



İSTANBUL MEDENİYET ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
ÖZEL HUKUK ANABİLİM DALI

**AB Dijital Hizmetler Kanunu ve Yapay Zekâ Kanunu
Kapsamında Yapay Zekâ Aracılığıyla Sosyal Medyada
Yapılan Müdahaleler**

Yüksek Lisans Tezi

Muhammed Enes Demirtaş

Eylül 2025



İSTANBUL MEDENİYET ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
ÖZEL HUKUK ANABİLİM DALI

**AB Dijital Hizmetler Kanunu ve Yapay Zekâ Kanunu
Kapsamında Yapay Zekâ Aracılığıyla Sosyal Medyada
Yapılan Müdahaleler**

Yüksek Lisans Tezi

Muhammed Enes Demirtaş

Danışman

Dr. Öğr. Üyesi Şerafettin Ekici

Eylül 2025

TEZ JÜRİSİ ONAYI

Muhammed Enes Demirtaş tarafından hazırlanan "AB Dijital Hizmetler Kanunu ve Yapay Zekâ Kanunu Kapsamında Yapay Zekâ Aracılığıyla Sosyal Medyada Yapılan Müdahaleler" başlıklı bu Yüksek Lisans Tezi, Özel Hukuk Anabilim Dalı'nda hazırlanmış ve jürimiz tarafından kabul edilmiştir.

JÜRİ ÜYELERİ

İMZA

Tez Danışmanı:

Dr. Öğr. Üyesi Şerafettin Ekici
İstanbul Medeniyet Üniversitesi

Üyeler:

Doç. Dr. Harun Eryiğit
İstanbul Medipol Üniversitesi

Dr. Öğr. Üyesi Abdurrahman Hamza Tüzgen
İstanbul Medeniyet Üniversitesi

Tez Savunma Tarihi: 19/09/2025

BEYANLAR

Yazım ve Kaynak Gösterme Kılavuzu Beyanı

Danışmanlığımda yazılan bu tezin Chicago Manual of Style 18th Edition (notes and bibliography) yazım ve kaynak gösterme kılavuzunda belirtilen kurallara uygun olarak yapılandırıldığı ve bu kılavuzun dipnot kaynak gösterme standartlarının bu tezde tutarlı olarak uygulandığı tarafımdan incelenerek teyit edilmiştir.

İmza

Dr. Öğr. Üyesi Şerafettin Ekici

Etik İlkeler Sadakat Beyanı

Hazırladığım bu tezin tamamen kendi çalışmam olduğunu, akademik ve etik kuralları gözeterek çalıştığımı ve her alıntıya kaynak gösterdiğimi beyan ederim.

İmza

Muhammed Enes Demirtaş

ÖZET

AB Dijital Hizmetler Kanunu ve Yapay Zekâ Kanunu Kapsamında Yapay Zekâ Aracılığıyla Sosyal Medyada Yapılan Müdahaleler

Demirtaş, Muhammed Enes

Yüksek Lisans Tezi, Özel Hukuk Anabilim Dalı

Danışman: Dr. Öğr. Üyesi Şerafettin Ekici

Eylül 2025

20. yüzyılda gelişmeye başlayan ve milenyumla birlikte gelişimi devam eden oyun değiştirici iki güç, sosyal medya ve yapay zekâdır. Web (internet) tabanlı bir çevrim içi ortam olan sosyal medya, toplumun sosyalleşmesinde, çeşitli içeriklerin paylaşımında ve bilgi aktarımı ve üretilmesinde önemli bir rol oynamaktadır. Makine öğrenmesi, derin öğrenme, doğal dil işleme ve veri biliminden müteşekkil bir olgu olan yapay zekâ ise toplumsal dengeleri yeniden oluşturmaktadır. Yapay zekâ, kişilerin angarya olarak nitelendirilen işlerini saniyeler içinde yaparken sosyal medya platformlarının çevrim içi ortamda yardımcısı olmaktadır. Sosyal medya platformları “Topluluk Kuralları”nı uygulamak ve kullanıcılarının çevrim içi deneyimini iyileştirmek için yapay zekâ teknolojisinden faydalanmaktadır. Bu doğrultuda kullanılan yazılımlar, kullanıcı tarafından sağlanan içeriği incelemekte, platform kurallarını ihlal eden bir durumda söz konusu içeriğe erişimi engellemekte yahut içeriği erişimden kaldırmaktadır. Kullanıcıların içeriklerine yapılan bu müdahale hukuka uygun olabileceği gibi hukuka aykırı da olabilmektedir. Söz konusu yapay zekâ yazılımının hatalı müdahalesi durumunda platform kullanıcılarının başta ifade özgürlüğü olmak üzere temel hak ve hürriyetleri kısıtlanmaktadır. Avrupa Birliği kanun koyucusu gerek sosyal medya gerek yapay zekâ teknolojisinin toplumsal yaşamdaki bu gibi olumsuz etkilerini azaltmak ve AB vatandaşlarının güvenli, şeffaf bir çevrim içi deneyim yaşamalarını sağlamak ve temel hak ve hürriyetlerini güvence altına almak amacıyla Dijital Hizmetler Kanunu’nu ve Yapay Zekâ Kanunu’nu ihdas etmiştir. Türk Hukukunda sosyal ağ sağlayıcı olarak ifade edilen çevrim içi platformlar için Dijital Hizmetler Kanunu ile pasif durumdan aktif bir rol almaları yönünde hükümler ihdas edilmiştir. Yapay Zekâ Kanunu kapsamında ise yapay zekâ sistemlerinin temel hak ve hürriyetleri dikkate alan, insanı merkeze alacak şekilde geliştirilmesi hedeflenmektedir.

Anahtar Kelimeler: Yapay Zekâ, Sosyal Medya, Dijital Hizmetler Kanunu, Yapay Zekâ Kanunu, Filtreleme

ABSTRACT

Interventions In Social Media By Means of Artificial Intelligence Under The EU Digital Services Act And The EU Artificial Intelligence Act

Demirtas, Muhammed Enes

Master's Thesis, Department of Private Law

Supervisor: Ast. Prof. Dr. Serafettin Ekici

September 2025

Two game-changing forces that began to develop in the 20th century and continued to evolve with the millennium are social media and artificial intelligence. Social media, an online environment based on the web (internet), plays a significant role in the socialisation of society, the sharing of various content, and the transfer and production of information. Artificial intelligence, a phenomenon comprising machine learning, deep learning, natural language processing, and data science, is reshaping social balances. Artificial intelligence performs tasks that individuals consider tedious in seconds while assisting social media platforms in the online environment. Social media platforms utilise artificial intelligence technology to enforce their “Community Guidelines” and improve their users' online experience. In this regard, the software used reviews content provided by users and, in cases where platform rules are violated, blocks access to or removes the content in question. Such intervention in users' content may be lawful or unlawful. In the event of erroneous intervention by the artificial intelligence software in question, the fundamental rights and freedoms of platform users, primarily freedom of expression, are restricted. The European Union legislator has enacted the Digital Services Act and the Artificial Intelligence Act to reduce such negative effects of social media and artificial intelligence technology on social life, to ensure that EU citizens have a safe and transparent online experience, and to safeguard their fundamental rights and freedoms. The Digital Services Act introduces provisions requiring online platforms, referred to as social network providers in Turkish law, to take on an active role rather than a passive one. Under the Artificial Intelligence Act, the aim is to develop artificial intelligence systems in a way that takes fundamental rights and freedoms into account and puts people at the centre.

Keywords: Artificial Intelligence, Social Media, Digital Services Act, AI Act, Filtering

İÇİNDEKİLER

ŞEMA LİSTESİ.....	V
KISALTMALAR.....	VI
GİRİŞ.....	1

BİRİNCİ BÖLÜM

SOSYAL MEDYA VE YAPAY ZEKÂ

I) SOSYAL MEDYA.....	3
A. SOSYAL MEDYANIN TANIMI.....	3
B. SOSYAL MEDYANIN TARİHİ.....	8
C. SOSYAL MEDYA SÜJELERİ.....	12
1. İçerik Sağlayıcı.....	12
2. Yer Sağlayıcı	14
3. Erişim Sağlayıcı.....	16
4. Toplu Kullanım Sağlayıcı	18
5. Sosyal Ağ Sağlayıcı.....	19
a) Temsilci Belirleme ve Bildirme Yükümlülüğü	23
b) Başvurulara Cevap Verme Yükümlülüğü.....	27
c) Raporlama Yükümlülüğü	28
d) BTK ve Kolluk Birimlerine Bilgi Verme Yükümlülüğü.....	29
e) Yargı Mercilerine Bilgi Verme Yükümlülüğü.....	30
f) Türkiye’deki Kullanıcıların Verilerini Türkiye’de Barındırma ve Kullanıcı Haklarına İlişkin Düzenlemelere Uyma Yükümlülüğü.....	32
g) Çocuklara Özgü Ayrıştırılmış Hizmet Sunma Yükümlülüğü.....	34

h) Etkin Başvuru Mekanizması Kurma ve Kriz Planı	
Oluşturma ve Bildirme Yükümlülüğü.....	34
II) YAPAY ZEKÂ.....	35
A. KAVRAMSAL ÇERÇEVE VE TANIM.....	36
B. YAPAY ZEKÂNIN TARİHİ	39
C. YAPAY ZEKÂNIN ALT DALLARI	41
D. YAPAY ZEKÂ TÜRLERİ	43
1. Gelişmişlik Düzeyine Göre Ayrım	43
2. Fonksiyonlarına (İşlevlerine) Göre Ayrım	44
E. YAPAY ZEKÂNIN HUKUKİ NİTELİĞİ	46

İKİNCİ BÖLÜM

DİJİTAL HİZMETLER KANUNU VE YAPAY ZEKÂ KANUNU EKSENİNDE SOSYAL MEDYA VE YAPAY ZEKÂ

I) DİJİTAL HİZMETLER KANUNU (DSA)	52
A. DÜZENLEMENİN GEREKLİLİĞİ VE AMACI.....	53
B. SOSYAL AĞ SAĞLAYICILARINA GETİRİLEN YÜKÜMLÜLÜKLER.	58
1. İrtibat Noktası ve Yasal Temsilci Belirlenmesi	60
2. Hizmet Şartlarının Belirlenmesi	64
3. Şeffaflık Raporlama Yükümlülüğü	68
4. Bildirim ve Eylem Mekanizmaları	74
5. İçeriğe Karşı Kısıtlamalarda Gerekçe Gösterilmesi	78
6. Çok Büyük Çevrimiçi Platformlara Getirilen Ek Yükümlülükler	82
7. Tüketicileri Korumaya Yönelik Hükümler	87
II) YAPAY ZEKÂ KANUNU (AI ACT)	90
A. DÜZENLEMENİN GEREKLİLİĞİ VE AMACI.....	91

B. RİSK TEMELLİ YAPAY ZEKÂ YAKLAŞIMI.....	96
1. Yasaklı Yapay Zekâ Sistemleri.....	98
2. Yüksek Riskli Yapay Zekâ Sistemleri	101
3. Sınırlı (Düşük) Riskli Yapay Zekâ Sistemleri.....	104
4. Minimal Riskli Yapay Zekâ Sistemleri	107
C. YAPAY ZEKÂ SİSTEMLERİ İÇİN YASAL GEREKLİLİKLER	110
1. Yüksek Riskli Yapay Zekâ Sistemleri İçin Gereklilikler.....	111
2. Belirli Yapay Zekâ Sistemleri İçin Şeffaflık Yükümlülüğü	113
III) ARA DEĞERLENDİRME	116

ÜÇÜNCÜ BÖLÜM

YAPAY ZEKÂ ARACILIĞIYLA SOSYAL MEDYAYA YAPILAN MÜDAHALELER

I) ERİŞİMİN ENGELLENMESİ VE FİLTRELEME	122
A. PLATFORM TEMELLİ ENGELLEME	126
B. KURUMSAL ENGELLEME	128
C. İNTERNET OMURGASI TEMELLİ ENGELLEME.....	129
D. BİREYSEL ENGELLEME	131
E. SOSYAL TEKNİKLER.....	131
II) SOSYAL MEDYAYA MÜDAHALE KONUSUNDAKİ YARGI KARARLARI	132
A. İFADE ÖZGÜRLÜĞÜ	133
1. Anlamı	133
2. Unsurları	137
3. Sınırlandırılması.....	139
B. HUKUKA AYKIRI İÇERİK	142

1. Anlamı	142
2. Unsurları	147
3. Sınırlandırılması.....	149
C. İFADE ÖZGÜRLÜĞÜ VE HUKUKA AYKIRI İÇERİK	
AÇISINDAN VERİLEN KARARLAR.....	150
PROBLEMİN ÇÖZÜMÜ: DENGE	155
SONUÇ	160
KAYNAKÇA	165

ŞEMA LİSTESİ

Şema 1: Sosyal Medyanın Tarihi	11
Şema 2: Sosyal Ağ Sağlayıcının Yükümlülükleri	23
Şema 3: Yapay Zekânın Alt Dalları.....	43
Şema 4: Yapay Zekâ Türleri.....	46
Şema 5: Yapay Zekânın Hukuki Niteliği	51
Şema 6: VLOP/VLOSE Şeffaflık Raporlama Genel Bakışı.....	74
Şema 7: AI Act Risk Kategorileri.....	110
Şema 8: Yapay Zekâ Odaklı Sosyal Medya Müdahaleleri	126
Şema 9: AIHM'nin Sınırlama Yetkisi Sıralaması	141
Şema 10: Hukuka Aykırı İçerik Örnekleri	147

KISALTMALAR

5651 sayılı Kanun	: 04.05.2007 kabul tarihli 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun
7253 sayılı Kanun	: 29.07.2020 tarihli 7253 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda Değişiklik Yapılmasına Dair Kanun
7418 sayılı Kanun	: 13.10.2022 tarihli 7418 sayılı Basın Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun
AB/EU/Birlik	: Avrupa Birliği
ABD	: Amerika Birleşik Devletleri
ADHK/EDSB	: Avrupa Dijital Hizmetler Kurulu (European Digital Services Board)
AI Act	: Artificial Intelligence Act
AİHM	: Avrupa İnsan Hakları Mahkemesi
AİHS	: Avrupa İnsan Hakları Sözleşmesi
ARPA	: Advanced Research Projects Agency
BBS	: Bulletin Board System (Bülten Tahtası Sistemi)
bkz.	: Bakınız
BTK	: Bilgi Teknolojileri ve İletişim Kurumu/Kurulu
c.	: Cümle
CMK	: 5271 sayılı Ceza Muhakemesi Kanunu

DHK/DSC	: Dijital Hizmetler Koordinatörü (Digital Services Coordinator)
DSA	: 2000/31/EC sayılı Direktifi tadil eden ve Dijital Hizmetler için Tek Pazara ilişkin 19.10.2022 tarihli ve 2022/2065 (AB) sayılı Avrupa Parlamentosu ve Konsey Tüzüğü (Dijital Hizmetler Kanunu)
E.	: Esas
EC/ AT	: Avrupa Topluluğu (European Community)
ed.	: editör
ETD	: 08.06.2000 tarihli ve 2001/31/EC sayılı İç Pazarda Özellikle Elektronik Ticaret Olmak Üzere Bilgi Toplumu Hizmetlerinin Belirli Yasal Yönleri Hakkında Direktif (E-Ticaret Direktifi)
E-Ticaret/e-ticaret	: Elektronik Ticaret
ETK	: 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun
Faaliyet Belgesi Yönetmeliği	: Telekomünikasyon Kurumu Tarafından Erişim Sağlayıcılara ve Yer Sağlayıcılara Faaliyet Belgesi Verilmesine İlişkin Usul ve Esaslar Hakkında Yönetmelik
FSEK	: 5846 sayılı Fikir ve Sanat Eserleri Kanunu
İHEB	: İnsan Hakları Evrensel Beyannamesi
İnternet Yönetmeliği	: İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik
K.	: Karar
KVKK	: 24.03.2016 tarihli 6698 sayılı Kişisel Verilerin Korunması Kanunu

MSHS	: Medeni ve Siyasi Haklara İlişkin Sözleşme
m./md.	: madde
OJ	: Official Journal (AB Resmî Gazetesi)
par.	: Paragraf
R.G.	: Resmî Gazete
sy.	: Sayı
TBK	: 6098 sayılı Türk Borçlar Kanunu
TCK	: 5237 sayılı Türk Ceza Kanunu
TMK	: 4721 sayılı Türk Medeni Kanunu
TSY	: Ticaret Sicili Yönetmeliği
TTK	: 6102 sayılı Türk Ticaret Kanunu
vd.	: ve devamı
VLOP	: Very Large Online Platform (Çok Büyük Çevrimiçi Platform)
VLOSE	: Very Large Online Search Engine (Çok Büyük Çevrimiçi Arama Motoru)
www	: World Wide Web

GİRİŞ

Bilgi, insanın var olduđu günden bugüne kadar sosyalleşmesinde ve gelişmesinde kritik bir rol oynamıştır. Bilgiyi aktarım ihtiyacı ile insan sosyalleşmiş ve diğer insanlarla etkileşime girmiştir. Bu etkileşimle aktarılan ve paylaşılan bilgi, yeni bilgi ve tecrübelerin önünü açmıştır. Bu bilgi ve tecrübeler insanlığın tarihi ile eş değer olan teknolojinin de gelişimini desteklemiştir.

20. yüzyılın ikinci yarısı itibariyle iki büyük savaş görmüş olan dünya, bilimsel faaliyetlere ağırlık vermiş, bu doğrultuda teknolojik gelişme hız kazanmıştır. Bu doğrultuda internetin askeri ve istihbari faaliyetler yanında gündelik hayatta da yaygınlaşması, toplumsal hayatta yeni bir dönemin kapısını aralamıştır. Bu yeni dönemde bilginin aktarım sahası genişlemiş ve sosyal yaşamda sosyal medya olgusu ortaya çıkmıştır. Bu olgu sayesinde insanoğlunun sosyal hayatı kolaylaşmıştır. Örneğin, haftanın bazı günlerinde çalışanlar işe fiziksel olarak gitmeden çevrimiçi ortamda toplantılara görüntü de paylaşarak katılabilmektedir. Öte yandan sosyal medya platformları sayesinde arkadaşlar iletişim kurabilmekte, öğretmenler öğrencilerine ders içeriği sağlayabilmektedir.

21. yüzyıl itibariyle etkisini giderek artıran ve hissettiren diğer bir olgu ise yapay zekâdır. Toplumsal dengeleri değiştiren bu olgu hakkında hem olumlu hem olumsuz yönde bilim-kurgu senaryolar üretilmektedir. Yapay zekâ sayesinde insanlar angarya görülen çoğu işi bu teknoloji ile saniyeler içinde bitirmektedir. Herhangi bir mesleğe mensup olan bir kişi işinde bu teknolojiden faydalanarak işini daha hızlı bir şekilde yapmakta, arta kalan zamanını başka işlere ayırabilmektedir. Örneğin, çalışan bir kişi eve dönerken bu teknoloji ile donatılmış fırını akıllı telefonuyla tetikleyerek yemeğini pişirebilmektedir. Öte yandan gelen bir mailde belirtilen ve yapılması gereken bir işi bu teknoloji otomatik olarak görev listesine ekleyebilmekte ve kişiye hatırlatmada bulunmaktadır. Distopik bir örnek olarak bir baba ve oğlu arabada seyahat ederken bu teknoloji hakkında olumsuz bir yorumda bulunduğunda başka konuları konuşmaları yönünde sistem tarafından uyarılabilmektedir.

Milenyumdan bu yana toplumsal hayatta oyun deęiřtirici g olarak bulunan bu iki olgu bir arada bulunmakta ve toplumsal yařamı birlikte etkilemektedir. Nitekim popler sosyal medya platformları, sahip oldukları hkimiyet ile “Topluluk Kuralları”nı kullanıcıya dikte etmektedir. Bu doęrultuda bu platformlar bir nevi “kendi kanunlarına” aykırı buldukları bir ierięi yapay zek destekli algoritmalar ile platformlarından ıkarabilmekte ya da bu ierięi paylařan kullanıcıyı “hayalet hesap” haline getirebilmektedir. Yapay zek ile sosyal medya olgularının bu gibi etkileřimleri, evrimii ortamı kullananlar iin hakkaniyete aykırı sonular doęurabilmekte ve temel hak ve zgrlklerine mdahale teřkil edebilmektedir.

İřte, bu alıřmada 21. yzyılın oyun deęiřtirici gerlerinden olan bu iki olgunun etkileřimi incelenecektir. Bu etkileřim bu alıřmada  blme ayrılarak incelenecektir. Birinci blmde sosyal medya ve yapay zek olguları, kavramsal ereve, tarihi geliřim, bu olguların sjeleri ynnden teknik ve yer yer hukuki zeminde aıklanmaya alıřılacaktır. İkinici blmde Avrupa Birlięi tarafından ihdas edilen ve bu iki olguyu yakından ilgilendiren Dijital Hizmetler Kanunu ve Yapay Zek Kanunu sosyal medya ve yapay zek kapsamında incelenecektir. nc ve son blmde ise alıřmanın konusu kapsamında sosyal medyada yapılan mdahale eřitleri aıklanmıř, bu mdahalelerinin temelde temas ettięi hukuka aykırı ierik ve ifade zgrlę kavramları aıklanarak bu kapsamda yargı makamlarına intikal etmiř uyuřmazlıklar incelenecektir.

BİRİNCİ BÖLÜM

SOSYAL MEDYA VE YAPAY ZEKÂ

I) SOSYAL MEDYA

İnternetin icadı, insanoğlunun bilgiye erişiminde yeni bir safha açmıştır. Bu safhanın açılmasıyla bilgiye erişim kolaylaşmıştır. Bilgiye erişimin kolaylaşması, üretilen bilginin artmasını da sağlamıştır. Bilgi artışında hiç şüphesiz bilgi paylaşımının rolü büyüktür. Sosyal medyanın web 2.0 ile hayatımıza girmesiyle bilginin üretim ve paylaşım hızı artmıştır. Sosyal medya ile sadece bilgi özgürleşmemiş, aynı zamanda toplumun birbiriyle etkileşimi artmış ve toplumun dönüşümü de hızlanmıştır¹.

İşte, bu bölümde hayatımızı değiştirip dönüştüren sosyal medya olgusunun öncelikle kavramsal çerçevesi çizilecektir. Devamında bu olgunun tarihsel gelişimi ve son olarak bu olgunun gelişiminde rol oynayan sosyal medya süjeleri açıklanacaktır.

A. SOSYAL MEDYANIN TANIMI

21. yüzyılda etkisi derinden hissedilen ve toplumları geliştirip dönüştüren sosyal medya, ele alınan bağlam açısından farklı biçimlerde tanımlanabilmektedir. Bu durum, sosyal medya kavramının herkes tarafından uzlaşılmış bir tanımının yapılmasına engel olmaktadır. Bu başlık altında sosyal medyanın tanımı yapılırken öncelikle etimolojik tanımlara yer verilecektir. Devamında doktrin ve yargı makamları tarafından yapılan tanımlar aktarıldıktan sonra bu çalışmanın yazarının tanımı ile bitirilecektir.

¹ Jan A. G. M. VAN DIJK, *The Network Society: Social Aspect of New Media*, Second Edition (SAGE Publications Ltd, 2006), 2 Yazar, bilginin bu denli hızlı üretimi, paylaşımı ve iletiminden ötürü bilgi çağının bir ağ (network) çağı olduğunu ifade etmektedir.

Etimolojik olarak kelime bazında incelendiğinde sosyal kelimesi, Fransızca ve İngilizce *social* sözcüğünün karşılığıdır. Bu kelime ise Latince *socius* “yoldaş, ortak, müttefik” kelimesinden türetilmiş olup “dostluk ve yoldaşlık eden, cana yakın, topluma uygun, toplumu gözetken, toplumsal” anlamına gelmektedir². Medya kelimesi ise Latince “aradaki şey, araç” anlamına gelen *medium* sözcüğünden türetilen ve “araçlar, araçlar” anlamına gelen *media* kelimesinin karşılığıdır³. Sözlük ve etimolojik anlamlarından hareketle sosyal medyanın topluma uygun, insanlar arasındaki toplumsal araçlar olarak tanımlanması mümkündür.

Sosyal medyayı bizatihi tanımlayan sözlükler de bulunmaktadır. Türk Dil Kurumu (TDK) tarafından yayımlanan Güncel Türkçe Sözlükte sosyal medya, “Genel ağda oluşturulan sosyal ağlar üzerinden kullanıcılar arasında görsel ve işitsel malzeme paylaşımını, bilgi aktarımını, haberleşmeyi sağlayan iletişim ortamı”⁴, Cambridge sözlüğünde ise “İnsanların internet üzerinden iletişim kurmasına ve bilgi, görüş, resim, video vb. paylaşmasına olanak tanıyan web siteleri ve bilgisayar programları, özellikle sosyal ağ siteleri; insanların internet veya cep telefonlarını kullanarak iletişim kurmasına ve bilgi paylaşmasına olanak tanıyan medya biçimleri”⁵ olarak tanımlanmaktadır⁶.

Sosyal medya için yapılan akademik tanımlar, ele alınan bağlam doğrultusunda farklılık arz edebilmektedir. Bu tanımlar iletişim, pazarlama,

² <https://www.etimolojiturkce.com/kelime/sosyal> (Son Erişim Tarihi: 13.05.2025).

³ <https://www.etimolojiturkce.com/kelime/medya> (Son Erişim Tarihi: 13.05.2025).

⁴ <https://sozluk.gov.tr/?ara=sosyal%20medya> (Son Erişim Tarihi: 14.05.2025).

⁵ <https://dictionary.cambridge.org/dictionary/english/social-media> (Son Erişim Tarihi: 14.05.2025).

⁶ Sosyal medya ve sosyal ağ kavramları zaman zaman birbirinin yerine kullanılabilir. Ancak sosyal ağ kavramı sosyal medya kavramından daha dar bir anlama sahiptir. İşbu çalışmada anlam itibarıyla daha geniş olan sosyal medya kavramı kullanılacaktır. Sosyal ağ kavramının tanımı Cambridge Sözlüğünde şöyle yapılmıştır: “insanların bir bilgisayar veya cep telefonu kullanarak internet üzerinden iletişim kurmasına ve bilgi paylaşmasına olanak tanıyan bir web sitesi veya bilgisayar programı”. <https://dictionary.cambridge.org/dictionary/english/social-network> (Son Erişim Tarihi: 14.05.2025). Ayrıca sosyal medya ve sosyal ağ arasındaki farklar için bkz. Simeon EDOSOMWAN vd., “The History of Social Media and its Impact on Business”, *The Journal of Applied Management and Entrepreneurship* 16, sy 3 (2011): 5-6.

eğitim-öğretim, medya, teknoloji, siyasi katılım gibi temeller üzerine inşa edilmektedir⁷.

İletişim bağlamında yapılan bir tanımda Boyd ve Ellison sosyal medyayı “Bireylerin sınırlı bir sistem içinde herkese açık veya yarı açık bir profil oluşturmalarına, bağlantı paylaştıkları diğer kullanıcıların bir listesini ifade etmelerine ve kendi bağlantı listelerini ve sistem içinde başkaları tarafından yapılan bağlantıları görüntülemelerine ve dolaşmalarına olanak tanıyan web tabanlı hizmetler” olarak tanımlamışlardır⁸. Bu bağlamda yapılan bir diğer tanıma göre sosyal medya “iletişimi interaktif diyaloga dönüştürmek için web tabanlı ve mobil teknoloji kullanımı” olarak tanımlanmıştır⁹. İletişim temelinde doktrinde yapılan diğer bir tanıma göre sosyal medya “bilgi, düşünce ve duygulara ilişkin ifade biçimlerini oluşturma, yayınlama ve yorumlamayı sağlayan, etkileşimli iletişim için kurulan internet aracılı teknolojilerin tamamıdır”¹⁰.

İletişim bağlamında en geniş tanımları yapan Blossom ise sosyal medyayı “Herhangi bir bireyin diğer bireylerden oluşan grupları kolayca etkilemesini sağlayan, yüksek düzeyde ölçeklenebilir ve erişilebilir herhangi bir iletişim teknolojisi veya tekniği” olarak ifade etmiştir¹¹.

Pazarlama bağlamında yapılan diğer bir tanıma göre sosyal medya, “Web 2.0’ın ideolojik ve teknolojik temelleri üzerine inşa edilen ve Kullanıcı Tarafından

⁷ Sinan Sami AKKURT, *Sosyal Medyada Gerçekleşen İhlaller Karşısında Kişilik Hakkının Korunması*, 3. Baskı (Seçkin Yayıncılık, 2023), 97.

⁸ Danah M. BOYD ve Nicole B. ELLISON, “Social Network Sites: Definition, History, and Scholarship”, *Journal of Computer-Mediated Communication* 13, sy 1 (2007): 211, <https://doi.org/10.1111/j.1083-6101.2007.00393.x>.

⁹ Francois Quintin CILLIERS, “The Role and Effect of Social Media in the Workplace”, *Northern Kentucky Law Review* 40, sy 3 (2013): 571.

¹⁰ Cemile TURGUT, *Kişilik Hakkının Bir Görünümü Olarak Unutulma Hakkı*, 1. Baskı (On İki Levha Yayıncılık, 2021), 393.

¹¹ John BLOSSOM, *Content Nation: Surviving and Thriving as Social Media Changes Our Work, Our Lives, and Our Future*, 1. Baskı (Wiley Publishing, Inc., 2009), 29; iletişim bağlamında yapılan diğer tanımlar için bkz. AKKURT, *Sosyal Medyada Gerçekleşen İhlaller Karşısında Kişilik Hakkının Korunması*, 97.

Oluşturulan İçeriğin [User-Generated Content] oluşturulmasına ve değiş tokuş edilmesine olanak tanıyan bir grup İnternet tabanlı uygulama” olarak tanımlanmıştır¹².

Doktrinde yapılan bir diğer tanıma göre sosyal medya, “*internet altyapısı ve web 2.0 teknolojisine dayanan, kişilerin ortak ilgi, bilgi, duygu ve düşünceleri bağlamında karşılıklı etkileşim, iletişim, paylaşım, iş birliği, topluluk oluşturma ve kendi içeriklerini yaratmasını sağlayarak sosyalleşmesine imkân tanıyan araç ve ortamların bütünü*”dür¹³.

Başka bir tanımda ise sosyal medya, “*kullanıcıların internet tabanlı ortamlarda birbiri ile kapalı yahut herkese açık şekilde, veri alışverişinde, iletişim ve etkileşimde bulunmasına, topluluk oluşturma ve içerik oluşturmaya imkân sağlayan ortam ve araçlar*”¹⁴ olarak tanımlanmıştır.

Sosyal medya konusunda bu çalışmanın yazarı tarafından yapılan tanıma geçmeden önce Anayasa Mahkemesi tarafından sosyal medyanın kısmen tanımlandığı iki karardan bahsetmekte fayda vardır. Yüksek mahkeme, 2014 yılında verdiği bir kararında sosyal medyayı “*medya içeriğini oluşturmak yayınlamak ve yorumlamak şeklinde bireysel katılıma imkan veren, şeffaf ve karşılıklı iletişim kurulan bir platform*”¹⁵ olarak tanımlarken 2017 yılında 5651 sayılı Kanun¹⁶ m. 8 kapsamında

¹² Andreas M. KAPLAN ve Michael HAENLEIN, “Users of The World, unite! The challenges and opportunities of Social Media”, *Business Horizons* 53, sy 1 (2010): 61, <https://doi.org/10.1016/j.bushor.2009.09.003>; benzer bir tanım için bkz. Abdurrahman Hamza TÜZGEN, *Türk Hukukunda Sosyal Medya Reklamları*, 1. Baskı (On İki Levha Yayıncılık, 2023), 119.

¹³ Aynı yönde bkz. Mine KAYA, *Elektronik Ortamda (Elektronik Haberleşme - İnternet - Sosyal Medya) Kişilik Hakkının Korunması*, 1. Baskı (Seçkin Yayıncılık, 2015), 76; AKKURT, *Sosyal Medyada Gerçekleşen İhlaller Karşısında Kişilik Hakkının Korunması*, 100; Gönül AKYASAN BİRSEN, *Sosyal Medyada Paylaşılan İçerik Nedeniyle Kişilik Hakkı İhlalleri*, 1. Baskı (Seçkin Yayıncılık, 2020), 47; Süleyman YILMAZ ve Vehbi Umut ERKAN, “Sosyal Medya Hesaplarının Miras Yoluyla İntikal Edip Edemeyeceği Sorusunun Kişisel Verileri Koruma Hukuku Kapsamında İncelenmesi”, *İnönü Üniversitesi Hukuk Fakültesi Dergisi* 11, sy 2 (2020): 576, <https://doi.org/10.21492/inuhfd.789817>.

¹⁴ Şerafettin EKİCİ, *Bilişim ve Teknoloji Hukuku*, Güncellenmiş 2. Baskı (Seçkin Yayıncılık, 2023), 101.

¹⁵ 29.05.2014 tarihli ve 2014/4705 Başvuru Numaralı Kararı, No. 2014/4705 (Anayasa Mahkemesi 29 Mayıs 2014), de Paragraf 40, 06/06/2014 tarihli 29022 sayılı Resmî Gazete, <https://www.resmigazete.gov.tr/eskiler/2014/06/20140606-10.pdf>.

¹⁶ 23/05/2007 tarihli ve 26530 sayılı Resmî Gazete, <https://www.resmigazete.gov.tr/eskiler/2007/05/20070523-1.htm>.

somut norm denetimi yaparken “kitle haberleşme ve iletişim aracı olan internet siteleri veya uygulamaları” olarak nitelendirmiştir¹⁷.

Sosyal medya hakkında yapılan ve yukarıda verilen tanımlardan görüleceği üzere sosyal medyanın web tabanlı, insanlar arası iletişimi ve etkileşimi artırma, kullanıcı odaklı olma özellikleri ağır basmaktadır. Yukarıda da bahsedildiği üzere sosyal medyanın ele alındığı bağlamlardan en çok “iletişim” temelli tanımlar çoğunluktadır. Ayrıca sosyal medya, parlamasını sağlayan teknoloji olan web 2.0 teknolojisi ekseninde tarif edilmektedir.

Son yıllarda blok zinciri¹⁸ ve dayandığı teknoloji olan dağıtık defter teknolojilerine bağlı olarak web 3.0 tabanlı sosyal medya uygulamaları da gündeme gelmektedir. COVID-19 pandemisi ve devamında dezenformasyonun hızla yükselişe geçmesinde sosyal medya da etkili olmuştur¹⁹. Bu noktada web 3.0 tabanlı sosyal medya çözümleri kullanıcı deneyimini, güvenlik düzeyini artırmaktadır²⁰.

Bu açıklamalardan hareketle kanaatimizce sosyal medya, Web (internet) tabanlı uygulamalarda kullanıcı sıfatıyla kişilerin duygu, düşünce paylaşımında bulunduğu, fikir ve sanat eserlerini ürettiği, kişisel verilerini paylaşarak mal ve hizmet alım-satımı vb. içerik paylaşımında bulunduğu bir ortamdır.

¹⁷ 15.11.2017 Tarihli ve 2015/76 E., 2017/153 K. Sayılı Kararı, No. 2015/76 (Anayasa Mahkemesi 15 Kasım 2017), de Paragraf 26, 07/02/2018 tarihli ve 30325 sayılı Resmî Gazete, <https://www.resmigazete.gov.tr/eskiler/2018/02/20180207-7.pdf>.

¹⁸ Blok zinciri kavramı hakkında ayrıntılı bilgi için bkz. Salih KARADENİZ, *Blokszincir Teknolojisi ile Gerçekleştirilen Merkeziyetsiz Otonom Organizasyonların (DAO'ların) Hukuki Niteliği*, 1. Baskı (Adalet Yayınevi, 2024), 19-22.

¹⁹ Yuanzhu ZHAN vd., “A conceptual model and case study of blockchain-enabled social media platform”, *Technovation*, 2022, 2, <https://doi.org/10.1016/j.technovation.2022.102610>.

²⁰ ZHAN vd., “A conceptual model and case study of blockchain-enabled social media platform”, 2; web 3.0 tabanlı sosyal medyada veri gizliliğinin sağlanması noktasında ayrıntılı teknik bilgi için bkz. Sara SALIM vd., “Data analytics of social media 3.0: Privacy protection perspectives for integrating social media and Internet of Things (SM-IoT) systems”, *Ad Hoc Networks* 128, sy 102786 (2022), <https://doi.org/10.1016/j.adhoc.2022.102786>.

B. SOSYAL MEDYANIN TARİHİ

Sosyal medyanın tarihsel gelişimine bakıldığında sosyal medyayı 17-18. yüzyıla dayandıran yazarlar²¹ olduğu gibi 20. yüzyılın ikinci yarısından itibaren bu konuyu inceleyenler yazarlar²² da mevcuttur.

Edosomwan ve diğerlerine göre sosyal medyanın tarihini 1792 yılına ve telgrafa kadar götürmek mümkündür. Nitekim telgraf, uzak mesafelerde bulunan kişiler arası haberleşme aracı işlevini görmekteydi. Ayrıca *Edosomwan ve diğerlerine* göre Emile Durkheim ve Ferdinand Tonnies, “sosyal ağların öncüleri” olarak düşünülmektedir²³.

20. yüzyıl itibarıyla sosyal medya tarihine bakıldığında sosyal medyanın temeli olarak nitelendirilen internet²⁴ ile başlamak mümkündür. İnternetin temelleri ise ABD’de bir ajans olan Gelişmiş Araştırma Projeleri Ajansı (*Advanced Research Projects Agency-ARPA*) tarafından 1969’da geliştirilen ARPANET’e dayanmaktadır²⁵.

1970’lere gelindiğinde sosyal medya daha çok gelişim göstermeye başlamıştır. Çoklu Kullanıcı Alanı olarak ifade edilen MUD (*Multi-User Dimension*) ile role dayalı oyunlar oynanabiliyor, çevrimiçi sohbet ile kişiler eşzamanlı iletişim kurabiliyordu²⁶. 1978’de bir tür MUD olan *Bulletin Board System* (BBS) olarak ifade edilen Bülten Tahtası Sistemi ile yeni bir eşik aşılmıştır. Bu sistem, 1992’de

²¹ EDOSOMWAN vd., “The History of Social Media and its Impact on Business”, 1 vd.

²² TÜZGEN, *Türk Hukukunda Sosyal Medya Reklamları*, 120 vd.; AKYASAN BİRSEN, *Sosyal Medyada Paylaşılan İçerik Nedeniyle Kişilik Hakkı İhlalleri*, 48 vd.; Kübra DENİZ ÇELİK, *Sosyal Medya Kullanımının İş Sözleşmesine Etkisi*, 1. Baskı (On İki Levha Yayıncılık, 2019), 5 vd.; KAYA, *Elektronik Ortamda (Elektronik Haberleşme - İnternet - Sosyal Medya) Kişilik Hakkının Korunması*, 83.

²³ EDOSOMWAN vd., “The History of Social Media and its Impact on Business”, 2.

²⁴ İnternetin tanımı için bkz. Mehmet Bedii KAYA, *İnternet Hukuku*, 2. Baskı (On İki Levha Yayıncılık, 2021), 6; EKİCİ, *Bilişim ve Teknoloji Hukuku*, 58.

²⁵ Oğuzhan YEŞİLTUNA, *Hakikat ya da Neticeler: İfade Özgürlüğü Bağlamında Çevrimiçi Bilgi Çarpıtmayla Mücadele*, 1. Baskı (On İki Levha Yayıncılık, 2023), 39; EDOSOMWAN vd., “The History of Social Media and its Impact on Business”, 2.

²⁶ EDOSOMWAN vd., “The History of Social Media and its Impact on Business”, 2.

internetin dönüm noktalarından olan World Wide Web'in "atası" olarak ifade edilmektedir²⁷.

İlk önce askeri amaçlarla kullanılan internet, 1990 sonrasında özelleşmiş ve sivil nitelik kazanmaya başlamıştır. Bununla birlikte günümüzdeki sosyal medya araç ve ortamları gelişmeye başlamıştır. Six Degrees, Blogger, Epinions gibi sosyal medya uygulamaları www'nun²⁸ etkisiyle sosyal hayata entegre olmuştur.

Milenyuma gelindiğinde bugün birçoğuna aşina olunan ve sosyal hayatı çevreleyen sosyal medya uygulamaları piyasaya sürülmüştür. Bir wiki örneği olan Wikipedia, LiveJournal, Friendster, MySpace, LinkedIn, Facebook, X (ilk çıktığı adıyla Twitter), Instagram, Snapchat, TikTok, YouTube bunlardan bazılarıdır²⁹.

Bir önceki başlıkta görüleceği üzere sosyal medya tanımlanırken web 2.0 teknolojisinden bahsedilmektedir. Web 2.0 teknolojisinden ilk olarak 1999'da Darcy DiNucci bahsetmiştir. DiNucci, web 2.0'nin ilk ışıklarını göstermeye başladığını, bir embriyo gibi nasıl geliştiğine şahit olacağımızı ifade etmiştir³⁰. Sosyal medyanın bugünkü popülerliğini ve toplumsal yapının dönüşümünü sağlayan bu teknolojidir. Web 1.0 döneminde internet üzerinde bilgi akışı tek yönlü iken web 2.0 teknolojisi, bu yönü çift taraflı hale getirmiştir³¹. Bu doğrultuda sosyal medyanın teknolojik bağlamı ifade edilirken aktif rol oynayan web 2.0 teknolojisinden bahsedilmesi gerekmektedir.

²⁷ EDOSOMWAN vd., "The History of Social Media and its Impact on Business", 2.

²⁸ World Wide Web hakkında daha fazla bilgi için bkz. T. J. BERNERS-LEE vd., "The World-Wide Web", *Computer Networks and ISDN Systems* 25, sy 4 (1992): 454-59, [https://doi.org/10.1016/0169-7552\(92\)90039-S](https://doi.org/10.1016/0169-7552(92)90039-S).

²⁹ Sosyal medya araçları hakkında daha fazla bilgi için bkz. AKYASAN BİRSEN, *Sosyal Medyada Paylaşılan İçerik Nedeniyle Kişilik Hakkı İhlalleri*, 57-64; DENİZ ÇELİK, *Sosyal Medya Kullanımının İş Sözleşmesine Etkisi*, 18-33; KAYA, *Elektronik Ortamda (Elektronik Haberleşme - İnternet - Sosyal Medya) Kişilik Hakkının Korunması*, 87-97.

