiş temel platform hizmetleri sağlayan teknoloji şirketleridir. AB-DMA uyarınca, geçit bekçisi önemli pazar gücüne sahip ve işletmeler ile son kullanıcılar arasında temel dijital hizmetler için bir geçit

² Digital Services Act (DSA), <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act>

³ Digital Markets Act (DMA), https://digital-markets-act.ec.europa.eu/index_en

görevi gören büyük bir dijital platformdur. DMA, bu statüyü belirlemek için nicel ve nitel kriterlerin bir karışımını kullanır:

Bir geçit (kapı) bekçisi: Güçlü ekonomik konuma ve AB iç pazarı üzerinde önemli bir etkiye sahip büyük bir dijital platformdur. Birçok işletmenin son kullanıcılara ulaşmak için bağımlı olduğu, rakiplerine göre önemli avantajlara sahip ve dijital pazarda baskın bir konuma haiz platformlardır.

Büyüklüğü nedeniyle, geçit bekçileri daha küçük rakiplerine göre önemli avantajlara sahiptir ve dijital pazarda baskın bir konumdadır.

Temel platform hizmeti’, aşağıda sıralanan hizmetlerdir:

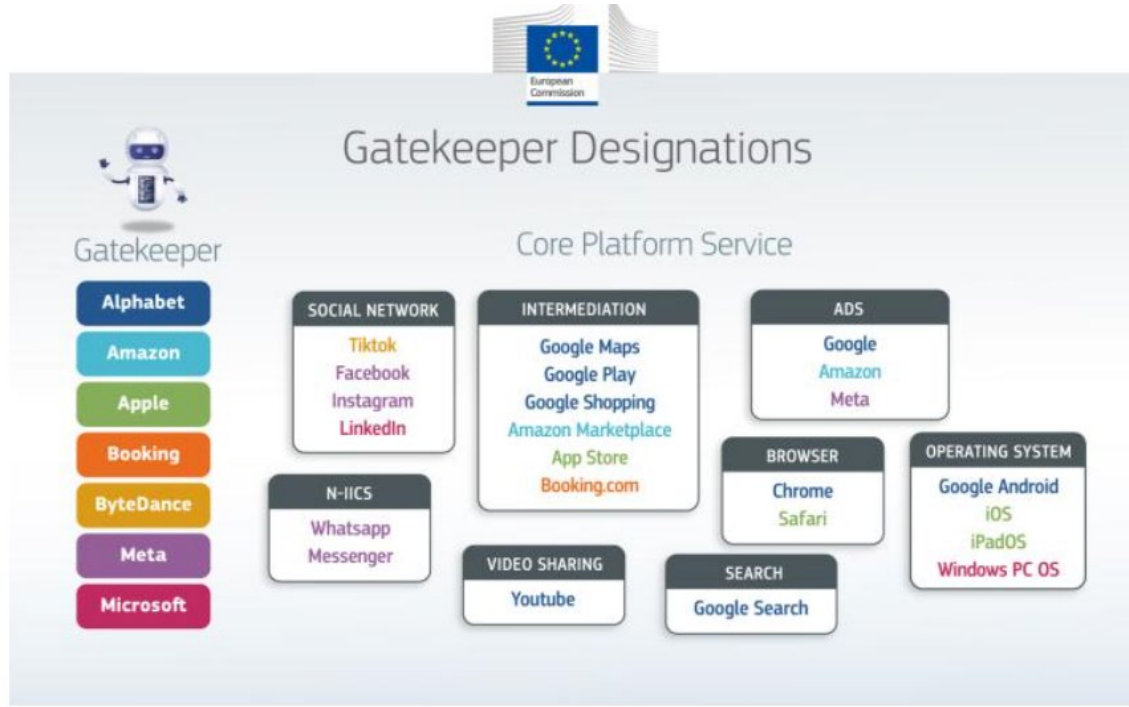
- Çevrim içi aracılık hizmetleri,
- Çevrim içi arama motorları,
- Çevrim içi sosyal ağ hizmetleri,
- Video paylaşım platformu hizmetleri,
- Numaradan bağımsız kişiler arası iletişim hizmetleri,
- İşletim sistemleri,
- Web tarayıcıları,
- Sanal asistanlar,
- Bulut bilişim hizmetleri,
- Çevrim içi reklam hizmetleri (reklam ağları ve borsaları dahil).

DMA ile Resmi Olarak Belirlenmiş Geçit (Kapı) Bekçisi Şirketler ve Servisleri⁴

- **Alphabet:** Google Search, Google Play, Google Maps, Google Shopping, YouTube, Chrome, Android ve çevrim içi reklam servisleri.
- **Amazon:** Amazon Pazaryeri ve Reklam Hizmetleri.
- **Apple:** App Store, Safari, iOS ve iPadOS.
- **Booking:** Booking.com
- **ByteDance:** TikTok
- **Meta:** Facebook, Instagram, WhatsApp, Messenger ve Meta Reklam Hizmetleri.

⁴ Geçit Bekçisi Şirketler ve Servisleri, https://digital-markets-act.ec.europa.eu/gatekeepers_en

- **Microsoft:** LinkedIn ve Windows PC OS



ŞEKİL 1-1: AB Gatekeepers - Geçit Bekçileri- (YZ ile hazırlanmıştır)

TABLO 1-1: Kavramlar ve Regülasyonda İlgili Maddeler

Kavram	Regülasyon	İlgili Madde
Dijital Hizmetler (Aracı Hizmetler)	DSA 2022/2065	Article 2 (scope & definitions via e-Commerce Directive)
Çevrim İçi Platform (DSA)	DSA 2022/2065	<i>Definitions section</i> (Article 2) — hosting services storing and disseminating info to the public
Çok Büyük Çevrim İçi Platform (VLOP)	DSA 2022/2065	Article 33 (designation threshold 45 M)
Geçit (Kapı) Bekçisi	DMA 2022/1925	Article 2(1) (designation definition)
Temel Platform Hizmeti	DMA 2022/1925	Article 2(2) (exhaustive list of digital services)

Dijital Düzenlemelerde Eşik Kriterleri: DMA ve DSA Ayrımı

Avrupa Birliği'nin dijital pazarları düzenleme stratejisi iki temele dayanmaktadır. Bu iki yasa benzer platformları hedef alsa da kriterleri ve amaçları bakımından farklılıklar vardır.

Önemli Not: DMA "piyasa rekabetini" korumayı hedefler iken; DSA "içerik güvenliği ve dezenformasyonu" engellemeyi amaçlar.

DMA Kapsamında "Geçit Bekçisi" (Gatekeeper) Kriterleri

Dijital Pazarlar Yasası (DMA) Madde 3; bir şirketin "geçit bekçisi" olarak tanımlanması için gerekli olan nicel eşikleri belirler. Bu kriterler platformun ekonomik gücünü ve pazardaki konumunu ölçer:

- **Ekonomik Etki:** Son üç mali yılda Avrupa Ekonomik Alanı'nda (AEA) yıllık en az **7,5 milyar Euro** ciro veya şirketin piyasa değerinin en az **75 milyar Euro** olması.
- **Kullanıcı Erişimi:** AB içinde aylık **45 milyondan fazla** aktif nihai kullanıcıya ve yıllık **10.000'den fazla** aktif kurumsal kullanıcıya sahip temel bir platform hizmeti işletmek.
- **Süreklilik:** Bu kullanıcı sayılarına son üç mali yılın her birinde ulaşmış olmak.

DSA Kapsamında VLOP ve VLOSE Tanımları

Dijital Hizmetler Yasası (DSA) ise ekonomik güçten ziyade, platformun toplumsal risklerine ve kullanıcı hacmine odaklanır. Bu kapsamda iki kategori belirlenmiştir:

- **VLOP (Çok Büyük Çevrim İçi Platformlar):** AB nüfusunun %10'una (yaklaşık **45 milyon kullanıcı**) eşdeğer veya daha fazla kullanıcıya sahip platformlar.
- **VLOSE (Çok Büyük Çevrim İçi Arama Motorları):** Aynı kullanıcı eşiğine sahip arama motorları.

Kapsamdaki Başlıca Platformlar

Regülasyonların hedefindeki "Sistemik Önemli" platformlar şunlardır:

Kategori	Platform Örnekleri
E-Ticaret & Pazaryeri	Amazon Store, Alibaba AliExpress, eBay, Zalando
Uygulama Mağazaları	Apple AppStore, Google Play
Sosyal Medya	Facebook, Instagram, TikTok, Snapchat, Twitter (X), LinkedIn, Pinterest
Arama Motorları (VLOSE)	Google Search, Bing
Diğer Hizmetler	Google Maps, Google Shopping, YouTube, Wikipedia, Booking.com

1.6. Dijital Platformların Akademik ve Fonksiyonel Tanımı

Akademik literatürde dijital platformlar, iki veya daha fazla bağımsız kullanıcı grubunun (temsilciler, hizmet sağlayıcılar, son kullanıcılar) etkileşimini dijital bir arayüz üzerinden koordine eden, "**işlem maliyetlerini**" (**transaction costs**) minimize eden ve "**ağ etkileri**" (**network effects**) üzerinden değer yaratan modüler yapılardır (Gawer & Evans, 2016).⁵

İşlevsel Sınıflandırma;

Literatürde platformlar, sundukları teknik altyapı ve ekonomik değer önerisine göre üç temel kategoride incelenmektedir:

- **İşlem Platformları (Transaction Platforms):** Farklı taraflar arasındaki doğrudan etkileşimi ve mal/hizmet değişimini kolaylaştıran dijital aracı kurumlardır (Cusumano ve ark., 2019)⁶. Bu yapılar, **arama ve eşleşme maliyetlerini** düşürerek piyasa etkinliğini artırır (Örn: Dijital pazaryerleri).
- **Yenilik Platformları (Innovation Platforms):** Üçüncü taraf geliştiricilerin mevcut bir teknolojik çekirdek (core) üzerinde yeni ürün veya hizmetler (app, eklenti vb.) geliştirmesine olanak tanıyan altyapılardır. Bu sistemler, "**modülerlik**" prensibiyle ekosistemin genişlemesini sağlar (Gawer, 2014).⁷
- **Entegre (Hibrit) Platformlar:** Hem işlem hem de yenilik fonksiyonlarını bünyesinde barındıran, veriyi ana üretim faktörü olarak kullanan karmaşık ekosistemlerdir.

Teknik Altyapı ve Yönetişim Parametreleri

Akademik bir perspektifle dijital platformlar, sadece birer "yazılım" değil, belirli kurallar dizisiyle işletilen "**yönetişim mekanizmalarıdır**" (Tiwana, 2013).⁸ Bu mekanizmalar şu teknik unsurları içerir:

- **Veri Toplama ve Kürasyon:** Platformun asimetrik bilgiyi optimize etmek amacıyla kullanıcı verilerini algoritmik olarak işleme ve içeriği düzenleme (Aggregators).
- **Erişim Kontrolü ve Standartlaştırma:** Platform sahibinin ekosisteme kimlerin hangi teknik şartlarla (API entegrasyonu, doğrulama protokolleri vb.) dahil olacağını belirleme.

⁵ Evans, P. C., & Gawer, A. (2016). *The Rise of the Platform Enterprise: A Global Survey*. The Center for Global Enterprise.

⁶ Cusumano, M. A., Gawer, A., & Yoffie, D. B. (2019). *The Business of Platforms: Strategy in the Age of Digital Competition, Innovation, and Power*. Harper Business.

⁷ Gawer, A. (2014). *Bridging differing perspectives on technological platforms: Toward an integrative framework*. Research Policy, 43(7), 1239-1249.

⁸ Tiwana, A. (2013). *Platform Ecosystems: Aligning Architecture, Governance, and Strategy*. Morgan Kaufmann

OECD Tanımı: OECD, Türkiye'nin de yer aldığı, G7 ülkeleri dahil olmak üzere 38 üye ülkeden oluşmaktadır.⁹ (The OECD: Organization for Economic Co-operation and Development)

OECD, çevrim içi platformları şu şekilde tanımlar: “İnternet üzerinden hizmet aracılığıyla etkileşim kuran, birbirinden farklı ancak birbirine bağımlı iki veya daha fazla kullanıcı grubu (şirket veya birey) arasındaki etkileşimleri kolaylaştıran dijital hizmetler. Bu tanım, işletmeden tüketiciye direkt (B2C) e-ticaret ve reklamsız içerik akışı gibi işletmeleri içermez, çünkü bunlar yalnızca bir müşteri grubuna hizmet vermektedir. Bununla birlikte, üçüncü taraf B2C e-ticaret ve reklam destekli içerik akışı gibi işletmeleri içermektedir, çünkü bu hizmetler iki ayrı kullanıcı grubunu kapsamaktadır.”¹⁰

Amerika Birleşik Devletleri Tanımı: (Defining and Regulating Online Platforms)¹¹

“Aşağıdaki federal kanunda tanımlanan terimler genel olarak çevrim içi platformları kapsadığı kabul edilir; liste kapsamlı değildir:

Elektronik iletişim hizmeti (18 U.S.C. §2510):

Kullanıcılarına kablolu veya elektronik iletişim gönderme veya alma olanağı sağlayan herhangi bir hizmet; bu, eyaletler arası veya yabancı ticareti etkileyen, kısmen veya tamamen kablolu, radyo, elektromanyetik, foto-elektronik veya foto-optik bir sistem aracılığıyla iletilen her türlü işaret, sinyal, yazı, görüntü, ses, veri veya bilginin aktarımı olarak tanımlanır, ancak şunları içermez:

(A) herhangi bir kablolu veya sözlü iletişim;

(B) yalnızca tonlu çağrı cihazı aracılığıyla yapılan herhangi bir iletişim;

(C) bir takip cihazından (bu başlığın §3117'sinde tanımlandığı gibi) gelen herhangi bir iletişim; veya

(D) bir finans kurumu tarafından fonların elektronik olarak saklanması ve aktarılması için kullanılan bir iletişim sisteminde saklanan elektronik fon transferi bilgileri;

Etkileşimli bilgisayar hizmeti (47 U.S.C. §230):

Birden fazla kullanıcının bir bilgisayar sunucusuna bilgisayar erişimini sağlayan veya mümkün kılan herhangi bir bilgi hizmeti, sistem veya erişim yazılımı sağlayıcısı; özellikle İnternet'e erişim sağlayan bir hizmet veya sistem ve kütüphaneler veya eğitim kurumları tarafından işletilen veya sunulan bu tür sistemler veya hizmetler.”

Hizmet sağlayıcı (17 U.S.C. §512):

⁹ OECD Üye Ülke Listesi, <https://www.oecd.org/en/about/members-partners.html>

¹⁰ OECD (2019). *An Introduction to Online Platforms and Their Role in the Digital Transformation*. OECD Publishing, Paris, <https://doi.org/10.1787/53e5f593-en>.

¹¹ Cho, Clare Y.; Zhu, Ling, (2023). *Defining and Regulating Online Platforms*. Library of Congress, USA. <https://www.congress.gov/crs-product/R47662>

(A) (a) alt bölümünde kullanıldığı şekliyle, "hizmet sağlayıcı" terimi, kullanıcının seçtiği materyalin, gönderilen veya alınan materyalin içeriğinde herhangi bir değişiklik yapılmadan, kullanıcı tarafından belirtilen noktalar arasında veya bunlar arasında dijital çevrim içi iletişim için iletim, yönlendirme veya bağlantı sağlama hizmeti sunan bir kuruluşu ifade eder.

(B) Bu bölümde, (a) alt bölümü dışında, "hizmet sağlayıcı" terimi, çevrim içi hizmetler veya ağ erişimi sağlayıcısı veya bunların tesislerinin işletmecisi anlamına gelir ve yukarıda (A) maddesinde açıklanan bir kuruluşu içerir.

BÖLÜM 2: ŞEFFAFLIK VE RAPORLAMA

Bölümün Amacı: Dijital platform faaliyetleri kapsamında "kara kutu" (black box) konusuna odaklanarak güven ve öngörülebilirliği artırmak; dev teknoloji şirketlerini yalnızca teknik araçlar olarak değil, kamusal kurallar, standartlar ve değerler üreten aktörler olarak ele almak suretiyle demokratik meşruiyet ve kamusal denetim zeminini inşa etmektir.

İçerik ve Kapsam:

- Çok Katmanlı Şeffaflık Boyutları: Algoritmik şeffaflık, veri yönetiřimi, ierik moderasyonu, reklam ve prosedürel şeffaflığın detaylandırılması.
- Standartlaştırılmış şeffaflık raporlamaları (ierik kaldırma, řikâyetler ve itirazlar) ve algoritmik sıralama sistemlerine ilişkin beyanların çerçevesi.
- Platformların gelir modellerinin ve seçim güvenliği için hayati olan "Politik ve Kamusal Reklam Arşivlerinin" (Ad Repositories) incelenmesi.
- Platformların yarı-kamusal rolü üzerinden hesap verebilirliğin siyasal boyutunun ve "Bağımsız Denetim" (Independent Auditing) mekanizmalarının kurgulanması

Temel Kavramlar:

- Kara Kutu Toplumu (The Black Box Society)
- Anlamlı Raporlama (Meaningful Reporting)
- Veri Kusması (Data Dumping) / Raporlama Tiyatrosu
- Bağımsız Denetim (Independent Auditing)

2.1. Dijital Platformlarda Yeni Güven Mimarisi ve Türkiye Perspektifi

Bu bölüm; Arama Motorları, Sosyal Ağlar ve E-Ticaret Platformlarının faaliyetlerinde "**Güven ve Öngörülebilirliği**" artırmak amacıyla; Avrupa Birliği Dijital Hizmetler Yasası (DSA)¹², Avrupa Birliği Dijital Piyasalar Yasası (DMA)¹³, Avrupa Birliği Yapay Zekâ Tüzüğü (AI Act)¹⁴, Avrupa Birliği Ağ ve Bilgi Güvenliği Direktifi (NIS2)¹⁵, İngiltere ve OECD^{16, 17, 18} kural ve standartlarını temel alan kapsamlı bir yönetim modeli sunmayı amaçlamaktadır. Günümüz dijital ekosisteminde şeffaflık konusu, sadece isteğe bağlı bir kurumsal iletişim tercihi olmayıp, aynı zamanda hukuki bir zorunluluk ve pazar rekabetçiliği unsuru olarak ele alınmaktadır. Bu bölüm kapsamında ortaya çıkan çalışma, küresel iyi uygulama örneklerini analiz etmek yoluyla, **Türkiye'nin dijital mevzuat stratejisi ve uluslararası harmonizasyon süreci** için stratejik bir zemin oluşturmayı hedeflemektedir.

Temel Yaklaşım: Risk Temelli ve Orantılılık

Bu bölümün temel felsefesi, dijital platformların toplumsal ve ekonomik etkilerinin dikkate alınması ve bunlarla orantılı olacak şekilde bir sorumluluk mantığına tabi tutulmasıdır. Bu bağlamda:

- Çok Büyük Çevrim İçi Platformlar (Very Large Online Platforms, VLOPs); kapsamlı ve detaylı riskleri (dezenformasyon, temel hak ihlalleri, seçim güvenliği) nedeniyle "en yüksek" hesap verebilirlik seviyesinde ele alınmıştır.
- Arama motorları için "bilgiye tarafsız erişim", sosyal ağlar için "algoritmik yankı odalarının yönetimi", e-ticaret için ise "satıcı doğrulaması ve adil rekabet" öncelikli risk alanları olarak tanımlanmıştır.

Türkiye özelinde bu yaklaşım; yerel piyasa dinamiklerini korurken, küresel standartlarla (AB, İngiltere ve OECD) uyumlu bir ekosistem inşasını oluşturmayı amaçlamaktadır.

¹² **DSA (Digital Services Act), European Union (2022).** Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act). Official Journal of the European Union, L 277/1.

¹³ **DMA (Digital Markets Act), European Union (2022).** Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act). Official Journal of the European Union, L 265/1.

¹⁴ **AI Act, European Union (2024).** Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union, L series.

¹⁵ **NIS2 Directive, European Union (2022).** Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive). Official Journal of the European Union, L 333/80.

¹⁶ **OECD (2020).** OECD Guidelines on Relevant Standards for Transparency and Accountability in the Digital Economy.

¹⁷ **OECD (2019).** Artificial Intelligence and Public Policy.

¹⁸ **OECD (2021).** Transparency reporting on content moderation: A review of current practices.

Stratejik Odak Alanları ve Bulgular

Şeffaflık: “Kara Kutu”nun Açılması

Platformların algoritmik "kara kutu" yapısı, son kullanıcı ve regülatör nezdinde öngörülebilirliği zayıflatmaktadır.

- **Algoritmik Öngörülebilirlik:** Kullanıcıların bir içeriği "neden" gördüklerini anlamaları ve hatta irdemeleri için ana sıralama parametrelerinin deklare edilmesi önerilmektedir.
- **Kapsamlı Reklam Arşivleri (Ad Repositories)**

Şeffaflık yükümlülüğü sadece politik reklamlarla sınırlı kalmamalı; **tüm reklam ekosistemini (ticari, politik ve kamusal)** kapsamalıdır.

- **Demokratik Denetim:** Seçim güvenliği için politik reklamların finansman ve hedef bilgilerinin paylaşılması önemlidir.
- **Kamusal ve Ticari Şeffaflık:** Kamu spotlarının erişim verileri ile ticari reklamların hedef kitlelerinin (yaş, konum, ilgi alanı vb.) kamusal denetime açılması gereklidir.
- **Denetlenebilirlik:** Türkiye’deki dijital reklam pazarında dezenformasyonu, haksız rekabeti ve manipülatif reklam modellerini engellemek amacıyla, gerekli durumlarda, regülasyona tabii olacak sistematik içerisinde, reklamların kim tarafından, hangi bütçeyle ve kime gösterildiğinin izlenebileceği bir veri tabanı kurulmalıdır.

Raporlama: Standartlaşma ve Veri Bütünlüğü

Çok fazla veri, içerik veya rapor ile ‘*Veri Kusması*’ (Data Dumping) şeffaflık sağlamaz; esas olan gerektiği zaman ulaşılabilir ve faydalı olan bir "anamlı raporlama" (Meaningful Reporting) sistemi oluşturmaktır.

- **Standartlaştırma:** Platformlar arası karşılaştırmayı sağlamak için OECD standartlarındaki ortak metriklerin (örn: içerik kaldırma hızları, itiraz kabul oranları) kullanımı önerilmektedir. Ayrıca, yapay zekâ hata payları ve yerel yasal taleplerin işlenme süreçleri OECD standartlarındaki gibi raporlanmalıdır.
- **İşlevsel Dökümler:** İçerik moderasyonunun (sosyal medya, web siteleri ve dijital platformlarda kullanıcılar tarafından oluşturulan içeriklerin (yorum, video, fotoğraf), platformun kurallarına ve yasalara uygunluğunu denetleme işleminin ne kadarının yapay zekâ ne kadarının insan eliyle yapıldığının beyanı, sistemin hata paylarının denetlenmesi için gereklidir.

Özetle, Türkiye’deki mevcut bildirim yükümlülüklerinin, AB-DSA ve OECD standartlarıyla uyumlu hale getirilerek daha niteliksel bir boyuta taşınması hedeflenmelidir.

Hesap Verebilirlik: Denetim ve Kurumsal Sorumluluk

Hesap verebilirlik, şeffaflığın yaptırım gücüyle birleştiği noktadır.

- **Bağımsız Denetim:** Platform beyanlarının yılda en az bir kez bağımsız ve dış kuruluşlarca (Auditing) denetlenmesi, yerel düzenleyiciler (BTK¹⁹, KVKK²⁰, Rekabet Kurumu²¹) için de faydalıdır ve denetim gücünü artıracaktır.
- **Siber Dayanıklılık:** NIS2 ve Türkiye'nin Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2024-2028)²² doğrultusunda, kritik platform altyapılarının güvenliği ve veri ihlallerinin hızlı bildirimini kurumsal hesap verebilirliğin ayrılmaz bir parçası olacaktır.

Şeffaflığın Çok Katmanlı Yapısı ve Hesap Verebilirliğin Siyasal Boyutu

Dijital platform ekonomisinde şeffaflık, tek boyutlu bir kurumsal veri paylaşımı olmaktan çıkıp; **algoritmik şeffaflık, veri yönetimi şeffaflığı, içerik moderasyonu şeffaflığı, reklam şeffaflığı ve karar verme süreçlerinde prosedürel şeffaflık** gibi birbirini tamamlayan alt katmanlar üzerinden ele alınmalıdır. Bu çok katmanlı yapı, platformların yalnızca teknik birer aracı değil, bilginin yayılımını ve kamusal tartışmaları şekillendiren "yarı-kamusal rol" üstlenmiş aktörler olduğunu görünür kılmaktadır.

Bu bağlamda, platformların hesap verebilirliği yalnızca kurumsal uyum, standart raporlama veya teknik düzenleyici çerçeveye sınırlı tutulamaz. Devasa özel teknoloji şirketlerinin, kendi hizmet şartları ve algoritmik tercihleri eliyle milyarlarca kullanıcı için adeta "**kamusal norm ürettiği**" bir ekosistemde hesap verebilirliğin mutlaka bir siyasal/toplumsal boyutu da olmalıdır. Bir STK raporu vizyonu ile ele alındığında; platform iktidarının dengelenmesi, ancak **demokratik meşruiyetin** tesis edilmesi ve bu "özel regülatörlerin" eylemlerinin şeffaf bir **kamusal denetim** mekanizmasına tabi tutulmasıyla mümkündür.

Türkiye İçin Stratejik Önem ve Sonuç

Bu bölüm, Türkiye'nin dijital egemenlik vizyonu ile küresel serbest piyasa kuralları arasında bir köprü kurmayı amaçlar. Platform ekonomisinde güvenin tesisi; algoritmaların "açıklanabilir", kararların "itiraz edilebilir", verilerin "denetlenebilir" ve kullanıcıların da "korunabilir" olduğu bir ekosisteme bağlıdır. Bunun yanında, yerel mevzuatın AB, İngiltere ve OECD ile harmonizasyonunun, sadece yasal uyumu

¹⁹ **Bilgi Teknolojileri ve İletişim Kurumu (BTK) (2024).** Sosyal Ağ Sağlayıcıları Şeffaflık Raporları Analizi.

²⁰ **6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) (2016).** T.C. Resmi Gazete, 29677, 7 Nisan 2016.

²¹ **Rekabet Kurumu (2021).** Dijital Platformlar Hakkında Sektör Araştırması Ön Raporu.

²² **T.C. Cumhurbaşkanlığı (2024).** Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2024-2028) Hakkında 2024/11 Sayılı Genelge. T.C. Resmi Gazete, 32655, 7 Eylül 2024.

sağlayacağı değil, aynı zamanda dijital ekonomideki inovasyon kapasitesini ve kullanıcı sadakatini de artıracaklarını öngörmektedir. Önerilen model, Türkiye'nin dijital hizmet sağlayıcıları için öngörülebilir bir hukuki zemin oluştururken, vatandaşlar için daha güvenli bir dijital kamusal alan vaat etmektedir.

2.2. Genel Tanımlar

2.2.1. Arama Motorları

Arama motorları, günümüz dijital bilgi ekosisteminin temel yapı taşlarından biridir ve bu yönüyle çevrim içi bilgiye erişimin ana kapısı olarak, bir nevi dijital kamusal alanın fiili düzenleyicileri olmuştur. Günümüzdeki küresel internet trafiğinin %90'ından fazlası, halihazırda kullanılagelen ve aynı zamanda kullanıcıların bilgiye erişimini hızlandıran arama motorları aracılığıyla yönlendirilmektedir. Sadece Google, 2023–2024 dönemi dikkate alındığında, tek başına küresel arama pazarının yaklaşık %88–92'sini kontrol etmektedir²³. Haliyle bu durum sınırlı sayıda aktöre orantısız bir yapısal güç kazandırmaktadır.

Arama motorları, yapıları gereği algoritmalar aracılığıyla milyarlarca sayfa içeriğini analiz ederek karar verir. Ancak, bu karar süreçleri çoğu zaman kullanıcıların gözünde net olarak belli olmamakta ve sonuçların ***nasıl*** ve ***neden*** sıralandığı, ***hangi*** kriterlerin ağırlık taşıdığı ve ***ne tür*** verilerin kullanıldığı belirsizliğini korumaktadır. Bu sorular, yalnızca teknik değil; aynı zamanda hukuki, etik ve toplumsal bir mesele olarak ortada durmaktadır.

Ayrıca, arama motorları kapsamında; bilgiye erişimde görünmez yönlendirme, ticari sonuçlarla editoryal içeriğin iç içe geçmesi ve rekabet üzerinde dolaylı baskı gibi kritik risk alanlarından bahsedilebilir.

Bu ölçekte bir bilgi aracısının karar mekanizmaları; **şeffaflık**, **raporlama** ve **hesap verebilirlik** ilkeleri çerçevesinde değerlendirilmediği sürece, bilgiye erişimde yapısal asimetrliler ve riskler ortaya çıkabilmektedir.

Şeffaflık- Sayısal Göstergeler

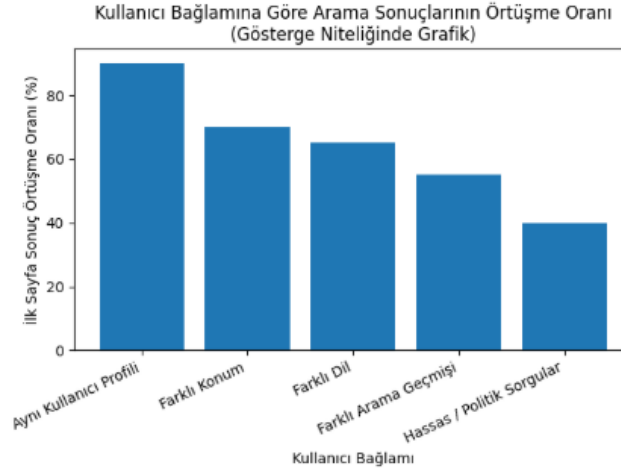
Mevcut uluslararası veriler, şeffaflığın sınırlı ve asimetrik olduğunu göstermektedir:

- Arama motorlarının **ayrı kullanıcı profillerine göre sonuçları nasıl uyarladığını deneysel olarak inceleyen güncel bir araştırma** (Damião ve ark., 2025)²⁴:
 - Google, DuckDuckGo ve Yahoo gibi arama motorlarında,
 - **aynı sorgu** için farklı kullanıcı konumları, dilleri ve geçmişleri kullanılarak,
 - tekrarlanmasını esas alan **audit (denetim) metodolojisi** de kullanılarak,
 - sonuç farklılaşmasının boyutunu ölçmeyi amaçlamıştır.

²³ Google (2024). *How Search Works: From algorithms to answers*. Google Search Central.

²⁴ Íris Damião, José M. Reis, Paulo Almeida, Nuno Santos, Joana Gonçalves-Sá (2025). *Digital Gatekeeping: An Audit of Search Engine Results shows tailoring of queries on the Israel-Palestine Conflict*.

Sözkonusu araştırma, diyalog ve politika açısından hassas konularda (ör. İsrail-Filistin çatışması gibi) arama sonuçlarının **kullanıcı konumu ve geçmişine göre anlamlı biçimde farklılaştığını** göstermiştir. Bu durum, klasik “tek tip arama sonucu” varsayımını sorgulayarak, **algoritmik kişiselleştirme ve konum temelli uyarlamanın arama sonuçlarını etkilediğini** ortaya koymaktadır.



Yukarıdaki grafikte de görüleceği üzere; kullanıcı bağlamı değiştikçe, özellikle hassas sorgularda, arama sonuçlarının benzerliği anlamlı bir biçimde düşmektedir. Bu grafik, güncel audit-temelli literatürden türetilmiş gösterge niteliğinde bir görselleştirmedir. Değerler, tek bir platforma değil; farklı çalışmalarda gözlemlenen eğilimlere dayalı aralıkları temsil etmektedir.

Bu akademik çalışma (Damião ve ark., 2025), eski veri setlerine dayanmayan, **2025 itibarıyla güncel davranışı** ölçen çalışmalardan biridir. Özellikle:

- Arama motorlarının **algoritmik özelleştirme / kişiselleştirme** pratiklerini,
- Farklı kullanıcı profillerine göre Arama Motoru Sonuçları Sayfası (**Search Engine Results Page - SERP**) varyasyonlarını,
- Politik açıdan hassas sorgularda bu etkilerin daha belirgin olduğunu

ampirik olarak ortaya koyar.

- Google, 2024 itibarıyla arama sonuçlarını etkileyen **200’den fazla sıralama parametresi** olduğunu belirtmekte; ancak bu sinyallerin yalnızca sınırlı bir kısmını (ör. PageRank, içerik alaka düzeyi, sayfa deneyimi) genel hatlarıyla açıklamaktadır.

Avrupa Birliği kapsamında; DSA standartları dikkate alındığında, çok büyük arama motorları (aylık ≥ 45 milyon kullanıcı, yani AB nüfusunun yaklaşık %10’u) sıralama parametrelerinin ana kategorilerini açıklamakla yükümlüdür.

Raporlama - Sayısal Veriler ve Uluslararası Uygulamalar

Google gibi büyük arama motorları kendi **Şeffaflık Raporları**’nı düzenli olarak yayımlamaktadır. Bu raporlar, kullanıcı verilerinin nasıl işlendiğini, hükümet talepleriyle ne kadar içerik kaldırıldığını veya ne tür içerik güvenlik önlemlerinin alındığını detaylandırmaktadır. Bu kapsamda; Google Transparency Report isimli şeffaflık raporları vasıtasıyla:

- Hükümetlerin talep ettiği kullanıcı verisi sayısı ve türü,
- Telif hakkı ihlallerine yönelik kaldırma talepleri,
- Güvenli tarama kapsamında tespit edilen kötü amaçlı site sayıları gibi istatistikleri paylaşır.

Bu raporların varlığı, şeffaflığın pratikte nasıl sayısal biçimde raporlanabileceğine dair önemli bir örnek teşkil etmektedir.

Google ve benzeri büyük arama motorlarının yayımladığı şeffaflık raporlarından öne çıkan bazı göstergeleri aşağıdaki şekilde görmek mümkündür:

- 2023 yılında dünya genelinde:
 - Başta telif hakkı ihlalleri olmak üzere; çeşitli yasal gerekçelerle **1,5 milyar’ı aşkın URL kaldırma talebinin**, platformların içerik politikaları ve uluslararası hukuk standartları dikkate alındığında, **yaklaşık %90’ı** “erişime engelleme” veya “indeksten çıkarma (de-indexing)” işlemleri ile sonuçlanmıştır.
 - Devlet mercileri tarafından teknoloji platformlarına iletilen **300.000’i aşkın kullanıcı verisi talebinin yaklaşık %70’i**, yasal dayanakların uygunluğu çerçevesinde “veri paylaşımı” yapılması ile sonuçlanmıştır.
- Güvenli tarama (Safe Browsing) sistemleri sayesinde:
 - Günlük ortalama **50.000–60.000** zararlı web sitesi tespit edilerek erişim engeli getirilmektedir.

Bu tür raporlar, arama motorlarının yalnızca teknik değil, **toplumsal etki üreten sistemler** olduğunu nicel olarak görünür kılmaktadır.

Avrupa Birliği tarafından 2024 başından itibaren yürürlüğe giren **DSA**, çevrim içi arama motorları ve platformlara yönelik *şeffaflık ve hesap verilebilirlik* kurallarını kapsamlı şekilde düzenlemektedir. DSA kapsamında “Very Large Online Search Engines” (VLOSE) tanımı, **ayda 45 milyonun üzerinde aktif kullanıcısı olan arama motorlarını** ifade eder. Bu aktörlere yönelik **raporlama ve açıklama yükümlülükleri** şöyle özetlenebilir:

- İçerik moderasyonu, risk değerlendirmesi ve kullanıcı etkileşimi gibi alanlarda raporların **en az altı ayda bir** kamuoyuna açıklanması gerekmektedir.
- Raporlar, ilgili topluluk dillerinde ve Avrupa Komisyonu’na sunulan denetim raporlarının kamuya açık özetlerini içermelidir.
- Arama motorları, aylık ortalama hizmet kullanıcısı sayısını ve risk değerlendirmesi sonuçlarını açıkça yayımlamalıdır.

Bu düzenleme, şeffaflığın hukuksal bağlamda sayısal verilerle nasıl birleştirilebileceğinin güncel bir örneğini sunmaktadır.

DSA tarafından zorunlu kılınan içerik moderasyonu raporları ve Gerekçe Beyanları (Statements of Reasons) gibi veri kayıtları, araştırmacılar tarafından da gerçekleştirilen çalışmalarda sayısal analizlere konu olmuştur. Örneğin; teknoloji devlerinin ilettiği verileri analiz eden bağımsız araştırma kurumlarınca, yaklaşık 2 aylık bir süre zarfında toplanan 150 milyondan fazla içerik moderasyonu kaydının incelendiği bir çalışmada²⁵, farklı platformlar arasındaki moderasyon frekansında **350 kata varan sapmalar** olduğu görülmüştür. Sadece bu çalışma bile raporlama ve hesap verilebilirlik standartlarının neden daha somutlaştırılması gerektiği hususunu istatistiklerle ortaya koymaktadır.

Hesap Verebilirlik- Akademik ve Uluslararası Sayısal Göstergeler

- Robert Epstein ve Ronald E. Robertson (2015) tarafından yapılan, "Search Engine Manipulation Effect (SEME)" yani "Arama Motoru Manipülasyon Etkisi" olarak adlandırılan ve arama motoru sıralamalarındaki taraflılığın kararsız seçmenler üzerindeki etkisini ölçen çalışmaya göre²⁶; arama sonuçlarının sıralamasının değiştirilmesi yoluyla belirli adayların veya ideolojilerin görünürliğünün artırılmasının:
 - **kararsız seçmenlerin oy verme tercihlerini %20 veya daha fazla oranda değiştirebildiğini,**
 - **bazı demografik gruplarda ve spesifik deney koşullarında ise bu değişim oranının %80'e kadar çıkabildiğini**bilimsel olarak kanıtlamıştır.
- DSA ile birlikte:
 - Kullanıcılar, arama sonuçlarının kaldırılmasına veya sıralama değişikliklerine karşı **itiraz mekanizmalarına** erişim hakkı kazanmaktadır.
 - Denetleyici kurumlar, yükümlülük ihlallerinde ve algoritmik risklerin yeterince azaltılmaması hâlinde **küresel cironun %6'sına kadar para cezası** uygulayabilmektedir.
- 2024 itibarıyla AB DSA'ya göre, büyük platformlara yönelik **20'den fazla sistemik risk soruşturması** başlatmıştır; bunların önemli bir kısmı arama ve öneri sistemleri ile ilgilidir.

Bu gelişmeler, hesap verebilirliğin artık gönüllü değil, **yaptırıma bağlı bir yönetim unsuru** hâline geldiğini göstermektedir.

²⁵ Hofmann, V., Murauer, L., & Bondorf, S. (2023). *Content moderation on social media in the EU: Insights from the DSA Transparency Database*. <https://doi.org/10.48550/arXiv.2312.04431>

²⁶ Epstein, R., & Robertson, R. E. (2015). "The search engine manipulation effect (SEME) and its possible impact on the outcomes of elections." *Proceedings of the National Academy of Sciences (PNAS)*, 112(33), E4512-E4521.

2.2.2. Sosyal Ağlar

Sosyal ağlar, bireylerin ve toplulukların dijital ortamda içerik oluşturmaya, paylaşmaya ve etkileşime girmesine olanak tanıyan web tabanlı platformlar olarak tanımlanabilir. Sözkonusu sosyal ağlar, geleneksel medyanın aksine bilginin tek bir merkezden yayıldığı bir yapıya değil, kullanıcıların hem tüketici hem de üretici olduğu dinamik bir yapıya sahiptir. Bu platformlar; kişisel profiller, bağlantı listeleri ve akış algoritmaları aracılığıyla toplumsal iletişimi zamandan ve mekandan bağımsız hale getirerek dijital kamusal alanın ana taşıyıcısı konumuna gelmiştir.

Sosyal ağlar, bireylerin bilgiye erişimini, kamusal tartışmaları ve siyasal katılım biçimlerini köklü biçimde dönüştürmüştür. Facebook, Instagram, X (Twitter), TikTok ve YouTube gibi platformlar, artık yalnızca özel şirketler değil; **kamusal alanın fiili altyapı sağlayıcıları** olarak işlev görmektedir. Bu dönüşüm, sosyal ağların nasıl çalıştığına, hangi içerikleri öne çıkardığına ve hangi kararları hangi gerekçelerle aldığına ilişkin soruları kaçınılmaz hâle getirmiştir.

Sosyal Ağlar kapsamında; algoritmik görünürlük ve içerik bastırma riskleri, dezenformasyonun yayılım hızı ve moderasyon kararlarında tutarsızlık ve şeffaflık eksikliği gibi kritik risk alanlarından bahsetmek mümkündür.

Günümüzde sosyal ağlar, yalnızca bireysel sosyalleşme araçları değil, aynı zamanda ekonomik ve politik süreçlerin yönetildiği devasa ekosistemlerdir. Reklam modelleri, veri madenciliği ve yapay zekâ tabanlı öneri sistemleri üzerine kurulu olan bu yapılar, bilginin yayılım hızını artırırken dezenformasyon, yankı odaları ve algoritmik ayrışma gibi sistemik riskleri de beraberinde getirmektedir. Bu karmaşık yapı, modern hukuk düzenlerinde şeffaflık ve hesap verebilirlik ilkeleri çerçevesinde regüle edilme ihtiyacını doğurmuş; platformların toplumsal sorumluluklarını belirleyen DSA ve 5651 sayılı Kanun²⁷ gibi yasal düzenlemelerin odağı haline gelmiştir.

Akademik literatürde sosyal ağlar sıklıkla “platform iktidarı”, “algoritmik yönetim” ve “özel aktörler eliyle kamusal düzenleme” kavramlarıyla ele alınmaktadır (Pasquale, 2015²⁸ ve Gillespie, 2018²⁹). İçerik sıralama, öneri sistemleri ve moderasyon kararları, kullanıcı davranışlarını doğrudan etkileyen **normatif sonuçlar** üretmektedir.

Araştırmalar, sosyal ağ algoritmalarının:

- Bilgi yankı odalarını güçlendirebildiğini,
- Yanlış ve zararlı içeriğin yayılımını hızlandırabildiğini,

²⁷ 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun (2007). *T.C. Resmî Gazete*, 26529, 23 Mayıs 2007.

²⁸ Pasquale, F. (2015). *The Black Box Society: The Secret Algorithms That Control Money and Information*. Harvard University Press.

²⁹ Gillespie, T. (2018). *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media*. Yale University Press.

- Kullanıcılar açısından öngörülemez ve açıklanamaz kararlar ürettiğini ortaya koymaktadır (Rieder et al., 2022)³⁰.

Bu bağlamda şeffaflık, raporlama ve hesap verebilirlik, yalnızca teknik gereklilikler değil; **demokratik meşruiyet araçları** olarak değerlendirilmektedir.

Şeffaflık: Sosyal Ağların Görünmez Karar Mekanizmaları

Şeffaflık, sosyal ağların algoritmik sıralama, içerik önerme ve moderasyon süreçlerine ilişkin temel bilgileri kamuoyuyla paylaşmasını ifade eder. Mevcut durumda büyük platformlar, algoritmalarının “ticari sır” niteliğini gerekçe göstererek sınırlı açıklama yapmaktadır.

- Küresel kullanıcıların yaklaşık %70’i, sosyal ağlarda gördüğü içeriğin neden karşısına çıktığını bilmediğini belirtmektedir (Pew Research Center, 2023)³¹.
- Algoritmik önerilerin, platformlardaki toplam izlenme süresinin %60–80’ini yönlendirdiği tahmin edilmektedir (Ricci, F., Rokach, L., & Shapira, B., 2021)³².

Bu durum, kullanıcı özerkliği ve bilinçli tercih hakkı açısından ciddi bir asimetri yaratmaktadır.

Özetle; sosyal ağlarda şeffaflık eksikliği, kullanıcıların değil platformların bilgi üstünlüğünü kurumsallaştırmaktadır.

Raporlama: İçerik Yönetiminin Ölçülebilirliği

Raporlama, sosyal ağların içerik kaldırma, hesap kapatma, reklam şeffaflığı ve devlet taleplerine ilişkin düzenli veri yayımlamasını kapsar. Meta³³, Google³⁴ ve TikTok³⁵ gibi şirketler periyodik şeffaflık raporları yayımlasa da bu raporlar **ülkeler arası karşılaştırmaya elverişli değildir**. 2023 verilerine göre;

- Meta platformlarında (Facebook ve Instagram) kaldırılan içerik birimi 20 milyarın üzerinde bir adete ulaşmıştır. Bu devasa hacim, dijital platformlar tarihindeki en yüksek yıllık moderasyon rakamlarından biri olarak kayda geçmiştir.

³⁰ Rieder, B. et al. (2022). Algorithmic influence on public discourse. *New Media & Society*.

³¹ Pew Research Center. (2023). *Understanding the Algorithmic Experience: How Users Perceive and Interact with Social Media Recommendation Systems*. Washington, D.C.

³² Ricci, F., Rokach, L., & Shapira, B. (2021). *Recommender Systems Handbook*. Springer.

³³ Meta. *Community Standards Enforcement Reports*.

³⁴ Google (çeşitli yıllar). *Transparency Report*.

³⁵ TikTok. *Transparency Report*.

- Herhangi bir kullanıcı şikâyeti olmaksızın, Meta'nın proaktif yapay zekâ ve makine öğrenmesi sistemleri tarafından tespit edilen ve ihlal içeren paylaşımların %95'inden fazlası etkisiz hale getirilmiştir.
- Dünya genelinde hükümetler ve adli makamlarca iletilen içerik kısıtlama ve veri talebi talepleri 1 milyon sınırına yaklaşmıştır. Bu durum, devletlerin dijital alan üzerindeki denetim ve yasal müdahale arayışının küresel çapta arttığını göstermektedir.

Türkiye özelinde ise bu verilerin ayrıntı düzeyi oldukça sınırlıdır. Kısaca, standartlaştırılmamış raporlama, düzenleyici denetimi zayıflatmaktadır.

Hesap Verebilirlik: Kararların Sonuçlarından Kim Sorumlu?

Hesap verebilirlik, sosyal ağların aldığı kararlar nedeniyle ortaya çıkan toplumsal, hukuki ve bireysel sonuçlar için **itiraz, denetim ve yaptırım mekanizmalarının** varlığını ifade eder.

Roberts (2019), *Behind the Screen* adlı çalışmasına göre³⁶, kullanıcıların içerik kaldırma veya hesap askıya alma kararlarına karşı etkili başvuru yollarına sahip olmadığını göstermektedir. Örneğin:

- İtirazların %60–70'i otomatik sistemler tarafından yeniden değerlendirilmektedir.
- İnsan denetimine ulaşabilen başvurular oldukça sınırlı sayıdadır.

2.2.3. E-Ticaret

E-ticaret platformları, alıcı ve satıcıların fiziksel olarak bir araya gelmesine gerek kalmadan mal ve hizmet takasını gerçekleştirdikleri dijital pazar yerleridir. Geleneksel perakendecilikten farklı olarak bu platformlar, geniş ürün yelpazesine anlık erişim, fiyat karşılaştırma imkanı ve 7/24 alışveriş kolaylığı sağlayarak küresel ticaretin çehresini değiştirmiştir. Günümüzde e-ticaret, sadece bir satış kanalı değil; lojistik, ödeme sistemleri ve veri analitiğinin entegre olduğu karmaşık bir teknolojik ekosistem olarak tanımlanmaktadır. Bu yapılar, özellikle "Pazar Yeri" (Marketplace) modeliyle küçük işletmelerin küresel pazarlara açılmasına aracılık ederek dijital ekonominin büyümesinde lokomotif görevi üstlenmektedir.

Bu platformların işleyişi, arka planda çalışan sofistike algoritmalar ve devasa veri tabanları tarafından yönetilir. Kişiselleştirilmiş öneri sistemleri, dinamik fiyatlandırma araçları ve kullanıcı yorumları gibi bileşenler, tüketici davranışlarını şekillendiren temel unsurlardır. Ancak bu devasa ekonomik güç, beraberinde adil rekabetin korunması, sahte ürünlerle mücadele ve tüketici verilerinin güvenliği gibi kritik sorumlulukları da getirmektedir. Bu nedenle, Avrupa Birliği'nin Dijital Pazarlar Yasası (DMA) ve Türkiye'nin 6563 sayılı Elektronik Ticaret Kanunu³⁷ gibi düzenlemeler, platformların "geçit (kapı) bekçisi"

³⁶ Roberts, S. T. (2019). *Behind the Screen: Content Moderation in the Shadows of Social Media*. Yale University Press.

³⁷ 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun (2014). *T.C. Resmî Gazete*, 29168, 7 Kasım 2014.

(gatekeeper) rollerini denetleyerek piyasada şeffaf, güvenli ve rekabetçi bir yapının sürdürülebilirliğini hedeflemektedir.

E-ticaret platformları, ürün ve hizmetlerin sunumundan fiyat oluşumuna, satıcı-tüketici ilişkilerinden lojistik süreçlere kadar geniş bir ekonomik ekosistemi yönetmektedir. Amazon, Trendyol, Hepsiburada, Alibaba ve benzeri platformlar, artık yalnızca aracılık eden pazar yerleri değil; **piyasa davranışlarını şekillendiren dijital altyapılar** hâline gelmiştir.

Bu dönüşüm, e-ticaret platformlarının algoritmik sıralama, dinamik fiyatlama, satıcı performans değerlendirmesi ve tüketici yönlendirme mekanizmalarının ne ölçüde şeffaf, denetlenebilir ve hesap verebilir olduğu sorusunu gündeme getirmektedir. Ayrıca, e-ticaret platformları kapsamında; ürün sıralamasında sıralama, dinamik fiyatlama ve komisyon şeffaflığı eksikliği ve satıcı-platform güç asimetrisi gibi kritik risk alanlarından bahsetmek mümkündür.

Akademik literatürde e-ticaret platformları; "platform ekonomisi", "algoritmik piyasa tasarımı" ve "özel aktörler eliyle rekabet düzenlemesi" kavramları çerçevesinde ele alınmaktadır (Rochet & Tirole, 2003³⁸ ve Pasquale, 2015³⁹). Platformların ürün sıralama ve tavsiye algoritmaları, tüketici tercihlerini ve satıcıların piyasa görünürlüğünü doğrudan etkilemektedir.

Araştırmalar (Khan, 2017⁴⁰ ve Ezrachi & Stucke, 2020⁴¹), e-ticaret algoritmalarının:

- Fiyat ayrımcılığını güçlendirebildiğini,
- Platform içi kendi ürünlerini kayırma riskleri doğurduğunu,
- Küçük ve orta ölçekli satıcılar açısından öngörülemez sonuçlar üretebildiğini ortaya koymaktadır.

Şeffaflık- Sayısal Göstergeler

- Tüketicilerin %65'ten fazlası, bir ürünün neden üst sıralarda gösterildiğini bilmediğini ifade etmektedir (AB Eurobarometer, 2023)⁴².
- Büyük platformlarda satışların yaklaşık %70'i, ilk sayfada listelenen ürünlerden gerçekleşmektedir (Feedvisor, 2022⁴³ ve Brynjolfsson, E., Hu, Y. J., & Rahman, M. S., 2013⁴⁴).

³⁸ Rochet, J.-C., & Tirole, J. (2003). Platform competition. *Journal of the European Economic Association*.

³⁹ Pasquale, F. (2015). *A.g.e.*

⁴⁰ Khan, L. (2017). Amazon's antitrust paradox. *Yale Law Journal*.

⁴¹ Ezrachi, A., & Stucke, M. (2020). *Virtual Competition*. Harvard University Press.

⁴² European Commission. (2023). *Eurobarometer 535: Online platforms and consumer protection*. Directorate-General for Communication

⁴³ Feedvisor (2022). *The Amazon Consumer Behavior Report: Inside the minds of consumers and their purchasing habits*.

⁴⁴ Brynjolfsson, E., Hu, Y. J., & Rahman, M. S. (2013). "Competing in the Age of Omnichannel Retailing." *MIT Sloan Management Review*.

- Sponsorlu ürünlerin, organik sıralamalara kıyasla tıklanma oranını %30–50 artırdığı tahmin edilmektedir (Jungle Scout, 2023⁴⁵ ve Ghoshal, A., & Mukhopadhyay, T., 2022⁴⁶).

Özetle; şeffaf olmayan sıralama ve fiyatlama sistemleri hem tüketici refahını hem de satıcılar arası adil rekabeti zedeleyebilmektedir.

Raporlama: Pazar Yeri Faaliyetlerinin Ölçülebilirliği

Raporlama, e-ticaret platformlarının işlem hacmi, satıcı–platform ilişkileri, şikâyet ve iade süreçleri ile kamu otoritelerinden gelen taleplere ilişkin düzenli veri yayımlamasını ifade eder. Küresel ölçekte raporlama uygulamaları platformdan platforma büyük farklılıklar göstermektedir.

Sayısal Göstergeler

- Küresel e-ticaret hacmi 2023 itibarıyla 6 trilyon ABD dolarını aşmıştır (Insider Intelligence / eMarketer., 2023)⁴⁷.
- Büyük platformlarda iade oranları %20–30 aralığındadır (National Retail Federation (NRF) & Appriss Retail, 2023)⁴⁸.
- Satıcı şikâyetlerinin %50’den fazlası, sıralama ve komisyon politikalarıyla ilgilidir (AB Raporu 2020, *Impact Assessment on the Observatory on the Online Platform Economy*)⁴⁹.

Türkiye özelinde bu verilerin çoğu kamuya açık ve standartlaştırılmış değildir. Standart raporlama eksikliği sebebiyle, düzenleyici denetimi ve politika tasarımı da zorlaşmaktadır.

2.3. Şeffaflık (Algoritmik Öngörülebilirlik, Bilgilendirme ve Güven İnşası)

Dijital platformların sosyo-ekonomik hayatın içine girmesi ve hatta merkezine yerleşmesi ile bu yapıların nasıl karar verdiğine dair "anamlı bir şeffaflık" (meaningful transparency) talebi ortaya çıkmıştır. Literatürde "**Algoritmik Yönetişim**" (Algorithmic Governance) olarak adlandırılan bu süreç; platformların sadece teknik kodlardan ibaret olmadığını, aksine toplumsal değerleri ve piyasa dengelerini şekillendiren politik aktörler olduğunu savunur (Gillespie, 2018)⁵⁰.

⁴⁵ **Jungle Scout.** (2023). *Amazon Advertising Report: Key Trends and Benchmarks for E-commerce Sellers.*

⁴⁶ **Ghoshal, A., & Mukhopadhyay, T. (2022).** "Impact of Sponsored Search on Organic Results and Total Clicks in E-commerce." *Management Science & Information Systems.*

⁴⁷ **Insider Intelligence / eMarketer (2023).** *Worldwide Ecommerce Forecasts 2023: Global Retail Sales and Market Share.*

⁴⁸ **National Retail Federation (NRF) & Appriss Retail (2023).** *2023 Retail Returns Survey: A Year-End Analysis.*

⁴⁹ **European Commission (2020).** *Impact Assessment on the Observatory on the Online Platform Economy*

⁵⁰ **Gillespie, T. (2018).** *A.g.e.*

Şeffaflık, aynı zamanda modern dijital yönetişimin temel taşıdır. Pasquale (2015) tarafından kavramsallaştırılan "**Kara Kutu Toplumu**" (**The Black Box Society**) riski; platformların, “neye inanacağımız”, “neyi satın alacağımız” ve kiminle etkileşime gireceğimiz” gibi kararları -bir nevi bizim yerimize- kapalı kapılar ardında vermesinden kaynaklanmaktadır⁵¹.

Bu bölümde; şeffaflık olgusu, arama motorları, sosyal ağlar ve e-ticaret platformları özelinde, AB’nin **DSA**, **DMA** ve **AI Act** normları çerçevesinde akademik bir perspektifle detaylandırılmaktadır.

Algoritmik Sıralama ve Öneri Sistemlerinde Şeffaflık

Algoritmik şeffaflık, platformun bir içeriği diğerlerinin önüne çıkarma gerekçelerini açıklama kapasitesidir. Buna ilaveten algoritmik şeffaflık, aynı zamanda, bir platformun kullanıcıya sunduğu içeriği hangi kriterlere göre seçtiğini, sıraladığını ve önceliklendirdiğini açıklama yükümlülüğüdür.

AB Dijital Hizmetler Yasası (DSA) Madde 27, platformların "ana parametreleri" açıklaması gerektiğini açıkça belirtir⁵². Buna ilaveten; Ananny & Crawford’ın 2018 tarihli çalışmasında, sadece kodun paylaşılmasının yeterli olmadığı, "**ilişkisel şeffaflığın**" yani algoritmanın kullanıcı üzerindeki etkisinin açıklanması gerektiği savunulur⁵³. Diakopoulos’un 2016 tarihli çalışmasında ise, algoritmik kararların "insan hayatını etkileyen gizli mantıklar" içerdiğini belirterek, bu mantığın kamusal denetime açılması gerektiğini savunur⁵⁴.

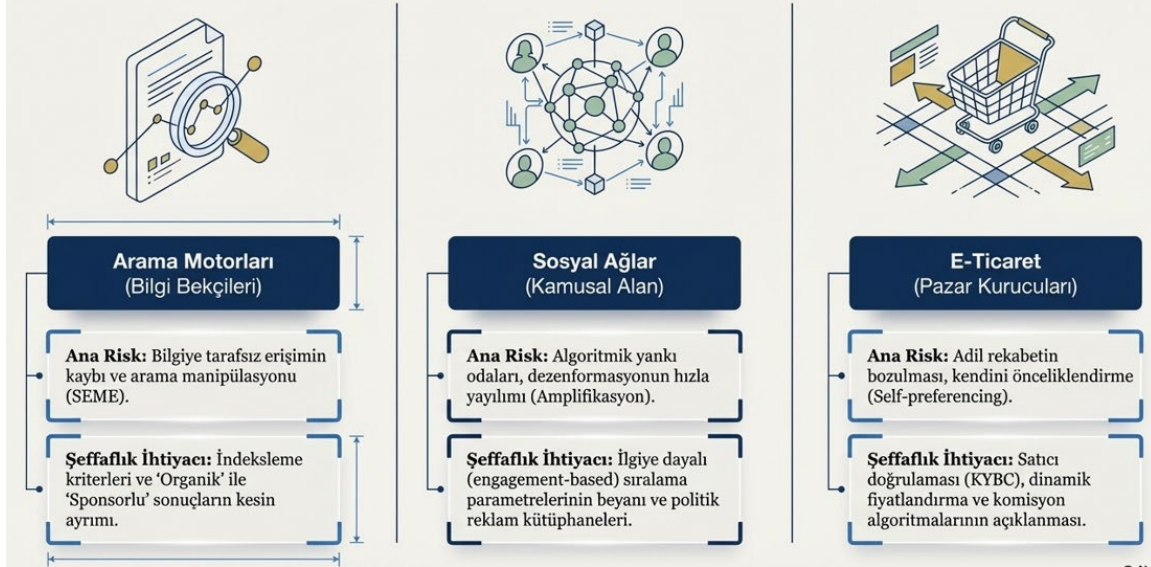
⁵¹ Pasquale, F. (2015). *A.g.e.*

⁵² DSA (Digital Services Act), European Union (2022). *A.g.e.*

⁵³ Ananny, M., & Crawford, K. (2018). "Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability." *New Media & Society*.

⁵⁴ Diakopoulos, N. (2016). "Algorithmic Accountability: Journalistic investigation of computational power structures." *Digital Journalism*.

Şeffaflığın Çok Katmanlı Anatomisi: Sektörel Risk Haritası



ŞEKİL 2-1: Şeffaflık Anatomisi (YZ ile hazırlanmıştır)

2.3.1. Arama Motorları: İndeksleme, Otorite ve Bilgiye Erişim

Arama motorları, bilginin "geçit (kapı) bekçileri"dir (gatekeepers). Şeffaflık burada iki kolda incelenir:

- **Sıralama Parametreleri:** Google'ın "Arama Nasıl Çalışır?" dokümantasyonunda (2024) belirttiği gibi; alaka düzeyi (relevance), kaynak otoritesi (authority) ve kullanılabilirlik temel kriterlerdir⁵⁵. Introna & Nissenbaum 2000 tarihli çalışması, arama motorlarının tarafsız olmadığını, "teknolojik bir siyaset" yürüttüğünü savunur⁵⁶. Bu nedenle, **ücretli içeriklerin (paid results)** organik sonuçlardan görsel ve yapısal olarak kesin bir şekilde ayrıştırılması, öngörülebilirlik açısından kritiktir.
- **Manipülasyonun Önlenmesi:** Arama motoru algoritmalarının manipülatif SEO gibi tekniklerle kötüye kullanımı maalesef mümkündür. Bunu engellemeye yönelik denetim mekanizmalarının şeffaf bir çerçevede sunulması ile etik kurallara uyan işletmelerin dijital görünürlüğü korunmuş olacak ve bunun sonucunda da pazarın rekabet koşulları daha çok öngörülebilir bir hale gelecektir.

Bunun yanı sıra, arama motorları bilginin hiyerarşisini belirleyen modern kütüphanecilerdir. Ancak bu kütüphanecilerin "tarafsızlığı" akademik dünyada yoğun tartışma konusudur.

- **Ana Parametrelerin Beyanı:** DSA Madde 27 uyarınca, arama motorları sıralamayı etkileyen en önemli parametreleri (anahtar kelime uyumu, sayfa otoritesi (page authority), yerellik, güncellik, vb.) kullanıcıya açıklamalıdır.

⁵⁵ Google (2024). *A.g.e.*

⁵⁶ Introna, L. D., & Nissenbaum, H. (2000). "Shaping the Web: Why the Politics of Search Engines Matters." *The Information Society*, 16(3), 169-185.

- **Arama Taraflılığı (Search Bias):** Noble (2018), *Algorithms of Oppression (Baskı Algoritmaları)* adlı çalışmasında, arama motorlarının veri setlerindeki önyargıları nasıl yeniden ürettiğini ortaya koymuştur. Bu nedenle şeffaflık, sadece "hangi parametrelerin kullanıldığını" değil, bu parametrelerin nasıl "denetlendiğini" de kapsamalıdır⁵⁷. Bu konudaki bir başka akademik ifade "Algoritmalar, denklemlere gömülmüş görüşlerdir." (Cathy O'Neil, 2016)⁵⁸
- **Ticari ve Organik Ayrımı:** DMA kapsamında, "Gatekeeper" statüsündeki arama motorlarının kendi yan hizmetlerini (Örn: Google Uçuşlar) organik arama sonuçlarında haksız şekilde öne çıkarması (self-preferencing) yasaklanmıştır. Bu, pazar öngörülebilirliği için hayati bir şeffaflık normudur.

2.3.2. Sosyal Ağlar: Etkileşim Ekonomisi ve Psikolojik Etkiler

Sosyal ağlardaki şeffaflık, içeriğin yayılım hızını belirleyen "etkileşim odaklı" algoritmaların deşifre edilmesiyle ilgilidir.

- **Kişiselleştirme ve Yankı Odaları:** Sunstein (2017), algoritmaların kullanıcıyı sadece kendi görüşlerini destekleyen içeriklerle sarmaladığı "Yankı Odaları" (Echo Chambers) riskine dikkat çeker⁵⁹. Şeffaflık, kullanıcıya "neden bu içerik?" sorusunun cevabını sadece teknik bir dille değil, aynı zamanda anlaşılır bir dille sunmalıdır.
- **Öneri Sistemlerinde AI Act Uyum:** AI Act, yapay zekâ sistemlerinin şeffaflığına vurgu yapar. Sosyal ağların öneri sistemleri, kullanıcının ruh sağlığı veya demokratik seçim süreci üzerinde sistemik risk oluşturuyorsa, bu algoritmaların "açıklanabilir yapay zekâ" (XAI) prensiplerine uygun olması beklenir.

Sosyal ağlardaki şeffaflık sorunu, "ilgiye dayalı sıralama" (engagement-based ranking) modelinden doğar.

- **Haber Akışı (Feed) Algoritmaları:** Kullanıcının geçmiş davranışları, konum verisi ve ağındaki kişilerin aktiviteleri sıralamayı belirlemektedir. Literatürde bu durumun "**Filtre Balonları**" (Filter Bubbles) yarattığına dair geniş bir mutabakat vardır (Pariser, 2011)⁶⁰.
- **Öngörülebilirlik Gereksinimi:** Kullanıcıya "Neden bu gönderiyi görüyorum?" (Why am I seeing this post?) seçeneği sunulması, şeffaflığın bireysel düzeyde hayata geçirilmesidir. Sosyal ağlar, algoritmalarının toplumsal kutuplaşma üzerindeki etkilerini "Risk Değerlendirme" raporlarında beyan etmekle yükümlüdür.

⁵⁷ Noble, S. U. (2018). *Algorithms of Oppression: How Search Engines Reinforce Racism*. NYU Press.

⁵⁸ O'Neil, C. (2016). *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. Crown.

⁵⁹ Sunstein, C. R. (2017). *#Republic: Divided Democracy in the Age of Social Media*. Princeton University Press.

⁶⁰ Pariser, E. (2011). *The Filter Bubble: What the Internet Is Hiding from You*. Penguin Press.

2.3.3. E-Ticaret Platformları: Fiyatlandırma ve Güvenli Ticaret

E-ticaret platformlarında şeffaflık; tüketicinin korunması, tüketicinin doğrudan cüzdanı ve satıcılar arası adil rekabet ile ilgilidir.

- **Sıralama ve Satıcı Şeffaflığı:** Ürünlerin neden "en çok satan" veya "tavsiye edilen" olarak etiketlendiği açıklanmalıdır. Komisyon ödeyen satıcıların öne çıkarılması durumunda, bu durum "reklam" veya "sponsorlu" ibaresiyle netleştirilmelidir.
- **Dinamik Fiyatlandırma Algoritmaları:** Kullanıcının tarayıcı geçmişine veya cihazına göre fiyatın değişip değişmediği (fiyat ayrımcılığı), şeffaflık raporlarının en kritik başlıklarından biridir.
- **"En İyi Eşleşme" ve "Buy Box" Dinamikleri:** Bir ürünün neden listenin başında yer aldığı (stok durumu, kargo hızı, komisyon oranı vb.) beyan edilmelidir. DMA (Dijital Pazarlar Yasası), platform sahibinin kendi markalı ürünlerini (self-preferencing) haksız şekilde öne çıkarmasını yasaklar.
- **Satıcı Puanlama ve Yorum Şeffaflığı:** Sahte yorumların (fake reviews) elenmesi için kullanılan algoritmaların etkinliği, e-ticarete olan güvenin temelidir.

2.4. Reklam ve Gelir Modellerinin Beyanı

Dijital platformların temel gelir kaynağı olan reklam modelleri, kullanıcı verisinin metalaştırılması üzerine kuruludur. Dijital platformların pek çoğu "ücretsiz" hizmet karşılığında kullanıcı verisini paraya dönüştüren (data-for-service) bir modelle çalışır. Zuboff'un (2019) "**Gözetim Kapitalizmi**" olarak tanımladığı bu süreçte şeffaflık, verinin nasıl metalaştırıldığına açıklanmasını gerektirir⁶¹. Ayrıca, kullanıcıların davranışsal verilerinin onların rızası ve bilgisi dışında "davranışsal artık" olarak işlendiğini savunur.

Arama motorlarında ana gelir kalemi, anahtar kelime bazlı açık artırmalar yoluyla sunulan sponsorlu sonuçlardan oluşmaktadır. Bu içerikler çoğu zaman organik arama sonuçlarıyla benzer biçimde sunulmakta ve kullanıcılar açısından ayrıştırılması güçleşmektedir.

Bu gelir modellerinin ortak özelliği; **kullanıcılar, satıcılar ve kamu otoriteleri açısından sınırlı şeffaflıkla işletilmesidir**. Reklamın ve ticari önceliklendirmelerin algoritmik sıralama üzerindeki etkisi çoğu zaman açıkça beyan edilmemekte; platformların toplam gelirleri içinde reklamın payı, ülke bazlı kırımlar ve sektörler göre dağılımlar gibi bilgiler kamuoyuyla paylaşılmamaktadır. Bu durum hem rekabet hukuku hem de tüketicinin bilgilendirilmesi ilkeleri açısından yapısal bir asimetri yaratmaktadır. Bu nedenle dijital platformlardan, reklam ve gelir modellerine ilişkin **açık, karşılaştırılabilir ve ülke bazlı beyan yükümlülükleri** talep edilmesi; dijital piyasalarda şeffaflık ve hesap verebilirliğin temel önkoşullarından biri olarak değerlendirilmektedir.

⁶¹ Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs.

2.4.1. Gelir Kaynakları ve Veri İlişkisi

Platformlar, yıllık şeffaflık raporlarında gelirlerinin ne kadarının doğrudan reklam ne kadarının veri satışı veya abonelik modellerinden geldiğini ve hangi veri setlerinin (konum, ilgi alanları, üçüncü taraf çerezler) reklam hedeflemesinde kullanıldığını beyan etmelidir. Böylece, kullanıcı "ürün mü öncelikli yoksa müşteri mi" hususunu anlayabilecektir.

Reklam Hedefleme Parametreleri

Kullanıcılara neden belirli bir reklamın gösterildiğine dair (mikro-hedefleme) detaylı bilgi verilmelidir.

- **Kısıtlamalar:** AB AI Act ve GDPR, hassas veriler (etnik köken, siyasi görüş, cinsel yönelim) üzerinden profil oluşturulmasını ve reklam hedeflemesini katı kurallara bağlar.
- **Karanlık Tasarımlar (Dark Patterns):** Kullanıcıyı daha fazla veri paylaşmaya veya istemediği bir aboneliği veya gerçekten ihtiyacı olmayan ürünü satın almaya iten arayüz tasarımları, DSA tarafından yasaklanmıştır. Şeffaflık, arayüzün dürüstlüğü de kapsar.
- **Şeffaflık Araçları:** Reklamın üzerindeki "bilgi ikonu" aracılığıyla, reklamverenin kimliği ve hedefleme kriterleri (örn: "30-40 yaş arası, İstanbul'da yaşayan kadınlar") açıklanmalıdır.

2.4.2. Politik ve Kamusal Reklam Arşivleri: Demokratik Denetim

Dijital platformlar, politik ve kamusal reklamların dijital kamusal alandaki dolaşımında yapısal bir rol üstlenmektedir. Avrupa Birliği'nde Digital Services Act (DSA) başta olmak üzere Avrupa Konseyi⁶² ve Venedik Komisyonu (Resmî adıyla: Avrupa Hukuk Yoluyla Demokrasi Komisyonu)⁶³ tarafından geliştirilen ilkeler, politik reklamların şeffaflığına özel önem atfetmekte; reklamveren kimliği, finansman kaynağı, hedefleme kriterleri ve kampanya süresi gibi bilgilerin kamuya açık biçimde beyan edilmesini demokratik bütünlüğün temel unsurları arasında değerlendirmektedir. Arama motorlarında anahtar kelime bazlı politik reklamlar, bilgiye erişimi dolaylı biçimde yönlendirmektedir.