³⁰ Darcy DINUCCI, "Fragmented Future", *Print Magazine*, 1999, 32.

³¹ BERNERS-LEE vd., "The World-Wide Web".

DiNucci'den sonra bu teknolojiyi açıklayan O'Reilly, bu teknolojinin tanıma götüren temelde yedi prensibinin olduğunu ve fakat bu prensiplerinin artabileceğini ifade etmektedir³².

Web 2.0 kavramı ile ilgili olarak Kaya tarafından yapılan tanıma göre “Web 2.0 yüksek etkileşimli yeni nesil internet teknolojilerinin genel adıdır.”³³ Kaplan/Haenlein'a göre web 2.0 kavramı “içerik ve uygulamaların artık bireyler tarafından oluşturulup yayınlanmadığı, bunun yerine tüm kullanıcılar tarafından katılımcı ve işbirlikçi bir şekilde sürekli olarak değiştirildiği bir platform olarak” tanımlanmaktadır³⁴. Deniz Çelik'e göre ise web 2.0, “bu kavramla yakın ilişkili olan bloglar, wikiler, içerik paylaşım siteleri gibi herkesin ekleme ve düzenlemeler yapabildiği alanlardan oluşan ve sosyal olarak daha katılımcı bir web sağlayan teknolojiler olarak tanımlanabilir”³⁵.

Bu çalışmanın yazarı tarafından yapılan tanımda sosyal medyanın çağımızda web 3.0 teknolojisi tabanlı olabileceği, bu teknolojinin kullanıcı deneyimini ve güvenliğini artırdığı ifade edilmişti. Bu doğrultuda web 3.0 teknolojisinden de kısaca bahsetmek gerekmektedir. Bu kavram, New York Times'tan John Markoff tarafından üçüncü nesil web olarak önerilmiştir³⁶. Web 3.0 teknolojisi kısaca veri bağlantılarından oluşan ağ olarak tanımlanabilir. Web 3.0 aynı zamanda “semantik web” olarak ifade edilebilmektedir³⁷.

³² Prensipler hakkında ayrıntılı bilgi için bkz. Tim O'REILLY, “What is Web 2.0: Design Patterns and Business Models for the Next Generation of Software”, *Communications & Strategies*, sy 1 (2007): 18-36, <https://papers.ssrn.com/abstract=1008839>.

³³ KAYA, *İnternet Hukuku*, 24.

³⁴ M. KAPLAN ve HAENLEIN, “Users of The World, unite! The challenges and opportunities of Social Media”, 60-61.

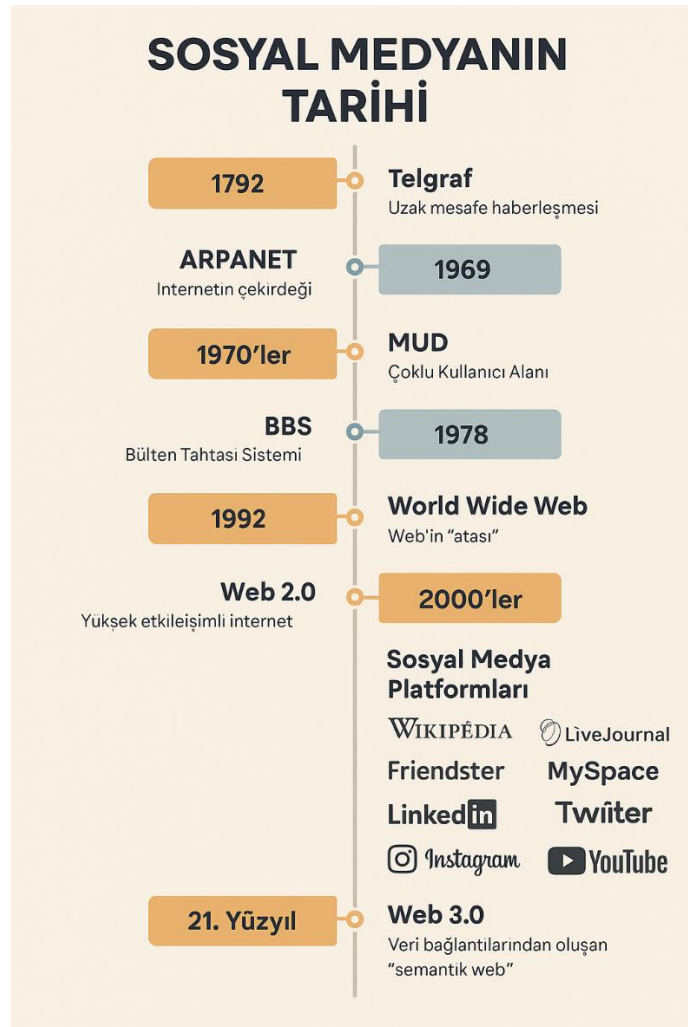
³⁵ DENİZ ÇELİK, *Sosyal Medya Kullanımının İş Sözleşmesine Etkisi*, 6.

³⁶ SALIM vd., “Data analytics of social media 3.0”, 3; Nupur CHOUDHURY, “World Wide Web and Its Journey from Web 1.0 to Web 4.0”, *International Journal of Computer Science and Information Technologies* 5, sy 6 (2014): 8097, <https://ijcsit.com/docs/Volume%205/vol5issue06/ijcsit20140506265.pdf>.

³⁷ Semantik web ile kullanıcıların içerikleri daha kolay bulup paylaşımlarının amaçlandığı yönünde bkz. CHOUDHURY, “World Wide Web and Its Journey from Web 1.0 to Web 4.0”, 8098.

Choudhury tarafından yapılan bir tanıma göre web 3.0 “web sitesi veya web sayfası kavramının ortadan kalktığı, verilerin sahiplenilmediği, bunun yerine paylaşıldığı, hizmetlerin aynı web veya aynı veri için farklı görünümler gösterdiği bir web” olarak tanımlanmaktadır³⁸.

Tüm bu açıklamalardan hareketle sosyal medya kavramının web 1.0’de tek yönlü iken web 2.0 ile çift yönlülük kazandığı ve bu ortamı sağlayan araçların zaman içinde hızla arttığı görülmektedir. 21. yüzyılın getirdiği semantik web ile kullanıcı deneyiminin iyileştirilmesi, daha fazla etkileşime girerek paylaşımın artırılması hedeflenmektedir.



Şema 1: Sosyal Medyanın Tarihi

³⁸ CHOUDHURY, “World Wide Web and Its Journey from Web 1.0 to Web 4.0”, 8098.

C. SOSYAL MEDYA SÜJELERİ

İnsanların eş zamanlı fiziksel varlıkları olmaksızın etkileşim kurmasını, içerik üretip tüketmesini sağlayan sosyal medyanın tanımı ve tarihinden sonra sanal alanın süjelerini ele almak gerekmektedir. Bu süjeler kimi zaman sosyal medyaya içerik sağlarken kimi zaman bu içeriklerin paylaşımına ve dolaşımına internet ortamını sağlamaktadır:

1. İçerik Sağlayıcı

Sosyal medya olgusunun üzerinde döndüğü, çeşitli sosyal medya araçlarının ve platformlarının bağlılığını pekiştirmek için her gün yeni bir özelliği piyasaya sürdüğü özne, içerik sağlayıcıdır demek pek yanlış olmayacaktır. Zira gündelik hayatta daha çok “kullanıcı” sıfatıyla bilinen içerik sağlayıcılar (*content provider*), sosyal medyanın deyim yerindeyse başrolü ve ana öznesidir. Bu önemlidir ki içerik sağlayıcı kavramının çerçevesinin iyi çizilmesi, hukuki sorumluluğunun belirlenmesi açısından önem taşımaktadır.

5651 sayılı Kanun m. 2/1-f’de tanımlanan içerik sağlayıcı, internet ortamına (sosyal medyaya) her şeyden önce bir “içerik” sağlamaktadır. 5651 sayılı Kanun’da bizatihi bir “içerik” tanımı yapılmamakla birlikte içerik kavramına götüren iki kavram tanımlanmıştır. Bunlardan ilki olan “bilgi” kavramı, 5651 sayılı Kanun m. 2/1-ç’de “*verilerin anlam kazanmış biçimi*” olarak ifade edilirken diğer kavram olan veri ise 5651 sayılı Kanun m. 2/1-k’de “*bilgisayar tarafından üzerinden işlem yapılabilen her türlü değer*” olarak tanımlanmıştır. Bilgi ve veri kavramından hareketle içerik kavramı “dijital ortamda ifade edilebilen ve anlam kazanmış her türlü değer” olarak tanımlanabilir³⁹.

5651 sayılı Kanun’da içerik sağlayıcı kavramının çerçevesi çizilirken “internet ortamı” ibaresi kullanılmaktadır. Bu doğrultuda içerik sağlayıcı kavramını tanımlamadan önce “internet ortamı” ibaresinin kanuni tanımını

³⁹ Benzer bir tanım için bkz. AKKURT, *Sosyal Medyada Gerçekleşen İhlaller Karşısında Kişilik Hakkının Korunması*, 240.

vermekte fayda vardır. 5651 sayılı Kanun m. 2/1-g’de internet ortamı, “*Haberleşme ile kişisel veya kurumsal bilgisayar sistemleri dışında kalan ve kamuya açık olan internet üzerinde oluşturulan ortam*” olarak tanımlanmıştır. Bu tanımdan hareketle bir internet ortamı, (1) haberleşme sistemi, (2) kişisel/kurumsal bilgisayar sistemi ve/veya (3) kamuya kapalı ise 5651 sayılı Kanun kapsamında olmayacaktır.

İçerik sağlayıcı ise 5651 sayılı Kanun m. 2/1-f’de “*İnternet ortamı üzerinden kullanıcılara sunulan her türlü bilgi veya veriyi üreten, değiştiren ve sağlayan gerçek veya tüzel kişiler*” olarak ifade edilmektedir. Biraz önce internet ortamı tanımlanırken bahsedildiği üzere örneğin şirket bünyesindeki bilgisayar sisteminde herhangi bir bilgi veya verinin üretilmesi, değiştirilmesi ve sağlanması suretiyle 5651 sayılı Kanun kapsamında bir içerik sağlamaktan bahsedilemeyecektir⁴⁰. Çünkü söz konusu içeriğin üretildiği, değiştirildiği veya sağlandığı internet ortamı yukarıda bahsedilen özellikleri haiz değildir.

5651 sayılı Kanun kapsamında bir içerik sağlayıcıdan bahsedilebilmesi için söz konusu “kullanıcının” gerçek veya tüzel kişi olması gerekmektedir. Bu doğrultuda bu bölümün “II)” numaralı başlığında inceleneceği üzere henüz kişiliği üzerinde herhangi bir uzlaşının olmadığı yapay zekânın 5651 sayılı Kanun kapsamındaki bir internet ortamında içerik sağlayıcı olması mümkün değildir.

İçerik sağlayıcı konusunda değinilmesi gereken diğer bir husus, 5651 sayılı Kanun kapsamındaki bir internet ortamında (sosyal medyada) hesap sahibi olmadan içerik sağlayıcı sıfatının kazanılıp kazanılmayacağıdır. İçerik sağlayıcı kavramının yapılan tanımından görüleceği üzere kanun koyucu isabetli olarak internet ortamında içerik sağlanması için kişinin hesap sahibi sıfatını kazanmasını aramamaktadır⁴¹. Dolayısıyla şartları sağlayan bir internet ortamında hesap sahibi olsun veya olmasın bir kişi tarafından bir içerik sunuluyorsa içerik sağlayıcı olarak kabul edilmektedir.

⁴⁰ Zeynep YASAMAN, *Türk ve Avrupa Birliği Hukukunda İnternette Marka Hakkının İhlali*, 1. Baskı (On İki Levha Yayıncılık, 2020), 578.

⁴¹ EKİCİ, *Bilişim ve Teknoloji Hukuku*, 125.

İnternet ortamı üzerinde aktif bir rol üstlenen içerik sağlayıcının her davranışının hukuka uygun olması beklenebilirse de bu, her zaman böyle olmaz. Kanun koyucu da bu düşünceden hareketle içerik sağlayıcının sorumluluğunu düzenlemiştir. 5651 sayılı Kanun m. 4'e göre içerik sağlayıcı, internet ortamı üzerinden kullanıma sunduğu her türlü içerikten kural olarak sorumludur.

İçerik sağlayıcının bu sorumluluğunun istisnası ise başkasına ait içeriğe bağlantı sağlamasıdır. Örneğin (A) kişisi, bir sosyal medya platformunda (B) kişisine ait bir gönderiyi (hikâyeyi, tweeti) sadece paylaşırsa bu fiilinden ötürü sorumlu tutulamayacaktır. Kanun koyucu bu istisnaya da bir istisna getirmiştir. Buna göre içerik sağlayıcının başkasına ait içeriği sunuş biçiminden söz konusu içeriği benimsediği ve kullanıcıların bu içeriğe ulaşmasını istediği açıkça belli ise genel hükümlere göre sorumlu olacaktır.

İçerik sağlayıcının 5651 sayılı Kanun ve İnternet Yönetmeliği dışında birtakım özel yükümlülükleri de bulunmaktadır. Bu sorumluluklar TCK, TMK, TBK, CMK, ETK, FSEK gibi bazı temel kanunlarda dolaylı olarak düzenlenmiştir. Bu sorumluluklara değinilmesi, çalışmanın kapsamını ve hacmini aşacağından yukarıdaki açıklamalarla yetinilecektir⁴².

2. Yer Sağlayıcı

Yüzlerce kitabın okuyucuya hazır bulundurulabilmesi için kütüphaneye, yemek pişirmek için gereken araçlara şefin ulaşabilmesi için mutfak dolaplarına ihtiyacı vardır. Dijital ortamda herhangi bir yerden erişimimize hazır olan içerikler de bir saklayıcıya ihtiyaç duyar. Bunun gibi internet ortamında (sosyal medyada) içerik sağlayıcıların kullanıcılara içerik sağlaması için de bir internet ortamına ihtiyaçları vardır. Bu ihtiyacı sağlayan ve içerikleri kullanıcılarının hizmetine hazır ve nazır tutarak internet ortamı sağlayan kişiler bulunmaktadır. Yer sağlayıcı

⁴² Ayrıntılı bilgi için bkz. AKKURT, *Sosyal Medyada Gerçekleşen İhlaller Karşısında Kişilik Hakkının Korunması*, 258-318; Alp ÖZTEKİN, *Teori ve Uygulamada Türk İnternet Hukuku*, Güncellenmiş 2. Baskı (Seçkin Yayıncılık, 2023), 381-427.

(*hosting provider*), sağladığı donanım ve/veya sistemler dolayısıyla kullanıcıların içeriklerini barındırmaktadır.

5651 sayılı Kanun m. 2/1-m’de yer sağlayıcı, “*Hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişiler*” olarak tanımlanmıştır. Tanımdan görüleceği üzere yer sağlayıcı sıfatını haiz olabilmek için hizmet ve içerikleri barındıran sistemleri sağlamak ve/veya işletmek yeterli sayılmaktadır. Yer sağlayıcıya örnek olarak *Facebook, Instagram, X (Twitter), TikTok, Amazon, Sahibinden, YouTube, ekşi sözlük* verilebilir.

Yer sağlayıcılar, internet ortamına çeşitli şekillerde bilgi ve/veya veri sağlayan içerik sağlayıcıların verilerini kendi sisteminde, donanımında barındırmakta ve içerik sağlayıcının kullanımına hazır tutmaktadır. Yer sağlayıcı, verileri kendi sunucusunda tutabileceği gibi başka kişilerin donanımında, sanal depolama sunucusunda (*cloud-bulut depolamada*) da tutabilmektedir⁴³. Yukarıdaki tanımdan da görüleceği üzere yer sağlayıcılık için ilgili donanım yahut yazılıma bir zilyet yahut malik olmak gerekmemektedir⁴⁴.

Öte yandan yer sağlayıcılığın kapsamı belirlenirken “ön belleğe alma” (*caching*) kavramından bahsedilmesi gerekmektedir. Ön belleğe alma, bir verinin haberleşme ağında iletilmesinden oluşan ve bu bilginin bu iletim esnasında otomatik, geçici ve ara olarak depolanmasını ifade etmektedir. Bu faaliyeti esasında bir sonraki başlıkta açıklanacak olan erişim sağlayıcı gerçekleştirmektedir. Ancak ön belleğe alma faaliyetinde bir depolama durumunun olması, kafa karışıklığına sebebiyet verebilmektedir. Ön belleğe alınarak bir verinin geçici depolanması, yer sağlama hizmeti olarak ifade edilemeyecek olup birden çok internet kullanıcısının söz konusu veriye ulaşımında ağ performansını artırmak için gerekmektedir⁴⁵. Nitekim ikinci

⁴³ AKKURT, *Sosyal Medyada Gerçekleşen İhlaller Karşısında Kişilik Hakkının Korunması*, 137-38.

⁴⁴ ÖZTEKİN, *Teori ve Uygulamada Türk İnternet Hukuku*, 252; AKKURT, *Sosyal Medyada Gerçekleşen İhlaller Karşısında Kişilik Hakkının Korunması*, 139.

⁴⁵ YASAMAN, *Türk ve Avrupa Birliği Hukukunda İnternette Marka Hakkının İhlali*, 569-70.

bölümünün inceleme konusu olan Dijital Hizmetler Kanunu'nun (DSA)⁴⁶ 3. maddesinde aracılık hizmeti tanımlanırken ön belleğe alma hizmeti ile yer sağlama hizmeti ayrı olarak tanımlanmıştır.

Yer sağlayıcı olarak faaliyette bulunabilmek için sonraki başlıkta bahsedilen erişim sağlayıcıdan farklı olarak Faaliyet Belgesi Yönetmeliği'nde sermaye şirketi olma şartı aranmamaktadır. Yer sağlayıcı, faaliyet gösterebilmek için BTK'ya istenen evraklarla birlikte başvuru yapmak ve faaliyet belgesi almak zorundadır. Bu belgenin süresi ise Faaliyet Belgesi Yönetmeliği'nde 5 yıl olarak belirlenmiştir.

Yer sağlayıcı, barındırdığı içeriğin hukuka aykırı olup olmadığını kontrol etmekle yükümlü değildir. Ancak 5651 sayılı Kanun m. 8'e göre haberdar edilmesi halinde ilgili hukuka aykırı içeriği yayından çıkarmakla yükümlüdür. Öte yandan yer sağlayıcı, yer sağladığı hizmetlere ilişkin trafik bilgilerini 5651 sayılı Kanun ve İnternet Yönetmeliği tarafından öngörülen süre kadar muhafaza etmek zorundadır⁴⁷.

5651 sayılı Kanun m. 5/4, yönetmelikle yer sağlayıcıların yaptıkları işin niteliğine göre sınıflandırılacaklarını ve buna göre farklı hak ve yükümlülöklere tabi tutulabileceklerini ifade etmektedir.

3. Erişim Sağlayıcı

İçerik sağlayıcıların içerik sağlayabilmeleri için yukarıda açıklandığı üzere bir yer sağlama hizmetine ihtiyaç duyuyorlarsa aynı şekilde bu hizmeti kullanabilmeleri için bir internet ağına ihtiyaç duymaktadırlar. İşte, kanuni

⁴⁶ 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), L 277 OJ (2022), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R2065> DSA'nın Türkçe çevirisi için bkz. https://www.ab.gov.tr/siteimages/resimler/hcdb_dsa_14.10.2024.pdf (Son Erişim Tarihi: 27.05.2025).

⁴⁷ 5651 sayılı Kanun m. 5/3 uyarınca bu süre 1 yıldan az 2 yıldan fazla olmamak üzere belirlenirken İnternet Yönetmeliği m. 7/1-c'de azami bir süre öngörölmemiş, asgari olarak 6 aylık bir süre belirlenmiştir.

deyimiyle erişim sağlayıcıları (*access provider*) içerik sağlayıcılara bu imkânı tanımaktadır.

5651 sayılı Kanun m. 2/1-e’de erişim sağlayıcı, “*Kullanıcılarına internet ortamına erişim olanağı sağlayan her türlü gerçek veya tüzel kişiler*” olarak tanımlanmaktadır. Kanun’da her ne kadar her türlü gerçek veya tüzel kişinin erişim sağlayıcı olabileceği ifade edilse de Faaliyet Belgesi Yönetmeliği m. 4’e göre BTK tarafından erişim sağlayıcıya faaliyet belgesi verilebilmesi için erişim sağlayıcının sermaye şirketi olmasını aramaktadır. Günümüzde erişim sağlayıcıya örnek olarak TTNNet, Turkcell, Superonline, Türksat Kablonet, Vodafone verilebilir.

Öğretide ve uygulamada erişim sağlayıcı kavramı ile internet servis sağlayıcı kavramları zaman zaman birbiri yerine kullanılabilmektedir. İnternet servis sağlayıcı yukarıda incelenen yer sağlayıcı ile erişim sağlayıcıyı içine alan temel bir çatı kavramdır⁴⁸.

Erişim sağlayıcı 5651 sayılı Kanun m. 6 uyarınca kullanıcıların kendisi aracılığıyla eriştiği içeriklerin hukuka aykırı olup olmadığını kontrol etmekle yükümlü değildir. Böylelikle kanun koyucu erişim sağlayıcının sorumsuz olmasını hüküm altına almıştır. Gerçekten de kendisi aracılığıyla internet ortamına erişim olanağı elde eden çok sayıda kullanıcı olacağından erişim sağlayıcının bu kullanıcıların her birini tek tek incelemesi beklenemeyecektir.

Erişim sağlayıcının sorumsuzluğu kural olsa da erişim sağlayıcı tamamen sorumsuz da değildir. 5651 sayılı Kanun m. 6 uyarınca erişim sağlayıcı, bir kullanıcısının yayınladığı hukuka aykırı içerikten haberdar edilmesi halinde söz konusu içeriğe erişimi (alternatif erişim yöntemleri de dahil olmak üzere) engellemekle yükümlüdür. Ayrıca 5651 sayılı Kanun m. 6/A uyarınca faaliyet gösterebilmesi için Erişim Sağlayıcıları Birliği’ne üye olmak zorundadır. Erişim

⁴⁸ EKİCİ, *Bilişim ve Teknoloji Hukuku*, 133.

sağlayıcıların sağladığı hizmetlere ilişkin olarak trafik bilgilerini⁴⁹ mevzuatta öngörülen süre kadar saklama ve faaliyetlerine son vermeden önce BTK'ya bildirme yükümlülükleri de bulunmaktadır.

4. Toplu Kullanım Sağlayıcı

5651 sayılı Kanun m. 2/1-i'ye göre toplu kullanım sağlayıcı (*mass use provider*), “Kişilere belli bir yerde ve belli bir süre internet ortamı kullanım olanağı sağlayanı” ifade eder. Toplu kullanım sağlayıcıya örnek olarak internet kafeler, üniversiteler, kütüphaneler, ücretsiz internet kullanım olanağı sağlayan kamusal alanlar verilebilir. Sosyal hayat çerçevesinde kişiler belli mekânlara gittiğinde görevlilere “Buranın interneti var mı? Şifresi nedir?” sorularını sordukları yerlerdir.

Erişim sağlayıcı ve toplu kullanım sağlayıcı kavramları birbiri ile karıştırılabilecek kavramlardır. Kanuni tanıma göre misafirlğe gidilen bir evde internetini paylaşan ev sahibi de toplu kullanım sağlayıcı olabilmektedir. Ancak toplu kullanım sağlayıcı esasen internet ortamı kullanım olanağını erişim sağlayıcıdan aldığı yetki çerçevesinde sağlamaktadır. Kavramsal olarak muğlak ve karıştırılabilir olan bu durum öğretilde eleştirilmektedir⁵⁰.

Toplu kullanım sağlayıcıları 5651 sayılı Kanun ve İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik hükümlerine göre ticari amaçlı olup olmadıklarına göre ikiye ayrılarak yükümlülükleri belirlenmektedir. Ticari amaçlı olup olmadıklarına bakılmaksızın tüm toplu kullanım sağlayıcıları için içerik filtreleme, erişim bilgilerini saklama ve kullanıcıları tespiti yarayacak sistemleri kurma yükümlülüğü öngörülmüştür. Ticari amaçlı toplu kullanım sağlayıcılar ise ek olarak mülki idare amirinden izin almak, güvenli internet hizmeti sunmak,

⁴⁹ 5651 sayılı Kanun m. 2/1-j uyarınca trafik bilgisi, taraflara ilişkin IP adresi, port bilgisi, verilen hizmetin başlama ve bitiş zamanı, yararlanılan hizmetin türü, aktarılan veri miktarı ve varsa abone kimlik bilgilerini ifade eder.

⁵⁰ AKKURT, *Sosyal Medyada Gerçekleşen İhlaller Karşısında Kişilik Hakkının Korunması*, 327; EKİCİ, *Bilişim ve Teknoloji Hukuku*, 136.

erişim sağlayıcıdan sabit IP alıp kullanmak ve değişiklikleri mülki idare amirine bildirmek gibi mevzuatta öngörülen yükümlülöklere tabi tutulmuştur.

5. Sosyal Ağ Sağlayıcı

5651 sayılı Kanun'un yürürlöğe girdiğı 2007'den bu yana teknolojik gelişmeler artarak devam etmiş, sosyal medya platformlarının toplumsal hayattaki etkisi de aynı şekilde artmıştır. Toplumun sosyalleşmesini, etkileşim kurma imkânını artıran sosyal medya, hukuka aykırı fiillerin de görüldüğü bir ortam olmuştur. Bu durumun etkilerini azaltmak adına kanun koyucu harekete geçmiş ve Temmuz 2020'de 7253 sayılı Kanun⁵¹ ile hukukumuzda yeni bir sosyal medya süjesini kazandırmıştır. 5651 sayılı Kanun'a yer sağlayıcının bir görünümü olan sosyal ağ sağlayıcı eklenmiştir.

5651 sayılı Kanun m. 2/1-s'ye göre sosyal ağ sağlayıcı, *"Sosyal etkileşim amacıyla kullanıcıların internet ortamında metin, görüntü, ses, konum gibi içerikleri oluşturmalarına, görüntülemelerine veya paylaşımlarına imkân sağlayan gerçek veya tüzel kişiler"* olarak tanımlanmıştır. Sosyal ağ sağlayıcıya örnek olarak Meta (Facebook, Instagram), X (Twitter), TikTok, YouTube, LinkedIn verilebilir.

Anayasa Mahkemesi 11.10.2023 tarihinde yaptığı somut norm denetimi sonucunda kanuni tanımda geçen "sosyal etkileşim", "oluşturma", "görüntüleme", "paylaşma" ibarelerinin genel nitelikte olduğunu kabul etmiş ancak hukuki belirsizlik ve öngörülemezlik taşımadığını ifade ederek tanımın Anayasa'ya aykırı olmadığına hükmetmiştir⁵².

Doktrinde, Anayasa Mahkemesi'nin aksine tanımın son derece geniş olduğu, tanımda geçen "veya" ibaresi dolayısıyla sadece oluşturma, sadece

⁵¹ 31/07/2020 tarihli ve 31202 sayılı Resmî Gazete, <https://www.resmigazete.gov.tr/eskiler/2020/07/20200731-1.htm>.

⁵² 11.10.2023 Tarihli ve E. 2020/76, K. 2023/172 Sayılı Kararı, No. 2020/76 (Anayasa Mahkemesi 11 Ekim 2023), de Paragraf 11, 10/01/2024 tarihli ve 32425 sayılı Resmî Gazete, <https://www.resmigazete.gov.tr/eskiler/2024/01/20240110-3.pdf>.

görüntüleme, sadece paylaşma imkânı sağlayan bir kişinin sosyal ağ sağlayıcı olarak kabul edilebileceği ifade edilmiştir⁵³.

Sosyal ağ sağlayıcıya ilişkin hükümlerin Alman Ağ Yaptırım Kanunu⁵⁴ model alınarak ihdas edildiği ifade edilmektedir⁵⁵. Söz konusu düzenlemeye göre sosyal ağ sağlayıcı tanımlanırken iki husus dikkat çekmektedir. Bunlardan ilki, 5651 sayılı Kanun'da yer almayan "kâr elde etme amacı"dır⁵⁶. Böylelikle kâr elde etme amacı olmayan ancak kullanıcıların herhangi bir içeriği paylaşmalarına imkân sağlayan bir platform kapsam dışına çıkarılmış olmaktadır. 5651 sayılı Kanun açısından bakıldığında ise böyle bir ayırım yapılmamıştır. Sözel bir yorum yapıldığında Ağ Yaptırım Kanunu kapsamında olmayan platformların 5651 sayılı Kanun kapsamına girmesi söz konusu olacaktır.

Diğer bir dikkat çeken husus ise Ağ Yaptırım Kanunu'nda sosyal ağ sağlayıcı tanımlanırken sosyal etkileşim amacından bahsedilmemesidir⁵⁷. Türk kanun koyucusunun böyle bir amacı hükümde ifade etmesinin, sosyal ağ sağlayıcıyı yer sağlayıcıdan ayırmak ve kapsamı daraltmak istemesinden kaynaklandığını kanaatindeyiz.

Doktrinde sosyal medya platformlarının yer sağlayıcı olup olmadıkları noktasında iki görüş bulunmaktadır. *Bir görüşe göre* bu platformlar sadece söz konusu internet sitesini işlettikleri için yer sağlayıcı sayılmamalıdır. Bu çevrimiçi platformlar işlettikleri platformlardaki verileri başka şirketlerin sunucularında

⁵³ AKKURT, *Sosyal Medyada Gerçekleşen İhlaller Karşısında Kişilik Hakkının Korunması*, 186-90; ÖZTEKİN, *Teori ve Uygulamada Türk İnternet Hukuku*, 297-98; TURGUT, *Kişilik Hakkının Bir Görünümü Olarak Unutulma Hakkı*, 396.

⁵⁴ Düzenlemenin resmî metni için bkz. <https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html>.

⁵⁵ AKKURT, *Sosyal Medyada Gerçekleşen İhlaller Karşısında Kişilik Hakkının Korunması*, 183; TURGUT, *Kişilik Hakkının Bir Görünümü Olarak Unutulma Hakkı*, 395.

⁵⁶ Alman Ağ Yaptırım Kanunu m. 1.

⁵⁷ Alman Ağ Yaptırım Kanunu m. 1.

depolayabilir. Zira bu platformlar kanun koyucu tarafından sosyal ağ sağlayıcı olarak kabul edilmiştir⁵⁸.

Doktrindeki ikinci görüşe göre ise bu platformların söz konusu verileri başka şirketler nezdindeki sunucularda depolayabilmeleri yer sağlayıcı olarak kabul edilmelerine engel değildir. Bu platformların sağladıkları arayüzler başlı başına sistem olarak kabul edilmelidir⁵⁹. Nitekim kanun koyucu 7253 sayılı Kanun’la değişik 5651 sayılı Kanun Ek m. 4/17’de sosyal ağ sağlayıcıların içerik ve/veya yer sağlayıcı olmasından kaynaklanan yükümlülüklerini ortadan kaldırmayacağı hüküm altına alınmıştır⁶⁰.

Öte yandan kanun koyucu, 5651 sayılı Kanun Ek m. 4/21’de sosyal ağ sağlayıcıya ilişkin hükmün uygulanmasına ilişkin usul ve esasların BTK tarafından belirleneceğini hüküm altına almıştır. BTK, bu hüküm çerçevesinde 01.04.2023 tarihinde 2023/DK-İD/119 sayılı “Sosyal Ağ Sağlayıcı Hakkında Usul ve Esaslar” kararını Resmî Gazete’de yayımlamıştır⁶¹.

BTK, Sosyal Ağ Sağlayıcı Hakkında Usul ve Esaslar m. 1/3 ve m. 1/4’te sosyal ağ sağlayıcının kapsamına yönelik hükümler sevk etmiştir. Buna göre kişisel internet siteleri, elektronik ticaret siteleri ve haber siteleri gibi sosyal etkileşim amaçlı içeriğin ikincil ve yan bir hizmet olarak sunulduğu platformlar ile internet ortamında yapılan yayının sadece belirli bir kısmında sosyal etkileşim amaçlı içeriğe yer veren gerçek ve tüzel kişiler sosyal ağ sağlayıcı değildir.

Bu doğrultuda *WhatsApp* ve *Telegram* gibi sosyal mesajlaşma site ve uygulamaları, sosyal ağ sağlayıcı kapsamında değerlendirilemeyecektir. Nitekim

⁵⁸ ÖZTEKİN, *Teori ve Uygulamada Türk İnternet Hukuku*, 254.

⁵⁹ AKKURT, *Sosyal Medyada Gerçekleşen İhlaller Karşısında Kişilik Hakkının Korunması*, 138-40.

⁶⁰ Kanun koyucunun sosyal ağ sağlayıcı kavramını ihdas etmesiyle doktrindeki bu tartışmalarının önemini yitirdiği, zira sosyal ağ sağlayıcının yer sağlayıcının özel bir görünümü olduğu yönünde bkz. EKİCİ, *Bilişim ve Teknoloji Hukuku*, 127.

⁶¹ Bilgi Teknolojileri ve İletişim Kurumu, “Sosyal Ağ Sağlayıcı Hakkında Usul ve Esaslar (2023/DK-İD/119)”, R.G. 32150, 01 Nisan 2023, <https://www.resmigazete.gov.tr/eskiler/2023/04/20230401-13.pdf>.

bu uygulamalarda gruplar ve topluluklar kurulabilmekte ve sosyal etkileşim sağlanabilmektedir. Ancak BTK'nın anılan kararı uyarınca bu gruplar internet ortamındaki yayının belirli bir kısmını teşkil ettiği için sosyal mesajlaşma uygulamaları sosyal ağ sağlayıcı kapsamında sayılamayacaktır⁶².

Sosyal ağ sağlayıcıların kapsamının bir idari kararla belirlenmesi, *kanaatimizce* hukuki güvenlik, öngörülebilirlik ve belirlilik açısından ihtiyatla karşılanması gereken bir durumdur. Zira sosyal ağ sağlayıcı sıfatını haiz bir sosyal medya platformunun aşağıda inceleneceği üzere ciddi hukuki sonuçları olan yükümlülükleri bulunmaktadır. Dolayısıyla sosyal ağ sağlayıcı kavramının idari karar yahut yönetmelik gibi yürütme erki araçlarıyla değil, kanun formunda netleştirilmesi daha isabetli olacaktır⁶³.

Sosyal ağ sağlayıcının yükümlülükleri 7253 ve 7418 sayılı Kanun ile 5651 sayılı Kanun'a eklenen Ek Madde 4'te sayılmıştır. Ek Madde 4'te sayılan bu yükümlülükler, sosyal ağ sağlayıcıların günlük erişim sayısındaki farklılıklar ile yurt içi ve yurt dışı kaynaklı olmaları bakımından farklılaşabilmektedir.

⁶² Aynı görüşte bkz. ÖZTEKİN, *Teori ve Uygulamada Türk İnternet Hukuku*, 298-300; aksi görüş için bkz. AKKURT, *Sosyal Medyada Gerçekleşen İhlâller Karşısında Kişilik Hakkının Korunması*, 187-88.

⁶³ Aynı görüşte TURGUT, *Kişilik Hakkının Bir Görünümü Olarak Unutulma Hakkı*, 396.



Şema 2: Sosyal Ağ Sağlayıcının Yükümlülükleri

a) Temsilci Belirleme ve Bildirme Yükümlülüğü

Sosyal ağ sağlayıcıların yukarıda verilen yükümlülükleri hakkında açıklama yapmakta fayda vardır⁶⁴. Öncelikle temsilci belirleme ve bildirme yükümlülüğü, 5651 sayılı Kanun Ek m. 4/1’de hüküm altına alınmıştır. Bu hükme göre Türkiye’deki günlük erişimi *bir milyondan fazla* olan “yurt dışı” kaynaklı sosyal ağ sağlayıcı, BTK, Erişim Sağlayıcıları Birliği, adli veya idari makamlarca gönderilecek tebligat, bildirim veya taleplerin gereğinin yerine getirilmesi ve kişiler tarafından 5651 sayılı Kanun kapsamında yapılacak başvuruların

⁶⁴ Anayasa Mahkemesi tarafından 5651 sayılı Kanun m. 9 hükmü, kişilik haklarına yapılan saldırılara kademeli müdahale yöntemi getirmemesi, içeriğin kararın verildiği tarihten itibaren süresiz engellendiği ve bu yönüyle ifade ve basın özgürlüklerine ağır müdahale teşkil ettiği gerekçesiyle iptal etmiştir. Bu sebeple 5651 sayılı Kanun Ek m. 4’te zikredilen bu hükme sosyal ağ sağlayıcıların yükümlülükleri arasında yer verilmemiştir. 11.10.2023 Tarihli ve E. 2020/76, K. 2023/172 Sayılı Kararı, Paragraf 97-107.

cevaplandırılması ve 5651 sayılı Kanun kapsamındaki diğer yükümlülüklerin yerine getirilmesini temin için yetkili “en az” bir kişiyi Türkiye’de temsilci⁶⁵ olarak belirler ve bu kişinin iletişim bilgilerine kolayca görülebilecek ve doğrudan erişilebilecek şekilde internet sitesinde yer vermekle, bu kişinin kimlik ve iletişim bilgilerini BTK’ya bildirmekle yükümlü tutulmuştur⁶⁶.

Aynı hükme göre temsilcinin gerçek kişi olması hâlinde bu kişinin Türkiye’de mukim ve Türk vatandaşı olması zorunludur. Türkiye’den günlük erişimin *on milyondan fazla* olması hâlinde yurt dışı kaynaklı sosyal ağ sağlayıcı tarafından belirlenen gerçek veya tüzel kişi temsilci, *sosyal ağ sağlayıcının sorumlulukları saklı kalmak kaydıyla* teknik, idari, hukuki ve mali yönden tam yetkili ve sorumlu olup bu temsilcinin tüzel kişi olması hâlinde doğrudan sosyal ağ

⁶⁵ Bilgi Teknolojileri ve İletişim Kurumu, “Sosyal Ağ Sağlayıcı Hakkında Usul ve Esaslar (2023/DK-İD/119)”. Bu kararda temsilcinin görevleri m. 6’da şöyle ifade edilmiştir:

“Belirlenen temsilci;

a) Kurum, Birlik, adli veya idari makamlarca gönderilecek tebligat, bildirim veya taleplerin gereğinin yerine getirilmesini,

b) Kişiler tarafından bu Kanun kapsamında yapılacak başvuruların cevaplandırılmasını,

c) Raporlama yükümlülüğünün yerine getirilmesini,

ç) Sosyal ağ sağlayıcının içerik veya yer sağlayıcı olmasından doğan sorumluluk ve yükümlülüklerinin yerine getirilmesini,

d) Kanun kapsamındaki diğer yükümlülüklerin yerine getirilmesini, temin eder.”

⁶⁶ Bilgi Teknolojileri ve İletişim Kurumu, “Sosyal Ağ Sağlayıcı Hakkında Usul ve Esaslar (2023/DK-İD/119)”. Temsilciye ilişkin bilgi belgelerin gönderilmesi ile ilgili kararın 8. maddesinde şöyle bir hüküm bulunmaktadır: “(1) Sosyal ağ sağlayıcı, temsilci kimlik, unvan ve iletişim bilgilerini Kuruma bildirmekle yükümlüdür.

(2) Temsilcinin gerçek kişi olması hâlinde bu temsilcinin Türk vatandaşı ve Türkiye’de mukim olduğunu gösterir belgeler Kuruma gönderilir.

(3) Temsilcinin tüzel kişi olması hâlinde, tüzel kişinin şirket sözleşmesi, ticaret sicil gazetesini örneği ve diğer kuruluş belgeleri ile tüzel kişiliği temsil ve ilzama yetkili kişilerin yetkili kılındığına dair ilgili mevzuat kapsamındaki belgelerle birlikte kimlik ve iletişim bilgileri Kuruma gönderilir.

(4) Türkiye’den günlük erişimi on milyondan fazla olan sosyal ağ sağlayıcının temsilcisinin tüzel kişi olması hâlinde, üçüncü fıkrafta yer alan bilgi ve belgelere ilave olarak bu Usul ve Esaslar’ın 5 inci maddesinde aranan şartları ispat edecek bilgi ve belgeler Kuruma gönderilir.

(5) Bu madde kapsamında gönderilen bilgi ve belgelerde değişiklik olması durumunda, bu değişiklikleri içeren bilgi ve belgeler derhal ve en geç yetmiş iki saat içinde Kuruma bildirilir.”

sağlayıcı tarafından “sermaye şirketi şeklinde kurulan bir şube⁶⁷” olması zorunlu tutulmuştur.

Temsilci belirleme ve bildirme yükümlülüğü, anılan hükümlerin lafzından yurt içi kaynaklı sosyal ağ sağlayıcılar için öngörülmediği anlamı çıkmaktadır. Dolayısıyla yurt içi kaynaklı bir sosyal ağ sağlayıcı, temsilci belirlemek ve BTK’ya bildirmek zorunda değildir⁶⁸. Diğer bir ifadeyle kanun koyucu içerik kaldırması için uyarı yapılan sosyal ağ sağlayıcılara ulaşma ve cevap alma zorluğunu dikkate alarak bu hükmü yurt dışı kaynaklı sosyal ağ sağlayıcılar için ihdas etmiştir.

Öte yandan bu yükümlülük için kanunda belirlenen eşikler, yükümlülüğün sükelerinin kim olacağına dair belirlemede bulunmaktadır. Bu doğrultuda Türkiye’deki günlük erişimi bir milyon ve altında olan yurt dışı kaynaklı sosyal ağ sağlayıcı bu yükümlülüğten muaftır. Bu erişim miktarının on milyon ve altında olması halinde yurt dışı kaynaklı sosyal ağ sağlayıcının belirlediği temsilci, teknik, idari, mali ve hukuki yönden tam yetkili sayılmayacak ve tüzel kişi temsilcinin

⁶⁷ Bilgi Teknolojileri ve İletişim Kurumu, “Sosyal Ağ Sağlayıcı Hakkında Usul ve Esaslar (2023/DK-ID/119)”. Bu kararda söz konusu şubenin sahip olması gereken nitelikler m. 5/2’de şöyle belirtilmiştir: “a) Sosyal ağ sağlayıcının unvanının ayırt edici ibaresi ile sermaye şirketinin kurulduğu ili de içeren ticaret unvanına sahip olması,

b) Paylarının tamamının sosyal ağ sağlayıcıya ait olması,

c) Şirket sözleşmesinde sosyal ağ sağlayıcının bünyesinde ve sosyal ağ sağlayıcıya bağlı olduğunu belirtmesi,

ç) Esas sermaye tutarının en az yüz milyon Türk Lirası olması,

d) Şirket sözleşmesinde, sosyal ağ sağlayıcı tarafından teknik, idari, hukukî ve mali yönden tam yetkili ve sorumlu kılındığının açıkça belirtilmesi.”