Demokratik süreçlerin korunması adına, politik reklamlar ticari reklamlardan farklı bir şeffaflık rejimine tabidir. Bu alan, OECD'nin "Dijital Demokraside Dürüstlük" ilkeleriyle birebir örtüşür. 2016 ABD seçimleri ve Cambridge Analytica skandalı, bu alandaki şeffaflık eksikliğinin ne tür krizlere yol açabileceğini ve AB'ni DSA ile DMA kural ve standartlarının bir an evvel oluşturulması ve hayata geçirilmesi hususunda harekete geçmesine yol açmıştır.

Reklam Kütüphaneleri (Ad Repositories)

⁶² Council of Europe. (2020) *Guidelines on Algorithmic Systems and Human Rights*.

⁶³ Venice Commission (2020). *Principles for a Fundamental Rights-compliant Use of Digital Technologies in Electoral Processes*. Council of Europe, Study No. 949/2019.

Meta Ad Library ve benzeri kütüphaneler, bağımsız araştırmacıların seçim manipülasyonlarını tespit etmesine olanak tanır. "Anlamlı şeffaflık", bu verilerin API'lar aracılığıyla dış denetime açılmasını gerektirir.

DSA Madde 39 uyarınca, Çok Büyük Çevrim İçi Platformlar (VLOPs), tüm reklamlarını içeren, aranabilir bir arşivi en az bir yıl boyunca kamuoyuna açık tutmalıdır. Bu arşiv rahatlıkla arama yapılabilir olmalı ve şunları içermelidir:

- Reklamın içeriği ve görseli.
- Reklamı veren gerçek veya tüzel kişinin adı.
- Reklam için harcanan toplam tutar.
- Yaş, bölge, siyasi eğilim gibi mikro-hedefleme kriterleri kullanılarak erişilen kullanıcı sayısı ve demografik kırılım (yaş, cinsiyet, bölge).

Örnek olarak AB yayınladığı bir duyuruda, TikTok'un reklam veritabanının, kamuoyunun bu bilgilere dayanarak reklamları kapsamlı bir şekilde aramasını sağlamadığını ve bunun da aracın kullanılışlığını sınırladığını ortaya koymaktadır⁶⁴.

2.4.3. Dezenformasyonla Mücadele ve Finansal Şeffaflık

Politik reklamların kim tarafından finanse edildiği (kara para: dark money) seçim manipülasyonlarını önlemek için hayati önemdedir. Benkler ve arkadaşlarının 2018'deki çalışması, şeffaf olmayan dijital reklamların "bilgi karmaşası" (information disorder) yarattığını kanıtlamaktadır⁶⁵. Kamuoyuna açık arşivler, gazetecilerin ve sivil toplum kuruluşlarının (STK) denetim yapmasına olanak tanımaktadır.

Risk Temelli ve Orantılı Yaklaşım

Şeffaflık sadece yazılı beyan değil aynı zamanda görsel bir sunumdur. Tasarımın kullanıcıyı yanıltmaması (örneğin; abonelikten çıkma butonunu saklamak veya kullanıcıyı onay vermeye zorlamak) "tasarımsal şeffaflık" kapsamında değerlendirilir.

- **Bilişsel Yük ve Şeffaflık:** Kullanıcıya sunulan bilginin karmaşıklığı şeffaflığı etkisiz kılabilir. Buna şeffaflık paradoksu (transparency paradox) denir. Burada, "katmanlı şeffaflık" (layered transparency) yaklaşımıyla, en kritik bilgi en basit haliyle ilk aşamada sunulmalıdır.

Şeffaflık sadece bir kavram olarak ele alınmamalıdır, zira şeffaflık aynı zamanda **risk odaklı** bir süreçtir.

- **VLOPs:** Çok Büyük Çevrim İçi Platformlar, toplumsal etkileri nedeniyle, küçük ölçekli bir e-ticaret sitesine göre çok daha ağır şeffaflık yükümlülüklerine tabidir.

⁶⁴ **European Commission (2025).** *Commission preliminarily finds TikTok's ad repository in breach of the Digital Services Act*, <https://digital-strategy.ec.europa.eu/en/news/commission-preliminarily-finds-tiktoks-ad-repository-breach-digital-services-act>

⁶⁵ **Benkler, Y., Faris, R., & Roberts, H. (2018).** *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*. Oxford University Press.

- **Ticari Sır vs. Şeffaflık:** Literatürde "Şeffaflık Paradoksu" olarak bilinen durum; tüm algoritmik detayların paylaşılmasının rakiplere avantaj sağlayabileceği veya kötü niyetli kişiler tarafından algoritmanın manipüle edilmesine (gaming the system) yol açabileceği uyarısını yapar. Bu nedenle rapor, "stratejik şeffaflığı" esas almalıdır.

Zelnick ve West (2021), veri simsarlığı (data brokerage) ekosistemini inceledikleri çalışmalarında, şeffaflığın algoritmik sistemlerin denetlenmesinde neden yetersiz bir çözüm olduğunu çarpıcı bir biçimde ortaya koyar⁶⁶. Buna göre, şeffaflık genellikle "bilgi ifşası" (disclosure) ile karıştırılmakta; ancak devasa veri ağlarının karmaşıklığı ve bu verilerin sürekli olarak yeniden paketlenip satılması, kullanıcıların veya denetçilerin veri akışını tam olarak kavramasını imkânsız hale getirmektedir.

Ayrıca, şeffaflık aslında bir "asimetri kalkanı" olarak da işlev görebilir: Şirketler yasal gereklilikleri yerine getirmek adına teknik detaylar paylaşırsalar da bu durum sistemin asıl işleyiş mantığını gizlemeye devam eder. Sonuç olarak, şeffaflığın tek başına yapısal bir hesap verebilirlik sağlamadığını, aksine gizlilik ihlallerinin sorumluluğunu kurumlardan alıp karmaşık politikaları anlaması beklenen bireylere yüklemektedir.

Bölüm Özeti ve Risk Temelli Değerlendirme

Şeffaflık, bir platformun büyüklüğü ve toplumsal etkisiyle orantılı olmalıdır. Bir e-ticaret sitesinin "indirim algoritması" şeffaflığı ile bir sosyal ağın "siyasi haber sıralama" şeffaflığı aynı risk kategorisinde değildir. AB normları (DSA ve DMA), bu ayrımı "**sistemik risk**" kavramı üzerinden yapar⁶⁷. Eğer bir algoritma, toplumsal huzuru veya demokratik seçimleri etkileyebiliyorsa, şeffaflık yükümlülüğü en üst düzeye çıkarılmalıdır.

2.5. Raporlama (Operasyonel Veri Setleri, İstatistiksel Beyan ve Denetlenebilirlik)

Raporlama, şeffaflık ilkesinin uygulama safhası olarak ele alınmaktadır. Platformların faaliyetlerini periyodik dökümler halinde kamuoyuna ve düzenleyici kurumlara sunması, "bilgi asimetrisini" (information asymmetry) azaltmanın en etkili yoludur.

Crawford ve Gillespie (2016), platformların sunduğu raporların sadece "ham veri" olmadığını, bu verilerin nasıl seçilip sunulduğunun başlı başına bir politika tercihi olduğunu savunur⁶⁸. Raporlama süreci, dijital platformların toplumsal sorumluluklarını rakamlar üzerinden meşrulaştırdığı bir arenadır⁶⁹. Helberger (2020), platformların sunduğu raporların genellikle "şirket lehine seçilmiş gerçekler" olduğunu savunarak,

⁶⁶ Zelnick, S., & West, S. M. (2021). "The Limits of Transparency: Data Brokerage and the Privacy of Algorithmic Systems." *New Media & Society*.

⁶⁷ European Commission (2023). *Guidelines on the implementation of risk assessments under the DSA*.

⁶⁸ Crawford, K., & Gillespie, T. (2016). "What is a Data Set?". *Social Media + Society*.

⁶⁹ Van Dijck, J., Poell, T., & De Waal, M. (2018). *The Platform Society: Public Values in a Connective World*. Oxford University Press. (Kamu değerleri ve raporlama zorunluluğu).

bağımsız akademik erişimin ve standartlaştırılmış raporlama şablonlarının önemini vurgular⁷⁰. Bu kısım, raporlamanın operasyonel dökümlerini dört ana katmanda derinleştirmektedir.

2.5.1. İçerik Moderasyonu ve Operasyonel Raporlama

İçerik moderasyonu, platformların dijital kamusal alanı nasıl şekillendirdiğinin sayısal kanıtıdır. AB DSA (Madde 15 ve 24), platformların içerik moderasyonu faaliyetlerine ilişkin kapsamlı raporlar yayınlamasını zorunlu kılar. Platformlar genellikle kaldırdıkları içerik sayısını verirler ancak bu içeriğin hangi "bağlamda" (context) kaldırıldığına dair veri sunmakta direnirler.

- **Hata Payı ve Duyarlılık Analizi:** Literatürde "The False Positive Problem" olarak bilinen olgu, hiciv veya gazetecilik faaliyeti gibi meşru içeriklerin yanlışlıkla kaldırılmasını kapsar. Genişletilmiş raporlama; sadece kaldırılan sayıları değil, "**karar kesinlik skorlarını**" (confidence scores) ve manuel denetimden geçen vakaların oranını da içermelidir.
- **Arama Motorlarında Görünürlük Kaybı, Gölge Yasaklama (Shadow Banning):** Şeffaflık raporları sadece "kaldırılan" içerikleri değil, sıralamada yapay olarak geriye itilen (demoted) veya arama önerilerinden çıkarılan içeriklerin istatistiklerini de kapsamalıdır. Bu durum, bilgiye erişim özgürlüğü bağlamında "dolaylı sansür" tartışmalarını (Gorwa, 2019) raporlama kapsamına sokar⁷¹.

Sosyal Ağlar: Moderasyonun Sayısal Anatomisi

Sosyal ağlarda raporlama, "hacim" ve "hız" odaklıdır. Roberts (2019), *Behind the Screen* adlı çalışmasında dijital moderasyonun görünmeyen emeğine ve bu süreçteki hata paylarına dikkat çeker⁷².

- Kaldırılan İçerik Kategorileri: Dezenformasyon, nefret söylemi, çocuk istismarı ve şiddet içeren içeriklerin dağılımı.
- Proaktif vs. Reaktif Tespit: İçeriklerin ne kadarının yapay zekâ tarafından (proaktif) henüz şikâyet gelmeden tespit edildiği, ne kadarının kullanıcı ihbarıyla (reaktif) işleme alındığı.
- Doğruluk Oranları: Yanlış pozitif (haksız kaldırma) ve yanlış negatif (gözden kaçırma) oranlarının beyanı. Literatürde bu, "Algoritmik Hata Payı Raporlaması" olarak tanımlanır.

Arama Motorları: Yasal Talepler ve Görünürlük

Arama motorları için raporlama, bilgiye erişimin kısıtlanma gerekçelerini belgeler.

- Telif Hakkı ve DMCA Talepleri: Hak sahiplerinden gelen kaldırma taleplerinin sayısı ve bu taleplerin ne kadarının işleme konulduğu.

⁷⁰ Helberger, N., et al. (2020). "The concept of the 'Gatekeeper' in the Digital Markets Act: A Legal and Economic Analysis." Common Market Law Review.

⁷¹ Gorwa, R. (2019). "What is platform governance?" Information, Communication & Society.

⁷² Roberts, S. T. (2019). A.g.e.

- Unutulma Hakkı (Right to be Forgotten): AB Adalet Divanı'nın "Google Spain" kararı sonrası gelişen süreçte, bireylerin kendi isimleriyle ilişkili linklerin kaldırılması taleplerine dair istatistikler.
- Hükümet Talepleri: Devlet kurumlarından gelen "içerik engelleme" veya "erişim kısıtlama" taleplerinin şeffaf dökümü.

E-Ticaret Platformları: Güvenli Pazar Yeri Verileri

E-ticaret platformlarında raporlama, ticari dürüstlüğü korumaya yöneliktir.

- Sahte Ürün (counterfeit) ve Satıcı Doğrulaması (Know Your Business Customer-KYBC) Raporları: Engellenen sahte satıcı sayısı, toplatılan ürün hacmi ve satıcı doğrulama süreçlerindeki başarı oranları.
- Tüketici Şikâyetleri: Ürün iadesi, lojistik sorunlar ve ödeme anlaşmazlıklarına dair çözüm istatistikleri.

2.5.2. Şikâyet ve İtiraz Mekanizmalarının Raporlanması

Şikâyet yönetimi raporlaması, platformun kullanıcıya karşı sahip olduğu keyfi gücü (arbitrary power) sınırlayan bir uygulamadır.

- **Yapay Zekâ Destekli İtiraz Çözümleri:** Birçok platform itirazları algoritmik sistemlerle değerlendirmektedir. Raporlamada, "insan denetimindeki itirazlar" ile "otomatik reddedilen itirazlar" arasındaki oran açıkça gösterilmelidir.
- **Sektörel Farklılıklar:**
 - **Sosyal Ağlar:** "Zararlı İçerik" tanımının ülkeden ülkeye değişmesi nedeniyle, raporlar bölgesel bazda (Geo-specific) sunulmalı ve yerel yasal taleplerin toplam taleplere oranı belirtilmelidir⁷³.
 - **E-Ticaret:** Sahte ürün itirazlarında satıcının sunduğu "orijinallik kanıtlarının" kabul edilme oranı piyasanın adaletini gösterir.

Sadece içeriğin kaldırılması değil bu süreçte yapılan itirazların nasıl yönetildiği, platformun "hukuki öngörülebilirliğinin" göstergesidir.

- **İtiraz Kabul Oranları:** Kullanıcıların itirazı sonrası geri yüklenen içeriklerin oranı, platformun moderasyon kalitesini yansıtır. Binns (2018), bu süreci "Algoritmik Adalet" (Algorithmic Justice) kavramı üzerinden analiz eder⁷⁴.
- **Yanıt Süreleri (Latency):** Bir şikâyetin incelenmesi ve bir karara varılması için geçen ortalama süre olarak tanımlanır. DSA, "gecikmeksizin" (without undue delay) ilkesini raporlama metriği olarak belirlemiştir.

⁷³ Unver, H. A. (2019). "Politics of Algorithmic Governance: Surveillance, Bias and Content Moderation." *EDAM Cyber Policy Paper*. (Bölgesel ve politik bağlam analizi için).

⁷⁴ Binns, R. (2018). "Algorithmic Accountability and Public Law." Public Law.

- **Dış Denetim Mercilerine Başvuru:** Kullanıcıların platform içi çözümle yetinmeyip bağımsız çözüm organlarına taşıdığı vaka sayıları olarak ele alınır.

2.5.3. Reklam Arşivi ve Ekonomik Veri Raporlaması

Reklam raporlaması sadece bir arşiv sunmak olarak ele alınmamalı, aynı zamanda reklamın toplumsal etkisini ölçmeyi sağlamalıdır⁷⁵.

- **Mikro-Hedefleme ve Ayrımcılık Verileri:** Ali et al. (2019)'ın çalışması, reklam algoritmalarının cinsiyet veya ırk bazında istihdam veya konut reklamlarını gizli şekilde filtrelediğini kanıtlamaktadır⁷⁶. Modern raporlama standartlarına göre, reklam sunumundaki "dağılımsal sapmalar" (distributional bias) raporlamaya dahil etmelidir.
- **Finansal Şeffaflık ve Veri Brokerları:** OECD'nin "Sınır Ötesi Veri Akışı ve Şeffaflık" ilkelerine göre, gelir modelinin ne kadarının üçüncü taraf veri aracılığı (data brokers) aracılığıyla beslendiğinin beyanı kritik bir öneme sahiptir.

Politik Reklamların İstatistiksel Dökümü

Politik reklam arşivleri sadece görsel bir kütüphane değil, analitik bir veri seti sunmalıdır.

- **Erişim ve Harcama Analizi:** Reklamın ulaştığı tekil kişi sayısı (reach) ile yapılan harcama arasındaki korelasyon olarak tanımlanır.
- **Mikro-Hedefleme Metrikleri:** Reklamın hangi spesifik ilgi gruplarına (örn: "kararsız seçmenler") yönlendirildiğine dair istatistiksel verilerdir. Benkler (2018), bu verilerin eksikliğinin "demokratik körlük" yarattığını savunur⁷⁷.

Gelir Modeli ve Veri İşleme Beyanları

Platformların gelirlerinin ne kadarının "davranışsal reklamcılık" üzerinden elde edildiğinin yıllık mali raporlarda (Financial Transparency) açıkça belirtilmesi, platformun kullanıcı profilini ne düzeyde "paraya çevirdiğinin" (monetization) kamuoyu tarafından bilinmesini sağlar.

2.5.4. Raporlama Standartları ve Veri Kalitesi (Standardization)

Raporlamanın en büyük sorunu, her platformun farklı metrikler kullanması nedeniyle "karşılaştırılabilirlik" (incomparability) problemidir.

- **Standart Metrikler:** OECD'nin "Vatandaş Odaklı Raporlama" standartları, platformlar arası kıyaslamayı mümkün kılacak ortak bir sözlük önerir.

⁷⁵ Tufekci, Z. (2017). *Twitter and Tear Gas: The Power and Fragility of Networked Protest*. Yale University Press. (Platformların toplumsal etkisi ve sorumluluğu).

⁷⁶ Ali, M., Sapiezynski, P., Bogen, M., Korolova, A., Mislove, A., & Rieke, A. (2019). "Discrimination through Optimization: How Facebook's Ad Delivery Can Lead to Biased Outcomes in Job and Housing Ads." *Proceedings of the ACM on Human-Computer Interaction*.

⁷⁷ Benkler, Y., Faris, R., & Roberts, H. (2018). *A.g.e.*

- **Ham Veriye Erişim:** Raporların sadece PDF formatında bir özet olarak değil, araştırmacıların analiz edebileceği ve makine tarafından okunabilir (machine-readable) formatlarda (JSON, CSV vb.) sunulması demektir. Literatürde bu, "Radikal Şeffaflık" olarak adlandırılır.
- **Dil ve Yerellik:** Raporların genellikle İngilizce olarak sadece merkez ofislerin dilinde değil, faaliyet gösterilen her ülkenin dilinde ve o ülkenin yerel risklerini (Örn: Türkiye'deki dezenformasyon trendleri) içerecek şekilde hazırlanması oldukça önemlidir.

Akademik literatürün en çok eleştirdiği konu, Google'ın sunduğu raporun Meta'ninkine veya Amazon'un sayfasındaki verilerle kıyaslanamaz olmasıdır.

- **Standart Veri Sınıflandırması (Taxonomies):** "Nefret Söylemi" tanımı her platformda farklıdır. Raporlama, uluslararası kabul görmüş (AB standartları) tanımlarla uyumunu deklare etmelidir.
- **API ve Veri Kazıma (Scraping) Politikaları:** Raporlamanın nihai hedefi, dış araştırmacıların (Auditors) platform verisini gerçek zamanlı denetleyebilmesidir. DSA Madde 40, araştırmacıların veri erişim haklarını yasal güvenceye alarak raporlamayı statik bir PDF formatından dinamik bir veri akışına sahip formatlara dönüştürmeyi amaçlar.

Literatür Tartışması: "Raporlama Tiyatrosu" (Reporting Theater)

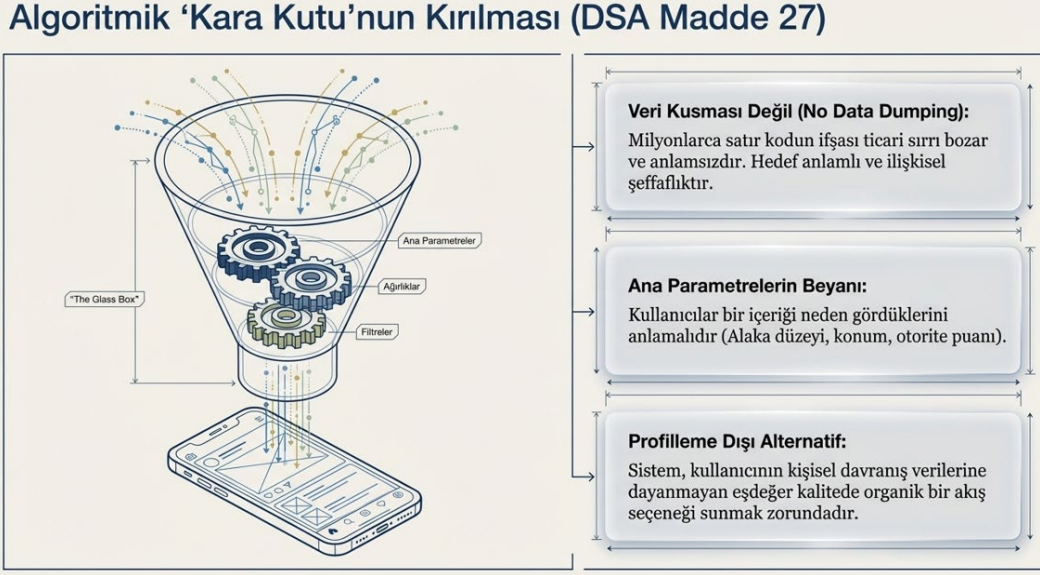
Akademik eleştiriler, platformların çok fazla veri paylaşarak aslında hiçbir şey anlatmadığı "Veri Kusması" (Data Dumping) stratejisine dikkat çeker. Wagner (2018), bunu "Şeffaflık İllüzyonu" olarak tanımlar⁷⁸. York (2021)'a göre ise; gerçek raporlama sayıların ötesine geçip, bu sayıların kullanıcıların temel hakları (ifade özgürlüğü, gizlilik vb.) üzerindeki etkisini niteliksel olarak da açıklamalıdır⁷⁹. Kayser-Bril (2020) de, raporlama tiyatrosu üzerine kritik bir analiz içerir⁸⁰.

Platformlar bazen çok fazla teknik veri sunmak suretiyle (over-reporting), regülatörü ve kamuoyunu asıl sorundan uzaklaştırabilir.

⁷⁸ **Wagner, B. (2018).** "Algorithmic Accountability: Towards a Policy Framework." Human Rights and Encryption.

⁷⁹ **York, J. C. (2021).** *Silicon Values: The Future of Free Speech under Surveillance Capitalism*. Verso Books.

⁸⁰ **Kayser-Bril, N. (2020).** "Why Transparency Reporting is Not Enough." AlgorithmWatch Report.



ŞEKİL 2-2: Algoritmik Kara Kutu (YZ ile hazırlanmıştır)

2.5.5. Operasyonel Şeffaflıktan Sayısal Hesap Verebilirliğe

Bu bölüm, dijital platformların beyan yükümlülüklerini sadece bir veri paylaşımı değil, bir "Yönetişim Standartı" olarak konumlandırmaktadır. Raporlama süreci, platformun vaatleri ile sahadaki uygulamaları arasındaki farkı ölçen bir turnusol kâğıdı görevi görmektedir.

Stratejik dezenformasyon olarak adlandırılan bu hususun önüne geçilebilmesi için raporlama süreçleri şu kriterlere dayanmalıdır:

- **"Anlamlılık" Testi:** Raporun, ortalama bir kullanıcının veya bir sivil toplum kuruluşunun anlayabileceği şekilde görselleştirilip görselleştirilmediği (Data Visualization Ethics) raporlama kalitesinin bir parçasıdır.
- **Bağımsız Denetim ve Nitelikli Veri Paylaşımı:** Şeffaflık yükümlülüklerinin etkili olabilmesi için platformların yalnızca standart faaliyet raporları yayımlaması yeterli değildir. Anlamlı ve proaktif bir şeffaflık tesisi için; içerik öneri sistemlerinin çalışma mantığı, otomatik moderasyon kararlarının hata oranları ve risk azaltma stratejilerinin sistemik etkisi gibi kritik göstergelerin düzenli olarak bağımsız araştırmacılar ve düzenleyici kurumlarla paylaşılması gerekmektedir.

Bölümün Temel Çıkarımları:

- **Metodolojik Standartlaşma:** Raporlamanın "anlamlı" olabilmesi için; OECD ve AB DSA standartları temel alınarak, platformlar arası kıyaslanabilirliği sağlayan ortak tanımlamanın, sınıflandırmanın, adlandırmanın ve düzenlemenin benimsenmesi bir zorunluluktur. Veri paylaşımı, "Reporting Theater" (Raporlama Tiyatrosu) riskinden arındırılmalı; nicelikten ziyade niteliğe odaklanmalıdır.

- **İçerik Moderasyonunun Sayısallaştırılması:** Sosyal ağlar ve arama motorları için sadece kaldırılan içerik sayıları değil; hata payları, itiraz kabul oranları ve algoritmik tespit yüzdeleri raporlamada yer almalıdır. Bu, "algoritmik adalet" (algorithmic justice) için temel şarttır.
- **Sektörel Raporlama Kırılımı:**
 - Arama Motorlarında: Yasal talepler ve "bilgiye erişim kısıtlamaları" odaklı,
 - Sosyal Ağlarda: Dezenformasyon ve kullanıcı etkileşim güvenliği odaklı,
 - E-Ticaret Platformlarında: Satıcı doğrulaması (KYBC) ve ticari dürüstlük verileri odaklı bir raporlama rejimi şarttır.
- **Dinamik ve Erişilebilir Veri:** Statik PDF formatındaki raporlardan, araştırmacıların ve regülatörlerin gerçek zamanlı analiz yapabileceği ve makine tarafından okunabilir (API tabanlı) veri paylaşım modellerine geçilmelidir.
- **Türkiye İzdüşümü:** 5651 Sayılı Kanun⁸¹ ve ETK düzenlemeleriyle Türkiye'de kurulan raporlama sisteminin, AB DSA ile harmonizasyonu hem Ülkemizdeki denetim kapasitesini artıracak hem de platformların küresel uyum maliyetlerini düşürecektir.

Sonuç olarak; raporlama, platformun "kara kutusunu" tamamen açamasa da, o kutunun dışarıya verdiği çıktıların toplum üzerindeki etkisini izlemeyi, ölçmeyi ve gerektiğinde müdahale etmeyi sağlayan en güçlü denetim köprüsü olarak görülmektedir.

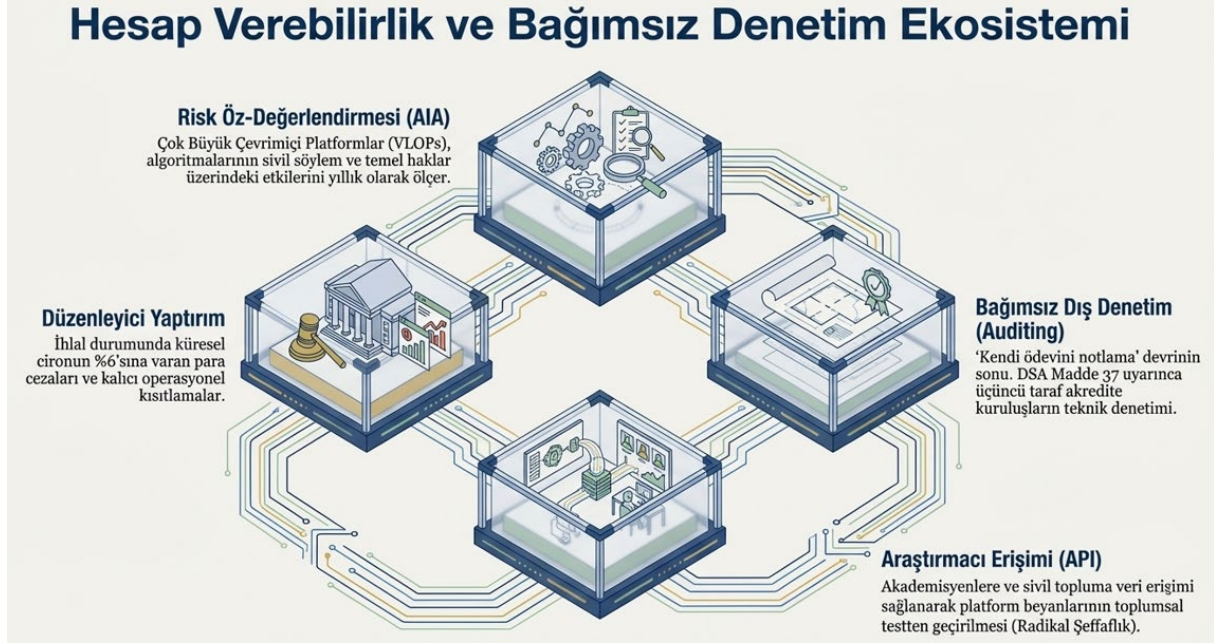
2.6. Hesap Verebilirlik (Risk Yönetimi, Bağımsız Denetim ve Kurumsal Sorumluluk)

Bu bölüm, raporun "eylem" ve "sorumluluk" aşamasını temsil eder. Şeffaflık "bilgi vermeyi", raporlama "beyan etmeyi" esas alırken; hesap verebilirlik (accountability), bu bilgilerin doğruluğunun teyit edilmesini, risklerin önceden yönetilmesini ve bir hata durumunda yaptırım ya da telafi mekanizmalarının işletilmesini kapsar.

Hesap verebilirlik, dijital platformların sadece kullanıcılarına karşı değil, demokratik kurumlara ve hukuk düzenine karşı olan yükümlülüklerinin somutlaşmış halidir. Bovens (2007); hesap verebilirliği "bir aktörün (platform), bir forum (regülatör/kamuoyu) önünde davranışlarını açıklama ve haklı çıkarma zorunluluğu hissettiği sosyal bir ilişki" olarak tanımlar⁸².

⁸¹ 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun (2007). T.C. Resmi Gazete, 26529, 23 Mayıs 2007.

⁸² Bovens, M. (2007). "Analysing and Assessing Accountability: A Conceptual Framework." European Law Journal.



ŞEKİL 2-3: Denetim Ekosistemi (YZ ile hazırlanmıştır)

2.6.1. Risk Temelli Öz-Değerlendirme (Self-Assessment), Önleyici Hesap Verebilirlik

AB DSA ve AI Act, "bir boyut her bedene uyar" yaklaşımını terk ederek, platformun toplumsal etkisine göre kademeli bir hesap verebilirlik rejimi getirmiştir.

Sistemik Risk Değerlendirmesi (DSA Madde 34-35)

Çok Büyük Çevrim İçi Platformlar (VLOPs), algoritmalarının ve hizmetlerinin topluma yönelik "sistemik risklerini" yıllık olarak analiz etmek zorundadır. Literatürde bu, "Algoritmik Etki Analizi" (Algorithmic Impact Assessment - AIA) olarak adlandırılır (Selbst, 2017)⁸³.

- **Demokratik Süreçler ve Kamu Sağlığı:** Sosyal ağlar, algoritmalarının seçim manipülasyonu veya gençlerin ruh sağlığı üzerindeki olumsuz etkilerini (cyber-bullying, yeme bozuklukları vb.) raporlamaktan ziyade, bu riskleri nasıl "hafiflettiklerini" (mitigation) kanıtlamalıdır.
- **Arama Motorlarında Bilgi Bütünlüğü:** Arama motorları, kriz anlarında (pandemi, savaş vb.) dezenformasyonun yayılımını engellemek için aldıkları tedbirlerin etkinliğini belgelemelidir.

Yapay Zekâ Uyumu

Yapay Zekâ Yasası, platformların kullandığı öneri sistemlerini ve profil oluşturma araçlarını "risk kategorilerine" göre ayırır. Hesap verebilirlik, bu sistemlerin tasarım aşamasından itibaren Tasarımla

⁸³ Selbst, A. D. (2017). "Disparate Impact in Algorithmic Decision-Making." Yale Law Journal.

Gizlilik (Privacy by Design) teknik dokümantasyonunun tutulmasını ve insan denetimi (Human-in-the-loop) mekanizmalarının kurulmasını gerektirir⁸⁴.

2.6.2. Bağımsız Denetim (Independent Auditing) ve Dış Gözetim

Hesap verebilirliğin en güçlü aracı, platformun kendi beyanlarının üçüncü taraflarca doğrulanmasıdır. Literatürde "The Audit Society" (Power, 1997) kavramı, dijital platformlar için "Algoritmik Denetim" (Algorithmic Auditing) olarak yeniden hayat bulmuştur⁸⁵.

- **Bağımsız Denetim Zorunluluğu:** DSA Madde 37 uyarınca, dev platformlar yılda en az bir kez bağımsız kuruluşlar tarafından denetlenmelidir. Bu denetimler; reklam kütüphanelerinin doğruluğunu, içerik moderasyonu kriterlerinin tarafsızlığını ve algoritmik sistemlerin temel haklara uyumunu dikkate alarak gerçekleştirir.
- **Veri Erişimi ve Araştırmacı Hakları:** Hesap verebilirlik, platformun verilerini "araştırmacı erişimine" açmasıyla güçlenir. Bruns (2019), "API Şeffaflığı"nın sadece teknik bir özellik değil, kamusal hesap verebilirliğin bir parçası olduğunu savunur⁸⁶. Akademik araştırmacılara sağlanan veri erişimi, platformun sivil toplum tarafından test edilmesine olanak tanır.

2.6.3. E-Ticaret ve Sosyal Ağlarda Spesifik Hesap Verebilirlik Modelleri

Satıcı Doğrulaması (KYBC) ve Tedarik Zinciri Sorumluluğu

E-ticaret platformları için hesap verebilirlik, piyasada faaliyet gösteren satıcıların tanınmasıyla (Know Your Business Customer) başlar.

Her bir platform, sahte ürün satan veya yasa dışı faaliyet yürüten satıcıların izini sürmek ve bunlarla ilgili regülatörlere bilgi vermekle yükümlüdür. Bu husus, "platformun pasif bir aracı" olduğu savunmasını zayıflatan ve onu "aktif bir denetleyici" konumuna getiren bir standarttır.

İçerik Konseyi ve Öz-Denetim Modelleri

Meta'nın "Gözetim Kurulu" (Oversight Board) örneğinde olduğu gibi, platformların kendi kararlarını yargılayacak bağımsız kurullar oluşturması, literatürde "Platform Anayasacılığı" (Platform Constitutionalism) olarak tanımlanmıştır (Klonick, 2018)⁸⁷. Bu tür mekanizmalar, devlet denetimi ile şirket çıkarları arasında bir "denge denetleme" organı işlevi görür.

⁸⁴ Costanza-Chock, S. (2020). *Design Justice: Community-Led Practices to Build the Worlds We Need*. MIT Press. (Tasarım aşamasında hesap verebilirlik).

⁸⁵ Power, M. (1997). *The Audit Society: Rituals of Verification*. Oxford University Press.

⁸⁶ Bruns, A. (2019). "After the API Calypso: Social Media Platforms and Their Fight Against Critical Independent Research." *Information, Communication & Society*.

⁸⁷ Klonick, K. (2018). "The New Governors: The People, Rules, and Processes Governing Online Speech." *Harvard Law Review*.

Hesap Verebilirlik: Rekabet, Tüketici Hakları ve İtiraz Mekanizmaları

Hesap verebilirlik; e-ticaret platformlarının algoritmik kararları nedeniyle ortaya çıkan rekabet ihlalleri, tüketici mağduriyetleri ve satıcı kayıpları karşısında etkili itiraz ve yaptırım mekanizmalarının bulunmasını gerektirir⁸⁸.

Araştırmalar:

- Satıcıların önemli bir bölümünün hesap askıya alma veya görünürlük düşüşlerine karşı etkili başvuru yollarına sahip olmadığını,
- Tüketici uyuşmazlıklarının büyük ölçüde platform içi kapalı sistemlerde çözüldüğünü ortaya koymaktadır.

2.6.4. Kurumsal Hesap Verebilirlik Yapısı: Uyum Görevlileri ve Regülatif İletişim

Dijital platformların hesap verebilirliği, yalnızca teknik sistemlerin denetlenmesiyle değil, aynı zamanda bu denetimi yürütecek ve sonuçlarından sorumlu olacak **kurumsal bir hiyerarşinin** tesisiyle mümkündür. AB Dijital Hizmetler Yasası (DSA Madde 11 ve 12) ve NIS2 Direktifi, platformları sadece birer teknoloji sağlayıcı olarak değil, regülatörler karşısında yasal muhataplığı olan "kurumsal aktörler" olarak yeniden tanımlamaktadır.

Parker ve Nielsen (2011), kurumsal uyum ve hesap verebilirlik mekanizmalarını inceledikleri kapsamlı çalışmalarında⁸⁹, şirketlerin düzenlemelere verdiği tepkilerin yalnızca yasal yaptırım korkusuyla şekillenmediğini savunur. Buna göre; "**sosyal lisans**" ve "**ekonomik hesap verebilirlik**" kavramları arasındaki dengeye dikkat verilmesi ile, işletmelerin içselleştirdiği etik değerler ve kurumsal kültür hususları, dışsal denetim mekanizmalarından daha belirleyici olabilmektedir. Hesap verebilirlik, bu perspektifte sadece kurallara kâğıt üzerinde uymak değil, paydaş beklentilerini yönetmek ve toplumsal meşruiyet kazanmak için geliştirilen stratejik bir süreçtir. Ayrıca, etkili bir hesap verebilirlik sisteminin inşası için cezalandırıcı yaklaşımlardan ziyade, işletmenin kendi iç denetim kapasitesini artıran ve uyumu bir "iş değeri" olarak gören hibrit modellerin gerekliliği de önem arz etmektedir.

Uyum Görevlilerinin (Compliance Officers) Rolü ve Bağımsızlığı

Hesap verebilirlik yapısının önemli bir kalemi olan **Uyum Görevlileri**, platformun iç denetim mekanizmalarını dış dünyayla (regülatörler, sivil toplum ve akademi) bağlayan köprü işlevi görür.

⁸⁸ Vries, K. D. (2020). "The Right to an Explanation: Algorithmic Decision-Making and the GDPR." *Oxford University Press*.

⁸⁹ Parker, C., & Nielsen, V. L. (2011). *Explaining Compliance: Business Responses to Regulation*. Edward Elgar Publishing.

- **Bağımsızlık ve Kaynak Tahsisi:** Literatürde "Compliance Professionalism" (Krawiec, 2003) olarak tartışılan kavram uyarınca; bu görevlilerin platformun kâr odaklı operasyonel birimlerinden bağımsız hareket edebilecek bütçe ve yetkiye sahip olması gerekir⁹⁰.
- **Risk Yönetimi Görevi:** Uyum görevlileri, özellikle AI Act kapsamında yüksek riskli sistemlerin dokümantasyonunu tutmak, algoritmik etki analizlerini (AIA) onaylamak ve olası ihlal durumlarında "erken uyarı" mekanizmasını işletmekle yükümlüdür.

Regülâtörlerle İletişim Kanalları ve Tek Nokta Temas (Single Point of Contact)

Modern dijital yönetim, platformlar ile kamu otoriteleri arasında kesintisiz ve şeffaf bir iletişim hattı kurulmasını önemser.

- **AB Komisyonu ve Dijital Hizmet Koordinatörleri (DSC):** DSA uyarınca her platform, AB Komisyonu ve faaliyet gösterdiği üye devletlerin regülâtörleri (örneğin İrlanda Coimisiún na Meán veya İngiltere Ofcom - Office of Communications, İngiltere'nin televizyon, radyo, telekomünikasyon ve posta hizmetlerini düzenleyen, içerik standartlarını belirleyen resmi denetleyici kurum) ile doğrudan iletişim kuracak bir "Tek Nokta Temas" (Single Point of Contact) birimi atamak zorundadır⁹¹.
- **Gerçek Zamanlı İş Birliği:** Ofcom'un (2023) Online Safety Act uygulama rehberinde belirttiği gibi; hesap verebilirlik, sadece yıllık raporlar üzerinden değil, kriz anlarında (terör saldırısı, seçim manipülasyonu vb.) regülâtörün bilgi taleplerine dakikalar içinde yanıt verebilecek "**dinamik iletişim kanalları**" üzerinden yürütülmelidir⁹².

Çok Katmanlı İletişim Stratejisi

Hesap verebilirlik yapısı; platformun sadece devletle değil, diğer paydaşlarla olan iletişimini de kurumsallaştırır. Aşağıda bunlardan bazı örnekleri görebiliriz.

1. **Regülâtör Hattı:** Yasal uyum, bildirimler ve denetim dökümanlarının paylaşımı için önemlidir.
2. **Güvenilir İşaretleyiciler (Trusted Flaggers):** Sivil toplum ve uzman kuruluşlardan gelen "hızlı müdahale" taleplerinin kurumsal olarak önceliklendirilmesi amacıyla kullanılmaktadır.
3. **Akademik Erişim Portalları:** DSA Madde 40 uyarınca, araştırmacıların platform verilerine erişimini yöneten portallerin tesisi gerekmektedir.

Kurumsal Sorumluluğun "Yönetim Kurulu" Düzeyine Taşınması

Hesap verebilirlik yapısının en üst basamağı, uyum süreçlerinin ve risk analizlerinin platformun Yönetim Kurulu tarafından onaylanmasıdır. Bu husus, hesap verebilirliğin bir "hukuk departmanı" işi olmaktan çıkıp, şirketin ana stratejik hedefi haline gelmesini sağlar. NIS2 ve DSA ihlallerinde öngörülen devasa para cezaları, bu kurumsal yapının ciddiyetini ve en üst düzeydeki sorumluluğunu pekiştirmektedir.

⁹⁰ **Krawiec, K. D. (2003).** "Cosmetic Compliance and the Failure of Negotiated Governance." Washington University Law Quarterly.

⁹¹ **European Commission (2024).** Guidelines on the designation of Single Points of Contact under the DSA.

⁹² **Ofcom (2023).** Compliance and Enforcement Approach for the Online Safety Act.

Siber Dayanıklılık ve NIS2 Uyumu

Hesap verebilirlik sadece içerikle sınırlı değildir, altyapı güvenliği de burada çok büyük bir öneme sahiptir.

- **Olay Bildirimi:** NIS2 Direktifi uyarınca, arama motorları ve sosyal ağlar, siber saldırıları veya teknik kesintileri "gecikmeksizin" ulusal otoritelere bildirmelidir. Bu, sistemik güvenilirliğin (reliability) teknik hesap verebilirliği olarak tanımlanabilir.
- **Tedarik Zinciri Güvenliği:** Platformlar, bulut bilişim hizmetlerinden başlayarak açık kaynak kütüphanelerine kadar kullandıkları tüm bileşenlerin güvenliğinden sorumlu tutulmalıdır.

Yaptırım Mekanizmaları

AB standartlarına göre; hesap verebilirliğin ihlali durumunda, platformun küresel cirosunun %6'sına kadar varan para cezaları öngörülmektedir.

- **Orantılılık İlkesi:** Küçük ölçekli platformlar için hesap verebilirlik "iyi niyetli çaba" üzerinden ölçülürken, Çok Büyük Çevrim İçi Platformlar (VLOPs) için "kesin sonuç" üzerinden değerlendirilir.
- **Zararın Tazmini:** Platformun algoritmik hataları sonucu (örn: haksız yere kapatılan bir e-ticaret hesabı) doğan zararların tazmin edilmesi, bireysel düzeyde hesap verebilirliğin bir parçasıdır.

2.6.5. Sorumluluk Rejimi ve Denetlenebilir Platform Ekosistemi

Bu bölüm, şeffaflık ve raporlama ile sağlanan bilgi akışının nasıl bir "Hesap Verebilirlik Mekanizmasına" dönüştüğünü analiz etmektedir. Hesap verebilirlik, platformların dijital kamusal alan üzerindeki güçlerini, hukuki ve etik sorumluluklarla dengeleme sürecidir.

Bölümün Temel Çıkarımları:

- **Reaktiften Proaktif Risk Yönetimi:** Hesap verebilirlik artık sadece bir hata oluşuktan sonra devreye giren bir süreç değildir. Sistemik Risk Analizi kapsamında sistemik risklerin önceden tespiti ve hafifletilmesi hususları, DSA ve AI Act ile birlikte zorunlu bir yönetim standardı haline gelmiştir.
- **Bağımsız Denetim (Auditing) Standartı:** Platformların öz-beyanlarının ötesine geçilerek, bağımsız üçüncü taraflarca yapılan algoritmik ve operasyonel denetimler, dijital güvenin yeni "Altın Standartı" olarak belirlenmiştir. Bu süreç, "Platform Anayasacılığı" kavramını güçlendirmektedir.
- **Sektörel Hesap Verebilirlik Odakları:**
 - **Arama Motorları ve Sosyal Ağlar:** Bilgi bütünlüğü, seçim güvenliği ve ruh sağlığı üzerindeki etkilerinden sorumludur.
 - **E-Ticaret:** Satıcıların kimlik doğrulaması (KYBC) ve tedarik zinciri güvenliği üzerinden ticari bir "güven garantörü" rolünü üstlenmektedir.

- **Teknik ve Hukuki Bütünlük (NIS2):** Hesap verebilirlik, içerik moderasyonunun ötesine geçerek siber dayanıklılık ve altyapı güvenliğini de kapsamına almıştır. Platformların teknik arızalar ve veri ihlalleri konusundaki şeffaflığı, kurumsal dürüstlüğün bir ölçütüdür.
- **Yaptırım ve Telafi:** Hesap verebilirliğin etkinliği, ciddi mali yaptırımlar ve kullanıcıların uğradığı zararların tazmin edilmesini sağlayan somut hukuk yolları (itiraz hakem heyetleri vb.) ile korunmaktadır.

Sonuç olarak; hesap verebilirlik, dijital platformları "yasaların üzerinde" olan kapalı yapılar olmaktan çıkarıp; devlet, sivil toplum ve kullanıcılar önünde somut sorumlulukları olan, denetlenebilir ve şeffaf kurumsal aktörlere dönüştürmektedir.

2.7. Türkiye Perspektifinde Şeffaflık, Raporlama ve Hesap Verebilirlik

Raporun bu bölümü, önceki bölümlerde ele alınan AB ve OECD normlarının Türkiye'deki mevcut yasal zemin (5651 Sayılı Kanun⁹³, 6563 Sayılı ETK⁹⁴, KVKK⁹⁵ ve Rekabet Kanunu⁹⁶) kapsamında analiz edilmesini içermektedir.

Türkiye, dijital platform yönetişiminde "yerelleşme" ve "hakların korunması" arasında stratejik bir denge kurmaya çalışmaktadır. Şimdiye kadar zikredilen şeffaflık, raporlama ve hesap verebilirlik ilkeleri; BTK ve Rekabet Kurumu gibi yerel kurumların ve bu kurumların yasa, yönetmelik ve genelgelerinin ana gündem maddesi haline gelmiştir.

Türkiye'de dijital platform yönetişimi, son yıllarda yapılan yasal düzenlemelerle (teknik olarak **5651 sayılı Kanun**'da yapılan köklü revizyonlardan olan; 2020'de yürürlüğe giren 7253 Sayılı Kanun'daki değişiklikler⁹⁷ ve 2022'de yürürlüğe giren 7418 Sayılı Kanun'daki değişiklikler⁹⁸) önemli bir dönüşüm yaşamıştır. Bu bölüm, yerel dinamikleri özellikle DSA ve DMA gibi küresel normlarla kıyaslayarak tartışmaktadır.

⁹³ **5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun (2007).** *T.C. Resmî Gazete*, 26529, 23 Mayıs 2007.

⁹⁴ **6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun (2014).** *T.C. Resmî Gazete*, 29168, 7 Kasım 2014.

⁹⁵ **6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) (2016).** *T.C. Resmî Gazete*, 29677, 7 Nisan 2016.

⁹⁶ **4054 sayılı Rekabetin Korunması Hakkında Kanun (1994).** *T.C. Resmî Gazete*, 22140, 13 Aralık 1994.

⁹⁷ **7253 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda Değişiklik Yapılmasına Dair Kanun (2020).** ("Sosyal Ağ Sağlayıcı" kavramını ve Türkiye'de temsilci bulundurma zorunluluğunu getiren temel düzenlemedir.) *T.C. Resmî Gazete*, 31202, 31 Temmuz 2020.

⁹⁸ **7418 Sayılı Basın Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun (Dezenformasyon Yasası) (2022).** (Şeffaflık raporlarının içeriğini genişleten, reklam yasaklarını ve dezenformasyonla mücadele kapsamında yeni sorumlulukları getiren düzenlemedir.) *T.C. Resmî Gazete*, 31987, 18 Ekim 2022.

2.7.1. Türkiye’de Şeffaflık: Algoritmalar ve Reklam Modelleri

Türkiye'deki şeffaflık tartışmaları, ağırlıklı olarak içerik kaldırma süreçleri ve kişisel verilerin korunması üzerine yoğunlaşsa da, algoritmik şeffaflık yeni bir odak noktasıdır.

- **Algoritmik Öngörülebilirlik:** Türkiye’de arama motorları ve sosyal ağların sıralama parametreleri üzerindeki denetim, büyük ölçüde Rekabet Kurumu üzerinden yürütülmektedir. Özellikle "kendini kayırma" (self-preferencing) vakalarında Rekabet Kurumu’nun Google ve diğer platformlara yönelik kararları, algoritmik şeffaflığın yerel piyasadaki en somut yansımasıdır⁹⁹.
- **Reklam Şeffaflığı ve Siyasi Reklamlar:** Türkiye’de seçim dönemlerinde dijital reklamların şeffaflığı konusunda, henüz AB’nin "Reklam Arşivi" standartlarına benzer kapsamlı bir yasal zorunluluk bulunmamaktadır. Ancak, küresel platformların kendi politikaları gereği sunduğu kütüphaneler (örn. Meta Ad Library), sivil toplum tarafından takip edilmektedir. Yerel mevzuatın bu kütüphaneleri yasal bir zorunluluk haline getirmesi, demokratik öngörülebilirlik açısından oldukça önem arzeden bir ihtiyaçtır.
- Türkiye bağlamında; **politik ve kamusal reklamlara ilişkin sistematik, ülke bazlı ve denetlenebilir reklam arşivlerinin bulunmaması**, seçim güvenliği, kamusal hesap verebilirlik ve bilgi bütünlüğü açısından yapısal bir boşluk yaratmaktadır. Platformların gönüllü uygulamalarına dayalı sınırlı şeffaflık adımları, harcama tutarları, hedefleme parametreleri ve reklam erişimi gibi kritik unsurların kamuoyu ve düzenleyici kurumlar tarafından bütüncül biçimde izlenmesini mümkün kılmamaktadır. Bu nedenle Türkiye’de faaliyet gösteren dijital platformlardan, **DSA ile uyumlu şekilde standartlaştırılmış politik ve kamusal reklam arşivleri oluşturmaları ve bu arşivleri düzenleyici kurumlara, bağımsız araştırmacılara ve kamuoyuna açık hâle getirmeleri** talep edilebilmelidir. Böyle bir yaklaşım, yalnızca seçim dönemlerine özgü bir tedbir değil; dijital kamusal alanın süreklilik arz eden şeffaflık ve hesap verebilirlik ihtiyacının kurumsal bir gereği olarak değerlendirilmelidir.

2.7.2. Raporlama Yükümlülükleri: Sayısal Veriler ve Yerellik

Türkiye, 5651 Sayılı Kanun’da yapılan değişikliklerle sosyal ağ sağlayıcılarına yönelik dünyanın en somut raporlama rejimlerinden birini kurmuştur.

- **İstatistiksel Beyanlar:** Sosyal ağ sağlayıcıları, Türkiye’den gelen içerik kaldırma ve erişim engelleme taleplerine dair altı aylık dönemlerle BTK’ye rapor sunmaktadır. Literatürde "Yerelleştirilmiş Raporlama" olarak bilinen bu husus, platformların küresel raporlarından farklı olarak Türkiye’ye özel hassasiyetleri ve yasal talepleri yansıtmaktadır. Ancak bu sistemin **kamu menfaatine hizmet edebilmesi için** verilerin sunum biçimi ve erişilebilirliği kritik önemdedir.
- **İstatistiksel Beyanların Niteliği:** Mevcut uygulamada bu verilerin ham veriler şeklinde kalması, verinin anlamlandırılmasını ve toplumsal bir denetim mekanizması oluşturulmasını güçleştirmektedir.
- **Şeffaflığın Kamusallaşması:** Literatürde 'Yerelleştirilmiş Raporlama' olarak geçen bu sürecin, sadece kurumlar arası bir veri aktarımı olmaktan çıkartılıp; araştırmacılar, sivil toplum ve son

⁹⁹ Rekabet Kurumu (2021). *Dijital Platformlar Hakkında Sektör Araştırması Ön Raporu*.

kullanıcılar için analiz edilebilir, makinece okunabilir ve şeffaf bir formatta kamuoyuna açılması gerekmektedir. Kamu menfaati, raporlamanın sadece varlığını değil, sunulan bilginin niteliğini ve toplum tarafından doğrulanabilirliğini kapsar.

- **E-Ticaret ve ETK Güncellemeleri:** 6563 Sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun'da yapılan son değişiklikler¹⁰⁰, e-ticaret hizmet sağlayıcılarına çok ciddi bir veri paylaşımı ve raporlama yükümlülüğü getirmiştir. Piyasa verilerinin Ticaret Bakanlığı ile paylaşılması¹⁰¹, piyasa şeffaflığını artırmayı hedeflerken, verinin gizliliği ve güvenliği hususları da akademik tartışmaları beraberinde getirmektedir.

2.7.3. Hesap Verebilirlik: Temsilcilikten Denetlenebilirliğe

Türkiye'de hesap verebilirlik, platformların yasal bir "muhatap" haline getirilmesi üzerinden şekillenmiştir.

- **Temsilcilik Modeli ve Sorumluluk:** Sosyal ağ sağlayıcılarına getirilen Türkiye'de temsilci bulundurma zorunluluğu, hesap verebilirliğin "fiziksel" boyutudur¹⁰². Bu model, platformun sadece teknik bir altyapı değil, yerel mahkemelere ve regülatöre karşı sorumlu bir tüzel kişilik olmasını sağlar.
- **Bağımsız Denetim ve Algoritmik Denetim (Auditing):** Türkiye'deki mevzuat henüz AB DSA'daki gibi "yıllık bağımsız denetim" zorunluluğunu tam anlamıyla tanımlamamıştır. Ancak, Rekabet Kurumu'nun yerinde inceleme yetkileri ve KVKK'nin veri işleme denetimleri, bir tür "kamusal hesap verebilirlik" mekanizması olarak işlev görmektedir. Türkiye'deki mevcut mevzuat, Rekabet Kurumu'nun piyasa denetimi ve KVKK'nin veri koruma incelemeleriyle güçlü bir "kamusal hesap verebilirlik" sunmaktadır¹⁰³. Ancak, kamu menfaatinin tam anlamıyla korunması için bu mekanizmalara ek olarak; platform algoritmalarının tarafsızlığını ve toplumsal etkilerini ölçen **düzenli ve bağımsız teknik denetimlerin** tanımlanması önerilmektedir. Böylece, bu durumun dijital ekosistemin güvenliğini sağlayan bir 'standart' haline getirilmesi amaçlanmaktadır.
- **E-Ticaret ve Lisanslama:** Büyük ölçekli e-ticaret platformlarının (Net İşlem Hacmi üzerinden) lisans alma zorunluluğu ve belirli harcama sınırlarına tabi tutulması, Türkiye'ye özgü bir hesap verebilirlik ve pazar dengeleme aracıdır.

2.7.4. Tartışma: Harmonizasyon ve Gelecek Projeksiyonu

Türkiye'nin dijital platform yönetişi, AB'nin DSA ve DMA modeline paralel ilerleme potansiyeline sahiptir. Ancak aşağıda görüleceği üzere, bazı temel farklılıklar da tartışılmaktadır:

¹⁰⁰ 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun (2014). *T.C. Resmi Gazete*, 29168, 7 Kasım 2014.

¹⁰¹ Ticaret Bakanlığı. (2023). *Türkiye E-Ticaret Ekosistemi ve Yeni Mevzuat Rehberi*.

¹⁰² 7253 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda Değişiklik Yapılmasına Dair Kanun (2020). ("Sosyal Ağ Sağlayıcı" kavramını ve Türkiye'de temsilci bulundurma zorunluluğunu getiren temel düzenlemedir.) *T.C. Resmi Gazete*, 31202, 31 Temmuz 2020.

¹⁰³ Yılmaz, M. C. (2021). "Kişisel Verilerin Korunması Kanunu ve Dijital Platformların Hesap Verebilirliği." *KVKK Hakemli Dergi*.

- **Orantılılık İlkesi:** Mevcut yerel düzenlemelerin, inovasyonu teşvik eden start-up ölçeğindeki platformlar ile Çok Büyük Çevrim İçi Platformlar (VLOPs) arasındaki ayrımı AB normlarındaki kadar keskin yapıp yapmadığı tartışmalıdır. Dev platformlar ile start-up gibi yeni girişimlere aynı ağır yükümlülükleri yüklemek, kâğıt üzerinde "eşitlik" gibi görünse de uygulamada küçük oyuncuların ezilmesine ve **rekabetin bozulmasına** neden olur. AB normlarındaki gibi **risk temelli bir sınıflandırma**, küçük ölçekli işletmelerin üzerindeki idari yükü hafifleterek ekosistemin büyümesini destekleyecektir. (Bkz. DSA, Madde 19, 24 ve 33; KOBİ Muafiyetleri ve VLOP Yükümlülükleri)
- **Veri Lokalizasyonu:** Türkiye'nin verinin ülke içinde kalmasına dair hassasiyetleri, küresel platformların hesap verebilirlik modelleriyle zaman zaman teknik tartışmalar yaratabilmektedir.
- **İtiraz Mekanizmaları:** Kullanıcıların içerik kaldırma kararlarına karşı platform içi itiraz süreçleri bulunmamaktadır. Bu durumun DSA Madde 20'deki kadar şeffaf ve bağlayıcı hale getirilmesi, Türkiye'deki kullanıcı hakları açısından bir sonraki aşama olarak görülmektedir.

BÖLÜM 3: İÇERİK YÖNETİŞİMİ VE KULLANICI KORUNMASI

Bölümün Amacı: İçerik yönetimini platformların keyfiyetine bırakmayıp şeffaf, hesap verebilir ve sürdürülebilir bir hukuki prosedüre oturtmak ana hedeftir. Ayrıca, zarar oluşunca aksiyon alan, mesela içeriği silmeye odaklanan "statik" yapı yerine, zararın oluşmasını önleyecek "risk temelli yönetim" modeli tesis edilmelidir.

İçerik ve Kapsam:

- Platform türüne göre farklılaşan, standart hale getirilmiş elektronik formatta "Bildir-ve-Aksiyon" protokollerinin oluşturulması.
- Platformların içerik kısıtlama kararlarını anlaşılır bir "Gerekçe Beyanı" ile yapması ve işlerliği olan "İtiraz Yolları" mekanizma sistematığının kurulması.
- Yargı yükünü hafifletecek ve bağımsız olacak "Mahkeme Dışı Uyuşmazlık Çözüm" kuruluşlarının oluşturulması.
- Sivil toplum kuruluşlarının uzmanlık marifeti ile "Güvenilir İşaretleyici" (Trusted Flaggers) mekanizmasının regülasyona entegre edilmesi.
- Kullanıcıyı manipüle eden algoritmik "Karanlık Tasarımların" (Dark Patterns) önlenmesi ve dijital arayüzlerde uluslararası erişilebilirlik standartlarının (WCAG/EAA) olması.
- Çocukların çevrim içi internet ortamlarında korunması amacıyla "Tasarım Yoluyla Güvenlik" (Safety by Design), ve mahremiyet odaklı yaş doğrulama sistemi olması.
- AB CSAM (Çocukların Cinsel İstismarıyla Mücadele) ile uyumlu tespit mekanizmalarının kurulması.
- Yerel girişimleri (startup) korumaya yönelik "Asimetrik Regülasyon" ve esnek "Birlikte Düzenleme" (Co-Regulation) modellerinin analiz edilmesi.

Temel Kavramlar:

Güvenilir İşaretleyici (Trusted Flaggers), Karanlık Tasarımlar (Dark Patterns), Tasarım Yoluyla Güvenlik (Safety by Design), Viralite, Birlikte Düzenleme (Co-Regulation), Asimetrik Regülasyon

3.1. Dijital Platformlar Mevzuat Reformu ve Küresel Uyum Stratejisi

Bu rapor ile, ülkemizin dijital platformlar temelindeki mevcut ekosistemin eksik ve iyileştirme gereken alanlarını belirleyerek, Türkiye'nin dijital platformlar temelindeki yönetim kriterlerini uluslararası standartlarla (DSA, OSA, OECD vb) uyumlu hale getirmek amaçlamıştır.

Bu kapsamda geliştirilecek model ile; şeffaflık, hesap verebilirlik ve paydaş katılımını esas alarak ülkemizin bu alanda etkin, yapıcı ve liderlik eden bir konumda olması hedeflenmektedir.

Önerilen stratejiler, uluslararası düzenlemeler ile uyumlu olan aşağıda verilen üç temel sütun üzerine inşa edilmiştir:

Hak Temelli Yaklaşım ve Demokratik Denge

İçerik yönetimi, **ifade özgürlüğü ile kişilik haklarının korunması** arasındaki hassas dengeyi korumalıdır. Kullanıcının bilgiye erişim hakkı ile özel hayatın gizliliği arasındaki denge, sadece idari kararlarla değil; itiraz mekanizmalarına erişimini kolaylaştıracak kriterler ile denetim ve şeffaflık ilkeleriyle güvence altına alınmalıdır. Dijital ortamda ortaya çıkan hak ihlallerinin giderilmesinde **yargısal denetim, şeffaflık ve hesap verebilirlik** ilkeleri ile desteklenen çok katmanlı bir yönetim yaklaşımı benimsemektedir.

Bu çerçevede önerilen model, erişim engelleme tedbirini ilk başvurulacak araç (prima ratio) olmaktan ziyade, hak ihlalinin önlenmesi amacıyla başvurulacak **orantılı ve istisnai bir müdahale (ultima ratio)** olarak le almaktadır. (Bkz. Colomo, 2024; Monti, 2012)¹⁰⁴

Statikten Risk Temelli Yönetişime Geçiş

Mevcut mevzuat daha çok "statik içerik kaldırma" yaklaşımında olup, daha proaktif bir sistematik yapı ile dijital dünyanın gereksinimi olan **"risk temelli yönetim modeline"** geçiş yapılması önerilmektedir.

Bu yapısal amaç sayesinde, zararlı içeriklerin yayılmasına olanak sağlayan sistemik riskler direkt olarak platformlar üzerinden engellenebilir olmalıdır. Bu dönüşüm ile dijital pazarlar sadece bir tüketim ortamı değildir, bilakis güvenli ve sürdürülebilir bir altyapılar halindedir.

Algoritmik Kürasyon ve Hukuki Sorumluluk Mimarisi

Bu yönetim sayesinde, **algoritmik kürasyonun hukuki sorumluluk içindeki rolünün** de netlikle tanımlanması hedeflenmektedir. Platformlar algoritmalar vasıtasıyla "seçen ve öne çıkaran" fonksiyonlara

¹⁰⁴ **Pablo Ibáñez Colomo, 2007.** "The Draft Digital Markets Act: A Restraint on the Exercise of Market Power or a Reimagining of the Role of the State in the Economy?", *European Law Review*, 46(3), 2021, s. 296; Giorgio Monti, *EC Competition Law*, Cambridge University Press, s. 61.

sahiptirler ve bu önemle ele alınması gereken bir sorumluluk olmalıdır. Bu kapsamdaki sorumluluklar ve mekanizmaları içerecek ve uluslararası ekosisteme uyum sağlanacak kapsamda, ülkemizin **dijital egemenliği** odağında; standartları takip eden yapıdan ziyade, standartların şekillenmesinde aktif olan bir sistemin bileşeni olması hedeflenmiştir.

3.2. Neden Bu Reform Gerekli?

Dijital ekosistem ve çevrim içi platformlar regülasyonların oluşturulduğu ilk dönemde "statik web" yapısındaydı, ancak zamanla gelişmiş algoritmaların, yapay zekânın ve büyük platformların ekonomik güçleri sayesinde oldukça karmaşık bir yapıya dönüşmüştür.

İnternetin erken dönemlerinde kullanıcılar, bir web sitesine kendi istekleriyle erişen daha ziyade pasif diye adlandırabileceğimiz konumundaydılar. Bu durumda iken **platformlar**, kendilerini içeriği taşıyan za da barındıran bir **teknik aracı** (hosting/intermediary) olarak konumlandırıdılar.

Günümüzde büyük dijital platformlar çok farklı alanda ve kapsamda yeteneklere sahiptirler; **algoritmalar ile çeşitli sıralama, öneri sistemleri ve yapay zekâ destekli içerik kürasyonu** gibi marifetlerle kullanıcıların karşılaştığı içerikleri belirleyebilme ve yönlendirmeye muktedirler. Kullanıcıların karşısına çıkan içerik, artık sadece kullanıcının tercihlerine göre değildir; zira artık **platformların tasarladığı algoritma** ile karar süreçleri etkilenmektedir.

Bu teknolojik ve sosyal dönüşüm artık platformların klasik söylemde “pasif aracı hizmet sağlayıcı” olduğu tanımlamasını tartışmalı hale getirmiştir. Zira platformlar hem algoritmalar hem de önceliklendirme mekanizmaları marifetiyle içerik akışında **editorial etki** ile yönlendirme yapmaktadır. Mevcut regülasyonlar ve düzenlemeler, platformların “**aktif yönlendirme**” mekanizmaları bakımından yeterince sorumlulu tutulduğu bir hukuki çerçevede değildir. Platformlar artık dijital kamusal alanı şekillendiren aktörler olarak ele alınmalıdır.

Yapılan düzenlemelerle mevzuata “**Sosyal Ağ Sağlayıcı**” gibi yeni tanımlar eklenmiş (5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi), bazı düzenlemelerle birlikte özellikle sosyal medya platformlarının Türkiye’de temsilci bulundurması, içerik kaldırma ve başvurulara cevap verme yükümlülükleri gibi bazı yeni sorumluluk mekanizmaları öngörülmüştür. Mevzuat düzenlemesi ile bir ilerleme olmasına rağmen, platform sorumluluk temel mimarisinin “aracı hizmet sağlayıcı” yaklaşımı üzerine kurulu olduğu değerlendirilmektedir. Bu durum, günümüz teknoloji koşulları dikkate alındığında önemli bir eksikliğe neden olmaktadır. Bu nedenle mevcut regülasyonların yeniden ele alınarak düzenlenmesini gerekli kılmaktadır.

Tanım Sorunu: Kanun metinlerinde var olan bazı terimler olan "Yer Sağlayıcı", "Erişim Sağlayıcı" ve "İçerik Sağlayıcı" tanımlarının eski klasik teknoloji mimarisine göre oluştuğu ifade edilebilir.

Algoritmik Kürasyon: Algoritmik kürasyonlar özetle, içeriklerin algoritmalar tarafından yönlendirilir ve kişiye göre sıralanabilir hale getirilen halidir denilebilir. Hangi içeriği kime, ne zaman, hangi sırayla gösterilir, tüm bunlar artık platformlar ile yönetilebilmektedir. Mevcut düzenlemeler, sosyal medya platformlarının (Instagram, TikTok, X vb.gibi) "algoritmik kürasyon" (içeriği öne çıkarma) marifetlerinin olmadığı ya da kısıtlı yeteneklerinin olduğu bir dönemde yazılmıştır. Mevcut tanımlar, platformların bu karmaşık yeteneklerini kapsamakta eksik kalmaktadır. Haliyle bu durumda hukuki gri alanlar oluşabilmektedir.

Stratejik Dönüşüm: Yeni yapılanma ile temel hedef, sadece reaktif olan kısıtlayıcı müdahaleler yerine, teknolojik gelişmeleri içeren bir yaklaşımla regüle etmek, kullanıcı haklarını güvence altına almak ve proaktif bir sistematik sayesinde güvenli altyapılar kurulmasını sağlamaktır. Platformların standartlarını denetleyen, şeffaflık ve dijital süreçleri, sosyal yapının korunması amacıyla ve veri egemenliğini hedef alan dinamik ve kendini yenileyen proaktif bir işleyiş tesis edilmelidir.

3.3. Vizyon ve Stratejik Çerçeve

Hem Türkiye'nin dijital ekonomisini geliştirerek büyütme hem de kullanıcıları çevrim içi ortamlarda güvende tutmak amacıyla proaktif, şeffaf ve risk tabanlı bir yönetim modeline geçiş önerilmektedir. Bu kapsamda uluslararası mevzuata uyum sağlamak da küresel ekonominin gereği olarak öne çıkmaktadır. Bu nedenle **AB Dijital Hizmetler Yasası (DSA)**, **İngiltere (Birleşik Krallık) Çevrim İçi Güvenlik Yasası (OSA)** ve **OECD** standartlarını da referans alarak Türkiye için öneriler sunulmaktadır.

Önerilen model temelinde, mevzuat ile hem "**Teknik Düzenlemeler**" ve aynı zamanda dijital ortamda bir "**Anayasal Güvence**" mekanizması tesis etmek vardır. Bu çerçevede, aşağıda belirtilen temel kavramlar ele alınmaktadır:

İfade Özgürlüğü ve Bilgiye Erişim: İçerik kısıtlamalarının kullanıcıların veriye erişim hakkını engellemeden ve platformların moderasyon sorumluluklarını denetleyen kapsamda bir dengede oturtulması hedeflenmelidir.

Adil Yargılanma ve Etkili Başvuru Hakkı: Platformlar tek taraflı olarak karar alarak içerik kaldırma, hesap askıya alma gibi uygulamalar yapmaktadırlar. Buna karşı kullanıcılar, DSA'nın temel amaçlarından biri olan; hızlı, kolay ve maliyetsiz olarak **dahili itiraz ile mahkeme dışı çözüm yollarına** ulaşabilmelidirler.

Ayrımcılık Yasağı: Dijital platformların algoritmalar ile yaptığı öneri sistemleri içerik mekanizmaları, taraf olmayacak şekliyle, bireyler veya topluluklara yönelik **dil, ırk, etnik köken, siyasi görüş veya inanç kavramlarında ayrımcılık ve kayırmacılık oluşturmayacak** halde tasarlanmalı ve icra edilmelidir. Bu sorumluluk ile platformlar, algoritmik karar işleyişlerinde oluşabilecek **önyargı ve orantısız etki** risklerini tespit etmek için düzenli olarak **sistemik risk analizleri ve algoritmik etki değerlendirmeleri** yapmalı ve

denetlenmelidirler.

Bu sistematik sayesinde bireysel ve toplumsal hak ihlallerini önlemek ve platformların işleyişinde eşitlik ilkesi ile tarafsız bir yönetim modelinin oluşturulması amaçlanmaktadır.

Kullanıcı Koruması, Sistemik Riskler ve Dijital Refah

Dijital platformlarda içeriğin algoritmalar sayesinde hızla geniş kitlelere ulaştırılarak popüler hale getirilmesi mümkündür (Viralite). Dijital platformların algoritmalar ile çok fazla kullanıcıya, zararlı içeriklerin yayılımını hızlandırarak ulaştırabilme güçlerinin olması çeşitli riskler üretmektedir. Sadece yasal olmayan içeriklerin reaktif olarak kaldırılması yeterli değildir, teknolojik hızlara ayak uyduran bir platform yönetim regülasyonlarına ihtiyaç vardır.