⁶⁸ Aynı yönde bkz. EKİCİ, *Bilişim ve Teknoloji Hukuku*, 143; AKKURT, *Sosyal Medyada Gerçekleşen İhlaller Karşısında Kişilik Hakkının Korunması*, 195.

5651 sayılı Kanun uyarınca bir sermaye şirketi şeklinde kurulan bir şube⁶⁹ olma zorunluluğundan söz edilmeyecektir⁷⁰.

5651 sayılı Kanun Ek m. 4/2’de temsilci belirleme ve bildirme yükümlülüğünün yerine getirilmemesi halinde uygulanacak müeyyide katmanı belirlenmiştir. Anılan hükme göre BTK, temsilci belirleme ve bildirme yükümlülüğünü yerine getirmeyen sosyal ağ sağlayıcıya bildirimde bulunur. Bu bildirimden itibaren otuz gün geçmesine rağmen yükümlülük yerine getirilmezse BTK Başkanı tarafından on milyon Türk lirası idari para cezası uygulanacaktır. İdari para cezasının tebliğinden itibaren otuz gün içinde yükümlülüğün yerine getirilmemesi halinde otuz milyon Türk lirası “daha” idari para cezası verilecektir. Bu idari para cezasının tebliğinden itibaren otuz gün sonra yine yükümlülük yerine getirilmezse BTK Başkanı tarafından Türkiye’de yerleşik vergi mükellefi olan gerçek ve tüzel kişilerin ilgili sosyal ağ sağlayıcıya reklam vermesi, buna ilişkin sözleşme ve para transferi yapılması yasaklanacaktır.

Reklam yasağı kararının verildiği tarihten itibaren üç ay içinde bu yükümlülüğün yerine getirilmemesi hâlinde BTK Başkanı, sosyal ağ sağlayıcının

⁶⁹ 5651 sayılı Kanun Ek m. 4/1’de geçen bu ibare, ticari işletme hukuku açısından sorunlu bir ifadedir. Lafzi olarak bakıldığında sosyal ağ sağlayıcının temsilcisinin Türkiye’deki şubesinin sermaye şirketi olarak kurulması gerektiği anlamı çıkmaktadır. Burada kastedilen, sosyal ağ sağlayıcının belirleyeceği temsilcinin, sermaye şirketi şeklinde kurulmuş olan sosyal ağ sağlayıcının bir şubesi olduğudur. Buna ilişkin bir hüküm sevk edilmeyebilirdi. Zira, TTK m. 40/4 uyarınca merkezi Türkiye dışında olan ticari işletmelerin şubeleri için yerleşim yeri Türkiye’de bulunan tam yetkili ticari mümessilin atanacağı hüküm altına alınmıştır. Ayrıca şube olmanın ihtiyari bir unsuru olan müstakil sermaye, TSY m. 123/1-c uyarınca ticaret siciline tescil için gerekli görülmüştür. Burada kanun koyucu, sadece Sosyal Ağ Sağlayıcılar Hakkında Usul ve Esaslar m. 5/2-ç’deki gibi esas sermaye tutarını belirlemekle yetinebilirdi. Kanun koyucu, hükmü buna rağmen ihdas etmek istiyorsa hükümdeki bu hatalı ibareyi, “sermaye şirketi şeklinde kurulan sosyal ağ sağlayıcının şubesi” olarak değiştirmesi daha isabetli olacaktır. Şube kavramı hakkında ayrıntılı bilgi için bkz. Şaban KAYIHAN, *Ticari İşletme Hukuku*, Gözden Geçirilmiş ve Güncellenmiş 7. Baskı (Seçkin Yayıncılık, 2021), 63-66.

⁷⁰ 5651 sayılı Kanun’da ve Sosyal Ağ Sağlayıcı Hakkında Usul ve Esaslar’da eşiklerin belirlenmesi bakımından aynı veya farklı kullanıcılar arasında bir fark gözetilmemiştir. Yine aynı şekilde sitenin hangi sayfalarının dikkate alınacağı da belirlenmemiştir. Aynı yönde bkz. AKKURT, *Sosyal Medyada Gerçekleşen İhlâller Karşısında Kişilik Hakkının Korunması*, 194 Yazar, sosyal ağ sağlayıcılara ilişkin hükümlerin model düzenlemesi olarak belirtilen Alman Ağ Yaptırım Kanunu’nun aksine 5651 sayılı Kanun’da günlük erişim sayısının kıstas olarak kabul edildiğini ve site ana sayfasına dahi olsa erişimin dikkate alınmasının isabetli olacağını ifade etmektedir.

internet trafiđi bant geniřliđinin y zde elli oranında daraltılması i in sulh ceza h kimliđine bařvurabilecektir. H km n lafzından bu bařvurunun ihtiyari olduđu anlamı  ıkmaktadır.

řayet bařvuru yapılmıřsa bařvurunun kabul ne iliřkin h kim kararının uygulanmasından itibaren otuz g n i inde s z konusu y k ml l đ n yerine getirilmemesi h linde BTK Bařkanı, sosyal ađ sađlayıcının internet trafiđi bant geniřliđinin y zde doksan oranına kadar daraltılması i in sulh ceza h kimliđine bařvurabilir. H kim ikinci bařvuru  zerine vereceđi kararında, y zde elliden d ř k olmamak kaydıyla sunulan hizmetin niteliđini de dikkate alarak daha d ř k bir oran belirleyebilir. Bu kararlara karřı BTK Bařkanı tarafından CMK h k mlerine g re itiraz yoluna gidilebilir.

Temsilci belirleme ve bildirme y k ml l đ n n yerine getirilmesi h linde verilen idari para cezalarının d rtte biri tahsil edilir, reklam yasađı kaldırılır ve h kim kararları kendiliđinden h k ms z kalır. İnternet trafiđi bant geniřliđine yapılan m dahalenin sona erdirilmesi i in eriřim sađlayıcılara BTK tarafından bildirim yapılır.

b) Bařvurulara Cevap Verme Y k ml l đ 

5651 sayılı Kanun Ek m. 4/3'te 5651 sayılı Kanun m. 9/A kapsamındaki bařvurulara cevap verme y k ml l đ   ng r lm řt r. Bu h kme g re yurt i i veya yurt dıřı kaynaklı fark etmeksizin T rkiye'deki g nl k eriřimi *bir milyondan fazla* olan sosyal ađ sađlayıcı, m. 9/A kapsamında kiřilerce yapılacak bařvurulara bařvurudan itibaren en ge  48 saat i inde olumlu veya gerek eli olumsuz cevap

verme yükümü altına alınmıştır⁷¹. Bu yükümlülüğü yerine getirmeyen sosyal ağ sağlayıcıya idari para cezası verilecektir⁷².

c) Raporlama Yükümlülüğü

Diğer bir yükümlülük olan raporlama yükümlülüğüne ilişkin 5651 sayılı Kanun Ek m. 4/4'te Türkiye'den günlük erişimi *bir milyondan fazla* olan sosyal ağ sağlayıcı, kendisine bildirilen içeriğin çıkarılması ve/veya erişimin engellenmesi kararlarının uygulanmasına ve üçüncü fıkra kapsamındaki başvurulara ilişkin istatistiksel ve kategorik bilgileri içeren Türkçe hazırlanmış raporları altı aylık dönemlerle BTK'ya bildirmek zorundadır. Günlük erişimin bir milyon ve altında olması halinde sosyal ağ sağlayıcının raporlama yükümlülüğü bulunmamaktadır. Üçüncü fıkra da belirtilen 5651 sayılı Kanun m 9/A'ya ilişkin başvurular kapsamında işlenen kişisel verilere raporda yer verilmeyecek olup bu başvurulara ilişkin rapor, ilgili sosyal ağ sağlayıcının sitesinde de yayınlanacaktır.

Raporlama yükümlülüğü kapsamında sosyal ağ sağlayıcılar hesap verilebilirlik ilkesine uymakla, 5651 sayılı Kanun'un uygulanmasında şeffaf olmakla ve BTK tarafından bilgi ve belge talebine olumlu cevap dönüş yapmakla yükümlü kılınmıştır. Ayrıca sosyal ağ sağlayıcı, kullanıcılara öneride bulunurken dikkate aldığı parametreleri sitesinde yayınlamakla da yükümlü kılınmıştır. Bu yükümlülük kapsamında son olarak sosyal ağ sağlayıcı, bir reklam kütüphanesi

⁷¹ Sosyal ağ sağlayıcının başvurularda Türkçe dil desteği kullanılabilmesini sağlama ve Türkçe yapılan başvurularda Türkçe cevap verme yükümlülüğü olduğu yönünde bkz. Bilgi Teknolojileri ve İletişim Kurumu, "Sosyal Ağ Sağlayıcı Hakkında Usul ve Esaslar (2023/DK-İD/119)", md. 9.

⁷² Bilgi Teknolojileri ve İletişim Kurumu, "Sosyal Ağ Sağlayıcı Hakkında Usul ve Esaslar (2023/DK-İD/119)", md. 26. Bu hükme göre BTK, (a) Sosyal ağ sağlayıcının yükümlülüğünü etkin bir şekilde yerine getirmek için gerekli sistemleri kurup kurmaması,

(b) Sosyal ağ sağlayıcının belirli kişilere veya kurumlara düzenli olarak olumsuz cevap vermesi,

(c) Bu Usul ve Esaslarda belirlenen süreye sistematik olarak aykırı davranması,

(ç) Başvurulara verilen olumsuz cevapların gerekçesiz olması hususlarının başvurulara cevap verme yükümlülüğünü yerine getirip getirmediğini değerlendirirken dikkate alacaktır.

oluşturup sitesinde yayınlamakla mükelleftir. Raporlama yükümlülüğünün müeyyidesi olarak idari para cezası öngörülmüştür.

d) BTK ve Kolluk Birimlerine Bilgi Verme Yükümlülüğü

Sosyal ağ sağlayıcılara getirilen diğer bir yükümlülük ise BTK ve kolluk birimlerine bilgi verme yükümlülüğüdür. Bu yükümlülük hem yurt içi hem de yurt dışı kaynaklı sosyal ağ sağlayıcı için geçerlidir. Bu doğrultuda 5651 sayılı Kanun Ek m. 4/16'da kolluk kuvvetlerine, Ek m. 4/18'de BTK'ya bilgi verme yükümlülüğü düzenlenmiştir.

5651 sayılı Kanun Ek m. 4/16'ya göre tüm sosyal ağ sağlayıcılar, kişilerin can ve mal güvenliğini tehlikeye sokan içerikleri öğrenmesi ve gecikmesinde sakınca bulunması hâlinde, bu içeriği ve içeriği oluşturana ilişkin bilgileri yetkili kollukla paylaşmakla yükümlüdür. Buna göre tüm sosyal ağ sağlayıcılar, kişilerin can ve mal güvenliğini tehlikeye sokan bir içeriği öğrenmesi ve müdahalede gecikilmesinde sakınca bulunması durumunda bu içeriğe ve içeriği oluşturana ilişkin bilgileri kollukla paylaşmak zorundadır. Bu yükümlülüğe uymayan sosyal ağ sağlayıcıya BTK Başkanı tarafından bir önceki takvim yılındaki küresel cirosunun %3'üne kadar idari para cezası verilebilecektir.

Esasen toplumun sosyalleşmesine, içerik oluşturup paylaşmasına dijital bir ortam sunan sosyal ağ sağlayıcıların kişilerin can ve mal güvenliğini tehlikeye sokan içerikleri ve içinde bulunan hâlin gecikmesinde sakınca bulunan bir hâl olup olmadığını nasıl tespit edecekleri merak konusudur. Öte yandan bu hükümlerin hukuk düzenine entegre edilmesi, sosyal ağ sağlayıcıların bu tür içeriklere karşı sessiz kalmasına karşılık vatandaşların temel hak ve hürriyetlerinin korunması amacına da çelişki oluşturmaktadır. Bu çelişki, BTK tarafından yukarıda bahsedilen 2023/DK-İD/119 sayılı karar ile açıklığa kavuşturulabilirdi. Ancak yönetmelik yerine Resmî Gazete'de idari bir karar olarak yayınlanan Sosyal Ağ

Sağlayıcı Hakkında Usul ve Esaslar'da da çelişki giderilmemiş, kanun hükümleri kopyala-yapıştır ile tekrarlanmıştır⁷³.

Öte yandan hükmün lafzına bakıldığında kişilerin can ve mal güvenliğini tehlikeye sokan içeriği öğrenme ile gecikmesinde sakınca bulunma durumlarının birlikte gerçekleşmesi gerektiği anlaşılmaktadır. Dolayısıyla gecikmesinde sakınca bulunmayan ancak kişilerin can ve mal güvenliğini tehlikeye sokan içerikleri öğrenmesi bu hükmün kapsamı dışında kalmaktadır⁷⁴.

5651 sayılı Kanun Ek m. 4/18'de BTK'ya bilgi verme yükümlülüğü düzenlenmiştir. Buna göre tüm sosyal ağ sağlayıcılar, BTK'nın talep etmesi halinde kurumsal yapı, bilişim sistemleri, algoritmalar, veri işleme mekanizmaları ve ticari tutumlar dâhil her türlü açıklamayı, bilgi ve belgeyi BTK'ya en geç üç ay içinde teslim etmek zorundadır. Ayrıca bu hükme göre BTK, sosyal ağ sağlayıcının bütün tesislerinde yerinde inceleme yapma yetkisini haizdir. Bu yükümlülüğe uymayan sosyal ağ sağlayıcıya BTK Başkanı tarafından bir önceki takvim yılındaki küresel cirosunun %3'üne kadar idari para cezası verilebilecektir.

e) Yargı Mercilerine Bilgi Verme Yükümlülüğü

Sosyal ağ sağlayıcının temsilcisi, 5651 sayılı Kanun Ek m. 4/5'te sayılan katalog suçlara⁷⁵ konu internet içeriklerini oluşturan veya yayan faillere ulaşmak için gerekli olan bilgileri soruşturma aşamasında Cumhuriyet savcısı, kovuşturma

⁷³ Aynı görüşte bkz. AKKURT, *Sosyal Medyada Gerçekleşen İhlaller Karşısında Kişilik Hakkının Korunması*, 211; ÖZTEKİN, *Teori ve Uygulamada Türk İnternet Hukuku*, 331.

⁷⁴ EKİCİ, *Bilişim ve Teknoloji Hukuku*, 150 Yazar, 5651 sayılı Kanun Ek m. 4/16 hükmünün gecikmesinde sakınca bulunan bir hal ve kişilerin can ve mal güvenliğini tehlikeye sokan içerik olmak üzere iki şart öngördüğünü ifade etmektedir.

⁷⁵ Hükümde bahsedilen ve TCK'da yer alan katalog suçlar şunlardır:

- a) Çocukların cinsel istismarı (madde 103),
- b) Halkı yanıltıcı bilgiyi alenen yayma (madde 217/A),
- c) Devletin birliğini ve ülke bütünlüğünü bozmak (madde 302),
- ç) Anayasal Düzene ve Bu Düzenin İşleyişine Karşı Suçlar (madde 309, 311, 312, 313, 314, 315, 316),
- d) Devlet Sırlarına Karşı Suçlar ve Casusluk (madde 328, 329, 330, 331, 333, 334, 335, 336, 337).

aşamasında yargılamanın yürütüldüğü mahkeme tarafından talep edilmesi üzerine adli mercilere teslim edecektir.

Bu bilgilerin talep eden Cumhuriyet Başsavcılığı veya mahkemeye verilmemesi durumunda ilgili Cumhuriyet savcısı tarafından yurt dışı kaynaklı sosyal ağ sağlayıcının internet trafiği bant genişliğinin yüzde doksan oranında daraltılması talebiyle Ankara Sulh Ceza Hâkimliğine başvurulabilir. İnternet trafiği bant genişliğinin daraltılması kararı verilmesi hâlinde bu karar erişim sağlayıcılara bildirilmek üzere BTK'ya gönderilir. Kararın gereği bildirimden itibaren derhâl ve en geç dört saat içinde erişim sağlayıcıları tarafından yerine getirilir. Sosyal ağ sağlayıcı bu yükümlülüğünü yerine getirmesi hâlinde yaptırımlar⁷⁶ kaldırılır ve durum BTK'ya bildirilir.

Yükümlülüğünün öngörüldüğü hükümde hangi sosyal ağ sağlayıcıların bu yükümlülüğe tabi olduğu konusunda bir belirleme yapılmamıştır. Ancak düzenlemede gerekli bilgilerin sosyal ağ sağlayıcısının temsilcisi tarafından verileceği ifade edilmiştir. Bu doğrultuda temsilci belirleme ve bildirme yükümü altında bulunan yurt dışı kaynaklı sosyal ağ sağlayıcıların bu hükme tabi olduğu ancak yurt içi kaynaklı sosyal ağ sağlayıcının tabi olmadığı sonucuna ulaşılmalıdır. Dolayısıyla bu hükme, Türkiye'deki günlük erişimi bir milyon ve altında olan yurt dışı kaynaklı sosyal ağ sağlayıcılar ve günlük erişim sayısına bakılmaksızın tüm yurt içi kaynaklı sosyal ağ sağlayıcılar tabi değildir⁷⁷.

⁷⁶ ÖZTEKİN, *Teori ve Uygulamada Türk İnternet Hukuku*, 324 Yazar, bant genişliğinin daraltılmasına ilişkin uygulamanın bir idari tedbir niteliğinde olduğunu ifade etmektedir. Yazar, ayrıca bant genişliğinin daraltılmasına yönelik başvuruyu alan Ankara Sulh Ceza Hâkimliğinin KVKK ve sair norma göre "hukuka uygun" olarak tutulmuş log kayıtlarını "elinde bulundurmasına rağmen iletmemesi" durumunu tespit ederek bant genişliğini daraltma yönünde karar vermesi gerektiğini belirtmektedir.

⁷⁷ Aynı yönde bkz. EKİCİ, *Bilişim ve Teknoloji Hukuku*, 150.

f) Türkiye’deki Kullanıcıların Verilerini Türkiye’de Barındırma ve Kullanıcı Haklarına İlişkin Düzenlemelere Uyma Yükümlülüğü

5651 sayılı Kanun Ek m. 4/6 uyarınca Türkiye’deki günlük erişimi *bir milyondan fazla* olan tüm sosyal ağ sağlayıcılar, Türkiye’deki kullanıcıların verilerini Türkiye’de barındırma yönünde gerekli tedbirleri almak zorundadır. Kanun hükmünde bu verilerin Türkiye’de ne şekilde barındırılacağı yönünde bir belirleme yapılmamıştır. Bu kapsamda sosyal ağ sağlayıcı, Türkiye’de yerleşik bir yer sağlayıcının bir veri merkezini kullanabileceği gibi kendi veri merkezini kurarak kullanıcı verilerini Türkiye’de barındırabilecektir. Bu yükümlülüğe uymayan sosyal ağ sağlayıcıya BTK Başkanı tarafından bir önceki takvim yılındaki küresel cirosunun %3’üne kadar idari para cezası verilebilecektir.

Kullanıcıların hangi verilerinin Türkiye’de barındırılacağı konusunda hükümde bir açıklık olmasa da Sosyal Ağ Sağlayıcı Hakkında Usul ve Esaslar m. 13/2’de BTK tarafından bir belirleme yapılmıştır. Buna göre temel kullanıcı bilgileri ile BTK tarafından bildirilebilecek hususlara ilişkin veriler barındırılacak veriler bakımından öncelikli kabul edilmiştir. Bu doğrultuda bu veriler, en azından kullanıcının ilgili sosyal medya hesabındaki içerikleri ve bunlara ilişkin trafik bilgileri olacaktır.

Öğretide bir görüşe göre kullanıcı verilerinin Türkiye’de barındırılması yükümlülüğünün öngörülmüş olmasının, bu verilerin KVKK m. 9 uyarınca yurt dışına aktarılamayacağı anlamına gelmediğini ifade etmektedir⁷⁸. Zira bu yükümlülük, kullanıcı verilerini Türkiye’de barındırma yönünde “gerekli tedbirleri alması” olarak ihdas edilmiştir. *Öğretideki diğer bir görüşe göre ise* 5651 sayılı Kanun Ek m. 4’teki bu hükmün KVKK m. 9’daki ilkelerden ayrıldığını ve sosyal ağ sağlayıcının kullanıcı verilerini yurt dışında saklamasını ve dolayısıyla yurt dışına aktarmasını yasakladığını ifade etmektedir⁷⁹.

⁷⁸ AKKURT, *Sosyal Medyada Gerçekleşen İhlaller Karşısında Kişilik Hakkının Korunması*, 205.

⁷⁹ ÖZTEKİN, *Teori ve Uygulamada Türk İnternet Hukuku*, 316.

Tüm sosyal ağ sağlayıcılar için diğer bir yükümlölük ise 5651 sayılı Kanun Ek m. 4/13'te kullanıcı haklarına ilişkin düzenlemelere uyma olarak belirlenmiştir. Bu yükümlölüğe uymayan sosyal ağ sağlayıcıya BTK Başkanı tarafından bir önceki takvim yılındaki küresel cirosunun %3'üne kadar idari para cezası verilebilecektir.

Hükümde kullanıcı haklarından kastın ne olduđu belirtilmemiş ise de Sosyal Ağ Sağlayıcı Hakkında Usul ve Esaslar m. 15'te kullanıcı hakları ele alınmıştır. Buna göre sosyal ağ sağlayıcı, kullanıcılar arasında tarafsız ve eşit davranmakla yükümlü kılınmıştır. İkinci olarak sosyal ağ sağlayıcı, kullanıcılara önerdiği içeriklere ilişkin tercihleri güncelleme ve kişisel verilerinin kullanılmasını sınırlandırma seçeneđi sunacaktır.

Üçüncü olarak Türkiye'den erişen kullanıcıları doğrudan veya dolaylı biçimde etkileyen kullanıcı hesaplarına ilişkin önemli güvenlik ihlallerinin tespitinden itibaren en geç yetmiş iki saat içerisinde bu durum hakkında BTK ve kullanıcılar Türkçe dilinde açık ve anlaşılır şekilde bilgilendirilmelidir. Dördüncü olarak sosyal ağ sağlayıcı, sunduđu hizmetlerde kullanıcı haklarına etki eden güncellemelere kullanıcıların kolayca ulaşabilmesini temin etmelidir.

Beşinci olarak sosyal ağ sağlayıcı, kullanıcılara öneriler sunarken hangi parametreleri kullandığına internet sitesinde açık, anlaşılır ve kolaylıkla ulaşılabilir şekilde yer vermek zorundadır. Ayrıca sosyal ağ sağlayıcı, ele geçirilen veya başkasını taklit eden hesaplara yönelik Türkçe, açık, anlaşılır ve kolaylıkla ulaşılabilir bir başvuru mekanizması kurmakla ve başvuruları makul süre içinde sonuçlandırmakla yükümlüdür.

Sosyal Ağ Sağlayıcı Hakkında Usul ve Esaslar m. 15'te sayılan bu haklar, *numerus clausus*, tahdidi deđil, tadadi olarak sayılmıştır. Zira anılan hükmün son fıkrasında sosyal ağ sağlayıcıların BTK tarafından kullanıcı haklarına ilişkin yapılacak diğer düzenlemelere de uymakla yükümlü olduđu ifade edilmiştir.

g) Çocuklara Özgü Ayırıştırılmış Hizmet Sunma Yükümlülüğü

5651 sayılı Kanun Ek m. 4/7'ye göre tüm sosyal ağ sağlayıcılar, çocuklara özgü ayırıştırılmış hizmet sunma yükümlülüğüne tabi tutulmuştur. Bu yükümlülüğe uymayan sosyal ağ sağlayıcıya BTK Başkanı tarafından bir önceki takvim yılındaki küresel cirosunun %3'üne kadar idari para cezası verilebilecektir.

Kanun hükmünde çocuklara özgü hizmetin ne olduğu açıklanmamıştır. Ancak Sosyal Ağ Sağlayıcı Hakkında Usul ve Esaslar m. 14'te buna ilişkin bir belirlemede bulunulmuştur. Anılan hükmün ikinci fıkrasına göre sosyal ağ sağlayıcı, çocuk olduğu anlaşılabilen⁸⁰ kullanıcılara içerik, reklam ve diğer hizmetlerde şu hususları dikkate almalıdır:

- a) Çocuğun yaşı,
- b) Çocuğun üstün yararının gözetilmesi,
- c) Çocuğun fiziksel, psikolojik ve duygusal gelişiminin korunması,
- ç) Çocuğa yönelik cinsel istismar ve ticari sömürü risklerinin önlenmesi,
- d) Çocuğa ait kişisel verilerin korunmasında yüksek düzeyde gizlilik ayarları ile asgari düzeyde veri işlenmesinin sağlanması,
- e) Sözleşme, kullanıcı ayarları ve veri politikaları gibi hususların çocuğun anlayabileceği şekilde sunulması.

h) Etkin Başvuru Mekanizması Kurma ve Kriz Planı Oluşturma ve Bildirme Yükümlülüğü

5651 sayılı Kanun Ek m. 4/15'e göre sosyal ağ sağlayıcı, başlık etiketleri ve öne çıkarılan içeriklerin uyarı yöntemiyle kaldırılması için BTK ile iş birliği içinde etkin bir başvuru mekanizması kurmakla yükümlüdür. Sosyal Ağ Sağlayıcı

⁸⁰ Kullanıcının çocuk olup olmadığının nasıl belirleneceğine ilişkin ne 5651 sayılı Kanun'da ne de Sosyal Ağ Sağlayıcı Hakkında Usul ve Esaslar'da bir açıklama vardır. Buna ilişkin belirleme sosyal ağ sağlayıcının seçeceği yönteme bırakılmıştır. Kanaatimizce kanun koyucu bu konuda kıstaslar belirlemesi hukuki güvence ve belirliliğin sağlanabilmesi için daha isabetli olacaktır.

Hakkında Usul ve Esaslar m. 16/2 uyarınca sosyal ağ sağlayıcı, başlık etiketleri ve öne çıkarılan içeriklerin uyarı yöntemiyle kaldırılması için kurduğu mekanizmalar hakkında raporlama dönemlerinde BTK'ya bilgi vermek zorundadır.

Sosyal ağ sağlayıcı, başlık etiketleri veya öne çıkarılan içerikler aracılığıyla ortam sağladığı başkasına ait yayın yoluyla işlenen suçtan, kendisine hukuka aykırı içeriğin bildirilmiş ve buna rağmen içeriğin bildiriminden itibaren derhal ve en geç dört saat içinde kaldırılmamış olması durumunda söz konusu içerikten doğrudan sorumlu tutulmuştur.

Sosyal ağ sağlayıcı, 5651 sayılı Kanun Ek m. 4/19'a göre kamu güvenliğini ve kamu sağlığını etkileyen olağanüstü durumlara ilişkin kriz planı oluşturmakla ve BTK'ya bildirmekle yükümlüdür. Bu yükümlülüğe uymayan sosyal ağ sağlayıcıya BTK Başkanı tarafından bir önceki takvim yılındaki küresel cirosunun %3'üne kadar idari para cezası verilebilecektir.

Kamu güvenliği ve kamu sağlığı gibi muğlak ifadeler yanında kriz planına ilişkin diğer hususlar kanun koyucu tarafından açıklanmadığı gibi BTK tarafından yayınlanan Sosyal Ağ Sağlayıcı Hakkında Usul ve Esaslar m. 19'da da bu husus açıklığa kavuşturulmamıştır. Anılan BTK kararında sadece kriz planı oluşturulması ve BTK'ya bildirilmesine ilişkin hususlar BTK tarafından belirlenerek sosyal ağ sağlayıcıya bildirilebileceği ifade edilmiştir. Sosyal ağ sağlayıcı tarafından küresel cirosunun %3'ü gibi bir cezayla karşı karşıya kaldığı bu hususun kanun koyucu tarafından belirlenmesi daha isabetli olacaktır.

II) YAPAY ZEKÂ

21. yüzyılda insanlık, geldiği nokta itibariyle bir yapay zekâ (*Artificial Intelligence-AI*) tartışması içerisine girmiştir. Yapay zekâ, insanlığı köleleştirmekten başlayan distopyalardan insanlığın hizmetinde hayatı kolaylaştıracağı söylenen ütopyalara kadar geniş bir tartışma konusu olmuştur. Bu bölümde bilim-kurgu bir senaryo çizilmesinden ziyade yapay zekânın kavramsal olarak ele alınarak anlamının ortaya konulması önem arz etmektedir. Ardından,

kısaca yapay zekânın bugüne kadar hangi evrelerden geçtiği belirtildikten sonra alt dallarından bahsedilmiştir. Sonrasında yapay zekâ türlerine değinilmiş ve hukuki niteliği konusunda doktrindeki görüşlere yer verilmesinin faydalı olacağı değerlendirilmiştir.

A. KAVRAMSAL ÇERÇEVE VE TANIM

Yapay Zekâ kavramı ilk olarak 1955'te Dartmouth Araştırma Projesi için hazırlanan öneride John McCarthy, Marvin L. Minsky, Nathaniel Rochester ve Claude E. Shannon tarafından zikredilmiştir⁸¹. Bu kavram Türkiye'de 1959'da Ord. Prof. Dr. Cahit Arf tarafından Erzurum'daki bir konferans vesilesi ile ilk kez anılmıştır⁸².

İngilizce *artificial intelligence* (AI) kelimesinden Türkçeye çevrilen yapay zekânın kavramsal sınırının netleştirilmesi hukuki açıdan yapılacak tanım ve tasniflerde önem arz etmektedir. *Artificial* kelimesi Türkçeye genel olarak “yapay, suni, taklit, sahte, yalan”, *intelligence* ise “akıl, zekâ, idrak, anlama, istihbarat” olarak çevrilmektedir⁸³.

Güncel TDK Sözlüğünde yapay kelimesi “doğadaki örneklerine benzetilerek insan eliyle yapılmış veya üretilmiş, yapma, suni, doğal karşıtı, yapmacık”, zekâ kelimesi “İnsanın düşünme, akıl yürütme, objektif gerçekleri algılama, yargılama ve sonuç çıkarma yeteneklerinin tamamı, anlayış, dirayet, zeyreklik, feraset”, yapay zekâ ise “Bir bilgisayarın, bilgisayar kontrolündeki bir robotun veya programlanabilir bir aygıtın insana benzer biçimde algılama, öğrenme, fikir yürütme, karar verme, sorun çözme, iletişim kurma

⁸¹ John MCCARTHY vd., “A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence”, *AI Magazine* 27, sy 4 (2006): 12-14, <https://ojs.aaai.org/index.php/aimagazine/article/view/1904/1802>.

⁸² Cahit ARF, “Makine Düşünebilir Mi ve Nasıl Düşünebilir?”, *Atatürk Üniversitesi - Üniversite Çalışmalarını Muhite Yayıma ve Halk Eğitimi Yayınları Konferanslar Serisi No: 1*, Atatürk Üniversitesi, 1959, 91-103, <https://www.mbkaya.com/hukuk/cahit-arf-makine-dusunebilir-mi-orjinal.pdf>.

⁸³ <https://tureng.com/tr/turkce-ingilizce> (Son Erişim Tarihi: 06.12.2022). Bu çevrimiçi çeviri sitesine göre *artificial intelligence* “yapay zekâ, yapay us, yapay anlayış” anlamına gelmektedir.

vb. işlevleri sergileyebilme yeteneği” olarak tanımlanmaktadır⁸⁴. Kullanımı sık olan İngilizce sözlüklerden olan Cambridge Dictionary’de ise yapay zekânın bizatihi tanımı yapılmıştır. Buna göre yapay zekâ “daha önce insan zekâsına ihtiyaç duyan işleri yapan bilgisayar sistemlerinin geliştirilmesi ve bu sistemlerin bağlı olduğu disiplin”⁸⁵ olarak tanımlanmıştır.

İnceleme konumuz açısından *artificial* kelimesi daha derin anlamlara sahip olduğundan kanaatimizce sanal zekâ⁸⁶ olarak çevrilmesi isabetli olacaktır. Ancak bilindiği üzere meşhur bir galatı terk etmek kolay olmadığı için bu çalışmada da “yapay zekâ” terimi kullanılacaktır.

Yapay zekânın kavramsal çerçevesinin çizilmesi açısından “akıl” kelimesine de değinmek gerekir. Güncel Türkçe Sözlükte akıl kelimesi “Düşünme, anlama ve kavrama gücü, us, öğüt, salık verilen yol, düşünce, kanı, bellek”⁸⁷ olarak tanımlanmaktadır. Zekâ insan olmanın gereği olarak her insanda var olan bir durumdur. Ancak akıl, genetik yollar dışında içinde bulunan çevre koşullarından da etkilenmekte ve gelişimini sürdürmektedir. Dolayısıyla akıl sabit bir şekilde ilerlememekte, zaman zaman yavaşlayıp hızlanabilmektedir⁸⁸. Zekâ ise insanın durumlar ve/veya nesneler arasındaki ilişkiyi anlayabilme, sonuç çıkarabilme, yargılama vb. yeteneklerinin tümüdür. Yapay zekâda mevcut teknolojik imkânlarla insan zekâsı modellenenilirken akıl durağan olmaması nedeniyle modellenememektedir.

⁸⁴ <https://sozluk.gov.tr/> (Son Erişim Tarihi: 06.12.2022).

⁸⁵ <https://dictionary.cambridge.org/dictionary/english-turkish/artificial-intelligence> (Son Erişim Tarihi: 06.12.2022). Bu tanımın hukuki bir değerlendirme için son derece geniş olduğu yönünde bkz. Osman Gazi GÜÇLÜTÜRK, *Yapay Zekâ ve Verinin Kullanımı*, 1. Baskı (On İki Levha Yayıncılık, 2022), 36.

⁸⁶ Büşra KAYNAK BALTA, *Fikir ve Sanat Eserleri Kanunu Kapsamında Eser Kavramı ve Yapay Zeka Ürünleri*, 1. Baskı (Seçkin Yayıncılık, 2021), 65-66. Yazar, yapay zekâ yerine “yaratılmış zekâ” kavramını öneren görüşten bahsetmektedir. Ayrıca biyolojik zekâ ile yapay zekâ karşılaştırması da yapmaktadır.

⁸⁷ <https://sozluk.gov.tr/> (Son Erişim Tarihi: 06.12.2022).

⁸⁸ KAYNAK BALTA, *Fikir ve Sanat Eserleri Kanunu Kapsamında Eser Kavramı ve Yapay Zeka Ürünleri*, 62.

Teknoloji insan beyninden farklı olarak doğrusal değil, üssel anlamda bir gelişme sağlamak ve her geçen gün makine öğrenmesi (*machine learning*)⁸⁹ ve derin öğrenme (*deep learning*)⁹⁰ yoluyla yapay zekâ da gelişmektedir. Gelişen yapay zekâ insanla etkileşime girerek hayatı da etkilemektedir. Bu değişim ve gelişim, yapay zekânın kapsayıcı bir tanımının yapılmasında zorluklar çıkarmaktadır⁹¹. Bu doğrultuda yapay zekâ kavramına yönelik yapılan bazı tanımlar^{92, 93} şöyledir:

*“[Yapay zekâ] en genel haliyle, bir bilgisayarın veya bilgisayar kontrolündeki bir robotun çeşitli faaliyetleri zeki canlılara benzer şekilde yerine getirme kabiliyeti[dir].”*⁹⁴

*“Yapay zekâ, insanların doğal olarak sahip oldukları zekâ ile çözdükleri problemleri çözme becerisine sahip makinedir.”*⁹⁵

*“İnsan zekâsı ile gerçekleştirilen düşünme, anlama, kavrama, yorumlama ve öğrenme işlemlerini bilgisayar programları aracılığıyla problem çözümüne uygulanması[dır].”*⁹⁶

“İnsanın doğal olarak sahip olduğu zekâ ile problemleri çözme, veriler üzerinden anlam çıkarma, çıkardığı anlam doğrultusunda karar verme ve gerektiğinde harekete

⁸⁹ Ayrıntılı bilgi için bkz. II), C. Yapay Zekânın Alt Dalları.

⁹⁰ Ayrıntılı bilgi için bkz. II), C. Yapay Zekânın Alt Dalları.

⁹¹ Ayrıntılı bilgi için bkz. Erdem DOĞAN, *Yapay Zekanın Hukuki Statüsü ve Sorumluluğu*, 1. Baskı (Seçkin Yayıncılık, 2022), 20; Andreas M. KAPLAN ve Michael HAENLEIN, “Rulers of The World, unite! The Challenges and Opportunities of Artificial Intelligence”, *Business Horizons* 63, sy 1 (2020): 3, <https://doi.org/10.1016/j.bushor.2019.09.003>.

⁹² Doktrindeki tanımlamaların “insan merkezli” ve “rasyonel” olmak üzere iki temel yaklaşım üzerinden şekillendiği görüşü için bkz. DOĞAN, *Yapay Zekanın Hukuki Statüsü ve Sorumluluğu*, 21-22.

⁹³ Avrupa Parlamentosu ve Avrupa Konseyi nezdinde yapay zekânın tanımlanmasına ilişkin açıklamalar için bkz. GÜÇLÜTÜRK, *Yapay Zekâ ve Verinin Kullanımı*, 37-40.

⁹⁴ T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, *Ulusal Yapay Zekâ Stratejisi 2021-2025* (24.08.2021), <https://www.cbddo.gov.tr/UYZS> (Son Erişim Tarihi: 06.12.2022). Köşeli parantez içi açıklamalar tarafımızca eklenmiştir.

⁹⁵ Armağan Ebru BOZKURT YÜKSEL, *Yapay Zekâ, Endüstri 4.0 ve Robot Üreticiler Hukuki Bakış*, 1. Baskı (Aristo Yayınevi, 2019), 50.

⁹⁶ Pınar BACAŞIZ ve Seda Yağmur SÜMER, *Robotlar, Yapay Zeka ve Ceza Hukuku*, 1. Baskı (Adalet Yayınevi, 2021), 22. Köşeli parantez içi açıklamalar tarafımızca eklenmiştir.

geçme, öğrenme, deneyimlerden yararlanma gibi zihinsel süreçleri bir donanıma gerek duymaksızın gerçekleştirebilen, insan zekâsını taklit eden ve topladıkları bilgilerle yinelemeli olarak kendi kendini iyileştirebilen yazılımlardır.”⁹⁷

Kanaatimizce Bozkurt Yüksel’in tanımına katılmak mümkün değildir. Çünkü yapay zekâ bir makine değildir. Ekici’nin de bahsettiği üzere yapay zekâ fiziksel varlığa ihtiyaç duymamaktadır. Elbette yapay zekâyâ bir makineye yerleştirilerek fiziki varlık verilebilir. Ancak bu durumda yapay zekâ makine ile eş değer olamaz, makineye hayat veren bir yazılım olabilir⁹⁸. Bu doğrultuda Ekici’nin yapay zekâ tanımına katılmakla birlikte yapay zekâ olgusunun⁹⁹ alt dallarıyla birlikte düşünülmesi gerektiği kanaatindeyiz.

B. YAPAY ZEKÂNIN TARİHİ

Yapay zekânın tarihine ilişkin Antik Yunan düşünürlerinin eserlerinde yapay zekâyâ ilişkin işaretlerde bulunduğu ifade edilmektedir¹⁰⁰. Ayrıca yapay zekâ çeşitli roman ve öykülere de konu olmuştur. Bunlardan en çok bilineni Isaac Asimov’un *I Robot (Ben Robot)* isimli 9 öyküden oluşan romanıdır. Asimov, romanında 3 Robot Yasası ile yapay zekâyı mantıksal çerçevede ele almıştır. Bu yasalar sonradan çıkan bazı eserlerde yer bulmuş ve geliştirilmiştir¹⁰¹.

⁹⁷ EKİCİ, *Bilişim ve Teknoloji Hukuku*, 186.

⁹⁸ Yapay zekâ ve robot arasındaki fark için ayrıca bkz. Armağan Ebru BOZKURT YÜKSEL, *Buluşçu Yapay Zekâ ve Patent Hukuku*, 1. Baskı (Aristo Yayınevi, 2020), 16-19.

⁹⁹ Yapay zekâyı bir disiplin, bir bilim dalı olarak tanımlayan çalışmalar için bkz. Hitoshi NASU, “Artificial Intelligence and the Obligation to Respect and to Ensure Respect for IHL”, içinde *Ensuring Respect for International Humanitarian Law*, ed. Eve MASSINGHAM ve Annabel MCCONNACHIE (Taylor & Francis Group, 2020), 177; Enliang YAN vd., “Comparison of Support Vector Machine, Back Propagation Neural Network and Extreme Learning Machine for Syndrome Element Differentiation”, *Artificial Intelligence Review* 53, sy 4 (2020): 2454, <https://doi.org/10.1007/s10462-019-09738-z>.

¹⁰⁰ EKİCİ, *Bilişim ve Teknoloji Hukuku*, 188-89; BACAKSIZ ve SÜMER, *Robotlar, Yapay Zeka ve Ceza Hukuku*, 35.

¹⁰¹ BACAKSIZ ve SÜMER, *Robotlar, Yapay Zeka ve Ceza Hukuku*, 35-37; EKİCİ, *Bilişim ve Teknoloji Hukuku*, 190.

20. yüzyılın ikinci yarısı geride bırakıldığında ise Alan Turing, *Turing Testi* olarak bilinen modellemesi ile bir yazılımın yapay zekâ olup olmayacağını yayınladığı bir makalesinde tartışmıştır¹⁰². Bu teste göre bir kişi elektronik ortamda bir iletişim gerçekleştirmekte ve kişi karşısındakinin insan olmadığını fark edemezse yazılımın testi geçtiği ve yapay zekâ olarak nitelenebileceği ifade edilmektedir.

1970’li yıllarda ise yapay zekâ bir duraksama dönemine girmiş, doktrinde bu durum “yapay zekânın kışı” olarak adlandırılmıştır. Bu dönemde oluşturulan uzman sistemler dar bir hareket alanında çalışmaların yürütülmesi ve yüksek beklentiler sebebiyle gelişme gösterememiştir¹⁰³. Bundan sonra araştırmacılar ulaşılabilir hedefler koymaya başlamıştır. Önceki dönemde insan yerine geçecek bir uzman sistem yerine insana yardımcı sistemler geliştirilmeye başlanmış ve yapay zekâ çalışmaları yeniden artmaya başlamıştır¹⁰⁴.

1990’lı yıllara gelindiğinde ise IBM şirketince geliştirilen Deep Blue, dünya satranç şampiyonu G. Kasparov’u yenmiş¹⁰⁵, bu durum yapay zekâ ile ilgili tartışmaları ve çalışmaları da artırmıştır.

2000’li yıllara geldiğimizde artık yapay zekâya sahip teknolojik araçlar hayatımızı çevrelemeye başlamıştır. Roomba isimli ilk ev robotu çıkmış, 2016’da Google Deep Mind şirketinin geliştirdiği AlphaGo, satranç maçında Lee Sedol’u 4-1 yenmiş, 2017’de Hanson Robotics firması tarafından en insansı üretilen robot Sophia söylemleriyle gündem olmuştur. Günümüzde yapay zekâ insansız hava

¹⁰² BACAKSIZ ve SÜMER, *Robotlar, Yapay Zeka ve Ceza Hukuku*, 42-45; KAYNAK BALTA, *Fikir ve Sanat Eserleri Kanunu Kapsamında Eser Kavramı ve Yapay Zeka Ürünleri*, 73-75.

¹⁰³ KAYNAK BALTA, *Fikir ve Sanat Eserleri Kanunu Kapsamında Eser Kavramı ve Yapay Zeka Ürünleri*, 78-79.

¹⁰⁴ KAYNAK BALTA, *Fikir ve Sanat Eserleri Kanunu Kapsamında Eser Kavramı ve Yapay Zeka Ürünleri*, 79-80.

¹⁰⁵ Kasparov ve Deep Blue arasındaki maçın detayları için bkz. KAYNAK BALTA, *Fikir ve Sanat Eserleri Kanunu Kapsamında Eser Kavramı ve Yapay Zeka Ürünleri*, 80-81.

araçlarından insansı robotlara kadar hayatın her alanına dokunmaya devam etmektedir.

C. YAPAY ZEKÂNIN ALT DALLARI

Yapay zekânın alt dalları aslında henüz netleşmemiş, bir anda dallanıp budaklandığı gibi bir anda iki-üç alt disipline bölündüğü olmuştur. Kanaatimizce yapay zekâ temelde makine öğrenmesi (*machine learning*), derin öğrenme (*deep learning*), doğal dil işleme (*natural language processing*) ve veri biliminden (*data science*) müteşekkildir. Ancak aşağıda da değinileceği üzere derin öğrenme, makine öğrenmesinin alt birimi olarak da kabul edilebilmektedir. Bu başlık altında teknik ayrıntılarına girmeden sadece alt dalların tanımı yapılacaktır.

Makine öğrenmesi, işlem performansını artırmak ve daha isabetli sonuçlara ulaşmak için kullanılan tüm hesaplama metotlarını içeren bir kavramdır¹⁰⁶. Yani, makine öğrenmesi mevcut verilerdeki bağlantıları saptar ve yeni bir veri ile karşılaştığında geçmiş verilerden hareketle benzer sonuçlara ulaşabilen bir modeldir¹⁰⁷. Makine öğrenmesi de kendi içerisinde üçlü bir tasnife tabi tutulmaktadır: denetimli (gözetimli) öğrenme, denetimsiz (gözetimsiz) öğrenme ve yarı denetimli (pekiştirmeli) öğrenme¹⁰⁸.

Derin öğrenme, “normalde tek katmanda gerçekleştirilen öğrenme sürecinin insan beyninden ilham alınarak paralel olarak çalıştırılan bağlantılı birimlerin bulunduğu çok sayıda katman aracılığıyla gerçekleştirildiği özel bir makine öğrenmesi sürecini ifade etmektedir.”¹⁰⁹ İnsan beyninde veri alışverişini, iletişimi sağlayan nöronlar bulunur. Böylelikle insanlar veriler arasında bağlantı kurup anlamlı sonuçlar çıkarabilmektedir. Derin öğrenmede de buna benzer olarak yapay sinir ağları (*neural network*) bulunur. Yapay sinir ağları, yapay zekâ

¹⁰⁶ GÜÇLÜTÜRK, *Yapay Zekâ ve Verinin Kullanımı*, 57.

¹⁰⁷ Ayrıca makine öğrenmesinin aşamaları için bkz. GÜÇLÜTÜRK, *Yapay Zekâ ve Verinin Kullanımı*, 58.

¹⁰⁸ Ayrıntılı bilgi için bkz. GÜÇLÜTÜRK, *Yapay Zekâ ve Verinin Kullanımı*, 60-72.

¹⁰⁹ GÜÇLÜTÜRK, *Yapay Zekâ ve Verinin Kullanımı*, 72.

sistemlerinin çalışmasına olanak sağlar. Bu yapılar ile insan beyni taklit edilerek veriler arası bağlantı kurulmakta ve bazı sonuçlar çıkarılmaktadır. Bu sebeple makine öğrenmesinden farklı olarak derin öğrenmede daha fazla veriye ihtiyaç duyulmaktadır.¹¹⁰

Yukarıda yapay zekânın alt dalları sıralanırken makine öğrenmesi ile derin öğrenmenin birbirinden ayrıldığı belirtilmişti. Yapay sinir ağları sebebiyle derin öğrenme bir makine öğrenmesi süreci izlemekle birlikte bu alt daldan ayrılmaktadır¹¹¹.

Doğal dil işleme, insanlar tarafından konuşulan doğal dillerin analiz edilmesi, çözümlenmesidir¹¹² ve makine öğrenmesi ile derin öğrenme ile sıkı bir ilişkisi vardır. *Siri*, *Google Asistan* doğal dil işlemenin örnekleridir.

Veri Bilimi, yapılandırılmış veyahut yapılandırılmamış verilerden bir öngörü veya bilgi elde etmek için algoritma¹¹³, bilimsel yöntem kullanan bir disiplindir. Bu disiplin sayesinde devasa veri kümeleri (*big data-büyük veri*)¹¹⁴ üzerinde metin/veri madenciliği (*text/data mining*)¹¹⁵ yapılmakta ve makine öğrenmesi burada aktif rol almaktadır.

¹¹⁰ BACAŞIZ ve SÜMER, *Robotlar, Yapay Zeka ve Ceza Hukuku*, 24-25.

¹¹¹ Aksi yönde: DOĞAN, *Yapay Zekanın Hukuki Statüsü ve Sorumluluğu*, 50. Yazar tıpkı Güçlütürk gibi derin öğrenmenin makine öğrenmesinin bir alt dalı olduğunu ifade etmektedir.

¹¹² Ecem AKSOY, *Yapay Zeka'nın Sorumluluk Hukukundaki Konumu Ve Büyük Veri İle İlişkisi*, 1. Baskı (Seçkin Yayıncılık, 2022), 59.

¹¹³ Programın bir problemi çözmek için izleyeceği yöntem, metod olarak tanımlanabilir. Ayrıntılı bilgi için bkz. GÜÇLÜTÜRK, *Yapay Zekâ ve Verinin Kullanımı*, 23-25.

¹¹⁴ Ayrıntılı bilgi için bkz. Nathalie JAPKOWICZ ve Jerzy STEFANOWSKI, "A Machine Learning Perspective on Big Data Analysis", içinde *Big Data Analysis: New Algorithms for a New Society*, ed. Nathalie JAPKOWICZ ve Jerzy STEFANOWSKI, c. 16, *Studies in Big Data* (Springer International Publishing, 2016), https://doi.org/10.1007/978-3-319-26989-4_1.

¹¹⁵ Ayrıntılı bilgi için bkz. Eric PAQUET vd., "Data Mining in Finance: Current Advances and Future Challenges", içinde *Big Data Analysis: New Algorithms for a New Society*, ed. Nathalie JAPKOWICZ ve Jerzy STEFANOWSKI, c. 16, *Studies in Big Data* (Springer International Publishing, 2016), https://doi.org/10.1007/978-3-319-26989-4_7.



Şema 3: Yapay Zekânın Alt Dalları

D. YAPAY ZEKÂ TÜRLERİ

Yapay zekâ sınıflandırılırken çeşitli kıstaslar esas alınmaktadır. Bunlardan bazıları gelişmişlik düzeyi, insan özelliklerini taklit etme kapasitesi, günlük hayata etki eden uygulamaları ve kullanılan teknolojidir¹¹⁶. Doktrinde yapay zekâ çeşitli tasniflere de tabi tutulmaktadır. Doktrindeki bir tasnife göre dar/zayıf yapay zekâ (*narrow/weak AI*), genel/güçlü yapay zekâ (*general/strong AI*) ve süper yapay zekâ (*super AI*) olarak sınıflandırılırken diğer bir ayrıma göre tepki veren/reaktif yapay zekâ (*reactive AI*), sınırlı hafızalı yapay zekâ (*limited memory AI*), zihin teorisi düzeyinde yapay zekâ (*theory of mind AI*) ve bilinçli yapay zekâ (*self-aware AI*) olarak türlere ayrılmaktadır:

1. Gelişmişlik Düzeyine Göre Ayrım

Bu ayrıma göre yapay zekânın bir türü olan dar/zayıf yapay zekâ, daha önce belirlenmiş kurallar çerçevesinde ve belirli bir hareket alanı içerisinde önceden planlanmış işlemleri yapan bir türdür¹¹⁷. Bu türe *Google Asistan*, *Siri*,

¹¹⁶ DOĞAN, *Yapay Zekanın Hukuki Statüsü ve Sorumluluğu*, 30-31.

¹¹⁷ Hasan Kadir YILMAZTEKİN, *Yapay Zekanın Eser Sahipliği*, 1. Baskı (Adalet Yayınevi, 2021), 61; BOZKURT YÜKSEL, *Buluşçu Yapay Zekâ ve Patent Hukuku*, 13; Armağan Ebru BOZKURT YÜKSEL ve Başak BAK, "Yapay Zekâ", içinde *Futurist Hukuk*, 1. Baskı (Aristo Yayınevi, 2018), 9; BOZKURT YÜKSEL, *Yapay Zekâ, Endüstri 4.0 ve Robot Üreticiler Hukuki Bakış*, 53; AKSOY, *Yapay Zeka'nın Sorumluluk Hukukundaki Konumu Ve Büyük Veri İle İlişkisi*, 50-51; Nesrin SİNGİL,

Bixby, Alexa, Deep Blue, AlphaGo örnek olarak gösterilebilir. Genel/güçlü yapay zekâ, insan beynini taklit ederek dar yapay zekâyâ nispeten sınırsız sayıda hedef için çalışan bir türdür¹¹⁸. Bu tür uygulamaya geçmiş, örneklerini gördüğümüz bir tür değildir. Genel yapay zekâ tam anlamıyla hayata geçirilebilirse istihdamda ve insanın başat özne olduğu çoğu uğraşta insanı ikâme edebilir. Çünkü bu tür insan gibi düşünme, veriler arasında ilişki kurup gerektiğinde sonuç çıkarma ve yargılama yeteneğine sahip olabilecektir.

Süper yapay zekâ ise insanı aşan görev ve hedefleri belirleyip gerçekleştirebilen bir modeldir¹¹⁹. Elon Musk bu tür yapay zekâ için “insanlık için muazzam bir varoluşsal tehdit”¹²⁰ nitelemesini yapmaktadır. Bu tür yapay zekânın hayata geçmesiyle birlikte “Trans Human Çağı”nın başlayacağı, *singularity (teknolojik tekillik) akımı* tarafından savunulmaktadır¹²¹.

2. Fonksiyonlarına (İşlevlerine) Göre Ayrım

Bu ayrıma bakıldığında aslında dar ve geniş yapay zekânın iki alt ayrıma tabi tutularak detaylandırıldığını söylemek mümkündür¹²². Dar yapay zekânın buradaki birinci görünümü ise tepki veren/reaktif yapay zekâdır. Bu tür yapay zekâ sadece çevreyi algılar ve gördükleri üzerine tepki verir. Yani, bu türün

“Yapay Zekâ ve İnsan Hakları”, *Public and Private International Law Bulletin* 42, sy 1 (2022): 127, <https://10.26650/ppil.2022.42.1.970856>; DOĞAN, *Yapay Zekanın Hukuki Statüsü ve Sorumluluğu*, 31-33.

¹¹⁸ DOĞAN, *Yapay Zekanın Hukuki Statüsü ve Sorumluluğu*, 33-35; BOZKURT YÜKSEL, *Buluşçu Yapay Zekâ ve Patent Hukuku*, 13; BOZKURT YÜKSEL ve BAK, “Yapay Zekâ”, 9; BOZKURT YÜKSEL, *Yapay Zekâ, Endüstri 4.0 ve Robot Üreticiler Hukuki Bakış*, 53; SİNGİL, “Yapay Zekâ ve İnsan Hakları”, 127; YILMAZTEKİN, *Yapay Zekanın Eser Sahipliği*, 61; AKSOY, *Yapay Zeka’nın Sorumluluk Hukukundaki Konumu Ve Büyük Veri İle İlişkisi*, 51-53.

¹¹⁹ YILMAZTEKİN, *Yapay Zekanın Eser Sahipliği*, 61; SİNGİL, “Yapay Zekâ ve İnsan Hakları”, 127; DOĞAN, *Yapay Zekanın Hukuki Statüsü ve Sorumluluğu*, 35; BACAŞIZ ve SÜMER, *Robotlar, Yapay Zeka ve Ceza Hukuku*, 27.

¹²⁰ SİNGİL, “Yapay Zekâ ve İnsan Hakları”, 125.

¹²¹ Ayrıntılı bilgi için bkz. DOĞAN, *Yapay Zekanın Hukuki Statüsü ve Sorumluluğu*, 36-37; süper yapay zekânın biçimleri için bkz. BACAŞIZ ve SÜMER, *Robotlar, Yapay Zeka ve Ceza Hukuku*, 28-29; BOZKURT YÜKSEL, *Yapay Zekâ, Endüstri 4.0 ve Robot Üreticiler Hukuki Bakış*, 55.

¹²² BOZKURT YÜKSEL, *Yapay Zekâ, Endüstri 4.0 ve Robot Üreticiler Hukuki Bakış*, 53.

uzmanlığı tek bir alanla sınırlanmıştır¹²³. *AlphaGo* ve *Deep Blue* örnek olarak verilebilir. Dar yapay zekânın ikinci görünümü ise sınırlı hafızalı yapay zekâdır. Bu tür yapay zekâ, sınırlı bir belleğe sahiptir ve güncel veriler hakkında bu geçmiş tecrübelerine göre karar verir¹²⁴. Bu türe Amazon'a ait *Alexa* ve Apple'a ait *Siri* örnek gösterilebilir.

Dar yapay zekâda olduğu gibi genel yapay zekânın da burada iki görünümü mevcuttur. Bunlardan ilki zihin teorisi düzeyinde yapay zekâdır. Bu tür yapay zekâ, insan düşüncelerini ve bu düşünceleri etkileyen etmenleri algılayabilir ve insanlarla sosyal etkileşim kurabilir. Ayrıca her an öğrenme yeteneğine sahiptir¹²⁵. Hanson Robotics şirketinin *Sophia* isimli robotu, *Star Wars*'taki *R2-D2* karakteri ve *I Robot* filmindeki *Sonny* örnek olarak gösterilebilir. İkinci görünüm ve ayırmadaki son tür ise bilinçli yapay zekâdır. Bu yapay zekâ türü kendi varlığının farkındadır. Etrafındaki canlı varlıkların duygularını, düşüncelerini öngörebilir¹²⁶. *Ex Machina* filmindeki *Ava* ve *Terminatör* bu türe örnek olarak gösterilebilir.

¹²³ DOĞAN, *Yapay Zekanın Hukuki Statüsü ve Sorumluluğu*, 38; YILMAZTEKİN, *Yapay Zekanın Eser Sahipliği*, 59; BOZKURT YÜKSEL, *Buluşçu Yapay Zekâ ve Patent Hukuku*, 13; BOZKURT YÜKSEL, *Yapay Zekâ, Endüstri 4.0 ve Robot Üreticiler Hukuki Bakış*, 53; BOZKURT YÜKSEL ve BAK, "Yapay Zekâ", 9.

¹²⁴ DOĞAN, *Yapay Zekanın Hukuki Statüsü ve Sorumluluğu*, 38; YILMAZTEKİN, *Yapay Zekanın Eser Sahipliği*, 59; BOZKURT YÜKSEL, *Buluşçu Yapay Zekâ ve Patent Hukuku*, 53; BOZKURT YÜKSEL ve BAK, "Yapay Zekâ", 9.

¹²⁵ DOĞAN, *Yapay Zekanın Hukuki Statüsü ve Sorumluluğu*, 39; YILMAZTEKİN, *Yapay Zekanın Eser Sahipliği*, 60; BOZKURT YÜKSEL, *Buluşçu Yapay Zekâ ve Patent Hukuku*, 14; BOZKURT YÜKSEL, *Yapay Zekâ, Endüstri 4.0 ve Robot Üreticiler Hukuki Bakış*, 54; BOZKURT YÜKSEL ve BAK, "Yapay Zekâ", 10.

¹²⁶ DOĞAN, *Yapay Zekanın Hukuki Statüsü ve Sorumluluğu*, 39-40; YILMAZTEKİN, *Yapay Zekanın Eser Sahipliği*, 60; BOZKURT YÜKSEL, *Buluşçu Yapay Zekâ ve Patent Hukuku*, 14; BOZKURT YÜKSEL, *Yapay Zekâ, Endüstri 4.0 ve Robot Üreticiler Hukuki Bakış*, 54; BOZKURT YÜKSEL ve BAK, "Yapay Zekâ", 10.



Şema 4: Yapay Zekâ Türleri

E. YAPAY ZEKÂNIN HUKUKİ NİTELİĞİ

Yapay zekânın kapsamını belirlemedeki güçlükler hukuki niteliğini belirlemede de karşımıza çıkmaktadır¹²⁷. Çünkü hukuk ezelden beri beşerî bir varlık olan insan davranışlarına bir anlam yüklemiş ve hukuki belirlemelerde bulunmuştur. Yapay zekâyâ ilişkin hukuki nitelik tartışmaları kişilik bağlamında gelişmiş ve birtakım yazarlar yapay zekâyâ hukuki kişilik¹²⁸ tanınmasına gerek olmadığını belirtirken diğer bir grup yazar ise yapay zekâyâ belirli koşullarda kişilik tanınabileceğini ifade etmektedir¹²⁹.

Yapay zekâyâ hukuki manada kişilik tanınmasına gerek olmadığını savunan görüş, insanı diğer bütün varlıklara üstün tuttuğu için yapay zekâyı Roma hukukundaki köle benzeri bir statüye konumlandırmakta¹³⁰ ya da eşya¹³¹

¹²⁷ Ayrıntılı bilgi için bkz. DOĞAN, *Yapay Zekanın Hukuki Statüsü ve Sorumluluğu*, 20; M. KAPLAN ve HAENLEIN, "Rulers of The World, unite! The Challenges and Opportunities of Artificial Intelligence", 3.

¹²⁸ Sosyoloji ve felsefe bağlamında kişilik için bkz. DOĞAN, *Yapay Zekanın Hukuki Statüsü ve Sorumluluğu*, 162-63; Seda KARA KILIÇARSLAN, "Yapay Zekânın Hukuki Statüsü ve Hukuki Kişiliği Üzerine Tartışmalar", *Yıldırım Beyazıt Hukuk Dergisi*, sy 2 (2019): 371, <https://doi.org/10.33432/ybuhukuk.599224>.

¹²⁹ DOĞAN, *Yapay Zekanın Hukuki Statüsü ve Sorumluluğu*, 173 vd.; BACAŞIZ ve SÜMER, *Robotlar, Yapay Zeka ve Ceza Hukuku*, 138 vd.; KARA KILIÇARSLAN, "Yapay Zekânın Hukuki Statüsü ve Hukuki Kişiliği Üzerine Tartışmalar", 377 vd.

¹³⁰ KAYNAK BALTA, *Fikir ve Sanat Eserleri Kanunu Kapsamında Eser Kavramı ve Yapay Zeka Ürünleri*, 106; BACAŞIZ ve SÜMER, *Robotlar, Yapay Zeka ve Ceza Hukuku*, 139; KARA KILIÇARSLAN, "Yapay Zekânın Hukuki Statüsü ve Hukuki Kişiliği Üzerine Tartışmalar", 378.

¹³¹ Sinan Sami AKKURT, "Yapay Zekânın Otonom Davranışlarından Kaynaklanan Hukuki Sorumluluk", *Uyuşmazlık Mahkemesi Dergisi*, sy 13 (2019): 44, <https://doi.org/10.18771/mdergi.581875>.

olarak nitelenmesinin yeterli olacağını kabul etmektedir. Çünkü yapay zekâ nihayetinde bir insan ürünüdür.¹³² Hukuki kişilik tanınmasını reddeden görüşlerin gerekçeleri kişilik vasfı için lazım gelen niteliklere sahip olmaması, insan çıkarlarına aykırı olması, haklara ve borçlara ehil olmaması ve yapay zekâ davranışlarından kaynaklanan sorumluluk için kişiliğin elzem olmaması olarak ifade edilebilir¹³³. Ancak kanaatimizce de karmaşık yapısı olan ve türlerini göz ardı eden bu yaklaşım yapay zekâyı sıradan bir eşya olarak nitelemekte ve yapay zekânın (mesela otonom aracın bir kişiyi öldürmesi gibi) değişiklik yaptığı durumlarda sorumluluk ve hakkaniyet açısından hukuki açmazlara sebebiyet vermektedir¹³⁴.

Yapay zekâyâ hukuki kişilik tanınması gerektiğini söyleyen görüşler de mevcuttur¹³⁵. Bu görüşler kişiliğin hukuki ve şekli tarafını esas almakta ve sosyal uzlaşa ile hukuk politikasına aykırı olmamak koşuluyla yapay zekâyâ sahip varlıkların kişi olarak tanınabileceğini belirtmektedir¹³⁶. Doktrinde yapay zekâyâ kişilik tanınmasını kabul eden görüşlerin 3 esas noktadan hareket ettiği belirtilmektedir: özgün bilişsel nitelikleri dolayısıyla yapay zekânın işleyişinden kaynaklanan zararlarda sorumluluğun belirlenmesinde zorluk çıkması, eşya olarak kabul edilmesinin mümkün olmaması ve sosyal statü verilecek yapay zekâdan insanlığın en üst mertebede yararlanması amacı¹³⁷. Yararlanma açısından şu örneği vermek yerinde olacaktır: ABD’de eyaletlerin tamamına yakını

¹³² DOĞAN, *Yapay Zekanın Hukuki Statüsü ve Sorumluluğu*, 177-78; BACAŞIZ ve SÜMER, *Robotlar, Yapay Zeka ve Ceza Hukuku*, 138-41.

¹³³ İleri sürülen gerekçelere ve teorilere ilişkin ayrıntılı bilgi için bkz. DOĞAN, *Yapay Zekanın Hukuki Statüsü ve Sorumluluğu*, 176-90.

¹³⁴ Aynı görüşte: DOĞAN, *Yapay Zekanın Hukuki Statüsü ve Sorumluluğu*, 178; BACAŞIZ ve SÜMER, *Robotlar, Yapay Zeka ve Ceza Hukuku*, 139-41.

¹³⁵ Kanaatimizce de yapay zekâlı varlıklara kişilik statüsü verilmesi, hukuki güvenlik ve hesap verilebilirlik açısından son derece önem arz etmektedir. Aynı görüşte: DOĞAN, *Yapay Zekanın Hukuki Statüsü ve Sorumluluğu*, 195.

¹³⁶ Hukuki ve şekli kişilik hakkında ayrıntılı bilgi için bkz. DOĞAN, *Yapay Zekanın Hukuki Statüsü ve Sorumluluğu*, 157-62.

¹³⁷ DOĞAN, *Yapay Zekanın Hukuki Statüsü ve Sorumluluğu*, 190-91.

Columbia ve Virgin Adalarınca kabul edilen Tekdüzen Elektronik İşlemler Kanunu (*The Uniform Electronic Transactions Act-UETA*) ile sözleşmenin kurulması aşamasında makinelerin tarafların elektronik temsilcisi olarak sözleşme yapabilmesine cevaz vermektedir. Böylelikle sözleşmenin kurulması için gerekli irade beyanlarının olmadığı iddiaları geçersiz kabul edilmiş olmaktadır¹³⁸.

Burada kısaca yapay zekâ için öngörülen kişilik tiplerine değinmekte yarar vardır. Bunlardan ilki elektronik kişiliktir. Bu hukuki kişilikle kastedilen gerçek kişilerle aynı derece ve kapsamda kişilik değildir. Elektronik kişiliğe sahip bir yapay zekâ sınırlı bir alanda işlem yapabilecektir. Böylelikle otonomi özelliğine sahip bir yapay zekânın işlemlerinden kaynaklanan hukuki sorunlar çözülebilecek ve hukuki güvenlik tehlikeye girmemiş olacaktır. Bu kişilik için 16.02.2017 tarihli Avrupa Parlamentosu tarafından Robotik Alana İlişkin Medeni Hukuk Kurallarına ilişkin ilke kararı [*European Parliament Resolution of 16 February 2017 with Recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL))*]¹³⁹ yayınlanmıştır.

Diğer bir kişilik türü ise tüzel kişilik benzeri kişiliktir. Doğan bu statüyü yapay zekâ için en akılcı ve uygulanabilir yöntemlerden biri olarak ifade etmektedir¹⁴⁰. Çünkü kişi toplulukları da yapay zekâ gibi aynı amaç için kurgulanmıştır. Yani, toplumsal bir gereklilik doğduğu ve sosyal hayatın

¹³⁸ <http://euro.ecom.cmu.edu/program/law/08-732/Transactions/ueta.pdf> (Son Erişim Tarihi: 07.12.2022), DOĞAN, *Yapay Zekanın Hukuki Statüsü ve Sorumluluğu*, 192’den naklen.

¹³⁹ Elektronik kişilik için ayrıca bkz. DOĞAN, *Yapay Zekanın Hukuki Statüsü ve Sorumluluğu*, 197; BACAŞIZ ve SÜMER, *Robotlar, Yapay Zeka ve Ceza Hukuku*, 152-54; KARA KILIÇARSLAN, “Yapay Zekânın Hukuki Statüsü ve Hukuki Kişiliği Üzerine Tartışmalar”, 380; Ayrıntılı bilgi için bkz. EUROPEAN PARLIAMENT, “Resolution of 16 February 2017 with Recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL))”, 2017, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017IP0051> (Son Erişim Tarihi: 07.12.2022).

¹⁴⁰ DOĞAN, *Yapay Zekanın Hukuki Statüsü ve Sorumluluğu*, 200.

desteklenmesi için tasarlanmışlardır. Böylelikle yapay zekâ da tüzel kişiler gibi hak ve fiil ehliyetine sahip olabilecektir¹⁴¹.

Üçüncü olarak yarı kişilik türünden bahsetmek gerekir. Bu kişiliğin hareket noktası, sınırlı ehliyetsizlerdir. Buna göre ayırt etme gücüne sahip küçükler ve kısıtlılar tam ehliyetliler ile tam ehliyetsizler arasında ara bir form olduğu gibi yapay zekâ da aynı şekilde yarı kişiliğe sahip olmalıdır. Şöyle ki 14 yaşındaki bir çocuk ayırt etme gücüne sahip olmakla birlikte ergin olmadığı, icra ettiği fiilin hukuki anlam ve sonuçlarını tam olarak öngöremediği için sınırlanmaktadır. Mevcut koşullarda henüz bilinçli bir yapay zekâ mevcut olmadığı için bu türe konumlandırılarak yapay zekânın bazı işlemler için sınırlandırılması savunulmaktadır¹⁴².

Ayrıca yapay zekâ için insan olmayan kişi/yapay insan statüsü de önerilmiştir. Buna göre insan olmayan varlıklara (tüzel kişiler gibi) hukuki bir statü atfetmek toplumsal hayatın devamı ve sağlığı için faydalı görülmüştür. Her gün hayatımıza biraz daha giren yapay zekâyı da bu gibi faydacı gerekçelerle bu statünün verilebileceği ifade edilmektedir. Bu kişiliğin yukarıda bahsettiğimiz tüzel kişi benzeri kişilikten farkı, yapay zekânın insana ait birtakım özellikleri taklit etse de hiçbir zaman insanla özdeş olamayacağı temeline dayanmasıdır.¹⁴³

Doktrinde yapay zekâ için son öngörülen kişilik statüsü, “entegre kişilik”tir (InPerAI-integrity personality). Bu görüşe göre yapay zekâ, yetenekleri, otonom hareket kapasitesi ve bilişsel kapasitesine göre kategorize edilmekte¹⁴⁴ ve “ana

¹⁴¹ DOĞAN, *Yapay Zekanın Hukuki Statüsü ve Sorumluluğu*, 201-3; BACAŞIZ ve SÜMER, *Robotlar, Yapay Zeka ve Ceza Hukuku*, 146-51; KARA KILIÇARSLAN, “Yapay Zekânın Hukuki Statüsü ve Hukuki Kişiliği Üzerine Tartışmalar”, 379.

¹⁴² DOĞAN, *Yapay Zekanın Hukuki Statüsü ve Sorumluluğu*, 203-4.

¹⁴³ DOĞAN, *Yapay Zekanın Hukuki Statüsü ve Sorumluluğu*, 207-8; BACAŞIZ ve SÜMER, *Robotlar, Yapay Zeka ve Ceza Hukuku*, 154; KARA KILIÇARSLAN, “Yapay Zekânın Hukuki Statüsü ve Hukuki Kişiliği Üzerine Tartışmalar”, 381.

¹⁴⁴ Yazar, her yapay zekâ için bu kişiliği önermemektedir. Bu kişiliğe yapay genel zekâ, yapay süper zekâ, tam otonom yapay zekâ ve kendinin farkında olan yapay zekâ türlerinin bu kişiliğe sahip olması gerektiğini ifade etmektedir. Ayrıntılı bilgi için bkz. Şerafettin EKİCİ, “New Proposed

kişiliğe” (MaPer-*main person*) entegre bir kişiliğe sahip olmaktadır. Burada yapay zekâ bağımsız bir kişiliğe sahip olmayıp entegre olduğu gerçek veya tüzel kişi olan ana kişiliğe bağlıdır. Dolayısıyla InPerAI tarafından gerçekleştirilen eylemlerin sonucu olacak hak, borç ve sorumluluk MaPer tarafından üstlenilecektir¹⁴⁵.

Ekici, entegre kişilik modelini önerirken isabetli olarak önceki başlıkta da incelenen yapay zekâ türlerine göre bir ayırım yapmaktadır. Bu doğrultuda bir yapay zekânın, tam otonom bir yapay zekâ, geniş/güçlü yapay zekâ, zihin teorisi düzeyinde yapay zekâ, süper yapay zekâ olması gerekir. Aksi durumda dar bir yapay zekânın hukuki kişiliğinin tartışılmasının pratik bir önemi bulunmamaktadır¹⁴⁶. Dolayısıyla yapay zekânın hukuki niteliği ve kişiliği bağlamında açıklama ve öneri yapılırken yapay zekâ türlerine göre ayırım yapılmalı, fikir ve öneriler bu temel üzerinde inşa edilmelidir. Bu doğrultuda dar/zayıf, reaktif, sınırlı hafızalı yapay zekâ türleri için değil, geniş/güçlü, süper, bilinçli ve zihin teorisi düzeyindeki yapay zekâ türleri için hukuki nitelik ve kişilik tartışmalarının yürütülmesi ve önerilerde bulunulması daha isabetli olacaktır.

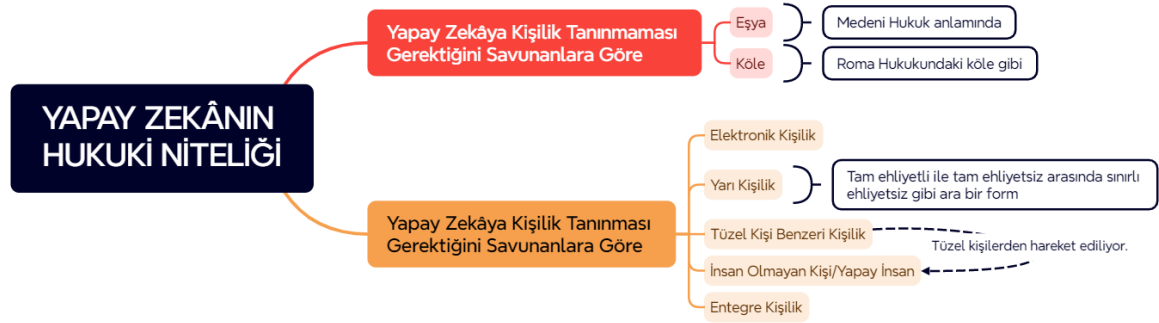
Toparlamak gerekirse yapay zekânın hukuki niteliği konusunda doktrinde farklı açılardan tasnif yapılmış, Roma hukukundaki köleye benzetenler olduğu gibi medeni hukuk anlamında eşya olarak görenler de olmuştur. Çünkü tüzel kişilere atfedilerek üretilen ve yukarıda bahsedilen kişilik türleri suistimale açıktır. Yani, yapay zekâ çalışmaları büyük oranda şirketler tarafından organize edilmekte ve pazarlanmaktadır. Bir tüzel kişinin üretimini tüzel kişi benzeri bir kişilik olarak kabul etmek hakkaniyetin tesisi ve sorumluluk açısından bazı çıkmazlara sebebiyet verebilir. Yarı kişilik ise henüz ana rahmine düşmemiş bir çocuk için yat almaya ve bu yatla taşınan yolcuların denizde boğulması halinde sorumluluğun nasıl olacağını tasavvur etmeye benzemektedir. Yani, ileride yapay zekânın

Personality Model for Artificial Intelligence: Integrated Personality”, *Bilişim Hukuku Dergisi* 7, sy 1 (2025): 340-42, <https://doi.org/10.55009/bilisimhukukudergisi.1686538>.

¹⁴⁵ EKİCİ, “Integrated Personality”, 339-40.

¹⁴⁶ EKİCİ, “Integrated Personality”, 338.

mutlaka süper yahut bilinç düzeyinde bir yapay zekâ olacağı kesin değilken ara bir form öngörülmesi fazla bir ayrıntı teşkil edecektir. Yapay zekânın bu aşamaya ulaşması durumunda *Ekici'* nin kişilik önerisinin benimsenmesi isabetli olacaktır.



Şema 5: Yapay Zekânın Hukuki Niteliği

İKİNCİ BÖLÜM

DİJİTAL HİZMETLER KANUNU VE YAPAY ZEKÂ KANUNU EKSENİNDE SOSYAL MEDYA VE YAPAY ZEKÂ

Birinci bölümde çalışmanın iki temel unsuru olan sosyal medya ve yapay zekâ teknik manada incelenmiş ve çalışmanın devamına ışık tutacak şekilde hukuki zeminde açıklamalar yapılmıştır.

Çalışmanın ikinci bölümü olan bu bölümde ise Avrupa Birliği tarafından yürürlüğe konan ve çalışmanın iki temel unsuruyla bağlantılı olan Dijital Hizmetler Kanunu ve Yapay Zekâ Kanunu incelenecektir. İncelencek olan bu düzenlemeler, çalışmanın konusuyla bağlantılı ve sınırlı olarak incelenecektir. Bu düzenlemeler incelendikten sonra son bölüme geçmeden önce inceleme sonucu elde edilen bulgular, “Ara Değerlendirme” başlığı altında paylaşılacaktır.

1) DİJİTAL HİZMETLER KANUNU (DSA)

İnternetin sivil nitelik kazanımıyla birlikte içinde sosyal medyanın da olduğu çevrimiçi faaliyetlerde artış yaşanmıştır. Çevrimiçi faaliyetlerdeki artış ve çeşitlilik, dijital ortamda sunulan hizmetlerin kalitesinin, hukuka uygunluğunun ve kullanıcı deneyiminin önem kazanmasına vesile olmuştur.

AB, çevrimiçi faaliyetlerin hukuka uygun devam etmesini ve Birlik vatandaşlarının güvenli bir çevrimiçi deneyim yaşamalarını temin etmek amacıyla çevrimiçi ortamı düzenleme yoluna gitmiştir. Bu çalışmanın konusu itibarıyla bu hukuki düzenlemelerden biri, 2000/31/AT sayılı Direktifi tadil eden ve Dijital Hizmetler için Tek Pazara ilişkin 19 Ekim 2022 tarihli ve (AB) 2022/2065 sayılı Avrupa Parlamentosu ve Konsey Tüzüğü’dür (Dijital Hizmetler Kanunu-DSA)¹⁴⁷.

¹⁴⁷ Doktrinde “regulation” kavramının çevirisi olarak kimi zaman “kanun” kimi zaman “tüzük” terimi tercih edilmektedir. DSA gibi bu bölümün sonraki başlığında incelenecek olan AI Act düzenlemesi de “regulation” biçiminde ihdas edilmiştir. AB hukukunda regulation terimi “tüzük” olarak çevrilmektedir. AB hukukundaki bu isimle anılan düzenlemeler, Birlik sınırları

Çalışmanın bu kısmında öncelikle DSA düzenlemesinin gerekliliği ve amacı açıklanacaktır. Devamında bu çalışmanın konusuyla bağlantılı ve sınırlı olarak sosyal ağ sağlayıcılarına DSA tarafından getirilen yükümlülükler incelenecektir.

A. DÜZENLEMENİN GEREKLİLİĞİ VE AMACI

Birinci bölümde sosyal medyanın tarihi başlığında açıklandığı üzere web 1.0, web 2.0 ve web 3.0 teknolojileri, internet kullanıcılarının deneyimlerini farklılaştırmış ve çeşitlendirmiştir. Kanun koyucunun bu teknolojilerden her birinin çıktıktan sonraki reaksiyonu en azından web 1.0 ve web 2.0 için farklı olmuştur.

Web 1.0 döneminde internetin yapısının tek yönlü oluşu, toplumun internetle olan bağının yeni yeni kurulması ve internet ortamını deneyimleyen bireylerin bu ortama olan güveninin sağlanması gibi sebepler, bu alanın hukuken düzenlenmesinde etkili olmuştur¹⁴⁸. AB, bu doğrultuda 8/06/2000 tarihli ve 2000/31/AT sayılı İç Pazarda Özellikle Elektronik Ticaret Olmak Üzere Bilgi Toplumu Hizmetlerinin Belirli Yasal Yönleri Hakkında Direktif'i (E-Ticaret Direktifi-ETD)¹⁴⁹ devreye almıştır¹⁵⁰.

çinde doğrudan, üye devletler tarafından uyumlaştırılması gerekmeksizin uygulanmaktadır. Çalışmanın bu bölümünde incelenen DSA ve AI Act düzenlemeleri de birer regulation yani tüzük olup AB genelinde doğrudan hüküm ve sonuç doğuran düzenlemelerdir. Çalışmada bu düzenlemeler için kullanılan "kanun" terimi ise Türkiye'deki okuyucular için daha anlaşılır olması için tercih edilmiştir. Tüzük hakkında ayrıntılı bilgi için bkz. İlke GÖÇMEN, *Avrupa Birliği Hukukunun Temelleri*, Gözden Geçirilmiş ve Güncellenmiş 2. Baskı (Seçkin Yayıncılık, 2023), 431-33; Işıl ÖZKAN, *Avrupa Birliği Kamu Hukuku: Brexit Sonrası Değişikliklerle*, Güncellenmiş 3. Baskı (Seçkin Yayıncılık, 2022), 124-25.

¹⁴⁸ Fülürya YUSUFOĞLU BİLGİN, *Dijital Piyasalarda Yer Sağlayıcıların Hukuki Sorumluluğu (Marka, Telif Hakkı ve Haksız Rekabet Kapsamında)*, 1. Baskı (On İki Levha Yayıncılık, 2022), 13.

¹⁴⁹ Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), L 178 OJ (2000), <http://data.europa.eu/eli/dir/2000/31/oj/eng>.

¹⁵⁰ 1996 tarihli ABD İletişim Ahlakı Yasası'nın (Communications Decency Act) hizmet sağlayıcıların düzenlenmesinde öncül bir düzenleme olduğu ve diğer ülke düzenlemeleri için ilham kaynağı olduğu yönünde bkz. Mehmet Bedii KAYA, *Avrupa Birliği P2B Tüzüğü: Aracı Hizmet Sağlayıcılar ve Arama Motorları İçin Adil ve Şeffaf Platform Kuralları*, 1. Baskı (On İki Levha Yayıncılık, 2022), 21.

ETD, AB kanun koyucusunun çevrimiçi dünyadaki faaliyetleri hukuki açıdan ele aldığı ilk düzenlemedir. ETD ile bilgi toplumu hizmetlerinin¹⁵¹ kolay bir şekilde dolaşımı teşvik edilerek iç pazarın düzgün işleyişini pekiştirmek ve kullanıcıların internet ortamına ve özellikle e-ticarete olan güvenini artırmak amaçlanmıştır¹⁵². ETD m. 4, AB üyesi devletlerin, hizmet sağlayıcıların bilgi toplumu hizmeti sunabilmesini özel bir onay sürecine bağlamasını yasaklamıştır.