Kullanıcının koruması kavramı sadece bireysel güvenlik veya çocukların zararlı içeriklerden korunması (Safety by Design) düzeyinde bırakılmamalıdır. Kapsamlı bir kullanıcı koruma ile veri sömürsünün engellenmesi, karanlık tasarımlar (dark patterns) ile yapılan manipülasyonların önlenmesi, hedefli reklamların ve demokratik süreçlerin etki altına alınmasının önüne geçecek sistemlerin kurulması elzem konulardır. STK'lar ve politika yapımcılar olarak reaktif model olan; zararın sonuçlarına göre hareket etmekten ziyade, zarara neden olan yapısal faktörleri proaktif bir şekilde ortadan kaldıracak sistemler kurmak ve bunları güvence altına alacak denetim mekanizmaları kurmak hedeflenmelidir.

Hızlı değişen teknolojiler ile dijital platformlar karşısında süreçlerin teknik ve idari uygulamalarının, uluslararası iyi uygulama örnekleri de dikkate alınarak güncellenmesi ve optimize edilmesi gereklidir.

3.4. Temel Reform Alanları ve Küresel Referanslar

Ana hedefimiz; dijital platformları küresel standartları referans alarak, ülkemiz menfaatini gözetten bir sistem kurmaktır. Avrupa Birliği'nde yürürlükte olan DSA (Dijital Hizmetler Yasası) ve DMA (Dijital Pazarlar Yasası) gibi düzenlemeler incelendiğinde; bu yapıların statik ya da edilgen değil, bilakis dinamik, hak dengesini gözetten ve çok paydaşlı bir yaklaşımı içeren regülasyonlar olduğu görülmektedir. Türkiye'deki mevcut yasalara bakıldığında temel kanunlar olarak; 6502 sayılı Tüketicinin Korunması, 5651 sayılı İnternet Ortamı Düzenlemeleri, 6563 sayılı E-Ticaret ve 4054 sayılı Rekabetin Korunması gibi bu alanlarda ki öncül düzenlemeler olduğu söylenebilir.

Teknolojinin gelişmesi ile platformların hızlı evrilen yetenekleri dikkate alındığında, ülkemizdeki düzenlemelerin küresel gelişim ihtiyacına yanıt vermekte doğal olarak yetersiz kaldığından bahsetmek yanlış olmayacaktır. Şöyle ki, tekrar etmek ve yeniden vurgulamak gerekirse, dijital ekosistemin hızla dönüşmesi, çevrim içi hak arama mekanizmalarının ve içerik moderasyonu süreçlerinin yeniden tanımlanmasını zorunlu kılmaktadır. Bu bakımdan ülkemizde mevcut öncü yasalardan 5651 sayılı Kanun'a bakıldığında, Kanun'un özellikle yukarıda örneklendirilen AB mevzuatına kıyasen daha durağan, hak

dengesinden ziyade suç riskini merkeze alan, çok paydaşlılık yerine daha devlet merkezli ve proaktif bir yaklaşım yerine reaktif bir yaklaşımı benimsediğini ifade etmek mümkündür. Bunların yanı sıra ayrıca Kanun'un birtakım operasyonel yetersizlikleri ve standart eksikliğinden de bahsetmek gerekir. Bu eksiklik kullanıcılar için "hak aramada sorunlar yaratabildiği gibi platformlar için de bazı hukuki belirsizlik alanlarına neden olabilecek niteliktedir.

Bu çerçevede, Türkiye dijital mevzuatının küresel standartlarla ve de özellikle Avrupa Birliği'nin Dijital Hizmetler Yasası (Digital Services Act - DSA) ile uyumlandırılmasına yönelik stratejik reform önerilerini içermektedir. Önerilen reformların temel amacı; dijital dünyada içerik yönetimini platformların "keyfiyetinden" çıkarıp, şeffaf, hesap verebilir ve sürdürülebilir bir "hukuki prosedür" mimarisine kavuşturmadır. Bu yaklaşım tüketicilerin, platform kullanıcılarının daha etkin bir mekanizma ile sorunlarına yanıt almalarını sağlarken, ülkemizde yer alan oyuncu ve girişimcilerin küresel rekabette öne çıkmasına da fayda sağlayacağı düşünülmektedir. Bu doğrultudaki önerilerimiz aşağıdaki sıralanan temel başlıklar altında şekillenmektedir.

3.4.1. Bildir-ve-Aksiyon (Notice-and-Action) Reformu

Bu bölümde eğer bir içerik mevzuata aykırı (yasadışı içerik veya ticari ihlal) olduğu gerekçesi ile başlayan bir süreçte ise, platformun türüne ve ihlal niteliğine istinaden bir "**hukuki prosedür**" oluşturulmasıdır.

Platform Türlerine Göre Farklılaşan Bildirim Rejimi

"Bildir-ve-Aksiyon" mekanizması ile, platform da verilen teknik hizmetin niteliği ve ilgili operasyonel risk seviyesi uyumsuzlukların çözümünde önerilen teknik sınıflandırma aşağıda verilmektedir:

- **Sosyal Ağ Sağlayıcılar:** Paylaşılan içeriklerin hukuki niteliği ve bireysel hak ihlallerine yönelik bildirim süreçleri (5651 ve 7418 sayılı kanunlar kapsamında tanımlanan usuller).
- **Dijital Pazaryerleri (E-Ticaret):** Ürün güvenliği, fikri mülkiyet hakları ve ticari rekabet kurallarına yönelik bildirim süreçleri (6563 sayılı kanun ve ilgili sektörel düzenlemeler kapsamında).
- **Arama Motorları:** Dizinleme (indeksleme) faaliyetleri, bilgiye erişim standartları ve verilerin korunmasına yönelik endeks yönetimi süreçleri.

Bu ayırıştırma sayesinde, her platform türünün çalışma sistematığına göre, teknik olarak uygulanabilir ve yasal olarak tanımlanmış bir bildirim sistemi amaçlanmaktadır.

Küresel Standartlar ve Teknik Uyum: "Bildir-ve-Aksiyon" (Notice-and-Action) Mimarisi

Uluslararası standartlar, bilhassa Avrupa Birliği Dijital Hizmetler Yasası (DSA) Madde 16¹⁰⁵, bu karmaşıklığı "**Elektronik Bildirim Formu**" mekanizması ile aşmayı hedeflemektedir. Bu yapıda platformlara, bir bildirimin hukuki geçerlilik kazanabilmesi için içermesi gereken asgari teknik unsurları (URL bazlı kesin konum verisi, somut gerekçelendirme ve doğruluk beyanı gibi) belirler. Böylece hizmet sağlayıcının yasal sorumluluk çerçevesi, bildirimin içeriğine dair teknik veriler sayesinde netlik kazanmaktadır.

Bu sayede:

- **Hak Sahipleri İçin:** karmaşık başvuru süreçlerinin yerine, kolay yönetilebilir ve hukuki geçerliliği olan teknik bir standart oluşturulur.
- **Hizmet Sağlayıcılar İçin:** bildirimlerin hukuki niteliği ve teknik veriler üzerinden operasyonel netlik sağlanır.

Mevcut Durum ve Teknik Uygulama Standartları

5651 sayılı Kanun, internet ortamındaki içeriklere müdahale usullerini genel hatlarıyla belirlemiş olsa da, özellikle ticari pazaryerleri ve çok işlevli (hibrit) platformlar özelinde **bildirim süreçlerinin teknik bir standarda kavuşmadığı** görülmektedir. Mevcut durumda hak sahipleri; noter ihtarnamesi, platform bazlı münferit formlar veya e-posta gibi farklı kanallar üzerinden bildirimde bulunmaktadır.

Bu çok kanallı yapı, içerik bildirimlerini bir "hukuki rejim belirsizliği"nden ziyade bir "**usuli karmaşıklık**" sorununa dönüştürmektedir.

Türkiye'deki dijital ekosistemde ihtiyaç duyulan temel iyileştirme; yeni bir maddi hukuk rejimi değil, mevcut koruma mekanizmalarına erişimi kolaylaştıracak **standartlaştırılmış bir bildirim mimarisi** entegre etmektir.

3.4.2. Stratejik Öneri: Standart Dijital Bildirim Protokolü

Dijital platformlarda içerik ve işlem bildirimlerine ilişkin standart bir uygulama sağlanması için, Bilgi Teknolojileri ve İletişim Kurumu (BTK) ile Ticaret Bakanlığı koordinasyonunda, Türkiye'de faaliyet gösteren platformlar için "**Standart Dijital Bildirim Protokolü**" oluşturulması önerilmektedir.

Bu protokol sayesinde bildirim süreçleri, olası uyumsuzlıklara ait teknik ve hukuki niteliğine göre iki ana kategori altında oluşturulabilir: Adli İçerikli Bildirimler ve Sektörel ve Ticari Bildirimler.

¹⁰⁵ DSA Madde 16, https://www.eu-digital-services-act.com/Digital_Services_Act_Article_16.html

Bu protokolün uygulamaya geçirilmesiyle birlikte; bildirimin niteliğine göre hukuki sınıflandırması (adli suç ya da , içerik ihlali veya ticari ihlal) sistem tarafından otomatik olarak sınıflandırılıp ilgili süreçlere yönlendirilmesi mümkündür. Böylece hem platformlar hem de hak sahipleri açısından **bildirim süreçlerinin izlenebilirliği, öngörülebilirliği ve işlem hızı** teknik bir standart aracılığıyla güvence altına alınmış olacaktır.

Bildirim Formu Standartları (AB-DSA Madde 16 referans) ile yasal gerekçe ve kimlik bilgilerini içeren "Elektronik Bildirim Formları" zorunlu kılınarak bildirimler hukuki belge statüsüne kavuşturulmalıdır. Platform hizmeti sağlayıcıları, kullanıcıların yasadışı içerik bildirimlerini sade ve hızlı erişilebilir formatta almalarını sağlayan elektronik bir mekanizma kurmalarını zorunlu tutar. Bu mekanizma genellikle bir e-bildirim formu şeklinde olur.

Bu bildirimin içermesi gereken asgari unsurlar metin olarak açıkça belirlenmiştir:

- İçeriğin neden yasadışı kabul edildiğine dair gerekçeli açıklama,
- İçeriğin kesin adresi/URL,
- Bildirimi yapan gerçek veya tüzel kişinin adı ve e-posta adresi (istisnai durumlar hariç),
- İyi niyetle ve doğruluğu taahhüt eden bir beyan.

3.4.3. Güvenilir Bildirici (Trusted Flaggers)

DSA Madde-22 uyarınca **uzman kuruluşlara öncelikli bildirim hattı (hotline vb.) sağlanmalıdır.**¹⁰⁶

İnternetteki zararlı içeriklerin (çocuk istismarı, terör propagandası, siber saldırı vb.) tespitinde sivil toplumun yaygın görüş ve uzmanlık gücünden yararlanılması proaktif kontrol mekanizmaları açısından çok önemlidir.

Tespit: Türkiye’de mevcut düzenlemeler kapsamında, bir sivil toplum kuruluşunun yaptığı kritik bildirim ile sıradan bir kullanıcı tarafından yapılan bildirim arasında mevzuat düzeyinde tanımlanmış bir önceliklendirme mekanizması yoktur. Bu durum, uzman kuruluşların (Ör: siber güvenlik uzmanı, hukuk derneği, tüketici derneği çocuk hakları örgütü vb.) platform moderasyon ekiplerine doğrudan ulaşabileceği bir sistemin bulunmaması nedeniyle bir uygulama boşluğu oluşturmaktadır.

Küresel Çözüm: EU DSA Madde 22, belirli bir teknik uzmanlık, bağımsızlık ve liyakat kriterlerini karşılayan kuruluşlara "Güvenilir İşaretleyici" statüsü verilmesini sağlar. Platformlar, bu statüdeki kurumlardan gelen bildirimleri "öncelikli" olarak aksiyon almakla yükümlüdür.

¹⁰⁶ DSA Madde 22, https://www.eu-digital-services-act.com/Digital_Services_Act_Article_22.html

Stratejik Tavsiye: Dijital platformlarda toplumsal risklere neden olabilecek içeriklerin hızlı biçimde tespit edilmesi ve yayılımının sınırlandırılması için proaktif gözetim mekanizmaları kurmak amacıyla, teknik ve hukuki liyakati kamuoyu nezdinde kabul görmüş kuruluşlara “**Güvenilir İşaretleyici**” (**Trusted Flagger**) statüsü verilmesi önerilmektedir. Bu kapsamda, Türkiye Bilişim Derneği (TBD) ve benzeri teknik ve hukuki uzmanlığı bulunan kurumların belirli alanlarda yetkilendirilmesi önerilmektedir.

Bu statü ile veri güvenliği, ürün güvenliği, çocukların korunması, çevrim içi dezenformasyon veya siber güvenlik ve benzeri alanlarda uzmanlığı bulunan kuruluşların platformlara yaptıkları bildirimlerinin **öncelikli ve hızlı aksiyon statüsüne** sahip olmasını garanti edecektir.

Bu mekanizma sayesinde toplumsal etkisi olan zararlı içeriklerin yayılımı erken aşamada tespit edilip sınırlandırılabilir ve platformların karar süreçlerinde şeffaflık, itiraz hakkı ve yargısal denetim ilkeleriyle dengelenecek şekilde bir dijital yönetim modeli oluşturulacaktır.

AB-DSA Madde 22 (Güvenilir Bildirici-“Trusted Flaggers”) kavramını düzenler ve bu statüye sahip kuruluşların bildirimlerinin **öncelikli işlenmesini** zorunlu kılar. DSA kapsamında bu statüler sadece belirli uzmanlığa sahip, bağımsız ve güvenilir kuruluşlara imtiyaz olarak verilir.

Platformlar, bu kuruluşların bildirimlerini “öncelikli” değerlendirmek ve karar vermek için gerekli teknik/organizasyonel tedbirleri almakla yükümlüdürler.

AB, DSA kapsamında “Trusted flagger” statüsü, ilgili kuruluşun uzmanlık, bağımsızlık ve objektiflik standartlarını sağlaması halinde o kuruluşun yer aldığı Üye Devletin Dijital Hizmetler Koordinatörü tarafından verilir.

Bu kapsamda Özel Statü verilmiş bazı AB üyesi Örnekler:

Almanya: Bundesnetzagentur (TR'deki BTK muadili kurum) tarafından “Trusted flagger” onaylanmış kuruluşlar;¹⁰⁷

- **Bundesverband Onlinehandel e.V. (BVOH):** e-ticaret alanında uzman ulusal bir dernek.
- **HateAid gGmbH:** Dijital şiddet, dolandırıcılık ve yanıltıcı içeriklerle mücadele eden bir sivil toplum kuruluşu.
- **Verbraucherzentrale Bundesverband e.V. (vzbv):** Alman Tüketici Koruma Derneği; özellikle e-ticaret ve tüketici hakları alanında uzman.

¹⁰⁷ Bundesnetzagentur, Almanya'daki Güvenilir Bildirici Kuruluşlar,

https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/EN/2025/20250602_TrustedFlagger.html

Fransa: Arcom (TR'deki BTK muadili kurum) tarafından tanınan "Trusted flagger" kuruluşlar;¹⁰⁸

- **e-Enfance:** 18 yaş altı kişilerin çevrim içi korunmasına odaklanan kuruluş.
- **ALPA:** Görsel-işitsel korsanlıkla mücadele eden örgüt.
- **IFAW:** doğal hayatın korunması ve ilgili siber suçlarla mücadele örgütü.
- **INDECOSA-CGT:** Tüketicilerin bilgi ve savunmasıyla ilgilenen örgüt.
- **Point de contact :** Siber şiddetle mücadele ve mağdurların korunması.
- **Crif :** antisemitizm ve ırkçılıkla mücadele eden kuruluş.

AB Komisyonu: "Trusted flagger" bazı kuruluşlar;¹⁰⁹

- **Tekijänoikeuden tiedotus- ja valvontakeskus ry:** Finlandiya merkezli telif hakkı ihlalleri uzman kuruluşu.
- **Internet Hotline (Macaristan) :** Çevrim içi içerik ihlallerinin raporlanması için hotline.
- **Schutzverband gegen unlauteren Wettbewerb –** Avusturya'da haksız rekabet ve fikri mülkiyet ihlallerinde uzman.
- **Rat auf Draht gemeinnützige GmbH:** Avusturya'da çocuk istismarı ve benzeri risklere odaklanan kuruluş.

3.4.4. Gerekçeli Karar ve Şeffaflık

Platformlar, içerik kaldırma kararlarını **AB-DSA Madde:17** uyarınca "**Gerekçe Beyanı**" ile açıklamalıdır.¹¹⁰

Platformların karar verme yönünde "hâkim" gibi davranıp gerekçe sunmadan içerik kaldırmasına kısıtlamalar getirilmesi önerilmektedir.

Tespit: Platformlar bir içeriği kaldırdığında kullanıcıya genellikle "Topluluk kurallarımıza uymadığı için..." benzeri otomatik mesaj gönderir. Bu durum, kararın keyfi olup olmadığını, bir algoritma hatası mı yoksa insan hatası mı olduğunu belirtmez. Kullanıcı, hangi kuralı tam olarak nasıl ihlal ettiğini bilemeyebilir.

Türkiye'de sosyal medya platformlarına ilişkin temel düzenleme: 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi Hakkında Kanun 2020 ve 2022 değişiklikleriyle sosyal ağ sağlayıcılarına

¹⁰⁸ Arcom, Fransa'daki Güvenilir Bildirici Kuruluşlar, <https://www.arcom.fr/en/about-us-our-missions/supervise-online-platforms-and-social-networks/digital-services-agreement-dsa-list-trusted-flaggers-designated-arcom>

¹⁰⁹ AB'ndeki Güvenilir Bildirici Kuruluşlar, <https://digital-strategy.ec.europa.eu/en/policies/trusted-flaggers-under-dsa>

¹¹⁰ DSA Madde 17, https://www.eu-digital-services-act.com/Digital_Services_Act_Article_17.html

bazı yükümlülükler getirmiştir. Bu kapsamda platformlar: kullanıcı başvurularına 48 saat içinde cevap vermek, içerik kaldırma taleplerini gerekçeli olarak sonuçlandırmak ve yıllık şeffaflık raporu yayımlamak zorundadır.

Ancak kanun şu konuları ayrıntılı düzenlememektedir: moderasyon kararını insan mı yoksa algoritmanın mı verdiği, ihlal edilen kuralın detaylı açıklaması ve sürecinin teknik gerekçesi. Bu nedenle mevzuatın “**cevap yükümlülüğü**” getirdiği ancak **algoritmik şeffaflık zorunluluğu getirmediği** değerlendirilmektedir.

Küresel Çözüm: AB-DSA Madde 17 kapsamında getirilen "Gerekçe Beyanı" zorunluluğuna istinaden, platform; kararın hangi yasal maddeye veya politika kuralına dayandığını, kararın algoritmik bir araçla mı verildiğini ve itiraz yollarını belirten detaylı bir açıklama sunmakla yükümlüdür.

Bu kapsamda platformlar:

- İçeriğin kaldırılıp kaldırılmadığını, erişimin engellenip engellenmediğini veya görünürlüğünün kısıtlanıp kısıtlanmadığını belirtmelidir.
- Alınan kararın somut gerekçelerini, hangi hukuki dayanağa veya hizmet şartı ihlaline dayandığını açıklamalıdır.
- Otomatik araçların kullanılıp kullanılmadığını ve itiraz/telafi yollarını kullanıcıya açıklamalıdır.
- Alınan kararın türü (kaldırma, erişim engelleme, görünürlük azaltma vb.) ve süresi/etki alanı.
- Kararın dayandığı gerçekler ve koşullar, ilgili bildirim (örneğin Madde 16’ya göre yapılan) veya platformun kendi inisiyatifi.
- Hukuki veya sözleşmesel dayanak ile neden bu içerik veya davranışın yasadışı veya hizmet şartlarına aykırı olduğu açıklaması.
- Kullanıcıya başvuru/itiraz yolları ve şikâyet süreçlerine dair bilgi.

Stratejik Tavsiye: Dijital platformlarda içerik kaldırma, görünürlük azaltma veya hesap kısıtlama gibi moderasyon kararlarının şeffaf ve denetlenebilir bir çerçeveye kavuşturulması amacıyla, platformlara yönelik “**Şeffaflık Standartları**” getirilmesi önerilmektedir. Bu kapsamda platformların aldığı her içerik kısıtlama kararının; kullanıcıya **anlaşılabilir bir içerikte Türkçe** olarak ve somut gerekçelerle bildirilmesi sağlanmalıdır. Bildirimde sıralanan unsurların yer alması önem taşımaktadır: İhlal edildiği iddia edilen kural veya politika maddesi, kararın kapsamı (içeriğin kaldırılması, görünürlük azaltma, hesap kısıtlaması vb.), kararın algoritmik bir süreç sonucu mu yoksa insan moderasyonu ile mi verildiği ve kullanıcıya tanınan itiraz ve inceleme mekanizmaları.

Buna ilaveten platformların bu moderasyon kararlarına ilişkin verileri **toplu ve anonimleştirilmiş şekilde**

düzenli olarak raporlamalıdır. Bu raporlamanın, BTK (Bilgi Teknolojileri ve İletişim Kurumu) gibi yetkili bir otoriteye sunulması veya kamuya açık veri tabanları aracılığıyla yayımlanması önerilmektedir.

Bu doğrultuda, Avrupa Birliği’nde Digital Services Act kapsamında oluşturulan “**DSA Transparency Database; Şeffaf Veritabanı**” benzeri bir sistemin Türkiye’de de geliştirilmesi değerlendirilebilir. Böyle bir veri tabanı, platformların içerik kısıtlama kararlarının **istatistiksel olarak izlenmesini, karşılaştırılmasını ve kamuoyu tarafından denetlenebilmesini** mümkün kılarak dijital platform yönetişiminde hesap verebilirliği güçlendirecektir.

3.5. Kullanıcı Hakları ve Şikâyet Yönetimi

Platformların tek taraflı gücü denetleme mekanizmalarıyla sınırlanmalıdır. Kullanıcının platformla olan uyumsuzluğunu ilk aşamada, platform içerisinde ancak nitelikli bir süreç ile çözebilmesinin sağlanması hedeflenmektedir.

Tespit: Türkiye’de bir kullanıcının içeriği kaldırıldığında veya hesabı askıya alındığında platformların sunduğu “itiraz et” seçeneği çoğu zaman sınırlı bir geri bildirim mekanizması olarak işlemekte ve çoğu durumda kullanıcıya itirazın gerçekten yeniden incelenip incelenmediği, incelemeyi yapan kişinin yetkinliği veya hangi gerekçelere istinaden işlem yapıldığı konusunda yeterli açıklama yapılmamaktadır.

Bu durum, kullanıcıların platform kararlarına karşı etkili bir savunma yapmasına olanak vermemekte ve süreçlerinin kullanıcı açısından **şeffaf olmayan algoritmik sistemler** tarafından yürütüldüğü algısını pekiştirmektedir.

Küresel Çözüm: Avrupa Birliği’nde bu sorun, DSA (Digital Services Act, Dijital Hizmetler Yasası) 20. maddesi kapsamında getirilen düzenlemelerle ele alınmıştır. Platformlar, içerik kaldırma veya hesap kısıtlama kararlarına karşı kullanıcıların başvurabileceği **ücretsiz ve erişilebilir bir iç şikâyet mekanizması** oluşturmak zorundadır. Bu sistemde kullanıcılar, kararın kendilerine bildirilmesinden itibaren **en az altı ay boyunca** platform içinde itiraz edebilmektedir ve itirazlar ilk **karardan bağımsız, nitelikli personel tarafından değerlendirilir**. DSA Madde 20 uyarınca, en az 6 ay süresince, liyakatli personel tarafından yürütülen ücretsiz iç şikâyet sistemleri kurulmalıdır.¹¹¹

Stratejik Tavsiye: Dijital platformların içerik kaldırma, görünürlük azaltma veya hesap kısıtlama kararlarına karşı kullanıcıların etkili bir başvuru yoluna sahip olabilmesi amacıyla, ilgili kanun (5651) kapsamında platformlara “**Etkin İç İtiraz Yolu**” kurma yükümlülüğü getirilmesi önerilmektedir.

¹¹¹ DSA Madde 20, https://www.eu-digital-services-act.com/Digital_Services_Act_Article_20.html

Söz konusu mekanizma çerçevesinde platformlar: içerik kaldırma veya hesap kısıtlama kararlarına karşı kullanıcıların belirli bir süre içinde itiraz edebilmesini sağlamalı, yapılan itirazları makul süre içinde yeniden incelemeli, ve inceleme sonucunu kullanıcıya **somut ve anlaşılabilir gerekçelerle** bildirmelidir.

Bu bildirimler yalnızca “onaylandı” veya “reddedildi” şeklinde otomatik yanıtlarla sınırlı kalmayıp; ihlal kuralın açıkça belirtilmesi, kararın kapsamının açıklanması ve kullanıcının başvurabileceği diğer itiraz yollarına ilişkin bilgilendirmeleri de ihtiva etmelidir.

3.5.1. Mahkeme Dışı Çözüm

Mahkemelerin iş yükünü azaltmak amacıyla DSA Madde 21 gereğince uyumlu ve bağımsız uyuşmazlık çözüm organları sertifikalandırılmalıdır.¹¹²

Her dijital tartışmanın mahkemeye taşınması, sistemin hantallığına ve de adaletin gecikmesine neden olabilir.

Tespit: Bir platformla uyuşmazlık yaşayan (Örn.: haksız telif ihtarı veya haksız hesap kapatma) kullanıcının yasal yolu izleyerek dava açması gerekir. Mahkemelerin yoğunluğu ve dijital terminolojiye uzak kalabilmesi nedeniyle, süreç aylarca sürebilir ve de maliyetli olmasına neden olur. Bu durum küçük işletmeleri ve bireysel kullanıcıları platformun gücü karşısında zor durumda bırakabilir.

Küresel Çözüm: EU DSA Madde 21 gereğince; Platformlar, bağımsız ve sertifikalı **mahkeme dışı uyuşmazlık çözüm organlarının** (bir nevi arabuluculuk sistemi) kararlarına uymayı (bazı istisnalar hariç) taahhüt eder. Bu aracı yapılar mahkemeden çok daha hızlı ve teknik uzmanlıkla karar veren "Dijital Ombudsmanlar" gibi çalışır. Bu organlar, AB üye devletlerindeki dijital hizmet koordinatörleri (DSC) tarafından belirli kriterlere (bağımsızlık, uzmanlık, verimlilik) göre sertifikalandırılır.

Stratejik Tavsiye: Türkiye’de arabuluculuk ve tüketici hakem heyetleri gibi alternatif uyuşmazlık çözüm mekanizmaları bulunmaktadır ancak, bu kurumlar dijital platformlar la ilişkili uyuşmazlıkları çözmek üzere tasarlanmamıştır. Bu sorunu çözecek şekilde DSA-21. madde uyarınca bir düzenleme önerilmektedir.

3.5.2. Dijital Uyuşmazlık Yönetimi ve Yetkilendirme Mekanizması

İnternet ekosistemindeki içerik uyuşmazlıklarının teknik ve hızlı bir şekilde çözüme kavuşturulması amacıyla, **BTK denetiminde** veya yetkilendirilmiş **STK’lar bünyesinde** işletilecek bir "**Dijital Uyuşmazlık Yönetim Sistemi**" kurulması önerilmektedir. Bu yapı sayesinde platformlar ile kullanıcılar

¹¹² DSA Madde 21, https://www.eu-digital-services-act.com/Digital_Services_Act_Article_21.html

arasındaki uyuşmazlıklar yargı aşamasına taşınmadan idari ve teknik bir değerlendirmeden geçirecek yetkinlikte bir sertifikasyon sistemi olarak tasarlanmalıdır.

Sistemin Temel Bileşenleri:

- **Yetkilendirilmiş Kurullar:** BTK ve benzeri kurum tarafından belirli teknik ve hukuki kriterlere göre akredite edilmiş, tarafsızlığı tescilli uzman kuruluşlardır. (Örn: Türkiye Bilişim Derneği (TBD), Barolar veya uzman arabuluculuk merkezleri).
- **Hızlı Karar ve Teknik İnceleme:** Bu kuruluşlar dijital telif, içerik kaldırma ve platform kurallarına aykırılık gibi konularda, düşük maliyetli ve hızlı işlevde **"idari ön inceleme/hakemlik"** mekanizması olarak görev yaparlar.
- **Standartlaştırma:** Çalışma usulleri ve kararların formatları yayımlanan teknik düzenlemelerle standardize edilir.

Platformların Türkiye’de milyonlarca kullanıcıya hizmet verdiği düşünülürse, **son merci olan mahkemelere gitmeden önce bağımsız bir çözüm mekanizması** ciddi bir eksikliği doldurabilir.

3.6. Karanlık Tasarım (Dark Patterns) ve Erişilebilirlik

Dijital platformlarda kullanıcı davranışını manipüle etmeye yönelik **karanlık tasarımlar** (dark patterns), kullanıcıların hak arama yollarına erişimini zorlaştırabilmekte ve platformlar ile kullanıcılar arasındaki haksız bir güç dengesizliğine neden olmaktadır. Avrupa Birliği- DSA-Madde 25 ile bu tür manipülatif arayüz tasarımlara sınırlandırma getirmiştir ve platformların kullanıcıyı yanıltmaya veya yönlendirmeye sevk eden uygulamaları kullanması yasaklanmıştır.¹¹³

Hak arama yolları, kullanıcının karşısına bir "labirent" gibi çıkarılmamalıdır.

Tespit: Türkiye’de dijital platform faaliyetlerine ilişkin çeşitli hukuki düzenlemeler yürürlüktedir. (5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi Hakkında Kanun, 6502 sayılı Tüketicinin Korunması Hakkında Kanun, 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun, 6698 sayılı Kişisel Verilerin Korunması Kanunu, ayrıca 6102 sayılı Türk Ticaret Kanunu’nun haksız rekabete ilişkin hükümleri ile Ticari Reklam ve Haksız Ticari Uygulamalar Yönetmeliği)

Söz konusu düzenlemeler; tüketicinin korunması, ticari iletişim ve reklam uygulamaları, içerik sorumluluğu, haksız rekabet ve kişisel veri güvenliği gibi alanlarda koruma mekanizmaları oluşturmakta ve belirli ölçüde kullanıcıların ekonomik ve kişisel menfaatlerini güvence altına almaktadır.

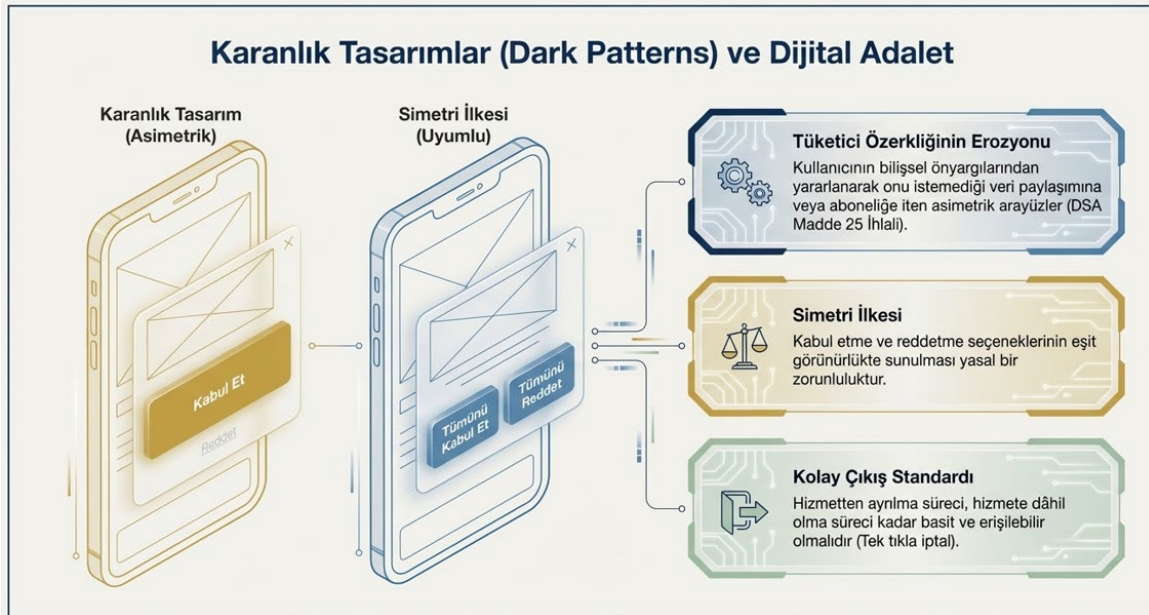
¹¹³ DSA Madde 25, https://www.eu-digital-services-act.com/Digital_Services_Act_Article_25.html

Ancak, bu mevzuatta dijital platformların kullanıcı arayüzlerinde başvuru manipülatif tasarım teknikleri (dark patterns) bakımından açık bir düzenleme yer almamaktadır.

Uygulamada bazı küresel platformların itiraz veya şikâyet mekanizmalarının bazen İngilizce olarak sunulduğu, ya da bu mekanizmaların kullanıcıların başvuru yapmasını zorlaştıracak şekilde **karmaşık menü yapıları içinde konumlandırıldığı** örnekler görülmektedir. Dijital hizmetlere erişilebilirlik, hem eşitlik ilkesi hem de kamu hizmetlerine erişim açısından önem taşımaktadır.

Küresel Çözüm: EU-DSA Madde 25'e istinaden, kullanıcıyı bir karara yönlendiren veya karar vermesini zorlaştıran "Karanlık Tasarımlar" yasaklanmıştır. Ayrıca süreçlerin kullanıcının kendi dilinde, açık ve erişilebilir olması şartı getirilmiştir.

Stratejik Tavsiye: Türkiye'de faaliyet gösteren dijital platformların kullanıcı destek, şikâyet ve itiraz mekanizmalarının **Türkçe seçenekli olarak sunulması** ve bu arayüzlerin **uluslararası erişilebilirlik standartlarına** uygun şekilde tasarlanması yasal bir zorunluluk haline getirilmelidir. Bu kapsamda platform arayüzlerinin en az **WCAG 2.1 (Web Content Accessibility Guidelines)** veya üzeri erişilebilirlik standartlarına uyumu sağlanmalıdır. Dijital hizmetlere eşit erişimin sağlanması için **engelli bireylerin hak arama yollarına kolay erişebilmesi** de temel bir dijital hak olarak ele alınmalıdır. ABD'de de kamu kurumları için 'Section 508 of the Rehabilitation Act' çerçevesinde WCAG tabanlı erişilebilirlik standartları uygulanmaktadır. Bu yaklaşım ile WCAG standartları, dijital hizmetlerin tasarımında erişilebilirlik ve kullanıcı haklarının korunması bakımından temel referans çerçevesi olarak kabul görmektedir.



ŞEKİL 3-1: Karanlık Tasarımlar (Dark Patterns) (YZ ile hazırlanmıştır)

Çocukların Korunması: UK Online Safety Act (OSA)¹¹⁴ ve OECD Çocuk Tavsiyesi¹¹⁵ uyarınca; "Özen Yükümlülüğü" (Duty of Care) ve "Tasarım Yoluyla Güvenlik" (Safety by Design) ilkeleriyle yaş doğrulaması zorunlu kılınmalıdır.

Online Safety Act 2023, teknoloji şirketlerine yasal bir "Duty of Care" (Özen Yükümlülüğü) yükler. Yasanın 79-84. bölümleri, özellikle çocukların zararlı içeriklere (pornografi gibi) erişimini engellemek için "Age Verification" (Yaş Doğrulaması) sistemlerini zorunlu kılar.

OECD'nin 2021 tarihli Çocuk Tavsiyesi, dijital ürünlerin henüz fikir aşamasındayken güvenli tasarlanmasını (Safety by Design) bir standart olarak belirler.

Çocuklar için pasif bir yasaklama yerine, aktif bir koruma kalkanı oluşturulmalıdır.

3.7. AB-CSAM Işığında Türkiye’de Çocuk Koruma Mekanizmaları

Avrupa Birliği'nin Çocukların Cinsel İstismarıyla Mücadele (CSAM: Child Sexual Abuse Material) mevzuat tasarısı, teknoloji şirketlerinin yasa dışı içerikleri tespit edip kaldırmadaki yetersizlikleri ve ilaveten üye ülkelerin birbirinden farklı ulusal yasaları nedeniyle AB-Dijital Birlik Pazarındaki hukuksal karışıklıklara neden olması sebeplerinden dolayı gerekli olmuştur.

Internet Watch Foundation (IWF) verilerine göre¹¹⁶, küresel çapta hızla artarak 2023 yılında 35,9 milyona ulaşan istismar bildirimlerine konu olan içeriklerin %59'unun AB üyesi ülkelerde oluşmuştur. Bu sebeple AB nin bu zorunlu düzenlemeye olan ihtiyacı acil hale gelmiştir.

Dijital platform ortamlarında çocukların korunması amacıyla, Avrupa Birliği'nin **Çocukların Cinsel İstismarıyla Mücadele (CSAM)¹¹⁷ Tasarısı'nda COM (2022) 209 Tasarısıyla¹¹⁸** öngörüldüğü üzere, "Tasarım Yoluyla Güvenlik" (Safety by Design) ilkesini temel alan proaktif ve yapısal tedbirlerin ulusal mevzuata entegre edilmesi bir zorunluluk haline gelmiştir. Bu kapsamda ulusal mevzuatta aşağıdaki mekanizmaların kurgulanması önerilmektedir:

¹¹⁴ Online Safety Act (OSA) in UK, <https://www.legislation.gov.uk/ukpga/2023/50/contents/enacted>

¹¹⁵ Recommendation of the Council on Children in the Digital Environment, <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0389>

¹¹⁶ EU still hosts the most child sexual abuse material in the world <https://www.iwf.org.uk/news-media/news/eu-still-hosts-the-most-child-sexual-abuse-material-in-the-world/>

¹¹⁷ Protecting children from sexual abuse, https://home-affairs.ec.europa.eu/policies/internal-security/protecting-children-sexual-abuse_en

¹¹⁸ Proposal for laying down rules to prevent and combat child sexual abuse, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0209>

1) **Risk Yönetimi Standartlarının Belirlenmesi:** Platformların çocuk istismarı materyallerini tespit eden süreçlerin yasal standartlara bağlanması elzem hale gelmiştir. Türkiye'de aynı hedef altında ele alınmalıdır. Barındırma (hosting) ve iletişim (mesajlaşma vb.) hizmeti sağlayıcılarına birtakım yaptırımlar getirilmeli ve çocukların cinsel amaçlı manipülasyonu (grooming) önlemek için düzenli olarak analiz etme ve bu riskleri ortadan kaldıracı algoritmik ve yapısal tedbirler alma yükümlülüğü ivedilikle getirilmelidir.

2) **Hedefli Tespit Emirleri (Detection Orders) Mekanizmasının Kurulması:** Mevcut mevzuatımızda yetkili makamların içerik kaldırma yetkileri bulunmaktadır. Buna ilave olarak, zararlı içeriği platformun tespit edip proaktif bir yapıda engelleyecek bir hukuki yapıya ihtiyaç duyulmaktadır. AB-CSAM tasarısına göre, risk azaltıcı önlemlerin yetersiz kaldığı durumlarda, bağımsız idari veya adli otoritelerce "Hedefli Tespit Emirleri" verilebilmelidir.

Bu emirler ile, CSAM içeriklerini ve "grooming" (cinsel amaçlı manipülasyon) faaliyetlerini tespit edecek teknolojileri kullanacak şekilde olacaktır. Tespit emri tüm platformun bir bölümüne, belirli kanallara veya izole edilebilen belirli kullanıcı gruplarına yönelik olarak kısıtlanabilir.

3) **Güvenilir ve Mahremiyet Odaklı Yaş Doğrulama (Age Verification) Altyapısının Kurulması:** Mevcut 5651 sayılı Kanun taslağında 15 yaş altı kullanıcılara yönelik hizmet yasağı getirilmesi ve platformlara yaş doğrulama yükümlülüğü verilmesi önemli bir adımdır. Ancak, yaş doğrulama (Age Verification) mekanizmalarının tasarımı ve işletilmesinin tamamen teknoloji şirketlerinin inisiyatifine bırakılması gereklidir. Kişisel verilerin korunması (KVKK/GDPR) ile ulusal güvenlik prensipleri açısından güvenilirlik zafiyetleri barındırmamasına yönelik uygulamalar getirilmelidir.

Avrupa Birliği'nin yaş doğrulama sistemlerini dijital kimlik cüzdanlarıyla (eIDAS) entegre etme planı özetle; **kimlik detaylarını platformlara ifşa etmeden, doğrulama işleminin yalnızca bağımsız otoritelerce yapılarak çocukların mahremiyetinin "tasarım yoluyla" (privacy by design) korunduğu güvenli bir altyapı kurulması amaçlamaktadır.**¹¹⁹

Bu bağlamda Türkiye'nin; kullanıcıların kimlik belgelerini doğrudan platformlara sunmak yerine, e-Devlet gibi ulusal güvenli altyapılarla entegre ve platformlara kullanıcının sadece "ilgili yaş sınırının üstünde/altında olduğu" bilgisini aktaran, devlet güvencesindeki bir yaş doğrulama sistemi kurulması gereklidir.

4) **Dijital Çocuk Koruma İhtisas Biriminin Kurulması:** Platformların algoritmik taramalar sonucunda buldukları şüpheli durumları yönetecek, "AB Çocuk Cinsel İstismarı Merkezi" (EUCSA) modeline benzer bir yapının oluşturulması önerilmektedir. BTK veya USOM bünyesinde kurulabilecek bu biriminin muhtemel görevleri listelenmiştir:

- Platformlara tespit süreçlerinde kullanmaları için güvenilir veri tabanları (hash özetleri, URL listeleri vb) sağlamak.

¹¹⁹ The EU approach to age verification, <https://digital-strategy.ec.europa.eu/en/policies/eu-age-verification>

- Platformlardan gelen tespit raporlarını adli makamlara iletilmeden önce teknik bir ön değerlendirmeden geçirerek doğruluk oranını artırmak.
- Mağdur çocukların tespiti ve kurtarılması süreçlerinde kolluk kuvvetleriyle iletişim ve işbirliği yapmak.
- Yurt dışındaki içerik sağlayıcısına ulaşamayan platformlarda tutulan CSAM içeriklerinin Türkiye'den erişiminin kesilmesi için, doğrulanmış URL listelerine dayalı olarak, internet erişim sağlayıcılarına (ISP) hızlı ve doğrudan "Erişim Engelleme Emirleri" (Blocking Orders) verilebilmesine olanak tanıyan net bir hukuki standart oluşturulmalıdır.

Bu adımlar sayesinde, Türkiye'nin içerik yönetişimi çocukları aktif algoritmik sistemlerle koruyan ve uluslararası teknik standartlarla (AB CSAM) uyumlu bir duruma getirecektir.

3.8. Seçim Dürüstlüğü ve Reklam Şeffaflığı:

Çok büyük çevrim içi platformlar (VLOP), **DSA Madde 34**¹²⁰ uyarınca seçim süreçlerine müdahale veya ifade özgürlüğü gibi konularda yılda en az bir kez risk analizi yapmakla yükümlüdür. DSA Madde 39 ile de reklam arşivlerinin (Ad Repository) platformda son kez gösterilmesinden itibaren 1 yıl süreyle tutulması ve erişilebilir olmasını zorunlu kılar. Bireysel cezalandırmadan ziyade, manipülasyonu besleyen sistemik zafiyetlerin giderilmesi öncelik olarak hedeflenir.

Şeffaflık Raporlaması ve "Kara Kutu" (Black Box) Sorunu

Şeffaflık, dijital platformların ne yaptığından başka, nasıl yaptığını açıklamak olarak özetlenebilir. Mevcut sistemde platformlar "veriyi paylaştık" diyerek sorumluluktan kaçma yoluna gidebilirler. OECD'nin yaklaşımında şeffaflık bir "istatistik" değil, bilakis "denetim aracı" olarak yer alır.

Burada hedefimiz; raporların niteliksel (kalitatif) derinliğini artırmak, bağımsız denetim mekanizmalarını sisteme entegre etmek ve "toplumsal katılım" yaklaşımıyla kamu-özel sektör-akademi dinamik etki üçgenini oluşturmaktır.

OECD Gönüllü Şeffaflık Raporlama Çerçevesi (Voluntary Transparency Reporting Framework-VTRF)¹²¹ , raporlamanın sadece niceliksel değil, yönetsel olmasını koşul olarak belirtir. Şeffaflık raporları için OECD VTRF standartları yasal temel olarak kabul edilebilir. Platformlar; içerik

¹²⁰ DSA Madde 34, https://www.eu-digital-services-act.com/Digital_Services_Act_Article_34.html

¹²¹ OECD (2021), "Transparency reporting on terrorist and violent extremist content online: An update on the global top 50 content sharing services", *OECD Digital Economy Papers*, No. 313, OECD Publishing, Paris, <https://doi.org/10.1787/8af4ab29-en>.

algoritmelerde kullanılan yapay zekâ araçlarının hata paylarını ve hangi dillerde ne kadar doğruluk oranıyla işlendiğini raporlarında beyan etmelidir.

OECD'nin "Terörist ve Şiddet İçerikli Aşırı Söylemler" (TVEC) üzerine kurduğu VTRF çerçevesi, sadece "kaç içerik sildik?" gibi sayısal verilerle yetinmez. Şirketlerin; algoritmik hataları, "False Positive" (yanlışlıkla silinen meşru içerik) oranlarını ve moderasyon süreçlerindeki insan müdahalesinin niteliklerinin de raporlamasını gerekli kılar.

"Algoritma öyle çalışıyor" tarzı bahanelerin sorgulanabileceği hukuki denetlenebilirlik mekanizmaları oluşturulmalıdır.

Tespit: Platformlar, algoritmalarının nasıl çalıştığını "ticari sır" gerekçesiyle kamuoyuna ve bağımsız denetçilere kapatabilirler. Bu kısıtlama, toplumsal olaylarda (Örn.: doğal afetler, toplumsal protestolar vb) verilerin nasıl kullanıldığının veya nasıl manipüle edildiğinin bilimsel olarak kanıtlanmasını imkansız kılar.

Küresel Çözüm: EU DSA Madde 40: Bu madde uyarınca, "onaylanmış araştırmacılar" (vetted researchers) ve kamu otoriteleri, sistemik riskleri ölçmek amacıyla platformların anonimleştirilmiş ham verilerine erişim hakkına sahiptir.¹²²

Stratejik Tavsiye: Akademisyenlerin ve kamu yararı gözetilen sivil toplum kuruluşlarının, toplumsal menfaate istinaden, platformların algoritmik etkilerini (dezenformasyonun yayılma hızı vb.) ölçebilmesi için "Denetlenmiş Veri Erişimi" kanalları açılmalıdır. Algoritmalar bir "kara kutu" olmaktan çıkarılmalıdır. AB-DSA Madde 40 uyarınca; çok büyük platformlar, sistemik riskleri incelemek üzere onaylanmış araştırmacılara (vetted researchers) veri sağlamakla yükümlüdür.

Türkiye Karşılaştırması: AB'deki Dijital Hizmetler Yasası'nın (DSA) aksine, Türkiye'deki 5651 veya 7418 sayılı kanunlar kapsamında, dijital platformların verilerini bağımsız araştırmacıların erişimine açma yükümlülüğü yer almamaktadır. (Veri paylaşım yükümlülüğü yetkili kamu kurumları ve adli makamlar ile sınırlıdır.) Platformlar (Instagram, X, TikTok vb.) içerikleri hangi kriterlere göre öne çıkardıklarını veya kısıtladıklarını belirleyen algoritmalarını fikri mülkiyet kapsamında ticari sır olarak kabul ederler.

TABLO 3-1: Şeffaflık Konusunda Türkiye ve AB Mevzuat Karşılaştırma Tablosu

Karşılaştırma Alanı	Türkiye Mevzuatı (5651 & 7418)	AB Mevzuatı (DSA) / Uluslararası Standart	Not
Algoritmik Şeffaflık	Sınırlı. 7418 ile BTK'ya veri isteme yetkisi verilmişse de halka açık bir şeffaflık veya denetim yoktur.	Zorunlu. Algoritmaların toplum üzerindeki riskleri (sistemik risk) raporlanmalıdır.	DSA Madde 34 & 35

¹²² DSA Madde 40, https://www.eu-digital-services-act.com/Digital_Services_Act_Article_40.html

Karşılaştırma Alanı	Türkiye Mevzuatı (5651 & 7418)	AB Mevzuatı (DSA) / Uluslararası Standart	Not
Araştırmacı Veri Erişimi	Yok. Bağımsız araştırmacıların (Akademisyenlerin veya STK'lar) ham veriye (manipülasyon analizi için) erişim hakkı bulunmamaktadır.	Zorunlu. Platformlar, onaylanmış araştırmacılara veri setlerini açmakla yükümlüdür.	DSA Madde 40
Bağımsız Denetim	Sınırlı/Yargısal. Denetim yalnızca adli/idari (BTK/Mahkeme) kanallarla yapılır.	Zorunlu. Yıllık bağımsız denetim (Independent Audit) şarttır.	DSA Madde 37
Kullanıcı Hakları	Reaktif. İçerik kaldırıldıktan sonra itiraz edilir; algoritma seçimine müdahale hakkı yoktur.	Proaktif. Kullanıcıya, içeriğin neden gösterildiğine dair bilgi alma hakkı tanınır.	DSA Madde 27 (Tavsiye Sistemleri)

3.9. Bağımsız Denetim ve Yeni Yönetişim Modeli

Platformların "kendi kendini denetlediği" sistemler yeterli değildir ve dış bağımsız denetime olanak veren yapılanmalar gerekmektedir.

Tespit: Türkiye'deki mevcut denetim mekanizmasında, platformların risk yönetim stratejilerinin, algoritma güvenliğinin veya toplumsal etkilerinin bağımsız kuruluşlarca düzenli olarak denetlendiği bir '**Bağımsız Denetim**' (Audit) zorunluluğu bulunmamaktadır. Her ne kadar BTK'nin, veriye erişim yetkisi olsa da, platformun sistemik risklerini teknik bir denetçi gözüyle periyodik olarak incelemek ve kamuoyuna raporlamak şeklinde bir fonksiyon olarak tanımlanmamıştır.

Küresel Çözüm: EU DSA Madde 28: Çok Büyük Çevrim İçi Platformlar (VLOP), yılda en az bir kez "**Bağımsız Denetim**" (Independent Audit) kuruluşları tarafından denetlenmek ve kriterleri karşılayacak halde bir uyum raporu almak zorundadır.¹²³

Stratejik Tavsiye: Belirli bir ciro veya kullanıcı sayısını aşan platformlara sertifikalı ve bağımsız teknik kuruluşlar tarafından periyodik "Uyum Denetimi" (Compliance Audit) yaptırma zorunluluğu getirilmelidir. Bu denetimlerin raporları BTK, yetkili STK'lar ve kamuoyu ile paylaşılmalıdır.

Dijital platformları düzenlemek, sadece ceza kesmek değildir; platformların sağlıklı bir rekabet ortamında toplumsal fayda üretmesini sağlamaktır.

Sektörel büyümeyi engellemeden, etkin denetim için önerilen yapılar:

¹²³ DSA Madde 28, https://www.eu-digital-services-act.com/Digital_Services_Act_Article_28.html

3.9.1. Bağımsız Dijital Hizmetler Koordinatörü:

BTK bünyesinde veya bağımsız bir yapı altında, bağımsız ve apolitik olarak, sadece teknik ve hukuki denetim yapacak özerk bir birim kurulmasında fayda vardır. Denetimin teknik ve hukuki özerkliğini sağlamak, yatırımcıya güven vermek ve aynı zamanda ifade özgürlüğünü güvence etmek için elzem koşuldur.

Tespit: Türkiye'deki mevcut dijital denetim yapısında, düzenleyici kurumların **idari özerklik ve karar alma süreçlerindeki şeffaflık** düzeyine ilişkin yapısal tartışmalar bulunmaktadır.

Küresel Çözüm: AB-DSA Madde 38 uyarınca her üye ülke, bir **"Dijital Hizmetler Koordinatörü" (Digital Services Coordinator)** atamak zorundadır. Bu koordinatör; tam bir hiyerarşik ve mali bağımsızlığa sahip olmalıdır ve siyasi etkiden arındırılmış şekilde sadece yasal uyumu denetlemelidir.

Stratejik Tavsiye: BTK bünyesinde veya özerk bir yapı altında, AB ile uyumlu olacak kriterlerde sadece teknik ve hukuki denetim yetkisiyle donatılmış bir **Dijital Hizmetler Koordinatörlüğü** kurulabilir. Bu yapı, liyakat sahibi uzmanlardan oluşmalı ve kararlarını şeffaf olarak denetime açık şekilde almalıdır.

3.9.2. Birlikte Düzenleme (Co-Regulation):

AB uyumlu, platformların kendi etik kurallarını (Code of Conduct) oluşturduğu ve devletin bu uyumu denetlediği esnek bir model tesis edilebilir. Sektörel gelişim için esnek ve katılımcı yönetim modelleri önerilmektedir.

Tespit: Türkiye'deki dijital regülasyon çerçevesi, teknolojik inovasyonun hızına karşın geleneksel yasama süreçlerinin statik ya da yavaş olarak tanımlayabileceğimiz uyumsuzlukları nedeniyle, 'Pacing Problem' (Hız Sorunu) riskiyle yüzleşmektedir.

Küresel Çözüm: EU DSA Madde 45-48 ve OECD Dijital Yönetişim İlkeleri. ^{124, 125, 126}

Bu modelde devlet, genel çerçeveyi (çerçeve yasa) belirler; platformlar ise bu çerçeveye uyum için kendi **"Etik: Davranış Kodlarını" (Codes of Conduct)** oluşturur. Devlet görev olarak, platformların kendi koydukları ve taahhüt ettikleri bu kurallara uyup uymadığını denetler.

Stratejik Tavsiye: Platformların (özellikle VLOP'ların) kendi özdenetim mekanizmalarını kurduğu ve devletin bu süreci akredite ettiği bir **"Birlikte Düzenleme" (Co-Regulation)** modeli benimsenmelidir. Bu sayede, örneğin dezenformasyonla mücadele veya çocuk koruma gibi alanlarda platformların teknik yetkinliği, devletin denetim gücüyle birleştirilmiş olur. Bu model dijital pazarda küresel rekabet ve istikrar açısından stratejik bir öneme sahiptir.

¹²⁴ DSA Madde 45, https://www.eu-digital-services-act.com/Digital_Services_Act_Article_45.html

¹²⁵ DSA Madde 48, https://www.eu-digital-services-act.com/Digital_Services_Act_Article_48.html

¹²⁶ OECD, Digital Government, <https://www.oecd.org/en/topics/digital-government.html>

3.9.3. Asimetrik Regülasyon ve Kademeli Sorumluluk Modeli:

Dijital pazarda rekabetin korunması ve yerli teknoloji ekosisteminin (startup/scale-up) sürdürülebilirliği için "tek tip regülasyon" uygulaması yeterli olmamaktadır. Asimetrik regülasyon denilen model ile, regülatif düzenlemeler ve yükümlülükler için kriterler belirlenir. Platformun pazar gücü, kullanıcı sayısı ve oluşturduğu sistemik riskle orantılı olarak bu kriterler belirlenebilir. Bu modelin temel amacı, yerli girişimlerin henüz büyüme aşamasındayken "uyum kriterleri ve maliyetleri" altında ezilmesini engellemek ve küresel devlere karşı rekabet desteği sağlamaktır.

Uygulama Çerçevesi ve Segmentasyon

Kapsam (Segmentasyon)	Temel Strateji	Operasyonel Hedef
Mikro ve Küçük Yerli Girişimler (Startuplar)	Muafiyet ve Esneklik: Ağır denetim ve raporlama yükümlülüklerinden muaf tutulmalıdır.	İnovasyon bariyerlerini minimize ederek, yerli sermayenin pazara girişini ve büyümesini kolaylaştırmak.
Orta Ölçekli Platformlar	Kademeli Uyum: Ölçek büyüdükçe artan, ancak operasyonel kapasiteyle uyumlu sınırlı sorumluluklar.	Büyüme sürecindeki şirketleri kurumsallaşmaya hazırlamak.
Çok Büyük Çevrim içi Platformlar (VLOPs)	Sıkı Denetim ve Şeffaflık: DSA standartlarında tam kapsamlı bağımsız denetim ve algoritmik hesap verebilirlik.	Toplumsal ölçekli sistemik risklerin (dezenformasyon, seçim manipülasyonu, veri güvenliği) proaktif kontrolü.

3.10. Stratejik Sonuç: Küresel Rekabetçilik ve Uyum

Önerilen bu reform süreci, Türkiye'nin dijital pazarını sadece yerel bir mevzuatla sınırlamak yerine, küresel ekosistemle uyumlu çalışabilir (interoperable) bir yapıya imkân sağlayacaktır. Bu dönüşümün ortaya çıkaracağı stratejik değerler aşağıda yer alan ana başlıklarda özetlenebilir:

Hukuki Öngörülebilirlik ve Yatırım İklimi

Dijital ekonominin istikrarlı olması ve sürdürülebilir büyümesi, regülasyonlar, hukuki çerçeve ve öngörülebilirlik ile doğrudan ilişkilidir. Kuralların ve düzenlemelerin net olarak önceden tanımlandığı, şeffaf süreçler ve bağımsız denetim mekanizmalarıyla desteklenen bir yönetim yaklaşımı, piyasa aktörleri açısından oldukça önemli kriterlerdir. Bu tür güvenilir işlevsellik ile, dijital pazarın daha da istikrarlı bir yapıya kavuşması; yatırımların teşvik edildiği, fikri mülkiyet haklarının korunduğu ve operasyonel güvenliğin güçlendiği bir ekosistemin gelişip büyümesine katkı sağlayacaktır.

Startup Ekosistemi İçin Küresel Kaldıraç Etkisi

OECD ve AB standartlarıyla (DSA/DMA ve EAA) uyum sağlamak, Türk teknoloji girişimleri (startup) için sadece bir uyum meselesi değil, aynı zamanda küresel pazarlara girişi kolaylaştıran bir stratejik unsurdur. Yerli girişimler, Türkiye sınırları içerisinde bu yüksek standartlara göre yapılandıklarında, Avrupa ve dünya pazarlarına açıldıklarında karşılaşacakları "regülasyon bariyerlerini" henüz yolun başındayken aşmış olacaklardır. Bu durum, şüphesiz ki "Türkiye'den çıkan teknoloji" imajını küresel ölçekte "güvenilir ve uyumlu" bir statüye yükseltecektir.

Dijital Egemenlik ve Proaktif Yönetişim

Dijital egemenlik, dijital ekosistemin içerisinde yer alarak; bu ekosistemi şekillendiren standartların oluşturulmasına destek vererek güçlendirilebilir. Bu kapsamda geliştirilecek bir yönetim modeli, şeffaflık, hesap verebilirlik ve paydaş katılımı temeline dayanmalıdır.

Dijital egemenlik teknolojik ekosistemi, şeffaf, hesap verebilir ve uluslararası teknik normlarla uyumlu bir yönetim modelinin kurulması ile mümkündür. Bu model, Türkiye'nin dijital ekosistemini küresel dijital ölçekte değer bulan ve güvenilir bir teknoloji üssü olma hedeflerini destekleyecektir.

BÖLÜM 4: DİJİTAL PLATFORM EKONOMİSİNDE REKLAM, GELİR, P2B VE ŞEFFAFLIK

Bölümün Amacı: Dijital platform ekonomisinde reklam, gelir modelleri ve P2B (Platformdan İşletmeye) ilişkilerindeki yapısal çıkar çatışmalarını dengelemek; platformların hem kural koyucu "hakem" hem de satıcı "oyuncu" olmasından kaynaklanan haksız rekabeti önleyerek inovasyonun adil, şeffaf ve insan odaklı bir zeminde gelişmesini sağlamaktır.

İçerik ve Kapsam:

- Dijital reklamcılık değer zincirinin (DSP, SSP, Ad Exchange, Veri Aracıları) ve bu alandaki algoritmik şeffaflık gereksiniminin analizi
- E-ticaret platformlarının "hibrit modeli" ile kendi ürünlerini kayırmasının (self-preferencing) engellenmesine ilişkin regülasyonlar (DMA/P2B)
- Kullanıcı özerkliğini zedeleyen manipülatif tasarım kalıplarının (Dark Patterns) ve dinamik fiyatlandırma risklerinin bulunması ve önlenmesi
- Yerel satıcıların (KOBİ'ler) platformlara olan ekonomik bağımlılığı, veri asimetrisi ve kilitlenme (lock-in) etkisine karşı veri taşınabilirliği çözümleri
- Hedefli reklamcılıkta (targeted advertising) profil çıkarma sınırları ve çocukların manipülasyonuna karşı davranışsal reklam yasakları

Temel Kavramlar:

- Hakem ve Oyuncu Çatışması (Dual Role Paradox)
- Kendine Öncelik Verme (Self-Preferencing)
- Karanlık Tasarımlar (Dark Patterns)
- Kilitlenme Etkisi (Lock-in Effect)
- Dikkat Ekonomisi (Attention Economy)
- Algoritmik Gizli Anlaşma (Collusion)

Dijital platform ekonomisi, yalnızca bir teknoloji katmanı olarak değil; algoritmik sistemlerin, veri temelli gelir modellerinin ve kullanıcı davranışlarının birlikte şekillendirdiği bir pazar yapısı olarak ele alınmalıdır. Bu yapı, kendi içinde işleyen ve farklı aktörlerin etkileşimiyle oluşan sistemik bir pazar yeri niteliği taşımaktadır. Bu bölümde ele alınan dinamikler, dijital reklamcılıktan e-ticaret pazaryerlerine uzanan ekosistemde, ekonomik verimlilik ile kullanıcı hakları arasında kurulan hassas dengeyi anlamaya odaklanmaktadır.

Bu bölümün temel yaklaşımı, dijital platformlarda şeffaflığın bir maliyet unsuru olarak değil, uzun vadede güven oluşturma ve pazarın sürdürülebilirliğini sağlamanın önemli bir bileşeni olarak görülmesi gerektiğidir. Bu çerçevede düzenleyici müdahalenin amacı, inovasyonu sınırlamak değil; daha adil, daha şeffaf ve insanı merkeze alan bir ortam içinde gelişmesini desteklemektir.

4.1. Dijital Platform Ekonomisi: Stratejik Mimari ve Gelir Modelleri

Dijital platform ekonomisi, arama motorları, sosyal ağlar ve e-ticaret yapılarının algoritmik sistemler üzerinden şekillendirdiği karmaşık bir ekosistemdir. Bu sistemde reklam, yalnızca bir pazarlama aracı değil; aynı zamanda veri toplama, kullanıcı deneyimi ve ticari erişimi belirleyen temel gelir mekanizmasıdır. Bu yönüyle mevcut yapı, kullanıcı şeffaflığı, pazar yoğunlaşması ve KOBİ'lerin dijital pazara erişimi gibi alanlarda bazı yapısal riskler de barındırmaktadır.

Reklam altyapısının veri temelli ve algoritmik doğası, kullanıcı şeffaflığı, rekabet dengesi, KOBİ'lerin pazara erişimi, tüketici manipülasyonu riski ve pazar yoğunlaşması gibi başlıklarda doğrudan etkiler üretmektedir. Bu alanlara Avrupa Birliği düzenleyici çerçevesi; şeffaflık (DSA)¹²⁷, rekabet (DMA)¹²⁸ ve veri koruma (GDPR)¹²⁹ eksenlerinde, birbirini tamamlayan bir yaklaşımla müdahale etmektedir.

Bu yapı, doğrusal bir iletimden ziyade, **DSP (Talep Tarafı), SSP (Arz Tarafı), Ad Exchange (Reklam Borsası)** ve veri aracıları arasındaki milisaniyelik etkileşimlerle işleyen döngüsel bir mekanizma üzerinden ilerlemektedir. Bu mekanizma temel olarak üç aşamada ele alınabilir:

Veri ve Profileme: Kullanıcı davranışlarına ait sinyaller, veri aracıları ve birinci taraf çerezler üzerinden toplanmakta; bu veriler anlamlandırılarak segmentlere ayrılmakta ve hedefleme için anonim profillere dönüştürülmektedir.

¹²⁷ DSA (Digital Services Act), <https://eur-lex.europa.eu/eli/reg/2022/2065/oj>

¹²⁸ DMA (Digital Markets Act), <https://eur-lex.europa.eu/eli/reg/2022/1925/oj>

¹²⁹ GDPR (General Data Protection Regulation), <https://eur-lex.europa.eu/eli/reg/2016/679/oj>

Algoritmik Optimizasyon (RTB Süreci): Reklamverenin talebini yöneten DSP ile yayıncının envanterini sunan SSP, Ad Exchange üzerinde Gerçek Zamanlı Açık Artırma (RTB) modeliyle eşleşmektedir. Bu süreç, çok kısa süreler içinde gerçekleşerek reklamın hangi kullanıcıya gösterileceğini belirler.

Performans Ölçümü ve Geri Besleme: Reklam gösterimi sonrasında elde edilen veriler işlenmekte, reklamın başarısı ölçülmekte ve bu çıktılar doğrultusunda optimizasyon modelleri sürekli güncellenmektedir.

Bütüncül Düzenleyici Yaklaşım: DSA, DMA ve GDPR Eksenli

Avrupa Birliği düzenleyici çerçevesi, bu döngüsel yapının ortaya çıkardığı riskleri üç ana başlık altında ve birbirini tamamlayan bir yaklaşımla ele almaktadır:

- 1. Sistemik Risk Yönetimi ve Şeffaflık (DSA):** Dijital Hizmetler Yasası (DSA), reklam alanını yalnızca bir şeffaflık yükümlülüğü olarak ele almaz. Özellikle çok büyük çevrim içi platformlar (VLOPs) için bu alan; dezenformasyonun yayılması, temel hakların korunması ve kamu sağlığı gibi konularda aktif bir risk yönetimi sorumluluğu da içerir. Bunun yanında platformların sunduğu reklam kütüphaneleri (ad repositories), hangi reklamın kim tarafından finanse edildiğini ve hangi hedefleme kriterleriyle gösterildiğini görünür hale getirir. Bu sayede algoritmik manipülasyon riskine karşı daha denetlenebilir bir yapı oluşur.
- 2. Dijital Pazarlar Yasası (DMA):** Dijital Pazarlar Yasası (DMA), platformların aynı anda hem alıcı tarafı (DSP), hem satıcı tarafı (SSP) hem de pazar yeri (Exchange) rolünü üstlenmesinden kaynaklanan çıkar çatışmalarına odaklanır. Özellikle “geçit bekçisi” (gatekeeper) konumundaki oyuncuların kendi hizmetlerini öne çıkarmasını (self-preferencing) sınırlar. Ayrıca reklam teknolojisi maliyetlerinin (“ad tech tax”) daha şeffaf hale getirilmesini zorunlu kılarak, KOBİ’lerin pazara erişimini korumayı hedefler.
- 3. Veri Koruması ve Onay Yönetimi (GDPR):** Reklam ekosisteminin temel girdisi olan kişisel verilerin işlenmesi, GDPR ile kullanıcının açık rızasına ve veri minimizasyonu ilkesine bağlanır. Bu yaklaşım, özellikle profil oluşturma ve hedefleme süreçlerini daha kontrollü hale getirmeyi amaçlar.

Bu üçlü yapı birlikte değerlendirildiğinde, platformların aynı anda pazar yeri operatörü, açık artırma yöneticisi ve ölçüm sağlayıcısı olarak hareket etmesinden kaynaklanan şeffaflık sorunlarını ve rekabet dengesizliklerini sınırlamaya yönelik bir çerçeve ortaya çıkmaktadır.

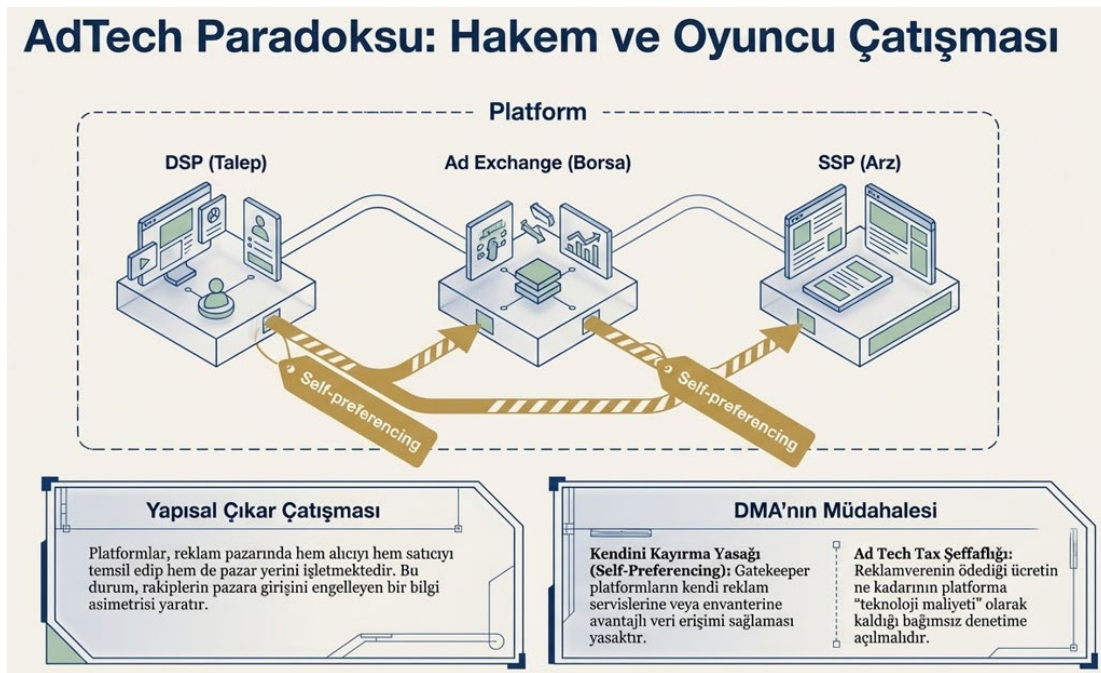
4.1.1. Ekosistemin Yapısı ve Değer Zinciri

Dijital reklam pazarları, platformların kullanıcı dikkatini ve reklamveren talebini bir araya getirdiği çok taraflı (multi-sided) bir yapı üzerine kuruludur. Bu süreç, klasik anlamda doğrusal bir reklam iletiminden ziyade, sürekli tekrar eden bir döngü şeklinde işlemektedir:

1. **Veri ve Profileme:** Kullanıcı davranışlarına ilişkin sinyallerin toplanması ve anlamlı segmentlere ayrılması.
2. **Algoritmik Optimizasyon:** Bu veriler üzerinden gerçek zamanlı açık artırma (RTB) süreçlerinin çalıştırılması ve reklam görünürlüğünün yönetilmesi.
3. **Performans Ölçümü:** Reklam gösterimi sonrasında elde edilen verilerin analiz edilmesi ve bu verilerle modelin sürekli güncellenmesi.

Bu döngü içinde platformların; pazar yeri operatörü, açık artırma yöneticisi ve ölçüm sağlayıcısı rollerini aynı anda üstlenmesi, beraberinde çıkar çatışması ve şeffaflık sorunlarını da getirmektedir.

Reklam Teknolojisi (AdTech) Değer Zinciri ve Yapısal Çıkar Çatışmaları



ŞEKİL 4-1: Hakem-Oyuncu Paradoksu (YZ ile hazırlanmıştır)

Rekabet Hukuku Analizi: "Hakem-Oyuncu" Sorunsalı

Bu döngü içinde platformların; pazar yeri operatörü (Ad Exchange), açık artırma yöneticisi (SSP/DSP) ve ölçüm sağlayıcısı rollerini aynı anda üstlenmesi, rekabet hukuku açısından ciddi bir **çıkar çatışması** yaratmaktadır. Bir platformun hem alıcıyı hem satıcıyı temsil etmesi ve aynı zamanda pazar yerini işletmesi, aşağıdaki riskleri beraberinde getirir:

1. **Kendine Öncelik Tanıma (Self-Preferencing):** Platformun kendi reklam servislerine veya envanterine daha avantajlı veri erişimi sağlaması.

2. **Operasyonel Şeffaflık Eksikliği:** Reklamverenin ödediği ücretin ne kadarının “teknoloji maliyeti” (ad tech tax) olarak aracıya gittiğinin net şekilde görülememesi.
3. **Bilgi Asimetrisi:** Rakiplerin açık artırma dinamiklerine erişememesi nedeniyle pazara girişin zorlaşması ve rekabetin sınırlanması.

Dijital reklam pazarları, iki taraflı (two-sided) ya da çok taraflı platform ekonomileri içinde konumlanmaktadır. Platformlar bir tarafta kullanıcı dikkatini, diğer tarafta reklamveren talebini bir araya getirerek değer üretir. OECD de bu yapıyı; veri temelli açık artırma sistemleri ve algoritmik optimizasyon süreçleriyle çalışan karmaşık bir ekosistem olarak tanımlamaktadır.¹³⁰

Bu ekosistemin temel bileşenleri; reklam verenler (advertiser), platformlar (arama, sosyal medya, e-ticaret), açık artırma ve hedefleme sistemleri, ölçümleme ve performans analitiği ile kullanıcı veri işleme altyapılarıdır.

Sonuç olarak bu yapı, görünürlüğü kontrol eden taraf ile gelir üreten tarafın aynı aktörde birleşmesine yol açmaktadır. Bu durum da rekabet hukuku, tüketici koruma ve veri koruma açısından daha dikkatli ve dengeli bir düzenleme ihtiyacını beraberinde getirmektedir.

Vaka Analizi: Rekabet Kurumu’nun Google Kararları (Caselaw)¹³¹

Teorik olarak tartışılan bu “Hakem-Oyuncu” sorunsalı, Türk Rekabet Hukuku uygulamasında da somut karşılık bulmuştur. Özellikle Google’ın reklam teknolojileri zincirindeki hâkim durumunu kötüye kullandığına yönelik kararlar, bu alanda önemli bir dönüm noktası olarak değerlendirilmektedir:

- **Genel Arama Hizmetleri ve Reklamcılık:** Rekabet Kurumu, Google’ın arama sonuçları sayfasında kendi yerel arama ve konaklama fiyatı karşılaştırma hizmetlerini rakiplerine kıyasla daha avantajlı konumda sunmasını (self-preferencing) hukuka aykırı bulmuştur.
- **AdTech Soruşturmaları:** Google’ın reklam teknolojisi tedarik zincirindeki (Ad Stack) dikey bütünleşmiş yapısı; reklamveren ve yayıncı arasındaki veri akışını kontrol etmesi ve bu yolla rakiplerini dışlaması gerekçesiyle incelemeye alınmış, çeşitli idari para cezaları ve yükümlülöklere konu olmuştur.

Not: Rekabet Kurumu’nun güncel kararları (örn. 21-19/227-94 sayılı karar), dijital platformların yalnızca pazar gücünü değil, bu gücü yan pazarlara nasıl taşıdığını (leveraging) da yakından izlediğini ve bu alanda daha sıkı bir denetim yaklaşımı benimsediğini göstermektedir.¹³²

¹³⁰ OECD (2021), “Competition in Digital Advertising Markets”, *OECD Roundtables on Competition Policy Papers*, No. 259, OECD Publishing, Paris, <https://doi.org/10.1787/f2209674-en>.

¹³¹ **Rekabet Kurumu (2024).** <https://www.rekabet.gov.tr/tr/Guncel/google-reklamcilik-ve-pazarlama-ltd-sti--5c808b3e47b9ef1193d90050568585c9>

¹³² **Rekabet Kurumu’nun Google ile ilgili kararları.** https://www.google.com/url?q=https://www.rekabet.gov.tr/tr/Kararlar?page%3D1%26sayfaAdi%3DGoogle&sa=D&source=docs&ust=1773259931301155&usg=AOvVaw35L0shw1f7mjE8OrjNHM_J

Dijital "Geçit Bekçiliği" (Gatekeeping) ve P2B İlişkisi

Geleneksel ticaretten farklı olarak, dijital pazarlarda platformlar artık sadece bir aracı değil, doğrudan “pazarın kendisi” haline gelmiştir. Bu durum, **Platformdan İşletmeye (P2B)** ilişkisini klasik bir tedarik zinciri ilişkisinin ötesine taşıyarak, daha yapısal bir bağımlılık ilişkisine dönüştürmektedir.

- **Ekonomik Bağımlılık ve Şebeke Etkisi (Network Effects):** Bir platformun kullanıcı sayısı arttıkça, satıcılar için o platformda yer almamanın maliyeti de hızla artar. Bu nedenle satıcılar, görünür kalabilmek için çoğu zaman platformun belirlediği kuralları ve komisyon yapısını kabul etmek durumunda kalır.
- **Altyapısal Güç:** Platformlar; ödeme sistemleri, lojistik ağlar ve müşteri verileri üzerinde ciddi bir kontrol sahibidir. Bu kontrol, platformlara pazardaki diğer oyuncular üzerinde yönlendirici bir etki kurma, hatta bazı durumlarda rakipleri dışlama imkânı sağlar.
- **Referans:** [AB 2019/1150 P2B Regülasyonu - Resmî Gerekçe Metni](#) - *Bu tüzük, platformların orantısız gücüne karşı ticari kullanıcıları korumayı amaçlayan ilk küresel hukuk normudur.*

Hibrit Model ve Çift Rol (Dual Role) Paradoksu

E-ticaretin gelişimiyle birlikte platformlar, yalnızca bir “aracı” (intermediary) olmaktan çıkıp doğrudan bir “oyuncu” (competitor) haline gelmiştir. Bu durum, rekabet hukukunda “**hibrit iş modeli**” olarak tanımlanmaktadır.

- **Hakem ve Oyuncu Çatışması:** Platform bir yandan pazarın kurallarını belirleyen (algoritma, sıralama kriterleri, katılım şartları) bir “hakem” rolündeyken, diğer yandan bu kurallar içinde rekabet eden bir “oyuncu” olarak yer alır. Bu ikili yapı, kaçınılmaz olarak yapısal bir çıkar çatışması doğurur.
- **Dikey Bütünleşmenin Riskleri:** Platformun kendi perakende faaliyetleri ile üçüncü taraf satıcılar arasındaki rekabet, pratikte eşit koşullarda gerçekleşmez. Platform, altyapı maliyetlerini diğer satıcılara yansıtırken, kendi ürünlerini daha düşük maliyet avantajıyla sunabilmektedir.
- **Referans:** [OECD - Competition in Digital Advertising and Online Intermediaries \(2020\)](#) - *Bu çalışma, hibrit modellerin pazar üzerindeki bozucu etkilerini teorik çerçeveye oturtur.*

4.1.2. Gelir Modelleri, Yapısal Riskler ve Politika Tasarımı

Platform ekonomisinde sürdürülebilirlik, büyük ölçüde tercih edilen gelir modeline bağlı olarak şekillenir. Her model, beraberinde farklı yapısal riskler de getirir. Bu nedenle geliştirilen politika tasarım ilkeleri, bir yandan platformların pazar gücünü dengelemeyi, diğer yandan kullanıcı haklarını korumayı amaçlar.

Aşağıdaki tablo, platformların temel gelir modellerini, bu modellerin ortaya çıkardığı riskleri ve bu risklere karşı önerilen düzenleme yaklaşımlarını karşılaştırmalı olarak özetlemektedir:

TABLO 4-1: Gelir Modelleri, Yapısal Riskler ve Politika Tasarımı Tablosu

Gelir Modeli	İşleyiş ve Odak Noktası	Yapısal Risk Alanları	Politika Tasarım İlkesi
Reklam Temelli	Kullanıcı erişimi ücretsizdir; gelir reklam verenden sağlanır.	Gelir-Veri Yoğunlaşması: "Dikkat ekonomisi" manipülasyonu ve aşırı veri toplama baskısı.	Veri Ayırıştırma: Çapraz veri kullanımının sınırlandırılması ve veri mahremiyeti.
Abonelik	Kullanıcı hizmet için doğrudan ve düzenli ödeme yapar.	Abonelik Tutsaklığı: Otomatik yenileme ve kasıtlı olarak zorlaştırılan iptal süreçleri.	Rekabet-Tüketici Dengesi: Şeffaf fiyatlandırma, kolay çıkış ve "iptal hakkı" güvencesi.
Komisyon Bazlı	E-ticaret platformlarında satış başına alınan paydır.	Kendini Önceliklendirme (Self-Preferencing): Platformun kendi ürünlerini algoritmalarda avantajlı konumlandırması.	Orantılı Yükümlülük: Sistemik (gatekeeper) platformlara ek şeffaflık ve denetim sorumluluğu.
Hibrit Modeller	Yukarıdaki modellerin veri analitiği ile birleşimidir.	Çapraz Sübvansiyon: Bir pazardaki gelirin diğer pazardaki rekabeti bozmak için kullanılması.	Gelir Modeli Nötrlüğü: Modelin kendisini değil, yarattığı somut rekabet riskini düzenleme.

Rol Birleşimi ve Çıkar Çatışması

Platformlar günümüzde tek bir işlevin ötesine geçerek; aynı anda pazar yeri operatörü, açık artırma yöneticisi, ölçüm sağlayıcısı ve görünürlük belirleyicisi gibi birden fazla rolü üstlenebilmektedir.

Bu durum beraberinde bazı temel sorunları da getirir:

- **Çıkar Çatışması:** Platformun hem hakem hem de oyuncu olması, tarafsızlık ilkesini zayıflatır.
- **Şeffaflık Eksikliği:** Algoritmik kararların ve sıralama kriterlerinin yeterince görünür olmaması, piyasada dengesizliklere yol açabilir.

- **Ekonomik Güç Yoğunlaşması:** Veri avantajı ile gelir gücünün birleşmesi, yeni oyuncuların pazara girişini zorlaştırabilir ve zamanla inovasyonu baskılayabilir.

Bu nedenle politika tasarımı yapılırken, platformun yalnızca teknolojik altyapısına değil, bu çoklu rol yapısının yarattığı daha geniş etkilerin de dikkate alınması gerekir.

4.1.3. Türkiye’de Yapısal Görünüm ve Risk Analizi

Türkiye’de dijital reklam yatırımları büyük ölçüde küresel arama motorları ve sosyal medya platformlarında yoğunlaşmaktadır. TBD perspektifinden bakıldığında öne çıkan temel risk alanları şu şekilde özetlenebilir:

- **Pazar Yoğunlaşması:** Gelirlerin sınırlı sayıda platformda toplanması, ekonomik güç dengesizliğine yol açmaktadır.
- **Ölçümleme Bağımlılığı:** Performans verilerinin büyük ölçüde platform içi metriklere dayanması, bağımsız denetimi zorlaştırmaktadır.
- **KOBİ Bağımlılığı:** Yerel işletmelerin dijital görünürlük için platform politikalarına olan bağımlılığı giderek artmaktadır.
- **Veri Avantajı:** Platformlarda biriken veri, yeni oyuncular için pazara girişte önemli bir engel oluşturabilmektedir.

Sektörün büyüklüğü ve kanal dağılımı açısından en önemli referans kaynaklardan biri IAB Türkiye Medya ve Reklam Yatırımları Raporlarıdır.¹³³

4.1.4. Stratejik Politika Önerileri ve KPI Mekanizması

AB'nin **DSA**, **DMA** ve **P2B**¹³⁴ düzenleme mimarisiyle uyumlu, Türkiye’ye özgü bir yol haritası önerilmektedir. Bu kapsamda öne çıkan başlıklar şu şekilde özetlenebilir:

- **Sistemik Platform Tanımı:** Geçit Bekçisi “Gatekeeper” niteliğindeki platformlara yönelik önleyici (ex-ante) yükümlülükler geliştirilmelidir.
- **Bağımsız Ölçüm Erişimi:** Reklam performans verilerine bağımsız üçüncü tarafların erişimi sağlanmalı ve bu verilerin doğrulanabilir olması güvence altına alınmalıdır.
- **Şeffaflık Raporlaması:** Platformların; reklam payı, komisyon oranları ve sıralama kriterlerini içeren KPI bazlı raporları yıllık olarak yayımlaması beklenmelidir.

¹³³ IAB Türkiye Medya ve Reklam Yatırımları Raporları. <https://iabtr.org/turkiye-tahmini-medya-ve-reklam-yatirimlari/>

¹³⁴ P2B Regulation, European Union (2019). <https://eur-lex.europa.eu/eli/reg/2019/1150/oj>

- **Abonelik ve İptal Standartları:** “Kolay çıkış” ilkesi doğrultusunda, iptal süreçleri üyelik süreçleri kadar basit ve erişilebilir olmalıdır.
- **Yetkili Denetim ve Ölçüm Yapısı:** Reklam performans verilerine ve algoritmik parametrelere erişim; Rekabet Kurumu koordinasyonunda, BTK’nın teknik desteği ve akredite bağımsız denetçiler aracılığıyla sağlanmalıdır. Bu yaklaşım, platformların kendi performansını tek taraflı ölçtüğü mevcut yapının daha dengeli hale gelmesine katkı sağlayacaktır.
- **Raporlama ve Yayın Sıklığı:** Geçit bekçisi konumundaki platformlar, reklam kütüphanelerini ve performans verilerini mümkün olduğunca güncel tutmalı; ideal olarak gerçek zamanlı, en geç 24 saat gecikmeyle erişilebilir kılmalıdır.
- **Sistemik Denetim:** Bağımsız denetim raporları altı aylık periyotlarla ilgili kurumlara sunulmalı, temel bulgular ise kamuoyuyla paylaşılmalıdır.

Uyumsuzluk Halinde Yaptırım Rejimi:

- **Veri Paylaşım İhlali:** Bağımsız ölçüm araçlarının engellenmesi veya eksik veri sunulması durumunda, platformun ilgili mali yıldaki küresel cirosu üzerinden %1 ile %10 arasında kademeli idari para cezaları uygulanabilir.
- **Sürekli Durdurma:** İhlalin devam etmesi halinde, belirli reklam hedefleme yeteneklerinin veya veri işleme süreçlerinin, uyum sağlanana kadar geçici olarak askıya alınması değerlendirilebilir.

4.2. Hedefli Reklamcılık ve Profilleme: Veri Yönetişimi ve Koruma

Hedefli reklamcılık (targeted advertising), platform ekonomisinin gelir merkezinde yer almasına rağmen; kullanıcı özerkliği, ayrımcılık ve veri mahremiyeti açısından önemli riskler barındırmaktadır. Avrupa Birliği (AB), bu alanı tamamen yasaklamak yerine DSA, GDPR ve AI Act çerçevesinde risk temelli bir denetim yaklaşımı benimsemiştir. Türkiye’de ise KVKK kapsamında temel bir çerçeve bulunmakla birlikte, dijital reklamcılığa özel uygulama rehberliği ve yaptırım kapasitesinin geliştirilmesi gerektiği görülmektedir.

Avrupa Birliği tarafında çocuklara yönelik hedefli reklamlar ve hassas veri temelli profil oluşturma (DSA kapsamında) sınırlandırılmakta; GDPR ile otomatik karar verme ve profil çıkarma süreçlerinde kullanıcıya bilgilendirme ve itiraz hakkı tanınmaktadır. Ayrıca Yapay Zekâ Yasası (AI Act), yüksek riskli sistemlerde veri yönetişimi ve ayrımcılığın azaltılmasına yönelik ek yükümlülükler öngörmektedir.¹³⁵

Veri Sahipliği ve Veri Erişimi

¹³⁵ AI Act, European Union (2024). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689>

Pazaryeri modelinde veri, platform ile satıcının ortak faaliyetinden doğar; ancak bu verinin teknik kontrolü büyük ölçüde platformun elindedir.

- **Sorun Alanı:** Satıcılar, platform üzerinden gerçekleşen satışlardan doğan müşteri davranış verilerine (örneğin hangi ürünlerin incelendiği veya talebin hangi bölgelerden geldiği) çoğu zaman sınırlı ölçüde erişebilir. Platformların bu veriyi “ticari sır” ya da veri koruma düzenlemeleri kapsamında değerlendirmesi, satıcıların kendi işlerini geliştirmesini zorlaştırabilmektedir.
- **Veri Asimetrisi:** Platformun aynı veriyi kendi ürünlerini (private label) geliştirmek için kullanması, özellikle dikey bütünleşik yapılarda rekabet açısından avantaj yaratmaktadır.
- **Referans:** OECD - Data Governance and Competition (2022) - *Veriye erişimin dijital pazarlarda nasıl bir giriş engeli (barrier to entry) oluşturduğunu inceleyen temel dokümandır.*

Kilitleme Etkisi (Lock-in Effect)

Bir satıcı, yıllar içinde oluşturduğu müşteri yorumlarını ve “başarılı satıcı” gibi itibar göstergelerini başka bir platforma taşıyamadığı sürece, mevcut platformun koşullarına bağlı kalmak zorunda kalabilir. Bu durum, platform değiştirme maliyetini artırarak bağımlılığı güçlendirir.

- **Çözüm Yaklaşımı:** Veri taşınabilirliği, satıcının kendi itibar verilerini makine tarafından okunabilir bir formatta alıp başka platformlara aktarabilmesini mümkün kılar. Bu yaklaşım, satıcıların aynı anda birden fazla platformda var olabilmelerini (multi-homing) kolaylaştırarak rekabeti destekler.
- **Referans:** AB Dijital Pazarlar Yasası (DMA)- Madde 6(9) - *Geçit bekçisi platformların, hem kullanıcılara hem de ticari kullanıcılara verilerini gerçek zamanlı ve sürekli olarak taşıma imkânı sunmasını emreden maddedir.*



ŞEKİL 4-2: E-Ticarette Adil Rekabet (YZ ile hazırlanmıştır)**4.2.1. Kavramsal ve Teknik Altyapı**

Profil çıkarma, kişisel verilerin otomatik olarak işlenmesi yoluyla bireylerin ekonomik durumu, davranış eğilimleri ve risk skorları gibi özelliklerinin değerlendirilmesi sürecidir. GDPR, profil çıkarmayı “kişisel verilerin belirli kişisel yönleri değerlendirmek amacıyla otomatik işlenmesi” olarak tanımlar. Ancak her profillemeye faaliyetinin doğrudan hukuki sonuç doğuran bir “otomatik karar alma” anlamına gelmediği de özellikle belirtilmektedir. Bu ayrım, şeffaflık yükümlülüklerini ortadan kaldırmaz.

Bu kapsamda yapılan değerlendirmeler genellikle şu alanları içerir:

- Ekonomik durum
- İlgili alanları
- Davranış eğilimleri
- Konum bilgisi
- Güvenilirlik veya risk skoru

Hedefli reklamcılıkta profil çıkarma süreci çoğunlukla şu adımlar üzerinden ilerler:

- Davranışsal veri toplama (clickstream, arama geçmişi, etkileşim süresi)
- Segment oluşturma (örneğin “yüksek satın alma eğilimli kullanıcı”)
- Açık artırma bazlı hedefleme
- Performans optimizasyonu

Bu yapı, veri temelli tahmin modelleri ile ekonomik kararlar arasında doğrudan bir ilişki kurmaktadır.

4.2.2. AB Karşılaştırmalı Düzenleme Tablosu

AB mevzuatı ile Türkiye'deki mevcut durumun hedefli reklamcılık özelindeki karşılaştırması aşağıdadır:

TABLO 4-2: Reklamcılık Konusunda AB Mevzuatı ve Türkiye'deki Durum Karşılaştırması

Düzenleme	Kapsam ve Temel Yükümlülükler	Türkiye Karşılığı / Durum
DSA (Art. 26-28)	Reklam veren kimliğinin ve hedefleme parametrelerinin (Neden bu reklam?) açıklanması zorunluluğu. Çocuklara yönelik hedefli reklam yasağı.	KVKK'de benzer bir doğrudan yasak bulunmamaktadır; uygulama rehberliği sınırlıdır.

Düzenleme	Kapsam ve Temel Yükümlülükler	Türkiye Karşılığı / Durum
GDPR (Art. 9 & 22)	Hassas veri ile profil yasağı. Otomatik kararlara karşı itiraz ve insan müdahalesi talep hakkı.	KVKK, GDPR ile benzer bir yapı sunsa da algoritmik şeffaflık pratikleri henüz yerleşmemiştir.
AI Act	Yüksek riskli sistemlerde veri yönetimi, önyargı azaltımı ve teknik dokümantasyon zorunluluğu.	Türkiye'de yapay zekâ sistemlerine özgü bir denetim mekanizması henüz yasalaşmamıştır.

Özetle, Avrupa Birliği, hedefli reklamcılığı spesifik düzenlemelerle (DSA, AI Act) sıkı bir denetim altına alırken, Türkiye'deki uygulama henüz genel veri koruma prensipleri çerçevesinde kalmakta ve dijital ekosistemin ihtiyaç duyduğu sektörel derinlikten yoksun görünmektedir.

4.2.3. Risk Odaklı Politika Tasarımı

Hedefli reklamcılığın yarattığı riskler, doğrudan çözüm odaklı politika ilkeleriyle ele alınmalıdır. Bu kapsamda öne çıkan başlıklar şunlardır:

- **Algoritmik Ayrımcılık:** Segmentasyon süreçlerinin tarihsel önyargıları yeniden üretme riskine karşı, “bağımsız ayrımcılık testi” gibi denetim mekanizmalarının devreye alınması gerekmektedir.
- **Kırılgan Gruplar:** Çocuklar ve düşük gelirli bireyler gibi grupların manipülasyona açık olması nedeniyle, bu gruplara yönelik davranışsal reklamcılığın sınırlandırılması ya da belirli durumlarda yasaklanması değerlendirilebilir.
- **Opaklık ve Kontrol Eksikliği:** Kullanıcıların neden hedeflendiğini anlamakta zorlanması önemli bir sorundur. Bu nedenle asgari şeffaflık standartlarının oluşturulması ve kullanıcıya gerçek bir “profillemeye dışı seçenek” sunulması gerekmektedir. Bu yaklaşım, yalnızca klasik “opt-out” mekanizmalarının ötesine geçmeyi hedefler.
- **Profillemeye Dışı Eşdeğer Seçenek:** Kullanıcılara, kişisel verilerine dayalı profillemeye yapılmadan da benzer hizmet kalitesine erişebilecekleri alternatifler sunulmalıdır. Bu, rızanın gerçekten özgür iradeyle verilmesini destekleyen önemli bir kullanıcı özerkliği unsurudur.
- **Veri Sınırları:** Sağlık bilgileri, siyasi görüşler ve etnik köken gibi hassas verilerin profil oluşturma süreçlerinde kullanılmasının açık ve net şekilde sınırlandırılması gerekmektedir.

4.2.4. İzleme ve KPI Mekanizması

Politikaların etkinliği, aşağıdaki göstergeler üzerinden düzenli olarak takip edilmelidir:

- **Erişim Oranı:** “Neden bu reklam?” açıklama butonunun kullanıcılar tarafından ne ölçüde kullanıldığı ve anlaşıldığı.
- **İhlal Sayısı:** Çocuklara yönelik hedefli reklam yasağına aykırı kampanya sayısı.
- **Kontrol Verimliliği:** Kullanıcıların profillemeye dışı kullanım seçeneğini (opt-out) tercih etme oranı.
- **Denetim Kapasitesi:** Yıllık olarak yayımlanan algoritmik ayrımcılık test raporu sayısı.

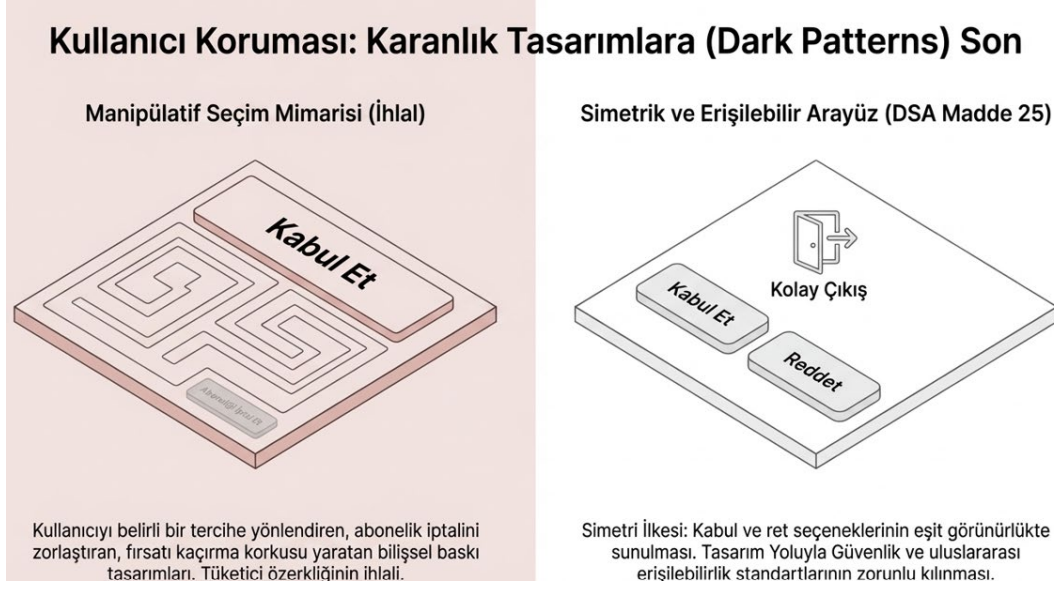
Bu göstergelerin düzenli ve sistematik şekilde izlenmesi, düzenlemelerin yalnızca şekli bir uyumla sınırlı kalmamasını sağlar. Aynı zamanda dijital pazarda hesap verebilirliğin güçlenmesine, kullanıcı güveninin artmasına ve algoritmik şeffaflığın daha ölçülebilir hale gelmesine katkı sunar.

4.3. Manipülatif Tasarım Kalıpları (Dark Patterns) ve Dijital Adalet

(Davranışsal Yönlendirme, Tüketici Özerkliği ve Dijital Adalet Perspektifi)

Karanlık tasarım kalıpları (dark patterns), kullanıcıların bilinçli ve özgür iradeye dayalı karar verme süreçlerini, arayüz tasarımı üzerinden yönlendiren uygulamaları ifade eder. Dijital platformlarda veri toplama, aboneliklerin devamlılığını sağlama ve gelir artırma amacıyla kullanılan bu yöntemler; tüketici özerkliği ve bilgilendirilmiş onay ilkeleri açısından önemli riskler barındırır. Bu bölümde, söz konusu uygulamaların teknik yapısı ele alınmakta ve Türkiye’nin dijital denetim kapasitesini güçlendirmeye yönelik bir politika çerçevesi önerilmektedir.

Avrupa Birliği düzenlemeleri, dark pattern uygulamalarına karşı daha net bir yaklaşım benimsemiştir. Digital Services Act (DSA), kullanıcıları yanıltan veya manipüle eden arayüz tasarımlarını açık şekilde sınırlandırmaktadır. Buna ek olarak UCPD (Haksız Ticari Uygulamalar Direktifi), tüketiciyi yanıltan ticari uygulamaları yasaklamaktadır. GDPR ise rıza mekanizmalarında özgür, açık ve bilgilendirilmiş onay ilkesini zorunlu hale getirmektedir.



ŞEKİL 4-3: Karanlık Tasarımlar (YZ ile hazırlanmıştır)

4.3.1. Kavramsal Tanımlama ve Uygulama Biçimleri

“Dark patterns” (manipülatif tasarım), kullanıcıyı belirli bir tercihe yönlendirmek amacıyla tasarlanan arayüz stratejileridir. OECD bu uygulamaları, “kullanıcının bilişsel önyargılarından yararlanarak ekonomik kararlarını etkileyen dijital mimari uygulamalar” olarak tanımlamaktadır. Bu tür tasarımlar, özellikle reklam ve abonelik temelli iş modelleriyle doğrudan ilişkilidir.

Sektörde Sıkça Gözlemlenen Uygulamalar:

- **Onay Dayatması:** Önceden işaretlenmiş onay kutuları aracılığıyla, kullanıcı iradesinin varsayılan seçeneklerle yönlendirilmesi.
- **Asimetrik Tasarım:** Abonelikten çıkış veya çerez reddetme seçeneklerinin görsel olarak geri planda bırakılması ya da karmaşık süreçlere bağlanması.
- **Bilişsel Baskı:** “Fırsatı kaçırma” gibi aciliyet hissi yaratan mesajlarla, kullanıcının daha hızlı ve yeterince düşünmeden karar vermeye yönlendirilmesi.

Bu tür uygulamalar, özellikle reklam, veri işleme ve abonelik bazlı gelir modelleriyle doğrudan bağlantılıdır.

Dikkat Ekonomisinin Psikolojik Varlığı:

OECD karanlık tasarımları, kullanıcının ekonomik kararlarını etkileyen dijital mimari tasarım uygulamaları olarak tanımlamaktadır. Bu tasarım mimarisi gerek ticari onay süreçlerinde ve gerekse sosyal medya platformlarında kullanıcıları maksimum sürede ekranda tutmak amacına dayanan tasarım teknikleridir.

- **İçerik Döngüleri:** İçerik belirsizliğiyle merak etme ve ilgiyi canlı tutar.
- **Sonsuz Kaydırma:** Cazip gelecek içeriklerle durma isteğini sönümler ve ekranda kalma süresi uzatılır.
- **Bildirimler:** Merak uyandıran içerikler ve yöntemlerle platforma girişi özendirir.
- **Sosyal Onay ve Görünürlük:** Beğeni ve yorum almak ya da yazmak, önemli kişi hissiyatı oluşturmak platformların etkili güçlerindendir ve kullanıcıların platforma bağımlılığını tetikleyen bir unsurdur.
- **Sonsuz İçerik Gösterimi:** İçerikleri ardısıra sunarak kullanıcının dikkatini çekme ve platformda uzunca sürelerde tutabilme etkisi vardır.
- **Kaçırma Korkusu (FOMO-Fear Of Missing Out):** 24 saat içerisinde silinecek veya belirli süreli içeriklere kaybolmadan bakmak gerekli mecburiyeti hissettirir.
- **Kişiselleştirilmiş Algoritmalar:** Kişinin dijital tercihleri ya da ilgilerine dayalı algoritmalar marifetiyle platformdan ayrılmayı geciktirir.
- **Onay Dayatması:** Çoğu kullanıcıların bilinçsizce önceden işaretlediği onay çerezleri sayesinde, kullanıcının çeşitli akış ve seçeneklere yönlendirilmesi.
- **Karmaşık Menü Tasarımı:** Abonelikten çıkış veya çerez reddetme seçeneklerinin var ancak görünürlüğünün çok az olması ya da karmaşık menüler altında gizlenmesi.

Bu tasarımların büyük çoğunluğu kasıtlı olarak geliştirilmiştir ve "Dikkat ekonomisi" de denen bu modelde, kullanıcının zamanı ve dikkati reklam verenler için bir ürün haline dönüşür.

4.3.2. Dinamik Fiyatlandırma ve Algoritmik Gizli Anlaşmalar (Collusion)

Yapay zekâ, rakiplerin fiyatlarını anlık olarak takip ederek platformun veya satıcının fiyatlarını otomatik biçimde güncelleyebilir.

- **Risk Faktörü:** Eğer platformun kendi satış birimi, üçüncü taraf satıcılara ait fiyat verilerini yapay zekâ modellerini eğitmek için kullanıyorsa, bu durum “yıkıcı fiyatlandırma” (predatory pricing) riskini beraberinde getirebilir.
- **Algoritmik Gizli Anlaşma:** Farklı platformlara veya satıcılara ait algoritmalar, insanlar arasında doğrudan bir iletişim olmadan da fiyatları belirli bir seviyede tutacak şekilde uyumlu davranışlar geliştirebilir. Bu durum, rekabet hukukunda tespiti en zor alanlardan biri olarak değerlendirilmektedir.

- **Referans:** OECD - Algorithms and Collusion: Competition Policy in the Digital Age - Algoritmaların kendi aralarında nasıl fiyat birliği yapabileceğini ve buna karşı geliştirilen denetim yöntemlerini açıklar.

4.3.3. Düzenleyici Çerçeve: AB ve Türkiye Karşılaştırması

Mevcut düzenleme yaklaşımı, manipülatif tasarımları giderek daha fazla bir hak ihlali olarak ele alma yönünde ilerlemektedir:

- **Avrupa Birliği Yaklaşımı:** Digital Services Act (DSA) Madde 25, kullanıcıyı yanıltan arayüz tasarımlarını açık şekilde yasaklamaktadır. GDPR, “özgürce verilmiş rıza” standardı ile manipülatif onay mekanizmalarını hukuken geçersiz sayarken; UCPD bu tür uygulamaları haksız ticari uygulama kapsamında değerlendirmektedir.
- **Türkiye’deki Mevcut Durum:** Türkiye’de “dark patterns” kavramı henüz mevzuatta doğrudan yer almamaktadır. Bununla birlikte, Tüketici Koruma Kanunu, Ticari Reklam Yönetmeliği ve KVKK çerçevesinde dolaylı bir denetim söz konusudur. Ancak özellikle çerez yönetimi ve abonelik iptal süreçleri gibi alanlarda, dijital platformlara özgü daha sistematik bir düzenleme ihtiyacı dikkat çekmektedir.

Risk Analizi ve Etki Değerlendirmesi

Manipülatif tasarımlar, dijital ekosistemde aşağıdaki risk alanlarını derinleştirmektedir:

- **Kullanıcı Özerkliğinin Erozyonu:** Bilinçli tercih hakkının, yönlendirici tasarım pratikleriyle zayıflatılması.
- **Haksız Rekabet:** Bu yöntemleri kullanan aktörlerin, daha şeffaf çalışan platformlar karşısında avantaj elde etmesi.
- **Hukuki Geçersizlik:** Veri işleme süreçlerinde alınan rızanın, özgür iradeyi yansıtmaması nedeniyle hukuken tartışmalı hale gelmesi.
- **Kırılgan Gruplar:** Çocuklar ve dijital okuryazarlığı düşük bireylerin manipülasyona daha açık hale gelmesi.

Politika Tasarım İlkeleri ve Öneriler

TBD Çalışma Grubu perspektifiyle, Türkiye’de uygulanabilir bazı politika adımları şu şekilde özetlenebilir:

- **Simetri İlkesi:** Kabul etme ve reddetme seçeneklerinin eşit görünürlükte, boyutta ve renkte sunulması sağlanmalıdır.
- **Davranışsal Denetim Metodolojileri:** Düzenleyici kurumlar, platformların rıza mekanizmalarını kullanıcı deneyimi denetimleri (UX audit) ve seçim mimarisi testleri (choice architecture testing)

ile değerlendirmelidir. Bu yaklaşım, rızanın manipülatif tasarımlardan etkilenip etkilenmediğini anlamak açısından kritik önemdedir.

- **Kolay Çıkış Standardı:** Hizmetten ayrılma süreci, hizmete katılım süreci kadar basit ve erişilebilir olmalıdır.
- **İdari Koordinasyon:** Reklam Kurulu ile KVKK arasında dijital arayüz denetimlerine yönelik bir iş birliği mekanizması kurulmalı ve bu alana özel bir “Manipülatif Tasarım Rehberi” yayımlanmalıdır.

İzleme ve KPI Göstergeleri

Politika etkinliğini izlemek için aşağıdaki metrikler takip edilebilir:

- **Uyum Oranı:** Platformların simetrik tasarım standartlarına ne ölçüde uyum sağladığı.
- **Süreç Verimliliği:** Abonelik iptali için gereken ortalama adım sayısı ve işlem süresi.
- **Şikâyet ve Tespit:** Kullanıcı şikâyetleri içinde manipülatif tasarım kaynaklı başvuruların oranı ve tespit edilen rıza geçersizliği vakaları.

4.4. Gelir Modelleri ve Platform Ekonomisi

(Reklam, Abonelik ve Veri Temelli Değer Üretimi Perspektifi)

Dijital platformların ekonomik sürdürülebilirliği, büyük ölçüde benimsedikleri gelir modellerine bağlıdır. Reklam temelli yapılar, abonelik sistemleri, komisyon bazlı pazar yerleri ve hibrit modeller; platformların kullanıcı deneyimini, veri işleme pratiklerini ve rekabet davranışlarını doğrudan şekillendirir.

Gelir modeli yalnızca ticari bir tercih değildir; aynı zamanda tüketici hakları, veri koruma, pazar yoğunlaşması ve adil rekabet üzerinde belirleyici etkiler yaratır. Avrupa Birliği düzenlemeleri de gelir modellerini doğrudan hedeflemek yerine, bu modellerin ortaya çıkardığı risklere odaklanmaktadır. Digital Markets Act (DMA), sistemik platformların ekonomik gücünü sınırlamayı amaçlarken; Digital Services Act (DSA), şeffaflık ve kullanıcı koruması üzerinden dolaylı bir etki yaratmaktadır.

Bu bölüm, dijital platformların gelir modellerinin arkasındaki ekonomik mantığı ortaya koymayı; Türkiye’deki mevcut uygulamaları değerlendirmeyi ve risk temelli bir politika yaklaşımı geliştirmeyi amaçlamaktadır.

Platform Ekonomisinde Yapısal Özellikler ve Türkiye Panoramasi

Dijital platform ekonomisi; ağ etkileri, ölçek ekonomisi ve veri avantajı gibi temel dinamiklerle şekillenir. Bu yapı, özellikle DMA kapsamında “gatekeeper” (geçit bekçisi) olarak tanımlanan platformların rekabet üzerinde baskı kurma riskini de beraberinde getirmektedir. OECD analizleri, veri birikiminin dijital pazarlarda yeni oyuncular için ciddi bir giriş engeli oluşturabileceğine işaret etmektedir.

Türkiye Bağlamında Mevcut Durum:

- **Baskın Modeller:** Reklam temelli modeller ile e-ticarete komisyon ve sponsorlu ürün yapıları pazarda belirleyici konumdadır.
- **Pazar Dinamikleri:** Platform içi çapraz hizmet gelirlerinin artması, ekonomik yoğunlaşmayı güçlendirmekte ve KOBİ'lerin platformlara olan bağımlılığını daha da artırmaktadır.

4.4.1. Politika Önerileri, KPI ve İzleme

Düzenleyici çerçevenin etkinliğini ölçmek için aşağıdaki mekanizmaların hayata geçirilmesi önerilmektedir:

1. **Risk Analizi:** Sistemik platformlara, benimsedikleri gelir modeline bağlı olarak periyodik risk raporlama yükümlülüğü getirilmelidir.
2. **Şeffaflık Standartları:** Komisyon oranlarının, sponsorlu sıralamaların ve çapraz veri kullanımının açık ve anlaşılır şekilde paylaşılması sağlanmalıdır.
3. **Kullanıcı Hakları:** Abonelik iptal süreçlerinde “tek tıkla çıkış” gibi basit ve erişilebilir standartlar belirlenmelidir.

İzleme Göstergeleri (KPI):

- İlk 3 platformun toplam gelir payı (pazar yoğunlaşması)
- Sponsorlu içeriklerin toplam içeriğe oranı
- Abonelik iptali için harcanan ortalama süre
- Komisyon oranlarına ilişkin şeffaflık seviyesi

Dijital ekonomide gelir modelleri artık yalnızca finansal bir tercih değil; pazarın rekabet yapısını ve kullanıcı özerkliğini doğrudan etkileyen bir unsur haline gelmiştir. Bu nedenle politika tasarımının odağı, gelir modellerini yasaklamak değil; bu modellerin veri hakimiyeti ve pazar gücü üzerindeki etkilerini dengelemek olmalıdır.

4.5. Tüketicie Sunulan Ticari Bilginin Şeffaflığı

Perspektif: Fiyatlandırma, Sıralama ve bilgilendirilmiş karar verme

Dijital platformlarda sunulan ticari bilgiler; fiyat, indirim oranı ve sıralama kriterleri gibi unsurlar üzerinden tüketicinin ekonomik kararlarını doğrudan etkiler. Şeffaflığın yetersiz olduğu durumlarda, algoritmik sistemler ve “karanlık desenler” (dark patterns) kullanıcıların bilinçli karar verme kapasitesini zayıflatabilmektedir.

Ticari Bilginin Üç Boyutu ve AB Mevzuatı

Tüketici kararlarını etkileyen ticari bilgi, üç temel başlık altında ele alınabilir:

1. **Fiyat Şeffaflığı:** Gerçek satış fiyatı ve indirim geçmişinin açık şekilde sunulması (UCPD / Omnibus Direktifi).
2. **Sıralama Şeffaflığı:** Listeleme kriterlerinin temel parametrelerinin kullanıcıyla paylaşılması (P2B Regulation).
3. **Ticari İçerik Tanımlama:** Reklam ve sponsorlu içeriklerin diğer sonuçlardan açık şekilde ayrıştırılması ve etiketlenmesi (DSA).

Bu kapsamda ticari bilgi; tüketicinin kararını etkileyebilecek fiyat, kampanya, indirim, sıralama ve benzeri tüm ticari unsurları kapsar.

Türkiye’deki Mevcut Durum ve Risk Analizi

Türkiye’de bu alan büyük ölçüde Tüketici Koruma Kanunu ve Reklam Kurulu kararları çerçevesinde ele alınmaktadır. Ancak dijital platformlara özgü bazı risk alanları öne çıkmaktadır:

- **Dinamik Fiyatlandırma Opaklığı:** Kişiyi özel fiyatlandırma uygulamalarında, bu durumun kullanıcıya açık şekilde belirtilmemesi.
- **Yapay Kıtlık Mesajları (dark patterns):** “Son 2 ürün” gibi doğrulanmamış ifadelerle kullanıcı üzerinde psikolojik baskı oluşturulması.
- **Sponsorlu Ürün Gizleme:** Reklam içeriklerinin, organik sonuçlarla görsel olarak benzer şekilde sunularak ayırt edilmesinin zorlaştırılması.

4.5.1. E-Ticaret, P2B İlişkileri ve Self-Preferencing (Kendine Öncelik)

E-ticaret platformları hem pazar yeri işletmecisi hem de satıcı olarak faaliyet gösterdiğinde, yapısal bir çıkar çatışması ortaya çıkar. Bu çift rol, platformun kendi ürünlerine öncelik tanıma (self-preferencing) riskini beraberinde getirir. Özellikle sıralama algoritmaları, veri erişimi, komisyon oranları ve sponsorlu görünürlük uygulamaları; küçük ve orta ölçekli işletmeler (KOBİ’ler) açısından rekabet koşullarını doğrudan etkiler.

Avrupa Birliği bu alandaki riskleri iki temel düzenleme üzerinden ele almaktadır. Platform-to-Business Regulation (P2B), platform ile ticari kullanıcılar arasındaki şeffaflık yükümlülüklerini düzenlerken; Digital Markets Act (DMA), sistemik platformların self-preferencing ve veri avantajı yoluyla rekabeti bozmasını sınırlamayı hedeflemektedir.

Algoritmik Sıralama ve Tasarım Yoluyla Yönlendirme (Steering)

Modern e-ticaret platformları, tüketicinin karar verme sürecini büyük ölçüde arayüz tasarımı ve seçim mimarisi (choice architecture) üzerinden şekillendirir. Bu bağlamda self-preferencing, çoğu zaman algoritmaların içine gömülü bir ticari strateji olarak ortaya çıkar.

- **Teknik Mekanizma:** Algoritmalar genellikle “alaka düzeyi” (relevance) üzerinden çalıştığını iddia eder. Ancak uygulamada, platformun kendi lojistik ağını kullanan veya kendi markasına ait ürünlere ek avantajlar sağlayan katsayılar devreye girebilir. Bu durum, organik sonuçların tarafsızlığını zayıflatır.
- **Ekonomik Perspektif – Arama Maliyeti (Search Cost):** Tüketiciler çoğu zaman sınırlı dikkatle hareket eder. Bu nedenle ilk sayfada yer almayan bir ürün, pratikte görünmez hale gelir. Platform, kendi ürünlerini daha görünür kılarak rakip ürünlerin erişimini zorlaştırdığında, arama maliyetlerini yapay şekilde artırmış olur. Bu da zamanla rekabetin daraldığı bir yapı ortaya çıkarır.

Referans: OECD - Self-preferencing by Digital Platforms (2022) - *Bu rapor, platformların algoritma tasarımlarıyla rakipleri nasıl marjinalleştirdiğini teorik modellerle açıklar.*

4.5.2. Self-Preferencing ve DMA Yaklaşımı

Self-preferencing (kendini önceliklendirme), platformun kendi hizmetlerini algoritmik olarak avantajlı konumlara yerleştirmesidir. AB'nin **Digital Markets Act (DMA)** düzenlemesi bu riski üç ana başlıkta sınırlar:

Uygulama	Rekabet Riski	DMA Müdahalesi
Ayrıcalıklı Sıralama	Rakip satıcının görünmez kılınması.	Algoritmik şeffaflık ve adil sıralama yükümlülüğü.
Veri Kullanımı	Satıcı verisiyle rakip ürün üretme.	Ticari kullanıcı verisine erişim yasağı.
Çapraz Entegrasyon	Lojistik/Ödeme hizmetine zorlama.	Hizmetlerin birbirinden ayrıştırılması (Paketleme - Bundling - yasağı).

Politika Hedefleri; Platform-İşletme dengesini sağlamak adına:

1. **Sıralama Şeffaflığı:** Ücretli sıralamanın organik sonuçlardan net ayrımı.
2. **Erişim Eşitliği:** KOBİ'lerin platform verilerine (kendi satış verileri bazında) adil erişimi.
3. **Haksız Sözleşme Şartları:** Komisyon ve hizmet bedellerinde öngörülebilirlik

Tüketiciye sunulan ticari bilginin şeffaf hale getirilmesi ile platformlar arası adil rekabetin tesisi birbirini besleyen süreçlerdir; zira 'kendini önceliklendirme: self-preferencing' sadece rakip işletmeye değil, yanıltıcı sıralama yoluyla doğrudan tüketicinin ekonomik refahına da zarar vermektedir.

4.6. Platform Yönetişiminin Politik Ekonomisi: Jeopolitik Dinamikler ve Güç Dengesi

Dijital platformların yalnızca ekonomik araçlar olmaktan çıkıp kamusal alanı şekillendiren altyapılara dönüşmesi, yönetim tartışmalarını teknik bir uyum meselesinin ötesine taşımıştır. Bu süreç artık daha çok stratejik ve hatta jeopolitik bir güç mücadelesi olarak ele alınmaktadır. Bu çerçevede, dijital platform ekonomisini düzenleme çabalarının arkasındaki temel yaklaşım ve küresel dinamikler birkaç ana başlık altında değerlendirilebilir:

Yönetişim Modellerinin Normatif Mantığı ve Devlet-Platform-Toplum Güç Dengesi:

Dijital pazarlarda platformlar artık yalnızca hizmet sunan ticari yapılar değildir. Aynı zamanda pazarın kurallarını belirleyen, algoritmalar üzerinden kullanıcı davranışlarını yönlendiren ve kamusal tartışma alanını etkileyen aktörler haline gelmiştir. Bu nedenle çoğu zaman “özel regülatör” (private regulator) ya da fiilen kamusal alan altyapısı sağlayıcısı olarak konumlanmaktadır.

Bu durum, klasik “devlet–vatandaş” ilişkisinin arasına güçlü bir üçüncü aktör olarak platformların girmesine yol açmıştır. Ortaya çıkan bu güç dengesizliği, yeni nesil düzenlemelerin de temel çıkış noktasını oluşturur.

DSA ve DMA gibi düzenlemelerin arkasındaki yaklaşım, geçmişteki “sorumsuzluk” (safe harbor) anlayışını sınırlayarak platformlara topluma karşı daha fazla sorumluluk yüklemektir. Bu çerçevede hedeflenen model; devletin kuralları önceden belirlediği, sivil toplum ve akademinin denetim süreçlerine dahil olduğu ve platformların daha fazla hesap verdiği çok paydaşlı bir yönetim yapısıdır.

Dijital Egemenlik, Veri Milliyetçiliği ve Küresel Platform Gücü:

Büyük veri havuzlarına ve güçlü altyapılara sahip küresel platformlar, artık ulus-devletlerle müzakere edebilen aktörlere dönüşmüştür. Bu durum, farklı ülkelerin düzenleme boşluklarının birbirine karşı kullanıldığı “düzenleyici arbitraj” riskini de beraberinde getirmektedir.

Devletlerin bu tabloya verdiği tepkilerden biri, veriyi ülke sınırları içinde tutmaya yönelik “veri milliyetçiliği” yaklaşımıdır. Ancak Türkiye açısından daha sürdürülebilir bir yaklaşım, tamamen içe kapanan bir modelden ziyade; uluslararası standartlarla uyumlu, birlikte çalışabilirliği (interoperability) esas alan ve şeffaf bir dijital ekosistem kurmaktır.

Gerçek anlamda dijital egemenlik, veriyi sadece sınırlar içinde tutmak değil; küresel değer zincirinde söz sahibi olabilen ve standart belirleyebilen bir konuma ulaşabilmektir.

Yapay Zekâ (YZ) Yönetişiminde Bloklaşma ve Standart Rekabeti:

Dijital platformlar ve yapay zekâ alanında küresel ölçekte belirgin bir düzenleme ayrışması yaşanmaktadır. Bu alanda üç ana yaklaşım öne çıkmaktadır:

- Avrupa Birliği modeli: Temel haklar, sosyal refah ve adil rekabeti önceliklendirir
- ABD modeli: İnovasyonu ve piyasa dinamiklerini ön plana çıkarır
- Çin modeli: Veri ve platform gücünü daha çok devlet kontrolü altında tutmayı hedefler

Bu küresel rekabet ortamında Türkiye'nin yalnızca kuralları takip eden bir aktör olması yeterli değildir. Özellikle “Brüksel Etkisi”nin (Brussels Effect)¹³⁶ küresel standartları şekillendirdiği bir dönemde, Türkiye'nin uluslararası platformlarda (GPAI¹³⁷, ICN¹³⁸) daha aktif rol alması önemlidir.

Türkiye'nin hedefi; yerel kapasitesini OECD ve AB normlarıyla uyumlu şekilde güçlendirerek, bölgesel ölçekte söz sahibi olan ve belirli alanlarda “kural koyucu” rol üstlenebilen bir yapıya ulaşmak olmalıdır.

¹³⁶ **Bradford, Anu.** *The Brussels Effect: How the European Union Rules the World*. Oxford University Press, 2020. <https://global.oup.com/academic/product/the-brussels-effect-9780190088583>

¹³⁷ **GPAI (Global Partnership on Artificial Intelligence).** <https://oecd.ai/en/>

¹³⁸ **ICN (International Competition Network).** <https://www.internationalcompetitionnetwork.org/>

4.7. Bütünleşik Denetim, Yaptırımlar ve Politika Önerileri

Risk Alanı	AB Karşılığı	Türkiye İçin Öneri	KPI
Reklam Kimliklendirme Opaklığı	DSA [1]	Dijital Reklam Şeffaflık Standardı	Açık etiketli reklam oranı
Çocuklara Yönelik Hedefleme	DSA [1], GDPR [3]	Çocuklara davranışsal reklam yasağı	Çocuk hedefli reklam ihlal sayısı
Hassas Veri Profil Çıkarma	GDPR [3]	Hassas veri temelli segmentasyon sınırı	Hassas veri kampanya oranı
Dark Patterns	DSA [1], UCPD [8]	Manipülatif Tasarım İlkeleri Rehberi	Simetrik tasarım uyum oranı
Self-Preferencing	DMA [2]	Sistemik platformlarda açık yasak	Self-preferencing şikâyet sayısı
Sıralama Opaklığı	P2B [6]	Sıralama parametre açıklama yükümlülüğü	Parametre açıklık oranı
Komisyon Belirsizliği	P2B [6]	Önceden bildirim zorunluluğu	Komisyon bildirim süresi
Veri Yoğunlaşması	DMA [2], OECD [4]	Veri erişim hakkı ve ayrıştırma	Veri erişim talep oranı
Sahte İndirim	UCPD [8]	Referans fiyat zorunluluğu	Sahte indirim tespit sayısı
Dinamik Fiyat Opaklığı	UCPD [8], DSA [1]	Dinamik fiyat bildirim standardı	Dinamik fiyat açıklama oranı
KOBİ Platform Bağımlılığı	DMA [2], OECD [4]	Yoğunlaşma ve bağımlılık raporu	İlk 3 platform pazar payı
Ölçümleme Opaklığı	OECD [4]	Bağımsız reklam ölçüm erişimi	Bağımsız doğrulama oranı

P2B ilişkileri ve adil rekabet konusunda dünyada iki ana ekol öne çıkmaktadır:

- **Avrupa Birliği Modeli (Normatif Yaklaşım):** DMA ve DSA ile "geçit bekçisi" platformlara ex-ante (önleyici) ve sert yükümlülükler getirir. Sosyal refah ve adil pazarı önceler.
- **ABD Modeli (Piyasa Odaklı Yaklaşım):** Geleneksel olarak inovasyonu korumak adına daha esnek bir tutum sergilese de son yıllarda "Big Tech" üzerindeki antitröst baskısını artırmıştır (Örn: American Innovation and Choice Online Act).
- **Asya (Çin) Modeli:** Platformların finansal güçlerini ve veri tekellerini kırmaya yönelik ani ve yapısal müdahalelerle karakterize edilir.

- **Referans:** UNCTAD- Digital Economy Report 2024 -¹³⁹ *Dünya genelindeki dijital yönetim modellerinin ekonomik kalkınma üzerindeki etkilerini kıyaslayan kapsamlı rapor.*

BÖLÜM 5: YAPAY ZEKÂ VE ALGORİTMİK SİSTEMLER

Bölümün Amacı: Çevrim içi platformların tarafsız vitrinler olmaktan çıkıp toplumsal ve ekonomik akışı düzenleyen altyapılara dönüşmesinde belirleyici rol oynayan algoritmik sistemleri; sadece teknik bir verimlilik aracı olmaktan çıkarıp demokrasi, temel haklar, adil rekabet ve kamusal yarar ekseninde şeffaf, hesap verebilir ve denetlenebilir bir yönetim çerçevesine oturtmaktır.

İçerik ve Kapsam:

- AB Yapay Zekâ Yasası (AI Act) ve Dijital Hizmetler Yasası (DSA) standartlarında, tekil içerik kararları yerine sistem düzeyinde "risk temelli" bir yapay zekâ yönetimi mimarisinin kurulması.
- Öneri ve sıralama sistemlerinin yarattığı "yankı odaları", veri kümelerindeki algoritmik ayrımcılık (bias) ve çocukları/kırılgan grupları hedef alan bağımlılık yapıcı manipülasyonların önlenmesi.
- Üretken yapay zekâ (GenAI) kaynaklı sentetik içeriklerin (deepfake) etiketlenmesi, makine-okunur şekilde işaretlenmesi ve dezenformasyonla mücadele yükümlülükleri.
- Platformların "kara kutu" yapısını açmak için bağımsız denetim metodolojileri, araştırmacı veri erişimi (vetted researchers) ve "Algoritmik Etki Değerlendirmesi" (AIA) araçlarının operasyonelleştirilmesi.
- Yenilikçiliği boğmadan regülasyona uyumunu test etmeye yarayan "Düzenleyici Kum Havuzları"nın (Regulatory Sandboxes) inşası

Temel Kavramlar:

- Algoritmik Sistemler
- Üretken YZ (Generative AI) ve Sentetik İçerik
- Algoritmik Kapı Bekçiliği (Algorithmic Gatekeeping)
- Algoritmik Etki Değerlendirmesi (AIA)

¹³⁹ <https://unctad.org/publication/digital-economy-report-2024>

- *Düzenleyici Kum Havuzu (Regulatory Sandbox)*

5.1. Özet

Çevrim içi platformların tarafsız vitrinler olmaktan çıkıp toplumsal ve ekonomik akışı düzenleyen altyapılara dönüşmesinde yapay zekâ (YZ) ve algoritmik sistemler belirleyici rol oynar. Platformlar içerik akışları, arama sonuçları, sizin için sayfaları, reklam hedefleme, ürün ve satıcı sıralaması, spam ve sahte hesap tespiti gibi işlevlerde algoritmik sistemleri yoğun biçimde kullanır. Söz konusu algoritmik sistemler ile, kullanıcı deneyimi yönlendirmenin yanında, bilginin erişilebilirliği, algoritmik hiyerarşi, ekonomik değerin tercih edilen paydaşlar arasında dağılımı, ve sosyo-politik ifadelerin dijital ekosistemdeki yayılım hızı ile dinamiklerini de belirleyici bir güce sahiptir. Bu nedenle YZ ve algoritmik sistemler platform yönetişiminin teknik bir alt başlığı olmakla beraber, şeffaflık, hesap verebilirlik, kullanıcı güvenliği, rekabet ve temel haklar mimarisinin kesişim noktasıdır.

Çevrim içi platformlarda kullanılan algoritmik sistemler yalnızca teknik verimlilik araçları değildir. Bu sistemler, kamusal tartışmanın görünürlüğü, ekonomik aktörlerin erişim imkânlarını, kullanıcıların maruz kaldığı bilgi akışını ve kırılgan grupların dijital deneyimini şekillendiren bir güç mimarisi üretir. Bu nedenle platform algoritmalarına ilişkin yönetim meselesi, sadece teknoloji politikası değil; demokrasi, temel haklar, adil rekabet ve kamusal yarar meselesidir.

Bu alandaki düzenleyici eğilim, tek tek içerik kararları yerine sistem düzeyi risk ve kurumsal süreç odaklı bir denetim anlayışına kaymaktadır. Örneğin, AB Dijital Hizmetler Yasası (Digital Service Act - DSA), çok büyük çevrim içi platformlar ve arama motorları için hizmetin tasarımından ve algoritmik sistemler dahil olmak üzere ilgili sistemlerinden kaynaklanan sistemik risklerin düzenli biçimde değerlendirilmesini, risk azaltım önlemlerinin uygulanmasını ve bağımsız denetimi öngörür. DSA ayrıca öneri sistemlerinin temel parametrelerinin anlaşılır biçimde açıklanmasını ve belirli durumlarda profil çıkarmaya dayanmayan seçenekler sunulmasını da platform sorumluluğunun parçası hâline getirmektedir.¹⁴⁰

Benzer biçimde, AB YZ Yasası (EU AI Act), risk temelli bir çerçeve kurarak “yüksek riskli” olarak sınıflandırılan YZ sistemleri için yaşam döngüsü boyunca risk yönetimi, veri yönetimi, insan gözetimi, dayanıklılık ve siber güvenlik, piyasaya arz sonrası izleme ve ciddi olay bildirimi gibi yükümlülükler getirmektedir. Ayrıca sentetik içerik üreten sistemlerde makine-okunur işaretleme ve sentetik içerik (deepfake) üretimi ve dağıtımında kullanıcıya açıklama gibi şeffaflık ödevleri öne çıkarmaktadır. Genel

¹⁴⁰ Digital Services Act. <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act>.

amaçlı YZ (General Purpose of AI - GPAI) modelleri için teknik dokümantasyon ve eğitim verisi içeriğine dair özet yayımlama gibi hükümler de platform ekosistemini doğrudan etkileyebilir.¹⁴¹

Veri koruma boyutunda ise GDPR, kişisel veriye dayalı profil çıkarma ve otomatik karar verme bağlamında anlamlı bilgilendirme, yalnızca otomatik işlemeye dayalı ve benzer ölçüde önemli etkiler doğuran kararlar bakımından itiraz ve insan müdahalesi gibi korumalar ve hassas veri kategorileriyle ilgili sınırlamalar içermektedir. Bu çerçeve, özellikle reklam hedefleme, risk skrolama, içerik görünürlüğü, hesap ve ürün kısıtları gibi platform kararlarının meşruiyeti açısından kritik öneme sahiptir.¹⁴²

Uluslararası iyi uygulamalar ise yalnızca AB'ye özgü değildir. OECD YZ İlkeleri insan hakları, şeffaflık, açıklanabilirlik, sağlamlık ve hesap verebilirlik gibi değerleri devletlerarası standart seviyesine taşımaktadır.¹⁴³ Avrupa Konseyi'nin 2024 tarihli "YZ, İnsan Hakları, Demokrasi ve Hukukun Üstünlüğü" Çerçeve Sözleşmesi, YZ sistemlerinin yaşam döngüsünde risk ve etki yönetimini, şeffaflık ve gözetimi ve hak ihlallerine karşı etkili başvuru yollarını hukuken bağlayıcı bir zemine taşımaktadır.¹⁴⁴

Platformların yayımladığı şeffaflık raporları, bağımsız denetim, veri erişimi, etki değerlendirmesi ve etkili başvuru mekanizmalarıyla desteklenmediğinde, hesap verebilirlikten ziyade kurumsal meşruiyet üretme işlevi görebilir. Bu risk, özellikle YZ etiği söyleminin bağlayıcı kurumsal yükümlülükler yerine gönüllü beyanlarla sınırlandığı durumlarda daha görünür hale gelir.

Bu bölümün temel tezi şudur: Platformlarda algoritmik sistemlere ilişkin politika seti;

- 1) Risk temelli,
- 2) Çok paydaşlı,
- 3) Denetlenebilir ve
- 4) Ölçülebilir yükümlülükler üzerinden tasarlanmadığında, şeffaflık raporları "bilgi sunan fakat hesap vermeyen" belgelere dönüşebilir.

Buna karşılık, iyi tasarlanmış yönetim araçları, kullanıcı güvenliği, çocukların korunması, ifade özgürlüğü, ayrımcılığın önlenmesi ve adil rekabet gibi hedefleri birlikte ilerletme potansiyeli taşımaktadır.

¹⁴¹ EU Artificial Intelligence Act, Up-to-date Developments and Analyses of the EU AI Act. <https://artificialintelligenceact.eu/>

¹⁴² GDPR, (General Data Protection Regulation), (2024). <https://gdpr-info.eu/>.

¹⁴³ OECD, AI Principles. <https://www.oecd.org/en/topics/sub-issues/ai-principles.html>.

¹⁴⁴ European Networks of National Human Rights Institutions (ENNHRI), (2025). European Regulatory Frameworks on AI. <https://ennhri.org/ai-resource/european-regulatory-frameworks-on-ai/>.

5.2. Kavramsal Temeller: Platformlarda Algoritmik Sistemler Ne Anlama Gelir?

Algoritmik sistemler, platformun bir hedefe (örneğin: etkileşimi artırma, zararlı davranışı azaltma, gelir optimizasyonu) yönelik olarak girdileri (kullanıcı etkileşimleri, metin ve görüntü, profil verisi, bağlamsal sinyaller vb.) işleyip çıktı (tahmin, öneri, sıralama, karar, kısıtlama) ürettiği sosyo-teknik düzeneklerdir. NIST AI RMF, YZ sistemlerini belirli hedefler için tahminler, öneriler veya kararlar gibi çıktılar üreten mühendislik ve makine tabanlı sistemler olarak tarif eder.¹⁴⁵ Avrupa Konseyi Çerçeve Sözleşmesi de benzer şekilde YZ sistemlerini girdiden tahmin, içerik, öneri veya karar üreten, fiziksel ve sanal çevreyi etkileyen makine temelli sistemler olarak tanımlar.¹⁴⁶

Platform bağlamında algoritmik sistemler içerik öneren veya sıralayan araçlar olmanın ötesinde görünürlüğü, Herbert A. Simon'ın temellerini attığı dikkat ekonomisini (attention economy)¹⁴⁷, ticari fırsatları ve kullanıcı davranışlarını düzenleyen yönetsel mekanizmalardır. Bu nedenle algoritmik sistemlerin teknik performansı kadar hangi toplumsal ve ekonomik sonuçları ürettiği de değerlendirme konusu olmalıdır. Veri (bilgi) bolluğunun yaşandığı dijital ekosistemde kısıtlı bir kaynak olan 'insan dikkatini' yönlendirebilen bu algoritmalar, ekonomik değerin etkin belirleyicisi konumundadır. Bu nedenle, algoritmik sistemlerin yalnızca teknik performansı değil, bu 'dikkat yönetimi' aracılığıyla hangi toplumsal ve ekonomik sonuçları ürettiği de ele alınacak önemli bir değerlendirme konusudur.

Bu bölümde “algoritmik sistemler” şemsiyesi altında, platform pratiklerinde en sık görülen aşağıdaki türler kastedilir:

- **Otomasyon ve kural tabanlı sistemler:** Basit eşik değerleri, kara liste, ak liste ve “if-then” kuralları ile çalışan; spam filtreleme veya basit güvenlik kontrollerinde görülen yapılardır.
- **Öneri sistemleri:** Kullanıcının geçmiş davranışlarından veya benzer kullanıcıların tercihlerinden hareketle içerik, ürün ve hesap öneren sistemlerdir. DSA, öneri sistemleri için temel parametrelerin şartlarda anlaşılır biçimde açıklanmasını gerektirir.¹⁴⁸
- **Sıralama ve görünürlük sistemleri (ranking):** İçerik, ürün ve satıcıların hangi sırayla ve hangi bağlamda gösterileceğini belirler. AB P2B Yasası, çevrim içi aracılık hizmetlerinde “sıralamayı belirleyen ana parametreler” ve görece önemlerinin şartlarda açıklanmasını öngörür.¹⁴⁹
- **Hedefleme ve optimizasyon sistemleri (özellikle reklam):** Kitle segmentasyonu, açık artırma optimizasyonu, gösterim frekansı, dönüşüm tahmini gibi alt sistemlerdir. DSA, reklamın “kime

¹⁴⁵ National Institute of Standards and Technology (NIST), US Department of Commerce. AI Risk Management Framework, (2025). <https://www.nist.gov/itl/ai-risk-management-framework>.

¹⁴⁶ Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (2024). <https://rm.coe.int/1680afae3c>

¹⁴⁷ Herbert A. Simon, "Designing Organizations for an Information-Rich World" in *Computers, Communications, and the Public Interest*, ed. Martin Greenberger (Baltimore, MD: The Johns Hopkins Press, 1971), 40–41

¹⁴⁸ DSA, (2022). <https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng>.

¹⁴⁹ P2B Regulation, (2019). <https://eur-lex.europa.eu/eli/reg/2019/1150/oj/eng>.

neden gösterildiğine” dair ana parametre bilgisini ve belirli veri türleriyle profil çıkarmaya dair kısıtları düzenler.

- **Üretken YZ (generative AI) ve etkileşimli arayüzler:** Metin, görsel, video ve ses üretimi; sohbet botları, içerik özetleme ve arama yanıtları. AB YZ Yasası, sentetik içerik üreten sistem çıktılarının (teknik olarak mümkün olduğu ölçüde) işaretlenmesini ve sentetik içeriklerde (deepfake) açıklama yapılmasını zorunlu kılmaktadır.
- **Karar-destek ve yaptırım sistemleri:** İçerik kaldırma, etiketleme, hesap kapama, erişim kısıtlama, ürün listeleme gibi kararlara puan, risk skoru veya öncelik sağlayan araçlardır. GDPR, belirli koşullarda “yalnızca otomatik işlemeye dayalı” ve kişi üzerinde önemli etki doğuran kararlar bakımından insan müdahalesi gibi güvencelere işaret eder.

Sosyo-teknik nitelik, bu sistemlerin yalnızca kod ve model parametrelerinden öte platform politikalarından, ticari teşviklerden, moderasyon süreçlerinden, veri toplama pratiklerinden ve kullanıcı davranışlarından birlikte etkilenmesi anlamına gelir.

Bu sistemler, platformların altyapısına çoğu zaman tek bir model olarak değil, birden çok aşamalı **işleyiş mekanizmaları** olarak gömülüdür:

- Veri toplama,
- Aday içerik ve ürün seçimi,
- Sıralama ve filtreleme,
- Arayüz sunumu,
- Kullanıcı geri bildirimi,
- Model güncelleme.

DSA’nın sistemik risk değerlendirmesi yaklaşımı, bu zincirde yalnızca içeriğin kendisini değil, öneri, reklam ve moderasyon gibi algoritmik tasarım öğelerini de riskin kaynağı olarak görmektedir.

5.3. Platform YZ Sistemlerinde Temel Risk Alanları

Platformlardaki algoritmik riskler çoğu zaman tekil yazılım hatalarının yanı sıra, sistemin tasarım hedeflerinden, optimizasyon mantığından ve geri besleme döngülerinden doğmaktadır. Bu nedenle riskler yalnızca yanlış karar örnekleri üzerinden değil, hangi içeriklerin sistematik olarak yükseltildiği, hangi kullanıcı gruplarının görünmezleştiği ve hangi hakların yapısal biçimde zayıflatıldığı üzerinden analiz edilmelidir. Oluşan riskler, tekil yanlış karar vakalarından ziyade, sistemin tasarım hedefleri (örneğin etkileşim optimizasyonu vb.), veri kümeleri, geri besleme döngüleri ve denetim zayıflıklarıyla dahada büyüebilir.

DSA'nın VLOP¹⁵⁰ ve VLOSE'lar¹⁵¹ için tanımladığı risk kategorileri:

- Yasa dışı içeriğin yayılması,
- Temel haklara olumsuz etkiler,
- Sivil söylem/seçim süreçleri ve
- Kamu güvenliği üzerindeki etkiler ile çocuklar ve kırılgan gruplara yönelik zararlar gibi geniş bir spektrumu kapsamaktadır.