ETD, hizmet sağlayıcıların bilgi toplumu hizmeti sunabilmesi için özel koruma sağlayan hükümler ihdas etmiştir. Aracı hizmet sağlayıcılar¹⁵³, güvenli liman (*safe harbour*) rejimi ile ihlal teşkil eden içerik hakkında bilgi sahibi olmadığı, bu içerik bakımından aktif konumda olmadığı ve bu içerikten haberdar olduktan sonra içeriği kaldırdığı veya içeriğe erişimi engellediği sürece AB düzeyinde sorumluluktan muaf tutulmuştur¹⁵⁴. Bu doğrultuda aracı hizmet sağlayıcılar, salt iletim (*mere conduit*), ön belleğe alma (*caching*) ve yer sağlama (*hosting*) hizmeti sağlamalarından ötürü sorumlu olmayacaktır¹⁵⁵. Böylelikle hizmet sağlayıcıların

¹⁵¹ Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 Laying down a Procedure for the Provision of Information in the Field of Technical Regulations and of Rules on Information Society Services, OJ L 241 (2015), md. 1(1)(b), <http://data.europa.eu/eli/dir/2015/1535/oj/eng>. Direktif'in anılan hükmüne göre bilgi toplumu hizmeti, çoğunlukla ücret karşılığı, uzaktan, elektronik araçlarla ve hizmet alıcısının bireysel talebi üzerine sağlanan hizmet olarak tanımlanmıştır.

¹⁵² KAYA, *Avrupa Birliği P2B Tüzüğü*, 21.

¹⁵³ ETD, aracı hizmet sağlayıcıları bizzat tanımlamamış olmakla birlikte Bölüm 4'te sorumluluktan muafiyetleri için gereken şartları belirlemiştir. Aracı hizmet sağlayıcı kavramı ise bizzat DSA'da tanımlanmıştır. Bu kavram hakkındaki açıklamalar için bkz. bu çalışmanın ikinci bölümünün I), B) başlığı.

¹⁵⁴ Güvenli liman kapsamında aracı hizmet sağlayıcıların sorumluluktan muafiyetleri için aranan şartlar hakkında ayrıntılı bilgi için bkz. YUSUFOĞLU BİLGİN, *Dijital Piyasalarda Yer Sağlayıcıların Hukuki Sorumluluğu (Marka, Telif Hakkı ve Haksız Rekabet Kapsamında)*, 95-142.

¹⁵⁵ KAYA, *Avrupa Birliği P2B Tüzüğü*, 23.

Birlik içinde serbestçe faaliyette bulunabilmesinin önü açılmış¹⁵⁶ ve bilgi toplumu hizmetleri çevrimiçi ortamda gelişebilmiştir¹⁵⁷.

ETD yürürlüğe girdikten sonra web 2.0 teknolojisinin milenyumla birlikte hızla yükselişi ve teknolojinin üssel gelişimi, bilgi toplumu hizmetlerine de sirayet etmiş, aracı hizmet sağlayıcıların sunduğu hizmetleri de çeşitlendirmiştir. Güvenli liman ilkesinin getirdiği konforla sınır tanımaksızın Birlik sınırları içinde ve dünyanın her yerinde faaliyet gösteren büyük teknoloji şirketleri ortaya çıkmıştır. Bilgi toplumu hizmetlerindeki bu artış, internet ortamının yararlı hedefler için kullanılmasını kolaylaştırırsa da bu ortamda hukuka aykırı içeriklerin yayılımını da kolaylaştırmıştır¹⁵⁸. Ayrıca sosyal medyada dezenformasyon ve nefret söylemi yaygınlaşmış ve seçmen davranışları manipüle edilmiştir¹⁵⁹.

Öte yandan ETD'nin esasen bir direktif olması ve Birlik genelinde doğrudan uygulanmayıp üye devletlerce iç hukuklarıyla uyumlaştırılmasının gerekmesi¹⁶⁰, Alman Ağ Yaptırım Kanunu gibi üye devletlerin ulusal düzeydeki farklı düzenlemeleri¹⁶¹ ve yukarıda bahsedilen diğer sebepler, ETD'nin etkililiğini ve

¹⁵⁶ KAYA, *Avrupa Birliği P2B Tüzüğü*, 23; Amélie Pia HELDT, "EU Digital Services Act: The White Hope of Intermediary Regulation", içinde *Digital Platform Regulation: Global Perspectives on Internet Governance*, ed. Terry FLEW ve Fiona R. MARTIN, Palgrave Global Media Policy and Business (Palgrave Macmillan, 2022), 70, https://doi.org/10.1007/978-3-030-95220-4_4.

¹⁵⁷ Digital Services Act (DSA), Gerekeçe 16.

¹⁵⁸ Digital Services Act (DSA), Gerekeçe 5.

¹⁵⁹ Alper IŞIK, *İnternet Aktörleri ve Egemenliğin Değişen Boyutları*, Güncellenmiş 2. Baskı (On İki Levha Yayıncılık, 2025), 118; Kübra Sıla MAMALI, *Dijital Hizmetler Yasası ve AB E-Ticaret Direktifi Kapsamında İnternette Hizmet Sağlayıcıların Hukuka Aykırı İçerikten Sorumluluğu*, 1. Baskı, Hukuk Yayınları Dizisi 3492 (Seçkin Yayıncılık, 2023), 36-37; YUSUFOĞLU BİLGİN, *Dijital Piyasalarda Yer Sağlayıcıların Hukuki Sorumluluğu (Marka, Telif Hakkı ve Haksız Rekabet Kapsamında)*, 332; HELDT, "EU Digital Services Act", 70.

¹⁶⁰ KAYA, *Avrupa Birliği P2B Tüzüğü*, 23.

¹⁶¹ MAMALI, *Dijital Hizmetler Yasası ve AB E-Ticaret Direktifi Kapsamında İnternette Hizmet Sağlayıcıların Hukuka Aykırı İçerikten Sorumluluğu*, 35.

verimliliğini olumsuz etkilemiş ve bu konuda daha kapsamlı bir düzenleme yapılması gereğini ortaya koymuştur¹⁶².

15/12/2020’de Avrupa Komisyonu tarafından DSA ve Dijital Piyasalar Kanunu (*Digital Markets Act*) tekliflerini içeren bir paket açıklanmıştır¹⁶³. Bu paket ile kullanıcıların güvenilir ürünlere erişimini sağlayarak haklarını korumak ve dijital pazarda adil bir rekabet ortamını sağlamak amaçlanmıştır¹⁶⁴.

DSA teklifi kapsamında 2021 yılı içinde Avrupa Ekonomik ve Sosyal Komitesi¹⁶⁵, Avrupa Veri Koruma Denetçisi¹⁶⁶ ve Avrupa Bölgeler Komitesi¹⁶⁷ görüş sunmuştur. Temmuz 2022’ye gelindiğinde Avrupa Parlamentosu yapılan değişiklikleri içeren ilk DSA pozisyonunu açıklamıştır¹⁶⁸. Bu okuma pozisyonu, AB Konseyi tarafından 4 Ekim 2022’de onaylanmıştır¹⁶⁹. 19 Ekim 2022’de ise DSA, AB Parlamentosu ve AB Konseyi tarafından resmen kabul edilmiş ve 27 Ekim 2022’de AB Resmî Gazetesi’nde yayınlanmıştır¹⁷⁰. DSA, AB Resmî Gazetesi’nde yayımlanmasını takip eden 20. günde yürürlüğe girmiştir. DSA m. 93 uyarınca DSA, 17 Şubat 2024 itibariyle uygulanmaya başlamıştır. Ancak aynı hükme göre

¹⁶² MAMALI, *Dijital Hizmetler Yasası ve AB E-Ticaret Direktifi Kapsamında İnternette Hizmet Sağlayıcıların Hukuka Aykırı İçerikten Sorumluluğu*, 38; HELDT, “EU Digital Services Act”, 70-71; KAYA, *Avrupa Birliği P2B Tüzüğü*, 26.

¹⁶³ https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2347.

¹⁶⁴ <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package>. DSA ve bu bölümün ikinci başlığında incelenecek AI Act, esasen sosyal ağ sağlayıcılar, yapay zekâ geliştiricileri, sağlayıcıları, yerleştiricileri, dağıtıcıları gibi süjeler için temel hak ve özgürlükleri kısıtlayıcı niteliktedir. Bu düzenlemelerle temelde bireylerin ve bahsedilen teknolojileri elinde tutanların hak ve özgürlükleri arasında “denge” sağlanmaya çalışılmaktadır.

¹⁶⁵ Görüş için bkz. <https://eur-lex.europa.eu/legal-content/EN/AUTO/?uri=celex:52021AE0022>

¹⁶⁶ Görüş için bkz. [https://eur-lex.europa.eu/legal-content/EN/AUTO/?uri=celex:52021XX0427\(01\)](https://eur-lex.europa.eu/legal-content/EN/AUTO/?uri=celex:52021XX0427(01)).

¹⁶⁷ Görüş için bkz. <https://eur-lex.europa.eu/legal-content/EN/AUTO/?uri=celex:52020AR5356>.

¹⁶⁸ Ayrıntılı bilgi için bkz. https://www.europarl.europa.eu/doceo/document/TA-9-2022-07-05_EN.html#sdocta1.

¹⁶⁹ AB Konseyi kararı için bkz. <https://data.consilium.europa.eu/doc/document/ST-13164-2022-INIT/EN/pdf>.

¹⁷⁰ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2022:277:TOC>.

- Şeffaflık raporlama yükümlülüğüne ilişkin DSA m. 24/2, DSA m. 24/3 ve DSA m. 24/6,
- Bağımsız denetime ilişkin DSA m. 37/7,
- Veri erişimine ilişkin AB Komisyonu'nun yetki devrine dayanan tasarruflarını düzenleyen DSA m. 40/13,
- Denetim ücretini düzenleyen DSA m. 43,
- VLOP/VLOSE'lara ilişkin denetim, soruşturma, yürürlüğe koyma ve izleme ile ilgili ihdas edilen DSA m. 64 ilâ DSA m. 83,
- Uygulamaya ilişkin ortak hükümleri düzenleyen DSA m. 84-85-86 ve
- Yetki devrine dayanan tasarruflar ile uygulama tasarruflarını düzenleyen DSA m. 87-88 hükümleri 16 Kasım 2022'den itibaren uygulanmaya başlamıştır.

DSA m. 91 uyarınca AB Komisyonu, DSA'nın tamamen yürürlüğe girdiği tarihten itibaren 5 yıl içinde (18/02/2027'ye kadar) KOBİ'ler üzerinde bu düzenlemenin potansiyel etkilerini değerlendirmekle ve AB Parlamentosu'na, AB Konseyi'ne ve Avrupa Ekonomik ve Sosyal Komitesi'ne rapor olarak sunmakla yükümlendirilmiştir. Ayrıca AB Komisyonu, her beş yılda bu düzenlemeyi değerlendirip az önce ifade edilen kurumlara sunmakla yükümlü tutulmuştur.

AB Komisyonu DSA teklifini açıklarken bu düzenlemenin etki değerlendirmesine ilişkin dokümanları da yayınlamıştır¹⁷¹. Etki değerlendirmelerinde DSA'nın neden gerekli olduğu ve bu düzenleme ile ne amaçlandığı açıklanmaktadır. Bu kapsamda dijital hizmetlerin yaygınlaşmasının hukuka aykırı içeriklerin ve dezenformasyonun yayılmasında önemli bir rol oynadığı ifade edilmektedir. Öte yandan çevrimiçi platformların algoritmik sıralama ve tavsiye sistemleri, bilgi manipülasyonuna neden olmakta, şeffaflık

¹⁷¹ Ayrıntılı bilgi için bkz. <https://digital-strategy.ec.europa.eu/en/library/impact-assessment-digital-services-act>.

eksikliği ortaya çıkmakta ve temel hak ve hürriyetlerin korunmasındaki yetersizliği gözler önüne sermektedir. Ek olarak yukarıda da ifade edildiği üzere üye devletlerin farklı hukuki çerçeveler ile bu alanı düzenlemesi sebebiyle şirketler farklılaşan ve artan yükümlülükle karşı karşıya kalmaktadır.

DSA m. 1’de düzenlemenin temel amacı, AB iç pazarının düzgün işlemlerini sağlamaktır. Bu doğrultuda alt amaçlar belirlenmiştir. Bu alt amaçlar, tüketicileri ve temel hak ve hürriyetleri daha etkin bir şekilde korumak, sosyal medya ve çevrimiçi platformlar için sorumlulukları daha açık ve net olarak belirlemek, hukuka aykırı içerik, nefret söylemi ve dezenformasyonla mücadele etmek, raporlama yükümlülükleriyle şeffaflığı artırmak ve ihdas edilecek düzenleyici kurumlar ile mevcut kurumlar arasındaki iş birliğini ve uyumu artırmak olarak ifade edilebilir.

B. SOSYAL AĞ SAĞLAYICILARINA GETİRİLEN YÜKÜMLÜLÜKLER

DSA kapsamında öngörülen yükümlülükler incelenmeden önce düzenlemede zikredilen terminolojik tanımlara yer vermek gerekmektedir. Bu noktadan itibaren DSA kapsamında yükümlülükler açıklanırken yükümlülerin öznesi ve yeknesak bir terim olarak “sosyal ağ sağlayıcı” ibaresi kullanılacaktır.

“Sosyal ağ sağlayıcı” ibaresi açıkça DSA’da tanımlanmamıştır. DSA kapsamında süjeler, aracı hizmet sağlayıcı, çevrimiçi platform, çevrimiçi arama motoru, çok büyük çevrimiçi platform (VLOP) ve çok büyük çevrimiçi arama motorudur (VLOSE). Bunlardan sadece çevrimiçi platform ve çevrimiçi arama motoru açıkça DSA m. 3’te tanımlanmış olup diğerleri düzenlemenin gerekçelerinde (resital) ve hükümlerinde zikredilmektedir.

DSA kapsamında açıklanması gereken ilk kavram, aracı hizmet sağlayıcıdır. Bu süje, DSA m. 3/g’de tanımlanan “aracılık hizmeti” esas alınarak tanımlanmaktadır. Aracılık hizmeti, her şeyden önce bir “bilgi toplumu hizmeti”

olarak tanımlanmaktadır. Bilgi toplumu hizmetlerinden sadece iletim¹⁷², önbellege alma¹⁷³ ve yer sağlama¹⁷⁴ hizmetlerini sunan kişiler, aracı hizmet sağlayıcıdır.

Aracı hizmet sağlayıcının bir üst versiyonu olarak ifade edilebilecek süje ise çevrimiçi platformlardır. DSA m. 3/i'de açıkça tanımlanan bu süje, hizmet alıcısının¹⁷⁵ talebi üzerine bilgileri depolayan ve kamuya yayan bir yer sağlama hizmeti olarak tanımlanmaktadır. DSA Gerekçe 13'e göre bir yer sağlama hizmetinin çevrimiçi platform olarak sayılabilmesi için "hizmet alıcısının talebi üzerine bilgiyi saklama" ve "kamuya yayma"¹⁷⁶ unsurlarının bir arada bulunması gerekmektedir.

DSA m. 3'te tanımlanan diğer bir süje ise çevrimiçi arama motorudur. DSA m. 3/j'ye göre çevrimiçi arama motoru, kullanıcıların; anahtar kelime, sesli istek, ifade veya başka bir girdi şeklinde herhangi bir konudaki bir sorgu temelinde, prensip olarak tüm internet sitelerinde veya belirli bir dildeki tüm internet sitelerinde arama yapmak için sorgu yapmalarına olanak tanıyan ve istenen içerikle ilgili bilgilerin bulunabileceği herhangi bir formatta sonuçlar veren bir aracılık hizmetidir.

¹⁷² DSA m. 3/g'ye göre sadece iletim, hizmet alıcısı tarafından sağlanan bilgilerin bir haberleşme ağında iletilmesinden veya bir haberleşme ağına erişim sağlanmasından oluşan hizmettir.

¹⁷³ DSA m. 3/g'ye göre önbellege alma, hizmet alıcısı tarafından sağlanan bilginin bir haberleşme ağında iletilmesinden oluşan, bu bilgilerin otomatik, ara ve geçici depolanmasını içeren, yalnızca bilginin talepleri üzerine diğer alıcılara daha etkin bir şekilde iletilmesini sağlamak amacıyla gerçekleştirilen hizmettir.

¹⁷⁴ DSA m. 3/g'ye göre yer sağlama, bir hizmet alıcısının talebi üzerine ve kendisi tarafından sağlanan bilgilerin depolanmasından oluşan hizmettir.

¹⁷⁵ DSA m. 3/b: "hizmet alıcısı, özellikle bilgi aramak veya bilgiyi erişilebilir kılmak amacıyla bir aracılık hizmetini kullanan herhangi bir gerçek veya tüzel kişidir." Hizmet alıcısı kavramının net olmadığı yönünde bkz. Ilaria BURI ve Joris VAN HOBOKEN, "The Digital Services Act (DSA) Proposal: A Critical Overview", Institute for Information Law (IVIIR), 2021, 14, https://dsa-observatory.eu/wp-content/uploads/2021/11/Buri-Van-Hoboken-DSA-discussion-paper-Version-28_10_21.pdf; Hizmet alıcısı ile kastedilenin isabetli olarak içerik sağlayıcı olduğunu yönünde bkz. YUSUFOĞLU BİLGİN, *Dijital Piyasalarda Yer Sağlayıcıların Hukuki Sorumluluğu (Marka, Telif Hakkı ve Haksız Rekabet Kapsamında)*, 346.

¹⁷⁶ DSA m. 3/k: "'kamuya yayma', bilgiyi sağlayan hizmet alıcısının talebi üzerine, bilginin potansiyel olarak sınırsız sayıda üçüncü tarafın kullanımına sunulmasıdır." Ayrıntılı bilgi için bkz. MAMALI, *Dijital Hizmetler Yasası ve AB E-Ticaret Direktifi Kapsamında İnternette Hizmet Sağlayıcıların Hukuka Aykırı İçerikten Sorumluluğu*, 106-8.

Son açıklanacak olan s jeler ise VLOP ve VLOSE'lerdir. Bu s jeler esasında DSA'nın d zenleme amacı ve gereklilięi d ř n ld ę nde en  nemli s je olarak g r lmektedir. Bu s jeler, az  nce zikredilen  evrimi i platform ve  evrimi i arama motorundan oluřumlarındaki ve hizmet alıcılarına etkilerindeki farklılık sebebiyle ayrılmaktadır¹⁷⁷. DSA m. 33 ve DSA Gerek e 76'da da ifade edildięi  zere Avrupa n fusunun en az %10'u kadar (45 milyona eřit veya daha fazla) kullanıcısı (hizmet alıcısı) olan  evrimi i platformlar ve  evrimi i arama motorları VLOP ve VLOSE olarak ek y k ml l klere ve denetimlere tabi olmaktadır.

Bu a ıklamalar doęrultusunda  alıřmanın bu b l m nde sosyal aę saęlayıcı kavramı, aracı hizmet saęlayıcıyı,  evrimi i platformu ve bazı yerlerde VLOP'u ifade etmek  zere kullanılacaktır.

1. İrtibat Noktası ve Yasal Temsilci Belirlenmesi

DSA,  evrimi i ortamda g venli bir pazar hedefi doęrultusunda sosyal aę saęlayıcılara (aracı hizmet saęlayıcılarına)  nemli sorumluluklar y kleemektedir. Bu sorumluluklardan ilki, DSA m. 11-12-13'te d zenlenen irtibat noktası ve yasal temsilci belirleme y k ml l ę d r. Sosyal aę saęlayıcıları, DSA m. 11 uyarınca AB  yesi devlet yetkilileri, Avrupa Komisyonu ve DSA m. 61'de belirtilen Avrupa Dijital Hizmetler Kurulu (ADHK-*European Digital Services Board*) ile doęrudan elektronik yollarla iletiřim kurmalarını saęlayacak tek bir irtibat noktası belirlemek zorundadır. Bu irtibat noktasına iliřkin bilgilerin kolayca eriřilebilir, g ncel ve kamuya a ık olması gerekmektedir. Ayrıca, iletiřim i in yaygın olarak anlařılan bir dilin yanı sıra AB  yesi devletlerin resm  dillerinden bir veya daha fazlasının belirtilmesi de beklenmektedir.

Bu y k ml l ę n temel gerek eleri DSA'nın 42 ve 43 numaralı gerek elerinde ele alınmaktadır. Gerek e 42,  evrimi i ortamda g veni tesis etmek i in yetkili makamlar ve sosyal aę saęlayıcıları arasında doęrudan ve etkili bir

¹⁷⁷ Folkert WILMAN, *The Digital Services Act (DSA) - An Overview*, 2022, 3, <https://dx.doi.org/10.2139/ssrn.4304586>.

iletiřim kanalının nemini vurgulamaktadır¹⁷⁸. Bu doęrultuda irtibat noktasının elektronik bir irtibat noktası olabileceęi, fiziksel bir konuma sahip olmasının gerekmedięi ifade edilmektedir. Bu ykmllk kapsamında dikkat edilmesi gereken bir husus ise sosyal aę saęlayıcıların DSA gereklilikleri ve amaları doęrultusunda aynı irtibat noktasını belirleyebilmeleridir.

Gereke 43'te saęlayıcının kolay erişilebilir yollarla hızlı, doęrudan ve etkili iletiřime olanak tanıyacak řekilde hizmet alıcıları iin tek bir irtibat noktası¹⁷⁹ belirlemelerinin gerekli olduęu ifade edilmiřtir. Hizmet alıcısı bir kiři sohbet robotları ile iletiřime getięinde bu durum aıka belirtilmelidir. Sosyal aę saęlayıcıları, ayrıca hizmet alıcılarının sadece otomatik aralara dayanmayan doęrudan ve etkili iletiřim aralarını semelerine izin vermelidir. Sosyal aę saęlayıcıları, bu iletiřimin zamanında ve etkin bir řekilde gerekleřtirilmesini saęlamak zere yeterli insan kaynaklarının ve mali kaynakların tahsis edilmesini gvence altına almak iin tm makul abayı gstermelidir¹⁸⁰.

DSA m. 13'te ise AB'de kurulu olmayan ancak AB iinde hizmet sunan sosyal aę saęlayıcıları iin zel bir ykmllk getirmektedir: hizmet sundukları AB yesi devletlerden birinde yazılı olarak bir yasal temsilci belirleme ve atama zorunluluęu. Yasal temsilci, sosyal aę saęlayıcıların yanı sıra veya onların yerine AB yesi devletlerin yetkili makamları, Avrupa Komisyonu ve ADHK tarafından dzenlemenin uygulanması, kararlara uyulması ve bunların icra edilmesi iin gerekli tm konularda muhatap alınabilmektedir. Sosyal aę saęlayıcılar, yasal temsilcilerine yetkili makamlarla verimli ve zamanında iř birlięi yapmalarını ve kararlara uymalarını garanti edecek gerekli yetkileri ve yeterli kaynakları saęlamalıdır¹⁸¹. Yasal temsilcinin adı, posta adresi, e-posta adresi ve telefon

¹⁷⁸ Digital Services Act (DSA), Gereke 42.

¹⁷⁹ AB kanun koyucusu bu irtibat noktalarına rnek olarak telefon numaraları, e-posta adresleri, elektronik irtibat formları, sohbet robotları veya anlık mesajlařmayı gstermiřtir. Bu sayım tahdidi olmayıp sosyal aę saęlayıcılar tarafından bařka irtibat noktaları da belirlenebilecektir.

¹⁸⁰ Digital Services Act (DSA), Gereke 43.

¹⁸¹ Digital Services Act (DSA), Gereke 44.

numarası, temsilcinin ikamet ettiği veya kurulduğu AB üyesi devletin Dijital Hizmetler Koordinatörüne (DHK/DSC-Digital Services Coordinator) bildirilmek ve kamuya açık, kolayca erişilebilir ve güncel tutulmak zorundadır. Doktrinde bu yükümlülük, etkili iletişimi¹⁸², kamu denetimini ve uygulanmasını kolaylaştırmanın bir yolu olarak görülmektedir¹⁸³.

Burada dikkat edilmesi gereken husus, atanan yasal temsilcinin, sosyal ağ sağlayıcının “kendi sorumluluğuna hanel gelmeksizin” DSA kapsamındaki yükümlülüklerle uyulmamasından sorumlu tutulabilmesidir. Ayrıca DSA’nın öngördüğü yükümlülüklerle uymak koşuluyla birden fazla sosyal ağ sağlayıcı aynı yasal temsilciyi temsilci olarak belirleyebileceği gibi bu yasal temsilciyi ayrıca irtibat noktası olarak belirleyebilir¹⁸⁴.

Bu yükümlülüklerin getirilmesinin temel amacı, sosyal ağ sağlayıcıları, özellikle de çok büyük çevrimiçi platformlar (VLOP’lar) ve çok büyük çevrimiçi arama motorları (VLOSE’lar) tarafından uyumun denetlenmesi, soruşturulması, uygulanması ve izlenmesi için yetkililere gerekli bilgileri sağlamaktır. Bu, AB’nin dijital yönetişimini güçlendirmede ve hesap verebilirliği sağlamada hayati bir rol oynamaktadır.

Yasal temsilci ile ilişkili sorumluluklar ve yükümlülükler, sosyal ağ sağlayıcılar için önemli bir hukuki yük oluşturmaktadır. Yasal temsilci sadece bir posta adresi olmamakta, ayrıca DSA yükümlülüklerine uyulmamasından sorumlu tutulabilmektedir. Bu, yetkililerle zamanında ve verimli iş birliği yapmayı gerektirmekte ve DSA yükümlülüklerinin derinlemesine anlaşılmasını zorunlu kılmaktadır. Bu karmaşıklık, sağlayıcıları iç personel yerine uzmanlaşmış harici firmaları kullanmaya teşvik etmektedir. Bu ise AB’de hukuki uyum hizmetleri için yeni bir niş pazarın doğmasına yol açmaktadır. Bu durumun, daha küçük platformların bu yüküyle başa çıkmakta daha fazla zorlanabileceğini ve bunun daha

¹⁸² WILMAN, *The Digital Services Act (DSA) - An Overview*, 9.

¹⁸³ WILMAN, *The Digital Services Act (DSA) - An Overview*, 14.

¹⁸⁴ Digital Services Act (DSA), Gerekçe 44.

büyük, daha fazla kaynağa sahip oyuncuları destekleyebileceğini ifade etmek gerekmektedir.

Doktrin, DSA'nın bu hükümlerle getirdiği yükümlülüklerin önemini vurgulamaktadır. *Buri/Van Hoboken*, AB'de kurulu olmayan sosyal ağ sağlayıcıları için yasal temsilci atanması zorunluluğunun düzenlemeye uyulmamasından sorumlu tutulabilmeleri açısından önemli olduğunu belirtmektedir¹⁸⁵. Bu durum, DSA'nın yargı dışı etkisini ve AB hukuk sisteminin coğrafi sınırları aşan erişimini göstermektedir¹⁸⁶.

Sosyal ağ sağlayıcıların öngörülen bu yükümlülüklerle gösterdikleri uyuma da değinmek gerekmektedir. Bu doğrultuda Meta (*Facebook, Instagram*) gibi platformlar, Meta Platforms Ireland Limited'i posta yoluyla iletişim için bir irtibat noktası olarak belirtmekte ve hizmet şartları ile ilgili sorular için bir e-posta adresi sunmakta¹⁸⁷, genel yardım merkezleri de kullanıcı desteği sağlamaktadır¹⁸⁸. Google, AB üyesi devlet yetkilileri, Avrupa Komisyonu ve Güvenilir İşaretleyiciler (*Trusted Flaggers*) gibi profesyonel kuruluşlarla doğrudan ve verimli iletişim kurmak için özel bir "DSA İrtibat Noktası" sayfası oluşturmuştur¹⁸⁹. Bu sayfa, iletişim kanallarını ve rollerini açıklamakla birlikte, belirli bir yasal temsilcinin adını açıkça belirtmemektedir. TikTok'un Şeffaflık Merkezi'nde "Bildirimler" altında bir "İrtibat noktaları" bölümü bulunmaktadır¹⁹⁰. Ayrıca, gizlilikle ilgili konular için veri koruma görevlisi ile iletişime geçmek üzere bir form sunulmaktadır¹⁹¹. X (eski adıyla Twitter) ile ilgili bir Hollanda Mahkemesi kararı,

¹⁸⁵ BURI ve VAN HOBOKEN, "The Digital Services Act (DSA) Proposal: A Critical Overview", 19.

¹⁸⁶ Aina TURILLAZZI vd., "The Digital Services Act: An Analysis of Its Ethical, Legal, and Social Implications", *Law, Innovation and Technology* 15, sy 1 (2023): 104, <https://doi.org/10.1080/17579961.2023.2184136>.

¹⁸⁷ https://help.instagram.com/639208781107982/?helpref=related_articles.

¹⁸⁸ <https://www.meta.com/help/>.

¹⁸⁹ <https://support.google.com/legal/troubleshooter/13966113?hl=en>.

¹⁹⁰ <https://www.tiktok.com/transparency/en/dsa-transparency>.

¹⁹¹ <https://www.tiktok.com/legal/report/dpo>.

X'in etkili bir iletişim kanalı sağlamayarak DSA'yı ihlal ettiğini tespit etmiştir¹⁹². Bu karar, yalnızca bir e-posta adresi sağlamanın yeterli olmadığını, kullanıcı dostu ve kolay erişilebilir irtibat noktalarının önemini vurgulamaktadır. X, bu kararın ardından Yardım platformunda açıklamalar eklemiştir¹⁹³.

Bu gelişmelerin önemli bir sonucu, DSA m. 13'te belirtilen yasal temsilci zorunluluğunun DSA'nın yargı dışı etkisini güçlendiren doğrudan bir mekanizma olmasıdır. DSA, sağlayıcıların AB'deki kuruluş yerinden bağımsız olarak hizmet sunmaları durumunda uygulanmaktadır. AB dışındaki kuruluşlar için yasal temsilci atanması, AB hukuk sisteminde somut bir iletişim ve hesap verebilirlik noktası sağlamakta, böylece yabancı kuruluşların yalnızca AB dışında olmaları nedeniyle yükümlülüklerden kaçınmasını engellemektedir. Bu durum, AB hukukunun "Brüksel Etkisi" olarak bilinen küresel düzenleyici standartları belirleme yeteneğini pekiştirmektedir¹⁹⁴.

2. Hizmet Şartlarının Belirlenmesi

DSA m. 14, sosyal ağ sağlayıcıların hizmet şartlarını (hüküm ve koşullarını) belirlemesine ilişkin şeffaflık ve açıklık yükümlülüklerini düzenlemektedir. Bu madde, çevrimiçi platformların içerik denetimi uygulamalarını kullanıcılar için daha anlaşılır hale getirmeyi ve temel haklara saygı göstermeyi amaçlamaktadır.

DSA m. 14'e göre sosyal ağ sağlayıcıları, hizmetlerinin kullanımıyla ilgili olarak hizmet alıcıları tarafından sağlanan bilgilere uyguladıkları her türlü kısıtlamaya ilişkin bilgileri hizmet şartlarına dahil etmek zorundadır. Bu bilgiler, algoritmik karar verme ve insan incelemesi dahil olmak üzere içerik yönetimi amacıyla kullanılan politikaları, prosedürleri, önlemleri ve araçları ile iç şikâyet

¹⁹² Global Freedom of Expression, "Danny Mekić v. X (formerly Twitter) Shadow Banning", <https://globalfreedomofexpression.columbia.edu/cases/mekic-v-x-formerly-twitter-shadow-banning/>.

¹⁹³ <https://help.x.com/en/rules-and-policies/european-union>.

¹⁹⁴ Anupam CHANDER, "When the Digital Services Act Goes Global", *Berkeley Technology Law Journal* 38, sy 3 (2023): 1067-88, <https://papers.ssrn.com/abstract=4606282>.

işleme sistemlerinin usul kurallarını içermelidir. Bu bilgilerin “açık, sade, anlaşılır, kullanıcı dostu ve net bir dilde” belirtilmesi ve kamuya açık, kolayca erişilebilir ve makine tarafından okunabilir bir formatta sunulması gerekmektedir.

Sağlayıcılar, hizmet şartlarındaki önemli değişiklikleri hizmet alıcılarına bildirmekle yükümlüdür. Özellikle esas olarak küçüklere yönelik veya ağırlıklı olarak onlar tarafından kullanılan bir hizmetin sağlayıcısı, hizmetin kullanım koşullarını ve kısıtlamalarını küçüklerin anlayabileceği bir şekilde açıklamak zorundadır. Sağlayıcılar, DSA m. 1’de belirtilen kısıtlamaları uygularken ve icra ederken “özenli, objektif ve orantılı bir şekilde” hareket etmeli, hizmet alıcılarının Avrupa Birliği Temel Haklar Şartı’nda yer alan temel hakları dahil olmak üzere ilgili tüm tarafların haklarına ve meşru menfaatlerine gereken özeni göstermelidir. Çok büyük çevrimiçi platformlar (VLOP’lar) ve çok büyük çevrimiçi arama motorları (VLOSE’lar) için ek yükümlülükler de getirilmiştir: hizmet şartlarının kısa, kolay erişilebilir ve makine tarafından okunabilir bir özetini sunmak ve hizmet verdikleri tüm Üye Devletlerin resmi dillerinde yayınlamak. DSA Gerekçe 81, özellikle küçükler için açık ve anlaşılır şartların önemini vurgulayarak onların bilinçli kararlar alabilmelerini ve riskleri anlayabilmelerini sağlamayı hedeflemektedir.

Doktrinde, DSA m. 14’ün içerik denetimi kararlarında AB temel hakları hukukunun uygulanıp uygulanmadığına dair tartışmalar bulunmaktadır. *Buri/van Hoboken*, DSA m. 14’ün bu konudaki belirsizliğini dile getirmiş ve açıklık getirilmezse hükmün “kâğıttan bir kaplan” olarak kalabileceği, etkinliğinin gelecekteki mahkeme yorumlarına bağlı olacağı uyarısında bulunmuştur¹⁹⁵. *Quintais, Appelman ve Fathaigh*, DSA m. 14’ün, çevrimiçi platformlar ile kullanıcılar arasındaki yatay ilişkide temel hakların dolaylı yatay etkisini temelde mümkün kıldığını savunmaktadır. Ancak bu potansiyelin tam olarak gerçekleşmesi için uluslararası ve Avrupa temel hakları standartları çerçevesinde hareket edilmesi

¹⁹⁵ BURI ve VAN HOBOKEN, “The Digital Services Act (DSA) Proposal: A Critical Overview”, 20.

gerektiği belirtilmektedir¹⁹⁶. *Leerssen/van Duin/Toepoel/van Hoboken*, DSA m. 14'ün yanlış içerik denetimi ve kullanıcıların temel haklarının korunmasıyla ilgili davalar için güçlü bir temel oluşturduğunu belirtmektedir¹⁹⁷.

Sosyal ağ sağlayıcılar DSA'ya uyum sağlamak amacıyla hizmet şartlarında birtakım güncellemeler yapmaktadır. *Facebook* ve *Instagram* gibi platformlar, içerik denetimi kararları ve itiraz seçenekleri hakkında daha fazla bilgi sağlamak üzere hizmet şartlarını güncellemiştir¹⁹⁸. *Spotify*'ın kullanım koşulları, platform kurallarını içererek platformdaki tüm içeriklere uygulanan yönergeleri ve politikaları belirlemektedir¹⁹⁹. *Bluesky Social*'ın şartları, platformun kendi şartlarını veya topluluk yönergelerini ihlal eden kullanıcı içeriğini kaldırma veya değiştirme yetkisi vermektedir²⁰⁰. *Meta*, hizmet şartlarında kötüye kullanım ve veri kazıma (*data scraping*) ile ilgili daha net ifadeler eklemiş ve *Facebook*, *Messenger*, *Instagram* ve *Threads* için topluluk standartlarını tek bir merkezi konuma taşımıştır²⁰¹. Ayrıca, avatar ve yapay zekâ kullanımıyla ilgili özel nitelendirmeler ekleyerek ayrı yapay zekâ şartlarına atıfta bulunmuştur²⁰². *Google*'ın *Ad Manager* ve *AdSense* hizmetleri, yayıncıların AB'deki reklamlar için yasal gerekliliklere uymasını zorunlu kılmaktadır. Bu doğrultuda kullanıcıların hukuka aykırı içeriği

¹⁹⁶ João Pedro QUINTAIS vd., "Using Terms and Conditions to apply Fundamental Rights to Content Moderation", *German Law Journal* 24, sy 5 (2023): 903, <https://doi.org/10.1017/glj.2023.53>.

¹⁹⁷ Paddy LEERSSEN vd., *Pathways to Private Enforcement of the Digital Services Act* (Institute for Information Law, University of Amsterdam, 2025), 18, <https://dsa-observatory.eu/2025/06/05/report-pathways-to-private-enforcement-of-the-digital-services-act-dsa/>.

¹⁹⁸ <https://about.fb.com/news/2023/08/new-features-and-additional-transparency-measures-as-the-digital-services-act-comes-into-effect/>

¹⁹⁹ https://www.spotify.com/safetyandprivacy/transparency/eu_20250213_dsa_report.pdf

²⁰⁰ <https://bsky.social/about/support/tos>

²⁰¹ <https://transparency.meta.com/en-gb/policies/community-standards/>

²⁰² *Meta* avatarları için bkz. https://www.facebook.com/legal/avatars_terms, *Meta* yapay zekâları için bkz. <https://www.facebook.com/legal/ai-terms>

bildirmeleri için mekanizma sağlanmaktadır²⁰³. Ayrıca, reklam içi şeffaflık bilgileri için kontroller sunulmaktadır²⁰⁴.

DSA m. 14/4'te yer alan "temel haklara gereken özeni gösterme" hükmü, sosyal ağ sağlayıcıların rolünü temelden değiştirebilecek bir potansiyele sahiptir. Bu hüküm, platformları yalnızca içerik barındırıcı olmaktan çıkarıp çevrimiçi ifade özgürlüğünün "yarı düzenleyicileri" konumuna getirmektedir. Çünkü ETD'de "güvenli liman" ilkesi kabul edilmişti. Sosyal ağ sağlayıcılar bu doğrultuda sadece içeriği barındıran (yer sağlayan) olarak hareket etmekte, uyar-kaldır yöntemi ile pasif bir tutum sergilemekteydiler. Ancak anılan DSA hükmü ile birlikte sosyal ağ sağlayıcılar pasif konumdan aktif bir konuma geçmek durumunda kalmıştır. Bu durum ise onları "yarı-düzenleyici" bir noktaya taşımaktadır.

DSA m. 14/4, platformların hizmet şartlarını uygularken temel hakları dikkate almasını açıkça zorunlu kılmaktadır. Bu durum, geleneksel devlet-vatandaş hakları uygulamasından özel kuruluşlar (platform-kullanıcı) arasındaki yatay bir uygulamaya geçişini ifade etmektedir. Hüküm, kullanıcıların içerik denetimi kararlarına temel haklar temelinde itiraz etmeleri için yasal bir zemin oluşturmakta ve platformların insan hakları üzerindeki etkileri konusunda hesap verebilirliğini artırmaktadır²⁰⁵.

DSA m. 14'ün etkinliği, büyük ölçüde yargısal yorumlamaya ve platformların tutarlı uygulamasına bağlıdır. Doktrin, "gereken özen" kavramındaki belirsizliğe dikkat çekmektedir²⁰⁶. Açık operasyonel yönergeler veya tutarlı mahkeme kararları olmadan platformlar bu hükmü, temel hakların

²⁰³ <https://support.google.com/admanager/answer/14335032?hl=en>

²⁰⁴ <https://support.google.com/adsense/answer/14335032?hl=en>

²⁰⁵ QUINTAIS vd., "Using Terms and Conditions to apply Fundamental Rights to Content Moderation", 904.

²⁰⁶ BURI ve VAN HOBOKEN, "The Digital Services Act (DSA) Proposal: A Critical Overview", 20.

korunması ruhunu tam olarak benimsemeden sorumluluktan kaçınmak için minimum düzeyde yorumlayabilir²⁰⁷.

“Açık, sade, anlaşılır, kullanıcı dostu” dil gerekliliği, karmaşık hukuki ve teknik hizmet şartları için önemli bir zorluk teşkil etmektedir. Platformların hizmet şartları genellikle uzun ve karmaşık olup kullanıcıların gerçek anlamda anlamasını zorlaştırmaktadır. DSA m. 14, bu durumu tüm kullanıcılar, özellikle de küçükler için basitleştirmeyi zorunlu kılmaktadır²⁰⁸. Bu doğrultuda Avrupa Komisyonu yaş doğrulama yöntemleri ve küçükler için yönelik hüküm ve koşullarda bulunması gereken hususlara yönelik bir rehber yayınlamıştır²⁰⁹.

3. Şeffaflık Raporlama Yükümlülüğü

DSA, sosyal ağ sağlayıcılara, özellikle de VLOP’lar ve VLOSE’lara, içerik denetimi faaliyetlerine ilişkin kapsamlı şeffaflık raporlama yükümlülükleri getirmektedir. Bu yükümlülükler, DSA m. 15, DSA m. 24 ve DSA m. 27’de detaylandırılmıştır.

DSA m. 15’e göre sosyal ağ sağlayıcıları (mikro ve küçük işletmeler hariç), içerik denetimi faaliyetlerine ilişkin “açık, kolay anlaşılır ve ayrıntılı raporları” yılda en az bir kez kamuya açık bir şekilde yayınlamak zorundadır. Bu raporlar, üye devlet yetkililerinden alınan emirlerin sayısını, bildirim ve eylem prosedürü aracılığıyla sunulan bildirimlerin sayısını, kendi inisiyatifleriyle alınan içerik denetimi önlemlerinin türlerini ve dahili şikâyet işleme sistemi aracılığıyla alınan şikâyetleri içermelidir.

²⁰⁷ QUINTAIS vd., “Using Terms and Conditions to apply Fundamental Rights to Content Moderation”, 910.

²⁰⁸ Digital Services Act (DSA), Gerekçe 45-46.

²⁰⁹ EUROPEAN COMMISSION, “Communication to the Commission - Approval of Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online”, 2025, <https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-protection-minors>.

Sosyal ağ sağlayıcılar için DSA m. 24, DSA m. 15'teki bilgilere ek olarak mahkeme dışı uyuşmazlık çözüm organlarına sunulan uyuşmazlıkların sayısını, sonuçlarını ve çözüm sürelerini, ayrıca açıkça hukuka aykırı içerik, açıkça temelsiz bildirimler veya şikâyetler nedeniyle uygulanan askıya alma işlemlerini raporlamayı zorunlu kılmaktadır. Ayrıca bu sağlayıcılar, AB'deki ortalama aylık aktif hizmet alıcılarının sayısını en az altı ayda bir kamuya açık bir şekilde yayınlamakla yükümlüdür. Çevrimiçi platformlar, DSA m. 17'de belirtilen gerekçe beyanlarını kişisel verilerden arındırarak Avrupa Komisyonu tarafından yönetilen kamuya açık, makine tarafından okunabilir bir veritabanına (DSA Şeffaflık Veritabanı) sunmak zorundadır.