Algoritmik opaklık ve açıklanabilirlik açığı: Kullanıcılar için “Neden bunu görüyorum?” sorusu çoğu zaman yanıtsızdır; düzenleyiciler ve bağımsız denetçiler için de sistemin mantığı, testleri ve çalışma biçimi kapalı kutu kalabilir. DSA, öneri sistemlerinin ana parametrelerinin ve bu parametrelerin görelî öneminin anlaşılır biçimde açıklanmasını ister; ayrıca çok büyük platformlar için veri erişimi ve algoritmik sistem açıklaması yükümlülükleri öngörür. P2B Yasası da sıralama parametrelerinin açıklanmasını zorunlu kılar; ancak manipölasyonu kolaylaştıracak düzeyde algoritma ifşasının gerekli olmadığını vurgulayarak şeffaflık ticari sır dengesine işaret etmektedir. Bu noktada iki farklı şeffaflık düzeyi arasında ayırım yapmak gerekir. Kullanıcı için anlamlı ve erişilebilir açıklama ile denetçi, araştırmacı ve düzenleyici için kanıta dayalı denetlenebilirlik aynı şey değildir. Birincisi “neden bunu görüyorum?” sorusuna yanıt vermeyi, ikincisi ise sistemin hangi veri, test, performans ve risk kayıtlarıyla çalıştığının incelenebilmesini gerektirir.

Önyargı ve ayrımcılık riskleri: Veri kümelerindeki tarihsel önyargılar (bias), temsil eksiklikleri veya hatalı etiketleme, reklam hedefleme, içerik görünürlüğü, iş ve satıcı fırsatları ve moderasyon kararlarında sistematik ayrımcılığa dönüşebilir. AB YZ Yasası, yüksek riskli YZ sistemlerinde veri yönetişimi kapsamında olası önyargıların incelenmesini, bunların tespit ve azaltımına yönelik önlemleri açıkça düzenlemektedir. GDPR ayrıca profil çıkarmada ayrımcı etkilerin önlenmesi yönündeki gerekçeleri ve otomatik karar verme bağlamındaki korumalar ile bu risk alanını veri koruma düzleminde tamamlamaktadır.

Manipölasyon, bağımlılık tasarımı ve yükseltici etkileri: Öneri ve sıralama sistemleri, etkileşim temelli hedeflere göre tasarlandığında sansasyonel, kutuplaştırıcı veya yanlış içerikleri orantısız biçimde öne çıkarabilir. DSA, risk değerlendirmelerinde öneri sistemlerinin ve diğer algoritmik sistemlerin etkisinin özellikle dikkate alınmasını; ayrıca hizmetin kasıtlı manipölasyonunun (sahte ve otomatize kullanım) ve içerik amplifikasyonunun riskleri nasıl etkilediğinin analiz edilmesini istemektedir.

Demokratik ve epistemik riskler: Algoritmik sıralama ve öneri sistemleri, kullanıcıların hangi bilgiye maruz kaldığını belirlediği ölçüde bireysel deneyime ek olarak ortak kamusal gerçeklik zeminini de etkiler.

¹⁵⁰ Çok Büyük Çevrim İçi Platform (Very Large Online Platform): DSA'ya göre, AB içinde aylık ortalama en az 45 milyon aktif kullanıcıya ulaşan çevrim içi platformlar VLOP olarak sınıflandırılır.

¹⁵¹ Çok Büyük Çevrim İçi Arama Motoru (Very Large Online Search Engine): AB'de aylık en az 45 milyon aktif kullanıcıya ulaşan arama motorları VLOSE olarak sınıflandırılır.

Yanlış bilgi, kutuplaştırıcı içerik ve sentetik medya çıktılarının yükseltilmesi; toplumsal güvenin aşınmasına, kamusal tartışmanın parçalanmasına ve özellikle seçim dönemlerinde bilgi bütünlüğünün bozulmasına yol açabilir.

Çocuklar, gençler ve kırılgan gruplar açısından riskler: Platformların öneri ve etkileşim optimizasyonu mantığı, çocuklar ve kırılgan kullanıcı grupları bakımından bağımlılık üretici tasarımlar, zararlı içeriklere tekrar tekrar maruz kalma, manipülatif hedefleme ve dijital hakların zayıflaması gibi sonuçlar doğurabilir. Bu nedenle çocukların korunması, genel kullanıcı güvenliğinin alt başlığı olarak değil, özel ve güçlendirilmiş bir yönetim alanı olarak ele alınmalıdır.

YZ-tabanlı içerik moderasyonu zorlukları: Otomatik moderasyon araçları ölçek avantajı sağlar; ancak bağlamı kaçırma, dil ve kültür farklılıkları, yanlış pozitifler (meşru içeriğin kaldırılması) ve yanlış negatifler (zararlı içeriğin kalması) gibi sorunlar hem ifade özgürlüğü hem kullanıcı güvenliği yönünden yüksek risk taşımaktadır. Yapay zekâ tabanlı içerik moderasyonunda "**yanlış negatifler**" (**false negatives**), ile ifade edilmek istenen şudur; sistemin kuralları ihlal eden veya zararlı olan bir içeriği "zararsız" ya da "güvenli" olarak sınıflandırması durumudur. Bu hatalı sınıflandırma nedeniyle sistem bir tehdidi tespit ederek "zararsız" olarak etiketler. Bu örnek durumdan da anlaşılacağı üzere, algoritmalar tek başına yeterli olmayacaktır ve mutlaka "**insan denetçilere**" (**human-in-the-loop**) ihtiyaç duyulacaktır.

DSA, içerik kısıtlamalarında kullanıcılara gerekçe bildirimini (statement of reasons) verilmesini ve bu kararların daha sonra denetlenebilir olmasını öngörür; ayrıca moderasyon kararı süreçlerinde otomasyon kullanılıyorsa bunun bildirimlerde yer almasını şart koşmaktadır.

Üretken YZ kaynaklı riskler (dezenformasyon, sentetik içerik, sentetik etkileşim): Sentetik içerik üretimi, yanlış bilginin düşük maliyetle çoğaltılması, kimlik sahteciliği, görüntü kanıtı manipülasyonu ve seçim dönemlerinde algı operasyonları gibi riskleri artırmaktadır. AB YZ Yasası, sentetik içerik (deepfake) niteliğindeki görsel ve işitsel içeriklerde bunun yapay olarak üretildiğinin veya manipüle edildiğinin açıklanmasını; ayrıca sentetik içerik üreten sistem çıktılarının **makinelerce okunabilir bir formatta işaretlenmesini ve ayırt edilebilir şekilde etiketlenmesini** zorunlu kılmaktadır. r. Avrupa Konseyi Çerçeve Sözleşmesi de şeffaflık ve gözetim ilkesi kapsamında YZ tarafından üretilen içeriğin tanımlanmasına ilişkin önlemleri açıkça anımsatmaktadır.¹⁵²

Büyük ölçekli platformlarda sistemik risk ve yönetim açığı: Çok büyük platformlarda küçük bir parametre değişikliği dahi milyonlarca kullanıcıya, yerel dillere ve hassas topluluklara farklı etkilerle yansiyabilir. DSA, bu yüzden yıllık risk değerlendirmesi ve kritik etki doğurması muhtemel yeni işlevler devreye alınmadan önce risk değerlendirmesi yapılmasını zorunlu tutmaktadır. Buna karşılık risk azaltımında algoritmik sistemlerin test edilmesi ve uyarlanması gibi önlemler saymaktadır.

¹⁵² Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (2024). <https://rm.coe.int/1680afae3c>

Pazar gücü, algoritmik kapı bekçiliği (guardrails) ve kendini kayırma: Pazaryeri (marketplace), arama ve sıralama altyapıları, doğrudan ekonomi politığının merkezidir:

- Satıcı görünürlüğü,
- Komisyon gelirleri,
- Reklam ile organik görünürlük etkileşimi
- Platformun kendi ürünlerini kayırması gibi pratikler algoritmik kapı bekçiliği tartışmalarını doğurmaktadır.

AB dijital rekabet mimarisi, “geçit bekçisi” platformların kendini kayırma gibi davranışlarına müdahale edebilecek araçlar geliştirmiştir.¹⁵³ Bu risk, yalnızca rekabet hukuku meselesi olmaktan ziyade şeffaflık, denetlenebilirlik, gerekçelendirme ekseninde platform yönetişimi meselesidir.

5.4. Yönetişim Boyutları ve Uluslararası Çerçeveler

Platformlarda YZ yönetişimi çoklu bir normatif ekosisteme oturtulmaktadır. Bu sistemde hukuk (yasalar), insan hakları sözleşmeleri, standartlar, risk yönetimi çerçeveleri ve sektörel uygulamalar birlikte çalışmaktadır. Bu bölümde, platform yönetişimi perspektifi ile en kritik kesişim noktaları aşağıda sentezlenmektedir.

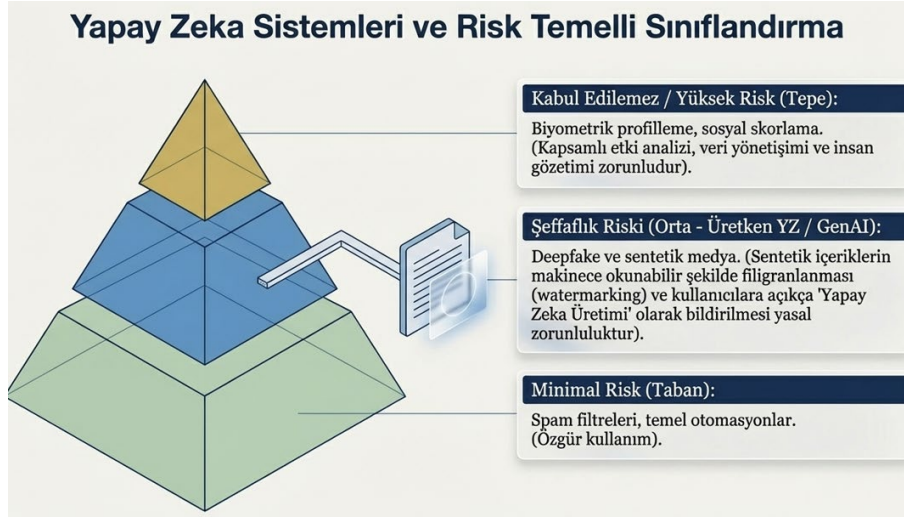
Risk-temelli yaklaşım ve sınıflandırma: AB YZ Yasası, yüksek riskli sistemlerde yaşam döngüsü boyunca risk yönetim sistemi kurulmasını, bunun sürekli ve iteratif bir süreç olarak işletilmesini öngörmektedir. Avrupa Konseyi Çerçeve Sözleşmesi de risk ve etki yönetimi çerçevesinin riskin şiddeti ve olasılığıyla orantılı biçimde kademelendirilmesini istemektedir. Bu iki yaklaşım, platformlarda her algoritmaya aynı yükümlülük yerine, kullanım bağlamına göre farklılaşan yükümlülük tasarımı desteklemektedir.

Şeffaflık yükümlülükleri ve kullanıcıya anlamlı bilgi: DSA, öneri sistemlerinin ana parametrelerinin ve kullanıcıların bunları etkileme seçeneklerinin şartlarda açıkça belirtilmesini istemektedir. AB YZ Yasasında ise

- 1) Kullanıcı ile doğrudan etkileşen sistemlerde “insanların bir YZ sistemiyle etkileştiğinin” bildirilmesini,
- 2) Sentetik içerik çıktılarının işaretlenmesini ve
- 3) Sentetik içerikte (deepfake) açık etiketlemeyi düzenlemektedir.

¹⁵³ DMA. https://digital-markets-act.ec.europa.eu/index_en.

GDPR ise otomatik karar verme ve profil çıkarmaya ilişkin olarak “mantık hakkında anlamlı bilgi, önem ve öngörülen sonuçlar” gibi bilgilendirme öğelerini veri koruma perspektifinden çerçevelemektedir.



ŞEKİL 5-1: YZ Sistemleri ve Risk Temelli Sınıflandırma (YZ ile hazırlanmıştır)

Denetlenebilirlik, dokümantasyon ve iz kayıtları: AB YZ Yasası, yüksek riskli sistemlerde veri yönetimi, test ve performans metrikleri, insan gözetimi ve yaşam döngüsü boyunca dayanıklılık ve siber güvenlik gerekliliklerini düzenler; ayrıca piyasaya arz sonrası izleme planı ve ciddi olay bildirimi gibi operasyon sonrası hesap verebilirlik araçları getirmektedir. DSA ise VLOP ve VLOSE’lar için bağımsız denetim ve risk değerlendirmesi sonuçları ile risk azaltım önlemleri ve denetim raporlarıyla birlikte belirli sürelerde yayımlanmasını öngörmektedir.

İnsan gözetimi ve hesap verebilirlik zinciri: AB YZ Yasası, yüksek riskli sistemlerin insanlar tarafından etkin biçimde gözetlenebilir tasarlanmasını, çıktıyı geçersiz kılma, geri alma, durdurma gibi insan kontrol mekanizmalarının ve gözetimin risk düzeyiyle orantılı olmasını düzenlemektedir. GDPR, otomatik karar verme bağlamında insan müdahalesi ve karara itiraz gibi asgari güvenceleri vurgulamaktadır. DSA ise VLOP ve VLOSE’larda yönetim organının sistemik risk yönetimi stratejilerinden sorumlu olmasını ve uyum fonksiyonunun bağımsızlığını kurumsal yönetişimin parçası hâline getirmektedir.

Etki değerlendirmeleri, araştırmacı erişimi ve kamusal denetim: DSA, sistemik riskleri anlamak ve azaltım önlemlerini değerlendirmek amacıyla yetkili otoritelerin algoritmik sistemlerin tasarımı, mantığı, işleyişi ve testleri hakkında açıklama istemesine ve “vetted researchers”¹⁵⁴ için veri erişimi mekanizmalarına yer vermektedir. Ayrıca Avrupa Komisyonu tarafından işletilen DSA Şeffaflık

¹⁵⁴ “Vetted researchers”, belirli kriterler doğrultusunda ön incelemeden geçirilmiş, uygunluğu doğrulanmış ve yetkilendirilmiş araştırmacılar anlamına gelir. Türkçe olarak “Yetkilendirilmiş araştırmacılar” tanımı kullanılabilir.

Veritabanı, içerik moderasyonu kararlarına ilişkin gerekçe bildirimlerini makine-okunur biçimde kamuya açarak denetim ve araştırma kapasitesini artırmayı amaçlamaktadır.

Küresel normlar ve standartlar: OECD YZ İlkeleri, insan hakları ve demokratik değerler, şeffaflık ve açıklanabilirlik, sağlamlık, güvenlik ve hesap verebilirlik gibi temel başlıklarda politika yapıcılara ve YZ aktörlerine esnek bir ortak dil sağlamakta olup 2019’da kabul edildi ve 2024’te güncellendiği OECD tarafından vurgulanmaktadır.¹⁵⁵ UNESCO, 2021’de kabul edilen “YZ Etiği Tavsiye Kararı”nı küresel bir standart olarak konumlandırır; insan hakları, şeffaflık, adalet ve insan gözetimi gibi ilkeleri politika eylem alanlarıyla ilişkilendirir.¹⁵⁶ YZ uygulamalarının kurumsal düzeyde yönetimi için ise ISO/IEC 42001 standardı, YZ yönetim sistemi (AIMS) yaklaşımıyla “politikalar–süreçler–sürekli iyileştirme” ekseninde bir çerçeve sunar.¹⁵⁷

5.5. Kurumsal ve Örgütsel Sorumluluklar

Platform işletmecilerinin sorumlulukları (operatör perspektifi): DSA, özellikle VLOP ve VLOSE’lar için sistemik risk yönetimini şirket içi yönetişimin kalbine yerleştirir: risk değerlendirmesi (yıllık ve kritik yeni işlevlerden önce), risk azaltım önlemleri (algoritmik sistemlerin test edilmesi/uyarlanması dâhil), bağımsız denetim ve bu çıktılarla ilgili kamuya açık raporlama. AB YZ Yasası ise platformu;

- a) Yüksek riskli sistemlerde sağlayıcı veya kullanan ve uygulayıcı (deployer) olarak,
- b) Üretken sistemler nedeniyle sentetik içerik/derin sahte şeffaflığı açısından veya
- c) Genel amaçlı YZ modellerinin ekosistem etkileri bakımından yükümlülük

altına alabilir.

Kurumsal sorumluluk yalnızca yönetim organlarının politika benimsemesiyle sınırlı değildir; moderasyon ekiplerinin kapasitesi, dilsel ve kültürel uzmanlık, itiraz süreçlerinin erişilebilirliği ve insan incelemesinin gerçekten etkili olup olmadığı da bu sorumluluğun parçasıdır. Aksi halde insan gözetimi kâğıt üzerinde var olup uygulamada etkisiz kalabilir.

Düzenleyicilerin rolü (çok otoriteli denetim): Platform YZ sistemleri, tek bir düzenleyici kurumun tam sahibi olamayacak kadar çok boyutludur: içerik ve çocuk koruma, veri koruma, tüketici korunması, rekabet ve siber güvenlik gibi alanlar birlikte çalışmalıdır.

¹⁵⁵ OECD, AI Principles. <https://www.oecd.org/en/topics/sub-issues/ai-principles.html>.

¹⁵⁶ UNESCO, Ethics of Artificial Intelligence, (2021). <https://www.unesco.org/en/artificial-intelligence/recommendation-ethics>.

¹⁵⁷ ISO/IEC 42001:2023. <https://www.iso.org/standard/42001>.

DSA düzeninde Dijital Hizmetler Koordinatörleri ve Komisyon, algoritmik sistem açıklaması isteme ve araştırmacı erişimi gibi araçlarla denetime kapasite kazandırmaktadır. AB YZ Yasası kapsamında ise AB düzeyinde kurumsal kapasiteyi güçlendirmek için YZ Ofisi (AI Office) kurumsallaştırılmıştır.¹⁵⁸

Bağımsız denetçiler ve uygunluk değerlendirmesi ekosistemi: DSA, VLOP ve VLOSE'lar için yıllık bağımsız denetim öngörür ve denetimin etkin yürütülmesi için denetçilere ilgili verilere erişim ve iş birliği yükümlülükleri getirmektedir. AB YZ Yasası ise uygunluk değerlendirmesi, teknik dokümantasyon ve piyasaya arz sonrası izleme gibi mekanizmalarla yüksek riskli sistemlerde denetim ve uygunluk altyapısını ayrıntılandırır.

Sivil toplum ve akademinin rolü (kamusal yarar denetimi): Kurumsal şeffaflık, tek başına toplumsal hesap verebilirliğe dönüşmez; sivil toplumun, araştırmacıların ve gazeteciliğin denetim kapasitesiyle birleşmesi gerekir. DSA Şeffaflık Veritabanı'nın kamuya açık ve makine-okunur tasarımı, bu denetim kapasitesini güçlendirmeyi hedeflemektedir.¹⁵⁹ Avrupa Konseyi Çerçeve Sözleşmesi de çok paydaşlı iş birliği ve izleme mekanizmaları dahil olmak üzere “uygulamanın izlenmesi” yaklaşımını kurumsal bir süreç olarak tarif eder.¹⁶⁰

5.6. Politika ve Düzenleme Değerlendirmeleri

Politika tasarımında temel mesele, platformların yalnızca bilgi veren olmaktan ziyade, açıklama yapabilen, denetlenebilen ve sonuçlarından sorumlu tutulabilen aktörlere dönüştürülmesidir. Bu nedenle düzenleyici yaklaşım, genel etik ilkelerden çok ölçülebilir yükümlülükler, kayıt tutma, bağımsız denetim, kullanıcı başvuru yolları ve araştırmacı erişimi gibi uygulanabilir araçlara dayanmalıdır.

Bu bölüm, platformlardaki YZ ve algoritmik sistemlerin yönetişimi için uygulanabilir, orantılı ve denetlenebilir politika seçeneklerini (özellikle düzenleyici tasarımın çatışma alanlarını görünür kılarak) çerçevelerdir.

Orantılılık: Sistemik platformlar ile KOBİ'ler arasında yükümlülük tasarımı
DSA, bazı yükümlülükleri tüm platformlara yayarken, sistemik risk yönetimi ve bağımsız denetim gibi ağır ödevleri çok büyük aktörlere (kullanıcı eşiği ve atama mekanizması) bağlamaktadır. Avrupa Konseyi Çerçeve Sözleşmesi de önlemlerin riskin şiddetine ve olasılığına göre kademeli ve farklılaştırılmış olmasını

¹⁵⁸ Commission Decision Establishing the European AI Office, (2024). <https://digital-strategy.ec.europa.eu/en/library/commission-decision-establishing-european-ai-office>.

¹⁵⁹ DSA Transparency Database : Questions and Answers, (2025). <https://digital-strategy.ec.europa.eu/en/faqs/dsa-transparency-database-questions-and-answers>

¹⁶⁰ Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (2024). <https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence>.

istemektedir. Bu yaklaşım, ulusal politika tasarımı “aynı rapor formatı ve aynı denetim yükü” yerine ölçek, risk profili ve iş modeline göre farklılaştırılmış şeffaflık ve denetim yükümlülüklerini meşrulaştırır.

Şeffaflığın niteliği: Anlaşılabilir parametreler ve Denetlenebilir deliller: P2B ve DSA birlikte okunduğunda, beklenen şeffaflık algoritma kodunu açmaktan ziyade sıralama, öneri ve hedefleme kararlarına yön veren ana parametrelerin ve göreceli önemlerin anlaşılır biçimde açıklanmasıdır. Kapsamlı denetim için ise yalnızca anlatı metni değil, test sonuçları, performans ve adalet metrikleri, loglar ve değişiklik kayıtları gibi kanıt katmanını gerekir. ABYZ Yasası risk yönetimi, veri yönetimi (önyargı tespit ve azaltım), insan gözetimi ve piyasaya arz sonrası izleme yaklaşımı bu kanıt katmanını kurumsallaştırır. Bu nedenle şeffaflık, salt bilgi ifşası olarak değil, bağımsız incelemeyi, karşılaştırmayı ve itirazı mümkün kılan bir hesap verebilirlik altyapısı olarak tasarlanmalıdır. Aksi halde şeffaflık kurumsal iletişim pratiğine indirgenebilir.

Etki değerlendirmesi araçları: Kâğıt üzerinde değil Operasyonel Etki değerlendirmeleri:

- 1) Yalnızca bir defalık uygunluk belgesi değil,
- 2) Ürün güncellemeleri ve politika değişiklikleriyle birlikte yinelenen bir süreç olmalıdır.

DSA yıllık risk değerlendirmesi ve kritik yeni işlevlerden önce deseni bu yönde kurmaktadır. Kamu sektöründe risk temelli değerlendirmeye örnek olarak Kanada’nın Algoritmik Etki Değerlendirmesi (Algorithmic Impact Assessment - AIA) aracı, risk soruları ve azaltım sorularıyla etki seviyesini belirleyen bir yöntem sunar ve yayınlama/yenileme disiplini tarif eder.¹⁶¹ Bu tür araçlar, platform düzenlemesi için de yapısal şablon olarak değerlendirilebilir (örneğin: risk kayıtları, paydaş danışmaları, şikâyet ve itiraz tasarımı).

Bağımsız denetim ve denetçi bağımsızlığı DSA, bağımsız denetimi zorunlu kılar; denetimin etkili olması için denetçilerin veri erişimi ve işbirliği güvencesine ihtiyaç olduğunu açıkça belirtir. Politika tasarımı kritik soru, “denetçi kimdir?” sorusudur: denetçi bağımsızlığı, çıkar çatışması yönetimi ve denetim metodolojisinin asgari standartları belirlenmezse denetim sembolleşebilir. Bu noktada ISO/IEC 42001 gibi yönetim sistemi standartları kurum içi yönetim için tamamlayıcı bir çerçeve sunabilir.

Araştırmacı erişimi, veri koruma ve ticari sır dengesi DSA, araştırmacı erişimini sistemik riskleri anlamaya bağlayarak tasarlar; ayrıca otoritelerin denetim amaçlı veri kullanımını kişisel veri koruma ve ticari sır gibi menfaatleri gözeterek sınırlandırır. P2B aynı gerilimi algoritma ifşası zorunlu değildir; ancak ana parametrelerin açıklanması reddedilemez çizgisiyle ele alınır. Bu denge, hem düzenleyici hem sivil toplum için “erişim mi, ifşa mı?” ayrımını netleştirir: amaç kodu ele geçirmek değil, sonuçları ve sistem tasarım tercihlerini değerlendirebilmektir.

¹⁶¹ Treasury Board of Canada Secretariat, Algorithmic Impact Assessment Tool, (2026).

<https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/algorithmic-impact-assessment.html>.

5.7. İyi Uygulama Örnekleri ve Öneriler

Uluslararası deneyimler algoritmik şeffaflık söyleminin tek bir araca indirgenmemesi gerektiğini göstermektedir. Şeffaflık raporları, kullanıcı kontrolleri, bağımsız denetim, araştırmacı erişimi ve gerekçelendirme mekanizmaları birlikte kurgulandığında anlamlı sonuç üretiyor. Bununla birlikte, iyi uygulama örnekleri tek başına ideal modeller olarak değil gerek ilerleme gerekse sınırlılık barındıran deneyimler olarak okunmalıdır. Bir platformun açıklama sunması, o açıklamanın yeterli, doğrulanabilir veya etki yaratıcı olduğu anlamına gelmez.

İyi uygulama örnekleri:

- **DSA Şeffaflık Veritabanı, kamuya açık moderasyon gerekçeleri:** Avrupa Komisyonu, DSA kapsamındaki gerekçe bildirimlerini makine-okunur bir veritabanında toplayarak içerik moderasyonu kararlarının denetlenmesini kolaylaştırmayı hedefliyor. Veritabanının kamuya açık olması ve veri indirme ve şema dokümantasyonu gibi unsurlar, sivil toplum ve akademi için pratik bir gözetim altyapısı oluşturuyor.
- **Algoritma açık kaynaklaşması, topluluk temelli inceleme kapasitesi:** X (Twitter), öneri algoritmasına ilişkin kaynak kod depoları üzerinden (GitHub) sistemin nasıl çalıştığına ilişkin görünürlük sağlamayı hedefleyen bir model sunmuştur. Bu yaklaşım, şeffaflık alanında radikal bir yöntem olmakla birlikte, kodun güncelliği, kapsamı ve yorumlanabilirliği gibi yeni tartışma başlıkları da doğurur.¹⁶²
- **Şeffaflık raporları ve politika uygulama metrikleri:** Meta periyodik “Community Standards Enforcement” raporlarıyla moderasyon uygulamalarına ilişkin ölçümler yayımlar. Bu raporlar, politika alanlarının uygulanmasına dair en azından nicel bir görünürlük (kaldırma oranları, proaktif tespit vb.) sağlar; DSA’nın raporlama mantığıyla da uyumludur.¹⁶³
- **Öneri sistemi açıklamaları ve kullanıcı kontrolü anlatıları:** YouTube, öneri sisteminin genel mantığına ilişkin kamuya açık açıklamalar ve kullanıcıların önerileri yönetmesine ilişkin bilgi sayfaları sunar. Bu tür açıklamalar DSA’daki “ana parametreleri anlaşılır biçimde açıklama” yaklaşımıyla benzer bir kullanıcı odaklı şeffaflık pratiğidir.¹⁶⁴
- **Platform destek sayfaları ve öneri mantığının basitleştirilmiş anlatımı:** TikTok, önerilerin hangi etkileşim sinyallerine dayanabileceğine ilişkin kamuya açık rehberler yayımlar. Bu tür

¹⁶² Twitter/The-algorithm: Source Code for the X Recommendation Algorithm.” n.d. GitHub. <https://github.com/twitter/the-algorithm>.

¹⁶³ Community Standards Enforcement Reports | Transparency Center.” n.d. <https://transparency.meta.com/reports/community-standards-enforcement/>.

¹⁶⁴ Cristos Goodrow, On YouTube’s Recommendation System, (2025) Blog. Youtube (blog). <https://blog.youtube/inside-youtube/on-youtubes-recommendation-system/>.

içerikler, “kullanıcıya anlaşılır açıklama” açısından taban oluşturur; ancak bağımsız denetime elverişli kanıt katmanı (test sonuçları, risk azaltım verileri) ayrıca gereklidir.¹⁶⁵

- **Risk değerlendirme şablonları, zorunlu soru setleri:** Kanada’nın AIA aracı, etki düzeyleriyle bağlantılı zorunlu azaltım önlemleri ve güncelleme disiplini (periyodik gözden geçirme) tarif eden bir yaklaşım sunar. Platform bağlamına uyarlanırken “temel haklar, ayrımcılık, çocukların korunması, güvenlik, şeffaflık ve başvuru yolları” gibi alanlar için benzer soru setleri geliştirilebilir.¹⁶⁶

5.8. Öncelikli öneriler

- 1) **Ortak kavram seti ve asgari şeffaflık standardı geliştirme:** Platform yönetişimi açısından temel kavramların farklı aktörler tarafından farklı şekillerde yorumlanması hem düzenleyici uygulamalarda hem de denetim süreçlerinde belirsizlik yaratmaktadır. Bu nedenle “algoritmik sistem”, “öneri sistemi”, “sıralama”, “profil çıkarma” ve “sentetik içerik” gibi terimler için kısa, anlaşılır ve uygulamaya dönük bir sözlük oluşturulması kritik önem taşımaktadır. Ancak bu sözlük yalnızca tanımlayıcı bir araç olarak kalmamalıdır. Öte yandan DSA’nın öneri sistemi parametrelerine ilişkin şeffaflık yaklaşımı ve AB YZ Yasası’nın sentetik içerik ve bu içeriğin şeffaflığı yükümlülükleriyle uyumlu, standartlaştırılmış bir açıklama ve dokümantasyon çerçevesine dönüşmelidir. Bu kapsamda platformlardan kullandıkları algoritmik sistemlere ilişkin temel parametreleri, karar mantığını ve etki alanlarını belirli bir formatta ve karşılaştırılabilir şekilde açıklamaları talep edilmelidir. Böyle bir yaklaşım, kullanıcıya yönelik şeffaflığın yanı sıra düzenleyici kurumlar ve bağımsız denetçiler için karşılaştırılabilir ve doğrulanabilir bir bilgi katmanı oluşturacaktır.
- 2) **“Sistem envanteri + risk kaydı” yaklaşımını savunuculuk gündemine almak:** Platformlardan;
 - a) Hangi algoritmik sistemleri hangi amaçla kullandıklarını,
 - b) Bu sistemlerin hangi risklere temas ettiğini,
 - c) Hangi test ve izleme metrikleriyle yönetildiğini gösteren bir envanter ve risk kaydı talep edilmeli.

Bu talep, AB YZ Yasası risk yönetimi ve post-market izleme mantığı ile DSA’nın sistemik risk değerlendirmesi mantığını birleştiren bir “asgari kurumsal sorumluluk” standardı olarak çerçelenebilir.

- 3) **Bağımsız denetim kapasitesi için metodoloji ve asgari kriterler:** DSA’nın bağımsız denetim yaklaşımı, yalnızca denetimin zorunlu kılınmasının yanında “neyin, nasıl ve hangi kanıtlarla denetleneceği” sorusunun netleştirilmesini gerektirir. Bu kapsamda, denetim sürecinin kapsamı

¹⁶⁵ **How TikTok Recommends Content.** n.d. <https://support.tiktok.com/en/using-tiktok/exploring-videos/how-tiktok-recommends-content>.

¹⁶⁶ **Treasury Board of Canada Secretariat, Algorithmic Impact Assessment Tool, (2026).** <https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/algorithmic-impact-assessment.html>.

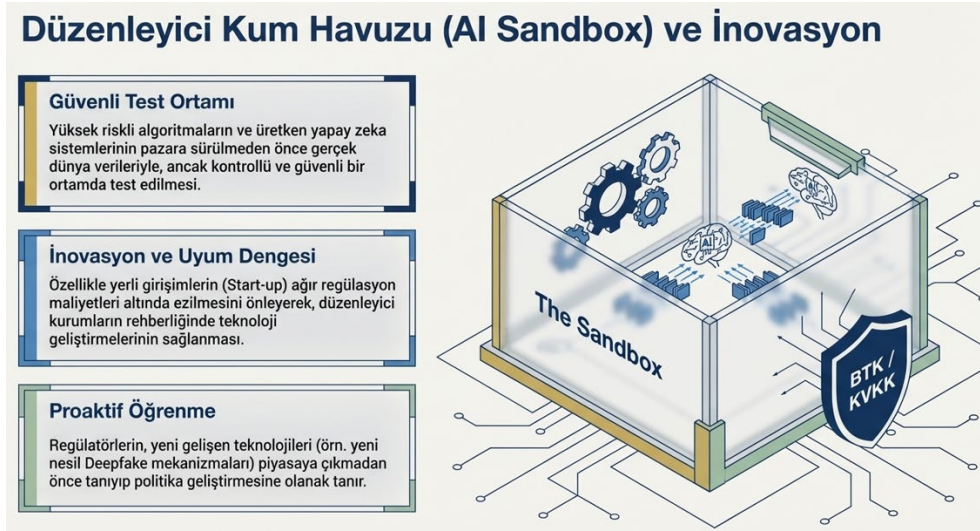
(öneri sistemleri, reklam sistemleri ve içerik moderasyonu dahil), veri erişim koşulları, çıkar çatışması yönetimi ve raporlama formatı gibi alanlarda asgari kriterlerin tanımlanması kritik önem taşımaktadır. Bununla birlikte, denetimin yalnızca politika ve süreç belgeleri üzerinden değil, test sonuçları, performans ve adalet metrikleri, model davranış analizleri ve sistem logları gibi kanıta dayalı bir değerlendirme katmanı üzerinden yürütülmesi gerekmektedir. Bu doğrultuda, bağımsız denetim mekanizmalarının etkinliğini sağlamak için hem denetçi bağımsızlığını güvence altına alan kurumsal düzenlemeler hem de denetim metodolojilerinin belirli standartlara (örneğin ISO/IEC 42001 gibi yönetim sistemi yaklaşımlarıyla uyumlu şekilde) yapılandırılması gereklidir. Bu yaklaşım, denetimin sembolik bir uygulama olmaktan çıkıp ölçülebilir ve karşılaştırılabilir bir güven mekanizmasına dönüşmesini sağlar.

- 4) **Kullanıcıyı güçlendirme odaklı politika paketi:** Platformlarda kullanıcıların algoritmik sistemler üzerindeki etkisinin sınırlı olması, şeffaflık ve hesap verebilirlik mekanizmalarının etkinliğini doğrudan zayıflatmaktadır. Bu nedenle kullanıcı güçlendirme, tekil araçlardan ziyade bütüncül bir politika paketi olarak ele alınmalıdır. Bu kapsamda, öneri sistemleri için “neden bu içeriği görüyorum?” sorusuna anlamlı yanıtlar sunan açıklama mekanizmaları, profil çıkarmaya dayanmayan alternatif akış seçenekleri, reklam hedefleme parametrelerine ilişkin şeffaflık ve kullanıcıların bu parametreleri yönetebilmesine yönelik araçlar ile etkili itiraz ve başvuru yolları birlikte tasarlanmalıdır. Bununla birlikte, bu mekanizmaların yalnızca sunulması değil, kullanım oranları, kullanıcı tercihleri ve itiraz süreçlerinin sonuçları gibi göstergeler üzerinden ölçülmesi ve izlenmesi gerekmektedir. Bu yaklaşım, DSA’daki öneri sistemi şeffaflığı ve reklam parametrelerine ilişkin yükümlülüklerle uyumlu olmakla birlikte, kullanıcıların platform üzerindeki karar süreçlerine daha etkin biçimde katılımını sağlayan ölçülebilir bir güçlendirme çerçevesi sunar.
- 5) **Sentetik içerik ve sentetik içerik (deepfake) için işaretleme, bağlam ve erişilebilirlik üçlüsü:** AB YZ Yasası kapsamında öngörülen işaretleme ve sentetik içerik (deepfake) açıklama yükümlülükleri, platform düzeyinde yalnızca görünür etiketleme ile sınırlı kalmamalıdır. Aynı zamanda içerik üretiminde kullanılan veri kümelerinin niteliği, kaynağı ve üretim süreçlerine ilişkin standartlaştırılmış bir çerçeve ile desteklenmelidir. Bu bağlamda, sentetik içeriklerin sadece işaretlenmesinin ötesinde, hangi veri kümelerinin ve hangi yöntemlerle üretildiğinin izlenebilir olması kritik önem taşır. Algoritmik çıktılarda kullanılan veri kümeleri için veri hacmi, temsil gücü, sentetik ve gerçek veri oranı ile güncellik gibi unsurları kapsayan asgari kalite göstergeleri tanımlanmalıdır. Kullanıcıya sunulan içeriklerde ise üretim süreci, veri kaynağına ilişkin özet bilgi ve güvenilirlik sinyallerini içeren bağlamsal açıklamalar sağlanmalıdır. Bu yaklaşım, örneğin aynı kullanıcı puanına sahip ancak veri yoğunluğu ve güvenilirliği farklı olan içeriklerin eşdeğer algılanmasının önüne geçerek daha doğru bir bilgi ekosisteminin oluşturulmasına katkı sağlamaktadır. Ayrıca, bu veri kümelerinin belirli standartlara göre test edilmesi, versiyonlanması ve bağımsız denetime açık olması sağlanmalıdır. Ulusal veya sektörel düzeyde referans veri kümeleri, test ve doğrulama mekanizmaları ile YZ sistemleri için veri temelli sertifikasyon veya olgunluk göstergeleri geliştirilmelidir. Bu tür bir yaklaşım, sentetik içerik yönetişimini yalnızca şeffaflık düzeyinde değil, ölçülebilir ve denetlenebilir bir yapı haline getirecektir.
- 6) **Araştırmacı erişimi ve sivil toplum izlemesi için güvenli yollar:** Platformlarda algoritmik sistemlerin toplumsal etkilerinin bağımsız biçimde incelenebilmesi, yalnızca kurumsal şeffaflık

mekanizmalarının yanı sıra araştırmacı ve sivil toplum aktörlerine sağlanan güvenli veri erişim kanallarıyla mümkün olmaktadır. Bu nedenle DSA'nın "vetted researcher" veri erişimi yaklaşımına benzer mekanizmaların mahremiyet ve güvenlik kalkanlarıyla birlikte yerel bağlamda da geliştirilmesi ve savunulması kritik önem taşımaktadır. Ancak bu erişim yalnızca veri paylaşımıyla sınırlı kalmamalıdır. Anonimleştirilmiş ve farklı kaynaklardan gelen veri kümeleri, kontrollü API erişimi ve kamuya açık veri kaynakları üzerinden çok katmanlı bir erişim modeli oluşturulmalıdır. Bu kapsamda, veri erişim süreçlerinin kimler tarafından, hangi amaçla ve hangi kapsamda kullanıldığını izleyen erişim kayıtları (access logs), sorgu bazlı denetim mekanizmaları ve mahremiyeti koruyan veri işleme teknikleri (örneğin anonimleştirme ve diğer mahremiyet koruyucu (privacy-preserving) yöntemler ile desteklenmesi gerekmektedir. Ayrıca, bu mekanizmaların etkinliği, veri erişim taleplerinin sayısı, kullanım alanları, araştırma çıktıları ve politika etkileri gibi göstergeler üzerinden düzenli olarak izlenmeli ve raporlanmalıdır. Bu tür bir yaklaşım, algoritmik sistemlerin dışsal denetimini mümkün kılarak platform yönetiminde sürekli ve kanıta dayalı bir kamusal gözetim katmanı oluşturur.

- 7) **Kurumsal yönetim kapasitesini ölçen gösterge seti:** Platformların YZ sistemlerini ne ölçüde sorumlu, güvenli ve hesap verebilir biçimde yönettiğinin değerlendirilmesi, politika beyanlarının ötesinde ölçülebilir kurumsal kapasite göstergeleriyle mümkün olmaktadır. Bu doğrultuda, NIST AI RMF'in yönetim ve risk yönetimi fonksiyonları (GOVERN, MAP, MEASURE, MANAGE) temel alınarak platformların "kurumsal olgunluk" düzeyini ortaya koyan bütüncül bir gösterge seti geliştirilmesi önerilmektedir. Ancak bu gösterge seti yalnızca kavramsal bir çerçeve olarak kalmamalıdır. Liderlik sorumluluğu, organizasyonel yapı, dokümantasyon kalitesi, test ve doğrulama izleri, olay (incident) yönetimi süreçleri ve paydaş katılım mekanizmaları gibi alanlarda somut ve ölçülebilir kriterler içermelidir. Bu kapsamda, platformların belirli periyotlarla kendi değerlendirmelerini yapmaları, bu değerlendirmelerin bağımsız denetim süreçleriyle doğrulanması ve sonuçların karşılaştırılabilir bir formatta raporlanması sağlanmalıdır. Ayrıca, bu göstergeler üzerinden oluşturulacak bir olgunluk skorlama ve benchmarking yaklaşımı, platformlar arasında karşılaştırılabilirlik sağlayarak hem düzenleyiciler hem de kamuoyu için anlamlı bir değerlendirme zemini sunacaktır. Bu tür bir yapı, YZ yönetişimini statik bir uyum süreci olmaktan çıkararak sürekli iyileşmeye dayalı, ölçülebilir ve izlenebilir bir kurumsal kapasite modeli haline getirecektir.
- 8) **AB YZ Düzenleyici Kum Havuzu (EU AI Regulatory Sandbox) yaklaşımının uygulanabilir ve sürdürülebilir bir çerçeveye dönüştürülmesi:** AB YZ Yasası kapsamında tanımlanan düzenleyici kum havuzu (regulatory sandbox) mekanizması, YZ sistemlerinin gerçek dünya koşullarına yakın ancak kontrollü ortamlarda test edilmesini sağlayarak yenilikçiliği ile düzenleyici uyum arasında denge kurmayı amaçlamaktadır. Ancak bu mekanizmanın farklı ülke bağamlarına uyarlanması, yasal bir çerçevenin benimsenmesinin yanında uygulanabilir ve sürdürülebilir bir operasyonel modelin tasarlanmasıyla mümkündür. Bu kapsamda, kum havuzlarının test ortamı sunan yapılar olmalarının ötesinde, veri erişimi, teknik doğrulama, risk değerlendirmesi ve regülasyon rehberliğini entegre eden çok paydaşlı bir ekosistem olarak kurgulanması gerekmektedir. Özellikle erken aşama girişimler açısından veri erişimi, veri işleme kapasitesi ve uyum maliyetleri önemli bir engel oluşturduğundan, bu yapıların girişimlerin bu kaynaklara kontrollü ve güvenli şekilde erişebileceği mekanizmalar içermesi kritik önem taşır.

Bu doğrultuda, kum havuzlarının test süreçlerinin kapsamı, risk değerlendirme metodolojileri, veri erişim modelleri ve regülatör geri bildirim mekanizmaları gibi unsurlar açısından açık ve standartlaştırılmış bir çerçeveye sahip olması gerekmektedir. Ayrıca bu mekanizmaların etkinliği, katılımcı sayısı, test edilen sistemlerin türü, tespit edilen riskler, sağlanan uyum iyileştirmeleri ve piyasaya geçiş oranları gibi göstergeler üzerinden düzenli olarak izlenmeli ve değerlendirilmelidir. Bu tür bir yaklaşım, kum havuzlarını yalnızca düzenleyici bir araç olmaktan çıkarak, YZ sistemlerinin güvenli ve sorumlu biçimde geliştirilmesini destekleyen ölçülebilir ve sürdürülebilir bir yönetim altyapısı haline getirecektir.



ŞEKİL 5-2: Düzenleyici Kum Havuzu (YZ ile hazırlanmıştır)

BÖLÜM 6: SİBER GÜVENLİK VE SİBER (Operasyonel) DAYANIKLILIK

Bölümün Amacı: Dijital dünyada siber güvenlik sadece tehditlere karşı korunmak için "duvar örmek" değildir. Ana hedef, duvarların içindeki verinin dış etkenlerden bağımsız olarak proaktif bir "hizmet sürekliliği" ve "operasyonel dayanıklılık" işlevine dönüştürülmesidir. Türkiye'nin dijital egemenliğini, platform bütünlüğünü ve kamu yararını küresel regülasyonlar ve düzenlemeler ile (NIS2, DORA, CRA vb) uyumlu olacak şekilde güvence altına alınmasıdır.

İçerik ve Kapsam:

- Platform araçlarının kötüye kullanımı, manipülasyonu, veri ihlalleri ve sistem kesintilerine karşı önleyici, tespit edici ve toparlayıcı stratejiler.
- Geleneksel içerik moderasyonunun ötesinde, bot ağları ve "Koordine Yapay Davranışlar" (CIB) yoluyla bilgi manipülasyonu yapan güvenlik riskleri ile mücadele.
- AB-NIS2 Direktifi ile siber olayların bildirim süreçleri ve DORA (Dijital Operasyonel Dayanıklılık Yasası) kapsamında çoklu bölge (multi-region) mimarisi ile Afet Yönetimi (DR) standartları.
- Bulut jeopolitikler ekseninde, küresel bulut sağlayıcılarına (hyperscalers) olan bağımlılığın neden olduğu sistemik riskleri ve tedarik zinciri güvenliği.
- Siber Dirençlilik Yasası (CRA) standartlarına uygun olarak Türkiye'nin teknik test ve sertifikasyon altyapısının güçlendirilmesi.

Temel Kavramlar:

- Güvenlik ve Dayanıklılık (Security vs. Resilience)
- Koordine Yapay Davranışlar (CIB)
- Operasyonel Egemenlik
- Güvenilirlik Mühendisliği (Trust Engineering)
- Sistemik Çöküş (Systemic Collapse) ve Tek Nokta Zafiyeti

6.1. Giriş ve Amaç

Dijital dünyada siber güvenlik sadece tehditlere karşı korunmak için "duvar örme" değildir; esas olan bu duvarların içindeki yönetim algoritmalarının ve dinamiklerin dış etkenlerden bağımsız (egemen) olmasıdır.

Siber güvenlik artık sadece bir savunma değil, bir süreklilik kültürüdür. Modern literatürde güvenlik "sızmayı engellemek", dayanıklılık ise "darbe aldığında ayakta kalabilmek" olarak kabul edilmektedir.

Temel Doktrin: NIST SP 800-160 Vol. 2 Bu belgede tanımlar şu şekilde yer alır:¹⁶⁷

Güvenlik (Security): Tehditlerin içeri girmesini engellemeye (protection/prevention) odaklanır.

Dayanıklılık (Resilience): Sistemin bir saldırıya uğradığını veya sızmanın gerçekleştiğini varsayarak (adversarial posture), operasyonların devam etmesine ve hızla toparlanmaya odaklanır.

Dijital Platformlarda Egemenlik ve Siber Dayanıklılık

Günümüzde dijital ve çevrim içi platformlar, "teknik servis sağlayıcı" olmanın çok ötesine geçmiş olup, kamusal tartışmaların yapıldığı, ekonomik faaliyetlerin olduğu ve toplumsal verilerin işlendiği önemli bir **sosyo-teknik ekosistemler** haline dönüşmüştür.

Bu rapor, AB'nin (**DSA, NIS2, DORA**), Birleşik Krallık'ın (**OSA**) ve **OECD**'nin ilgili düzenlemelerini referans alarak, Türkiye'nin dijital egemenliğini korumak ve platform bütünlüğünü sağlamak adına stratejik bir yol haritası sunmayı hedeflemiştir. ^{168, 169, 170, 171}

Stratejik Hedefler

Siber güvenlik ve operasyonel dayanıklılık politikalarının temel hedefi; hizmet sürekliliğini garanti altına alarak bu sayede kamu yararını korumaktır. Bu kapsamda platformların sıralanan dört temel tehdide karşı **önleyici, tespit edici ve toparlayıcı** yetkinliklere sahip olması gerekmektedir:

- **Kötüye Kullanım:** Platform araçlarının etik dışı amaçlar için kullanımı.
- **Manipülasyon:** Dezenformasyon ile algı yönetimi faaliyetleri.
- **Siber Saldırıları:** Veri ihlalleri ile altyapılara karşı yapılan saldırılar.
- **Sistem Kesintileri:** Hizmet sürekliliğini bozan teknik arızalar ve aksaklıklar.

¹⁶⁷ Developing Cyber-Resilient Systems: A Systems Security Engineering Approach, (2021). <https://csrc.nist.gov/pubs/sp/800/160/v2/r1/final>

¹⁶⁸ DSA. https://www.eu-digital-services-act.com/Digital_Services_Act_Articles.html

¹⁶⁹ NIS2 Directive, (2022). <https://eur-lex.europa.eu/eli/dir/2022/2555/2022-12-27/eng>

¹⁷⁰ Digital Operational Resilience Act (Regulation (EU) 2022/2554). <https://www.digital-operational-resilience-act.com/>

¹⁷¹ Online Safety Act, (2023). <https://www.legislation.gov.uk/ukpga/2023/50>

Küresel düzenlemeler ile, dijital platformlar teknik yapılar olmaktan ziyade, kamusal etkisi büyük unsurlar olarak tanımlanmaktadır.

6.2. Koordine Yapay Davranışlar ve Platform Bütünlüğü

Koordine Yapay Davranışlar (Coordinated Inauthentic Behavior – CIB), münferit kullanıcı hatalarının dışında, bilgi ekosisteminin işleyişine yönelik yapısal ve bilinçli bir müdahale olarak tanımlanabilir. Wardle (2019)¹⁷² tarafından kavramsallaştırılan 'bilgi bozukluğu' çerçevesinde, bu tür faaliyetler bilgi küresinin (infosphere) bütünlüğünü bozan ekosistem kirliliği olarak kabul edilir. Floridi (2021)¹⁷³ ise bu durumu, dijital altyapıların kamu yararı ile olan uyumunu bozan **sistemik bir risk** olarak niteler. **OECD** ve **AB** düzenlemelerinde bu teknik tespitler desteklenmekte olup söz konusu manipülasyonların toplumsal etkileri, kurumsal güven ve piyasa istikrarı üzerindeki sistemik etkileri önemle vurgulanmaktadır.

Dijital platformlar bağlamında sistemik risk, bilgi ekosisteminin temel mekanizmalarının koordineli olarak dış etkenlerin yapay müdahaleleri ile (CIB) bozulmasıdır.

Güncel regülasyonlar, platformlardan yalnızca içerik denetimi değil, sistemik bir koruma yapısı oluşturmasını istemektedir şöyle ki:

- **Risk Değerlendirmesi:** Platform içi risklerin periyodik olarak raporlanması.
- **Algoritmik Denetim:** Yapay zekâ ve algoritmaların içeriği yayma (amplifikasyon) süreçlerinin şeffaflığı.
- **Şeffaflık:** Reklam ve siyasi içeriklerin kaynağının belirtilmesi.
- **Stratejik İş Birliği:** Manipülasyon ataklarına ve kampanyalarına karşı ortak savunma mekanizmaları oluşturulması.

Önemli Not: İngiltere-Birleşik Krallık (UK) Çevrim İçi Güvenlik Aktı (**Online Safety Act**), ile platformlara “makul önleyici tedbir alma” yükümlülüğü getirmiştir ve pasif kalmayı bir regülasyon ihlali olarak tanımlamaktadır.¹⁷⁴

Dijital platformlarda güvenliğin tesisi için, içeriklerin organize bir şekilde yayılmasını sağlayan kötü niyetli sistemlerin tespit edilmesi amacıyla savunma amaçlı sistemlerin geliştirilmesi hedeflenmiştir. Bu çerçevede iki temel yaklaşım yer almaktadır:

¹⁷² Wardle, C. (2019). *Information Disorder: Toward an interdisciplinary framework for research and policymaking*. First Draft News.

¹⁷³ Floridi, L. (2021). *The Ethics of Artificial Intelligence: Principles, Challenges, and Opportunities*. Oxford University Press.

¹⁷⁴ Online Safety Act, (2023). <https://www.legislation.gov.uk/ukpga/2023/50>

- **Bütüncül Yaklaşım:** Organize edilmiş biçimde finansal, toplumsal veya politik amaçlara hizmet eden manipülatif kampanyalar, "içeriğe bakılmaksızın bir güvenlik riski" olarak ele alınmalıdır.
- **Algoritmik Hesap Verilebilirlik:** Platformlar proaktif tespit mekanizmaları kurmalıdırlar, pasif kalmak bir "düzenleme ihlali" sayılmalı ve özellikle de algoritmik amplifikasyonun (etki artırma) denetimi sıkılaştırılmalıdır.

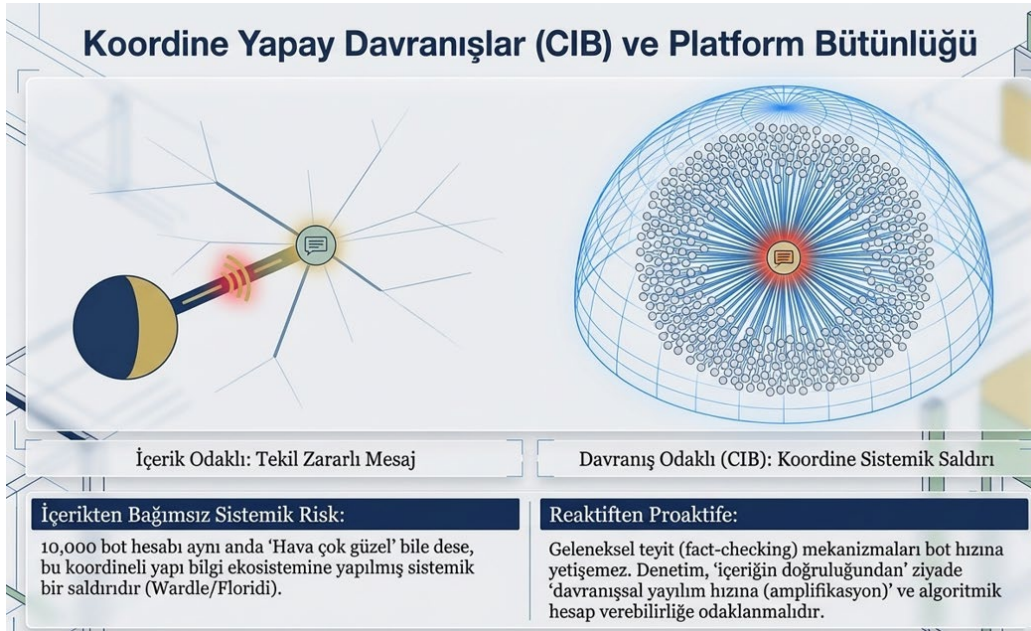
İçerikten Bağımsız Güvenlik Riski (Davranışsal Odak)

Geleneksel içerik denetimi manipülasyonun hızıyla yarışamaz. Bu nedenle Meta (Facebook), Twitter ve kamu otoriteleri " **Koordine Yapay Davranışlar**" (CIB) kavramını merkeze almıştır. (*"inauthentic behavior"*: gerçek olmayan davranış)

Meta'nın CIB tanımı, içeriğin doğru olup olmadığına bakmaksızın, grup halindeki kullanıcıların birbirleriyle koordineli şekilde hareket etmesini platform bütünlüğüne saldırı olarak değerlendirir.¹⁷⁵

Mesela, eğer 10.000 bot hesabı aynı anda "Hava çok güzel" derse bile, bu koordineli ve riskli bir eylemdir. İçerik zararsız görüne bile, böyle bir kolektif manipülasyon eylemi üzerinden platformun güvenilirliğine zarar gelebilir.

İçerik moderasyonu yöntemlerinin organize olarak kitlesel manipülasyonlar karşısındaki yetersizliği, "Koordine Yapay Davranışlar- (CIB)" olgusunu bir 'sistemik risk' ve 'altyapı güvenliği' meselesi olarak tanımlamayı zorunlu kılmıştır.



ŞEKİL 6-1: Koordine Yapay Davranışlar (YZ ile hazırlanmıştır)

¹⁷⁵ **Inauthentic Behaviour, Meta Reports, (2026).** <https://transparency.meta.com/policies/community-standards/inauthentic-behavior/>

Algoritmik Hesap Verilebilirlik ve Amplifikasyon

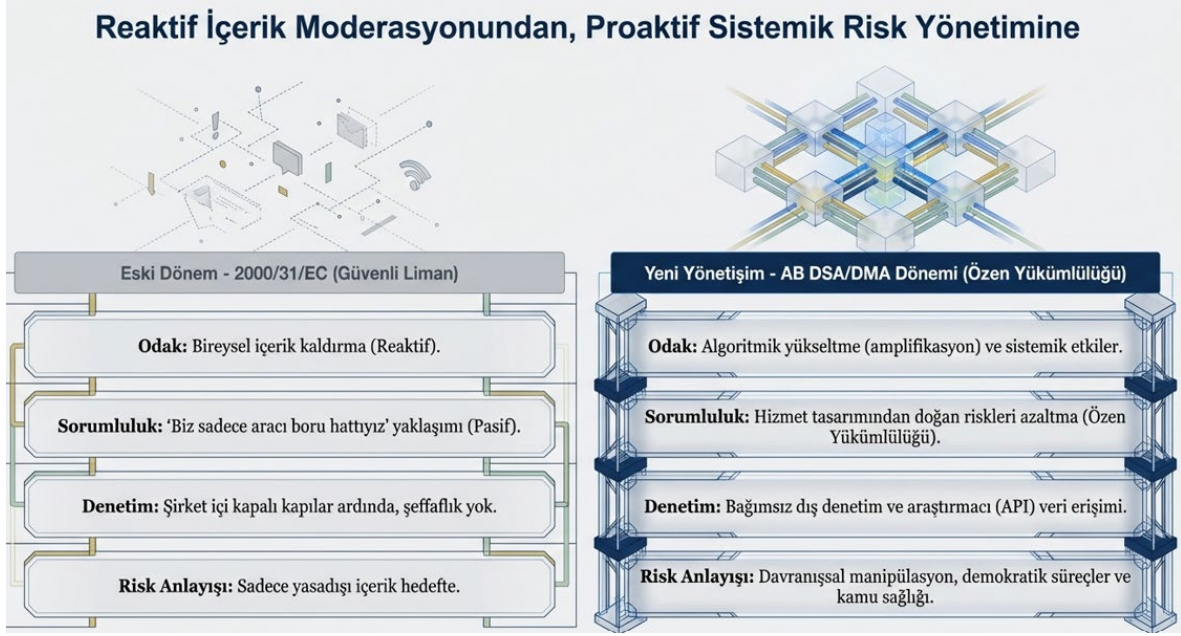
Platformlar artık sadece birer "kütüphane" (pasif içerik sağlayıcı) değildirler, bilakis etkileri büyük birer "editör" (algoritmik küratör) gibi ele alınmaktadır.

AB Dijital Hizmetler Yasası (DSA Madde 34 & 35): 2024 itibarıyla yürürlüğe giren bu yasa, çok büyük çevrim içi platformları (VLOPs) algoritmalarının yarattığı "sistemik risklerden" sorumlu tutar. Eğer bir algoritma radikal veya manipülatif içeriği öne çıkarıyorsa (amplifikasyon), bu platformun operasyonel bir hatası olarak kabul edilir.

Düzenleme İhlali: Pasif kalmak, yani "Biz sadece platformuz, kullanıcı ne yaparsa biz o içeriği sadece iletmekle sorumluyuz" argümanı geçerli bir savunma olarak kabul edilmez. Algoritmalar birer "amplifikatör" (yükseltici) olduğu için, bu durum denetim gerektiren ve doğrudan kamu güvenliğini ilgilendiren bir unsurdur.

Eski düzenlemelerde (2000 tarihli AB E-Ticaret Direktifi (2000/31/EC)), platformlar "*sadece bir boru hattıyız, içinden ne geçerse biz sorumlu değiliz*" diyebiliyordu. Ancak, **2022/2065 sayılı DSA (Dijital Hizmetler Yasası)** ile bu durum değişti:

- **Aktif Sorumluluk:** Eğer bir algoritma etkileşimi (engagement) artırmak için içeriği bilinçli olarak öne çıkarıyorsa, bu artık "tarafsız bir iletim" değil, bir **tasarım tercihi** sayılıyor.
- **Şeffaflık Zorunluluğu:** Platformlar, algoritmaların neden belirli bir içeriği kullanıcıya sunduğunu açıklamak ve kullanıcılara "kişiselleştirilmemiş" (profillemeye yapılmayan) alternatifler de sunmak zorundadırlar.



ŞEKİL 6-2: Reaktiften Proaktif Risk Yönetimine (YZ ile hazırlanmıştır)

6.3. Operasyonel (Siber) Dayanıklılık ve Olaylara Müdahale

Dijital platformların kesintisiz çalışması sadece bir kullanıcıyı etkileyen bir mesele olmayıp; doğrudan kamu güvenliğini, toplumsal ve ekonomik istikrarı etkileyebilecek kapsamda ele alınmalıdır. Bu nedenle, operasyonel dayanıklılık ve olaylara müdahale mekanizmaları ulusal ve uluslararası regülasyonların odağında yer almaktadır.

Siber Olay Bildirimi ve Şeffaflık (AB-NIS2 Uyum)

Siber olayların etkilerini minimize etmek ve ekosistemi korumak adına, AB-NIS2 (Network and Information Security: Ağ ve Bilgi Güvenliği) Direktifi ile uyumlu bir bildirim mekanizması esas alınmalıdır.¹⁷⁶

Bildirim Süreleri ve Süreç

Önemli siber olayların USOM (Ulusal Siber Olaylara Müdahale Merkezi) ve BTK'ye bildirilmesinde NIS2 Madde 23 te belirlendiği gibi bir standart raporlama takvimi belirlenmelidir; kuruluşların "önemli bir siber olayı" tespitinden sonraki 24 saat içinde bir "erken uyarı" ve 72 saat içinde bir "olay bildirimi" raporlaması yapmasını zorunlu kılar.

Kök Neden Analizi ve Şeffaflık

Büyük ölçekli kesintiler sonrasında kamuoyunun ve otoritelerin bilgilendirilmesi zorunlu hale getirilmelidir:

¹⁷⁶ NIS2 Directive, (2022). <https://eur-lex.europa.eu/eli/dir/2022/2555/2022-12-27/eng>

- **Kök neden analizi:** (Post Incident Review- PIR) kök neden analizini, edinilen deneyimleri, alınan dersleri ve gelecekteki benzer olayları önleyecek stratejileri ve karşı aksiyon adımlarını içeren raporların sunulması gerekir.
- **Şeffaf Bilgilendirme:** Kamusal sonuçlar doğuran vakalarda, belirlenen standartlarda kamuoyu açıklaması yapılması oldukça önemlidir.

6.3.1. Asgari Teknik Standartlar ve DORA Uyumu

Avrupa Birliğinin Finansal ve kritik sektörlerdeki dijital dayanıklılığı hedefleyen **DORA** (Digital Operational Resilience Act- Dijital Operasyonel Dayanıklılık Yasası) çerçevesindeki kriterler dijital ve çevrim içi platformlar için de geçerlidir. Zira, Çevrim içi platformlar da (BİT sağlayıcılar) kapsamında olup bu düzenlemenin doğrudan veya dolaylı bir unsurudur.

DORA Madde 28-30 (BİT Üçüncü Taraf Riskinin Yönetimi) maddeleri, finansal kuruluşların platform sağlayıcılarla yapacağı sözleşmelerde yer alması gereken asgari güvenlik ve teknik standartları açıkça tanımlar.¹⁷⁷



ŞEKİL 6-3: Siber Güvenlik Dayanıklılığı - NIS2 ve DORA (YZ ile hazırlanmıştır)

DORA uyumu kapsamında, sadece kurum içi sistemleri dikkate alarak planlama yapmak yeterli gelmez, zira hizmet alınan bulut sağlayıcılar ve yazılım tedarikçileri de güvenlik denetim zincirine dahil edilmelidir.

¹⁷⁷ DORA (Digital Operational Resilience Act - Regulation (EU) 2022/2554). <https://www.digital-operational-resilience-act.com/>

6.3.2. Yedeklilik ve Afet Yönetimi (DR)

Kritik altyapı sağlayıcıları için aşağıdaki standartlar asgari gerekliliktir:

- **Çoklu Bölge (Multi-region) Mimarisi:** Hizmetin tek bir veri merkezine bağımlı kalmaması için coğrafi yedeklilik yapılması.
- **Sürekli Test Edilen Afet Yönetimi (DR) Planları:** Felaket kurtarma senaryolarının kâğıt üzerinde kalmaması, düzenli stres testleri yapılarak ve kriz simülasyonu tatbikatları ile canlı tutulması gerekli olmakla birlikte, periyodik olarak yapılan testlerde tespit edilecek zayıf alanların düzeltilmesi elzemdir.

Bölgesel Kesintiler (AWS Örneği): 2021 yılında AWS'nin US-EAST-1 bölgesinde yaşanan kesinti, borsa platformlarından akıllı ev sistemlerine kadar binlerce servisi durdurdu. Sadece tek bölgede yedekli olan sistemler dahi devre dışı kaldı. **Bulut sağlayıcılarının bile bölge düzeyinde çökebildiği bir örnek vakadır olarak kayıtlara geçti.**¹⁷⁸

Bu vaka, verinin sadece ülke sınırları içinde tutulmasının (data residency) yeterli olmadığı durumların oluşabileceği ve operasyonel yedekliliğin bir 'ulusal egemenlik' unsuru olduğunu kanıtlamaktadır. Bu vaka ile platformların kritik işlevleri için dış kaynaklara olan 'bağımlılık haritasını' çıkartmasının stratejik gerekliliği anlaşılmaktadır.

Doğal Afetler ve Jeopolitik Riskler: Deprem, sel gibi doğal afetlerin yanında geniş çaplı enerji kesintileri ile bir veri merkezi fiziksel olarak erişilmez hale gelebilir. Kritik altyapı (enerji, finans, sağlık vb) durduğunda toplumsal kaos oluşacağı için, verinin coğrafi olarak gerekirse binlerce kilometre ötede çalışan bir yedeklemesinin olması zorunluluk halini aldığı aşikardır.

Sürekli Test Edilen Afet Yönetimi

Statik ve yalnızca dokümantasyon düzeyinde kalan afet durumu kurtarma planları, sistemin sürekli değişen dinamik yapısı (yazılım güncellemeleri, altyapı değişiklikleri ve yeni konfigürasyonlar) nedeniyle geçerliliğini hızla yitirebilir. Modern sistem mimarilerinde test edilip onaylanmayan bir yapının gerçek bir plan olmadığı ilkesi esas alınarak; düzenli tatbikat ve stres testleriyle doğrulanmayan hiçbir kurtarma senaryosunun kriz anında çalışma garantisi vermeyeceği kabul edilmektedir.

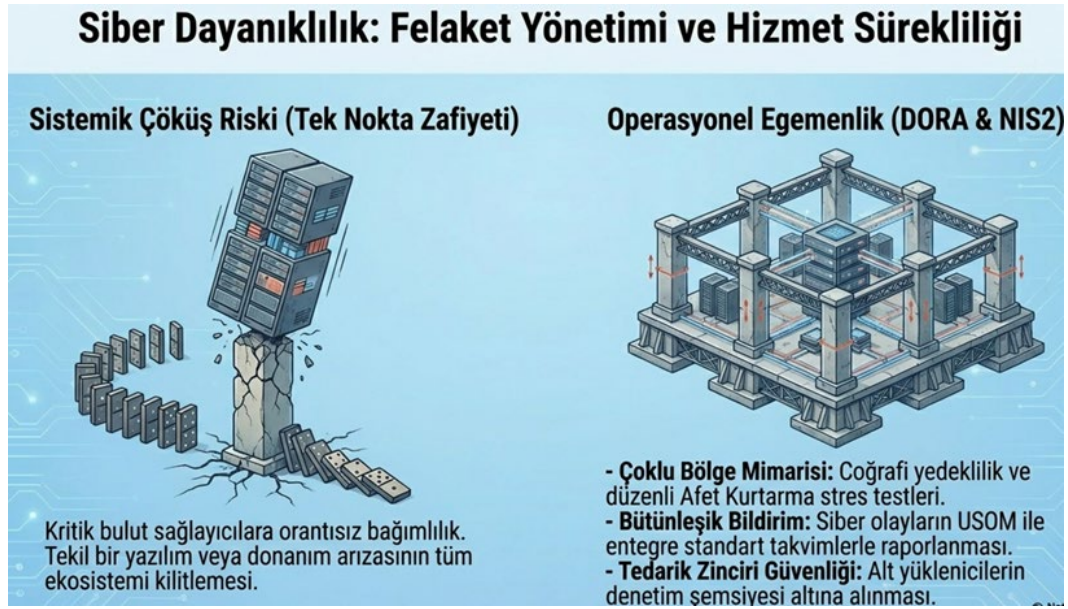
GitLab Veri Kaybı Vakası (2017): GitLab, 300 GB'lık canlı veriyi yanlışlıkla sildiğinde ellerinde tam 5 farklı yedekleme/DR mekanizması vardı. Ancak, hiçbirini düzgün çalışmadı çünkü **düzenli**

¹⁷⁸ Summary of the AWS Service Event in the Northern Virginia (US-EAST-1) Region, (2021).
<https://aws.amazon.com/message/12721/>

test edilmemişlerdi. Bu olay, "*yedeğinizin olması geri dönebileceğinizi garanti etmez*" ilkesinin en büyük kanıtıdır.¹⁷⁹

Sistem Kayması (Configuration Drift): Yazılım sistemleri sürekli olarak güncellenir. Mesela 6 ay önce çalışan bir kurtarma senaryosu, bugün değişen bir veritabanı şeması veya güvenlik sertifikası nedeniyle başarısız olacaktır.

Psikolojik Faktör ve Hız: Kriz anında panik durumu vardır. Sürekli tatbikat yapılmadığında, ekiplerin "Kurtarma Süresi Hedefi" (RTO) ve "Kurtarma Noktası Hedefi" (RPO) sürelerine uyması imkânsız hale gelir.



ŞEKİL 6-4: Siber Dayanıklılık ve Süreklilik (YZ ile hazırlanmıştır)

6.4. Stratejik Analiz ve Yeni Nesil Siber Güvenlik Yol Haritası

Bu bölüm, Türkiye'nin mevcut dijital mevzuatını (5651 Sayılı Kanun ve KVKK) küresel standartlar (AB-DSA, NIS2, DORA) ile karşılaştırarak stratejik dönüşüm alanlarını belirlemektedir. Ana hedef; "içerik odaklı" reaktif yapıdan, "**sistemik risk ve altyapı dayanıklılığı**" odaklı proaktif bir modele dönüşmektir.

¹⁷⁹ Postmortem of database outage of January 31, 2017. <https://about.gitlab.com/blog/postmortem-of-database-outage-of-january-31/>

6.4.1. Algoritmik Hesap Verilebilirlik ve Sistemik Risk

Mevcut yerel düzenlemeler ile platformlar statik birer veri havuzu olarak değerlendirilmekte olup, denetimi daha çok "tekil ihlaller" ile sınırlı tutmaktadır. Oysa modern platformların yönetimi, algoritmik işleyişin toplumsal sonuçlarını merkeze alarak yapılmalıdır.

- **Tespit:** Ulusal mevzuatta "sistemik risk" tanımı ve algoritmaların içeriği yayma (amplifikasyon) süreçlerine dair denetim mekanizması bulunmamaktadır.
- **Stratejik Öneri:** Platform mimarilerinin bilgi ekosistemi üzerindeki etkilerini ölçen "**Algoritmik Etki Değerlendirmesi**" zorunlu kılınmalıdır ve platformlar sadece "taşıyıcı" değil, içeriği öne çıkaran "algoritmik küratör" olarak sorumlu tutulmalıdır.

6.4.2. Koordine Yapay Davranışlar (CIB) ve Bilgi Bütünlüğü

Küresel standartların (DSA, OSA) aksine mevcut mevzuatta münferit kullanıcı ihlalleri ile teknoloji destekli organize manipülasyon ağları (botlar) arasında teknik bir ayrım yer almamaktadır.

- **Tespit:** Otomatik hesaplar ve yapay etkileşim ağları, bağımsız bir operasyonel risk veya sistem zafiyeti olarak tanımlanmamıştır.
- **Stratejik Öneri:** CIB, içeriğin niteliğinden bağımsız bir "**altyapı güvenliği ve bilgi bütünlüğü riski**" olarak raporlanmalıdır. Platform sağlayıcılarına, otomatik ağların tespiti ve proaktif savunma bariyerleri kurma yükümlülüğü getirilmelidir.

6.4.3. Operasyonel Dayanıklılık ve Kritik Hizmet Standartları

Dijital platformlar, kritik veri hacimlerine rağmen henüz "Kritik Hizmet Sağlayıcı" tanımının operasyonel ve yasal kapsamında değildir.

- **Tespit:** Mevzuatta siber olay bildirimleri münferittir ve sadece veri ihlalleriyle sınırlıdır. İş sürekliliği (BCP) ve felaket kurtarma (DR) için bağlayıcı teknik standartlar (RTO/RPO) tanımlı değildir.
- **Stratejik Öneri (NIS2/DORA Uyumu):** Büyük ölçekli platformlar "**Kritik Dijital Hizmet Sağlayıcı**" kategorisine alınmalıdır. USOM ile entegre; 24 saatlik "erken uyarı" ve 72 saatlik "olay bildirimi" takvimi ile vaka sonrası **Kök Neden Analizi (RCA)** zorunlu kılınmalıdır.

6.4.4. Dijital Egemenlik ve Bulut Jeopolitiği

Dijital dayanıklılık, sadece veriyi ülke sınırları içinde tutmak (data residency) değildir; esas olan kriz anlarında operasyonel bağımsızlığı koruyabilmektir.

- **Tespit:** Küresel bulut sağlayıcılarına (hyperscalers AWS, Azure vb.) olan aşırı bağımlılık, ambargo veya bölgesel kesinti anlarında "ulusal felç" riski (Single Point of Failure) oluşturmaktadır.
- **Stratejik Öneri:** Kritik altyapı bileşenlerinde coğrafi yedeklilik ve "**Çoklu Bulut (Multi-cloud)**" stratejileri tesis edilmelidir. Egemenlik vizyonu, platformun dışı olan bağımlılık zincirlerini (API, bulut, veri yolu vb) yönetebilme kapasitesi üzerine tasarlanmalıdır.

6.4.5. Şeffaflık, Etik Tasarım ve Bağımsız Denetim

Dijital ekosistemin güvenli bir yapıda sürdürülmesi için, idari denetimler ve bilimsel teknik analize açık bir şeffaflık gerekmektedir.

- **Tespit:** Denetim süreçleri halihazırda sınırlı bir idari çerçevede yürütülmekte olup platformların algoritmik işleyişine dair ham veriler, teknik inceleme ve akademik araştırmalar için bir erişim protokolü bulunmamaktadır.
- **Stratejik Öneri:** "**Yetkilendirilmiş Araştırmacı Erişimi**" ile bağımsız denetim mekanizmaları kurulmalıdır. YZ sistemlerinin "veri zehirlenmesi" ve sentetik içerik (deepfake) gibi yeni nesil saldırı yüzeylerine karşı dayanıklılığı, periyodik stres testleriyle denetlenmelidir.

TABLO 6-1: Stratejik Regülatif Analiz ve Gelişim Tablosu

Analiz Alanı	Mevcut Durum (Türkiye)	Hedef Standart (AB/UK/OECD)	Stratejik Mevzuat Geliştirme Alanları
Sistemik Risk & Mimari	Reaktif Yaklaşım: Odak noktası sadece münferit içeriklerin kaldırılmasıdır.	DSA (Madde 34-35): Platform mimarisi ve algoritmaların toplumsal etkilerinin yönetimi.	"Sistemik risk" tanımının mevzuata girişi; algoritmik süreçlerin ve yayılım (amplifikasyon) yöntemlerinin denetimi.
Yapay Davranışlar (CIB) & Botlar	Tanımlanmamış Risk: Otomatik hesaplar bağımsız bir zafiyet alanı olarak ele alınmamaktadır.	DSA & OSA: Organize manipülasyon ve	Bot ağlarıyla teknik mücadele yükümlülüğü; koordine davranışların "bilgi güvenliği riski" olarak raporlanması.

Analiz Alanı	Mevcut Durum (Türkiye)	Hedef Standart (AB/UK/OECD)	Stratejik Mevzuat Geliştirme Alanları
		yapay ağırlara karşı proaktif mücadele.	
Olay Bildirim Mekanizmaları	Parçalı Yapı: Bildirimler veri ihlali odaklıdır ve kurumsal eşgüdüm düşüktür.	NIS2 Uyumu: Kritik hizmet sağlayıcılar için merkezi ve hızlı raporlama sistemi.	Büyük platformların "Kritik Dijital Hizmet Sağlayıcı" olarak tanımlanması; USOM ile entegre standart bildirim takvimi.
Operasyonel Dayanıklılık	İnisiyatif Bazlı: BCP ve felaket kurtarma (DR) için bağlayıcı teknik standartlar eksiktir.	DORA Uyumu: Dijital altyapının her türlü kesintiye karşı teknik sürdürülebilirliği.	Asgari teknik mimari kriterleri (coğrafi yedeklilik vb.); zorunlu stres testleri ve 3. taraf (bulut) risk yönetimi.
Şeffaflık & Denetim	Kapalı Devre: Denetim sadece idari kurumlarla sınırlıdır; veri erişimi kısıtlıdır.	Bağımsız Denetim: Bilimsel doğrulamaya ve akademik araştırmaya açık veri modelleri.	Yetkilendirilmiş araştırmacı modeli; algoritmik hesap verebilirlik raporları ve kamuya açık şeffaflık özetleri.

Değerlendirme: 7545 Sayılı Siber Güvenlik Kanunu, Kapasite İnşası ve Küresel Uyuma İlişkin Perspektif

Türkiye’de yakın dönemde yürürlüğe giren **7545 sayılı Siber Güvenlik Kanunu**, ulusal siber güvenlik mimarisinin kurumsallaştırılması bakımından önemli bir adım teşkil etmektedir. Kanun, özellikle kritik altyapıların korunması, ulusal siber olay müdahale kapasitesinin güçlendirilmesi ve kamu kurumları ile özel sektör arasında koordinasyon mekanizmalarının geliştirilmesi yönünde güvenlik odaklı bir çerçeve ortaya koymaktadır.

Bununla birlikte, küresel siber yönetim literatürü incelendiğinde siber güvenliğin yalnızca **tehditlere karşı savunma (security)** perspektifiyle değil, aynı zamanda **sistemlerin kesintisiz çalışabilme kabiliyeti ve krizlere uyum sağlayabilme kapasitesi (resilience)** üzerinden ele alındığı görülmektedir. Bu bağlamda, ulusal düzenlemelerin yalnızca güvenlik tedbirleriyle sınırlı kalmayıp **operasyonel dayanıklılık, ürün güvenliği ve ekosistem kapasitesi** boyutlarını da içerecek şekilde geliştirilmesi önem taşımaktadır.

Bu noktada özellikle **Avrupa Birliği Siber Dirençlilik Yasası (Cyber Resilience Act – CRA)** dikkat çekmektedir. CRA, siber güvenliği yalnızca ağ ve sistem güvenliği perspektifiyle değil, **dijital ürünlerin tasarımından test edilmesine ve piyasaya arz edilmesine kadar tüm yaşam döngüsü boyunca güvenli olmasını zorunlu kılan bir düzenleme** olarak öne çıkmaktadır. Bu yaklaşım, siber güvenliğin yalnızca operasyonel bir savunma meselesi değil, aynı zamanda **ürün güvenliği ve endüstriyel kapasite** meselesi olduğunu ortaya koymaktadır.

Türkiye açısından bu gelişmeler iki kritik politika alanını gündeme getirmektedir:

Birincisi, insan kaynağı ve uzmanlık kapasitesi. Siber güvenlik alanındaki düzenlemelerin etkin biçimde uygulanabilmesi; yalnızca teknik altyapıya değil, aynı zamanda **nitelikli siber güvenlik uzmanlarının, güvenlik analistlerinin, olay müdahale ekiplerinin ve güvenli yazılım geliştirme uzmanlarının yetiştirilmesine** bağlıdır. Bu nedenle ulusal düzeyde geliştirilecek stratejilerin, üniversiteler, teknik eğitim kurumları ve sektör iş birlikleri üzerinden sürdürülebilir bir **siber güvenlik insan kaynağı politikası** oluşturması gerekmektedir.

İkincisi, teknik test ve doğrulama altyapısının geliştirilmesidir. CRA benzeri düzenlemeler, siber güvenlik ürünlerinin ve dijital sistemlerin piyasaya sunulmadan önce bağımsız teknik değerlendirmelerden geçmesini öngörmektedir. Bu nedenle Türkiye’de;

- Siber güvenlik ürünlerinin test edilmesine yönelik **akredite laboratuvar altyapılarının kurulması,**

- Güvenli yazılım ve donanım geliştirme süreçlerini doğrulayacak **sertifikasyon ve uygunluk değerlendirme mekanizmalarının geliştirilmesi**,
- Yerli siber güvenlik teknolojilerinin küresel standartlarla uyumlu şekilde test edilmesini sağlayacak **ulusal teknik kapasitenin güçlendirilmesi** stratejik önem taşımaktadır.

Sonuç olarak, **7545 sayılı Siber Güvenlik Kanunu’nun oluşturduğu kurumsal çerçevenin** küresel düzenlemelerle uyumlu bir şekilde **operasyonel dayanıklılık, ürün güvenliği ve teknik kapasite geliştirme politikalarıyla tamamlanması**, Türkiye’nin dijital egemenliğini ve siber güvenlik ekosisteminin sürdürülebilirliğini güçlendirecektir. Bu doğrultuda hazırlanacak kapsamlı bir **ulusal siber güvenlik kapasite ve istihdam stratejisi raporu**, hem düzenlemelerin etkin uygulanmasına katkı sağlayacak hem de Türkiye’nin küresel siber güvenlik standartlarıyla entegrasyonunu hızlandıracaktır.

BÖLÜM 7: DENETİM, YAPTIRIMLAR VE HUKUKİ ÇÖZÜM MEKANİZMALARI

Bölümün Amacı: Dijital piyasalarda sadece kâğıt üzerinde mevzuat oluşturmak değil, bu mevzuatın ihlal maliyetini ihlal kazancından yüksek kılacak etkin bir uygulama (enforcement) ve caydırıcılık (deterrence) gücünü yaratmak önem arz etmektedir. Temel hedef; asimetrik güç dengesini düzeltmek, kullanıcıları tek başına platformlarla karşı karşıya getirmemek ve denetimi statik bir "hukuki kontrol" olmaktan çıkarıp "veri ve algoritma odaklı" dinamik bir mimariye kavuşturmadır.

İçerik ve Kapsam:

- Geleneksel idari denetimden, algoritmaları "tersine mühendislik" ile inceleyebilecek veri bilimcilerle donatılmış, teknik ve kurumsal olarak tam bağımsız denetim otoritesi modeline geçiş.
- Rekabet, veri koruma ve iletişim regülatörleri arasındaki yetki çakışmalarını önleyecek, İngiltere DRCF modelinden ilham alan "Dijital Ekosistem Düzenleme Kurulu" eşgüdüm vizyonunun Türkiye için tasarlanması.
- Trilyon dolarlık platformlar için "iş yapma maliyeti" olarak görülen maktu cezalar yerine; küresel ciro bazlı kademeli para cezaları ile desteklenen Davranışsal ve Yapısal Tedbirlerin uygulanması.
- Mahkemelerin iş yükünü azaltacak ve kullanıcılara hız kazandıracak "Yargı Dışı Uyuşmazlık Çözüm" (Alternative Dispute Resolution- ADR) kurullarının ve "Kolektif Hak Arama" (Sınıf Davaları) mekanizmalarının tesisi.

Temel Kavramlar:

- Caydırıcılık ve Etkin Uygulama (Deterrence & Enforcement)
- Davranışsal ve Yapısal Tedbirler
- Yargı Dışı Çözüm Kurulları (ADR - Out-of-court Settlement)
- Kolektif Hak Arama (Sınıf Davaları - Class Actions)
- Düzenleyici Arbitraj (Regulatory Arbitrage) ve Hukuki Eşgüdüm

7.1. Giriş

Dijital platformların modern ekonominin ve toplumsal yaşamın merkezine yerleşmesi, bu yapıların yalnızca ekonomik birer aktör değil, aynı zamanda dijital ekosistemin kurallarını belirleyen "özel regülatörler" haline gelmesine neden olmuştur. Bu durum, geleneksel hukuk normlarının yetersiz kaldığı yeni bir düzenleme ihtiyacını doğurmuştur. Bu bölüm, platform ekonomisindeki asimetrik güç dengesini düzeltmeyi, kullanıcı haklarını korumayı ve piyasa dinamiklerini piyasaya yeni girenler lehine dengelemeyi amaçlayan denetim ve yaptırım mekanizmalarını ele almaktadır.¹⁸⁰

Etkin Uygulama ve Caydırıcılık Odaklı Bir Ekosistem İnşası

Bu bölümün temel amacı, dijitalleşen piyasalarda sadece mevzuat oluşturmak değil, bu mevzuatın **etkin bir şekilde uygulanmasını (enforcement)**¹⁸¹ ve ihlallere karşı **caydırıcılığı (deterrence)** sağlayacak bir hukuki mimari tasarlamaktır.

OECD'nin "Dijital Pazarlarda Etkin Düzenleme" prensipleri doğrultusunda, zararın oluşmasını bekleyen reaktif yaklaşımlar yerine, riskleri önceden tespit eden **proaktif denetim** mekanizmalarının kurulması hedeflenmektedir.^{182, 183}

Caydırıcılık, yalnızca yüksek meblağlı para cezalarıyla değil; aynı zamanda AB DMA¹⁸⁴ ve DSA¹⁸⁵ yasalarında da görüldüğü üzere, sistemik ihlallerde operasyonel müdahale (yapısal tedbirler) riskinin masada olmasıyla sağlanacaktır. Kısaca, caydırıcılık sadece devletin cezasıyla değil, mağdur edilen milyonlarca kullanıcının "hak arama" gücüyle de sağlanır.

Bunlara ilaveten, "Etkin uygulama" (enforcement) kavramının artık sadece ulusal bir çaba değil, G7 ölçeğinde bir "ortak denetim standardı" haline geldiğini vurgulayan G7 raporu, dünya teknoloji devlerinin (Big Tech) farklı ülkelerdeki farklı kuralları birbirine karşı kullanmasını (regulatory arbitrage) engellemek için hazırlanan küresel bir envanterdir. Ayrıca, sözkonusu raporda, caydırıcılığın ancak "küresel ölçekte benzer yaptırım riskleri" (aligned sanctions) ile mümkün olabileceği argümanı desteklenmektedir.¹⁸⁶

¹⁸⁰ Cusumano, M. A., Gawer, A., & Yoffie, D. B. (2021): *The Business of Platforms: Strategy in the Age of Digital Competition, Innovation, and Power*. Harper Business.

¹⁸¹ Geradin, D. (2023): *The Digital Markets Act (DMA): A New Era for EU Competition Law in the Digital Sector*, Journal of European Competition Law & Practice.

¹⁸² OECD (2023): *Handbook on Competition Policy in the Digital Age*. OECD Publishing, Paris.

¹⁸³ OECD (2022). *Recommendation of the Council on the Governance of Digital Platforms*. OECD/LEGAL/0482

¹⁸⁴ Digital Markets Act (DMA). Regulation (EU) 2022/1925 on contestable and fair markets in the digital sector.

¹⁸⁵ Digital Services Act (DSA). Regulation (EU) 2022/2065 on a Single Market For Digital Services

¹⁸⁶ G7 Enforcers' Summit (2023). *Inventory of Rules and Enforceability in the Digital Economy*. Joint Report by G7 Competition Authorities. Tokyo/Hiroshima.

7.1.1. Kapsam ve Metodoloji: Platform Ekonomisinde Regülasyonun Evrimi

Dijital platform regülasyonları, tarihsel süreçte "serbest bırak-gelişsin" (laissez-faire) yaklaşımından, günümüzün "ex-ante" (öncül) ve risk temelli düzenleme dönemine evrilmiştir.

Evrimsel olarak, ilk aşamada içerik sağlayıcılardan sorumlu tutulmayan platformlar (Safe Harbor), bugün AB DSA ve İngiltere Online Safety Act (OSA)¹⁸⁷ ile "özen yükümlülüğü" (duty of care) altında kapsamlı sorumluluklar üstlenmektedir.

Bu bölüm hazırlanırken; AB'nin **DSA, DMA, AI Act**¹⁸⁸ ve **NIS2**¹⁸⁹ dördlüsü temel referans alınmış; İngiltere'nin **Ofcom** merkezli denetim modeli ile Kanada'nın **Bill C-27 (Dijital Şart Uygulama Yasası)**¹⁹⁰ kapsamında önerilen veri koruma ve yapay zekâ standartları karşılaştırmalı olarak analiz edilmiştir. Bunlara ilaveten, OECD prensipleri de incelenerek dikkate alınmış ve hizmet sağlayıcı, kullanıcı, güvenlik ve ekonomi perspektiflerini birleştiren "çoklu paydaş analizi" yöntemi kullanılmıştır.

Temel Kavramlar

Bölüm boyunca kullanılacak olan anahtar kavramlar, uluslararası literatürle uyumlu olarak şu şekilde tanımlanmıştır:

Sistemik Risk (Systemic Risk): DSA kapsamında tanımlandığı üzere; bir platformun tasarımının, algoritmasının veya kullanımının toplum geneli üzerinde (demokrasi, kamu sağlığı, temel haklar veya güvenlik) yaratabileceği yaygın ve derin etkilerdir. Denetim odak noktası, tekil ihlallerden ziyade bu risklerin yönetimidir.¹⁹¹

Kapı Eşiği (Gatekeeper): DMA literatüründe yer alan bu kavram; geniş bir kullanıcı kitlesine sahip olan, işletmelerin müşterilerine ulaşması için "darboğaz" teşkil eden ve piyasada kalıcı bir güce sahip olan devasa platformları ifade eder. Bu aktörler için genel kuralların ötesinde "asimetrik yükümlülükler" öngörülür.

Veri Egemenliği (Data Sovereignty): Bireylerin kendi verileri üzerindeki kontrolünü (Kanada CPPA örneği- Consumer Privacy Protection Act) ve bir devletin kendi sınırları içindeki dijital altyapı ve veri trafiği üzerindeki düzenleme yetkisini ifade eder. Bu kavram, NIS2 direktifi bağlamında siber dayanıklılığın ve ekonomik güvenliğin ayrılmaz bir parçası olarak ele alınmaktadır.¹⁹²

¹⁸⁷ **Birleşik Krallık (İngiltere), Online Safety Act 2023 (OSA):** Ofcom's regulatory framework for online safety and duty of care.

¹⁸⁸ **Artificial Intelligence Act (AI Act).** Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence.

¹⁸⁹ **NIS2 Directive.** Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union.

¹⁹⁰ **Kanada, Bill C-27 (Digital Charter Implementation Act):** Including Consumer Privacy Protection Act (CPPA) and Artificial Intelligence and Data Act (AIDA).

¹⁹¹ **Zuboff, S. (2019):** *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power.* PublicAffairs. (Veri egemenliği ve platform gücü analizi için)

¹⁹² **Zuboff, S. (2019):** *a.g.e.* (Veri egemenliği ve platform gücü analizi için)

7.2. Stratejik Paydaş Analizi ve Perspektifler

Dijital platformların düzenlenmesi, kimi zaman birbiriyle çatışan ve kimi zamanda birbirini tamamlayan çok boyutlu çıkarların dengelenmesini gerektirir. Bu bölümde, ekosistemin ana aktörleri ve temel düzenleme sütunları uluslararası standartlar ışığında analiz edilmektedir.

7.2.1. Hizmet Sağlayıcılar: Uyum Maliyetleri ve Operasyonel Öngörülebilirlik

Hizmet sağlayıcılar (özellikle gatekeeper statüsündekiler), yeni nesil regülasyonların operasyonel ve mali yükümlülüklerini üstlenmektedir.

AB DMA ve DSA, Uyum Maliyetleri kapsamında, platformlara düzenli bağımsız denetim raporları sunma ve veri taşınabilirliği altyapısı kurma zorunluluğu getirmiştir. OECD, bu maliyetlerin özellikle KOBİ ölçeğindeki platformlar için "pazara giriş engeli" oluşturmaması gerektiğini vurgular.¹⁹³

Buna ilaveten, uyum büyük ölçekli platformlar için artık sadece hukuki olmaktan çıkıp yoğun bir veri mühendisliği problemine dönüşmektedir. Platformların DSA kapsamında sunduğu şeffaflık raporlarını analiz eden bir AB Raporu'na göre, içerik moderasyonu kararlarının %99'unun algoritmalarla alındığı ve "insan denetimi" (human-in-the-loop) maliyetlerinin operasyonel bütçelerin %15'ine ulaştığı belirtilmektedir.¹⁹⁴

İngiltere'deki Stratejik Pazar Durumu (Strategic Market Status-SMS); sadece şirket büyüklüğüne odaklanmaz, buna ilaveten şirketin belirli bir dijital faaliyette sahip olduğu "stratejik güce" ve bu gücün rekabet üzerindeki etkisine de dikkat çeker.¹⁹⁵

Kanada'nın Bill C-27 (AIDA) düzenlemesi, "çevik regülasyon" (agile regulation) yaklaşımını benimseyerek, teknolojik gelişmelere göre güncellenebilir bir çerçeve sunar.

Platformların "çok paydaşlı pazar" doğası gereği, bir tarafa getirilen uyum yükünün (örneğin sıkı içerik denetimi) diğer tarafları (kullanıcılar ve reklam verenler) nasıl etkilediği analiz edilmeli ve regülasyon "operasyonel esneklik" ile dengelenmelidir.¹⁹⁶

¹⁹³ OECD (2022). *A.g.e.*

¹⁹⁴ European Commission (2025), *"The Impact of DSA on Digital Platforms : Transparency and content moderation report"*. Shaping Europe's Digital Future.

¹⁹⁵ UK Parliament (2024). *Digital Markets, Competition and Consumers Act 2024*. Strategic Market Status (SMS) framework and regulatory codes of conduct. London: Stationery Office.

¹⁹⁶ Cusumano ve ark. (2021), *a.g.e.*

7.2.2. Hizmet Alanlar (Kullanıcılar): Hak Arama Yolları ve Dijital Esenlik

Kullanıcı perspektifi, dijital ortamda pasif bir tüketici olmaktan çıkıp, hakları korunan bir "dijital vatandaş" olmaya evrilmiştir.

Hak Arama Yolları kapsamında; AB DSA, kullanıcılara platformların içerik kaldırma kararlarına karşı "yargı dışı uyuşmazlık çözümü" mekanizmalarına başvurma hakkı tanır.

Kullanıcıların artık "yargı dışı" hızlı çözüm mekanizmalarına erişimi, hak arama hızı açısından kritiktir. 2024 ve 2025 yıllarında AB'de kurulan "Yargı Dışı Uyuşmazlık Çözüm" (Out-of-court settlement) kurullarının, Facebook ve TikTok kararlarını %52 oranında kullanıcı lehine çevirdiği bilinmektedir.¹⁹⁷

Dijital Esenlik bağlamında ise; İngiltere Online Safety Act (OSA), platformlara "Özen Yükümlülüğü" (Duty of Care) getirerek, özellikle çocukların ruh sağlığını korumayı ve zararlı içeriklere maruz kalmayı önlemeyi yasal bir zorunluluk haline getirmiştir.

Buna ilaveten, Zuboff kullanıcı verilerinin rıza dışı metalaştırılmasını eleştirirken, regülasyonun temel amacının kullanıcının "karar verme özerkliğini" geri kazandırmak olması gerektiğini savunur.¹⁹⁸

7.2.3. Ekonomi ve Rekabet: Yarışılabilirlik (Contestability) ve İnovasyon

Dijital ekonomide rekabet, artık fiyat odaklı olmaktan çıkmış, veri erişimi ve ekosistem kontrolüne de önem verir hale gelmiştir.

Yarışılabilirlik alanında; AB DMA, "kendine öncelik verme" (self-preferencing) yasakları ile pazara yeni girenlerin büyük platformlarla rekabet edebilmesini hedefler. OECD'nin 2023 tarihli Rekabet El Kitabı, bu durumu "pazarın donmasını engellemek" olarak tanımlar.¹⁹⁹

Rekabetin sağlanması için sadece "devleri engellemek" değil, "veriye erişimi" demokratikleştirmek gerekir. OECD'nin bir çalışması, DMA gibi ex-ante (öncül) düzenlemelerin klasik antitröst soruşturmalarına göre piyasaya girişi %20 daha hızlı tetiklediğini savunur.²⁰⁰

Geradin ise, DMA'nın getirdiği ex-ante (öncül) kuralların, geleneksel antitröst davalarının yıllar süren hantallığını aşarak piyasada "dinamik verimlilik" sağladığını vurgular.²⁰¹

İnovasyon Dengesi kapsamında; Kanada ve OECD prensipleri, regülasyonun inovasyonu boğmaması için "deney alanları" (regulatory sandboxes) oluşturulmasını teşvik eder.

¹⁹⁷ Quinn Emanuel (2025), "Litigating the DMA & DSA: Current Landscape"

¹⁹⁸ Zuboff, S. (2019): *a.g.e.*

¹⁹⁹ OECD (2023): *a.g.e.*

²⁰⁰ OECD (2024), "Competition Policy in Digital Markets: The Combined Effect of Ex Ante and Ex Post Instruments in G7 Jurisdictions".

²⁰¹ Geradin, D. (2023): *a.g.e.*

Haber yayıncılarının platformlar karşısındaki zayıf pazarlık gücünü hukuki bir koruma altına alan Kanada'daki Bill C-18 yasası, "ekonomik dengesizliğin giderilmesi" tartışmasında temel dayanak olmuştur. Örneğin; Google ve Meta gibi devlerin, haber kuruluşlarının ürettiği içeriklerden elde ettikleri trafik ve veri üzerinden oluşan "değer transferini" (value gap) dengelemeleri adına, bu yasa ile "**zorunlu pazarlık**" (mandatory bargaining) modeli getirilmiştir.²⁰²

7.2.4 Hukuk ve Güvenlik: Siber Dayanıklılık ve Algoritmik Hesap Verebilirlik

Güvenlik, dijital platformların sadece içeriğiyle değil, altyapısal sağlamlığıyla da ilgilidir.

Siber Dayanıklılık konusunda; AB'nin NIS2 Direktifi, kritik dijital hizmet sağlayıcılarını siber güvenlik risk yönetimi ve raporlama yükümlülüğü altına sokar. Bu, sistemik bir sökülmenin (systemic collapse) ekonomik güvenliği tehdit etmesini önlemek içindir.

Algoritmik Hesap Verebilirlik konusunda ise; AB AI Act ve Kanada AIDA, yüksek riskli yapay zekâ sistemlerinin (örneğin sosyal ağlardaki tavsiye algoritmaları) şeffaf olmasını ve insan gözetimine tabi tutulmasını şart koşar.

NIS2 ve AI Act yasaları platformların siber güvenliğini "ürün güvenliği" haline getirmiştir. AB'nin bir çalışması, NIS2'deki siber güvenlik raporlama yükümlülükleri ile AI Act'teki algoritmik risk yönetimi arasındaki çakışmaları ve bu ikisinin nasıl "bütünleşik bir denetim" (integrated audit) gerektirdiğini analiz eder.²⁰³

Burada; siber güvenlik ve kişisel verileri koruma arasındaki bağın, "güvenli tasarım" (security by design) ilkesiyle hukuki bir zemine oturtulduğu görülmektedir.

7.3. Yetkili Denetim Otoritesi: Kurumsal Yapı ve Yetkiler

Dijital çağda denetim, statik bir "mevzuata uyum" kontrolünden ziyade, dinamik bir "teknik müdahale" sürecine dönüşmüştür. Dijital ekosistemin denetimi, geleneksel idari denetim yöntemlerinin ötesinde, teknolojik derinlik ve kurumlar arası dinamik bir eşgüdüm gerektirmektedir. Etkin uygulama (enforcement) ve caydırıcılık, otoritenin kurumsal mimarisiyle doğrudan ilintilidir. Bu bölümde, etkin bir denetim otoritesinin yapısal gereklilikleri ve çoklu regülatör yapısındaki işbirliği modelleri analiz edilmektedir.

²⁰² **Government of Canada (2023).** *Online News Act (Bill C-18): An Act respecting online communications platforms that make news content available to persons in Canada.* Ottawa: Justice Laws Website.

²⁰³ **European Parliament Study (2025),** *"Interplay between the AI Act and the EU digital legislative framework".*

7.3.1. Otorite Bağımsızlığı ve Veri Odaklı Denetim

Dijital platformların algoritmik yapıları, denetim otoritesinin sadece hukukçulardan değil, teknik uzmanlardan oluşmasını zorunlu kılar. Otoritenin başarısı, platformların algoritmik sistemlerini "tersine mühendislik" (reverse engineering) ve veri analitiği ile denetleyebilme becerisine bağlıdır.

AB DSA Madde 31 ve AI Act Madde 64; Teknik Kapasite ve Algoritmik Denetim kapsamında otoritelere, platformların veri havuzlarına ve algoritma kaynak kodlarına erişim ve veri denetimi yetkisi tanır. Bu süreçte sadece hukukçuların değil, "algoritma denetçileri" (algorithm auditors) ve veri bilimcilerin istihdamı zorunludur. Bu yüzden otorite bünyesinde "Veri Bilimi Birimleri" kurulmalıdır. AB'nin 2025 yılındaki raporunda DSA'nın Madde 31'sinin uygulamaları detaylıca anlatılmaktadır.²⁰⁴

Bu hususu destekleyen çalışmalardan biri olan Mökander, denetimin etkinliğinin "üçüncü taraf bağımsız denetçiler" ve "kamusal denetçiler" arasındaki veri paylaşım hızına bağlı olduğunu ortaya koymuştur.²⁰⁵ Cusumano da platformların "kara kutu" (black box) doğasını vurgulayarak, denetimin ancak "veri odaklı mühendislik yetkinliği" ile mümkün olabileceğini belirtir.²⁰⁶

İngiltere, Ofcom bünyesinde kurduğu "Algorithmic Assessment" birimi ile platformların zararlı içerik filtrelerini bizzat test edebilmektedir.²⁰⁷ Buna ilaveten, yine aynı bünyede kurulan "Data Engineering and Machine Learning" birimi sayesinde de, sosyal ağların içerik yönetim sistemleri gerçek zamanlı simülasyonlarla test edilebilmektedir.

OECD "Dijital Platform Yönetişimi" ilkeleri de otoritenin hem siyasi hem de ticari baskılardan arındırılmış, bağımsız olarak bütçesel özerkliğe sahip olmasını şart koşar.²⁰⁸

7.3.2. Kurumlar Arası Eşgüdüm Modelleri

Dijitalleşme; rekabet, veri koruma, tüketici hakları ve içerik güvenliği alanlarını iç içe geçirmiş ve bir nevi "tek bir potada" eritmiştir. Bu durum, "tek bir otorite" ve geleneksel kurumsal siloların (insularity) yerine "otoriteler arası ağ" yapısını gerekli kılar.

Rekabet, Veri İşleme, Veri Koruma ve Sektörel Regülatörler Arası Protokollerin Önemi

Platformların ekonomik gücü (Rekabet), veriyi işleme hızıyla birleştiğinde "geçilmez kaleler" oluşturur ve platformların bu gücü, veri toplama ve pazar hakimiyeti arasındaki döngüden beslenir.

²⁰⁴ **European Commission (2025).** "Guidelines on the implementation of Art. 31 of the DSA (Data Access)."

²⁰⁵ **Mökander, J., Morley, J., Taddeo, M., & Floridi, L. (2024).** *Auditing High-Risk AI Systems: A Governance Framework for the EU AI Act.* International Journal of Law and Information Technology.

²⁰⁶ **Cusumano ve ark. (2021), a.g.e.**

²⁰⁷ **Ofcom (2024).** "Approach to Algorithmic Assessment in Online Safety."

²⁰⁸ **OECD (2022).** *A.g.e.*

AB DMA, eşgüdümün hukuki zemini olarak Avrupa Veri Koruma Kurulu (EDPB) ile Avrupa Rekabet Ağı (ECN) arasında zorunlu bilgi paylaşımı öngörür.

Veri Odaklı Rekabet hususunda; OECD'nin 2024 tarihli "Data-Driven Competition" konulu raporunda, veri koruma otoriteleri ile rekabet kurumlarının ayrı çalışmasının "regülatörlerin birbirini etkisiz kılmasına" (regulatory paralysis) yol açabileceği uyarısında bulunmaktadır.²⁰⁹

Buna ilaveten; OECD, regülatörler arasındaki "yetki çatışmalarının" platformlar tarafından "hukuki boşluk" (regulatory arbitrage) olarak kullanılabileceği konusunda uyarılmaktadır.²¹⁰

Monti ve Colomo, dijital regülasyonların "çok katmanlı yönetim" (multi-layered governance) gerektirdiğini ve kurumlar arası bağlayıcı protokollerin hukuki öngörülebilirlik için şart olduğunu vurgulamaktadır.²¹¹

G7 Envanteri de, rekabet otoritelerinin veri koruma otoriteleriyle nasıl işbirliği yapması gerektiğine dair dünyadaki en güncel "en iyi uygulama" listesini sunar.²¹²

Dijital Düzenleme İşbirliği Forumu (İngiltere DRCF Örneği)

Dünyadaki "iş birliği yoluyla denetim" (regulation by cooperation) modelinin öncüsü olan ve en başarılı eşgüdüm modeli olarak kabul edilen İngiltere DRCF (Digital Regulation Cooperation Forum) yapısal bir örnek teşkil eder.

DRCF Modeli; rekabet konularındaki otorite olan CMA (Competition and Markets Authority), veri koruma ofisi olan ICO (Information Commissioner's Office), medya ve iletişim otoritesi Ofcom ve finans otoritesi FCA (Financial Conduct Authority) kurumlarından oluşur. Bu yapı, ortak bir sekreteryaya sahiptir ve "Algoritmik Şeffaflık", "Veri Taşınabilirliği", "Çevrim İçi Zarar" ve "Yapay Zekâ Denetimi" gibi konularda ortak çalışma programları yürütür.²¹³ Bu model, Platformlar için "tek durak ofis" mantığına yaklaşan bir öngörülebilirlik sağlar.

Geradin, DRCF benzeri yapıların, kaynak israfını önlediğini ve regülatörler arası "bilgi asimetrisini" giderdiğini savunur.²¹⁴ Alexandre de Streel ise; DRCF modelinin, platformlar üzerindeki "denetim

²⁰⁹ OECD (2024), "Cooperation Between Competition and Data Protection Authorities". OECD Competition Policy Roundtables.

²¹⁰ OECD (2024), "Competition Policy in Digital Markets: The Combined Effect of Ex Ante and Ex Post Instruments in G7 Jurisdictions".

²¹¹ Monti, G., & Colomo, P. I. (2025). *Interplay of Digital Regulations: DMA, DSA and Beyond*. Oxford University Press.

²¹² G7 Enforcers' Summit (2023). *a.g.e.*

²¹³ DRCF (2024). "Annual Plan and Collaborative Projects."

²¹⁴ Geradin, D. (2023): *a.g.e.*

baskısını" (regulatory pressure) artırırken, dürüst oyuncular için "uyum karmaşasını" azalttığını ispatlamaktadır.²¹⁵

Diğer uygulama örnekleri olarak; Kanada, Bill C-27 kapsamında benzer bir "Yapay Zekâ ve Veri Komisyonu" yapısını ve koordinasyon ofisini kurup, veri koruma otoritesiyle entegre bir şekilde kurgularken; Avustralya DPDRF (Digital Platform Regulators Forum) ile rekabet ve içerik denetimini tek bir stratejik plan altında toplamıştır.

Bunlara ilaveten; burada İngiltere DMCC Yasası'nın, otoritelerin platformun tüm faaliyetlerine değil, sadece stratejik güç sahibi olduğu alana (örneğin sadece uygulama mağazası veya sadece arama motoru) odaklanarak "terzi usulü" kurallar koyma kararlılığından da bahsetmek gerekir.²¹⁶

7.4. Uluslararası Mevzuat Analizi ve Karşılaştırmalı Hukuk

Dijital platformların dünyanın neredeyse her yerinde çalışabilmesi, ulusal düzenlemelerin ötesinde, küresel standartlarla uyumlu bir mevzuat setini zorunlu kılmaktadır. Bu bölümde, "Brüksel Etkisi" (Brussels Effect)²¹⁷ olarak adlandırılan AB düzenlemeleri ile diğer öncü hukuk sistemlerinin dinamik yapısı; "etkin uygulama" ve "caydırıcılık" parametreleri ışığında analiz edilmektedir.

7.4.1. Avrupa Birliği Dijital Müktesebatı: Çok Katmanlı Denetim Mimarisi

AB, dijital ekosistemi tek bir kanunla değil, birbirini tamamlayan dört temel sütun üzerinden yönetmektedir. Bu yapı, platformun sadece ekonomik gücünü değil, toplumsal etkisini ve teknik güvenliğini de denetim altına alır.

Dijital Hizmetler Yasası (DSA) ve Sistemik Risk Yönetimi

DSA, dijital platformlar için "modern bir anayasa" niteliğindedir. Geleneksel "Safe Harbor" (Sorumsuzluk Rejimi) anlayışını, "Özen Yükümlülüğü" (Due Diligence) ile değiştirmiştir.

Asimetrik Yükümlülükler kapsamında; aylık 45 milyon kullanıcıyı aşan "Çok Büyük Çevrim İçi Platformlar" (VLOPs), sistemik risk analizleri yapmak ve bağımsız denetçilere kapılarını açmak

²¹⁵ De Streel, A. (2024). *The Institutional Architecture of Digital Regulation: Efficiency, Accountability and Independence*. Centre on Regulation in Europe (CERRE).

²¹⁶ UK Parliament (2024). *A.g.e. DMCC Act 2024*.

²¹⁷ Bradford, A. (2023). *The Brussels Effect: How the European Union Rules the World*. (Updated Edition). Oxford University Press.

zorundadır. Avrupa Komisyonu'nun 2026 raporuna göre, ilk 18 aydaki denetimler sonucunda, VLOP'ların algoritma tasarımlarında %30'a yakın iyileştirme gözlemlenmiştir.²¹⁸

Ayrıca, Algoritmik Şeffaflık konusunda, tavsiye algoritmalarının neden o içeriği kullanıcıların önlerine çıkardığına dair açık bilgi verilmesi zorunluluğu getirilmiştir. Floridi, bu şeffaflığın "bilişsel özerkliği" (cognitive autonomy) korumada kilit rol oynadığını belirtir.²¹⁹

Dijital Pazarlar Yasası (DMA) ve Gatekeeper Denetimi

DMA, rekabet hukukunda bir devrim yaparak "Ex-ante" (öncül) müdahaleyi başlatmıştır. Ayrıca, gatekeeper (Kapı Eşiği) statüsündeki platformların kendi servislerini ön plana çıkarması (self-preferencing) ve verileri farklı platformlar arasında izinsiz birleştirmesi yasaklanmıştır.

Caffarra & Morton, Piyasa Dinamiği açısından; DMA'nın "contestability" (yarışılabilirlik) amacına ulaşması için veriye erişimin demokratikleşmesi gerektiğini savunur.²²⁰

Yapay Zekâ Yasası (AI Act) ve Risk Temelli Yaklaşım

Platformların kullandığı tavsiye sistemleri ve içerik moderasyon araçları artık AI Act kapsamındadır. Böylece; iş bulma, kredi verme veya demokratik süreçleri etkileme potansiyeli olan algoritmalar "yüksek riskli" kabul edilir ve yoğun bir teknik dokümantasyon sürecine tabi tutulur. Ayrıca, bireyleri sosyal puanlamaya tabi tutan ve bilinçaltı yönlendirme yapan algoritmalar tamamen yasaklanmıştır.

NIS2 Direktifi ve Siber Dayanıklılık

Dijital platformların artık "kritik bir altyapı" olarak görülmesinden dolayı; NIS2, platformların sadece yazılımsal değil, fiziksel ve kurumsal siber güvenlik stratejilerini de denetlemektedir. Brous & Janssen, NIS2'nin "tedarik zinciri güvenliği" vurgusunun, platformların alt yüklenicilerini de denetim şemsiyesi altına soktuğunu belirtir.²²¹

²¹⁸ **European Commission (2026).** *Comprehensive Review of the Digital Services Act Implementation: Year Two Report*. Brussels.

²¹⁹ **Floridi, L. (2024).** *The Ethics of Artificial Intelligence: Principles, Challenges, and Opportunities*. Oxford University Press.

²²⁰ **Caffarra, C., & Morton, F. S. (2024).** "Gatekeeper Governance: The First Wave of DMA Enforcement", Yale School of Management Research Paper.

²²¹ **Brous, P., & Janssen, M. (2024).** "Sovereign Clouds and Cyber-Resilience: Navigating NIS2", Journal of Strategic Information Systems.

7.4.2. Birleşik Krallık (İngiltere) Yaklaşımı: Online Safety Act (OSA)²²²

İngiltere, AB'nin kuralcı (prescriptive) yapısından ziyade "ilke temelli" (principle-based) bir modeli tercih etmiştir.

OSA, platformlara kullanıcılarını "önlenebilir zararlardan" koruma yükümlülüğü getirir. Bu kavram, klasik tazminat hukukundan regülasyon dünyasına devrim niteliğinde bir transferdir. Buna, Özen Yükümlülüğü (Duty of Care) denmektedir.

Regülatör Ofcom, platformların risk değerlendirmelerini yetersiz bulursa, doğrudan algoritma değişikliği talep edebilir. Scott & Yeung, "Algorithmic Regulation" üzerine yaptıkları çalışmada, bu modelin platformların "içsel denetim kültürünü" (internal compliance culture) geliştirmede daha başarılı olduğunu savunur.²²³

Özetle; İngiltere modeli, platforma özel yükümlülükler getiren daha esnek ve diyaloga dayalı bir yapıdadır (evidence-based and participative).

7.4.3. Kanada Modeli: Bill C-27 ve Dijital Şart (Digital Charter)

Kanada, veri koruma ve yapay zekâyı tek bir "Dijital Şart" altında birleştirerek daha bütünleşik bir yaklaşım sergilemektedir. Tüketici Gizliliğini Koruma Yasası (CPPA), kişisel verilerin korunmasında bireye "veriyi silme" ve "taşınabilirlik" haklarını çok daha sert yaptırımlarla sunmaktadır.

AIDA (Yapay Zekâ ve Veri Yasası) ise, yapay zekâ sistemlerinin önyargıdan arındırılması (bias mitigation) konusuna odaklanır.²²⁴

Kanada modeli, regülatörün (AI & Data Commissioner) platformlarla sürekli diyalog halinde olduğu "çevik" bir yapıya sahiptir.

7.4.4. OECD Bakış Açısı²²⁵

Özellikle dünya genelindeki farklı regülasyon modellerinin birbiriyle nasıl etkileşime girdiğini ve bu süreçteki küresel eğilimleri bu rapor sayesinde analiz edebiliriz. Söz konusu OECD Rapor'unda şu üç temel argümanın altı çizilmiştir:

²²² Ofcom UK (2025). *Online Safety Act: Final Codes of Practice and Enforcement Guidelines*.

²²³ Scott, C., & Yeung, K. (2025). *Algorithmic Governance and the Law*. Edward Elgar Publishing.

²²⁴ Canadian Ministry of Innovation (2025). *The AIDA Companion: A Guide to the Artificial Intelligence and Data Act*.

²²⁵ OECD (2024). *Report on Emerging Trends in Digital Platform Regulation*. OECD Digital Economy Papers.

Regülatörlerin Küresel Yakınsaması (Regulatory Convergence): Farklı ülkelerin (AB, İngiltere, Kanada) farklı yaklaşımları olsa da aslında "risk temelli denetim" ve "ex-ante (öncül) müdahale" konusunda küresel bir fikir birliğine varıldığı görülmektedir.

Yatay Regülasyon Eğilimi: Regülasyonun artık sadece "rekabet" veya sadece "içerik" ile sınırlı kalmadığı ve veri, yapay zekâ ve siber güvenliğin iç içe geçtiği "yatay (cross-cutting) düzenleme" dönemi ile bir nevi tanımının değiştiği gözlenmektedir.

Uygulama Kapasitesi ve İş Birliği: Özellikle gelişmekte olan ülkelerin dev teknoloji şirketlerini denetlerken karşılaşılan "teknik kapasite eksikliği" riski önem arz etmektedir. Bu sebeple, denetimin kağıt üzerinde kalmaması için OECD'nin önerdiği "uluslararası işbirliği ve bilgi paylaşımı" gerekliliği ortaya çıkmaktadır.

7.4.5. Karşılaştırmalı Analiz ve Akademik Perspektifler

Bu düzenlemelerin etkinliği, literatürde "esneklik" ve "caydırıcılık" ekseninde tartışılmaktadır.

Scott & Yeung, AB'nin katı kurallarının bazen inovasyonu baskıladığını, ancak İngiltere'nin "ilke temelli" (principle-based) yaklaşımının denetimde daha çevik sonuçlar verdiğini savunur.²²⁶

Siber Güvenlik Kesitinden bakıldığı zaman; Brous & Janssen, NIS2 ve AI Act'in kesişiminde, platformların artık sadece veri hırsızlığından değil, "algoritmik manipülasyonun yol açtığı sistemik güvenlik açıklarından" da sorumlu tutulacağını belirtmektedir.²²⁷

Uygulama Zorlukları ve Akademik Tartışmalar

Uluslararası literatürde bu düzenlemeler üç ana eksenle eleştirilmektedir:

İnovasyon vs. Regülasyon Dengesi: Bradford (2023), "Brüksel Etkisi"nin küresel standartları yükselttiğini kabul ederken, aşırı regülasyonun Avrupa merkezli dev platformların çıkmasını engellediği (innovation chilling effect) tezini tartışır.²²⁸

Uygulanabilirlik Krizi: Monti & Colomo, kurumlar arası (örneğin veri koruma otoritesi ile rekabet otoritesi) yetki çakışmalarının platformlar tarafından "hukuki boşluk yaratmak" için kullanılabileceği uyarısını yapar.²²⁹

²²⁶ Scott, C., & Yeung, K. (2025). *A.g.e.*

²²⁷ Brous, P., & Janssen, M. (2024). *A.g.e.*

²²⁸ Bradford, A. (2023). *A.g.e.*

²²⁹ Monti, G., & Colomo, P. I. (2025). *A.g.e.*

Teknik Denetim Açığı: Mökander ve arkadaşları, yasaların mükemmel olabileceğini ancak devletlerin VLOP'ları denetleyecek yeterli "veri bilimcisi" istihdam edememesi durumunda yasaların "kâğıt üzerinde kalacağını" vurgular.²³⁰

7.5. Platform Özelinde Uygulama Stratejileri

Dijital ekonomide "herkese uyan tek bir ürün" (one-size-fits-all) yaklaşımı, denetimin etkinliğini zayıflatmaktadır. Arama motorlarının veri indeksleme gücü, sosyal ağların algoritmik kürasyonu ve e-ticaret platformlarının piyasa yönetimi farklı risk profilleri sunar. Bu bölümde, AB DSA ve DMA, İngiltere ve Kanada pratikleri ışığında platform bazlı denetim stratejileri analiz edilmektedir.

7.5.1. Arama Motorları: Algoritmik Tarafsızlık ve Veri İndeksleme Denetimi

Arama motorları, dijital dünyanın "rehberleri" konumundadır. Bu platformlar üzerindeki denetim, bilginin hiyerarşisini ve rekabetin adilliğini hedeflemelidir.

AB DMA kapsamındaki Kendine Öncelik Verme (Self-Preferencing) Yasağı'na göre; Google gibi "gatekeeper" arama motorlarının, organik sonuçları baskılayacak şekilde, kendi alışveriş, uçuş veya yerel hizmetlerini arama sonuçlarında rakiplerinin üzerinde konumlandırması yasaktır.

Cusumano, arama motorlarının "tarafsız" olmadığını, ancak "şeffaf" olması gerektiğini savunur (Algoritmik Şeffaflık). Denetim otoritesi; arama sonuçlarını etkileyen, alakalılık (relevance), güvenilirlik (authority), güncellik (freshness) gibi ana parametrelerin kullanıcılara açıklanıp açıklanmadığını kontrol etmelidir.²³¹

Akademik perspektiften bir bakışla Grimmelmann, arama motorlarının "editöryal özgürlük" ile "kamusal altyapı" arasındaki ince çizgide durduğunu ve denetimin "manipülasyonu engellemek" ile sınırlı kalması gerektiğini vurgular.²³²

Geradin'in 2024 tarihli çalışması ile, şu iki temel hukuki ve ekonomik tespit desteklenmektedir:²³³

“Algoritmik Yönlendirme” ve “Gatekeeper” Davranışları kapsamında Geradin, AB DMA kapsamında belirlenen ilk “gatekeeper” (kapı eşiği) platformların (Google, Amazon, Apple vb.) arama sonuçlarında veya uygulama mağazalarında kendi yan hizmetlerini nasıl öne çıkardığını incelemektedir. Bu tür

²³⁰ Mökander, J. et al. (2024). *A.g.e.*

²³¹ Cusumano ve ark. (2021), *a.g.e.*

²³² Grimmelmann, J. (2024). “The Law of Search Engines: Governance and Neutrality”, Columbia Law Review.

²³³ Geradin, D. (2024). “Self-Preferencing in the Digital Age: Lessons from the first DMA designations”, Journal of European Competition Law.

davranışların pazarın "yarışılabilirliğini" (contestability) nasıl öldürdüğü anlatılırken bu güncel makaleye atıf yapılmıştır.

Geradin, DMA'nın Uygulama Pratiği kapsamında; Kendine Öncelik Verme (Self-Preferencing) gibi teorik yasakların pratikte platform arayüzlerine nasıl yansıdığını analiz etmiştir. Burada, denetim otoritesinin platform arayüzlerindeki "görsel hiyerarşiyi" denetlerken, dikkat etmesi gereken kriterler Geradin'in sunduğu "ilk uygulama dersleri" üzerinden kurgulanmıştır.

Bunlara ilaveten, arama motorlarının "tarafsızlık" ilkesinin, yayıncı haklarıyla nasıl çatıştığı ve Kanada'nın bu süreci "ticari tahkim" yoluyla nasıl çözmeyi hedeflediği örneği de oldukça dikkat çekicidir. Platformların; haber linklerini göstermek için ödeme yapmak yerine, bu linkleri platformdan kaldırma (link blocking) gibi "misilleme" (retaliation) risklerine karşı, Kanada'daki regülatörün (CRTC) müdahale yetkisi bulunmaktadır.²³⁴

7.5.2. Sosyal Ağlar: Algoritmik Kürasyon, Dezenformasyon ve Çocuk Koruma

Sosyal ağlar "dikkat ekonomisi" (attention economy) üzerine kuruludur. Buradaki denetim, içeriğin kendisinden ziyade, içeriği yayan "algoritmik yükseltme" (amplification) mekanizmalarına odaklanmalıdır.

AB DSA, sosyal ağların yasa dışı içerikleri (nefret söylemi, terörizm) kaldırmasının ötesinde; dezenformasyonun yayılmasını engelleyecek "sistemik risk azaltma" planları sunmasını şart koşar (Risk Temelli İçerik Moderasyonu).

İngiltere Online Safety Act (OSA), özen yükümlülüğü ve çocukların korunması kapsamında; sosyal ağlara çocukların ruh sağlığını bozabilecek (ancak teknik olarak yasa dışı olmayan) içeriklere karşı "yaş doğrulama" ve "tasarımsal güvenlik" (safety by design) yükümlülüğü getirir.²³⁵

TikTok ve Instagram 2025-2026 denetimlerinde, "sonsuz kaydırma" (infinite scroll) ve "beğeni" algoritmalarının bağımlılık yapıcı etkileri, AI Act kapsamında "yüksek riskli psikolojik müdahale" olarak değerlendirilmektedir.

Zuboff 2019 tarihli çalışmasında²³⁶ ve 2025 tarihli makalesinde²³⁷, sosyal ağların "davranışsal modifikasyon" kapasitesinin demokratik süreçler üzerindeki sistemik riskine dikkat çekerek, denetimin "veri madenciliği" aşamasında başlaması gerektiğini belirtir.

Bunun yanında, Floridi'nin çalışması²³⁸ ise, özellikle şu iki temel argümanı desteklemektedir:

²³⁴ **Government of Canada (2023).** *A.g.e. Bill C-18.*

²³⁵ **Ofcom UK (2025).** *Protecting Children from Online Harm: Codes of Practice for Social Media.*

²³⁶ **Zuboff, S. (2019):** *a.g.e.*

²³⁷ **Zuboff, S. (2025).** *"The New Frontiers of Behavioral Manipulation in Social Networks"*, Journal of Social Computing.

²³⁸ **Floridi, L. (2024).** *The Ethics of Algorithmic Curation in Social Media.* Springer.

Algoritmik kürasyon ve bilişsel özerklik kapsamındaki bu çalışma, sosyal ağlardaki algoritmaların sadece içerik sıralamadığını, aynı zamanda kullanıcının bilgiye erişim evrenini inşa ettiğini (kürasyon) savunur. Denetimin sadece "yasa dışı içeriği kaldırmak" ile sınırlı kalmaması, kullanıcının "**karar verme özerkliği**" koruyacak şekilde algoritmik şeffaflığı sağlaması gerektiği vurgulanmaktadır.

Etik denetim standartları düşünüldüğünde ise; algoritmaların "bağımlılık yapıcı" veya "kutuplaştırıcı" etkilerinin sadece teknik bir hata değil, bir **etik ihlal** olduğu temellendirilmektedir. Bu yüzden, denetim otoritesinin yapacağı "Algoritmik Etki Değerlendirmeleri" (AIA) için gerekli olan etik kriterler, Floridi'nin bu çalışmasından türetilmiştir.

7.5.3. E-Ticaret Platformları: Veri Çifte Rolü ve Hibrit Pazar Yönetimi

E-ticaret platformları hem bir "piyasa işletmecisi" hem de o piyasadaki bir "satıcı" (hibrit model) olarak faaliyet gösterirler. Bu "çifte rol" yapısal bir çıkar çatışması yaratır.

DMA Madde 6/2 ile, veri kullanım kısıtlamaları kapsamında; Amazon gibi platformların, piyasadaki üçüncü taraf satıcılardan elde ettiği (kime ne satılıyor, hangi fiyatta sunuluyor vb.) kamuya açık olmayan verileri, Amazon Basics gibi kendi markalı ürünlerini geliştirmek için kullanmasını yasaklanmıştır.

Karanlık Arayüzler (Dark Patterns) aracılığı ile, kullanıcıyı istemediği bir aboneliğe veya satın almaya zorlayan yanıltıcı tasarımlar, DSA'nın 25. maddesi ve Kanada Bill C-27 kapsamında yasaklanmıştır. Denetim otoritesi, platform arayüzlerinin "karar verme serbestisini" kısıtlayıp kısıtlamadığını test etmelidir.

DSA, e-ticaret platformlarına satıcıların kimliklerini doğrulama (KYBC: Know Your Business Customer) ve tedarik zincirinde yasa dışı ürün satışını engelleme sorumluluğu yükler. Bu, tüketici güvenliği için kritik bir "kapı bekçiliği" görevidir.

Bu konuda Khan, makalesinde e-ticaret devlerinin "bilgi asimetrisini" kullanarak rakiplerini nasıl oyun dışı bıraktığını ve yapısal ayrıştırmanın (structural separation) neden bir seçenek olması gerektiğini analiz eder.²³⁹

AB'nin 2026 tarihli güncel raporu²⁴⁰; özellikle kullanıcı arayüzlerinin psikolojik manipülasyon amaçlı kullanımı ve bu tasarımların denetimiyle ilgilidir. Burada şu üç kritik teknik analiz dikkat çekmektedir:

Karanlık Arayüzlerin (Dark Patterns) Tanımlanması: DSA'nın 25. maddesi uyarınca yasaklanan; kullanıcıların bilinçli karar verme yetisini zayıflatan "zorunlu süreklilik" (roach motel), "gizli maliyetler" ve "sahte aciliyet" (fake scarcity) gibi tasarım hilelerinin teknik kriterlerini belirlemek önemlidir.

²³⁹ Khan, L. M. (2025). "Platform Monopolies and Data Advantage: The Case for Structural Remedies", Yale Law Journal.

²⁴⁰ European Commission (2026). Guidance on the Prevention of Dark Patterns in E-Commerce Interfaces under the DSA.

Arayüz Denetim Metodolojisi: Denetim otoritesinin bir e-ticaret sitesini incelerken hangi tasarım öğelerini "ihlal" kabul edeceğine dair somut örnekler (örneğin: abonelikten çıkma butonunun, üye olma butonuna göre çok daha küçük veya gizli tasarlanması) dikkat çekmektedir.

Tüketici Özerkliği ve "Default" Ayarlar: Varsayılan (default) ayarların kullanıcıyı harcamaya teşvik edecek şekilde manipüle edilmesi "sistemik bir risk" olarak ele alınmaktadır.

E-ticaret platformlarının yapısal özelliklerinin ve veri kullanım stratejilerinin analiz edildiği OECD raporuna göre ise²⁴¹;

Hibrit Model ve Çıkar Çatışması: Bir platformun hem "piyasa işletmecisi" (pazar kurallarını koyan) hem de o piyasada "satıcı" (diğer satıcılarla rekabet eden) olmasının yarattığı yapısal bir çıkar çatışmasını doğurmaktadır. Rapordaki "**Veri Çifte Rolü**" vurgusu bu hususa dayanmaktadır.

Veri Avantajı ve Bilgi Asimetrisi: Platformun üçüncü taraf satıcılardan elde ettiği işlem verilerini (hangi ürünlerin popüler olduğu, hangi fiyat aralığının tercih edildiği vb.) kullanarak kendi markalı ürünlerini (private label) nasıl avantajlı konuma getirdiği bilimsel olarak açıklanır. Raporda, Amazon ve benzeri devlerin bu veri stratejilerinin rekabeti nasıl bozduğuna dair yapılan analizde bu çalışmaya atıf yapılmıştır.

Algoritmik Yönlendirme ve "Buy Box" Denetimi: E-ticaret platformlarındaki "satın alma kutusu" (Buy Box) veya "tavsiye edilen ürünler" listesinin algoritma tarafından nasıl belirlendiği incelenir. Platformların bu algoritmaları kendi ürünlerine öncelik verecek (self-preferencing) şekilde tasarlayıp tasarlamadığının denetlenmesi gerektiği raporun sunduğu "veri odaklı rekabet" çerçevesiyle detaylandırılmıştır.

E-ticaret platformları sadece bir "piyasa alanı" değil, aynı zamanda "kritik birer dijital altyapı" olarak ele alınmaktadır. Brous, P., & Janssen, M.'nın 2024 tarihli çalışmalarına göre, şu iki stratejik noktayı temellendirmek mümkündür²⁴²:

Süreklilik ve Tedarik Zinciri Güvenliği: NIS2 çerçevesindeki analiz, bir e-ticaret devinin siber saldırıya uğramasının sadece veri sızıntısı değil, lojistik ve ödeme sistemleri üzerinden "ekonomik bir duraksama" yaratacağını savunur. E-ticaret platformlarına getirilen "siber risk yönetimi" yükümlülüğü bu çalışmaya atfedilmektedir.

Sistemik Sökülme (Systemic Collapse) Riski: Platformların alt yüklenicileri ve satıcıları arasındaki dijital bağların yarattığı siber riskler incelenmiştir. E-ticaret platformlarının NIS2 kapsamında "operasyonel süreklilik" planları hazırlaması yasal bir zorunluluktur ve çalışmada geçen "siber dayanıklılık" (cyber-resilience) modeli esas alınmıştır.

²⁴¹ OECD (2024). *E-commerce and Competition: Data Strategies of Hybrid Platforms*. OECD Digital Economy Papers.

²⁴² Brous, P., & Janssen, M. (2024). *Siber Dayanıklılık ve E-Ticaret Altyapıları: NIS2 Uygulaması*.

Kanada Innovasyon Bakanlığı'nın 2025 tarihli raporu²⁴³, şu iki stratejik teknik analizi temellendirmek için kullanılmıştır:

Algoritmik Önyargı ve Ayrımcılık Denetimi: Kanada Yapay Zekâ ve Veri Yasası (AIDA), sosyal ağlardaki tavsiye algoritmalarının (recommender systems) kullanıcıları "yankı odalarına" (echo chambers) hapsedme veya belirli demografik gruplara karşı önyargılı içerik sunma riskini tanımlar. Denetim otoritesinin yapacağı "algoritmik etki değerlendirmeleri" için Kanada'nın sunduğu bu **etik kontrol listesi** (checklist) temel bir metodoloji olarak sunulmuştur.

Kullanıcı Deneyimi ve Şeffaflık: Kullanıcıların bir içeriği "neden gördüklerini" anlama hakkını ve bu algoritmik kararlara müdahale etme (opt-out) seçenekleri teknik standartlara bağlanmıştır. Sosyal ağların "tasarımsal şeffaflık" yükümlülükleri kapsamında, Kanada modelinin sunduğu kullanıcı odaklı yaklaşım, AB DSA'yı tamamlayıcı bir unsur olarak kullanılmıştır.

7.5.4. Denetim Stratejileri ve Teknik Uygulama

Denetimin teoriden pratiğe döküldüğü ve otoritenin teknik müdahale yöntemlerinin tartışıldığı Mökander, J. ve arkadaşlarının raporuna göre²⁴⁴, şu iki kritik uygulama stratejisi temellendirilmiştir:

Denetim Alanları (Regulatory Sandboxes): Yazarlar, AB DSA kapsamında oluşturulan "denetim kum havuzları" (sandboxes) üzerinden elde edilen ilk verileri analiz ederler.

Algoritmik Denetimin Sınırları ve Metodolojisi: Mökander ve arkadaşları, algoritmaların sadece "kod" üzerinden değil, "çıktılar" (outputs) ve "sosyal etkiler" üzerinden denetlenmesi gerektiğini savunur. Ayrıca, bu bölümde zikredilen "API Erişimi ve Veri Denetimi" stratejisi, sözkonusu makalede sunulan "algoritmik hesap verebilirlik matrisi" üzerinden kurgulanmıştır.

Etkin bir uygulama için otoriteler şu yöntemleri kullanmalıdır:

Mystery Shopping (Gizli Müşteri): E-ticaret ve arama motorlarında algoritma tarafsızlığını ölçmek için anonim testler öne sürülür.

API Erişimi ve Veri Denetimi: DSA Madde 31 uyarınca, araştırmacıların ve otoritenin platformun "iç işleyiş verilerine" erişmesi gerekmektedir.

Algoritmik Etki Değerlendirmesi (AIA): Platformun yeni bir özelliği devreye almadan önce bunun siber güvenlik (NIS2) ve etik (AI Act) risklerini raporlaması önem arz etmektedir.

²⁴³ Canadian Ministry of Innovation (2025). *AIDA: Ethical Guidelines for Recommender Systems in Social Networks*.

²⁴⁴ Mökander, J. et al. (2024). *Algorithm Auditing in Practice: Lessons from the DSA Sandbox*, AI & Society.

7.6. Yaptırım Rejimi ve Caydırıcılık: Etkin Uygulama Mekanizmaları

Dijital ekonomide regülasyonun başarısı, ihlalin maliyetinin, ihlalden elde edilen muhtemel kazançtan (expected utility) daha yüksek olmasına bağlıdır. Geleneksel hukukta yer alan "tazmin edici" mantık, trilyon dolarlık platformlar karşısında caydırıcı olamamaktadır. Bu nedenle, yeni nesil yaptırım rejimi; **finansal, davranışsal ve yapısal** olmak üzere üç katmanlı bir müdahale setini esas almalıdır.

7.6.1. Kademeli Para Cezaları ve Ekonomik Caydırıcılık Teorisi

Dijital platformların devasa nakit akışları göz önüne alındığında, maktu (sabit) para cezaları "iş yapma maliyeti" (cost of doing business) olarak görülmektedir. Caffarra & Morton (2024), cezaların "maliyet-fayda analizini" platformlar aleyhine çevirecek bir eşikte olması gerektiğini vurgular.²⁴⁵

Küresel Ciro Bazlı Cezalandırma: AB DSA kapsamında, yükümlülüklerin ihlali durumunda platformun bir önceki mali yılına ait toplam küresel cirosunun **%6'sına** kadar para cezası öngörülür. DMA'da ise bu oran sistematik ihlallerde **%10'a**, tekrarı halinde (mükerrerlik) **%20'ye** kadar yükseltilmiştir. Bu, sadece bir ceza değil, şirketin borsa değerini ve yatırımcı güvenini doğrudan etkileyen bir "piyasa sinyali"dir.

Günlük Periyodik Cezalar (Astraint): İhlalin devam ettiği her gün için günlük ortalama cironun **%5'ine** kadar gecikme cezaları uygulanır. Bu mekanizma, platformun uyum sürecini (remediation) hızlandırmak için bir "zorlama aracı" (coercive instrument) olarak kullanılır.

SMS Statüsü ve İngiltere Modeli: UK DMCC Act 2024 uyarınca, Stratejik Pazar Statüsü (SMS) atanan şirketler, "Davranış Standartlarını" ihlal ettiklerinde sadece para cezasıyla değil, doğrudan tazminat yükümlülükleriyle de karşı karşıya kalırlar. G7 Inventory (2023), bu tür ciro bazlı cezaların küresel bir standart haline geldiğini teyit etmektedir.

AB Komisyonu'nun Çok Büyük Çevrim içi Platformlara (VLOPs) yönelik uyguladığı ilk ciddi yaptırım dalgasının sonuçlarını içeren ve ciro bazlı cezaların sembolik olmaktan çıkıp, platformlar için gerçek bir finansal risk etkisini gösteren Avrupa Komisyonu raporuna göre; 2024 ve 2025 yıllarında başlatılan soruşturmalar neticesinde VLOP'lara kesilen cezaların, bu şirketlerin borsa değerleri ve uyum bütçeleri üzerindeki somut etkisini verilerle kanıtlanmıştır.²⁴⁶

Cezaların miktarının belirlenmesinde kullanılan "ekonomik rasyonellik" modellerini temellendiren OECD'nin 2024 tarihli raporu; dijital pazarlarda "ihlalden elde edilen beklenen kazancın" (expected gain), ceza miktarından düşük olması gerektiğini matematiksel olarak modeller. Raporda, para cezalarının sadece geçmiş cezalandırmakla kalmayıp, gelecekteki olası ihlalleri önleyecek bir "caydırıcılık eşiği" (deterrence

²⁴⁵ Caffarra, C., & Morton, F. S. (2024). *"The Economics of Enforcement under the DMA"*, Yale University School of Management.

²⁴⁶ European Commission (2026). *Implementation Report on VLOPs Sanctions under the DSA*.

threshold) oluşturması gerektiği vurgulanmaktadır. Ayrıca, ciro bazlı cezaların küresel bir standart haline gelmesinin ardındaki ekonomik gerekçeler bu çalışma üzerinden açıklanmıştır.²⁴⁷

7.6.2. Davranışsal Tedbirler: Süreç ve Tasarım Odaklı Müdahaleler

Para cezaları geçmişteki ihlali cezalandırırken, davranışsal tedbirler gelecekteki ihlalleri durdurmayı amaçlar. Scott & Yeung (2025), dijital ekosistemde "algoritmik hesap verebilirliğin" ancak operasyonel müdahalelerle sağlanabileceğini savunur.²⁴⁸

Algoritma Değişikliği ve Tasarımsal Uyum: Otorite, bir algoritmanın (örneğin e-ticaretteki sıralama algoritması veya sosyal ağdaki tavsiye motoru) sistemik risk yarattığını tespit ederse, algoritmanın temel parametrelerinin (weights) değiştirilmesini veya belirli özelliklerin (sonsuz kaydırma, dark patterns) tamamen kaldırılmasını emredebilir.

Komisyonun 2026 tarihli bu raporu, platformların para cezası ödemek yerine sistemlerinde yaptıkları "tasarımsal iyileştirmeleri" (remedy tracking) detaylandırmaktadır. Rapor aynı zamanda, otorite tarafından zorunlu kılınan "algoritma değişikliği" ve "karanlık arayüzlerin kaldırılması" gibi davranışsal emirlerin, platformlar tarafından ne oranda ve ne kadar sürede hayata geçirildiğini analiz etmektedir. Ayrıca, raporda "davranışsal tedbirlerin platformların kurumsal DNA'sını değiştirmedeki etkinliği" tartışılmış ve bu rapordaki "iyileştirme oranları" ve "mükerrer ihlal analizleri" temel referans alınmıştır.²⁴⁹

Bağımsız Denetim ve Veri Erişimi: Platformun kendi beyanları yerine, otorite tarafından onaylanmış bağımsız üçüncü taraf denetçilerce (independent auditors) hazırlanan yıllık "Uyum Raporları" zorunlu kılınır. Mökander vd. (2024), bu denetçilerin "kamu yararı" adına hareket eden geçici memurlar gibi yetkilendirilmesi gerektiğini belirtir.²⁵⁰

Uyum Taahhütleri (Commitments): Otorite, bir soruşturmayı kapatmak karşılığında platformdan bağlayıcı taahhütler alabilir. Bu taahhütlerin ihlali, doğrudan en üst sınırdaki para cezası ve faaliyet durdurma riskini doğurur.

7.6.3. Yapısal Tedbirler

Davranışsal ve finansal yaptırımların sonuç vermediği, platformun gücünü sistematik olarak kötüye kullandığı durumlarda "son çare" (ultima ratio) olarak yapısal müdahaleler devreye girer.

²⁴⁷ OECD (2024). *Design of Enforcement and Sanctions in Digital Markets*. OECD Digital Economy Papers.

²⁴⁸ Scott, C., & Yeung, K. (2025). *A.g.e.*

²⁴⁹ European Commission (2026). *Implementation ... a.g.e.*

²⁵⁰ Mökander, J. et al. (2024). *A.g.e.*

Mülkiyet hakkı ve teşebbüs hürriyeti ile kamu yararı (rekabetin korunması) arasındaki dengenin, yapısal tedbirler bağlamında nasıl kurulması gerektiğini açıklayan Monti, G. ve Colomo, P.I.'ın savunduğu üzere; yapısal müdahalelerin ancak davranışsal tedbirlerin (behavioral remedies) sonuç vermediği kanıtlandığında uygulanabileceği, yani bu yetkinin bir "son çare" (**ultima ratio**) olması gerektiğini belirtmişlerdir.²⁵¹

İş Birimi Elden Çıkarma (Divestiture): AB DMA (Madde 18) ve İngiltere DMCC 2024, sistematik ihlalcilerin belirli iş birimlerini (örneğin reklam teknolojisi birimi ile içerik biriminin ayrılması) elden çıkarmasını emretme yetkisini regülatöre tanır.