Çok büyük çevrimiçi platformlar (VLOP'lar) ve çok büyük çevrimiçi arama motorları (VLOSE'lar) için DSA m. 27, faaliyetlerinin boyutu ve etkisi nedeniyle daha sıkı şeffaflık gereklilikleri getirmektedir. Bu platformlar, şeffaflık raporlarını en az altı ayda bir yayınlamalı ve içerik denetimi ekipleri hakkında, nitelikleri ve dil uzmanlıkları dahil olmak üzere bilgi vermelidir. Ayrıca tavsiye sistemlerinde kullanılan ana ve en önemli parametreleri açıkça açıklamalı ve kullanıcılara tercih ettikleri tavsiye ayarlarını seçme veya değiştirme imkânı sunmalıdır. DSA Gerekçe 100, VLOP'lar ve VLOSE'ların risk değerlendirmeleri hakkında "kapsamlı" raporlama yapmaları gerektiğini belirtmektedir.

Şeffaflık raporlamasının etkinliği konusunda farklı görüşler bulunmaktadır. Avrupa Tüketici Örgütü (BEUC), şeffaflık raporlarının stratejik olarak yapılandırılabilceği riskine karşı uyarıda bulunmuş ve raporların yapısı, içeriği ve metodolojisi için ek kurallar önermiştir²¹⁰. *Shahi vd.na* göre, platformların DSA Şeffaflık Veritabanı gerekliliklerine biçimsel olarak uymasına rağmen genellikle önemli isteğe bağlı ayrıntıları atladığını, bunun da veritabanının pratik

²¹⁰ BEUC, "The Digital Services Act Proposal: BEUC Position Paper", 2021, 19, https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-032_the_digital_services_act_proposal.pdf.

kullanışlılığını ve güvenilirliğini sınırladığını göstermektedir²¹¹. Bu yazarlara göre sosyal ağ sağlayıcıların arasında kendi bildirdikleri denetim uygulamalarında önemli farklılıklar bulunmaktadır²¹².

Avrupa Komisyonu, DSA Şeffaflık Veritabanı'nı başlatmıştır²¹³. Bu veritabanı, gerekçe beyanlarını (DSA m. 17) neredeyse gerçek zamanlı olarak toplamakta ve kamuya açık hale getirmektedir. VLOP'lar, Ağustos 2023'ten itibaren gerekçe beyanlarını yayınlamaya başlamış, diğer tüm çevrimiçi platformların ise 17 Şubat 2024'e kadar bunu yapması zorunlu hale gelmiştir. Veritabanının veri saklama politikası, Şubat 2025'te güncellenerek günlük veri dökümlerinin beş yıl boyunca erişilebilir olması sağlanmıştır²¹⁴.

Sosyal ağ sağlayıcıların şeffaflık raporlama yükümlülüğü kapsamındaki uygulamalarına bakıldığında:

- Meta: *Facebook* ve *Instagram* için DSA m. 15, DSA m. 24 ve DSA m. 42 uyarınca şeffaflık raporları yayınlamaktadır²¹⁵. *Knight-Georgetown Enstitüsü* tarafından yayımlanan bir yazıda Meta'nın, söz konusu raporlarda fiziksel ve zihinsel refahı çok yönlü riskler olarak değerlendirdiğini ancak Meta'nın değerlendirmelerinin, ürün özelliklerinin sorunlu kullanıma nasıl teşvik edebileceğini yeterince dikkate almadığını ifade etmektedir²¹⁶.

²¹¹ Gautam Kishore SHAHI vd., *A Year of the DSA Transparency Database: What it (Does Not) Reveal About Platform Moderation During the 2024 European Parliament Election*, 2025, 2, <https://arxiv.org/pdf/2504.06976v1>.

²¹² SHAHI vd., *A Year of the DSA Transparency Database: What it (Does Not) Reveal About Platform Moderation During the 2024 European Parliament Election*, 2.

²¹³ <https://transparency.dsa.ec.europa.eu/>.

²¹⁴ Veri saklama politikası için bkz. <https://transparency.dsa.ec.europa.eu/page/data-retention-policy>.

²¹⁵ <https://transparency.meta.com/reports/regulatory-transparency-reports/>.

²¹⁶ KNIGHT-GEORGETOWN INSTITUTE, "Systemic Risk Assessment under the Digital Services Act", 2025, <https://kgi.georgetown.edu/research-and-commentary/systemic-risk-assessment-under-the-digital-services-act/>.

- Google: Google, DSA kapsamında VLOP/VLOSE Şeffaflık Raporu dahil olmak üzere çeşitli şeffaflık raporları yayınlamaktadır. *Google Arama, Haritalar, Play ve Shopping* de sistemik risk değerlendirme raporları (DSA m. 34) ve denetim raporları (DSA m. 37, DSA m. 42) yayınlamaktadır²¹⁷. *Google Shopping*, DSA Şeffaflık Veritabanı'na milyonlarca gerekçe beyanı göndermiştir²¹⁸.
- TikTok: TikTok, altı ayda bir şeffaflık raporları yayınlarak içerik denetimi faaliyetlerini, hukuka aykırı içerik bildirimlerini ve kullanıcı itirazlarını detaylandırmaktadır²¹⁹. Ayrıca yıllık sistemik risk değerlendirme raporları (DSA m. 34, DSA m. 35) ve bağımsız denetim raporları (DSA m. 37) da yayınlamaktadır. TikTok'un raporu, proaktif içerik denetimi ve küçüklerin korunmasına yönelik çabaları vurgulasa²²⁰ da Avrupa Komisyonu, TikTok hakkında tavsiye sistemleri, siyasi reklamlar ve araştırmacılar için veri erişimi ile ilgili olası ihlaller nedeniyle soruşturma başlatmıştır²²¹.
- X (eski adıyla Twitter): X'in 2025 şeffaflık raporu, spam ve platform manipölasyonunun önde gelen sorunlar olduğunu gösteren milyonlarca kullanıcı şikayetini içermektedir²²². X hakkında hukuka aykırı içerik, bilgi manipölasyonu, karanlık tasarımlar, reklam şeffaflığı ve

²¹⁷ <https://transparencyreport.google.com/report-downloads>.

²¹⁸ 05.09.2025 tarihi itibarıyla bu sayı 778.731.412'dir. Daha fazla ayrıntı için bkz. https://transparency.dsa.ec.europa.eu/statement?s=&platform_id%5B%5D=26&platform_id-26=on&created_at_start=&created_at_end=.

²¹⁹ <https://www.tiktok.com/transparency/en/dsa-transparency>.

²²⁰ Ayrıntılı bilgi için bkz. [https://sf16-va.tiktokcdn.com/obj/eden-va2/zayvwly_fjulyhwzuhy\[/ljhwZthlaukjlkulzlp/DSA_H2_2024/TikTok-DSA-Risk-Assessment-Report-2023.pdf](https://sf16-va.tiktokcdn.com/obj/eden-va2/zayvwly_fjulyhwzuhy[/ljhwZthlaukjlkulzlp/DSA_H2_2024/TikTok-DSA-Risk-Assessment-Report-2023.pdf).

²²¹ Ayrıntılı bilgi için bkz. https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1223.

²²² X'in 2025 şeffaflık raporu hakkında daha fazla bilgi için bkz. <https://transparency.x.com/en/reports/global-reports/2025-transparency-report>.

araştırmacılar için veri erişimi ile ilgili iddia edilen ihlaller nedeniyle soruşturma altındadır²²³.

DSA'nın şeffaflık raporlama yükümlülükleri, önemli bir "şeffaflık paradoksu"nu ortaya çıkarmaktadır. DSA, benzeri görülmemiş bir şeffaflık düzeyi hedeflemektedir. Ancak doktrin²²⁴, platformların kendi bildirdikleri verilerde tutarsızlıklar, eksik ayrıntılar ve farklı metodolojiler olduğunu ifade etmektedir. Bu durum, yalnızca raporlama gerekliliğinin yeterli olmadığını, aynı zamanda bildirilen verilerin *kalitesinin* standartlaştırılması ve sağlam bir şekilde denetlenmesinin de kritik olduğunu göstermektedir.

Platform Adı	Raporlama Sıklığı	Temel Raporlama Alanları	Belirtilen Uyum Güçlü Yönleri	Belirtilen Uyum Boşlukları (Zorlukları)
Meta	Yıllık Altı Aylık	İçerik denetimi hacmi, kullanıcı itirazları, sistemik risk değerlendirmeler i, reklam havuzları	Fiziksel ve zihinsel refahı çapraz kesen riskler olarak değerlendir me	Ürün özelliklerinin sorunlu kullanıma teşvik etme potansiyelini yeterince dikkate almama; Profilleme tabanlı

²²³ Ayrıntılı bilgi için bkz. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6709.

²²⁴ SHAHI vd., *A Year of the DSA Transparency Database: What it (Does Not) Reveal About Platform Moderation During the 2024 European Parliament Election*.

				olmayan akış seçenekleri sunmama
Google	Yıllık Altı Aylık	İçerik kaldırma talepleri, sistemik risk değerlendirmeleri, denetim raporları, reklam şeffaflığı	Kişiselleştirilmiş akışları devre dışı bırakma seçeneği sunma; Milyonlarca gerekçe beyanı yayınlama	Sistemik riskin tanımında belirsizlik; Denetimlerde veri kalitesi ve metodoloji eksikliği
TikTok	Altı Aylık Yıllık	İçerik denetimi, hukuka aykırı içerik bildirimleri, kullanıcı itirazları, sistemik risk değerlendirmeleri, reklam havuzları	Proaktif içerik denetimi küçüklerin korunmasına yönelik çabalar	Reklam havuzu şeffaflığında eksiklikler; Tavsiye sistemleri ve araştırmacı veri erişiminde sorunlar
X	Altı Aylık	Kullanıcı şikayetleri, spam ve manipülasyon,	Şeffaflık raporları yayınlama	Karanlık tasarımlar, reklam

		sistemik risk değerlendirmeler i		şeffaflığı ve araştırmacı veri erişiminde ihlaller; Tavsiye sistemleri denetiminde kaynak yetersizliği
--	--	--	--	---

Şema 6: VLOP/VLOSE Şeffaflık Raporlama Genel Bakışı

4. Bildirim ve Eylem Mekanizmaları

DSA, çevrimiçi platformlarda hukuka aykırı içeriğin bildirilmesi ve bu içeriğe karşı harekete geçilmesi için “bildirim ve eylem mekanizmaları”nı (DSA m. 16) ve “güvenilir işaretleyiciler” (DSA m. 22) sistemini detaylandırmaktadır. Bu hükümler, hukuka aykırı içeriğin etkin bir şekilde kaldırılması ile ifade özgürlüğü dengesini sağlamayı amaçlamaktadır.

DSA m. 16’ya göre, sosyal ağ sağlayıcılar, bireylerin veya kuruluşların, hizmetlerinde hukuka aykırı olduğunu düşündükleri belirli bilgi öğelerinin varlığını kendilerine bildirmelerine olanak tanıyan mekanizmalar (*notice and action*) oluşturmak zorundadır. Bu mekanizmaların “erişimi kolay ve kullanıcı dostu” olması ve “yeterince kesin ve yeterince gerekçelendirilmiş bildirimlerin” elektronik yollarla sunulmasına izin vermesi gerekmektedir. Bildirimler, bilginin neden hukuka aykırı olduğuna dair yeterince gerekçelendirilmiş bir açıklama, bilginin tam elektronik konumu (örneğin, URL), bildirimde bulunan bireyin veya kuruluşun adı ve e-posta adresi (çocuk cinsel istismarı suçları hariç) ve iyi niyet beyanı gibi unsurları içermelidir. Sağlayıcılar, bildirimin alındığını derhal teyit etmeli ve bildirim yapan kişiye kararlarını ve bu kararlara karşı başvuru yollarını

bildirmelidir. Kararlar “zamanında, özenli, keyfi olmayan ve objektif bir şekilde” işlenmeli ve otomatik araçların kullanılması durumunda bu kullanım hakkında bilgi verilmelidir.

DSA m. 22, “güvenilir işaretleyiciler”in (*trusted flaggers*) rolünü resmiyete kavuşturmaktadır. Güvenilir işaretleyiciler, Dijital Hizmetler Koordinatörleri (DSC’ler) tarafından sertifika alabilen uzman kuruluşlardır (hükümet veya sivil toplum kuruluşları). Diğer bir ifadeyle bireyler güvenilir işaretleyici statüsü alamamaktadır. Platformlar, güvenilir işaretleyiciler tarafından sunulan bildirimlere öncelik vermeli ve bunları gecikme olmaksızın işlemelidir. Bu, daha önce gönüllü olan bir çerçeveyi yasal bir zorunluluğa dönüştürmektedir. DSA, hukuka aykırı içeriğin etkin bir şekilde kaldırılması ile platform kullanıcılarının ve genel kamuoyunun ifade ve bilgi özgürlüğü arasında bir denge kurmayı amaçlamaktadır.

Sosyal ağ sağlayıcıların kullanıcıların hukuka aykırı içeriğin varlığını bildirmelerine olanak tanımak için platformlarının tasarımını ve hizmet şartlarını uyarlamaları gerekmektedir. Aksi durumda, kullanıcılar içerik denetimi kararlarına dahili şikâyet işleme veya mahkeme dışı uyuşmazlık çözümü yoluyla itiraz edebilecektir.

DSA’nın, hukuka aykırı içeriğin etkin bir şekilde kaldırılması ile ifade özgürlüğü arasında bir denge kurmaya çalıştığı ifade edilmektedir. Doktrinde güvenilir işaretleyici düzenlemelerinin başlangıçta platformların sivil toplum uzmanlığını içerik denetimi süreçlerine dahil etmeye yönelik gönüllü çabaları olduğu belirtilmektedir. DSA, bu durumu yasal bir zorunluluğa dönüştürmüş ve DSC’lerin tüm platformlar tarafından tanınan güvenilir işaretleyicileri seçmesini gerektirmiştir²²⁵.

Güvenilir işaretleyici katılımının, hukuka aykırılık veya hizmet şartları ile uyumsuzluk konusunda hata yapmaları durumunda internet kullanıcılarının

²²⁵ Jakob VAN DE KERKHOF, “Article 22 Digital Services Act: Building Trust with Trusted Flaggers”, *Internet Policy Review* 14, sy 1 (2025): 2-3, <https://doi.org/10.14763/2025.1.1828>.

konuşma özgürlüğünü gereksiz yere kısıtlayabilmesi mümkündür²²⁶. Teknoloji şirketleri tarafından finanse edilen güvenilir işaretleyicilerin bağımsızlığı konusunda da tartışmalar mevcuttur²²⁷.

Sosyal ağ sağlayıcılar, bildirim ve eylem mekanizmaları yükümlülüğünü uygulamak için çeşitli adımlar atmıştır. X, Apple, Pinterest, Facebook, Instagram ve TikTok gibi birçok platform, hukuka aykırı içeriği işaretlemek için yeni, kullanıcı dostu seçenekler sunmuştur²²⁸. Avrupa Dijital Haklar Örgütü (EDRi), X aleyhine güvenilir işaretleyicileri İngilizce dışındaki dillerde işlevsiz bir forma yönlendirerek çalışmalarını engellediği gerekçesiyle şikâyetle bulunmuştur²²⁹. *Meta*, bildirilen içeriğin standartlarını ihlal edip etmediğini değerlendirmekte ve hukuka aykırı içeriği etiketlendiği yargı yetkisi içinde kaldırmaktadır²³⁰. *Google'ın* DSA İrtibat Noktası sayfası, güvenilir işaretleyicilerin hukuka aykırı içeriği öncelikli olarak bildirmesine olanak tanımaktadır²³¹. *Amazon'un* bildirim mekanizmaları, 2024'ün ikinci yarısında yüz binlerce bildirim almış ve bunların çoğunu otomatik süreçlerle çözüme kavuşturmuştur. Amazon, temelsiz bildirimleri tekrar tekrar gönderen kullanıcılara karşı da önlem almıştır²³². Amazon'un ayrıca marka koruması için "Project Zero" adlı bir programı bulunmaktadır²³³. Spotify, e-posta adresi olan herkesin platform kurallarını ihlal ettiğini veya hukuka aykırı olduğunu düşündüğü içeriği güvenli bildirim formları aracılığıyla bildirmesine izin vermektedir. Kolluk kuvvetleri ve hükümet

²²⁶ VAN DE KERKHOF, "Article 22 Digital Services Act: Building Trust with Trusted Flaggers", 4-5.

²²⁷ VAN DE KERKHOF, "Article 22 Digital Services Act: Building Trust with Trusted Flaggers", 10.

²²⁸ Ayrıntılı bilgi için bkz. <https://digital-strategy.ec.europa.eu/en/policies/dsa-impact-platforms>.

²²⁹ Ayrıntılı bilgi için bkz. <https://edri.org/our-work/edri-files-dsa-legal-complaint-against-x/>.

²³⁰ <https://constitutionaldiscourse.com/content-moderation-on-social-media-platforms-in-the-eu/>.

²³¹ <https://support.google.com/legal/troubleshooter/13966113?hl=en>.

²³² Ayrıntılı bilgi için bkz. <https://trustworthyshopping.aboutamazon.com/digital-services-act-dsa-amazon-eu-store-transparency-report>.

²³³ VAN DE KERKHOF, "Article 22 Digital Services Act: Building Trust with Trusted Flaggers", 2.

kuruluşları da belirlenmiş güvenli kanallar aracılığıyla içerik bildiriminde bulunabilmektedir²³⁴.

“Güvenilir işaretleyiciler” sistemi, verimliliği artırmayı amaçlasa da aşırı kaldırma ve potansiyel yanlışlık veya siyasi etki risklerini de beraberinde getirmektedir. DSA m. 22, güvenilir işaretleyici bildirimlerine öncelik vermektedir²³⁵. Bu, açıkça hukuka aykırı içeriğin kaldırılmasını hızlandırırsa da bu kuruluşlara önemli bir güç vermektedir. Güvenilir işaretleyicilerin hata yapması veya belirli gündemleri olması durumunda, “gölge içerik yasaklaması” veya yasal konuşmanın aşırı kaldırılması (*risk of over-removal*) gibi durumlar ortaya çıkabilecektir. Dolayısıyla ifade özgürlüğünü ihlal edebilir²³⁶. Bu durum, verimlilik ile temel hakların korunması arasında bir gerilim yaratmakta ve güvenilir işaretleyicilerin kendilerinin sağlam bir şekilde denetlenmesi ihtiyacını ortaya koymaktadır²³⁷.

DSA m. 16, bildirimlerin işlenmesinde otomatik araçların kullanılmasına izin vermektedir²³⁸. Amazon gibi platformların otomatik süreçleri yoğun bir şekilde kullandığı yukarıda ifade edilmişti. Ancak DSA, hukuka aykırı içeriğin AB üyesi devletler arasında tek tip olarak tanımlanmadığını kabul etmektedir. Otomatik sistemler genellikle bağlam, hiciv veya kültürel nüanslarla başa çıkmakta zorlanmaktadır. Bu da sorunsuz bir konuşmanın yanlış tanımlanmasına ve kaldırılmasına yol açabilmektedir. Bu durum, karmaşık durumlarda ifade özgürlüğünü korumak ve aşırı sansürü önlemek için insan incelemesinin kritik önemini koruduğunu göstermektedir²³⁹.

²³⁴ Daha detaylı bilgi için bkz. https://www.spotify.com/safetyandprivacy/transparency/eu_20250213_dsa_report.pdf

²³⁵ VAN DE KERKHOF, “Article 22 Digital Services Act: Building Trust with Trusted Flaggers”, 4.

²³⁶ VAN DE KERKHOF, “Article 22 Digital Services Act: Building Trust with Trusted Flaggers”, 5.

²³⁷ VAN DE KERKHOF, “Article 22 Digital Services Act: Building Trust with Trusted Flaggers”, 6-7.

²³⁸ Digital Services Act (DSA), Gerekçe 54.

²³⁹ Gergely GOSZTONYI vd., “Theory and Practice of Social Media’s Content Moderation by Artificial Intelligence in Light of European Union’s AI Act and Digital Services Act”, *European*

Bildirim ve eylem mekanizması, kullanıcılara hukuka aykırı içeriği bildirme yetkisi verse de “yeterince kesin ve yeterince gerekçelendirilmiş” bildirimler sağlama yükünü kullanıcılara yüklemekte ve ardından başvuru mekanizmalarını kullanmalarını gerektirmektedir. DSA m. 16, kullanıcıların içeriğin neden hukuka aykırı olduğunu açıklamalarını ve tam konumunu belirtmelerini zorunlu kılmaktadır²⁴⁰. Bu, bildirimlerin kalitesini sağlasa da hukuki uzmanlığı olmayan ortalama kullanıcılar için önemli bir yük oluşturmaktadır. Ayrıca, DSA m. 21 uyarınca kullanıcılara kararlara itiraz etme hakkı tanınmasına rağmen dahili şikâyet işleme ve mahkeme dışı uyuşmazlık çözümünün etkinliği hala değerlendirilmekte olup tutarlılık ve tarafsızlık konusunda endişeler bulunmaktadır²⁴¹. Bu durum, resmi mekanizmaların var olmasına rağmen bireysel kullanıcılar için başvuru yollarının pratik erişilebilirliğinin ve etkinliğinin hala bir zorluk olduğunu göstermektedir.

5. İçeriğe Karşı Kısıtlamalarda Gerekçe Gösterilmesi

DSA m. 17, sosyal ağ sağlayıcılara içerik kısıtlamalarına ilişkin açık ve spesifik gerekçe beyanları sunma zorunluluğu getirmektedir. Bu hüküm, kullanıcıların içerik denetimi kararlarını anlamalarını ve bu kararlara karşı etkin bir şekilde itiraz etmelerini sağlamayı amaçlamaktadır.

DSA m. 17’ye göre sosyal ağ sağlayıcılar, hizmet alıcısı tarafından sağlanan bilgilerin hukuka aykırı içerik olması veya hizmet şartlarıyla uyumsuz olması nedeniyle uygulanan herhangi bir kısıtlama için etkilenen hizmet alıcılarına açık ve spesifik bir gerekçe beyanı sunmak zorundadır²⁴². Bu kısıtlamalar (1) belirli bilgi

Journal of Law and Political Science 4, sy 1 (2025): 40, <https://doi.org/10.24018/ejpolitics.2025.4.1.165>.

²⁴⁰ Digital Services Act (DSA), Gerekçe 53.

²⁴¹ Ayrıntılı bilgi için bkz. <https://dsa-observatory.eu/2025/01/20/expert-insights-fundamental-rights-in-dsa-dispute-resolution-procedures/>.

²⁴² Sosyal ağ sağlayıcıların gerekçe beyanı ve DSA kapsamında öngörülen diğer yükümlülüklerini yerine getirmemeleri durumunda DSA’nın Bölüm IV hükümleri uyarınca para cezası, tazminat gibi hukuki sorumlulukları doğacaktır.

öğelerinin görünürlüğünün kısıtlanması (içeriğin kaldırılması, erişimin engellenmesi veya düşürülmesi), (2) parasal ödemelerin askıya alınması veya sonlandırılması, (3) hizmetin tamamen/kısmen askıya alınması veya sonlandırılması veya (4) hizmet alıcısının hesabının askıya alınması veya sonlandırılması gibi durumları içermektedir. Bu yükümlülük, ilgili elektronik iletişim bilgilerinin sağlayıcı tarafından bilindiği durumlarda uygulanır ve kısıtlamanın uygulandığı tarihten itibaren en geç bu tarihte geçerli olur. Aldatıcı, yüksek hacimli ticari içeriklerde bu hüküm uygulanmaz.

Gerekçe beyanı en azından şu bilgileri içermelidir:

- Kararın bilginin kaldırılması, erişimin engellenmesi, düşürülmesi veya görünürlüğünün kısıtlanması veya bu bilgiyle ilgili parasal ödemelerin askıya alınması veya sonlandırılması olup olmadığına dair bilgi,
- Kararın alınmasında dayanak alınan olgular ve koşullar (DSA m. 16'ya göre bir bildirim üzerine mi yoksa inisiyatifle mi alındığı ve kesinlikle gerekliyse bildirimi yapanın kimliği dahil),
- Otomatik araçların kullanılıp kullanılmadığına dair bilgi,
- İddia edilen hukuka aykırı içerikle ilgiliyse dayanak alınan hukuki zemin ve neden hukuka aykırı kabul edildiğine dair açıklamalar,
- Sağlayıcının hizmet şartlarıyla uyumsuzluk iddia ediliyorsa dayanak alınan sözleşmesel zemin ve neden uyumsuz kabul edildiğine dair açıklamalar.

Ayrıca, hizmet alıcısına karara ilişkin mevcut başvuru yolları (dahili şikâyet işleme mekanizmaları, mahkeme dışı uyuşmazlık çözümü ve yargısal başvuru) hakkında açık ve kullanıcı dostu bilgi verilmelidir. Sağlayıcılar tarafından sağlanan bilgiler, ilgili hizmet alıcısının başvuru yollarını etkin bir şekilde kullanmasına olanak tanıyacak şekilde "açık, kolay anlaşılır ve mümkün olduğunca kesin ve spesifik" olmalıdır.

DSA m. 24/5 uyarınca sosyal ağ sağlayıcılar, bu kararları ve gerekçe beyanlarını kişisel verilerden arındırarak Avrupa Komisyonu tarafından yönetilen kamuya açık, makine tarafından okunabilir bir veritabanına sunmak zorundadır.

DSA Şeffaflık Veritabanı, çevrimiçi platformların gözlemlenebilirliğini devrim niteliğinde değiştirmeyi vaat eden, şeffaflık için benzeri görülmemiş bir araç olarak görülmektedir²⁴³. *Shahi vd.na* göre bildirilen verilerin doğasından kaynaklanan tutarsızlıklar ve uyumsuzluk sorunları tespit edilmiştir. Bu da veritabanının kullanılabilirliğini ve güvenilirliğini sınırlamıştır²⁴⁴. Yazarlar, platformların biçimsel olarak uyum sağlamasına rağmen gerekçe beyanlarında önemli isteğe bağlı ayrıntıları genellikle atladığını bulmuştur²⁴⁵. Öte yandan kararların gecikmeli bildirilmesi veya tersine çevrilmesi potansiyelinin kamu güvenine zarar verebileceği, bu nedenle sosyal ağ sağlayıcıların düzeltmeler veya açıklamalar yapmayı düşünmeleri gerektiği belirtilmektedir²⁴⁶.

Bu yükümlülük açısından sosyal ağ sağlayıcı uygulamalarına bakıldığında:

- Ağustos 2023'ten itibaren VLOP'lar, içerik kaldırıldığında veya kısıtlandığında kullanıcılara bilgi vermek ve "gerekçe beyanı"nda nedenlerini açıklamak zorundadır. Bu yükümlülük, 17 Şubat 2024'e kadar tüm barındırma hizmetlerine genişletilmiştir.
- DSA Şeffaflık Veritabanı: Platformlar, gerekçe beyanlarını bu veritabanına göndermektedir. Veritabanı, kısıtlama türü, kategori,

²⁴³ SHAHI vd., *A Year of the DSA Transparency Database: What it (Does Not) Reveal About Platform Moderation During the 2024 European Parliament Election*, 1.

²⁴⁴ SHAHI vd., *A Year of the DSA Transparency Database: What it (Does Not) Reveal About Platform Moderation During the 2024 European Parliament Election*, 2.

²⁴⁵ SHAHI vd., *A Year of the DSA Transparency Database: What it (Does Not) Reveal About Platform Moderation During the 2024 European Parliament Election*, 2.

²⁴⁶ Doris BUIJS, "The Digital Services Act and the Implications for News Media and Journalistic Content (Part 1)", DSA Observatory, 2022, Ayrıntılı bilgi için bkz., <https://dsa-observatory.eu/2022/09/29/digital-services-act-implications-for-news-media-journalistic-content-part-1/>.

kaynak, kullanılan otomatik araçlar gibi çeşitli kriterlere göre arama ve filtreleme yapılmasına olanak tanımaktadır.

- Meta (Facebook/Instagram): Meta'nın Şeffaflık Merkezi, kaldırma nedenleri dahil olmak üzere içerik denetimi eylemlerini raporlamaktadır. Meta'nın gerekçe beyanları DSA Şeffaflık Veritabanı'nda mevcuttur.
- Google: *Google Shopping*, DSA Şeffaflık Veritabanı'na milyonlarca gerekçe beyanı göndermiştir. Google'ın şeffaflık raporları da içerik kaldırma taleplerini kapsamaktadır.
- X (eski adıyla Twitter): Bir Hollanda mahkemesi, X'in bir kullanıcının hesap görünürlüğünü kısıtlaması için yeterli gerekçe sunmayarak sözleşme yükümlülüklerini ve DSA m. 17'yi ihlal ettiğini tespit etmiştir²⁴⁷. Bu durum, "gölge yasaklama" (*shadow banning*) olsa bile açık ve spesifik gerekçelerin önemini vurgulamaktadır²⁴⁸. X'in şeffaflık raporu, milyonlarca kullanıcı şikayetini göstererek çok sayıda denetim eylemi olduğunu ima etmektedir²⁴⁹.
- Spotify: Spotify'nın şeffaflık raporu, kaldırma veya keşfedilebilirlik/erişim kısıtlamalarının nedenleri dahil olmak üzere içerik denetimi eylemlerini detaylandırmaktadır²⁵⁰.

DSA m. 17'nin gerekçe beyanlarına ilişkin ayrıntılı gereklilikleri, sosyal ağ sağlayıcıların şeffaf olmayan uygulamalarının ötesine geçerek kullanıcıların kararlara etkin bir şekilde itiraz etmelerini sağlamak için kritik öneme sahiptir. DSA öncesinde kullanıcılar genellikle açıkça belirtilmeyen içerik denetimi

²⁴⁷ Global Freedom of Expression, "Danny Mekić v. X (formerly Twitter) Shadow Banning", <https://globalfreedomofexpression.columbia.edu/cases/mekic-v-x-formerly-twitter-shadow-banning/>.

²⁴⁸ Jakob VAN DE KERKHOF ve Catalina GOANTA, "Shadowbanned on X: The DSA in Action", *European Journal of Risk Regulation* 16, sy 1 (2025): 354, <https://doi.org/10.1017/err.2024.81>.

²⁴⁹ X'in 2025 şeffaflık raporu hakkında daha fazla bilgi için bkz. <https://transparency.x.com/en/reports/global-reports/2025-transparency-report>.

²⁵⁰ https://www.spotify.com/safetyandprivacy/transparency/eu_20250213_dsa_report.pdf.

kararlarıyla karşılaşılıyorlardı. DSA m. 17, kısıtlama türü, olgusal koşullar, hukuki/sözleşmesel dayanaklar ve başvuru yolları hakkında spesifik ayrıntılar talep etmektedir. Bu ayrıntılı bilgi, sadece şeffaflık sağlamakla kalmayıp aynı zamanda kullanıcının içeriğin *neden* kısıtlandığını anlamasını ve *nasıl* etkin bir şekilde itiraz edeceğini bilmesini doğrudan kolaylaştıracaktır. Böylece kullanıcı haklarını ve platform hesap verebilirliğini güçlendirir. Hollanda Mahkemesinin X aleyhindeki kararı²⁵¹, bu gerekliliğin hukuki olarak uygulanabilirliğini göstermektedir.

Otomatik sistemler tarafından alınan kararlar için açık ve spesifik gerekçe sağlamak, önemli bir teknik ve hukuki engel teşkil etmektedir. DSA m. 17, sosyal ağ sağlayıcıların kararda otomatik araçların kullanılıp kullanılmadığını açıklamasını zorunlu kılmaktadır. Sosyal ağ sağlayıcılar, içerik denetimi için yapay zekâya giderek daha fazla güvendidikçe karmaşık algoritmik kararlar için insan tarafından anlaşılabilir açıklamalar üretmek kritik hale gelmektedir. Bu durum, platformları, teknik verimlilik ile hukuki şeffaflık gereklilikleri arasındaki boşluğu kapatarak içerik denetimi için “açıklanabilir yapay zekâ” (*Explainable Artificial Intelligence-XAI*) geliştirmeye zorlamaktadır.

6. Çok Büyük Çevrimiçi Platformlara Getirilen Ek Yükümlülükler

DSA, aylık aktif kullanıcı sayısı 45 milyondan fazla olan çok büyük çevrimiçi platformlara (VLOP’lar) ve çok büyük çevrimiçi arama motorlarına (VLOSE’lar), hizmetlerinin büyük ölçekli etkisi ve toplumsal riskleri nedeniyle ek ve daha sıkı yükümlülükler getirmektedir²⁵². Bu ek yükümlülükler, DSA m. 19 ilâ DSA m. 43 arasında detaylandırılmıştır. Yükümlülükleri incelemeye geçmeden

²⁵¹ Global Freedom of Expression, “Danny Mekić v. X (formerly Twitter) Shadow Banning”, <https://globalfreedomofexpression.columbia.edu/cases/mekic-v-x-formerly-twitter-shadow-banning/>.

²⁵² AB Komisyonu 25 Nisan 2023’te VLOP ve VLOSE olarak değerlendirilecek platformları açıklamıştır. Belirlenen platformlar için bkz. <https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-slops>.

önce bu başlık altında yapılan açıklamalar, sosyal ağ sağlayıcı boyutuyla VLOP'lar için yapılacaktır.

Bu yükümlülüklerden ilki, DSA m. 34'te vücut bulan sistemik risk değerlendirmesidir. VLOP'lar, hizmetlerinin tasarımı veya işleyişinden (algoritmik sistemler dahil olmak üzere) veya hizmetlerinin kullanımından kaynaklanan sistemik riskleri belirlemek, analiz etmek ve değerlendirmek zorundadır. Bu riskler arasında hukuka aykırı içeriğin yayılması, temel haklar üzerindeki olumsuz etkiler, sivil söylem, seçim süreçleri, kamu güvenliğine yönelik tehditler ve toplumsal cinsiyete dayalı şiddet, küçüklerin korunması, zihinsel refahla ilgili olumsuz etkiler bulunmaktadır.

VLOP'lar diğer bir yükümlülük olarak belirlenen sistemik risklere özel olarak uyarlanmış makul, orantılı ve etkili azaltma önlemleri uygulamalıdır. Bu önlemler, hizmet şartlarını, platform tasarımını, tavsiye sistemlerini uyarlamayı, iç süreçleri güçlendirmeyi ve güvenilir işaretleyicilerle iş birliği yapmayı içerebilir. Seçimler sırasında riskleri azaltmaya yönelik özel yönergeler arasında yapay zekâ tarafından üretilen içeriğin (*deepfake*) etiketlenmesi ve güvenilir veri kaynaklarının sağlanması bulunmaktadır.

VLOP'lar DSA m. 37 ve DSA m. 42 uyarınca yıllık bağımsız uyum denetimlerinden geçmek zorundadır. Denetim raporları ve denetim uygulama raporları yıllık olarak yayınlanmalıdır.

DSA'da VLOP'lar için öngörülen diğer bir yükümlülük, araştırmacılara veri erişimi sağlamaktır (DSA m. 40). AB'deki sistemik riskleri incelemek ve azaltma önlemlerini değerlendirmek amacıyla onaylanmış araştırmacılara kamuya açık ve kamuya açık olmayan verilere erişim sağlamalıdır. Bu yükümlülükle çevrimiçi toplumsal etkilerin daha derinlemesine anlaşılmasını sağlamak ve DSA denetimini desteklemek hedeflenmektedir.

VLOP'lar, tavsiye sistemlerinin şeffaflığını DSA m. 27 ve DSA m. 38 uyarınca sağlamalıdır. VLOP'lar tavsiye sistemlerinin ana parametrelerini açıkça açıklamalı ve profillemeye dayanmayan en az bir seçenek sunmalıdır.

Kullanıcıların tavsiye ayarlarını doğrudan ve kolayca değiştirebilmeleri sosyal ağ sağlayıcılarca temin edilmelidir.

VLOP'lar için DSA m. 39'da öngörülen diğer bir yükümlülük, reklam şeffaflığıdır. VLOP olan sosyal ağ sağlayıcı, her bir reklama ilişkin içerik, reklam verenin kimliği, ödeme yapanın kimliği, hedef kitleler ve erişim gibi detaylı bilgileri içeren kamuya açık bir reklam havuzu bulundurmalıdır. Ayrıca VLOP'ların hassas kişisel verilere veya küçüklerin profillemesine dayalı hedefli reklamcılık kullanmaları yasaktır. DSA Gerekçe 95, VLOP'lar tarafından kullanılan reklam sistemlerinin benzersiz riskler taşıdığını ve artan kamu ve düzenleyici denetim gerektirdiğini belirtmektedir.

2024'ün sonlarında yayınlanan ilk sistemik risk değerlendirmelerinin, VLOP'ların sistemik riskleri raporlamasına rağmen platform tasarımının riskteki rolünü yeterince dikkate alınmadığı ve veri/ölçütlerde spesifiklik eksikliği olduğu ifade edilmektedir²⁵³. Veri erişimi hükümleri (DSA m. 40), devrim niteliğinde görülse de platformlardan kaynaklanan tutarsız uygulamalar, erişim kısıtlamaları ve teknik engellerle karşılaşıldığı, araştırmacıların uzun bekleme süreleri ve belirsiz ret kriterleri bildirdiği ifade edilmektedir²⁵⁴.

VLOP statüsündeki sosyal ağ sağlayıcı uygulamalarına bakıldığında:

- Meta: *Meta*, *Facebook* ve *Instagram* için sistemik risk değerlendirme sonuçları ve denetim raporları yayınlamaktadır²⁵⁵. Ancak *Meta* aleyhine EDRI tarafından profillemeye dayanmayan akış seçeneklerini kolayca erişilebilir şekilde sunmadığı gerekçesiyle şikâyetle bulunulmuştur²⁵⁶. *Meta* ayrıca hedefli reklamcılık için “ödeme yap veya kabul et” modeli

²⁵³ KNIGHT-GEORGETOWN INSTITUTE, “Systemic Risk Assessment under the Digital Services Act”.

²⁵⁴ Ayrıntılı bilgi için bkz. <https://en.ejo.ch/recent/cracking-the-code-social-data-access-and-the-dsas-impact-on-disinformation-research>.

²⁵⁵ <https://transparency.meta.com/reports/regulatory-transparency-reports/>.

²⁵⁶ <https://edri.org/our-work/civil-society-files-dsa-complaint-against-meta-for-toxic-profiling-fueled-feeds/>.

nedeniyle tüketici koruma otoritelerinin koordineli eylemiyle karşı karşıya kalmıştır²⁵⁷.

- Google: Google, *Google Arama, Haritalar, Play ve Shopping* için sistemik risk değerlendirme raporları ve denetim raporları yayınlamaktadır²⁵⁸. Google, kişiselleştirilmiş akışları devre dışı bırakma seçenekleri sunmaktadır.
- TikTok: TikTok, yıllık sistemik risk değerlendirme raporları yayınlamaktadır. Avrupa Komisyonu, TikTok hakkında reklam havuzu, tavsiye sistemleri ve araştırmacılar için veri erişimi ile ilgili olası ihlaller nedeniyle resmi soruşturma başlatmıştır²⁵⁹. TikTok, belirgin açıklama veya etiketleme olmaksızın gerçekçi sentetik medyayı yasaklayan politikalara sahiptir²⁶⁰.
- X (eski adıyla Twitter): X, karanlık tasarımlar, reklam şeffaflığı ve araştırmacılar için veri erişimi ile ilgili iddia edilen ihlaller nedeniyle soruşturma altındadır²⁶¹. X, uyumsuzluğa ilişkin ön bulgular ve potansiyel önemli para cezalarıyla karşı karşıya kalmıştır.

DSA'nın açık gerekliliklerine rağmen platformların ilk sistemik risk değerlendirmeleri, temel tasarım özelliklerinin ve algoritmik sistemlerinin sistemik riskleri nasıl oluşturduğunu veya şiddetlendirdiğini yeterince ele almamaktadır. DSA m. 34, "tavsiye sistemlerinin ve diğer ilgili algoritmik sistemlerin tasarımı"nı sistemik risk faktörü olarak açıkça içermektedir²⁶². Ancak

²⁵⁷ Ayrıntılı bilgi için bkz. https://ec.europa.eu/commission/presscorner/detail/en/ip_24_3862.

²⁵⁸ <https://transparencyreport.google.com/report-downloads>.

²⁵⁹ Ayrıntılı bilgi için bkz. https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1223.

²⁶⁰ Ayrıntılı bilgi için bkz. [https://sf16-v.a.tiktokcdn.com/obj/eden-va2/zayvwly_fjulyhwzuhy\[/ljhwZthlaukjlkulzlp/DSA_H2_2024/TikTok-DSA-Risk-Assessment-Report-2023.pdf](https://sf16-v.a.tiktokcdn.com/obj/eden-va2/zayvwly_fjulyhwzuhy[/ljhwZthlaukjlkulzlp/DSA_H2_2024/TikTok-DSA-Risk-Assessment-Report-2023.pdf).

²⁶¹ Ayrıntılı bilgi için bkz. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6709.

²⁶² Maximilian GAHNTZ ve Claire PERSHAN, "Action Recommended: How the Digital Services Act Addresses Platform Recommender Systems", *Verfassungsblog*, 2023, <https://dx.doi.org/10.17176/20230227-185115-0>.

raporlar, platformların içerik odaklı zararlara odaklanma eğiliminde olduğunu, oysa etkileşimi maksimize eden tasarımlarının (örneğin, zihinsel sağlık sorunlarına, dezenformasyon yayılımına veya bağımlılığa yol açan Meta'nın akış tasarımı) nasıl katkıda bulunduğunu yeterince incelemediğini göstermektedir²⁶³. Bu durum, platformların sistemik riski yüzeysel olarak yorumlayarak temel yeniden tasarımlardan kaçınabileceğini düşündürmekte ve DSA'nın amacını tam olarak yerine getirmede kritik bir boşluk oluşturmaktadır.