Veri Ayırıştırması (Data Siloing): Platformun farklı servislerinden (örneğin WhatsApp ve Facebook) gelen verileri birleştirmesi tamamen yasaklanabilir ve bu servislerin veri havuzları fiziksel ve mantıksal olarak birbirinden ayrılabilir.

Akademik Tartışmalar:

Khan (2025), "Platform Monopolies" çalışmasında, davranışsal tedbirlerin platformlar tarafından "yaratıcı uyum" (creative compliance) ile delindiğini, bu nedenle yapısal ayırıştırmanın (structural separation) rekabeti geri getirmek için tek kalıcı çözüm olduğunu savunur.²⁵²

Geradin (2024), platformlara sadece "kendine öncelik verme" (self-preferencing) yasağı getirmenin (yani davranışsal bir emir vermenin) denetlenmesinin ne kadar zor olduğunu ortaya koyar. Platformların algoritmik yapılarını çok küçük dokunuşlarla değiştirerek yasağın etrafından dolanabileceğini (creative compliance) ve otoritenin bunu her an takip etmesinin mümkün olmadığını savunan çalışma, davranışsal yaptırımların "sürekli bir kedi-fare oyunu" yarattığına dair bir analiz yapmıştır.²⁵³

Sözkonusu Geradin makalesi, davranışsal tedbirlerin sınırlarına ulaşıldığında, tek gerçek çözümün mülkiyetin veya operasyonel birimlerin ayrılması (yapısal tedbirler) olduğunu savunur. Yapısal tedbirlerin (structural separation) neden sadece "cezalandırıcı" değil, aynı zamanda "piyasayı iyileştirici" bir araç olduğunu açıklayan bu makalede, "yapısal müdahale, denetim maliyetini düşüren ve adil rekabeti kalıcı kılan tek yoldur" argümanı Geradin'in bu güncel içtihat analizinden türetilmiştir.

7.7. Hukuki Çözüm Mekanizmaları

Dijital platformların düzenlenmesinde etkin uygulama kadar, bu uygulamanın adil bir yargısal denetimden geçmesi ve paydaşların (kullanıcılar ve ticari kullanıcılar) hızlı hak arama yollarına sahip olması, hukukun üstünlüğü ilkesinin bir gereğidir. Geleneksel yargılama usullerinin dijital dünyanın hızına yetişememesi, "yeni nesil çözüm mekanizmalarını" zorunlu kılmıştır.

²⁵¹ Monti, G., & Colomo, P. I. (2025). *A.g.e*

²⁵² Khan, L. M. (2025). *A.g.e*.

²⁵³ Geradin, D. (2024). *A.g.e*.

7.7.1. İdari İtiraz Yolları ve Yargısal Denetim (Judicial Review)

Otorite tarafından verilen kararların (para cezaları, davranışsal emirler) yargısal denetimi, keyfiyetin önlenmesi için kritiktir.

Ön İtiraz Mekanizmaları: AB DMA ve DSA kapsamında, platformların otoritenin kararlarına karşı öncelikle idari bir "itiraz süreci" (internal review) yürütmesi öngörülür. Bu, idarenin kendi hatasını düzeltmesi için bir fırsat sunar.

Geradin (2024), DMA gibi devasa regülasyonların uygulanmasında, sadece Brüksel'deki merkezi yapının yeterli olmayacağını, yerel ve ulusal mahkemelerin (National Courts) platform ihlallerine karşı doğrudan müdahale ve tazminat süreçlerinde kilit rol oynayacağını savunur.²⁵⁴

Ayrıca, ulusal mahkemelerin kararları ile düzenleyici otoritenin kararları arasındaki "çelişki" riskini de analiz eden Geradin; yargısal denetimin etkinliği için "mahkemeler ile regülatör kurumlar" arasındaki bilgi paylaşımının ve hukuki tutarlılığın önemini vurgularken "**hukuki eşgüdüm**" modelini de bu çalışma ile sunmaktadır.

Monti & Colomo (2025), dijital regülasyon kararlarının denetiminin "genel idari mahkemelerden" ziyade, teknik ve ekonomik karmaşıklığı anlayabilecek "uzmanlaşmış yargı heyetleri" (İngiltere'deki CAT- Competition Appeal Tribunal gibi) tarafından yapılması gerektiğini savunur.²⁵⁵

Scott & Yeung (2025), "algoritmik kararların yargısal denetimi" konusunda mahkemelerin sadece hukuki uygunluğa değil, algoritmanın "teknik rasyonelliğine" de bakması gerektiğini belirtir.²⁵⁶

7.7.2. Alternatif Uyuşmazlık Çözüm (Alternative Dispute Resolution) Yolları

Milyarlarca içerik kaldırma veya hesap askıya alma kararı göz önüne alındığında, her uyuşmazlığın mahkemeye taşınması sistemi kilitler.

ADR (Alternative Dispute Resolution) Kurulları (Out-of-court Dispute Settlement): AB DSA Madde 21, kullanıcılara platformların içerik kaldırma veya hesap askıya alma kararlarına karşı; bağımsız, şeffaf, hızlı ve düşük maliyetli "Yargı Dışı Çözüm Kurullarına" başvurma hakkı tanır. Bu, mahkemelerin hantallığını aşan bir "dijital adalet" mekanizmasıdır. Platformlar, bu kuralların kararlarını kural olarak kabul etmek ve uyum sağlamak zorundadır.²⁵⁷

²⁵⁴ Geradin, D. (2024). "Adjudicating the DMA: The Role of National Courts", Journal of European Competition Law.

²⁵⁵ Monti, G., & Colomo, P. I. (2025). *The Interplay of Digital Regulation and Competition Law*. Oxford University Press.

²⁵⁶ Scott, C., & Yeung, K. (2025). *A.g.e.*

²⁵⁷ European Commission (2026). *Implementation Report on ADR Centers under the Digital Services Act*.

Zorunlu Tahkim (Kanada Örneği): Kanada Online News Act (Bill C-18), platformlar ile haber yayıncıları arasındaki telif uyuşmazlıklarını çözmek için "Final Offer Arbitration" (Nihai Teklif Tahkimi) modelini benimsemiştir. Bu model, tarafları orta yolda buluşmaya zorlayan en hızlı çözüm yoludur.

Quinn Emanuel (2025) analizi, AB'de 2024 sonrasında kurulan ADR merkezlerinin, uyuşmazlıkları ortalama 45 günde çözerek yargı yükünü %60 oranında hafiflettiğini ortaya koymaktadır.²⁵⁸

OECD'nin 2024 tarihli raporu, yaptırım süreçlerinin ne kadar hızlı (speed of enforcement) ve ne kadar az maliyetli olması gerektiğine dair bir "tasarım rehberi" sunar. Raporda ayrıca, yargı dışı çözüm yollarının (ADR) ve uzlaşma (settlement) mekanizmalarının, klasik dava süreçlerine göre neden daha "etkin" bir yaptırım aracı olduğunu savunulmaktadır. Otoritelerin sınırlı kaynaklarını en verimli şekilde kullanabilmesi için "kategorik yaptırım" modellerinin benimsenmesi gerektiği önerisi bu kaynağın sonuç raporuna dayandırılmıştır.²⁵⁹

7.7.3. Kolektif Hak Arama (Sınıf Davaları) ve Tazminat Hakları

Platformlar karşısında tek başına duramayan bireysel kullanıcılar için "birlikten doğan güç" ilkesi hukuki bir korumaya dönüşmüştür. Tüketici derneklerinin veya sivil toplum kuruluşlarının, veri ihlali veya haksız ticari uygulama mağduru binlerce kullanıcı adına devasa "temsilci davaları" açabilmesi sağlanmalıdır. Quinn Emanuel (2025), bu tür toplu davaların platformlar üzerinde "varoluşsal bir finansal risk" yaratarak caydırıcılığı maksimize ettiğini belirtir.²⁶⁰

Bütünleşik Tazminat Yolları: AB Tüketici Temsilci Davaları Direktifi ve DSA'nın ilgili maddeleri, sivil toplum kuruluşlarının (STK) binlerce mağdur kullanıcı adına "toplu tazminat" davası açmasına izin verir.

Tazminat rejiminin küreselleşmesi adına, Bradford'un "Brüksel Etkisi" teorisi çerçevesinde, AB'nin tüketici koruma ve dijital tazminat standartlarının (örneğin Temsilci Davaları Direktifi), AB dışında faaliyet gösteren platformları da bu standartlara uyum sağlamaya zorladığı vurgulanmıştır.²⁶¹

Sözkonusu "Brüksel Etkisi" teorisi, AB'nin bireysel hak arama yollarını "toplu dava" mekanizmalarıyla güçlendirmesinin, platformlar üzerindeki hukuki baskıyı küresel ölçekte artırdığını savunur. Platformların "sistemik zararları" için öngörülen toplu tazminat yollarının, sadece Avrupa'da değil tüm dünyada bir norm haline gelmeye başladığı belirtilmektedir.

²⁵⁸ Quinn Emanuel (2025). *Digital Litigation Trends: The Rise of Out-of-Court Dispute Settlements under the DSA*.

²⁵⁹ OECD (2024). *Design of ... A.g.e.*

²⁶⁰ Quinn Emanuel (2025), *a.g.e.*

²⁶¹ Bradford, A. (2023). *A.g.e.*

Sorumluluk Rejiminin Genişlemesi: İngiltere Online Safety Act (OSA), platformların "Özen Yükümlülüğü"nü (Duty of Care) ihlal etmeleri durumunda, bireylerin uğradığı psikolojik zararların da tazminat konusu olabileceği bir kapı açmıştır.²⁶²

Kanada'nın haber ekosistemi için getirdiği "zorunlu tahkim" (final offer arbitration) modeli, platformların içerik sağlayıcılarla adil pazarlık yapmaması durumunda bağlayıcı bir çözüm sunar.

Zuboff (2025), bireysel rızanın ötesinde, platformların toplumsal düzeyde yarattığı "sistemik zararların" ancak kolektif davalarla telafi edilebileceğini ve bu davaların platformların iş modellerini değiştirmeleri için en büyük baskı unsuru olduğunu savunur.²⁶³

Monti ve Colomo'nun çalışması ise, dijital regülasyonlar (DSA ve DMA gibi) ile klasik rekabet hukukunun yaptırım süreçlerinde nasıl iç içe geçtiğini (interplay) inceler. Bu çalışma, farklı otoritelerin (örneğin bir veri koruma otoritesi ile bir rekabet kurumunun) aynı eyleme farklı yaptırımlar uygulamasından doğabilecek "çifte cezalandırma" (ne bis in idem) riskini ve bu riskin hukuki çözüm yollarını tartışırken, ayrıca regülasyonların uygulanmasında "hukuki öngörülebilirlik" ve "tutarlılık" prensiplerinin yaptırım rejiminin meşruiyeti için neden şart olduğunu vurgulamıştır.²⁶⁴

Sonuç olarak, platformlar için "cezayı göze alıp ihlale devam etme" (pay-to-pollute) modeli sona erdirilmelidir. Kademeli yaptırım yapısı, dürüst oyuncular için yol gösterici bir "uyum rehberi" iken, sistemik ihlalciler için operasyonel varlığı tehdit eden bir "disiplin aracı" işlevi görür.

7.7.4. Algoritmik Kararlara Karşı "İnsan Müdahalesi" ve İtiraz Hakkı

Hukuki çözüm mekanizmalarının en teknik kısmı, yapay zekâ tarafından alınan kararlara (AI-driven decisions) itirazdır.

AI Act ve Açıklanabilirlik: AB AI Act, yüksek riskli sistemlerin kararlarından etkilenen kişilere "anlaşılabilir bir açıklama" alma hakkı tanır. Bu, platformun "algoritma öyle istedi" savunmasını hukuken geçersiz kılar.

İnsan Gözetimi (Human-in-the-loop): Kanada AIDA ve AB düzenlemeleri, otomatik kararlara karşı mutlaka "insan tarafından yapılacak bir inceleme" (human review) yolunun açık tutulmasını şart koşar.

Bağımsız denetim ve hukuki başvuru (Legal Redress) kapsamında; Mökander ve ekibi, bir algoritmanın haksız bir karar (örneğin sosyal ağda sebepsiz içerik kaldırma veya e-ticarette haksız sıralama düşürme) vermesi durumunda, mahkemelerin bu kararı denetleyebilecek teknik kapasiteye sahip olmadığını savunur.

²⁶² UK Parliament (2024). *Digital Markets, Competition and Consumers Act 2024: Appeal Mechanisms*.

²⁶³ Zuboff, S. (2025). "Collective Redress as a Check on Surveillance Capitalism", *Journal of Digital Rights*.

²⁶⁴ Monti, G., & Colomo, P. I. (2025). *A.g.e*

Ayrıca, bu noktada devreye girmesi gereken "bağımsız denetim kuruluşlarının" (independent auditing bodies), yargısal süreçlerde birer "teknik hakem" veya "bilirkişi" olarak rol alması gerekmektedir.²⁶⁵

Mökander ve ekibi, Yapay Zekâ denetiminde "İnsan Gözetimi" standartları göz önüne alındığında; AI Act ve benzeri regülasyonların öngördüğü "insan müdahalesi" (human review) hakkının, sadece şekli bir prosedür değil, teknik bir "hesap verebilirlik" (accountability) mekanizması olduğunu belirtmektedir. Kullanıcının itirazı üzerine yapılan incelemenin hangi teknik standartlara (veri kalitesi, önyargı analizi vb.) göre yapılması gerektiği Mökander'in sunduğu bu metodolojik çerçeve ile açıklanmıştır.

Floridi (2024), dijital adaletin sadece "hızlı" değil, aynı zamanda "anlamli" (meaningful accountability) olması gerektiğini, bunun da teknik kararların hukuki dille tercüme edilmesinden geçtiğini belirtir.²⁶⁶

7.8. Türkiye İçin Geleceğe Hazır Regülasyon Tasarımı

Dijital ekonominin dinamizmi, statik hukuk kurallarını hızla işlevsiz kılmaktadır. Türkiye için önerilen regülasyon mimarisi, sadece bugünün "kapı eşiği" platformlarını denetlemeyi değil, aynı zamanda Web3, Metaverse ve üretken yapay zekâ (GenAI) gibi yarının teknolojilerine de uyum sağlayabilecek esneklikte olmalıdır.

7.8.1. Kurumsal Mimari Önerisi: "Dijital Ekosistem Düzenleme Kurulu"

Türkiye'deki parçalı yapı (BTK, Rekabet Kurumu, KVKK) yerine, İngiltere'deki DRCF modelinden ilham alan ancak daha icracı bir eşgüdüm mekanizması kurulmalıdır.

De Streel (2024), dijital piyasalarda rekabet ve veri korumanın birbirinden ayrılamayacağını savunur. Türkiye, **Bütünleşik Denetim Modeli** olarak adlandırılacak bir modelle, bu kurumların uzmanlarını bir araya getiren "Dijital Ekosistem Düzenleme Kurulu"nu tesis etmelidir. Bu kurul, platformlara yönelik "tek durak ofis" (one-stop-shop) hizmeti sunarak regülasyon yükünü azaltırken denetim etkinliğini artıracaktır.²⁶⁷

Mökander vd. (2024), algoritmik denetimin hukukçulardan ziyade veri bilimciler tarafından yapılması gerektiğini belirtir. Kurul bünyesinde; platformların algoritmalarına, DSA kapsamında oluşturulan "kum havuzu" gibi, "denetim kum havuzu" (sandbox) ortamında erişebilecek teknik birimler oluşturulmalıdır.²⁶⁸

²⁶⁵ Mökander, J. et al. (2024). "Auditing AI: The Role of Independent Bodies in Legal Redress", AI & Society.

²⁶⁶ Floridi, L. (2024). *The Ethics of Artificial Intelligence*. A.g.e.

²⁶⁷ De Streel, A. (2024). A.g.e.

²⁶⁸ Mökander, J. et al. (2024). A.g.e.

Türkiye gibi ülkelerin yeni nesil algoritmik denetimlere geçerken, platformlarla kontrollü bir ortamda teknik testler yapması (sandbox uygulaması) gerekmektedir.



ŞEKİL 7-1: Türkiye Durum Analizi (YZ ile hazırlanmıştır)

7.8.2. Geleceğe Hazır (Future-Proof) Regülasyon Prensipleri

Statik kanunlar yerine, gelişen teknolojiye göre güncellenebilen "ikincil düzenlemeler" ve "davranış rehberleri" (codes of conduct) esas alınmalıdır.

Teknoloji Nötrlüğü: Düzenlemeler belirli bir yazılım veya donanıma değil, "fonksiyona" odaklanmalıdır. Floridi (2024), regülasyonun "platformun ismine" değil, "platformun yarattığı sistematik etkiye" bakması gerektiğini vurgular.²⁶⁹

SMS (Stratejik Pazar Statüsü) Yaklaşımı: AB DMA'nın katı "eşik değer" mantığı yerine, İngiltere DMCC 2024 yasasındaki SMS modeli benimsenmelidir. Bu model, Türkiye pazarında kritik öneme sahip yerel platformları da kapsayacak şekilde "stratejik bağımlılık" analizi üzerinden kurgulanmalıdır.

Esnek ve Cevap Veren (Responsive) Regülasyon: Scott & Yeung (2025), "öğrenen regülasyon" modelini önermektedir. Türkiye, altı aylık periyotlarla teknolojik trendleri analiz eden ve mevzuatı buna göre revize eden bir "Etki Değerlendirme Mekanizması" kurmalıdır.²⁷⁰

Monti ve Colomo (2025), mahkemelerin sadece mevcut kanunları değil, hızla değişen teknolojik standartları da dikkate alan bir "dinamik yorum" (dynamic interpretation) geliştirmesi gerektiğini

²⁶⁹ Floridi, L. (2024). *The Ethics of Artificial Intelligence*. A.g.e.

²⁷⁰ Scott, C., & Yeung, K. (2025). A.g.e.

savunmaktadır.²⁷¹ Buna ilaveten, yargının teknolojik gelişmelere ayak uydurabilmesi için gerekli olan "hukuki esneklik" ve "uzman hakemlik" önerileri de bu çalışmada yer almaktadır.

7.8.3. Türkiye İçin Öneriler

Türkiye'nin dijital egemenliğini korurken aynı zamanda inovasyonu teşvik etmesi için şu hukuki ve teknik adımların atılabileceği düşünülmüştür:

1. Türkiye'nin kendi yasal mevzuatını oluştururken hangi "iyi uygulamayı" hangi oranda ithal etmesi gerektiğine dair mevzuata baktığımızda; AB'nin DMA ve DSA gibi katı kuralları ve "yapısal sağlamlığı", İngiltere'nin "özen yükümlülüğü" ve "operasyonel esnekliği" ve Kanada'nın "veriye dayalı çevikliği" ile OECD'nin bakış açısının bir sentezi ile oluşturulacak hibrit bir "model"i Türkiye için en ideal ve rasyonel öneri olduğu değerlendirilmektedir.
2. Çoklu regülatör yapısına sahip ülkemiz; BTK, Rekabet Kurumu ve KVKK arasındaki işbirliğini "protokol" düzeyinden çıkarıp "sürekli bir koordinasyon forumu" (DRCF benzeri) düzeyine taşıma önerisini değerlendirmelidir. Ayrıca, BTK'nin teknik altyapı yetkisi, Rekabet Kurumu'nun piyasa gözetimi ve KVKK'nın veri mahremiyeti odaklı perspektifinin "eşgüdümlü bir yaptırım rejimi" altında birleştirilmesi uygun olacaktır.
3. BDDK ve TCMB'nin kurup uyguladığı finans alanı ile BTK'nin regüle ettiği haberleşme alanındaki mevcut sektörel uzmanlık ile genel platform regülasyonunun da sentezlenmesi konusunun değerlendirilmesinde yarar vardır.
4. Rekabet Kurumu'nun "Veri Taşınabilirliği" kararları ile KVKK'nın "Veri Güvenliği" standartlarının çelişmemesi için bağlayıcı iş birliği protokolleri elzemdir. Rekabet Kurumu ve KVKK arasındaki protokollerin sadece yerel bir ihtiyaç değil, G7 ülkelerinin (ABD, İngiltere, Japonya vb.) üzerinde mutabık kaldığı bir "yönetişim zorunluluğu" olduğu da unutulmamalıdır.
5. **Veri Lokalizasyonu ve Taşınabilirliği:** Zuboff (2025)'in vurguladığı "veri mülkiyeti" sorunu, kullanıcıların verilerini bir platformdan diğerine (interoperability) gerçek zamanlı taşıyabildiği teknik altyapı ile çözülmelidir.²⁷²
6. **Yatırım Dostu Denetim:** Regülasyon, yerli girişimlerin (start-up) büyümesini engellememeli, aksine dev platformların "yıkıcı devralmalarını" (killer acquisitions) engelleyerek yerli ekosisteme alan açmalıdır. Geradin (2024), denetimin "inovasyon dostu" (innovation-friendly enforcement) olması gerektiğini savunur.²⁷³
7. **Kolektif Hak Arama Reformu:** Bradford (2023)'un "Brüksel Etkisi" analizinde belirttiği gibi, bireyler platform devleri karşısında zayıftır. Türk Borçlar Kanunu ve Tüketici Kanunu'nda yapılacak değişikliklerle, dijital zararlar için "temsilci davası" (class action) yolu açılmalıdır.²⁷⁴ Ayrıca, bu konu özelinde tazminat hukukumuzu geliştirirken "Brüksel Etkisi" analizi ve benzeri örnekler de incelenmeli ve değerlendirilmelidir.

²⁷¹ Monti, G., & Colomo, P. I. (2025). *The Future of Digital Adjudication*.

²⁷² Zuboff, S. (2019): *a.g.e.*

²⁷³ Geradin, D. (2024). "Innovation-Friendly Enforcement of Digital Acts", *Journal of European Competition Law*.

²⁷⁴ Bradford, A. (2023). *A.g.e.*

8. Türkiye'deki mahkemelerin, karmaşık algoritmik ve ekonomik analiz içeren platform kararlarını denetlerken "teknik yargılama" (technical adjudication) kapasitesini geliştirmesi gerekmektedir. Burada Monti ve Colomo (2025) çalışması kaynak olarak alınabilir. Bu çalışma, dijital platform kararlarının klasik idari yargı süreçlerinde tıkanmaması için "Uzmanlaşmış Yargılama" (Specialized Adjudication) modelini savunur. Ayrıca, otorite kararlarının hızla kesinleşmesi ve dijital pazarın belirsizlikten kurtulması için "yargısal reformun" regülasyonun ayrılmaz bir parçası olduğu da bu çalışmada yer almaktadır.²⁷⁵
9. Bunlara ilaveten; İngiltere'deki CAT (Competition Appeal Tribunal) gibi, dijital regülasyon kararlarının denetiminin "genel idari mahkemelerden" ziyade, teknik ve ekonomik karmaşıklığı anlayabilecek "uzmanlaşmış yargı heyetleri" tarafından yapılması gerekliliğinden hareketle, ülkemiz de kendi yerel mahkemelerini dijital platform uyumsuzlukları konusunda yetkilendirmeli ve bu mahkemelerin "uzmanlaşmış" bir yapıya kavuşması durumunu değerlendirmelidir.
10. Türkiye, Küresel İşbirliği ve Standart Belirleme konuları kapsamında; dijital regülasyon alanında sadece bir "kural alıcı" (rule taker) değil, bölgesel bir "kural koyucu" (rule maker) olmalıdır.
 1. G7 Standartlarıyla Uyum konusunda, G7 Inventory (2023) raporunda belirtilen "enforcement convergence" (uygulama birliği) prensipleri çerçevesinde, Türk otoriteleri küresel ağlara dahil olmalıdır.²⁷⁶
 2. Türkiye, bölgesel gücünü kullanarak ortak bir "Dijital Pazar Standartları" seti oluşturmalı ve bu devasa veri havuzunu platformlarla olan pazarlıkta bir koz olarak kullanmalıdır.

²⁷⁵ Monti, G., & Colomo, P. I. (2025). *The Future of Digital Adjudication*. A.g.e.

²⁷⁶ G7 Enforcers' Summit (2023). A.g.e.

BÖLÜM 8: PAYDAŞ KATILIMI VE GÖZDEN GEÇİRME

Bölümün Amacı: Dijital platformların düzenlenmesini tek bir kurumun tahakkümünden çıkararak; kamu, akademi, özel sektör ve sivil toplumu kapsayan "Çok Paydaşlı Yönetişim" modeli kurmak ve mevzuatı statik bir metin olmaktan çıkarıp teknolojik hıza ayak uyduran, 2-3 yıllık döngülerle kendini güncelleyen "yaşayan çevik bir denetim" mekanizmasına dönüştürmektir.

İçerik ve Kapsam:

- Kamu kurumları (BTK, KVKK, Rekabet), akademi, platformlar (Gatekeepers/KOBİ'ler) ve STK'lardan oluşan "Dijital Ekosistem Danışma Kurulu"nın inşası.
- Sektörel risklere özel (Arama Motorları, Sosyal Ağlar, E-Ticaret) tematik çalışma gruplarının oluşturulması ve "Uygula veya Açıkla" (Comply or Explain) prensibiyle karar alma süreçleri.
- Yasaların her 2-3 yılda bir sahadaki uygulanabilirliğini, uyum maliyetlerini ve kullanıcı kazanımlarını ölçen "Periyodik Etki Değerlendirme" döngüsünün kurulması.
- AB Dijital Paketi (DSA, DMA, AI Act, NIS2) ile sürekli uyum, uluslararası düzenleyici ağlara (ICN, GPAI) entegrasyon ve 36 Aylık Uygulama Yol Haritası (Faz 1-2-3)

Temel Kavramlar:

- Çok Paydaşlı Yönetişim (Multi-stakeholder Governance)
- Çevik Yönetişim ve Öğrenen Regülasyon (Agile/Learning Regulation)
- Uygula veya Açıkla (Comply or Explain)
- Brüksel Etkisi (The Brussels Effect)
- Darboğaz Analizi

8.1. Katılımcı Yönetişim Modeli: Çok Paydaşlı Danışma Kurulu

Dijital platformların düzenlenmesi, yalnızca teknik bir süreç değil; hukuki, ekonomik ve toplumsal boyutları olan çok katmanlı bir meseledir. Bu nedenle kurulacak yapının "**Çok Paydaşlı Yönetişim**" (**Multi-stakeholder Governance**) modelini esas alması, regülasyonun meşruiyeti ve etkinliği açısından hayati önem taşır.

Kurumsal Yapı ve Üyelik Kompozisyonu

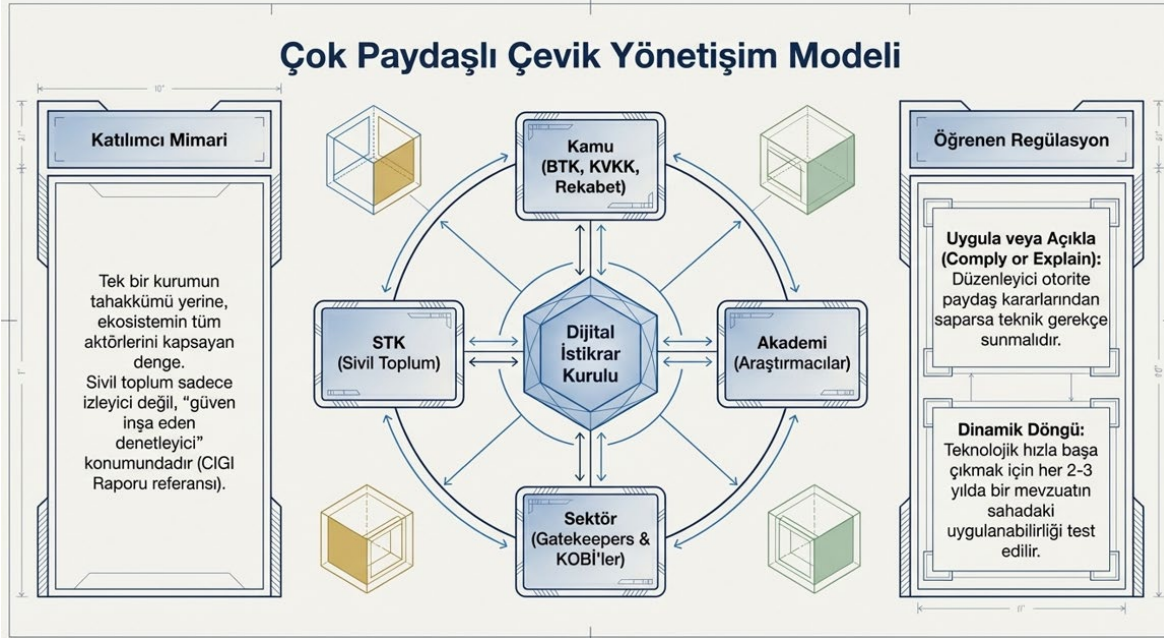
Kurul, tek bir kurumun tahakkümü yerine, ekosistemin tüm aktörlerini kapsayan bir denge üzerine inşa edilmelidir:

- **Kamu Temsiliyeti:** Bilgi Teknolojileri ve İletişim Kurumu (BTK), Kişisel Verileri Koruma Kurumu (KVKK), Rekabet Kurumu ve ilgili bakanlıklar (Ticaret, Aile, Sanayi ve Teknoloji).
- **Akademik Kanat:** Hukuk (Bilişim/Rekabet), Bilgisayar Mühendisliği (Algoritmik şeffaflık) ve Sosyal Bilimler (Etki analizi) alanlarından uzmanlar.
- **Sektör Temsilcileri:** "Gatekeeper" (Geçit bekçisi) statüsündeki dev platformlar ile yerli ve yabancı teknoloji girişimleri ve KOBİ birlikleri.
- **Sivil Toplum Kuruluşları ve Hak Örgütleri:** Dijital haklar, tüketiciyi koruma dernekleri ve veri gizliliği savunucuları.

Farklı uygulamalara göz attığımızda;

- OECD'nin "Digital Economy Outlook" raporları, bu tip kurullarda "Kapsayıcılık" (Inclusivity) ilkesinin, regülasyonun piyasa tarafından benimsenme hızını %40 oranında artırdığını vurgulamaktadır.
- Kanada merkezli, dijital platform yönetiminde sivil toplumun rolü üzerine akademik makaleler sunan CIGI (Centre for International Governance Innovation) raporları, platform yönetiminde "geleneksel devlet odaklı" yaklaşımdan "çok paydaşlı ve katılımcı" yaklaşıma geçişin en güçlü savunucularından biridir.²⁷⁷
- CIGI, finans dünyasındaki "Financial Stability Board" modeline benzer bir "**Dijital İstikrar Kurulu**" kurulmasını önermektedir. Araştırmalar, sivil toplumun sadece bir "izleyici" değil, aynı zamanda güven inşa eden bir "denetleyici" olması gerektiğini vurgular. CIGI, özellikle Kanada örneğinde (Digital Citizen Initiative), vatandaşların dezenformasyona karşı direncini artırmak için katılımcı mekanizmaların önemini kanıtlamıştır.

²⁷⁷ **CIGI (2023-2024).** *Global Platform Governance Network (GPGN) Series & Advancing Multi-stakeholderism for AI Governance.* Centre for International Governance Innovation.



ŞEKİL 8-1: Çok Paydaşlı Çevik Yönetişim Modeli (YZ ile hazırlanmıştır)

8.1.1. Operasyonel Çalışma Prensipleri ve Tematik Gruplar

Kurul, hantal bir yapıdan ziyade "**Çevik Yönetişim**" (**Agile Governance**) prensiplerini benimsemelidir.

Tematik Alt Çalışma Grupları: Platformların doğası gereği farklı riskler barındırması nedeniyle üç ana alan belirlenmiştir:

1. **Arama Motorları Grubu:** Algoritmik tarafsızlık ve veri taşınabilirliği odağı.
2. **Sosyal Ağlar Grubu:** Dezenformasyon, içerik moderasyonu ve çocukların korunması odağı. Örnek olarak İngiltere’de Ofcom, sosyal ağlarda dezenformasyon ve çocukların korunması gibi konularda paydaşlardan gelen verileri nasıl işleyeceğine dair detaylı bir "Kod Rehberi" (Codes of Practice) yayımlamıştır.²⁷⁸
3. **E-Ticaret Grubu:** Haksız ticari şartlar (self-preferencing) ve sahte ürün takibi odağı.

Karar Mekanizması: Kurul kararları "İstisnâ" niteliktedir; ancak düzenleyici otorite bu kararlardan saptığında "Uygula veya Açıkla" (Comply or Explain) prensibi gereği gerekçelendirme yapmalıdır. Ofcom’un yönetim modelinde, düzenleyici kurum paydaşlardan gelen risk değerlendirmelerini dikkate almak zorundadır. Eğer bir risk bildirimi göz ardı edilirse, bunun teknik gerekçesi şeffafca sunulur.

Tirole (2017), dijital platformların (Arama motorları, e-ticaret) doğal olarak tekelleri bir yapıya bürünme eğiliminde olduğunu ve klasik regülasyonların burada yetersiz kaldığını savunur. Tirole ayrıca, düzenleyici

²⁷⁸ **UK Ofcom (2023).** *Statement on Online Safety Governance*. (İngiltere’nin katılımcı denetim modeli ve sektörle işbirliği süreçleri).

kurumun, platformun iç işleyişi (algoritmalar, reklam modelleri) hakkında platformun kendisinden daha az bilgiye sahip olmasının (asimetrik bilgi) bir sorun olduğu söylenerek, paydaş katılımının bu bilgi boşluğunu doldurmak için şart olduğunu belirtir.²⁷⁹

8.1.2. Şeffaflık ve Hesap Verilebilirlik

AB DSA Madde 44, DMA ve Ofcom çerçevesinde vurgulanan "Bağımsız Denetim" ruhuna uygun olarak²⁸⁰:

- Toplantı gündemleri ve özet tutanakları kamuoyuna açık tutulmalı.
- Yıllık "Ekosistem Sağlık Raporu" yayınlanarak paydaş katılımının regülasyona etkisi belgelenmelidir.

8.2. Periyodik Gözden Geçirme ve Etki Değerlendirme Mekanizması

Dijital pazarların hızı, geleneksel statik yasaların hızla demode olmasına neden olmaktadır. Bu bölüm, kurulan düzenleyici yapının her **2–3 yılda bir** kendi etkinliğini sorguladığı ve piyasa dinamiklerine göre kendini güncellediği "yaşayan bir denetim" döngüsünü tanımlar.

8.2.1. Düzenli Değerlendirme Döngüsü (2–3 Yıl)

Mevzuatın her 2 veya 3 yılda bir sistemli olarak gözden geçirilmesi, kurumsal esnekliğin korunması açısından kritiktir.

Mevzuatın Sahadaki Uygulanabilirliğinin Analizi: Düzenlemelerin teorik hedefleri ile pratik sonuçları arasındaki boşluklar analiz edilir. Avrupa Komisyonu'nun "Better Regulation Guidelines" dokümanı, dijital yasaların "Refit" (Regulatory Fitness and Performance) programı kapsamında her 3 yılda bir gözden geçirilmesini, hangi kuralların halen işlevsel olduğunun ve hangilerinin bürokratik bir yük haline geldiğinin tespit edilmesini, aksi takdirde yasal boşlukların teknolojik gelişimin gerisinde kalacağını belirtmektedir.²⁸¹

Hizmet Sağlayıcılar Üzerindeki Uyum Maliyeti ve Ekonomi Analizi: Özellikle KOBİ niteliğindeki yerli teknoloji şirketlerinin regülasyona uyum sağlarken karşılaştıkları finansal ve operasyonel maliyetler

²⁷⁹ **Jean Tirole (2017).** *Economics for the Common Good*. (Dijital ekonomide regülasyonun paydaşlar arasındaki dengeyi nasıl kurması gerektiğine dair teorik temel).

²⁸⁰ **European Commission (2022).** *Digital Services Act (DSA) & Digital Markets Act (DMA) Frameworks*. (AB'nin paydaş katılımı ve bağımsız denetçi mekanizmaları üzerine temel rehber)

²⁸¹ **European Commission (2023).** *Better Regulation: Guidelines and Toolbox*. (AB'nin mevzuat etki değerlendirmesi ve gözden geçirme döngüleri için kullandığı resmi metodoloji).

ölçülür. Jean Tirole (2017)'ın platform ekonomisi teorisi ışığında, regülasyonun "pazara giriş engeli" yaratıp yaratmadığı test edilir.²⁸²

Hizmet Alanların (Kullanıcıların) Hak ve Güvenlik Kazanımlarının Ölçümü: Kullanıcıların dijital güvenliğindeki artış, dezenformasyona maruz kalma oranlarındaki değişim ve veri üzerindeki kontrol haklarının etkinliği anket ve veri analizleriyle ölçülür.

Dünya Ekonomik Forumu (WEF) tarafından yayımlanan "Agile Regulation for the Fourth Industrial Revolution" raporu, dijital otoritelerin "öğrenen bir yapı" (learning-based regulation) kurmasını, 2-3 yıllık periyotların bu öğrenme eğrisi için ideal olduğunu savunmaktadır.²⁸³

8.2.2. Veri Odaklı Denetim ve Raporlama

Denetim süreci, platformların sunduğu ham verilerin bağımsız bir perspektifle işlenmesine dayanır.

Platformların Şeffaflık Raporlarının (DSA ve DMA eksenli) Teknik Analizi: AB DSA Madde 15 ve 24 uyarınca talep edilen şeffaflık raporları; içerik kaldırma oranları, algoritmik parametreler ve reklam hedefleme kriterleri açısından incelenir. LSE (2022) raporunda önerilen "algoritmik hesap verebilirlik" metrikleri bu analizde temel alınır.²⁸⁴

Hukuki ve Teknik Uyumda Darboğaz Analizi: Yükümlülüklerin yerine getirilmesini engelleyen teknik kısıtlar veya hukuki yorum farkları (darboğazlar) raporlanır. Bu aşamada, Ada Lovelace Institute (2023) tarafından geliştirilen "denetim metodolojileri" kullanılarak sistemik riskler minimize edilir.²⁸⁵

8.2.3. Düzenleyici Adaptasyon: Teknolojik Değişimlere Göre Güncelleme Protokolleri

Değerlendirme sonuçları, mevzuatın statik kalmasını önlemek için birer "müdahale sinyali" olarak kullanılır.

Hızlı Güncelleme Mekanizması: Ana yasalarda değişiklik yapmaya gerek kalmadan, ikincil düzenlemelerle (tebliğ ve/veya yönetmelik) teknolojik değişimlere (örneğin Üretken Yapay Zekâ - GenAI entegrasyonu) hızlıca uyum sağlanır.

Öğrenen Regülasyon: OECD (2019) RIA rehberinde belirtilen "kanıt temelli politika" prensibi gereği, her gözden geçirme dönemi bir sonraki dönemin stratejik hedeflerini belirler.²⁸⁶

²⁸² Jean Tirole (2017). *A.g.e.*

²⁸³ World Economic Forum (2020). *Agile Regulation for the Fourth Industrial Revolution: A Toolkit for Regulators*. (Teknolojik hızla uyum sağlamak için "çevik" denetim mekanizmalarının tasarımı).

²⁸⁴ LSE (The London School of Economics and Political Science), (2022). *Algorithmic Accountability and Transparency Report*. (Platform verilerinin ve algoritmaların denetim metodolojisi).

²⁸⁵ Ada Lovelace Institute (2023). *Evaluating the Success of Digital Acts*. (Dijital düzenlemelerin etkinliğini ölçmek için geliştirilen yeni nesil metrikler).

²⁸⁶ OECD (2019). *Regulatory Impact Assessment (RIA)*.

8.3. Uluslararası İyi Uygulamalarla Sürekli Uyum Stratejisi

Dijital platformların dünyanın neredeyse her yerinde çalışabilmesi, ulusal düzenlemelerin ötesinde, küresel standartlarla uyumlu bir mevzuat setini zorunlu kılmaktadır. Bu bölüm, dinamik bir takip mekanizması ve uluslararası işbirliği ağlarına entegrasyon stratejisini tanımlar.

8.3.1. Dinamik Mevzuat Takibi

AB Dijital Paketine (DSA, DMA, AI Act, NIS2) Uyumda Kritik Güncellemeler: AB'nin dijital düzenlemeleri sadece birer yasa değil, sürekli güncellenen "yaşayan standartlar"dır.

DSA/DMA Entegrasyonu: Platformların "Gatekeeper" (Geçit Bekçisi) statüleri ve sistemik risk analizleri, AB Komisyonu'nun güncel kararları ışığında takip edilmelidir.²⁸⁷

AI Act & NIS2: Yapay zekâ risk kategorizasyonu ve siber dayanıklılık (NIS2) standartları, yerel mevzuatın "geleceğe hazır" (future-proof) hale getirilmesinde temel referanstır.

Bradford (2020) tarafından kavramsallaştırılan "The Brussels Effect", bu uyumun sadece bir tercih değil, küresel dijital pazara eklemlenmek için bir gereklilik olduğunu savunur.²⁸⁸

İngiltere ve Kanada Modelleri ile Benchmarking (Kıyaslama):

İngiltere (Ofcom): Ofcom'un "Güvenli Tasarım" (Safety by Design) yaklaşımı, teknik denetim metodolojisi için benchmark alınmalıdır (**Ofcom, 2023**).

İngiltere'nin inovasyon odaklı ve esnek regülasyon modeli için Bilim, İnovasyon ve Teknoloji Bakanlığı raporu baz alınabilir.²⁸⁹

Kanada (C-27): Kanada'nın bireysel veri haklarını koruyan "Digital Charter" modeli, platformların şeffaflık yükümlülükleri ile kullanıcı gizliliği arasındaki dengenin kurulmasında incelenmelidir.²⁹⁰

²⁸⁷ **European Commission (2023).** *The Digital Services Act Package*. (DSA/DMA uygulama ve güncelleme rehberi).

²⁸⁸ **Bradford, A. (2020).** *The Brussels Effect: How the European Union Rules the World*. Oxford University Press. (Küresel dijital standartların yayılım dinamiği üzerine temel eser)

²⁸⁹ **Department for Science, Innovation and Technology (UK, 2023).** *A Pro-innovation Approach to AI Regulation*.

²⁹⁰ **Government of Canada (2022).** *Bill C-27: Digital Charter Implementation Act*

8.3.2. Küresel İşbirliği ve Standart Birliği

Uluslararası Düzenleyici Ağlara Katılım ve Bilgi Paylaşımı: Tek taraflı denetim yerine, regülatörler arası ağlara (networked regulation) katılım, bilgi asimetrisini azaltır.

- **Küresel Ağlar:** ICN (International Competition Network) ve GPAI (Global Partnership on AI) gibi platformlarda aktif rol alınarak, yaptırım kararlarında eşgüdüm sağlanmalıdır.
- **Bilgi Paylaşımı:** Sınır aşan dezenformasyon veya haksız ticari uygulamalarla mücadelede, diğer ülke otoriteleriyle "eş zamanlı müdahale" protokolleri geliştirilmelidir.

CIGI (2024) raporlarında önerilen "Global Platform Governance Network (GPGN)" yapısı, farklı ülkelerdeki düzenleyicilerin platform verilerini ortak analiz etmesi gerektiğini vurgulamaktadır.²⁹¹

Sınır Ötesi Veri ve Güvenlik Protokollerine Adaptasyon:

Veri Egemenliği ve Güvenlik: OECD'nin 2022 bildirgesi, veriye erişim ve sınır ötesi veri transferi süreçlerinde "güvenilir bölge" (trusted zone) standartlarının oluşturulması için rehberdir.²⁹²

Siber Güvenlik Eşgüdümü: NIS2 direktifi ile uyumlu olarak, platformların siber saldırı bildirim süreçlerinin uluslararası CERT (Bilgisayar Acil Müdahale Ekipleri) ağlarıyla entegrasyonu sağlanmalıdır.

8.4. Uygulama Yol Haritası ve Eylem Planı

Stratejik çerçevesini eyleme dönüştürecek olan "**Uygulama Yol Haritası ve Eylem Planı**", kurulan yapının sürdürülebilirliğini ve uluslararası standartlara entegrasyonunu sağlar. Bu yol haritası, teorik çerçevesi çizilen yönetim modelinin 36 aylık bir zaman diliminde kademeli olarak hayata geçirilmesini öngörür.

8.4.1. Faz 1: Kurumsal Yapılanma ve Kapasite İnşası (0–6 Ay)

Bu fazın temel hedefi, yasal altyapının operasyonel hale getirilmesi ve paydaşların bir araya getirilmesidir.

- **Danışma Kurulunun Teşekkülü:** Kamu, akademi, STK ve sektör temsilcilerinin seçimi ve çalışma gruplarının (Arama Motorları, Sosyal Ağlar, E-Ticaret) atamalarının yapılması.
- **Çalışma Usul ve Esaslarının Belirlenmesi:** Şeffaflık protokollerinin ve "Uygula veya Açıkla" (Comply or Explain) mekanizmasının yönetmeliğe dökülmesi.

²⁹¹ **CIGI (2024).** *Advancing Multi-stakeholderism for AI and Platform Governance.* (Küresel yönetişimde çok paydaşlılık ve ağ tabanlı denetim).

²⁹² **OECD (2022).** *Declaration on Government Access to Personal Data Held by Private Sector Entities.* (Veri güvenliği ve sınır ötesi veri akışında uluslararası standartlar).

- **Veri Altyapısının Kurulması:** Platformlardan gelecek şeffaflık raporlarının analizi için teknik izleme biriminin (Data Unit) oluşturulması.

World Economic Forum (2020) raporu, ilk 6 ayın "kurumsal öğrenme" ve "güven inşası" için kritik olduğunu, bu aşamada esnek alt komitelerin kurulmasını tavsiye eder.²⁹³

8.4.2. Faz 2: Pilot Uygulama ve İlk Etki Analizi (6–18 Ay)

Mekanizmanın test edildiği ve platform bazlı ilk denetimlerin gerçekleştiği aşamadır.

- **Platform Spesifik Denetimler:** Sosyal ağlarda içerik moderasyonu ve e-ticarete haksız ticari uygulamalar üzerine ilk pilot incelemelerin yapılması.
- **Algoritmik Şeffaflık Testleri:** LSE (2022) standartları doğrultusunda, arama motorlarının tavsiye sistemleri üzerinde örneklem metodolojisiyle denetimlerin başlatılması.²⁹⁴
- **Uluslararası Entegrasyon:** AB DSA, AB DMA ve OECD çalışma gruplarına gözlemci statüsünde katılım ve bilgi paylaşımı protokollerinin imzalanması.

OECD (2019) RIA metodolojisi, pilot uygulamalardan elde edilen verilerin, ana regülasyonun "kalibrasyonu" için hayati olduğunu vurgular.²⁹⁵

8.4.3. Faz 3: Tam Uyum, Sürekli Gözden Geçirme ve Sürdürülebilirlik (18–36 Ay)

Yönetişim modelinin tam kapasiteyle çalıştığı ve ilk büyük "Gözden Geçirme" döngüsünün tamamlandığı fazdır.

- **Periyodik Etki Değerlendirme Raporu:** Mevzuatın 2. yılı sonunda piyasa üzerindeki ekonomik ve hukuki etkilerini içeren kapsamlı raporun yayınlanması.
- **Dinamik Mevzuat Güncellemesi:** Değerlendirme sonuçlarına ve Bradford (2020)'un tanımladığı "Brüksel Etkisi"ndeki yeni gelişmelere (AI Act güncellemeleri vb.) göre ikincil mevzuatın revize edilmesi.²⁹⁶
- **Küresel Liderlik ve Standart Belirleme:** Türkiye modelinin, bölgesel iyi uygulama örneği olarak CIGI (2024) benzeri uluslararası platformlarda sunulması ve sınır ötesi veri/güvenlik protokollerine tam uyum.²⁹⁷

²⁹³ **World Economic Forum (2020).** *A.g.e.*

²⁹⁴ **LSE (London School of Economics) (2022).** *A.g.e.*

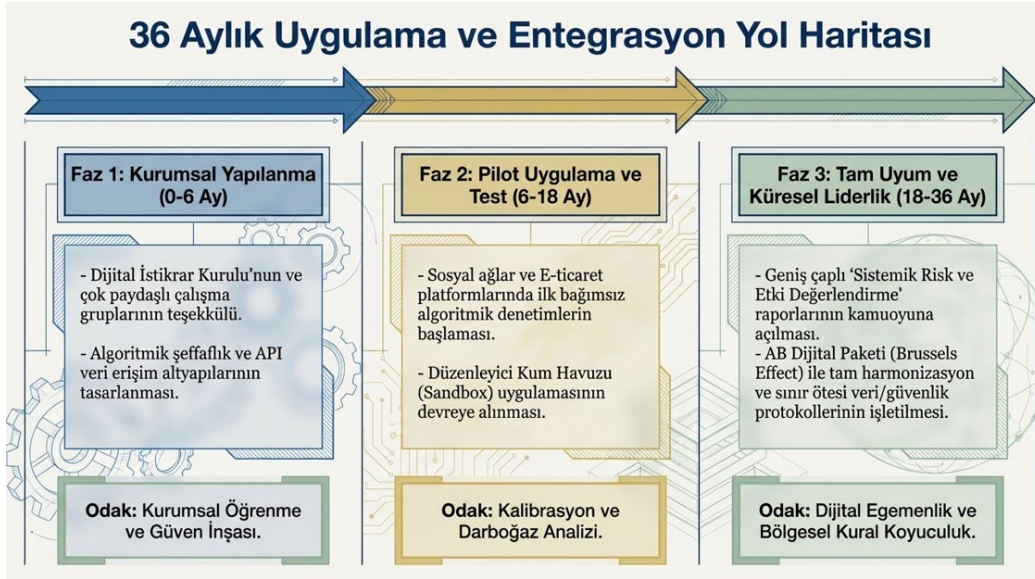
²⁹⁵ **OECD (2019).** *Regulatory Impact Assessment (RIA).* *A.g.e.*

²⁹⁶ **Bradford, A. (2020).** *A.g.e.*

²⁹⁷ **CIGI (2024).** *A.g.e.*

TABLO 8-1: Özet Uygulama Tablosu

Faz	Temel Odak	Kritik Çıktı	Dayanak Kaynak
Faz 1	Teşkilatlanma	Danışma Kurulu Tüzüğü	WEF (2020)
Faz 2	Denetim ve Veri	Algoritmik Şeffaflık Raporu	LSE (2022) / Ofcom (2023)
Faz 3	Uyum ve Reform	2 Yıllık Etki Analizi Raporu	OECD (2019) / CIGI (2024)



ŞEKİL 8-2: Uygulama ve Entegrasyon Yol Haritası (YZ ile hazırlanmıştır)

8.5. Politika Önerileri ve Sonuç

Bu bölüm boyunca incelenen AB, OECD ve Türkiye örnekleri; dijital platform yönetişiminin artık sadece "içerik kaldırma" odaklı değil, "süreç odaklı" bir yapıya evrildiğini göstermektedir. Güven ve öngörülebilirliğin artırılması için aşağıdaki politika önerileri, bir uyum matrisi olarak değerlendirilmelidir.

8.5.1. Regülatörler İçin Politika Önerileri (Kamu Sektörü)

- **Kademeli Regülasyon Modeli:** Türkiye'deki düzenlemelerin, platformun kullanıcı sayısı, pazar gücü ve sistemik riskine göre (DSA modelinde olduğu gibi) farklılaşması sağlanmalıdır. Küçük ölçekli yerli girişimlerin inovasyon kapasitesi korunurken, dev platformlara yönelik düzenlemeler/denetim artırılmalıdır.

- **Bağımsız Denetim Ekosisteminin Kurulması:** Algoritmik denetim ve şeffaflık raporlarının doğrulanması için akredite edilmiş bağımsız denetçi kuruluşların (third-party auditors) sisteme dahil edilmesi gerekmektedir.
- **Veri Erişimi ve Akademik İş Birliği:** Regülatörler, platformların ham verilerine (anonimleştirilmiş şekilde) akademik araştırmacıların erişimini yasal güvenceye almalıdır. Bu, "kanıta dayalı politika yapımı" (evidence-based policy making) için elzemdir.
- **Kurumlar Arası Koordinasyon:** BTK, Rekabet Kurumu ve KVKK arasında dijital platform özelinde "Ortak Çalışma Grupları" kurulmalı; veri, rekabet ve içerik güvenliği arasındaki geçişken alanlar gri bölge olmaktan çıkarılmalıdır.
- **Düzenleyici Kum Havuzlarının (Regulatory Sandboxes) İnşası:** AB AI Act ve DSA kapsamında uygulanan 'denetim kum havuzları' mekanizması Türkiye'ye uyarlanmalıdır. Yenilikçiliği ve inovasyonu boğmadan regülasyon uyumunu test edebilmek için, platform algoritmalarının ve YZ sistemlerinin gerçek dünya koşullarına yakın ancak kontrollü ortamlarda test edilmesi sağlanmalıdır. Özellikle veri erişimi ve uyum maliyetleri konusunda zorlanan erken aşama yerli girişimlerin (startup) bu kaynaklara güvenle erişebileceği çok paydaşlı bir test ekosistemi kurgulanmalıdır. Bu kum havuzlarının; test süreçleri, risk değerlendirme metodolojileri, veri erişim modelleri ve regülatör geri bildirim mekanizmaları açısından standartlaştırılmış bir yasal çerçevesi olmalı ve piyasaya geçiş oranları ile tespit edilen riskler düzenli olarak izlenmelidir.

8.5.2. Platformlar İçin Stratejik Öneriler (Özel Sektör)

- **Açıklanabilir Yapay Zekâ (XAI) Entegrasyonu:** Algoritmik sıralama parametreleri, sadece teknik ekiplerce değil, sıradan bir kullanıcının anlayabileceği basitlikte (katmanlı şeffaflık) deklare edilmelidir.
- **Etki Analizi Odaklı Tasarım:** Ürün ve hizmet tasarımlarında, piyasaya sürülmeden önce "Yapay Zekâ Etki Analizi" (AIA) yapılarak; sistemin yaratabileceği önyargılar, ayrımcılık riskleri ve demokratik süreçler üzerindeki etkileri önceden tespit edilmelidir.
- **Şeffaflık Raporlarının Niteliksel Dönüşümü:** Raporlar sadece birer "sayı dökümü" olmaktan çıkarılmalı; reddedilen itirazların gerekçeleri ve algoritmik sistemlerin hata payları dürüstçe kamuoyuyla paylaşılmalıdır.

Kullanıcı Hakları ve Demokratik Güvenceler

- **Etkin İtiraz Mekanizmaları:** Kullanıcıların içerik kaldırma veya hesap kısıtlama kararlarına karşı, platform içi çözüm yollarının yanı sıra "Bağımsız Dijital Hakem" mekanizmalarına erişimi kolaylaştırılmalıdır.
- **Reklam Okuryazarlığı ve Arşiv Erişimi:** Siyasi ve kamusal reklamların finansman ve hedefleme bilgilerine yönelik şeffaf dijital arşivlerin standartlaştırılması, manipülasyonla mücadelenin temelidir.

8.5.3. Arama Motorları için Politika Önerileri

Arama motorlarında şeffaflık, raporlama ve hesap verebilirliğin öneminin altını çizmekle birlikte; Türkiye için yalnızca teknik bir düzenleme alanı olmayıp **dijital egemenlik, rekabet gücü ve kamusal güven** açısından stratejik bir dijital yönetim meselesi olduğunu ortaya koymaktadır. Diğer yandan, Türkiye’de arama motorlarının işleyişine ilişkin **sistematiik, karşılaştırılabilir ve düzenli yayımlanan şeffaflık verilerinin eksikliği** de ortadadır.

Mevcut durumda:

- Türkiye’de arama motorlarına yönelik düzenleme, ağırlıklı olarak rekabet hukuku ve elektronik haberleşme mevzuatı üzerinden yürütölmektedir.
- Mevcut düzenleyici çerçeve, arama motorlarının algoritmik etkilerini kapsamakta yetersizdir.
- BTK altyapı ve erişim boyutuna odaklanırken, Rekabet Kurumu piyasa gücü ve hâkim durum analizleri yapmaktadır.
- Algoritmik sıralama, içerik kaldırma ve veri taleplerine ilişkin istatistikler kamuoyuna açık değildir.
- Düzenleyici kurumların kullanabileceği standartlaştırılmış raporlama çerçeveleri bulunmamaktadır.

Bu bağlamda, Türkiye için aşağıdaki adımlar kritik önem taşımaktadır:

1. Arama motorları için **asgari şeffaflık yükümlölüklerinin** mevzuatla tanımlanması
2. Arama motorları için **zorunlu ve standart periyodik (yıllık/altı aylık) şeffaflık raporları** rejiminin oluşturulması
3. **Bağımsız algoritmik denetim** ve etki değerlendirme mekanizmalarının kurulması
4. Algoritmik risk değerlendirmesine yönelik **düzenleyici veri taleplerinin** toplanması
5. Kullanıcılar için **etkili itiraz ve telafi yollarının** tanımlanması
6. BTK, KVKK ve Rekabet Kurumu arasında **kurumsal koordinasyonun** güçlendirilmesi ve **veri paylaşım ve analiz mekanizmasının** oluşturulması

Bu adımlar, Türkiye’nin yalnızca AB düzenlemelerine uyum sağlamasını değil; Türkiye’nin dijital egemenlik, kullanıcı hakları ve rekabet hedeflerini birlikte gerçekleştirmesine katkı sağlayacaktır. Aynı zamanda Türkiye’nin **kendi dijital politika kapasitesini ve yönetim egemenliğini** güçlendirmesini mümkün kılacaktır.

8.5.4. Sosyal Ağlar için Politika Önerileri

Sosyal ağların Türkiye’de yalnızca iletişim araçları değil; **kamusal etki üreten, norm koyucu dijital altyapılar** olduğunu ortaya koymaktadır. Akademik literatür, algoritmik sıralama ve içerik

moderasyonunun demokratik süreçler üzerinde ölçülebilir etkiler yarattığını göstermektedir (Pasquale, 2015²⁹⁸, Gillespie, 2018²⁹⁹ ve Gillespie, T. 2020³⁰⁰).

Türkiye’de sosyal ağların işleyişine ilişkin **ülke bazlı, karşılaştırılabilir ve düzenli yayımlanan şeffaflık verilerinin yetersizliği maalesef ortadadır**. Mevcut durumda:

- Platformların Türkiye özelinde yayımladığı içerik kaldırma ve moderasyon verileri sınırlıdır.
- Algoritmik sıralama ve öneri sistemlerine ilişkin herhangi bir sayısal açıklama bulunmamaktadır.
- Kullanıcı itiraz süreçlerine ilişkin başarı oranları kamuoyuna açık değildir.

Bu bağlamda Türkiye için aşağıdaki adımlar kritik önem taşımaktadır:

1. Sosyal ağlar için Türkiye’ye özgü **zorunlu ve periyodik şeffaflık raporları** (DSA Madde 42 referans alınarak),
2. Algoritmik sıralama ve öneri sistemlerine ilişkin **düzenleyici bilgi ve veri talepleri** (Rieder et al., 2022)³⁰¹,
3. Kullanıcı haklarını ölçmeye yönelik **standartlaştırılmış performans göstergeleri**,
4. İçerik kaldırma ve hesap askıya alma kararları için **insan denetimli itiraz mekanizmaları**,
5. BTK, KVKK ve Rekabet Kurumu arasında **ortak platform yönetişi ve veri paylaşım çerçevesi, oluşturulmalı ve yayınlanmalıdır**.

Bu adımlar, Türkiye’nin sosyal ağlar üzerindeki düzenleyici yaklaşımını reaktif bir içerik yönetimi modelinden, **proaktif ve hesap verebilir bir dijital yönetim mimarisine** dönüştürebilecektir. Ayrıca, düzenleyici kapasitesini güçlendiren ülkemiz, **dijital kamusal alanın demokratik meşruiyetini** de pekiştirecektir.

8.5.5. E-Ticaret Politika Önerileri

E-Ticaret platformlarının Türkiye’de yalnızca ticari araçlar değil; **piyasa davranışlarını, fiyat oluşumunu ve rekabet koşullarını fiilen yönlendiren stratejik dijital altyapılar** olduğunu ortaya koymaktadır. Akademik literatür, algoritmik sıralama ve fiyatlama mekanizmalarının hem tüketici refahı

²⁹⁸ Pasquale, F. (2015). *A.g.e.*

²⁹⁹ Gillespie, T. (2018). *A.g.e.*

³⁰⁰ Gillespie, T. (2020). "Content moderation, AI, and the question of scale." *Big Data & Society*.

³⁰¹ Rieder, B. et al. (2022). *A.g.e.*

hem de satıcılar arası rekabet üzerinde belirleyici etkiler yarattığını göstermektedir (Rochet & Tirole, 2003³⁰², Khan, 2017³⁰³ ve Ezrachi & Stucke, 2020³⁰⁴).

Bu çalışmanın temel bulgularından biri, Türkiye’de e-ticaret platformlarının işleyişine ilişkin **ülke bazlı, karşılaştırılabilir ve düzenli yayımlanan şeffaflık verilerinin yetersizliğidir**. Türkiye’de e-ticaret pazarı hızla büyümekle birlikte, düzenleyici çerçeve ağırlıklı olarak tüketici sözleşmeleri ve vergi yükümlülüklerine odaklanmaktadır. Buna karşılık:

- Algoritmik sıralama şeffaflığı,
- Platform–satıcı ilişkilerinin ölçülebilirliği,
- Rekabetçi tarafsızlık alanlarında sınırlı düzenleme bulunmaktadır.

Bu durum, özellikle yerli KOBİ’ler açısından yapısal riskler doğurabilmektedir.

Mevcut durumda:

- Platformların Türkiye özelinde ürün sıralama, sponsorlu listeleme ve komisyon yapısına dair verileri kamuya açık değildir, açık olmalıdır.
- Satıcı görünürlüğü, hesap askıya alma ve performans puanlarına ilişkin istatistikler paylaşılmamaktadır, paylaşılmalıdır.
- Tüketici iade, şikâyet ve uyuşmazlık çözüm oranları platform bazında karşılaştırılamamaktadır, karşılaştırılabilir olmalıdır.

Bu bağlamda Türkiye için aşağıdaki adımlar kritik önem taşımaktadır:

1. Ürün sıralama, sponsorlu içerik ve dinamik fiyatlandırma uygulamalarına ilişkin **zorunlu şeffaflık yükümlülükleri** (DMA ve P2B Regülasyonu referans alınarak),
2. E-ticaret platformu ile satıcı ilişkileri için **zorunlu ve standartlaştırılmış ve periyodik raporlama çerçevesi**,
3. Algoritmik sıralama (self-preferencing) ve ayrımcı fiyatlandırma risklerine karşı **rekabetçi denetim ve düzenleyici veri erişim yetki mekanizmaları**,
4. Satıcılar ve tüketiciler için **bağımsız, insan denetimli ve etkin itiraz yolları**,

sağlanmalıdır.

Bu adımlar, Türkiye’de e-ticaret ekosisteminin reaktif şikâyet temelli yaklaşımdan, **proaktif ve hesap verebilir bir platform yönetişimi modeline** evrilmesini mümkün kılacaktır. Ayrıca, Türkiye’nin e-ticaret pazarında **rekabetçi tarafsızlığı, tüketici güvenliğini ve KOBİ’lerin sürdürülebilirliğini** güçlendirecektir.

³⁰² Rochet, J.-C., & Tirole, J. (2003). *A.g.e.*

³⁰³ Khan, L. (2017). *A.g.e.*

³⁰⁴ Ezrachi, A., & Stucke, M. (2020). *A.g.e.*

EK BÖLÜM: MEVZUAT UYUMLULUK MATRİSİ VE TEKNİK ANALİZ

Bu ek bölüm, çalışmamızın pratik uygulamasını somutlaştıran, hukuk ve uyum (compliance) birimleri için bir "kontrol listesi" niteliği taşımaktadır. Aşağıda göreceğiniz matris; maddelerin ne anlama geldiğini, platformların hangi somut adımları atması gerektiğini ve Türkiye'deki yasal mevzuat karşılıklarını ekleyerek hazırlanmıştır.

MEVZUAT UYUMLULUK MATRİSİ VE TEKNİK ANALİZ

Bu matris, raporun önceki bölümlerinde ele alınan teorik çerçeveyi, AB'nin "Altın Standartları" olan DSA, DMA ve AI Act'ın belirli maddeleriyle eşleştirir.

1. Arama Motorları: Pazar Gücü ve Bilgi Tarafsızlığı

Mevzuat Maddesi	Kapsam ve Gereklilik	Somut Uygulama Adımı	Türkiye Mevzuatı Karşılığı
DSA Madde 27 (Parametre Şeffaflığı)	Arama sonuçlarını belirleyen ana kriterlerin açıklanması.	Algoritmanın hangi verileri (konum, tarih, alaka) kullandığı "anlaşılır" bir dille beyan edilmelidir.	Rekabet Kurumu - Algoritmik Şeffaflık Kararları
DMA Madde 6 (Kendi Hizmetini Kayırmama)	Platform sahibinin kendi ürünlerini organik sonuçlarda öne çıkarmasının yasaklanması.	Google'ın kendi alışveriş veya uçuş servislerini rakiplerinden daha avantajlı konumlandırmaması.	Rekabet Kanunu Madde 6 (Hâkim Durumun Kötüye Kullanılması)

Analiz: Arama motorları için temel risk, ""geçit (kapı) bekçiliği" (gatekeeping) yaparak bilginin akışını manipüle etmektir. DMA Madde 6, bu platformların sadece bir teknoloji sağlayıcı değil, aynı zamanda adil bir pazar kurucusu olmasını zorunlu kılar.

2. Sosyal Ağlar: İçerik Güvenliği ve Demokratik Denetim

Mevzuat Maddesi	Kapsam ve Gerekliklik	Somut Uygulama Adımı	Türkiye Mevzuatı Karşılığı
DSA Madde 39 (Reklam Arşivleri)	Politik ve kamusal reklamların tüm detaylarıyla (harcama, hedefleme) arşivlenmesi.	Kamuoyuna açık, aranabilir ve API üzerinden erişilebilir bir reklam kütüphanesi oluşturulması.	5651 Sayılı Kanun (Reklam Yasakları ve Bildirimleri)
AI Act (Öneri Sistemleri Riski)	Öneri algoritmalarının birey ve toplum üzerindeki risklerinin yönetilmesi.	Algoritmanın "yankı odası" yaratma veya dezenformasyonu yayma potansiyeline karşı "insan denetimi" mekanizması.	KVKK (Otomatik Karar Verme Süreçlerinde İlgili Kişinin Hakları)

Analiz: Sosyal ağlar için hesap verebilirlik, algoritmaların toplumsal psikoloji üzerindeki etkisinden doğar. AI Act, özellikle profil oluşturma tabanlı öneri sistemlerini "yüksek riskli" veya "şeffaflık gerektiren" kategorilere sokarak, platformu bu sistemlerin "mimarı" olarak sorumlu tutar.

3. E-Ticaret: Güvenli Ticaret ve Tüketici İzlenebilirliği

Mevzuat Maddesi	Kapsam ve Gerekliklik	Somut Uygulama Adımı	Türkiye Mevzuatı Karşılığı
DSA Madde 30-32 (Satıcı Doğrulaması ve İzlenebilirliği-KYBC)	Pazar yerindeki ticari kullanıcıların (satıcıların) kimliklerinin doğrulanması.	Satıcının banka hesabı, adresi ve iletişim bilgilerinin platform tarafından teyit edilmesi ("Know Your Business Customer").	6563 Sayılı ETK (Elektronik Ticaret Kanunu) Güncel Değişiklikler
Tüketici Hakları Normları	Algoritmik fiyatlandırma ve kişiselleştirilmiş tekliflerin şeffaflığı.	Bir ürünün fiyatının kullanıcının profiline göre değişip değişmediğinin (dynamic pricing) açıkça belirtilmesi.	Tüketicinin Korunması Hakkında Kanun

Analiz: E-ticarete şeffaflık "anonimliği" bitirmeyi amaçlar. DSA'nın 30-32. maddeleri, platformun "sadece bir aracı" olduğu savunmasını ortadan kaldırarak, platformu güvenli bir ticari alan sağlamaktan sorumlu bir "denetleyici" haline getirir.

Mevzuat Uyum Süreci İçin 3 Temel Tavsiye:

1. Etki Analizi Önceliği: Kurumlar, sadece mevcut kanunlara uyum sağlamakla yetinmemeli; AI Act ve DSA kapsamında kendi sistemlerinin yaratabileceği "temel hak ihlali" risklerini önceden raporlamalıdır.
2. Harmonizasyon Birimi: Türkiye'deki platformlar, BTK, Rekabet Kurumu ve KVKK üçgenindeki regülasyon karmaşasını aşmak için merkezi bir "Mevzuat Harmonizasyon Birimi" kurmalıdır.
3. Dinamik Raporlama: Raporlama süreci yılda bir kez yapılan bir faaliyetten, gerçek zamanlı veri akışına (API tabanlı raporlama) evrilmelidir.

ANALİZ: ALGORİTMİK SİSTEMLER VE GLOBAL BAZI DÜZENLEMELER

Dijital platformlar ve veri odaklı sistemlerin temel bileşeni haline gelen algoritmik sistemleri yalnızca teknik araçlar olarak değil, toplumsal etkileri olan sosyo-teknik yapılar olarak ele almaktır. Bu kapsam da, algoritmik sistemlerin ortaya çıkardığı risk alanlarını tanımlamak, uluslararası yönetim ve düzenleme yaklaşımlarını karşılaştırmalı olarak incelemek ve kurumsal düzeyde uygulanabilecek denetim ve uyum mekanizmalarını ortaya koymak hedeflenmektedir.

Bölüm ayrıca, Türkiye'nin mevcut politika çerçevesini bu küresel gelişmeler ışığında değerlendirmeyi ve algoritmik sistemlerin şeffaf, hesap verebilir ve güvenilir biçimde yönetilmesine yönelik temel bir analiz çerçevesi sunmayı amaçlamaktadır.

- Algoritmik sistemlerin kavramsal temelleri, dijital platformlardaki işlevleri ve sosyo-teknik etkilerinin ortaya konulması.
- Algoritmik önyargı, şeffaflık eksikliği, içerik amplifikasyonu, veri mahremiyeti ve güvenlik riskleri gibi temel risk alanlarının analizi.
- OECD Yapay Zekâ İlkeleri, Avrupa Birliği Yapay Zekâ Yasası (AI Act), UNESCO Yapay Zekâ Etiği Tavsiye Kararı ve NIST Yapay Zekâ Risk Yönetim Çerçevesi gibi uluslararası yönetim modellerinin karşılaştırmalı incelenmesi.
- Kurumsal düzeyde algoritmik yönetim mekanizmaları, ISO/IEC 42001 standardı, algoritmik etki değerlendirmesi (AIA) ve iç denetim süreçlerinin değerlendirilmesi.
- Türkiye'nin yapay zekâ stratejisi, mevcut düzenleyici çerçevesi ve Avrupa Birliği ile uyum süreci bağlamında mevcut durumunun analiz edilmesi.

Kavramsal Çerçeve

Algoritmik sistemler, belirli girdilerden hareketle tahmin, öneri veya karar üreten ve bu çıktılar aracılığıyla dijital ya da fiziksel ortamları etkileyebilen makine tabanlı yapılardır. Güncel tanımlara göre yapay zekâ sistemleri, açık veya örtük hedefler doğrultusunda girdilerden çıkarım yaparak çevre üzerinde etkili sonuçlar üretmektedir.³⁰⁵

Dijital platformlar bağlamında algoritmik sistemler; içerik sıralama, öneri sistemleri, hedefli reklamcılık, içerik moderasyonu ve arama sonuçlarının düzenlenmesi gibi işlevleri yerine getirmektedir. Bu sistemler,

³⁰⁵ OECD, “Recommendation of the Council on Artificial Intelligence”, OECD/LEGAL/0449, 2024,

<https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>

kullanıcı davranışlarını analiz ederek etkileşimi artırmaya yönelik optimizasyon yapar ve bu süreçte içerik görünürlüğünü belirleyen temel mekanizma haline gelir.

Bu nedenle algoritmik sistemler yalnızca teknik araçlar olarak değil, aynı zamanda kullanıcı davranışlarını yönlendiren ve bilgiye erişim biçimlerini şekillendiren sosyo-teknik yapılar olarak değerlendirilmelidir. Nitekim son yıllarda yapılan ampirik çalışmalar, etkileşim temelli sıralama sistemlerinin kronolojik akışa kıyasla duygusal yoğunluğu yüksek ve kutuplaştırıcı içerikleri daha görünür kılabilirdiğini göstermektedir.³⁰⁶ Bu bulgu, algoritmik tasarım tercihlerinin kamusal tartışma ortamı üzerinde doğrudan etkili olduğunu ortaya koymaktadır.

Algoritmik sistemlerin bir diğer temel özelliği, karar süreçlerinin çoğu durumda kullanıcılar açısından şeffaf olmamasıdır. Özellikle derin öğrenme tabanlı modellerde kararların nasıl üretildiğinin izlenmesi güçleşmekte, bu durum literatürde “kara kutu” sorunu olarak tanımlanmaktadır. Açıklanabilir yapay zekâ yaklaşımları, bu sorunu azaltmayı ve sistem çıktılarının anlaşılabilir hale getirilmesini amaçlamaktadır. Bununla birlikte, güncel politika belgelerinde şeffaflık kavramı giderek **itiraz edilebilirlik** ve **hesap verebilirlik** boyutlarıyla birlikte ele alınmaktadır.³⁰⁷

Genel amaçlı yapay zekâ (GPAI) modelleri ve üretken yapay zekâ sistemleri, algoritmik yönetim tartışmalarının kapsamını genişletmiştir. Büyük dil modelleri gibi sistemler, belirli bir görevle sınırlı olmaksızın çok çeşitli çıktılar üretebilmekte; bu durum dezenformasyon, fikrî mülkiyet ihlalleri ve içerik güvenliği gibi yeni risk alanlarını gündeme getirmektedir. Bu nedenle güncel düzenleyici çerçeveler, bu tür sistemleri ayrı bir kategori olarak ele almakta ve sağlayıcılara ek yükümlülükler getirmektedir.³⁰⁸

Bu bölümde ortaya konulan kavramsal çerçeve, algoritmik sistemlerin yalnızca teknik performans kriterleriyle değil; şeffaflık, hesap verebilirlik, adillik ve toplumsal etki boyutlarıyla birlikte değerlendirilmesi gerektiğini göstermektedir. Bu yaklaşım, izleyen alt bölümlerde ele alınacak risk alanları ve yönetim mekanizmalarının temelini oluşturmaktadır.

³⁰⁶ Agan, A. Y. et al., “Engagement, user satisfaction, and the amplification of divisive content on social media”, *PNAS Nexus*, 4(3), 2025,

<https://doi.org/10.1093/pnasnexus/pgaf062>

³⁰⁷ OECD, “Recommendation of the Council on Artificial Intelligence”, OECD/LEGAL/0449, 2024,

<https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>

³⁰⁸ European Parliament and Council, “Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)”, 2024,

<https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>

Uluslararası Yönetişim ve Düzenleme Yaklaşımları

Algoritmik sistemlerin yarattığı riskler, uluslararası düzeyde farklı yönetim ve düzenleme yaklaşımlarının geliştirilmesine yol açmıştır. Bu yaklaşımlar genel olarak üç ekseninde şekillenmektedir: ilke temelli çerçeveler, bağlayıcı düzenlemeler ve sektörel/operasyonel rehberler. Bu bölümde öne çıkan uluslararası modeller karşılaştırmalı olarak ele alınmaktadır.

Kriter	OECD	AB AI Act	UNESCO	ABD (NIST)	Çin
Tür	İlke	Yasa	Etik çerçeve	Rehber	Sektörel düzenleme
Odak	Değerler	Risk	Etik-toplum	Risk yönetimi	Kontrol
Güçlü Yan	Küresel referans	Netlik	Kapsayıcılık	Esneklik	Hız
Zayıf Yan	Yaptırım yok	Maliyet	Uygulama zayıf	Parçalı yapı	Özgürlük tartışması

OECD Yapay Zekâ İlkeleri

OECD tarafından 2019 yılında kabul edilen ve 2024 yılında güncellenen Yapay Zekâ İlkeleri, yapay zekâ alanında ilk hükümetlerarası standartlardan biridir.³⁰⁹ İlkeler, insan hakları, şeffaflık, hesap verebilirlik ve güvenlik gibi temel değerleri merkeze alır.

2024 güncellemesi ile çerçevenin kapsamı genişletilmiş; özellikle üretken yapay zekâ, dezenformasyon ve çevresel sürdürülebilirlik konuları daha belirgin biçimde ele alınmıştır.³¹⁰ Bu ilkeler bağlayıcı olmamakla birlikte, ulusal politika yapım süreçleri üzerinde önemli bir referans noktası oluşturmaktadır.

³⁰⁹ OECD, “Recommendation of the Council on Artificial Intelligence”, OECD/LEGAL/0449, 2024, <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>

³¹⁰ OECD, “OECD AI Principles: Overview and Updates”, 2024, <https://oecd.ai/en/ai-principles>

Avrupa Birliği Yapay Zekâ Yasası (EU AI Act)

Avrupa Birliği tarafından kabul edilen Yapay Zekâ Yasası, algoritmik sistemlerin düzenlenmesine yönelik en kapsamlı bağlayıcı çerçevelerden biridir.³¹¹ Yasa, risk temelli bir yaklaşım benimseyerek yapay zekâ sistemlerini dört kategoriye ayırmaktadır:

- Kabul edilemez risk: yasaklanan uygulamalar
- Yüksek risk: sıkı yükümlülüklerle tabi sistemler
- Sınırlı risk: şeffaflık yükümlülüğü
- Düşük risk: minimal düzenleme

Bu yaklaşım, düzenleyici müdahalenin sistemin potansiyel etkisine göre farklılaştırılmasını sağlamaktadır. Özellikle yüksek riskli sistemler için teknik dokümantasyon, insan gözetimi ve risk yönetimi gibi yükümlülükler öngörülmektedir.

Ayrıca yasa, genel amaçlı yapay zekâ (GPAI) modelleri için ayrı bir düzenleme alanı tanımlayarak, bu sistemlerin geliştirilmesi ve dağıtımı için ek sorumluluklar getirmektedir.³¹²

UNESCO Yapay Zekâ Etiği Tavsiye Kararı

UNESCO tarafından 2021 yılında kabul edilen Yapay Zekâ Etiği Tavsiye Kararı, küresel ölçekte en geniş katılımı benimsenen etik çerçevelerden biridir.³¹³

Bu belge, yapay zekâ yönetişimini insan hakları, insan onuru, toplumsal kapsayıcılık ve çevresel sürdürülebilirlik ilkeleri üzerine inşa etmektedir. Tavsiye kararı, yalnızca ilke seti sunmakla kalmayıp, aynı zamanda veri yönetişimi, eğitim, toplumsal cinsiyet eşitliği ve etik etki değerlendirmesi gibi alanlarda somut politika önerileri içermektedir.

UNESCO yaklaşımının ayırt edici yönü, teknik düzenlemeden ziyade etik ve toplumsal boyuta odaklanmasıdır.

³¹¹ European Parliament and Council, “Regulation (EU) 2024/1689 (Artificial Intelligence Act)”, 2024, <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>

³¹² European Commission, “AI Act: General-purpose AI models”, 2024, <https://digital-strategy.ec.europa.eu/en/faqs/general-purpose-ai-models-ai-act-questions-answers>

³¹³ UNESCO, “Recommendation on the Ethics of Artificial Intelligence”, 2021, <https://unesdoc.unesco.org/ark:/48223/pf0000380455>

ABD Yaklaşımı: NIST AI Risk Yönetim Çerçevesi

Amerika Birleşik Devletleri, kapsamlı bir federal yapay zekâ yasası yerine, daha esnek ve sektörel bir yaklaşım benimsemektedir. Bu yaklaşımın merkezinde NIST tarafından geliştirilen Yapay Zekâ Risk Yönetim Çerçevesi (AI RMF) yer almaktadır.³¹⁴

AI RMF, yapay zekâ sistemlerinin yaşam döngüsü boyunca risklerin tanımlanması, ölçülmesi ve yönetilmesine yönelik bir rehber sunar. Çerçeve dört temel işlev etrafında yapılandırılmıştır:

- Govern (yönetim)
- Map (haritalama)
- Measure (ölçme)
- Manage (yönetme)

Bu model bağlayıcı olmamakla birlikte, özellikle kamu kurumları ve büyük ölçekli kuruluşlar için fiilî bir standart haline gelmiştir.

Çin'in Sektörel Düzenleme Yaklaşımı

Çin, yapay zekâ alanında tek bir kapsamlı yasa yerine, kullanım alanlarına göre ayrılmış sektörel düzenlemeler geliştirmektedir. Bu yaklaşım, özellikle algoritmik öneri sistemleri, sentetik içerik (deepfake) teknolojileri ve üretken yapay zekâ uygulamaları üzerine odaklanmaktadır.

2022 yılında yürürlüğe giren algoritma öneri düzenlemeleri, platformlara şeffaflık ve kullanıcı kontrolü yükümlülükleri getirmiştir.³¹⁵ Bunu izleyen düzenlemeler, sentetik içeriklerin etiketlenmesi ve üretken yapay zekâ hizmetlerinin denetlenmesine yönelik kurallar içermektedir.³¹⁶

Bu model, hızlı düzenleyici müdahale kapasitesi sağlamakla birlikte, ifade özgürlüğü ve veri kontrolü açısından tartışmalara da konu olmaktadır.

³¹⁴ NIST, “Artificial Intelligence Risk Management Framework (AI RMF 1.0)”, 2023,

<https://www.nist.gov/publications/artificial-intelligence-risk-management-framework-ai-rmf-10>

³¹⁵ Cyberspace Administration of China, “Administrative Provisions on Recommendation Algorithms in Internet-based Information Services”, 2022, http://www.cac.gov.cn/2022-01/04/c_1642894606364259.htm

³¹⁶ Cyberspace Administration of China, “Interim Measures for the Management of Generative Artificial Intelligence Services”, 2023, http://www.cac.gov.cn/2023-07/13/c_1690898327029107.htm

Yaklaşımların Karşılaştırmalı Değerlendirmesi

Uluslararası düzenleme modelleri üç ana yaklaşım altında toplanabilir:

- Kapsamlı ve bağlayıcı model (AB): yüksek hukuki kesinlik, ancak yüksek uyum maliyeti
- Esnek ve rehber temelli model (ABD): inovasyon dostu, ancak parçalı yapı riski
- Sektörel ve devlet merkezli model (Çin): hızlı uygulama, ancak hak temelli tartışmalar

Bu farklılıklar, algoritmik sistemlerin düzenlenmesinde tek tip bir modelin bulunmadığını ve düzenleyici tercihlerin ülkelerin kurumsal yapıları ve politik öncelikleriyle yakından ilişkili olduğunu göstermektedir.

Kurumsal Sorumluluk ve Uyum Araçları

Algoritmik sistemlerin geliştirilmesi ve kullanımı, yalnızca teknik bir süreç değil, aynı zamanda kurumsal sorumluluk alanıdır. Bu sistemlerin yol açabileceği risklerin yönetimi, kuruluşların yönetim yapıları, iç kontrol mekanizmaları ve uyum süreçleriyle doğrudan ilişkilidir.

Kurumsal YZ Yönetişim Yapıları

Kuruluşlar açısından yapay zekâ yönetişimi, farklı disiplinleri bir araya getiren bütünlüklü bir yaklaşım gerektirir. Etkin bir yönetim modeli; veri bilimi, hukuk, etik, risk yönetimi ve bilgi güvenliği gibi alanların koordinasyonunu içerir.

Bu kapsamda kuruluşların, yapay zekâ sistemlerini sistematik biçimde izleyebilmek için envanter oluşturması, risk sınıflandırması yapması ve karar alma süreçlerinde insan gözetimini tesis etmesi beklenmektedir. Avrupa Birliği Yapay Zekâ Yasası da özellikle yüksek riskli sistemler için insan gözetimi ve kurumsal sorumluluğu açık bir yükümlülük olarak tanımlamaktadır.³¹⁷

Kurumsal yönetim yapılarının temel amacı, algoritmik sistemlerin geliştirme ve kullanım süreçlerinin izlenebilir, denetlenebilir ve hesap verebilir hale getirilmesidir.

³¹⁷ European Parliament and Council, “Regulation (EU) 2024/1689 (Artificial Intelligence Act)”, 2024,

<https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>

ISO/IEC 42001 Standardı

ISO/IEC 42001:2023 standardı, yapay zekâ yönetim sistemlerine yönelik ilk uluslararası standart olarak kabul edilmektedir.³¹⁸ Bu standart, kuruluşların yapay zekâ sistemlerini planlama, uygulama, izleme ve sürekli iyileştirme süreçlerini sistematik hale getirmeyi amaçlamaktadır.

ISO 42001, klasik yönetim sistemi standartlarına benzer şekilde Planla–Uygula–Kontrol Et–Önlem Al (PDCA) döngüsüne dayanır. Bu yapı, algoritmik sistemlerin yalnızca geliştirme aşamasında değil, tüm yaşam döngüsü boyunca değerlendirilmesini mümkün kılar.

Standart, özellikle şu alanlarda kurumsal gereklilikler tanımlar:

- risk yönetimi süreçleri
- veri yönetimi
- algoritmik şeffaflık ve dokümantasyon
- iç denetim ve sürekli iyileştirme

Bu yönüyle ISO 42001, kuruluşlar için denetlenebilir ve sertifikalandırılabilir bir uyum çerçevesi sunmaktadır.

Algoritmik Etki Değerlendirmesi (AIA)

Algoritmik Etki Değerlendirmesi (Algorithmic Impact Assessment – AIA), yapay zekâ sistemlerinin potansiyel etkilerini sistematik olarak analiz etmeyi amaçlayan bir araçtır. Bu değerlendirme süreci, sistemlerin toplumsal, etik ve hukuki sonuçlarını önceden tespit etmeye yöneliktir.

UNESCO’nun Yapay Zekâ Etiği Tavsiye Kararı, özellikle yüksek riskli sistemler için etik etki değerlendirmelerinin uygulanmasını önermektedir.³¹⁹ Bu yaklaşım, yalnızca teknik performansla değil, aynı zamanda sistemlerin bireyler ve toplum üzerindeki etkilerine odaklanır.

AIA süreçleri genellikle şu unsurları içerir:

- risklerin tanımlanması
- etkilenen paydaşların belirlenmesi
- olası zararların değerlendirilmesi
- risk azaltma stratejilerinin geliştirilmesi

³¹⁸ International Organization for Standardization (ISO), “ISO/IEC 42001:2023 – Artificial intelligence management system”, 2023, <https://www.iso.org/standard/81230.html>

³¹⁹ UNESCO, “Recommendation on the Ethics of Artificial Intelligence”, 2021, <https://unesdoc.unesco.org/ark:/48223/pf0000380455>

Bu araç, algoritmik sistemlerin proaktif şekilde yönetilmesini sağlar.

İç Denetim ve Algoritmik Denetim Mekanizmaları

Algoritmik sistemlerin güvenilirliği, yalnızca tasarım aşamasında değil, kullanım sürecinde yapılan denetimlerle sağlanır. Bu nedenle kuruluşların düzenli iç denetim mekanizmaları kurması gerekmektedir.

Bu kapsamda öne çıkan uygulamalar şunlardır:

- model performansının sürekli izlenmesi
- önyargı ve adillik testlerinin uygulanması
- model drift (performans sapması) takibi
- denetim izlerinin (audit trails) tutulması

Algoritmik denetim, klasik bilgi teknolojileri denetiminden farklı olarak olasılıksal sistemlerin değerlendirilmesini gerektirir. Bu nedenle teknik uzmanlık ve metodolojik gelişim bu alanda kritik öneme sahiptir.

NIST AI Risk Yönetim Çerçevesi de kuruluşlara, yapay zekâ sistemlerinin yaşam döngüsü boyunca risklerin izlenmesi ve yönetilmesi için kapsamlı bir yapı sunmaktadır.³²⁰

Kurumsal Kültür ve Sorumlu YZ Yaklaşımı

Teknik araçlar ve standartlar, tek başına yeterli değildir. Yapay zekâ sistemlerinin sorumlu biçimde kullanılması, kurumsal kültür ve organizasyonel farkındalık ile doğrudan ilişkilidir.

Bu bağlamda kuruluşların:

- çalışanlarına yapay zekâ okuryazarlığı kazandırması
- etik ilkeleri kurumsal politikalara entegre etmesi
- risk bildirim mekanizmaları oluşturması

beklenmektedir.

Avrupa Birliği Yapay Zekâ Yasası, kuruluşların ilgili personelin yeterli bilgi ve yetkinliğe sahip olmasını sağlama yükümlülüğünü açıkça vurgulamaktadır.³²¹

³²⁰ NIST, “Artificial Intelligence Risk Management Framework (AI RMF 1.0)”, 2023,

<https://www.nist.gov/publications/artificial-intelligence-risk-management-framework-ai-rmf-10>

³²¹ European Parliament and Council, “Regulation (EU) 2024/1689 (Artificial Intelligence Act)”, 2024,

<https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>

Bu yaklaşım, yapay zekâ yönetişimini yalnızca teknik bir uyum meselesi olmaktan çıkararak, kurumsal sorumluluk ve etik yönetim meselesi haline getirmektedir.

Türkiye Açısından Değerlendirme

Türkiye’de yapay zekâ ve algoritmik sistemlere ilişkin politika çerçevesi, son yıllarda yayımlanan strateji belgeleri ve eylem planları üzerinden şekillenmektedir. Bu süreçte temel referans metin, 2021 yılında yayımlanan **Ulusal Yapay Zekâ Stratejisi**³²².

Söz konusu strateji; insan kaynağı geliştirme, araştırma kapasitesinin artırılması, veri altyapısının güçlendirilmesi ve düzenleyici çerçevenin oluşturulması gibi öncelik alanlarını içermektedir. Bu çerçeve, Türkiye’nin yapay zekâ alanındaki kurumsal kapasitesini artırmayı hedeflemekle birlikte, algoritmik sistemlere yönelik spesifik düzenlemeler açısından henüz sınırlı bir derinlik sunmaktadır.

Ulusal Politika ve Strateji Belgeleri

Ulusal Yapay Zekâ Stratejisi’ni tamamlayıcı nitelikte olan 2024–2025 Eylem Planı, daha somut uygulama adımları içermektedir.³²³ Bu plan kapsamında özellikle veri erişimi, kamu uygulamalarında yapay zekâ kullanımı ve yerli teknolojilerin geliştirilmesi ön plana çıkmaktadır.

Bununla birlikte, bu belgelerde algoritmik şeffaflık, denetim mekanizmaları ve yüksek riskli sistemlerin sınıflandırılması gibi konuların henüz sınırlı düzeyde ele alındığı görülmektedir. Bu durum, düzenleyici çerçevenin gelişim aşamasında olduğunu göstermektedir.

Avrupa Birliği ile Uyum Süreci

Türkiye’nin Avrupa Birliği ile olan ilişkisi, yapay zekâ düzenlemeleri açısından önemli bir referans çerçevesi oluşturmaktadır. Özellikle AB Yapay Zekâ Yasası’nın yürürlüğe girmesiyle birlikte, Türkiye’de faaliyet gösteren şirketlerin bu düzenlemeye uyum sağlaması fiilî bir gereklilik haline gelmektedir.³²⁴

Bu durum, Türkiye açısından iki yönlü bir etki yaratmaktadır:

³²² T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi & Sanayi ve Teknoloji Bakanlığı, “Ulusal Yapay Zekâ Stratejisi 2021–2025”, 2021,

<https://cbddo.gov.tr/SharedFolderServer/Genel/File/TR-UlusalYZStratejisi2021-2025.pdf>

³²³ T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, “Ulusal Yapay Zekâ Stratejisi 2024–2025 Eylem Planı”, 2024,

<https://www.sanayi.gov.tr/assets/pdf/UlusalYapayZekâStratejisi2024-2025EylemPlani.pdf>

³²⁴ European Parliament and Council, “Regulation (EU) 2024/1689 (Artificial Intelligence Act)”, 2024,

<https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>

- bir yandan AB standartlarının dolaylı olarak iç piyasaya yansımaları
- diğer yandan ulusal düzenlemelerin bu çerçeveye uyumlu hale getirilmesi gerekliliği

Bu bağlamda, risk temelli yaklaşım ve yüksek riskli sistemlere yönelik yükümlülükler, Türkiye’deki düzenleme tartışmalarının da merkezinde yer almaktadır.

Mevcut Düzenleyici Çerçeve ve Boşluklar

Türkiye’de algoritmik sistemleri doğrudan düzenleyen kapsamlı bir yapay zekâ yasası henüz yürürlükte değildir. Bununla birlikte, kişisel verilerin korunması, elektronik ticaret ve dijital hizmetler gibi alanlarda mevcut düzenlemeler dolaylı olarak algoritmik sistemleri etkilemektedir.

Özellikle 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK), veri işleme faaliyetleri üzerinden algoritmik sistemlerin kullanımına sınırlar getirmektedir.³²⁵ Ancak bu düzenleme, algoritmik karar alma süreçlerinin şeffaflığı veya denetlenebilirliği gibi konuları doğrudan kapsamamaktadır.

Bu durum, mevcut düzenleyici yapının parçalı ve dolaylı bir karaktere sahip olduğunu göstermektedir.

Kurumsal ve Teknik Kapasite Değerlendirmesi

Algoritmik sistemlerin etkin biçimde yönetilmesi, yalnızca hukuki düzenlemelerle değil, aynı zamanda teknik ve kurumsal kapasiteyle de ilişkilidir. Türkiye’de son yıllarda kamu ve özel sektörde yapay zekâ uygulamalarının artmasına rağmen, algoritmik denetim, risk değerlendirmesi ve etik yönetim alanlarında uzmanlaşmış insan kaynağı sınırlıdır.

Bu bağlamda, uluslararası standartların (örneğin ISO/IEC 42001) ve risk yönetim çerçevelerinin (örneğin NIST AI RMF) benimsenmesi, kurumsal kapasitenin geliştirilmesi açısından önemli bir araç olarak değerlendirilebilir.

³²⁵ Türkiye Büyük Millet Meclisi, “6698 sayılı Kişisel Verilerin Korunması Kanunu”, 2016, <https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=6698&MevzuatTur=1&MevzuatTertip=5>

SONUÇ: Yeni Bir Dijital Mutabakata Doğru

İnternet, Dijital, Çevrim İçi, Platform, Yapay Zekâ, Siber Güvenlik, Dijital Egemenlik ve bu terimler etrafında şekillenen **sosyo-politik ve ekonomik ekosistemler**, yerel ve küresel ölçekte titizlik içerisinde ve bilimsel disiplinlerde ele alınması gereken hayati kavramlardır. Son derece dinamik ve yüksek teknolojik hızda ilerleyen bu unsurları derinden kavramak ve proaktif bir bileşen olarak yönetebilmek, **Dijital Egemenlik** için kilit-taşıdır.

Dijital ve çevrim içi platformlar hayatın akışında oldukça büyük ölçeklerde bireysel ve toplumsal etkileri olan teknolojik ve sosyal yapılar haline evrilmişlerdir. İnternetin yaygınlığı ve erişilebilirliğin yüksek hızda ilerleyişi, dijital platformların hayatın normal akışında yer almasında ve durmaksızın yeni uygulama alanlarına genişlemektedir.

Bilhassa devasa büyüklükteki teknoloji firmalarının kontrol ettiği platformlar, karmaşık ve kapalı algoritmik sistemler marifetiyle bireysel ve toplumsal kapsamda ekonomik ve hatta siyasal hayata etki eden yönlendirme gücüne sahiptirler.

Oldukça kapsamlı ve karmaşık yapılar haline gelen büyük platformların etkilerini iyi anlamak ve buna uygun yönetim sistemleri oluşturmak kaçınılmaz durumdur. Proaktif kabiliyette ve ekosistemin gereklerine uygun dinamik düzenlemeler içerisinde ilerlemek elzemdir.

Bu rapor, dijital ve çevrim içi platformların sadece teknik araçlar olmadıklarını, toplumsal ve global boyutta etkileri olan yapılar farkındalığını vurgulayarak küresel regülasyonlarla uyumlu teknolojik, idari ve hukuki alanlarda öneriler sunmuştur.

Stratejik odağımız Türkiye'nin dijital ve çevrim içi platformlar ekosisteminde daha etken, kendi standartlarını belirleyen, ekosistemde var olan teknoloji firmaları ile global regülasyonlara uyumlu lider ülkeler arasında yer almasıdır.

Küresel uyum için referans aldığımız Avrupa Birliği'nin bu konular için baz alınan regülasyonları (DSA, DMA, AI Act, NIS2 vb) ile Türkiye'deki mevcut düzenlemelerin karşılaştırmalı analizine istinaden, gerekli olduğuna inanılan düzenleme önerileri raporda sunulmuştur. AB bu konularda dünyada en kapsamlı regülasyonları uygulamaya koymuştur ve dinamik olarak güncellemeler yapmaktadır. Raporda küresel düzenlemeler için OECD ve UK gibi evrensel ilkeleri içeren regülatif referanslar da ayrıca dikkate alınmıştır.

Yerel dinamikler ve referans olarak kabul edilen küresel regülasyonlar ile uyumlu bir vizyon ile önerdiğimiz tekno-politik düzenlemeler sayesinde, nihai hedefimiz olan dijital egemenlik tesis edilmelidir. Ekosistemi kapsayacak bir 'Çevik Yönetişim Modeli' ile kamu, özel sektör, akademi ve sivil toplum kuruluşlardan oluşan süreklilikte çalışmalar icra edilmelidir.

Sonuç olarak, dijital platformların düzenlenmesi sadece teknik ya da ticari bir piyasa yönetiminden ibaret bir sistemden daha da ileri ve kapsamlı bir konudur. Sunulan öneriler sayesinde bireylerin, ekosistemin ve

özellikle de çocuklarımızın bilişsel olarak, platformların olası manipülatif ve karanlık tasarımlarına karşı korunmasının güvence altına alınması hedeflenmiştir.

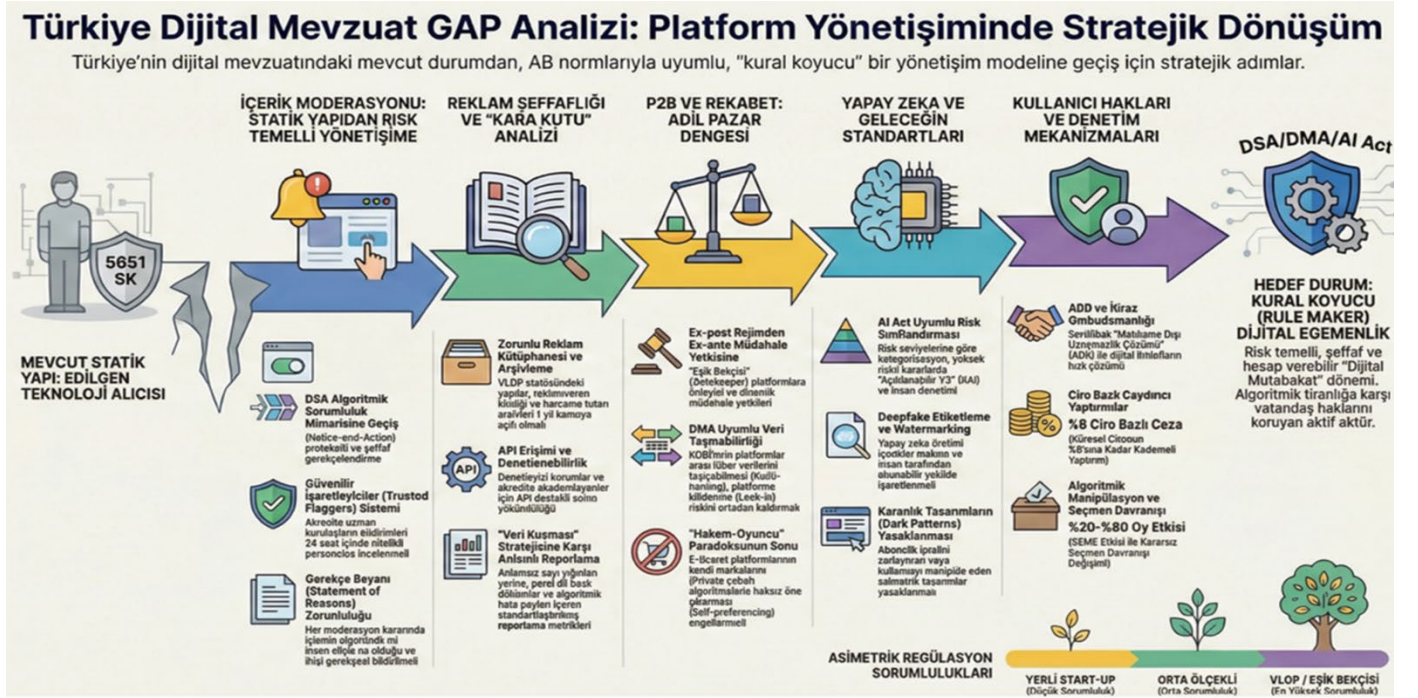
Raporda önerilen düzenlemeler ile dijital güvenin tesis edilerek, algoritmik şeffaflık ve adil rekabet kurallarının tesisi kurulması hedeflenmiştir. Bu sayede, küresel rekabetin desteklendiği ve yerel pazardaki küçük ve orta ölçekli teknoloji firmalarının haksız rekabet altında ezilmesinin de engellendiği, inovasyon stratejilerinin artırılması mümkün olacaktır.

Türkiye'nin dijital egemenlik vizyonu, yasal düzenlemelere ilaveten, BTK, KVKK ve Rekabet Kurumu gibi düzenleyici kurumlarla eşgüdümünde çalışacak, yetkilendirilmiş sivil toplum kuruluşlarını ve akademiye de sürece dahil eden 'Dijital Ekosistem Düzenleme Kurulu'nun hayata geçirilmesi ile güçlenecektir. Raporumuzda yer alan '36 Aylık Stratejik Uygulama Yol Haritası' ile bu dönüşümün icrası hakkındaki öneriler sunulmuştur.

İnovasyonu teşvik eden ve dijital adaleti tesis eden bir yönetim modeli kurmak mümkündür ve elzemdir.

Bu vizyon kapsamında sunulan öneriler sayesinde bugün ve gelecekteki teknolojilere hazırlıklı olan, proaktif bir Dijital Türkiye tasavvur edilmektedir.

Saygılarımızla.



ŞEKİL B: Türkiye Dijital Mevzuat Analizi-Stratejik Dönüşüm (YZ ile hazırlanmıştır)

EK: İNGİLİZCE TERİMLERİN TÜRKÇE KARŞILIĞI

Raporda kullanılan orijinal (İngilizce) terimlerin Türkçe karşılıkları aşağıdaki tabloda verilmiştir.

Bu dokümanda yer alan tanım, terim ve ifadeler hazırlanırken TDK ve BTK dokümanları ile web kaynaklarından yararlanılmıştır. Kavramların Türkçe karşılıklarının en uygun şekilde kullanılmasına özen gösterilmiştir.

Not: Düzeltmesi gerektiği değerlendirilen ifadeler için önerilerinizi memnuniyetle karşılız.

English Term	Türkçe Karşılığı
Ad Exchange	Reklam Borsası
Ad repositories	Reklam arşivleri
Ad Repositories	Politik ve Kamusal Reklam Arşivleri / Reklam Kütüphaneleri
Ad Tech Tax	Reklam Teknolojisi Maliyeti
ADR (Alternative Dispute Resolution)	Mahkeme Dışı Uyuşmazlık Çözümü
Age Verification	Yaş Doğrulaması
Agentic AI	Eylemsel Yapay Zekâ
Aggregator	Toplayıcı
Agile Governance	Çevik yönetim
Agile Regulation	Öğrenen (Esnek) Regülasyon
Agile Regulation	Çevik Yönetişim
AI Act	Yapay Zekâ Yasası
Algorithm	Algoritma
Algorithmic Governance	Algoritmik Yönetişim
Algorithmic Impact Assessment (AIA)	Algoritmik Etki Analizi
Algorithmic Systems	Algoritmik Sistemler
Amplification	Yükseltme / yaygınlaştırma
API (Application Programming Interface)	Uygulama Programlama Arayüzü
App Store	Uygulama Mağazası
Attention Economy	Dikkat ekonomisi
Audit	Denetim
Automated tools	Otomatik araçlar
Barrier to entry	Pazara giriş engeli

Behavioral remedies	Davranışsal tedbirler
Behavioral surplus	Davranışsal artık
Black box	Kara kutu
The Black Box Society	Kara Kutu Toplumu
Caching	Ön belleğe alma
Chatbot	Sohbet robotu
Choice architecture	Seçim mimarisi
Class Actions	Kolektif Hak Arama / Sınıf Davaları / Temsilci davaları
Co-Regulation	Birlikte Düzenleme
Collusion	Algoritmik Gizli Anlaşma
Competition policy	Rekabet politikası
Compliance	Uyum
Compliance Officers	Uyum Görevlileri
Comply or Explain	Uygula veya Açıkla
Confidence Index	Güven Endeksi
Confidence Scores	Karar Kesinlik Skorları
Content moderation	İçerik moderasyonu
Conversational AI	Diyalog bazlı Yapay Zekâ
Coordinated Inauthentic Behavior (CIB)	Koordine Yapay Davranışlar
Creative compliance	Yaratıcı uyum
CSAM (Child Sexual Abuse Material)	Çocukların Cinsel İstismarı Materyali
Dark patterns	Karanlık tasarımlar
Data Brokerage / Data Brokers	Veri aracısı / Üçüncü taraf veri araçları
Data collection	Veri toplama
Data Dumping	Veri Kusması
Data processing	Veri işleme
Data sharing	Veri paylaşımı
Data siloing	Veri ayrıştırması
Data Sovereignty	Veri Egemenliği
Database	Veri tabanı
Deepfake	Sentetik içerik
Generative AI (GenAI)	Üretken Yapay Zekâ

Deterrence & Enforcement	Caydırıcılık ve Etkin uygulama
Digital economy	Dijital ekonomi
Digital Markets Act (DMA)	Dijital Pazarlar Yasası
Digital Services Act (DSA)	Dijital Hizmetler (Servisler) Yasası
Divestiture	Elden çıkarma
DRCF Model	Çoklu Kurum Eşgüdüm Modeli
DSP (Demand Side Platform)	Talep Tarafı Platformu
Dual Role Paradox	Hakem ve Oyuncu Çatışması
Duty of Care	Özen Yükümlülüğü
Echo Chambers	Yankı Odaları
Ecosystem	Ekosistem
Engagement	Etkileşim
Ex-ante	Öncül (Önleyici)
Explainable AI (XAI)	Açıklanabilir Yapay Zekâ
False Positive / False Negative	Yanlış pozitif (haksız kaldırma) / Yanlış negatif (gözden kaçırma)
Filter Bubbles	Filtre Balonları
Gatekeeper	Geçit bekçisi
GDPR (General Data Protection Regulation)	Genel Veri Koruma Tüzüğü (Türkiye'deki KVKK'nın AB'ndeki versiyonu)
Grooming	Cinsel Amaçlı Manipülasyon
Hosting	Barındırma
Human-in-the-loop	İnsan Denetimi / Müdahalesi
Hybrid platforms	Hibrit platformlar
Independent Auditing	Bağımsız Denetim
Innovation platforms	Yenilik platformları
Interim Measures	Geçici Tedbirler
Intermediary Services	Aracı Hizmetler
Interoperability	Birlikte çalışabilirlik
Know Your Business Customer (KYBC)	İş Ortaklarını/Müşterilerini Tanıma Prosedürü
Learning Regulation	Öğrenen Regülasyon
Lock-in effect	Kilitlenme etkisi
Market dominance	Piyasa hakimiyeti
Meaningful Reporting	Anlamlı Raporlama

Mere conduit	İletim hizmeti
Multi-homing	Çoklu Platform Kullanımı
Multi-stakeholder Governance	Çok Paydaşlı Yönetişim
Network effects	Ağ etkileri
NIS2 Directive	NIS2 Direktifi
Notice-and-Action	Bildir-ve-Aksiyon
OECD (Organisation for Economic Co-operation and Development)	Ekonomik İşbirliği ve Kalkınma Örgütü
Online Marketplace	Çevrim İçi Pazaryeri
Out-of-court dispute settlement / ADR	Mahkeme Dışı Uyuşmazlık Çözümü
P2B (Platform to Business)	Platformdan İşletmeye
Platform capitalism	Platform kapitalizmi
Platform-to-Business (P2B)	Platformdan İşletmeye
Privacy by Design	Tasarımla Gizlilik (Mahremiyet)
Private Label	Kendi Markalı Ürün
Profiling	Profilleme
Prosumer	Hem tüketici hem üretici
Regulatory Arbitrage	Düzenleyici Arbitraj / Hukuki Boşluk
Regulatory Sandboxes	Düzenleyici Kum Havuzları / Denetim alanları
Reporting Theater	Raporlama Tiyatrosu
Right to be Forgotten	Unutulma Hakkı
Risk-based approach	Risk temelli yaklaşım
RTB (Real-Time Bidding)	Gerçek Zamanlı Açık Artırma
Rule-maker	Kural koyucu
Rule-maker / Rule-taker	Kural koyucu / Kural alıcı (Kuralları takip eden)
Rule-taker	Kural takip eden
Safe Harbor	Güvenli Liman
Safety by Design / Privacy by Design	Tasarım Yoluyla Güvenlik / Tasarımla Gizlilik
Search Bias	Arama Tarafıllığı
Search Engine	Arama motoru
Search Engine Manipulation Effect (SEME)	Arama Motoru Manipülasyon Etkisi
Search Engine Results Page (SERP)	Arama Motoru Sonuçları Sayfası
Self-preferencing	Kendine öncelik verme / Kendini kayırma

Shadow Banning	Gölge Yasaklama / Görünürlük kaybı
Single Point of Contact	Tek Nokta Temas
Single Point of Failure	Tek Nokta Zafiyeti
SSP (Supply Side Platform)	Arz Tarafı Platformu
Stakeholder	Paydaş
Statement of reasons	Gerekçeli açıklama
Structural remedies	Yapısal tedbirler
Structural separation	Yapısal ayrıştırma
Surveillance Capitalism	Gözetim Kapitalizmi
Systemic Collapse	Sistemik Çöküş / Sistemik Sökülme
Transaction costs	İşlem maliyetleri
Transaction platforms	İşlem platformları
Transparency	Şeffaflık
Transparency Database	Şeffaflık veri tabanı
Trust Engineering	Güvenilirlik Mühendisliği
Trusted Flaggers	Güvenilir İşaretleyiciler / Güvenilir Bildirici
UCPD (Unfair Commercial Practices Directive)	Haksız Ticari Uygulamalar Direktifi
Ultima ratio	Nihai oran
User autonomy	Kullanıcı özerkliği
Very Large Online Platforms (VLOPs)	Çok Büyük Çevrim İçi Platformlar
Very Large Online Search Engines (VLOSEs)	Çok Büyük Çevrim İçi Arama Motorları
Viralite (Virality)	Ağ Etkisiyle Organik Yayılım

ŞEKİL LİSTESİ

ŞEKİL A: Dijital Manifesto

ŞEKİL 1-1: AB Gatekeepers - Geçit Bekçileri

ŞEKİL 2-1: Şeffaflık Anatomisi

ŞEKİL 2-2: Algoritmik Kara Kutu

ŞEKİL 2-3: Denetim Ekosistemi

ŞEKİL 3-1: Karanlık Tasarımlar ‘Dark Patterns’

ŞEKİL 4-1: Hakem-Oyuncu Paradoksu

ŞEKİL 4-2: E-Ticarette Adil Rekabet

ŞEKİL 4-3: Karanlık Tasarımlar

ŞEKİL 5-1: YZ Sistemleri ve Risk Temelli Sınıflandırma

ŞEKİL 5-2: Düzenleyici Kum Havuzu

ŞEKİL 6-1: Koordine Yapay Davranışlar

ŞEKİL 6-2: Reaktiften Proaktif Risk Yönetimine

ŞEKİL 6-3: Siber Güvenlik Dayanıklılığı- NIS2 ve DORA

ŞEKİL 6-4: Siber Dayanıklılık ve Süreklilik

ŞEKİL 7-1: Türkiye Durum Analizi

ŞEKİL 8-1: Çok Paydaşlı Çevik Yönetişim Modeli

ŞEKİL 8-2: Uygulama ve Entegrasyon Yol Haritası

ŞEKİL B: Türkiye Dijital Mevzuat Analizi-Stratejik Dönüşüm

TABLO LİSTESİ

TABLO 1-1: Kavramlar ve Regülasyonda İlgili Maddeler

TABLO 3-1: Şeffaflık Konusunda Türkiye ve AB Mevzuat Karşılaştırma Tablosu

TABLO 4-1: Gelir Modelleri, Yapısal Riskler ve Politika Tasarımı Tablosu

TABLO 4-2: Reklamcılık Konusunda AB Mevzuatı ve Türkiye’deki Durum Karşılaştırması

TABLO 6-1: Stratejik Regülatif Analiz ve Gelişim Tablosu

TABLO 8-1: Özet Uygulama Tablosu

KAYNAKÇA

- 4054 sayılı Rekabetin Korunması Hakkında Kanun (1994). T.C. Resmî Gazete, 22140, 13 Aralık 1994.
- 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun (2007). T.C. Resmî Gazete, 26529, 23 Mayıs 2007.
- 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun (2014). T.C. Resmî Gazete, 29168, 7 Kasım 2014.
- 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) (2016). T.C. Resmî Gazete, 29677, 7 Nisan 2016.
- 7253 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda Değişiklik Yapılmasına Dair Kanun (2020). T.C. Resmî Gazete, 31202, 31 Temmuz 2020.
- 7418 Sayılı Basın Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun (Dezenformasyon Yasası) (2022). T.C. Resmî Gazete, 31987, 18 Ekim 2022.
- AB’ndeki Güvenilir Bildirici Kuruluşlar. <https://digital-strategy.ec.europa.eu/en/policies/trusted-flaggers-under-dsa>
- Ada Lovelace Institute (2023). “Evaluating the Success of Digital Acts”.
- Agan, A. Y. et al., “Engagement, user satisfaction, and the amplification of divisive content on social media”, PNAS Nexus, 4(3), 2025, <https://doi.org/10.1093/pnasnexus/pgaf062>
- AI Act, European Union (2024). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689>
- Ali, M., Sapiezynski, P., Bogen, M., Korolova, A., Mislove, A., & Rieke, A. (2019). "Discrimination through Optimization: How Facebook's Ad Delivery Can Lead to Biased Outcomes in Job and Housing Ads". Proceedings of the ACM on Human-Computer Interaction.
- Ananny, M., & Crawford, K. (2018). "Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability". New Media & Society.

- Arcom, Fransa'daki Güvenilir Bildirici Kuruluşlar. <https://www.arcom.fr/en/about-us-our-missions/supervise-online-platforms-and-social-networks/digital-services-agreement-dsa-list-trusted-flaggers-designated-arcom>
- Benkler, Y., Faris, R., & Roberts, H. (2018). "Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics". Oxford University Press.
- Bill C-18, Government of Canada (2023). "An Act respecting online communications platforms that make news content available to persons in Canada".
- Bill C-27, Government of Canada (2022). "Digital Charter Implementation Act. Including Consumer Privacy Protection Act (CPPA) and Artificial Intelligence and Data Act (AIDA)".
- Binns, R. (2018). "Algorithmic Accountability and Public Law". Public Law.
- Bovens, M. (2007). "Analysing and Assessing Accountability: A Conceptual Framework". European Law Journal.
- Bradford, A. (2020). "The Brussels Effect: How the European Union Rules the World". Oxford University Press.
- Bradford, A. (2023). "The Brussels Effect: How the European Union Rules the World. (Updated Edition)". Oxford University Press.
- Bradford, Anu. "The Brussels Effect: How the European Union Rules the World". Oxford University Press, 2020. <https://global.oup.com/academic/product/the-brussels-effect-9780190088583>
- Brous, P., & Janssen, M. (2024). "Sovereign Clouds and Cyber-Resilience: Navigating NIS2". Journal of Strategic Information Systems.
- Bruns, A. (2019). "After the API Calypse: Social Media Platforms and Their Fight Against Critical Independent Research". Information, Communication & Society.
- Brynjolfsson, E., Hu, Y. J., & Rahman, M. S. (2013). "Competing in the Age of Omnichannel Retailing". MIT Sloan Management Review.
- BTK (Bilgi Teknolojileri ve İletişim Kurumu) (2024). "Sosyal Ağ Sağlayıcıları Şeffaflık Raporları Analizi".

- Bundesnetzagentur, Almanya'daki Güvenilir Bildirici Kuruluşlar.
https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/EN/2025/20250602_TrustedFlagger.html
- Caffarra, C., & Morton, F. S. (2024). "Gatekeeper Governance: The First Wave of DMA Enforcement". Yale School of Management Research Paper.
- Caffarra, C., & Morton, F. S. (2024). "The Economics of Enforcement under the DMA". Yale University School of Management.
- Canadian Ministry of Innovation (2025). "AIDA: Ethical Guidelines for Recommender Systems in Social Networks".
- Canadian Ministry of Innovation (2025). "The AIDA Companion: A Guide to the Artificial Intelligence and Data Act".
- Cho, Clare Y.; Zhu, Ling, (2023). "Defining and Regulating Online Platforms". Library of Congress, USA. <https://www.congress.gov/crs-product/R47662>
- CIGI (Centre for International Governance Innovation) (2023-2024). "Global Platform Governance Network (GPGN) Series & Advancing Multi-stakeholderism for AI Governance".
- Çok Büyük Çevrim İçi Arama Motoru (Very Large Online Search Engine): AB'de aylık en az 45 milyon aktif kullanıcıya ulaşan arama motorları VLOSE olarak sınıflandırılır.
- Çok Büyük Çevrim İçi Platform (Very Large Online Platform): DSA'ya göre, AB içinde aylık ortalama en az 45 milyon aktif kullanıcıya ulaşan çevrim içi platformlar VLOP olarak sınıflandırılır.
- Commission Decision Establishing the European AI Office, (2024). <https://digital-strategy.ec.europa.eu/en/library/commission-decision-establishing-european-ai-office>
- Community Standards Enforcement Reports | Transparency Center n.d.
<https://transparency.meta.com/reports/community-standards-enforcement/>
- Costanza-Chock, S. (2020). "Design Justice: Community-Led Practices to Build the Worlds We Need". MIT Press.

- Council of Europe (2024). "Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law". <https://rm.coe.int/1680afae3c> ve <https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence>
- Council of Europe (2020). "Guidelines on Algorithmic Systems and Human Rights".
- Crawford, K., & Gillespie, T. (2016). "What is a Data Set?". Social Media + Society.
- Cristos Goodrow, (2025). "On YouTube's Recommendation System, Youtube Blog". <https://blog.youtube/inside-youtube/on-youtubes-recommendation-system/>
- Cusumano, M. A., Gawer, A., & Yoffie, D. B. (2021). "The Business of Platforms: Strategy in the Age of Digital Competition, Innovation, and Power". Harper Business.
- Cyberspace Administration of China, "Administrative Provisions on Recommendation Algorithms in Internet-based Information Services", 2022, http://www.cac.gov.cn/2022-01/04/c_1642894606364259.htm
- Cyberspace Administration of China, "Interim Measures for the Management of Generative Artificial Intelligence Services", 2023, http://www.cac.gov.cn/2023-07/13/c_1690898327029107.htm
- De Streel, A. (2024). "The Institutional Architecture of Digital Regulation: Efficiency, Accountability and Independence". Centre on Regulation in Europe (CERRE).
- Department for Science, Innovation and Technology, UK (2023). "A Pro-innovation Approach to AI Regulation".
- "Developing Cyber-Resilient Systems: A Systems Security Engineering Approach" (2021). <https://csrc.nist.gov/pubs/sp/800/160/v2/r1/final>
- Diakopoulos, N. (2016). "Algorithmic Accountability: Journalistic investigation of computational power structures." Digital Journalism.
- DMA (Digital Markets Act), https://digital-markets-act.ec.europa.eu/index_en ve <https://eur-lex.europa.eu/eli/reg/2022/1925/oj>
- DORA (Digital Operational Resilience Act - Regulation (EU) 2022/2554). <https://www.digital-operational-resilience-act.com/>

- DRCF (2024). "Annual Plan and Collaborative Projects."
- DSA (Digital Services Act), European Union (2022). <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act> ve <https://eur-lex.europa.eu/eli/reg/2022/2065/oj>
- DSA Madde 16, https://www.eu-digital-services-act.com/Digital_Services_Act_Article_16.html
- DSA Madde 17, https://www.eu-digital-services-act.com/Digital_Services_Act_Article_17.html
- DSA Madde 20, https://www.eu-digital-services-act.com/Digital_Services_Act_Article_20.html
- DSA Madde 21, https://www.eu-digital-services-act.com/Digital_Services_Act_Article_21.html
- DSA Madde 22, https://www.eu-digital-services-act.com/Digital_Services_Act_Article_22.html
- DSA Madde 25, https://www.eu-digital-services-act.com/Digital_Services_Act_Article_25.html
- DSA Madde 28, https://www.eu-digital-services-act.com/Digital_Services_Act_Article_28.html
- DSA Madde 34, https://www.eu-digital-services-act.com/Digital_Services_Act_Article_34.html
- DSA Madde 40, https://www.eu-digital-services-act.com/Digital_Services_Act_Article_40.html
- DSA Madde 45, https://www.eu-digital-services-act.com/Digital_Services_Act_Article_45.html
- DSA Madde 48, https://www.eu-digital-services-act.com/Digital_Services_Act_Article_48.html
- DSA Transparency Database : Questions and Answers, (2025). <https://digital-strategy.ec.europa.eu/en/faqs/dsa-transparency-database-questions-and-answers>
- Epstein, R., & Robertson, R. E. (2015). "The search engine manipulation effect (SEME) and its possible impact on the outcomes of elections". Proceedings of the National Academy of Sciences (PNAS), 112(33), E4512-E4521.
- EU Artificial Intelligence Act. "Up-to-date Developments and Analyses of the EU AI Act". <https://artificialintelligenceact.eu/>
- EU still hosts the most child sexual abuse material in the world. <https://www.iwf.org.uk/news-media/news/eu-still-hosts-the-most-child-sexual-abuse-material-in-the-world/>
- European Commission (2020). "Impact Assessment on the Observatory on the Online Platform Economy"

- European Commission (2023). “Better Regulation: Guidelines and Toolbox”.
- European Commission (2023). “Eurobarometer 535: Online platforms and consumer protection”. Directorate-General for Communication
- European Commission (2023). “Guidelines on the implementation of risk assessments under the DSA”.
- European Commission (2024). “Guidelines on the designation of Single Points of Contact under the DSA”.
- European Commission, “AI Act: General-purpose AI models”, 2024, <https://digital-strategy.ec.europa.eu/en/faqs/general-purpose-ai-models-ai-act-questions-answers>
- European Commission (2025), "The Impact of DSA on Digital Platforms: Transparency and content moderation report". Shaping Europe’s Digital Future.
- European Commission (2025). "Guidelines on the implementation of Art. 31 of the DSA (Data Access)".
- European Commission (2025). “Commission preliminarily finds TikTok’s ad repository in breach of the Digital Services Act”. <https://digital-strategy.ec.europa.eu/en/news/commission-preliminarily-finds-tiktoks-ad-repository-breach-digital-services-act>
- European Commission (2026). “Comprehensive Review of the Digital Services Act Implementation: Year Two Report”. Brussels.
- European Commission (2026). “Guidance on the Prevention of Dark Patterns in E-Commerce Interfaces under the DSA”.
- European Commission (2026). “Implementation Report on ADR Centers under the Digital Services Act”.
- European Commission (2026). “Implementation Report on VLOPs Sanctions under the DSA”.
- European Networks of National Human Rights Institutions (ENNHRI), (2025). “European Regulatory Frameworks on AI”. <https://ennhri.org/ai-resource/european-regulatory-frameworks-on-ai/>

- European Parliament and Council, “Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)”, 2024, <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>
- European Parliament Study (2025). "Interplay between the AI Act and the EU digital legislative framework".
- Evans, P. C., & Gawer, A. (2016). “The Rise of the Platform Enterprise: A Global Survey. The Center for Global Enterprise”.
- Ezrachi, A., & Stucke, M. (2020). “Virtual Competition”. Harvard University Press.
- Feedvisor (2022). “The Amazon Consumer Behavior Report: Inside the minds of consumers and their purchasing habits”.
- Floridi, L. (2024). “The Ethics of Algorithmic Curation in Social Media”. Springer.
- Floridi, L. (2024). “The Ethics of Artificial Intelligence: Principles, Challenges, and Opportunities”. Oxford University Press.
- G7 Enforcers’ Summit (2023). “Inventory of Rules and Enforceability in the Digital Economy. Joint Report by G7 Competition Authorities”. Tokyo/Hiroshima.
- Gawer, A. (2014). “Bridging differing perspectives on technological platforms: Toward an integrative framework”. Research Policy, 43(7), 1239-1249.
- GDPR (General Data Protection Regulation), (2024). <https://gdpr-info.eu/> ve <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- Geçit Bekçisi Şirketler ve Servisleri, https://digital-markets-act.ec.europa.eu/gatekeepers_en
- Geradin, D. (2023). “The Digital Markets Act (DMA): A New Era for EU Competition Law in the Digital Sector”. Journal of European Competition Law & Practice.
- Geradin, D. (2024). "Adjudicating the DMA: The Role of National Courts". Journal of European Competition Law.
- Geradin, D. (2024). "Innovation-Friendly Enforcement of Digital Acts". Journal of European Competition Law.

- Geradin, D. (2024). "Self-Preferencing in the Digital Age: Lessons from the first DMA designations". Journal of European Competition Law.
- Ghoshal, A., & Mukhopadhyay, T. (2022). "Impact of Sponsored Search on Organic Results and Total Clicks in E-commerce". Management Science & Information Systems.
- Gillespie, T. (2018). "Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media". Yale University Press.
- Gillespie, T. (2020). "Content moderation, AI, and the question of scale". Big Data & Society.
- Google (2024). "How Search Works: From algorithms to answer"s. Google Search Central.
- Google (çeşitli yıllar). Transparency Reports.
- Gorwa, R. (2019). "What is platform governance?". Information, Communication & Society.
- GPAI (Global Partnership on Artificial Intelligence). <https://oecd.ai/en/>
- Grimmelmann, J. (2024). "The Law of Search Engines: Governance and Neutrality", Columbia Law Review.
- Helberger, N., et al. (2020). "The concept of the 'Gatekeeper' in the Digital Markets Act: A Legal and Economic Analysis". Common Market Law Review.
- Herbert A. Simon, "Designing Organizations for an Information-Rich World" in Computers, Communications, and the Public Interest, ed. Martin Greenberger (Baltimore, MD: The Johns Hopkins Press, 1971), 40–41
- Hofmann, V., Murauer, L., & Bondorf, S. (2023). "Content moderation on social media in the EU: Insights from the DSA Transparency Database". <https://doi.org/10.48550/arXiv.2312.04431>
- How TikTok Recommends Content. n.d. <https://support.tiktok.com/en/using-tiktok/exploring-videos/how-tiktok-recommends-content>
- IAB Türkiye Medya ve Reklam Yatırımları Raporları. <https://iabtr.org/turkiye-tahmini-medya-ve-reklam-yatirimlari/>
- ICN (International Competition Network). <https://www.internationalcompetitionnetwork.org/>

- Inauthentic Behaviour, Meta Reports, (2026). <https://transparency.meta.com/policies/community-standards/inauthentic-behavior/>
- Insider Intelligence / eMarketer (2023). “Worldwide Ecommerce Forecasts 2023: Global Retail Sales and Market Share”.
- International Organization for Standardization (ISO), “ISO/IEC 42001:2023 – Artificial intelligence management system”, 2023, <https://www.iso.org/standard/81230.html>
- Introna, L. D., & Nissenbaum, H. (2000). "Shaping the Web: Why the Politics of Search Engines Matters". The Information Society, 16(3), 169-185.
- Íris Damião, José M. Reis, Paulo Almeida, Nuno Santos, Joana Gonçalves-Sá (2025). “Digital Gatekeeping: An Audit of Search Engine Results shows tailoring of queries on the Israel-Palestine Conflict.”
- ISO/IEC 42001:2023. <https://www.iso.org/standard/42001>
- Jean Tirole (2017). “Economics for the Common Good”.
- Jungle Scout. (2023). “Amazon Advertising Report: Key Trends and Benchmarks for E-commerce Sellers”.
- Kayser-Bril, N. (2020). "Why Transparency Reporting is Not Enough". AlgorithmWatch Report.
- Khan, L. (2017). “Amazon’s antitrust paradox”. Yale Law Journal.
- Khan, L. M. (2025). "Platform Monopolies and Data Advantage: The Case for Structural Remedies". Yale Law Journal.
- Klonick, K. (2018). "The New Governors: The People, Rules, and Processes Governing Online Speech". Harvard Law Review.
- Krawiec, K. D. (2003). "Cosmetic Compliance and the Failure of Negotiated Governance". Washington University Law Quarterly.
- LSE (The London School of Economics and Political Science), (2022). “Algorithmic Accountability and Transparency Report”.
- Meta. “Community Standards Enforcement Report”.

- Mökander, J. et al. (2024). "Algorithm Auditing in Practice: Lessons from the DSA Sandbox". AI & Society.
- Mökander, J. et al. (2024). "Auditing AI: The Role of Independent Bodies in Legal Redress". AI & Society.
- Mökander, J., Morley, J., Taddeo, M., & Floridi, L. (2024). "Auditing High-Risk AI Systems: A Governance Framework for the EU AI Act". International Journal of Law and Information Technology.
- Monti, G., & Colomo, P. I. (2025). "Interplay of Digital Regulations: DMA, DSA and Beyond". Oxford University Press.
- National Institute of Standards and Technology (NIST), US Department of Commerce (2025). "AI Risk Management Framework". <https://www.nist.gov/itl/ai-risk-management-framework>
- National Retail Federation (NRF) & Appriss Retail (2023). "2023 Retail Returns Survey: A Year-End Analysis".
- NIS2 Directive, (2022). <https://eur-lex.europa.eu/eli/dir/2022/2555/2022-12-27/eng>
- NIST, "Artificial Intelligence Risk Management Framework (AI RMF 1.0)", 2023, <https://www.nist.gov/publications/artificial-intelligence-risk-management-framework-ai-rmf-10>
- Noble, S. U. (2018). "Algorithms of Oppression: How Search Engines Reinforce Racism". NYU Press.
- OECD (2019). "An Introduction to Online Platforms and Their Role in the Digital Transformation". OECD Publishing, Paris, <https://doi.org/10.1787/53e5f593-en>
- OECD (2019). "Artificial Intelligence and Public Policy".
- OECD (2019). "Regulatory Impact Assessment (RIA)".
- OECD (2020). "OECD Guidelines on Relevant Standards for Transparency and Accountability in the Digital Economy".
- OECD (2020). "Competition in Digital Advertising Markets" <https://www.oecd.org/daf/competition/competition-in-digital-advertising-markets.html>

- OECD (2021), “Competition in Digital Advertising Markets”, OECD Roundtables on Competition Policy Papers, No. 259, OECD Publishing, Paris, <https://doi.org/10.1787/f2209674-en>
- OECD (2021), “Transparency reporting on terrorist and violent extremist content online: An update on the global top 50 content sharing services”. OECD Digital Economy Papers, No. 313, OECD Publishing, Paris, <https://doi.org/10.1787/8af4ab29-en>
- OECD (2021). “Transparency reporting on content moderation: A review of current practices”.
- OECD (2022). “Declaration on Government Access to Personal Data Held by Private Sector Entities”.
- OECD (2022). “Recommendation of the Council on the Governance of Digital Platforms. OECD/LEGAL/0482”
- OECD (2023): “Handbook on Competition Policy in the Digital Age.” OECD Publishing, Paris.
- OECD (2024), "Competition Policy in Digital Markets: The Combined Effect of Ex Ante and Ex Post Instruments in G7 Jurisdictions".
- OECD (2024). “Cooperation Between Competition and Data Protection Authorities”. OECD Competition Policy Roundtables.
- OECD (2024). “Design of Enforcement and Sanctions in Digital Markets”. OECD Digital Economy Papers.
- OECD (2024). “E-commerce and Competition: Data Strategies of Hybrid Platforms”. OECD Digital Economy Papers.
- OECD (2024). “Report on Emerging Trends in Digital Platform Regulation”. OECD Digital Economy Papers.
- OECD, “Recommendation of the Council on Artificial Intelligence”, OECD/LEGAL/0449, 2024, <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>
- OECD Üye Ülke Listesi, <https://www.oecd.org/en/about/members-partners.html>
- OECD, AI Principles. <https://www.oecd.org/en/topics/sub-issues/ai-principles.html>
- OECD, Digital Government, <https://www.oecd.org/en/topics/digital-government.html>
- OECD, “OECD AI Principles: Overview and Updates”, 2024, <https://oecd.ai/en/ai-principles>

- Ofcom (2023). “Compliance and Enforcement Approach for the Online Safety Act”.
- Ofcom (2024). "Approach to Algorithmic Assessment in Online Safety".
- Ofcom UK (2025). “Online Safety Act: Final Codes of Practice and Enforcement Guidelines”.
- Ofcom UK (2025). “Protecting Children from Online Harm: Codes of Practice for Social Media”.
- O'Neil, C. (2016). “Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy”. Crown.
- OSA (Online Safety Act) in UK, (2023).
<https://www.legislation.gov.uk/ukpga/2023/50/contents/enacted>
- P2B Regulation, European Union (2019). <https://eur-lex.europa.eu/eli/reg/2019/1150/oj>
- Pablo Ibáñez Colomo, 2007. "The Draft Digital Markets Act: A Restraint on the Exercise of Market Power or a Reimagining of the Role of the State in the Economy?". European Law Review, 46(3), 2021, s. 296; Giorgio Monti, EC Competition Law, Cambridge University Press, s. 61.
- Pariser, E. (2011). “The Filter Bubble: What the Internet Is Hiding from You”. Penguin Press.
- Parker, C., & Nielsen, V. L. (2011). “Explaining Compliance: Business Responses to Regulation”. Edward Elgar Publishing.
- Pasquale, F. (2015). “The Black Box Society: The Secret Algorithms That Control Money and Information”. Harvard University Press.
- Pew Research Center. (2023). “Understanding the Algorithmic Experience: How Users Perceive and Interact with Social Media Recommendation Systems”. Washington, D.C.
- Postmortem of database outage of January 31, 2017. <https://about.gitlab.com/blog/postmortem-of-database-outage-of-january-31/>
- Power, M. (1997). “The Audit Society: Rituals of Verification”. Oxford University Press.
- Proposal for laying down rules to prevent and combat child sexual abuse. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0209>
- Protecting children from sexual abuse. https://home-affairs.ec.europa.eu/policies/internal-security/protecting-children-sexual-abuse_en

- Quinn Emanuel (2025), "Litigating the DMA & DSA: Current Landscape"
- Quinn Emanuel (2025). "Digital Litigation Trends: The Rise of Out-of-Court Dispute Settlements under the DSA".
- Recommendation of the Council on Children in the Digital Environment.
<https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0389>
- Rekabet Kurumu (2021). "Dijital Platformlar Hakkında Sektör Araştırması Ön Raporu".
- Rekabet Kurumu (2024). <https://www.rekabet.gov.tr/tr/Guncel/google-reklamcilik-ve-pazarlama-ltd-sti--5c808b3e47b9ef1193d90050568585c9>
- Rekabet Kurumu'nun Google ile ilgili kararları.
https://www.google.com/url?q=https://www.rekabet.gov.tr/tr/Kararlar?page%3D1%26sayfaAdi%3DGoogle&sa=D&source=docs&ust=1773259931301155&usg=AOvVaw35L0shw1f7mjE8OrjNHM_J
- Ricci, F., Rokach, L., & Shapira, B. (2021). "Recommender Systems Handbook". Springer.
- Rieder, B. et al. (2022). "Algorithmic influence on public discourse". New Media & Society.
- Roberts, S. T. (2019). "Behind the Screen: Content Moderation in the Shadows of Social Media". Yale University Press.
- Rochet, J.-C., & Tirole, J. (2003). "Platform competition". Journal of the European Economic Association.
- Scott, C., & Yeung, K. (2025). "Algorithmic Governance and the Law". Edward Elgar Publishing.
- Selbst, A. D. (2017). "Disparate Impact in Algorithmic Decision-Making". Yale Law Journal.
- Summary of the AWS Service Event in the Northern Virginia (US-EAST-1) Region, (2021).
<https://aws.amazon.com/message/12721/>
- Sunstein, C. R. (2017). "#Republic: Divided Democracy in the Age of Social Media". Princeton University Press.
- The EU approach to age verification. <https://digital-strategy.ec.europa.eu/en/policies/eu-age-verification>
- Ticaret Bakanlığı. (2023). "Türkiye E-Ticaret Ekosistemi ve Yeni Mevzuat Rehberi".

- TikTok. “Transparency Report”.
- Tiwana, A. (2013). “Platform Ecosystems: Aligning Architecture, Governance, and Strategy”. Morgan Kaufmann
- Treasury Board of Canada Secretariat, (2026). “Algorithmic Impact Assessment Tool”
<https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/algorithmic-impact-assessment.html>
- Tufekci, Z. (2017). “Twitter and Tear Gas: The Power and Fragility of Networked Protest”. Yale University Press.
- Türk Dil Kurumu (TDK) Sözlüğü, <https://sozluk.gov.tr/>
- Türkiye Bilişim Derneği (TBD) Bilişim Terimleri Sözlüğü, 30 Mart 2026 tarihli güncellenmiş versiyon.
- Türkiye Büyük Millet Meclisi, “6698 sayılı Kişisel Verilerin Korunması Kanunu”, 2016,
<https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=6698&MevzuatTur=1&MevzuatTertip=5>
- T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi & Sanayi ve Teknoloji Bakanlığı, “Ulusal Yapay Zekâ Stratejisi 2021–2025”, 2021, <https://cbddo.gov.tr/SharedFolderServer/Genel/File/TR-UlusalYZStratejisi2021-2025.pdf>
- T.C. Cumhurbaşkanlığı (2024). “Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2024-2028) Hakkında 2024/11 Sayılı Genelge”. T.C. Resmî Gazete, 32655, 7 Eylül 2024.
- T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, “Ulusal Yapay Zekâ Stratejisi 2024–2025 Eylem Planı”, 2024, <https://www.sanayi.gov.tr/assets/pdf/UlusalYapayZekâStratejisi2024-2025EylemPlani.pdf>
- Twitter/The-algorithm: “Source Code for the X Recommendation Algorithm.” n.d. GitHub.
<https://github.com/twitter/the-algorithm>
- UK Parliament (2024). “Digital Markets, Competition and Consumers Act 2024. Strategic Market Status (SMS) framework and regulatory codes of conduct”. London: Stationery Office.
- UK Parliament (2024). “Digital Markets, Competition and Consumers Act 2024”. Appeal Mechanisms.

- UNESCO, Ethics of Artificial Intelligence, (2021). <https://www.unesco.org/en/artificial-intelligence/recommendation-ethics>
- Unfair Commercial Practices Directive (Directive 2005/29/EC), <https://eur-lex.europa.eu/eli/dir/2005/29/oj>
- Unver, H. A. (2019). "Politics of Algorithmic Governance: Surveillance, Bias and Content Moderation". EDAM Cyber Policy Paper.
- Van Dijck, J., Poell, T., & De Waal, M. (2018). "The Platform Society: Public Values in a Connective World". Oxford University Press.
- Venice Commission (2020). "Principles for a Fundamental Rights-compliant Use of Digital Technologies in Electoral Processes". Council of Europe, Study No. 949/2019.
- "Vetted researchers", belirli kriterler doğrultusunda ön incelemeden geçirilmiş, uygunluğu doğrulanmış ve yetkilendirilmiş araştırmacılar anlamına gelir. Türkçe olarak "Yetkilendirilmiş araştırmacılar" tanımı kullanılabilir.
- Vries, K. D. (2020). "The Right to an Explanation: Algorithmic Decision-Making and the GDPR." Oxford University Press.
- Wagner, B. (2018). "Algorithmic Accountability: Towards a Policy Framework". Human Rights and Encryption.
- Wardle, C. (2019). "Information Disorder: Toward an interdisciplinary framework for research and policymaking". First Draft News.
- World Economic Forum (2020). "Agile Regulation for the Fourth Industrial Revolution: A Toolkit for Regulators".
- Yılmaz, M. C. (2021). "Kişisel Verilerin Korunması Kanunu ve Dijital Platformların Hesap Verebilirliği". KVKK Hakemli Dergi.
- York, J. C. (2021). "Silicon Values: The Future of Free Speech under Surveillance Capitalism". Verso Books.
- Zelnick, S., & West, S. M. (2021). "The Limits of Transparency: Data Brokerage and the Privacy of Algorithmic Systems". New Media & Society.

- Zuboff, S. (2019). “The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power”. PublicAffairs.
- Zuboff, S. (2025). "Collective Redress as a Check on Surveillance Capitalism". Journal of Digital Rights.
- Zuboff, S. (2025). "The New Frontiers of Behavioral Manipulation in Social Networks". Journal of Social Computing.