Araştırmacılar için veri erişimi zorunluluğu getirilmiş olsa da bağımsız araştırmacıların platform verilerine erişimi önemli bir zorluk olmaya devam etmekte ve sistemik risklerin etkin dış denetimini engellemektedir. DSA m. 40, onaylanmış araştırmacılara veri erişimi sağlamaktadır. Diğer bir ifadeyle platformların verilerine erişim, platformların kendi değerlendirmelerini doğrulamak ve sistemik riskleri anlamak için kritik öneme sahiptir. Ancak uygulamada tutarsızlıklar yaşanmaktadır. Platformlar teknik engeller, erişim kısıtlamaları ve şeffaf olmayan onay süreçleri uygulamaktadır. Bu “veri erişim boşluğu”, güçlü platformları sorumlu tutmak için hayati önem taşıyan dış denetimi ciddi şekilde sınırlamakta ve DSA'nın daha geniş şeffaflık hedeflerini baltalayabilmektedir. Avrupa Komisyonu'nun yetkilendirilmiş eylemler aracılığıyla prosedürleri netleştirme çabaları sorunu tam anlamıyla çözmeye yetmemektedir.

Küçükleri hedefleyen reklamcılığın profillemeye dayalı olarak açıkça yasaklanması (DSA m. 28), açık ve yüksek etkili bir yükümlülüktür. Ancak uygulanması yaş doğrulama ve platform tasarımındaki zorluklarla karşılaşmaktadır. DSA m. 28 ve m. 39, küçükleri manipülatif reklamcılık uygulamalarından korumayı doğrudan hedeflemektedir. Ayrıca birçok platformun temel iş modeli, kapsamlı veri toplama ve profillemeye

²⁶³ KNIGHT-GEORGETOWN INSTITUTE, “Systemic Risk Assessment under the Digital Services Act”.

dayanmaktadır²⁶⁴. Bu durum, DSA'nın koruyucu amacı ile platformların ticari teşvikleri arasında bir çatışma meydana getirmekte yaş doğrulama ve küçükler için veri minimizasyonu için gelişmiş teknik çözümler gerektirmektedir.

7. Tüketicileri Korumaya Yönelik Hükümler

DSA, çevrimiçi platformlarda tüketicileri korumaya yönelik çeşitli hükümler de içermektedir. Bu hükümler, içerik denetiminin ötesine geçerek özellikle çevrimiçi pazaryerleri, reklam şeffaflığı ve “karanlık tasarımlar” gibi alanlarda adil ticaret uygulamalarını ve kullanıcı yetkilendirmesini sağlamayı hedeflemektedir. Bu hükümler, DSA m. 29-32 arasında yer almaktadır.

DSA m. 30'da çevrimiçi pazaryerleri için hüküm sevk edilmiştir. Bu hükümle hukuka aykırı ürün ve hizmetlerin çevrimiçi satışıyla mücadele etmek için çevrimiçi pazaryerlerine özel yükümlülükler getirilmektedir. Bu hükümler tacirlerin izlenebilirliğine ilişkin yükümlülükleri de içermektedir.

Tüketicileri korumaya yönelik diğer hükümler ise yukarıda açıklanan reklam şeffaflığına ilişkin DSA m. 29 ve DSA m. 39 hükümleridir. Buna göre platformlar, reklamların açık ve anlaşılır bilgilerini sağlamak zorundadır. Bu bilgiler, reklamın bir reklam olduğu gerçeğini, reklamın kimin adına sunulduğunu ve ödeme yapanın kimliğini içermelidir. VLOP'lar, her bir reklama ilişkin detaylı bilgileri içeren kamuya açık bir reklam havuzu (DSA m. 39) bulundurmaktadır.

DSA m. 28 ve DSA m. 32 uyarınca küçüklerin hizmetlerini kullandığından makul ölçüde emin olan sosyal ağ sağlayıcılar, çocuklar için yüksek düzeyde gizlilik, güvenlik ve emniyet sağlamalıdır. Bu kapsamda küçüklerin kişisel verilerinin profillenmesine dayalı hedefli reklamcılık kullanmaları yasaktır. VLOP'lar, küçüklerin zihinsel ve fiziksel refahına yönelik riskleri değerlendirmeli ve azaltmalıdır.

²⁶⁴ <https://edri.org/our-work/civil-society-files-dsa-complaint-against-meta-for-toxic-profiling-fueled-feeds/>.

DSA m. 25, “karanlık tasarımlar” (*dark patterns*) olarak bilinen yanıltıcı arayüzleri ve kullanıcıları yanıltmayı amaçlayan uygulamaları yasaklamaktadır. Bu hüküm, kullanıcıların özerk ve bilinçli seçimler yapmasını sağlamayı amaçlamaktadır. DSA Gerekçe 67, karanlık tasarımları, hizmet alıcılarının özerk ve bilinçli seçimler yapma yeteneğini kasıtlı veya etkili bir şekilde bozan veya zayıflatan uygulamalar olarak tanımlamaktadır. DSA Gerekçe 81, küçükleri yaşlarına uygun olmayan içerik ve bağımlılıktan korumanın önemini vurgulamaktadır.

DSA’nın karanlık tasarımlara karşı çerçevesinin parçalı olduğu ve birleşik bir hukuki tanım eksikliği nedeniyle hukuki belirsizliğe ve tutarsız uygulamaya yol açabileceğini vurgulanmaktadır²⁶⁵. DSA m. 25’ten Haksız Ticari Uygulamalar Direktifi (UCPD- *Unfair Commercial Practices Directive*) ve AB Genel Veri Koruma Tüzüğü (GDPR-*General Data Protection Regulation*) kapsamındaki uygulamaların hariç tutulması, potansiyel boşluklar oluşturmaktadır²⁶⁶. Çocuklara yönelik web sitelerinin önemli bir yüzdesinin izleyiciler ve hedefli reklamlar içerdiği, bunun da gizlilik düzenlemelerine uyumsuzluk gösterdiği ifade edilmektedir²⁶⁷.

Tüketicileri korumaya yönelik sosyal ağ sağlayıcı uygulamalarına bakıldığında:

- Amazon: Amazon, hukuka aykırı ürünlerle mücadele etmek için satıcı doğrulaması ve ürün güvenliği/uyumu için sağlam proaktif kontroller kullanmaktadır. Sistemleri, satıcı kimliklerini doğrulamak ve hesapları

²⁶⁵ EUROPEAN PARLIAMENT, “Regulating Dark Patterns in the EU: Towards Digital Fairness”, 2025, [https://www.europarl.europa.eu/RegData/etudes/ATAG/2025/767191/EPRS_ATA\(2025\)767191_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2025/767191/EPRS_ATA(2025)767191_EN.pdf).

²⁶⁶ EUROPEAN PARLIAMENT, “Regulating Dark Patterns in the EU: Towards Digital Fairness”.

²⁶⁷ Zahra MOTI vd., *Targeted and Troublesome: Tracking and Advertising on Children’s Websites*, 2023, <https://doi.org/10.48550/arXiv.2308.04887>.

dolandırıcılık açısından izlemek için gelişmiş teknoloji ve insan inceleyicileri kullanmaktadır²⁶⁸.

- Meta: Meta, profillemeye dayanmayan akış seçeneklerini kolayca erişilebilir şekilde sunmayarak DSA kullanıcı korumalarını ihlal ettiği gerekçesiyle şikayetlerle karşı karşıya kalmıştır²⁶⁹. Ayrıca, tüketici gruplarının yanıltıcı ve tüketici/veri koruma hukukunu ihlal ettiğini savunduğu “ödeme yap veya kabul et” (*pay or consent*) modeli nedeniyle incelemeye alınmıştır²⁷⁰.
- Google: Google, kişiselleştirilmiş akışları devre dışı bırakma seçenekleri sunmaktadır. Google Ad Manager ve AdSense, reklam veren kimliği ve hedefleme parametreleri dahil olmak üzere reklam içi şeffaflık bilgileri için kontroller sağlamaktadır.
- TikTok: TikTok, reklam havuzunun şeffaflığı (DSA m. 39) yükümlülüğünü ihlal etmesi nedeniyle soruşturma altındadır²⁷¹. Ayrıca TikTok, ticari içeriğin daha net tanımlanması dahil olmak üzere AB reklamcılık ve tüketici koruma kurallarına uyum sağlamayı taahhüt etmiştir²⁷².
- X (eski adıyla Twitter): X, yukarıda da ifade edildiği üzere karanlık tasarımlar ve reklam şeffaflığı nedeniyle soruşturma altındadır. AB Komisyonu, X’in premium abonelik paketini, mavi tiklerin doğrulama olmaksızın meşruiyet katması ve potansiyel olarak yanlış bilgiyi teşvik etmesi nedeniyle aldatıcı bulmuştur²⁷³.

²⁶⁸ Ayrıntılı bilgi için bkz. <https://trustworthyshopping.aboutamazon.com/digital-services-act-dsa-amazon-eu-store-transparency-report>.

²⁶⁹ <https://edri.org/our-work/civil-society-files-dsa-complaint-against-meta-for-toxic-profiling-fueled-feeds/>.

²⁷⁰ Ayrıntılı bilgi için bkz. https://ec.europa.eu/commission/presscorner/detail/en/ip_24_3862.

²⁷¹ Ayrıntılı bilgi için bkz. https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1223.

²⁷² Ayrıntılı bilgi için bkz. https://ec.europa.eu/commission/presscorner/detail/en/ip_22_3823.

²⁷³ Ayrıntılı bilgi için bkz. https://ec.europa.eu/commission/presscorner/detail/en/ip_24_3761.

DSA'nın açıkça yasaklamasına rağmen karanlık tasarımlara karşı etkinliği, mevcut daha geniş AB düzenlemeleriyle etkileşimi nedeniyle engellenmekte ve potansiyel olarak tutarsız uygulamalara yol açmaktadır. DSA m. 25, karanlık tasarımları açıkça yasaklamaktadır. Ancak UCPD ve GDPR kapsamındaki uygulamaları hariç tutulmaktadır²⁷⁴. Bu durum, bir karanlık tasarımın özel niteliğine (örneğin, gizlilik manipülasyonu veya ticari aldatma) bağlı olarak farklı hukuki çerçeveler altında değerlendirilebileceği anlamına gelmektedir. Bu farklılık, hukuki belirsizlik meydana getirmektedir. Bu durum, DSA'nın manipülatif tasarım üzerindeki etkisini azaltabilecektir.

II) YAPAY ZEKÂ KANUNU (AI ACT)

Birinci bölümde hakkında bilgi verilen ve 21. yüzyılın oyun değiştirici gücü olan yapay zekâ, AB dahil tüm dünyada etkisini giderek artırmaktadır. Bu teknoloji insan doğası gereği faydalı, olumlu iş ve eylemler için kullanılabildiği gibi olumsuz etkiye sahip iş ve eylemlerde de kullanılabilmektedir. Bu teknoloji, ekonomik açıdan çeşitli sektörde teknolojiyi kullananları lider konuma getirme potansiyeline sahiptir.

AB, bu teknoloji konusunda Birlik düzeyinde yeknesak kurallar ortaya koyarak yapay zekâ alanında lider olmayı hedeflemektedir²⁷⁵. Bu doğrultuda AB, Yapay zekâ ile ilgili uyumlaştırılmış kuralları belirleyen ve (AT) 300/2008, (AB) 167/2013, (AB) 168/2013, (AB) 2018/858, (AB) 2018/1139 ve (AB) 2019/2144 sayılı Tüzükleri ve 2014/90/AB, (AB) 2016/797 ve (AB) 2020/1828 sayılı Direktifleri değiştiren 13 Haziran 2024 tarihli Avrupa Parlamentosu ve Konseyi (AT) 2024/1689 Sayılı Tüzüğü'nü (AI Act-Yapay Zekâ Kanunu) kabul etmiştir.

²⁷⁴ EUROPEAN PARLIAMENT, "Regulating Dark Patterns in the EU: Towards Digital Fairness".

²⁷⁵ EUROPEAN PARLIAMENT ve COUNCIL OF THE EUROPEAN UNION, "Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)", 2024, Gerekçe 2, <http://data.europa.eu/eli/reg/2024/1689/oj/eng>.

Çalışmanın bu kısmında inceleme konusuyla sınırlı olarak AI Act ile ilgili açıklamalar yapılacaktır. Bu doğrultuda öncelikle AI Act düzenlemesinin gerekliliği ve amacı üstünde durulacaktır. Devamında bu düzenlemenin benimsediği risk temelli yapay zekâ yaklaşımı ve sınıflandırması açıklanacaktır. Bu başlıkta son olarak yüksek riskli ve belirli yapay zekâ sistemleri için AI Act'te öngörülen yasal gereklilikler açıklanacaktır.

A. DÜZENLEMENİN GEREKLİLİĞİ VE AMACI

Yapay Zekâ Kanunu (AI Act), AB'nin dijital stratejisinin önemli bir parçası olarak yapay zekâ (AI) sistemlerinin geliştirilmesi ve kullanılmasında güvenli ve güvenilir koşullar sağlamayı hedeflemektedir. Bu düzenlemenin ardındaki temel motivasyonlar, kabul edilme zaman çizelgesi ve nihai amaçları, kronolojik bir sıra izlenerek aşağıda detaylandırılmıştır.

AB, yapay zekânın sağlık hizmetleri, ulaşım, üretim ve enerji gibi birçok alanda önemli faydalar sağlayabileceğini kabul etmekle birlikte güvenlik, emniyet ve temel haklar açısından potansiyel riskler taşıdığını da fark etmiştir²⁷⁶. Bu riskler arasında yanlışlık, ayrımcılık, gizlilik ihlalleri ve yapay zekânın etik sonuçları yer almaktadır. Bu endişeler, kapsamlı bir düzenleyici çerçeveye duyulan ihtiyacı doğurmuştur.

AB'nin yapay zekâyâ yaklaşımı, "mükemmeliyet ve güven" üzerine odaklanmış, araştırma ve endüstriyel kapasiteyi artırmayı hedeflerken güvenlik ve temel haklara saygıyı da güvence altına almıştır²⁷⁷.

- Şubat 2020: Avrupa Komisyonu, "mükemmeliyet ve güvene Avrupa yaklaşımı" başlıklı Yapay Zekâ Beyaz Kitabı'nı yayınlayarak güvenilir

²⁷⁶ EUROPEAN PARLIAMENT ve COUNCIL OF THE EUROPEAN UNION, "Artificial Intelligence Act (AI Act)", Gereke 4-5.

²⁷⁷ Ayrıntılı bilgi için bkz. <https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence>.

yapay zekâ için bir çerçeve vizyonunu ve temel haklara yönelik riskleri ortaya koymuştur²⁷⁸. Bu, bir istişare sürecini başlatmıştır.

- Ekim 2020: Avrupa Parlamentosu, etik, hukuki sorumluluk (yüksek riskli yapay zekâ için katı sorumluluk çağrısı yaparak) ve fikri mülkiyet konularını kapsayan üç yapay zekâ kararı kabul etmiştir²⁷⁹.
- Nisan 2021: Avrupa Komisyonu, risk temelli bir yapay zekâ sınıflandırma sistemi oluşturan ilk AB Yapay Zekâ Kanunu teklifini sunmuştur²⁸⁰. Bu, Avrupa yapay zekâ yaklaşımını teşvik eden bir İletişim ve Yapay Zekâ Koordineli Planı'nın gözden geçirilmesi dahil olmak üzere daha büyük bir yapay zekâ paketinin parçasıydı²⁸¹.
- Ekim 2021: Avrupa Parlamentosu, ceza hukukunda yapay zekâyâ ilişkin bir karar kabul ederek “açık kırmızı çizgiler” belirlemiştir²⁸².
- 13 Mart 2024: Avrupa Parlamentosu, AI Act'i onaylamıştır²⁸³.
- 21 Mayıs 2024: AB Konseyi, AI Act'i resmi olarak kabul etmiştir²⁸⁴.
- 12 Temmuz 2024: AI Act, AB Resmî Gazetesi'nde yayınlanmıştır²⁸⁵.
- 1 Ağustos 2024: AI Act AB Resmî Gazetesi'nde yayımlanmasını takip eden 20. günde yürürlüğe girmiştir.

²⁷⁸ https://commission.europa.eu/document/d2ec4039-c5be-423a-81ef-b9e44e79825b_en.

²⁷⁹ <https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-white-paper-artificial-intelligence-and-follow-up?sid=8501>.

²⁸⁰ İlk teklif metni için bkz. <https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence>.

²⁸¹ Plan hakkında ayrıntılı bilgi için bkz. <https://digital-strategy.ec.europa.eu/en/library/coordinated-plan-artificial-intelligence-2021-review>.

²⁸² Ayrıntılı bilgi için bkz. [https://oeil.secure.europarl.europa.eu/oeil/en/procedure-file?reference=2020/2016\(INI\)](https://oeil.secure.europarl.europa.eu/oeil/en/procedure-file?reference=2020/2016(INI)).

²⁸³ <https://eur-lex.europa.eu/eli/C/2025/1027/oj/eng>.

²⁸⁴ <https://www.consilium.europa.eu/en/press/press-releases/2024/05/21/artificial-intelligence-ai-act-council-gives-final-green-light-to-the-first-worldwide-rules-on-ai/>.

²⁸⁵ https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202401689.

AI Act, kademeli bir uygulama yaklaşımı benimsemektedir:

- 2 Şubat 2025: “Yasaklı yapay zekâ uygulamaları” ve yapay zekâ okuryazarlığına ilişkin hükümler yürürlüğe girmiştir.
- 2 Ağustos 2025: Yönetişim yapısı, cezalar ve genel amaçlı yapay zekâ (GPAI-*General Purpose Artificial Intelligence Model*) modelleri sağlayıcıları için yükümlülükler yürürlüğe girmiştir.
- 2 Ağustos 2026: Yüksek riskli yapay zekâ sistemleri ve şeffaflık riski taşıyan sistemler dahil olmak üzere hükümlerin ana kısmı yürürlüğe girecektir.
- 2 Ağustos 2027: Yasanın tam olarak uygulanması başlayacaktır.

AI Act Gerekçe 25, insan odaklı ve güvenilir yapay zekâyı teşvik etmenin, sağlık, güvenlik ve temel hakların yüksek düzeyde korunmasını sağlamanın, zararlı yapay zekâ etkilerine karşı koruma sağlamanın ve inovasyon, bilim ve Ar-geyi desteklemenin önemini vurgulamaktadır.

AI Act’ın temel amacı, AB tek pazarında güvenli ve güvenilir yapay zekâ sistemlerinin geliştirilmesini ve benimsenmesini teşvik ederken AB vatandaşlarının sağlığını, güvenliğini ve temel haklara saygıyı güvence altına almaktır²⁸⁶.

AI Act’ın temel hedefleri şunlardır:

- Tüketicileri ve temel haklarını daha etkin bir şekilde korumak.
- Yapay zekâ sistemi sağlayıcıları ve uygulayıcıları için açık sorumluluklar tanımlamak.
- Hukuka aykırı içerik ve ürünlerle, nefret söylemi ve dezenformasyonla mücadele etmek.

²⁸⁶ EUROPEAN PARLIAMENT ve COUNCIL OF THE EUROPEAN UNION, “Artificial Intelligence Act (AI Act)”, Gerekçe 1.

- Daha iyi raporlama ve denetimle daha fazla şeffaflık sağlamak.
- AB iç pazarında inovasyonu, büyümeyi ve rekabet gücünü teşvik etmek.
- Yapay zekâ sistemlerinin güvenli, şeffaf, izlenebilir, ayrımcı olmayan ve çevre dostu olmasını sağlamak, insan denetiminde olmalarını temin etmek.
- Avrupa'yı yapay zekâ yönetiminde küresel bir lider ve veri konusunda "trend belirleyici" olarak konumlandırmak.

AB Komisyonu'nun Nisan 2025 tarihli "Yapay Zekâ Kıta Eylem Planı", AB'yi küresel bir lider haline getirerek yapay zekâ geliştirme ve benimsemeyi güçlendirmeyi amaçlamaktadır. Bu plan, bilişim altyapısı, veri erişimi, inovasyonu teşvik etme, becerileri güçlendirme ve düzenleyici uyum/basitleştirme konularına odaklanmaktadır²⁸⁷.

AI Act, yapay zekâ sistemleri için dünyanın ilk kapsamlı yasal çerçevesi olarak kabul edilmektedir²⁸⁸. Düzenleme, AB'nin teknoloji ve dijital politikalarda yüksek etik standartlara ve temel haklara öncelik verme konusundaki uzun süredir devam eden yaklaşımını yansıtmaktadır. AB'nin düzenleme odaklı yaklaşımının diğer bölgelere kıyasla inovasyonu engelleyebileceği savunulmaktadır²⁸⁹. Ancak şeffaflık gerekliliklerinin yapay zekâ inovasyonlarının patentlenebilirliğini engellemediğini savunanlar da bulunmaktadır²⁹⁰. AI Act,

²⁸⁷ Ayrıntılı bilgi için bkz. EUROPEAN COMMISSION, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions AI Continent Action Plan", 2025, <https://digital-strategy.ec.europa.eu/en/library/ai-continent-action-plan>.

²⁸⁸ Salih KARADENİZ, "Avrupa Birliği Yapay Zekâ Kanunu'nun Risk Grupları ve İlgililerin Yükümlülükleri Bağlamında İncelenmesi", *Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi* 29, sy 1 (2025): 312, <https://doi.org/10.34246/ahbvuhfd.1541455>.

²⁸⁹ Raluca CSERNATONI, "The EU's AI Power Play: Between Deregulation and Innovation", Carnegie Europe, 2025, 2, <https://carnegieendowment.org/research/2025/05/the-eus-ai-power-play-between-deregulation-and-innovation?lang=en>.

²⁹⁰ Luca HOLST vd., "The Impact of the EU AI Act's Transparency Requirements on AI Innovation", conference paper presented de 19th International Conference on Wirtschaftsinformatik, 2024, 7, <https://www.fim-rc.de/Paperbibliothek/Veroeffentlicht/4979/id-4979.pdf>.

inovasyonu teşvik etme ile kullanıcıları ve haklarını koruma arasında bir denge kurmayı amaçlamaktadır²⁹¹. *Karadeniz*, AI Act'ın AB tarafından öncü bir düzenleme olarak kabul edildiğini ve AB değerleriyle uyumlu, güvenli ve etik yapay zekâ geliştirme sağlamak için risk temelli bir yaklaşım benimsediğini belirtmektedir²⁹².

AI Act'ın küresel bir standart belirleme (Brüksel Etkisi) hedefi, düzenlemenin Avrupa'daki inovasyonu ve rekabet gücünü engelleyebileceği endişeleriyle karşı karşıyadır²⁹³. AB, yapay zekâ yönetiminde “küresel bir lider” ve “trend belirleyici” olmayı açıkça hedeflemektedir²⁹⁴. Bu “önce düzenleme” yaklaşımı, normatif bir güç projeksiyonu biçimidir. Doktrinde özellikle yüksek riskli sistemler için kapsamlı ve potansiyel olarak külfetli uyum gerekliliklerinin, Avrupalı startup'ları dezavantajlı duruma düşürebileceği ve bir “düzenleyici geri çekilmeye” veya inovasyonun başka yerlere kaymasına yol açabileceği endişeleri dile getirilmektedir²⁹⁵. Bu durum, AB'nin etik liderliği teknolojik çeviklik pahasına mı önceliklendirdiği, yoksa her ikisini birden başarabileceği mi sorusunu ortaya koyan temel bir çatışma meydana getirmektedir.

AI Act'ın kademeli uygulama zaman çizelgesi, sektörün uyum sağlamasına ve sürekli iyileştirmelere olanak tanıyan adaptif bir düzenleyici stratejiyi yansıtmaktadır. AI Act, farklı hükümler için birden fazla uygulama tarihine sahiptir. Bu kademeli geçiş, işletmelere yüksek riskli yapay zekâ gibi karmaşık yükümlülüklerle hazırlanmak için daha fazla zaman tanımaktadır. Ayrıca Avrupa

²⁹¹ Martin EBERS, “Truly Risk-Based Regulation of Artificial Intelligence: How to Implement the EU's AI Act”, *Stanford Law School*, sy EU Law Working Papers No: 101 (2024): 7, <https://law.stanford.edu/publications/no-101-truly-risk-based-regulation-of-artificial-intelligence-how-to-implement-the-eus-ai-act/>.

²⁹² KARADENİZ, “Avrupa Birliği Yapay Zekâ Kanunu'nun Risk Grupları ve İlgililerin Yükümlülükleri Bağlamında İncelenmesi”, 320.

²⁹³ KARADENİZ, “Avrupa Birliği Yapay Zekâ Kanunu'nun Risk Grupları ve İlgililerin Yükümlülükleri Bağlamında İncelenmesi”, 310.

²⁹⁴ EUROPEAN PARLIAMENT ve COUNCIL OF THE EUROPEAN UNION, “Artificial Intelligence Act (AI Act)”, Gerekçe 8.

²⁹⁵ CSERNATONI, “The EU's AI Power Play”, 7.

Komisyonu'nun daha fazla yönerge yayınlaması ve istişarelerde bulunması için bir fırsat sağlamaktadır. Bu da ilk uygulamanın gelecekteki ayarlamalara tecrübe kattığı bir “düzenleyici öğrenme” yaklaşımını ortaya koymaktadır. Bu esneklik, yapay zekâ teknolojisinin hızlı evrimine pragmatik bir yanıt olarak değerlendirilmektedir.

Son dönemdeki tartışmalar, AI Act'in basitleştirilmesi yönünde bir baskı olduğunu göstermektedir. Bu basitleştirme çabası, sivil toplum arasında gizlilik ve tüketici, işgücü ve çevresel güvenceleri sulandırabileceği ve dikkatle inşa edilmiş hukuki korumaları ortadan kaldıracabileceği endişelerini doğurmaktadır²⁹⁶.

B. RİSK TEMELLİ YAPAY ZEKÂ YAKLAŞIMI

AI Act, yapay zekâ sistemlerinin düzenlenmesinde “risk temelli bir yaklaşım (*risk-based approach*) benimsemektedir. Bu yaklaşım, yapay zekânın farklı kullanım durumlarının sağlık, güvenlik ve temel haklar üzerindeki potansiyel zararlarını dikkate alarak risk seviyesine göre farklı yükümlülükler getirmeyi amaçlamaktadır.

AI Act, yapay zekâ düzenlemesinde orantılı bir risk temelli yaklaşım benimsemektedir²⁹⁷. Bunun temel nedeni, yapay zekâ sistemlerinin sağlık, güvenlik ve temel haklar açısından farklı risk seviyeleri taşıdığının kabul edilmesidir. Topluma zarar verme riski ne kadar yüksekse kurallar da o kadar katılaşmaktadır. AI Act, yatay bir yasama felsefesiyle yapay zekâ sistemlerinin amaçlanan kullanımlarına odaklanmakta ve tüm sektörlerle ve endüstrilere uygulanmaktadır. Bu yaklaşım, aşırı düzenlemeyi önlemeyi, aynı zamanda güvenlik, şeffaflık, sürdürülebilirlik sağlamayı ve ayrımcı uygulamaları engellemeyi hedeflemektedir. İnovasyon ile etik sorumluluk arasında bir denge kurmayı amaçlamaktadır.

²⁹⁶ CSERNATONI, “The EU's AI Power Play”, 6.

²⁹⁷ EUROPEAN PARLIAMENT ve COUNCIL OF THE EUROPEAN UNION, “Artificial Intelligence Act (AI Act)”, Gerekeçe 26.

AI Act, yapay zekâ sistemlerini kabul edilemez risk (*unacceptable risk*), yüksek risk (*high risk*), sınırlı risk (*limited risk*) ve minimal risk olmak üzere dört risk kategorisine ayırmaktadır²⁹⁸.

Uygulamada risk temelli yaklaşımın uygulanmasındaki zorluklara dikkat çekilmektedir. AppliedAI tarafından 2023'te yapılan bir çalışma, incelenen 100'den fazla yapay zekâ sisteminin %18'inin yüksek riskli, %42'sinin düşük riskli olduğunu ve %40'ının ise belirsiz olduğunu ortaya koymuştur²⁹⁹. Bu belirsizlik, yatırım ve inovasyonu yavaşlatmaktadır³⁰⁰. Bazı uygulamaların sınıflandırma boşluklarından düşebileceği veya kabul edilemez risk kriterlerinin belirsiz olduğu yönünde endişeler dile getirilmiştir.

AppliedAI tarafından yapılan çalışma, incelenen yapay zekâ sistemlerinin %40'ının risk sınıflandırmasının "belirsiz" olduğunu ortaya koymaktadır. Bu belirsizlik, AI Act'in "hukuki kesinlik" sağlama hedefine ters düşmektedir. İşletmeler, bir yapay zekâ sisteminin risk seviyesinden emin olmadıklarında aşırı (yüksek riskli olduğunu varsayarak) uyum sağlayabilir veya yatırım yapmaktan çekinebilir. Bu durum maliyetleri artırabilir ve inovasyonu engelleyebilir³⁰¹. Bu durum, risk temelli yaklaşımın teorik olarak iyi niyetli olmasına rağmen pratikte net sınıflandırma konusunda önemli zorluklarla karşılaştığını ve Avrupa Komisyonu'nun daha fazla yönerge veya açıklama yapması gerektirdiğini göstermektedir.

²⁹⁸ KARADENİZ, "Avrupa Birliği Yapay Zekâ Kanunu'nun Risk Grupları ve İlgililerin Yükümlülükleri Bağlamında İncelenmesi", 319; EBERS, "Truly Risk-Based Regulation of Artificial Intelligence: How to Implement the EU's AI Act", 6; Doktrinde üçlü sınıflandırma da yapılmaktadır. Ayrıntılı bilgi için bkz. Mesut Serdar ÇEKİN vd., *Veri Hukuku*, 1. Baskı (On İki Levha Yayıncılık, 2023), 69-73.

²⁹⁹ INITIATIVE FOR APPLIED ARTIFICIAL INTELLIGENCE, "AI Act: Risk Classification of AI Systems from Practical Perspective", 2023, 12-13, <https://aai.frb.io/assets/files/AI-Act-Risk-Classification-Study-appliedAI-March-2023.pdf>.

³⁰⁰ INITIATIVE FOR APPLIED ARTIFICIAL INTELLIGENCE, "AI Act: Risk Classification of AI Systems from Practical Perspective", 16.

³⁰¹ INITIATIVE FOR APPLIED ARTIFICIAL INTELLIGENCE, "AI Act: Risk Classification of AI Systems from Practical Perspective", 6.

AI Act'in risk temelli yaklaşımı, öncelikli olarak bireysel yapay zekâ sistemlerine odaklanmakta ancak birden fazla düşük riskli sistemin etkileşiminden kaynaklanabilecek sistemik riskleri göz ardı edebilmektedir. AI Act, bireysel yapay zekâ sistemlerini sınıflandırmaya odaklanmaktadır. Bireysel olarak düşük riskli olan birkaç sistem, bir araya geldiğinde bireyler ve toplum için önemli riskler yaratabilir. Bu durum, mevcut doğrusal, bireysel sistem odaklı risk yaklaşımının karmaşık yapay zekâ ekosistemleri için yetersiz olabileceğini düşündürmektedir.

1. Yasaklı Yapay Zekâ Sistemleri

AI Act m. 5, “kabul edilemez risk” taşıyan belirli yapay zekâ sistemlerinin kullanımını yasaklamaktadır. Bu yasaklar, temel haklara yönelik açık tehditleri ortadan kaldırmayı amaçlamaktadır.

AI Act, insanların güvenliği, geçim kaynakları ve temel hakları için açık bir tehdit olarak kabul edilen belirli yapay zekâ sistemlerinin kullanımlarını yasaklamaktadır. Bu uygulamalar, doğası gereği zararlı veya etik dışı kabul edilmektedir. Yasaklı yapay zekâ uygulamalarına ilişkin hükümler, 2 Şubat 2025 tarihinde yürürlüğe girmiştir. Uyumsuzluk durumunda, operatörün³⁰² dünya genelindeki yıllık cirosunun %7'sine kadar veya 35 milyon Euro'ya kadar para cezaları uygulanabilmektedir.

³⁰² AI Act m. 3/8: “‘operatör’ bir sağlayıcı, ürün üreticisi, yerleştirici, yetkili temsilci, ithalatçı veya dağıtıcı anlamına gelir. (‘operator’ means a provider, product manufacturer, deployer, authorised representative, importer or distributor)”.

Deployer kavramı bu çalışmanın yazarı tarafından çevrilirken dağıtıcı olarak değil, yerleştirici olarak çevrilmiştir. Şöyle ki *deployer* kavramı genellikle yazılım ve teknoloji dünyasında kullanılan bir terimdir. Yazılım projelerinde son kullanıcıya ulaşması (canlıya alınması) kapsamında “deploy” kavramı kullanılmaktadır. AI Act'te de bu anlamda kullanılmaktadır. Bu sebeple bu kavramın bu düzenleme açısından dağıtım alma, yerleştirme manasında kullanılması isabetli olacaktır. Düzenlemede geçen distribütör kelimesi ise Türkçede aynı şekilde kullanılmakla birlikte deploy kelimesinin Türkçe çevirisi ile aynı olması sebebiyle dağıtıcı olarak çevrilmiştir.

AI Act, 8 uygulamayı açıkça yasaklamaktadır:

1. Zararlı Manipölasyon ve Aldatma: Bir kişinin davranışını önemli ölçüde bozarak fiziksel veya psikolojik zarara neden olan (veya neden olması muhtemel) bilinçaltı teknikler veya kasıtlı manipölatif/aldatacı teknikler kullanan yapay zekâ sistemleri.
2. Zafiyetlerin Sömürülmesi: Belirli bir yaş, fiziksel veya zihinsel engellilik veya sosyal/ekonomik durum nedeniyle belirli bir grup kişinin zafiyetlerini sömürerek davranışlarını önemli ölçüde bozan ve fiziksel veya psikolojik zarara neden olan yapay zekâ sistemleri.
3. Sosyal Puanlama: Gerçek kişilerin sosyal davranışlarına veya kişisel özelliklerine göre belirli bir süre boyunca değerlendirilmesi veya sınıflandırılması, bunun sonucunda ilgili olmayan sosyal bağlamlarda dezavantajlı veya olumsuz muameleye yol açan veya sosyal davranışlarına orantısız/haksız muamele gören yapay zekâ sistemleri.
4. Suç Tahmini: Gerçek kişilerin yalnızca profillemesine veya kişilik özelliklerinin değerlendirilmesine dayanarak gelecekte suç işleme riskini değerlendiren veya tahmin eden yapay zekâ sistemleri. İnsan değerlendirmesini destekleyen objektif gerçeklere dayalı istisnalar mevcuttur.
5. Rastgele Yüz Görüntüsü Kazıma: İnternette veya CCTV görüntülerinden rastgele yüz görüntüsü kazıyarak yüz tanıma veritabanları oluşturma veya genişletme.
6. İşyeri/Eğitimde Duygu Tanıma: İşyeri veya eğitim kurumlarında gerçek kişilerin duygularını çıkarsayan yapay zekâ sistemleri (tıbbi veya güvenlik nedenleri hariç).
7. Hassas Niteliklerin Biyometrik Kategorizasyonu: Biyometrik verilere dayanarak bireyleri ırk, siyasi görüş, sendika üyeliği, dini/felsefi

inançlar, cinsel yaşam veya cinsel yönelim gibi hassas niteliklere göre kategorize etme.

8. Kolluk Kuvvetleri Amacıyla Kamuya Açık Alanlarda Gerçek Zamanlı Uzaktan Biyometrik Tanımlama: Prensipde yasaklanmış olup önceden yargısal/idari izin gerektiren dar, sınırlı istisnalar bulunmaktadır. Bu istisnalar arasında kaçırılan/ticareti yapılan/cinsel istismara uğrayan kişilerin hedefli aranması, yaşam/güvenliğe yönelik ani tehditlerin veya terör saldırılarının önlenmesi ve ciddi suç zanlılarının tespiti yer almaktadır.

Avrupa Komisyonu, 4 Şubat 2025 tarihinde yasaklı yapay zekâ uygulamalarına ilişkin yönergeler yayınlayarak hukuki açıklamalar ve pratik örnekler sunmuştur³⁰³. Açık yasaklamalara rağmen yasaklı uygulamaların geniş ve bazen belirsiz tanımları, yorumlama ve uyum konusunda zorluklar oluşturmakta, potansiyel olarak “yapay zekâ aklama” veya yanlış sınıflandırmaya yol açmaktadır. “Bilinçaltı teknikler”, “zafiyetlerin sömürülmesi” veya “sosyal puanlama” gibi terimler, kesin teknik tanımlardan yoksundur ve bu da hukuki belirsizliğe yol açmaktadır. AB Komisyonu’nun bağlayıcı olmayan yönergeleri bir adım olsa da nihai yorum Avrupa Adalet Divanı’na aittir³⁰⁴. Bu belirsizlik, şirketlerin riski hafife almasına veya sistemleri yanlış sınıflandırmasına, hatta yapay zekâ dışı ürünleri pazarlama amacıyla yapay zekâ aklamaları yapmasına bile yol açabilir. Bu durum, hızla gelişen bir alanda geniş hukuki ilkeleri açık, uygulanabilir teknik standartlara dönüştürmenin zorluğuna işaret etmektedir.

Geniş yasaklar, özellikle veri kazıma ve biyometrik sistemler üzerindeki yasaklar, meşru akademik ve bilimsel araştırmaları olumsuz etkileyebilir. AI Act,

³⁰³ EUROPEAN COMMISSION, “Communication from the Commission Guidelines on Prohibited Artificial Intelligence Practices”, 2025, <https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act>.

³⁰⁴ EUROPEAN COMMISSION, “Communication from the Commission Guidelines on Prohibited Artificial Intelligence Practices”, 1.

araştırmayı desteklemeyi amaçlasa da rastgele yüz görüntüsü kazıma gibi bazı yasaklı uygulamalar, yapay zekâda yaygın olarak kullanılmaktadır. Yapay zekâ sistemi³⁰⁵ tanımının genişliği, araştırma demolarını veya açık kaynak modellerini kapsayabilir. Bu da araştırmacıları uyum yükümlülükleri ve potansiyel para cezalarıyla karşı karşıya bırakabilir³⁰⁶. Bu durum, hassas yapay zekâ alanlarında akademik özgürlük ve inovasyon üzerinde caydırıcı bir etki oluşturabilir ve potansiyel olarak araştırmayı AB dışına itebilir.

2. Yüksek Riskli Yapay Zekâ Sistemleri

AI Act m. 6, yüksek riskli yapay zekâ sistemlerini sınıflandırmakta ve bu sistemlere potansiyel zararları nedeniyle katı yükümlülükler getirmektedir. Bu sınıflandırma, iki ana kritere dayanmaktadır:

1. Ürünlerin Güvenlik Bileşeni: Bir yapay zekâ sistemi, eğer Ek I'de listelenen Birlik uyumlaştırma mevzuatı (örneğin oyuncaklar, tıbbi cihazlar, havacılık, arabalar, asansörler) kapsamında bir ürünün güvenlik bileşeni olarak kullanılmak üzere tasarlanmışsa veya kendisi bir ürün olmakla birlikte bu mevzuat uyarınca üçüncü taraf uygunluk değerlendirmesinden geçmesi gerekiyorsa yüksek riskli kabul edilir.

³⁰⁵ AI Act m. 3/1'e göre "'yapay zekâ sistemi', değişen seviyelerde özerklikle çalışmak üzere tasarlanmış ve konuşlandırıldıktan sonra uyarlanabilirlik gösterebilen ve açık veya örtük hedefler için, aldığı girdiden, fiziksel veya sanal ortamları etkileyebilecek tahminler, içerik, öneriler veya kararlar gibi çıktıları nasıl üreteceğini çıkaran makine tabanlı bir sistem anlamına gelir." ("AI system' means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments"). Tanımın sadece makine öğrenimini değil, mantık ve bilgiye dayalı yaklaşımları da kapsadığı yönünde bkz. EBERS, "Truly Risk-Based Regulation of Artificial Intelligence: How to Implement the EU's AI Act", 34; EUROPEAN PARLIAMENT ve COUNCIL OF THE EUROPEAN UNION, "Artificial Intelligence Act (AI Act)", Gerekeç 12.

³⁰⁶ Alina WERNICK ve Kristof MEDING, *Beware! The AI Act Can Also Apply to Your AI Research Practices*, 2025, 4, <https://arxiv.org/html/2506.03218v1>.

2. Belirli Kullanım Durumları (Ek III): Ek III'te listelenen yapay zekâ sistemleri, sağlık, güvenlik veya temel haklara önemli bir zarar riski oluşturmadıkları sürece yüksek riskli kabul edilir (AI Act m. 6/3).

Bu istisna, yapay zekânın dar bir prosedürel görevi yerine getirmesi, daha önce tamamlanmış bir insan faaliyetinin sonucunu iyileştirmesi, insan değerlendirmesini değiştirmeden veya etkilemeden karar verme kalıplarını tespit etmesi veya Ek III'te listelenen kullanım durumları için ilgili bir hazırlık görevi yapması durumunda uygulanır. Ancak bir yapay zekâ sistemi gerçek kişilerin profillemesini yapıyorsa Ek III'te belirtilen bir sistem olsa bile her zaman yüksek riskli kabul edilir.

Ek III uyarınca yüksek riskli yapay zekâ sistemlerine örnek şunlardır:

- Biyometrik Veriler: Uzaktan biyometrik tanımlama sistemleri, biyometrik kategorizasyon sistemleri (hassas niteliklere dayalı), duygu tanıma sistemleri.
- Kritik Altyapı: Kritik dijital altyapının, karayolu trafiğinin veya su, gaz, ısıtma veya elektrik tedarikinin yönetimi ve işletilmesinde güvenlik bileşeni olarak kullanılan yapay zekâ sistemleri.
- Eğitim ve Mesleki Eğitim: Eğitim kurumlarına erişimi/kabulü belirleyen, öğrenme sonuçlarını değerlendiren, eğitim seviyelerini değerlendiren veya testler sırasında öğrenci davranışlarını izleyen sistemler.
- İstihdam, İşçi Yönetimi ve Serbest Mesleğe Erişim: İşe alım/seçim (örneğin özgeçmiş filtreleme), iş ilişkilerinin koşullarını etkileyen kararlar (terfi/fesih), özelliklere dayalı görev dağılımı veya performans/davranış izleme sistemleri.
- Temel Özel/Kamu Hizmetlerine ve Faydalarına Erişim: Kamu otoriteleri tarafından faydalara (örneğin sağlık, sosyal güvenlik) uygunluğu değerlendirmek için kullanılan sistemler, kredi değerliliği

değerlendirmesi (dolandırıcılık tespiti hariç) veya hayat/sağlık sigortasında risk değerlendirme/siyasetlendirme.

- Kolluk Kuvvetleri: Suç işleme riskini değerlendiren, kanıt güvenilirliğini değerlendiren veya seçim sonuçlarını etkileyen sistemler (siyasi kampanya araçları hariç).
- Göç, İltica ve Sınır Yönetimi: Poligraf, düzensiz göç/sağlık risklerini değerlendiren sistemler veya vize başvurularının otomatik incelenmesi.
- Adalet Yönetimi ve Demokratik Süreçler: Mahkeme kararlarını hazırlayan veya seçim sonuçlarını etkileyen yapay zekâ çözümleri.

Sınıflandırma, potansiyel zararın ciddiyeti ve olasılığı ile hassas alanlardaki kullanımı olmak üzere iki kritere dayanmaktadır. Ek III'teki bir sistemi yüksek riskli olarak kabul etmeyen sağlayıcılar, piyasaya sürmeden önce değerlendirmelerini belgelemeli ve kayıt yükümlülüğüne tabi olmalıdır³⁰⁷. AB Komisyonu, AI Act m. 7 uyarınca Ek III listesini değiştirme yetkisine sahiptir³⁰⁸.

Ek III sistemleri için getirilen “önemli risk” (*significant risk*) istisnası esneklik sağlamayı amaçlasa da tutarsız yorumlama potansiyeli sunmaktadır. AI Act m. 6/3, Ek III'te yer alan yapay zekâ sistemlerinin önemli bir risk oluşturmamaları takdirde yüksek riskli olarak sınıflandırılmamasına izin vermektedir. Bu esneklik olumlu olsa da önemli risk kavramı özneldir. Bu durum, farklı sağlayıcılar veya AB üyesi devletler arasında tutarsız uygulamalara yol açabilir ve uyumlaştırılmış çerçeveyi zayıflatabilir. AB Komisyonu'nun yayımı yaklaşan yönerge ve rehberleri, bu belirsizliği azaltmak için kritik öneme sahip olacaktır.

³⁰⁷ EUROPEAN PARLIAMENT ve COUNCIL OF THE EUROPEAN UNION, “Artificial Intelligence Act (AI Act)”, Gerekçe 53.

³⁰⁸ Avrupa Komisyonu'nun Ek III'ü yapay zekâ teknolojisinin dinamikliği karşısında güncel tutmasının zor olduğu ve AB Komisyonu'nun böyle bir yetkiye sahip olmasının yetki dağılımı açısından endişelere yol açtığı yönünde bkz. EBERS, “Truly Risk-Based Regulation of Artificial Intelligence: How to Implement the EU's AI Act”, 28.

Sağlayıcıların, Ek III kapsamında yer alan bir yapay zekâ sistemini yüksek riskli olarak görmemeleri durumunda değerlendirmelerini belgeleme zorunluluğu, ispat yükünü sağlayıcılara kaydırmakta ve dahili uyum mekanizmalarını gerektirmektedir. Bir sağlayıcı, Ek III'teki yapay zekâ sisteminin yüksek riskli olmadığını düşünüyorsa bu değerlendirmeyi piyasaya sürmeden önce *belgelemek* zorundadır³⁰⁹. Bu, sınıflandırmalarını haklı çıkarma sorumluluğunun sağlayıcıya ait olduğu anlamına gelmektedir. Bu durum, bu tür değerlendirmeleri yapabilecek ve belgeleyebilecek sağlam iç hukuki ve teknik ekipleri gerektirmektedir. Bu da sağlayıcı tarafından düşük riskli kabul edilen sistemler için bile bir uyum yükü eklemektedir.

3. Sınırlı (Düşük) Riskli Yapay Zekâ Sistemleri

AI Act m. 50, sınırlı riskli yapay zekâ sistemleri için diğer risk kategorilerine kıyasla daha hafif ancak yine de önemli şeffaflık yükümlülükleri öngörmektedir. Bu kategori, kişisel etkileşim veya içerik üretimiyle ilgili belirli riskler taşıyan ancak sağlık, güvenlik veya temel haklar üzerinde önemli bir zarar verme olasılığı düşük olan sistemleri kapsamaktadır. AI Act'e göre bu sistemler "şeffaflık riski taşıyan yapay zekâ sistemleri" olarak da adlandırılmaktadır. Bu kategoriye giren sistemler için sadece kapsamlı olmayan şeffaflık yükümlülükleri getirilmiştir.

AI Act m. 50, sınırlı riskli yapay zekâ sistemleri için spesifik şeffaflık yükümlülüklerini belirlemektedir. Bu yükümlülükler, kullanıcıların yapay zekâ ile etkileşimde olduklarında bilinçli olmalarını sağlamayı amaçlamaktadır:

1. Doğrudan İnsanlarla Etkileşim Kuran Yapay Zekâ Sistemleri: Sağlayıcılar, gerçek kişilerin bir yapay zekâ sistemiyle etkileşimde olduklarını bilgilendirmelerini sağlamalıdır. Bu, makul ölçüde iyi bilgilendirilmiş, dikkatli bir kişi açısından açıkça belli olmadığı sürece geçerlidir. Bu yükümlülük, suçların tespiti, önlenmesi, soruşturulması

³⁰⁹ EUROPEAN PARLIAMENT ve COUNCIL OF THE EUROPEAN UNION, "Artificial Intelligence Act (AI Act)", Gerekeçe 53.

veya kovuşturulması için yasal olarak yetkilendirilmiş yapay zekâ sistemleri için geçerli değildir. Örnekler arasında chatbotlar ve dijital asistanlar yer almaktadır.

2. Sentetik İçerik Üreten Yapay Zekâ Sistemleri: Sentetik ses, görüntü, video veya metin içeriği üreten yapay zekâ sistemlerinin sağlayıcıları, sistem çıktılarının makine tarafından okunabilir bir formatta işaretlenmesini ve yapay olarak üretilmiş veya manipüle edilmiş olarak tespit edilebilir olmasını sağlamalıdır. Sağlayıcılar, teknik çözümlerinin teknik olarak mümkün olduğunca etkili, birlikte çalışabilir, sağlam ve güvenilir olmasını sağlamalıdır. Bu yükümlülük, standart düzenleme için yardımcı bir işlev gören veya giriş verilerini önemli ölçüde değiştirmeyen yapay zekâ sistemleri için geçerli değildir.
3. Duygu Tanıma veya Biyometrik Kategorizasyon Sistemleri: Bu sistemleri kullanan uygulayıcılar, maruz kalan gerçek kişileri sistemin işleyişi hakkında bilgilendirmelidir. Bu yükümlülük, suçların tespiti, önlenmesi veya soruşturulması için yasal olarak izin verilen sistemler için geçerli değildir.
4. Deepfake Üreten/Manipüle Eden Yapay Zekâ Sistemleri: Deepfake oluşturan veya manipüle eden yapay zekâ sistemlerinin uygulayıcıları, içeriğin yapay olarak üretildiğini veya manipüle edildiğini açıklamak zorundadır. İçerik açıkça sanatsal, yaratıcı, hicivsel, kurgusal veya benzeri bir eser veya programın parçasıysa şeffaflık yükümlülükleri, eserin gösterimini veya keyfini engellemeyen uygun bir şekilde bu tür üretilmiş veya manipüle edilmiş içeriğin varlığının açıklanmasıyla sınırlıdır.
5. Kamu Yararına Metin Üreten/Manipüle Eden Yapay Zekâ Sistemleri: Kamuyu ilgilendiren konularda bilgi verme amacıyla metin üreten veya manipüle eden yapay zekâ sistemlerinin uygulayıcıları, metnin yapay olarak üretildiğini veya manipüle edildiğini açıklamak zorundadır. Bu

yükümlülük, suçların tespiti, önlenmesi, soruşturulması veya kovuşturulması için yasal olarak izin verilen veya yapay zekâ tarafından üretilen içeriğin insan incelemesinden veya editoryal kontrolden geçtiği durumlarda geçerli değildir.

Şeffaflık, yapay zekâ sistemlerinin uygun izlenebilirlik ve açıklanabilirlik sağlayacak şekilde geliştirilmesi ve kullanılması, insanların bir yapay zekâ sistemiyle iletişim kurduklarının veya etkileşimde bulunduklarının farkında olmalarını sağlamak ve uygulayıcıları yapay zekâ sisteminin yetenekleri ve sınırlamaları hakkında bilgilendirmek anlamına gelmektedir. Bu, yapay zekâ teknolojileri için güvenilir ve şeffaf bir rejim oluşturma anahtarıdır. Doktrinde şeffaflık gerekliliklerinin inovasyonu etkileyebileceği ancak kanun koyucunun temel terimleri netleştirmesi halinde önemli bir etki oluşturmayacağı savunulmaktadır³¹⁰.

Sınırlı riskli yapay zekâ sistemleri için belirlenen şeffaflık yükümlülükleri, kullanıcıların yapay zekâ ile etkileşimde olduklarını anlamalarını sağlamayı amaçlamaktadır. Ancak bu yükümlülüklerin etkinliği, “açıkça belli olma” veya “teknik olarak mümkün olma” gibi kavramların yorumlanmasına bağlıdır. AI Act m. 50, yapay zekâ ile etkileşimin “açıkça belli” olduğu durumlarda bilgilendirme yükümlülüğünden muafiyet tanımaktadır. Bu, sübjektif bir değerlendirme alanı oluşturmaktadır. Bu durum, platformların bu muafiyeti geniş yorumlamasına yol açabilecektir. Ayrıca sentetik içeriğin “makine tarafından okunabilir bir formatta işaretlenmesi ve yapay olarak üretilmiş veya manipüle edilmiş olarak tespit edilebilir olması” gerekliliği, teknik olarak neyin mümkün olduğu ve bunun maliyeti konusunda belirsizlikler içermektedir. Bu durum, düzenlemenin uygulanabilirliğini ve teknolojik gelişmelere ayak uydurma yeteneğini sorgulatabilir.

³¹⁰ HOLST vd., “The Impact of the EU AI Act’s Transparency Requirements on AI Innovation”, 2.

Yapay zekâ tarafından üretilen içeriğin etiketlenmesi, dezenformasyonla mücadele ve kamuoyunun doğru bilgilendirilmesi için kritik öneme sahiptir. Deepfake’ler ve kamu yararına yayınlanan yapay zekâ tarafından üretilmiş metinler için açıklama zorunluluğu, yanlış bilginin yayılmasını önlemeyi ve kullanıcıların içeriğin kaynağı hakkında bilinçli kararlar almasını sağlamayı hedeflemektedir. Bu, özellikle seçim süreçleri gibi hassas dönemlerde yapay zekânın manipülatif potansiyeline karşı bir koruma katmanı oluşturmaktadır. Ancak sanatsal, yaratıcı veya hicivsel içeriklerdeki istisnalar, bu etiketleme yükümlülüğünün sınırlarını belirlemekte ve ifade özgürlüğü ile dezenformasyonla mücadele arasındaki hassas dengeyi yansıtmaktadır.

4. Minimal Riskli Yapay Zekâ Sistemleri

AI Act, yapay zekâ sistemlerini risk seviyelerine göre sınıflandırırken “minimal riskli yapay zekâ sistemleri”ni en düşük risk kategorisine yerleştirmektedir. Bu sistemler, sağlık, güvenlik veya temel haklar üzerinde çok az veya hiç risk oluşturmadığı kabul edilen uygulamaları kapsamaktadır. AI Act’te bu tür sistemler genellikle düzenleme kapsamı dışında bırakılmaktadır.

Minimal riskli yapay zekâ sistemlerine örnek olarak yapay zekâ destekli video oyunları, spam filtreleri ve çevrimiçi alışveriş sitelerindeki ürün tavsiye sistemleri verilebilir. Bu sistemler için AI Act, doğrudan bağlayıcı yükümlülükler öngörmemektedir. Bu doğrultuda işletmeler, gönüllü olarak AI Act’e uyum sağlayabilecektir.

Minimal riskli yapay zekâ sistemlerinin büyük ölçüde düzenleme dışında bırakılması, inovasyonu teşvik etme ve bürokrasiyi azaltma amacını taşımaktadır. AI Act, (AB pazarında mevcut yapay zekâ uygulamalarının çoğunu içeren) minimal riskli sistemleri düzenleme dışı bırakmaktadır. Bu yaklaşım, düzenleyici yükü azaltarak şirketlerin daha az karmaşık yapay zekâ uygulamalarını daha hızlı ve düşük maliyetle geliştirmesine ve piyasaya sürmesine olanak tanımaktadır. Bu, özellikle küçük ve orta ölçekli işletmeler (KOBİ’ler) için inovasyonun önünü açabilir ve yapay zekânın daha geniş bir yelpazede benimsenmesini sağlayabilir.

Ancak minimal riskli sistemlerin düzenleme dışında kalması, gelecekte ortaya çıkabilecek “birleşik riskler” veya “beklenmedik zararlar” için bir boşluk oluşturabilir. AI Act, tek tek minimal riskli sistemlerin kendi başlarına önemli bir risk oluşturmadığını varsaymaktadır. Ancak birden fazla bireysel olarak düşük riskli sistem etkileşime girerek bireyler ve toplum için önemli riskler oluşturabilir. Bu durum, düzenleyici çerçevenin zamanla ortaya çıkabilecek yeni risk senaryolarına karşı esnek ve uyumlu olması gerektiğini göstermektedir.

Risk Kategorisi	Tanım	Örnekler	Uygulanan Yükümlülük Düzeyi
Yasaklı Sistemler	Temel haklara, güvenliğe ve geçim kaynaklarına açık bir tehdit oluşturan, kabul edilemez risk taşıyan AI sistemleri. Doğrudan yasaklanmıştır.	Zararlı manipülasyon ve aldatma, zafiyet sömürüsü, sosyal puanlama, suç tahmini, hedef dışı yüz görüntüsü kazıma, işyeri/ eğitimde duygu tanıma, hassas biyometrik kategorizasyon, kamuya açık alanda gerçek zamanlı uzaktan biyometrik	Yasaklıdır. En yüksek para cezaları uygulanır (küresel cirosunun %7'sine kadar veya 35 milyon Euro)

		tanımlama (istisnalar hariç)	
Yüksek Riskli Sistemler	Sağlık, güvenlik veya temel haklar üzerinde ciddi riskler oluşturabilecek AI sistemleri. İzinlidir ancak katı düzenlemelere tabidir.	Kritik altyapılarda güvenlik bileşenleri (ulaşım, enerji), eğitimde erişim/ değerlendirme (sınav puanlaması), tıbbi cihazlar, işe alım/ çalışan yönetimi (özgeçmiş filtreleme), temel kamu/özel hizmetlere erişim (kredi puanlaması), kolluk kuvvetleri (kanıt güvenilirliği değerlendirmesi), göç/sınır kontrolü (vize başvurusu değerlendirmesi)	Katı Yükümlülükler: Risk yönetimi, veri kalitesi, teknik dokümantasyon, insan denetimi, doğruluk, sağlamlık, siber güvenlik, uygunluk değerlendirmesi, kalite yönetim sistemi

Sınırlı Riskli Sistemler	Kimlik taklidi veya aldatma gibi belirli riskler taşıyabilen, ancak önemli zarar veya temel hak ihlali olasılığı düşük olan AI sistemleri.	Chatbotlar ve dijital asistanlar, sentetik ses/görüntü/video/metin içeriği üreten sistemler (deepfake), kamu yararına metin üreten/manipüle eden sistemler, duygu tanıma sistemleri (eğlence sektöründe)	Şeffaflık Yükümlülükleri: Kullanıcılara yapay zekâ ile etkileşimde olduklarını bildirme, yapay zekâ tarafından üretilen içeriği işaretleme
Minimal Riskli Sistemler	Sağlık, güvenlik veya haklar açısından neredeyse hiç risk taşımayan AI sistemleri.	Yapay zekâ destekli video oyunları, spam filtreleri, çevrimiçi alışveriş sitelerindeki ürün tavsiye sistemleri	Çok Az veya Hiç Düzenleme Yok: Gönüllü davranış kuralları öngörülmektedir

Şema 7: AI Act Risk Kategorileri

C. YAPAY ZEKÂ SİSTEMLERİ İÇİN YASAL GEREKLİLİKLER

Önceki başlıklarda yapay zekânın AI Act ile neden düzenlendiği ve amacı açıklandıktan sonra düzenlemenin bel kemiği olan risk temelli yapay zekâ

yaklaşımı ve risk türleri incelenmiştir. Bu noktadan itibaren AI Act'te yüksek riskli ve belirli yapay zekâ sistemleri için öngörülen gereklilikler açıklanacaktır.

1. Yüksek Riskli Yapay Zekâ Sistemleri İçin Gereklilikler

AI Act, yüksek riskli yapay zekâ sistemleri için bir dizi katı yükümlülük öngörmektedir. Bu gereklilikler, bu sistemlerin sağlık, güvenlik ve temel haklar üzerindeki potansiyel ciddi zararlarını azaltmayı hedeflemektedir. Bu kapsamda önce temel yükümlülüklerden, devamında bazı ek yükümlülükler açıklanacaktır.

AI Act, yüksek riskli yapay zekâ sistemleri sağlayıcılarının yerine getirmesi gereken bir dizi bağlayıcı yükümlülük belirlemektedir. Bu yükümlülükler, yapay zekâ sisteminin tüm yaşam döngüsü boyunca risklerin yönetilmesini ve azaltılmasını sağlamayı amaçlamaktadır:

1. Risk Yönetim Sistemi (m. 9): Sağlayıcılar, sistemin tüm yaşam döngüsü boyunca risk değerlendirmesi ve yönetimi için bir sistem uygulamalıdır. Bu sistem, GDPR'daki Gizlilik Etki Değerlendirmesine (PIA-*Privacy Impact Assessment*) benzer şekilde sürekli risk değerlendirmesi ve azaltma önlemlerini içermelidir.
2. Veri Kalitesi ve Yönetimi (m. 10): Eğitim, doğrulama ve test verilerinin katı kalite ve yönetim kriterlerini karşılaması sağlanmalıdır. Veriler ilgili, yeterince temsil edici, hatasız ve eksiksiz olmalıdır.
3. Teknik Dokümantasyon (m. 11): Sağlayıcılar, sistemin tasarımı, amacı, performans verileri, değişiklik günlüğü ve üretimdeki performansını izleme planı dahil olmak üzere ayrıntılı teknik dokümantasyon hazırlamalı ve güncel tutmalıdır. Bu dokümantasyon, yetkililerin uyumu değerlendirmesine yardımcı olmalıdır.
4. Kayıt Tutma (m. 12): Yapay zekâ sistemi, yaşam süresi boyunca olayları (loglar) otomatik olarak kaydetmeye uygun olmalıdır. Ne zaman kullanıldığı, hangi veritabanını kontrol ettiği ve sonuçları kimin doğruladığı gibi bilgiler örnek verilebilir.

5. Şeffaflık ve Uygulayıcılara Bilgi Sağlama (m. 13): Yüksek riskli yapay zekâ sistemleri, uygulayıcıların sistemin çıktısını yorumlamasını ve uygun şekilde kullanmasını sağlayacak kadar şeffaf olacak şekilde tasarlanmalı ve geliştirilmelidir. Uygulayıcılara sistemin işleyişi, riskleri ve sınırlamaları hakkında net bilgi verilmelidir.
6. İnsan Denetimi (m. 14): Yapay zekâ sistemi, insan denetimine izin verecek şekilde tasarlanmalıdır. İnsan denetçinin sistemin çıktısını yorumlayabilmesi, kullanıp kullanmayacağına karar verebilmesi ve gerekirse çalışmasını durdurabilmesi gerekmektedir. Bu denetim, sağlık, güvenlik veya temel haklara yönelik riskleri önlemeyi veya en aza indirmeyi amaçlamaktadır.
7. Doğruluk, Sağlamlık ve Siber Güvenlik (m. 15): Yüksek riskli yapay zekâ sistemleri, doğru, sağlam ve güvenli olacak şekilde tasarlanmalıdır. Hatalara ve arızalara karşı dirençli olmalı, yedek planları olmalı ve zafiyetlerin kötüye kullanılmasına karşı korunmalıdır.
- CE İşareti ve Uygunluk Değerlendirmesi (m. 16, m. 43, m. 47, m. 48): Sağlayıcılar, yüksek riskli yapay zekâ sistemlerinin piyasaya sürülmeden veya hizmete alınmadan önce ilgili uygunluk değerlendirme prosedüründen geçmesini sağlamalı, bir AB uygunluk beyanı hazırlamalı ve sisteme CE işareti ilıstırmelidir.
- Kayıt Yükümlülüğü (m. 49): Sağlayıcılar, sistemlerini AB veritabanına kaydetmek zorundadır.
- Piyasa Sonrası İzleme ve Düzeltici Eylemler (m. 19, m. 20): Sağlayıcılar, sistem performansını izlemeli, sapmaları veya ortaya çıkan riskleri belgelemeli ve uyumsuzluk durumunda düzeltici eylemler yapmalıdır. Ciddi olaylar (temel hak ihlalleri dahil) ilgili makamlara bildirilmelidir.

Yüksek riskli yapay zekâ sistemleri için getirilen katı yükümlölükler, temel hakların korunması ve teknik uyum arasında bir çatışma meydana getirmektedir.

AI Act, yüksek riskli sistemler için kapsamlı gereklilikler belirleyerek temel hakları korumayı amaçlamaktadır. Ancak bu uyum yükü, özellikle KOBİ'ler için inovasyonu engelleyebilir. Ayrıca güven, hesap verebilirlik gibi düzenleyici dilin algoritmik terimlerle karşılanmasındaki belirsizlik, mühendislerin pratik uyum önlemleri konusunda belirsizlik yaşamasına neden olabilecektir.

Piyasa sonrası izleme ve olay bildirim yükümlülükleri, yapay zekâ sistemlerinin sürekli güvenliğini ve hesap verebilirliğini sağlamak için hayati öneme sahiptir ancak bunların etkinliği veri erişiminin şeffaflığına bağlıdır. Yüksek riskli yapay zekâ sistemleri, piyasaya sürüldükten sonra da sürekli izlenmeli ve ciddi olaylar ilgili makamlara bildirilmelidir. Bu, sistemlerin yaşam döngüsü boyunca güvenli ve etik kalmasını sağlamak için kritik öneme sahiptir. Ancak bu raporlama yükümlülüklerinin etkinliği, platformların veri erişimini araştırmacılara ve denetçilere ne kadar şeffaf bir şekilde sağladığına bağlıdır.

2. Belirli Yapay Zekâ Sistemleri İçin Şeffaflık Yükümlülüğü

AI Act hem sistemik risk taşıyan hem de taşımayan belirli yapay zekâ sistemleri için şeffaflık yükümlülükleri öngörmektedir. Bu yükümlülükler, kullanıcıların yapay zekâ ile etkileşimde olduklarında bilinçli olmalarını sağlamayı ve yapay zekâ tarafından üretilen içeriğin kaynağı hakkında şeffaflık sunmayı amaçlamaktadır. Bu hükümler, AI Act m. 50 ve AI Act m. 53'te yer almaktadır.

AI Act, farklı yapay zekâ sistemi veya model türlerine bağlı olarak farklı yükümlülükler getiren üç boyutlu şeffaflık kuralları belirlemektedir: yüksek riskli yapay zekâ sistemleri için şeffaflık gereklilikleri, genel amaçlı yapay zekâ (GPAI) modelleri sağlayıcıları için şeffaflık yükümlülükleri ve tüm ilgili yapay zekâ sistemlerine uygulanan genel şeffaflık kuralları.

AI Act m. 50, belirli yapay zekâ sistemleri için genel bir şeffaflık rejimi öngörmektedir. Bu hükümler, yüksek riskli yapay zekâ sistemleri veya GPAI

modelleriyle sınırlı olmamakla birlikte listelenen kullanım durumlarından birine giren herhangi bir yapay zekâ sistemi için geçerlidir:

1. Doğrudan İnsanlarla Etkileşim Kuran Yapay Zekâ Sistemleri: Sağlayıcılar, gerçek kişilerin bir yapay zekâ sistemiyle etkileşimde olduklarını bilgilendirmelerini sağlamalıdır. Bu, makul ölçüde iyi bilgilendirilmiş, dikkatli bir kişi açısından açıkça belli olmadığı sürece geçerlidir. Bu yükümlülük, suçların tespiti, önlenmesi, soruşturulması veya kovuşturulması için yasal olarak yetkilendirilmiş yapay zekâ sistemleri için geçerli değildir. Örnekler arasında chatbotlar ve dijital asistanlar yer almaktadır.
2. Sentetik İçerik Üreten Yapay Zekâ Sistemleri: Sentetik ses, görüntü, video veya metin içeriği üreten yapay zekâ sistemlerinin sağlayıcıları, sistem çıktılarının makine tarafından okunabilir bir formatta işaretlenmesini ve yapay olarak üretilmiş veya manipüle edilmiş olarak tespit edilebilir olmasını sağlamalıdır. Teknik çözümlerin etkili, birlikte çalışabilir, sağlam ve güvenilir olması gerekmektedir. Bu yükümlülük, standart düzenleme için yardımcı bir işlev gören veya giriş verilerini önemli ölçüde değiştirmeyen yapay zekâ sistemleri için geçerli değildir.
3. Duygu Tanıma veya Biyometrik Kategorizasyon Sistemleri: Bu sistemleri kullanan uygulayıcılar, maruz kalan gerçek kişileri sistemin işleyişi hakkında bilgilendirmelidir. Bu yükümlülük, suçların tespiti, önlenmesi veya soruşturulması için yasal olarak izin verilen sistemler için geçerli değildir.
4. Deepfake Üreten/Manipüle Eden Yapay Zekâ Sistemleri: Deepfake oluşturan veya manipüle eden yapay zekâ sistemlerinin uygulayıcıları, içeriğin yapay olarak üretildiğini veya manipüle edildiğini açıklamak zorundadır. Sanatsal, yaratıcı, hicivsel veya benzeri eserlerde şeffaflık yükümlülükleri, eserin gösterimini veya keyfini engellemeyen uygun bir şekilde varlığın açıklanmasıyla sınırlıdır.

5. Kamu Yararına Metin Üreten/Manipüle Eden Yapay Zekâ Sistemleri: Kamuyu ilgilendiren konularda bilgi verme amacıyla metin üreten veya manipüle eden yapay zekâ sistemlerinin uygulayıcıları, metnin yapay olarak üretildiğini veya manipüle edildiğini açıklamak zorundadır.

GPAI modelinin³¹¹ karmaşık özellikleri, işleyişlerini anlamada ve izlemede ek zorluklar yaratabilir. Bu nedenle, AI Act, GPAI modelleri sağlayıcılarına ayrı yükümlülükler getirmektedir:

- Teknik Dokümantasyon: GPAI modelleri için eğitim, test ve değerlendirme süreçlerini kapsayan teknik dokümantasyon oluşturulması ve güncel tutulması.
- Bilgi Sağlama: GPAI modelini ürünlerine entegre etmek isteyen yapay zekâ sistemi sağlayıcılarına, modelin yeteneklerini ve sınırlamalarını anlamalarına yardımcı olacak bilgi ve dokümantasyon sağlanması.
- Eğitim İçeriğinin Özeti: Şeffaflığı artırmak için eğitim içeriğinin ve verilerinin ayrıntılı bir özetinin sunulması.
- Sistemik Risk Taşıyan GPAI Modelleri İçin Ek Yükümlülükler (m. 55): Yüksek etkili yeteneklere sahip veya piyasada geniş erişime sahip GPAI modelleri, sistemik risk taşıdığı kabul edilmektedir. Bu sağlayıcılar, model değerlendirmeleri yapmalı, sistemik riskleri değerlendirmeli ve azaltmalı, ciddi olayları raporlamalı ve siber güvenlik korumaları sağlamalıdır.

³¹¹ AI Act m. 3/63: “genel amaçlı yapay zekâ modeli, böyle bir yapay zekâ modelinin büyük ölçekte kendi kendine denetim kullanılarak büyük miktarda veri ile eğitildiği durumlar da dahil olmak üzere, önemli bir genellik sergileyen ve modelin piyasaya sürülme şeklinden bağımsız olarak çok çeşitli farklı görevleri yetkin bir şekilde yerine getirebilen ve piyasaya sürülmeden önce araştırma, geliştirme veya prototip oluşturma faaliyetleri için kullanılan yapay zekâ modelleri hariç olmak üzere, çeşitli alt sistemlere veya uygulamalara entegre edilebilen bir yapay zekâ modeli anlamına gelir.” (*‘general-purpose AI model’ means an AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications, except AI models that are used for research, development or prototyping activities before they are placed on the market*).

AB Yapay Zekâ Ofisi, yapay zekâ tarafından üretilen veya manipüle edilen içeriğin tespitini ve etiketlenmesini kolaylaştırmak için Birlik düzeyinde davranış kurallarının hazırlanmasını teşvik etmektedir. Bu doğrultuda Genel Amaçlı Yapay Zekâ Davranış Kuralları'nın (*GPAI Code of Practice*) taslağı, 10 Temmuz 2025'te yayımlanmıştır³¹².

III) ARA DEĞERLENDİRME

Bu bölümde çalışmanın iki sac ayağı olan yapay zekâ ve sosyal medyanın hukuki boyutu ve AB'nin iki temel düzenlemesi olan Dijital Hizmetler Kanunu (DSA) ve Yapay Zekâ Kanunu (AI Act) kapsamında getirilen yükümlülükleri ve bunların çevrimiçi platformlar (sosyal ağ sağlayıcılar) üzerindeki etkileri incelenmiştir. Elde edilen bulgular, her iki düzenlemenin de dijital ekosistemde şeffaflık, hesap verebilirlik ve kullanıcı haklarının korunması hedeflerine ulaşmada hem önemli adımlar attığını hem de çeşitli zorluklarla karşılaştığını göstermektedir.

DSA kapsamındaki temel bulgulara bakılacak olursa sosyal ağ sağlayıcılara, özellikle de çok büyük çevrimiçi platformlara (VLOP'lar) geniş bir yelpazede yükümlülükler getirmektedir:

- İrtibat Noktası ve Yasal Temsilci: DSA m. 11 ve DSA m. 13 ile getirilen irtibat noktası ve yasal temsilci belirleme yükümlülükleri, AB dışındaki sağlayıcıların da AB hukuk sistemine entegre olmasını sağlamakta ve DSA'nın Brüksel etkisini güçlendirmektedir. Ancak X gibi platformlarla ilgili mahkeme kararları, "etkili iletişim" in sadece bir e-posta adresinden daha fazlasını gerektirdiğini ve platformların bu konuda daha kullanıcı dostu çözümler sunması gerektiğini ortaya koymaktadır. Bu durum, hukuki kesinliğin işlevsel detaylara nasıl yansıdığını göstermektedir.

³¹² GPAI Davranış Kuralları hakkında ayrıntılı bilgi için bkz. <https://digital-strategy.ec.europa.eu/en/policies/contents-code-gpai>.

- Hizmet Şartları: DSA m. 14, sosyal ağ sağlayıcıların hizmet şartlarını açık, sade ve anlaşılır bir dilde sunmasını, içerik denetimi politikalarını detaylandırmasını ve temel haklara “gereken özeni göstermesini” zorunlu kılmaktadır. Bu hüküm, temel hakların sosyal ağ sağlayıcılar ile kullanıcılar arasındaki yatay ilişkide uygulanabilirliğini prensipte mümkün kılmakla birlikte bunun etkinliği yargısal yorumlamalara ve platformların tutarlı uygulamalarına bağlıdır. Küçükler için özel olarak anlaşılır şartlar sunma gerekliliği, sosyal ağ sağlayıcıların kullanıcı odaklı tasarım yaklaşımını benimsemesini teşvik etmektedir.
- Şeffaflık Raporlama: DSA m. 15, DSA m. 24 ve DSA m. 27 ile getirilen şeffaflık raporlama yükümlülükleri ve DSA Şeffaflık Veritabanı’nın kurulması, sosyal ağ sağlayıcıların içerik denetimi faaliyetleri hakkında kamuoyunu bilgilendirmede önemli bir adımdır. Ancak doktrin, sosyal ağ sağlayıcıların raporlama kalitesinde ve metodolojisinde tutarsızlıklar olduğunu, isteğe bağlı detayların sıklıkla atlandığını ve platform tasarımının sistemik risklerdeki rolünün yeterince ele alınmadığını göstermektedir. Bu durum, şeffaflıkta niceliğin her zaman niteliğe dönüşmediği bir “şeffaflık paradoksu”nu ortaya koymaktadır.
- Bildirim ve Eylem Mekanizmaları: DSA m. 16 ve DSA m. 22, hukuka aykırı içeriğin bildirilmesi için kullanıcı dostu mekanizmalar ve “güvenilir işaretleyiciler” sistemini resmileştirmektedir. Bu mekanizmalar, hukuka aykırı içeriğin hızlı kaldırılmasını sağlarken güvenilir işaretleyicilerin aşırı kaldırma veya yanlışlık potansiyeli gibi endişeleri de beraberinde getirmektedir. Otomatik araçların kullanımı verimlilik sağlasa da içeriğin “hukuka aykırı” veya “zararlı” niteliğinin yorumlanmasında zorluklar yaşanmaktadır.
- İçeriğe Karşı Kısıtlamalarda Gerekçe Gösterilmesi: DSA m. 17, içerik kısıtlamalarına ilişkin açık ve spesifik gerekçe beyanları sunma zorunluluğu getirmektedir. Bu, kullanıcıların kararlara itiraz etme

haklarını etkin bir şekilde kullanmalarını sağlamak için kritik öneme sahiptir. DSA Şeffaflık Veritabanı, bu gerekçe beyanlarını toplayarak platformların içerik denetimi uygulamaları üzerinde kamu denetimi sağlamaktadır. Ancak otomatik sistemler tarafından alınan kararlar için anlaşılır gerekçeler sunmak teknik bir zorluk olmaya devam etmektedir.

- VLOP'lara Getirilen Ek Yükümlülükler: DSA m. 19-43, VLOP'lara sistemik risk değerlendirmesi, risk azaltma önlemleri, bağımsız denetimler, araştırmacılar için veri erişimi, tavsiye sistemleri şeffaflığı ve reklam şeffaflığı gibi ek yükümlülükler getirmektedir. Bu yükümlülükler, platformların toplumsal etkilerini yönetmeyi amaçlamaktadır. Ancak platformların ilk risk değerlendirmelerinde tasarım kaynaklı riskleri yeterince ele almadığı ve araştırmacılar için veri erişiminin pratik uygulamada hala zorluklarla karşılaştığı görülmektedir.

AI Act kapsamındaki temel bulgulara bakılacak olursa yapay zekâ sistemlerinin geliştirilmesi ve kullanımında güvenliği, şeffaflığı ve etik standartları sağlamayı amaçlayan risk temelli bir yaklaşım benimsenmektedir:

- Düzenlemenin Gerekliliği ve Amacı: AI Act, yapay zekânın potansiyel faydaları ile temel haklara yönelik riskleri dengelemek amacıyla AB'nin dijital stratejisinin bir parçası olarak ortaya çıkmıştır. Düzenleme, kademeli bir uygulama takvimiyle (yasaklı uygulamalar için Şubat 2025'ten itibaren, yüksek riskli sistemler için Ağustos 2026'dan itibaren) sektörün uyum sağlamasına olanak tanımaktadır. AB'nin bu düzenlemeyle küresel bir standart belirleme hedefi, inovasyonu engelleme potansiyeliyle ilgili endişelerle karşı karşıyadır.
- Risk Temelli Yaklaşım: AI Act, yapay zekâ sistemlerini kabul edilemez, yüksek, sınırlı ve minimal risk olmak üzere dört kategoriye ayırmaktadır. Bu yaklaşım, düzenleyici yükü risk seviyesine göre orantılı hale getirmeyi amaçlamaktadır. Ancak yapay zekâ sistemlerinin

sınıflandırılmasındaki belirsizlikler ve birden fazla düşük riskli sistemin etkileşiminden kaynaklanan sistemik risklerin göz ardı edilmesi gibi sorunlar bulunmaktadır.

- Yasaklı Yapay Zekâ Sistemleri: AI Act, manipölasyon, zafiyet sömürüsü, sosyal puanlama, suç tahmini ve belirli biyometrik uygulamalar gibi temel haklara açık tehdit oluşturan sekiz uygulamayı yasaklamaktadır. Bu yasaklar, AB'nin etik değerlere bağlılığını göstermekle birlikte bazı terimlerin yorumlanmasındaki belirsizlikler ve araştırma üzerindeki potansiyel "caydırıcı etki" gibi zorluklar taşımaktadır.
- Yüksek Riskli Yapay Zekâ Sistemleri: Bu sistemler, ürünlerin güvenlik bileşenleri olarak kullanılanlar veya Ek III'te listelenen hassas kullanım durumlarına girenler olarak tanımlanmaktadır. Bu sistemler için risk yönetimi, veri kalitesi, teknik dokümantasyon, insan denetimi, doğruluk, sağlamlık ve siber güvenlik gibi katı yükümlölükler öngörülmektedir. Ancak "önemli risk" istisnası ve "profilleme"nin her zaman yüksek riskli kabul edilmesi gibi ayrıntılar, sınıflandırmayı karmaşıklaştırmaktadır.
- Sınırlı (Düşük) Riskli Yapay Zekâ Sistemleri: Bu sistemler için kullanıcılara yapay zekâ ile etkileşimde olduklarını bildirme ve yapay zekâ tarafından üretilen içeriği (deepfake'ler dahil) etiketleme gibi şeffaflık yükümlölükleri getirilmiştir. Bu, dezenformasyonla mücadele ve bilinçli kullanıcı kararlarını teşvik etmeyi amaçlamaktadır.
- Minimal Riskli Yapay Zekâ Sistemleri: En düşük risk kategorisinde yer alan bu sistemler (örneğin spam filtreleri), AI Act kapsamında doğrudan bağlayıcı düzenlemelere tabi değildir. Bunun yerine, gönüllü davranış kuralları öngörülmektedir. Bu yaklaşım, inovasyonu teşvik etmeyi amaçlasa da gelecekte ortaya çıkabilecek birleşik riskler veya beklenmedik zararlar için bir boşluk meydana getirebilecektir.

Hem DSA hem de AI Act, dijital alanda şeffaflık ve hesap verebilirliği artırma konusunda iddialı hedefler belirlemektedir. DSA, sosyal ağ sağlayıcıların içerik

denetimi ve kullanıcı etkileşimlerindeki sorumluluklarını netleştirirken AI Act, yapay zekâ teknolojilerinin etik ve güvenli bir şekilde geliştirilmesini ve kullanılmasını sağlamayı hedeflemektedir.

Ancak her iki düzenlemenin de uygulanmasında **ortak zorluklar** bulunmaktadır:

- Tanımsal Belirsizlikler: “hukuka aykırı içerik”, “zararlı içerik”, “sistemik risk” ve “yapay zekâ sistemi” gibi temel terimlerin yorumlanmasındaki belirsizlikler, platformlar ve düzenleyiciler için uyumu karmaşıklştırmaktadır.
- Veri Kalitesi ve Erişimi: Şeffaflık raporlarının kalitesi ve araştırmacılar için veri erişiminin pratik uygulanabilirliği, düzenlemelerin tam potansiyeline ulaşmasını engellemektedir.
- Teknolojik Hız ve Düzenleyici Adaptasyon: Dijital teknolojilerin ve yapay zekânın hızlı gelişimi, düzenlemelerin sürekli olarak güncellenmesini ve uyumlu hale getirilmesini gerektirmektedir. Statik ve durağan kurallar, hızla değişen bir durumda yetersiz kalabilir.
- İnovasyon ve Güvenlik Dengesi: Düzenlemeler, inovasyonu engellemeden güvenlik ve temel hakları koruma arasında hassas bir denge kurmaya çalışmaktadır. Aşırı katı uyum gereklilikleri, özellikle KOBİ’ler için inovasyonu yavaşlatabilirken yetersiz düzenleme toplumsal zararlara yol açabilir.
- Küresel Uyum: AB düzenlemeleri, “Brüksel Etkisi” aracılığıyla küresel standartları etkileme potansiyeline sahiptir. Ancak farklı yargı bölgelerindeki farklı yaklaşımlar, küresel platformlar için karmaşık uyum senaryoları meydana getirebilecektir.

Sonuç olarak DSA ve AI Act, dijital çağın getirdiği zorluklara karşı AB’nin kapsamlı ve öncü bir yanıtını temsil etmektedir. Bu düzenlemeler, çevrimiçi ortamda daha şeffaf, güvenli ve hesap verebilir bir gelecek inşa etme yolunda

önemli birer kilometre taşıdır. Ancak tam potansiyellerine ulaşmaları, devam eden düzenleyici netleştirme çabalarına, platformların proaktif uyumuna ve küresel düzeyde iş birliğine bağlı olacaktır.

ÜÇÜNCÜ BÖLÜM

YAPAY ZEKÂ ARACILIĞIYLA SOSYAL MEDYAYA YAPILAN MÜDAHALELER

Çalışmanın iki temel unsuru olan sosyal medya ve yapay zekâ birinci bölümde teknik, ikinci bölümde hukuki anlamda incelendikten sonra üçüncü ve son bölümde yapay zekâ ile sosyal medyanın teknik olarak ilişkisi çalışma konusuyla sınırlı olarak ele alınacaktır. Bu kapsamda ilk olarak sosyal medyadaki içeriklerin yapay zekâ aracılığıyla nasıl müdahaleye maruz kaldığı incelenecektir. Devamında ifade özgürlüğü ve hukuka aykırı içerik bakımından yargıya intikal etmiş davalar ele alınacaktır.

I) ERİŞİMİN ENGELLENMESİ VE FİLTRELEME

Erişimin engellenmesi ve filtreleme, internet üzerindeki hukuka aykırı içeriklerle mücadele etmek amacıyla uygulanan temel kontrol mekanizmalarıdır. Erişimin engellenmesi, belirli bir içeriğe veya internet sitesine ulaşımın, yetkili makam kararı ile tamamen veya kısmen durdurulması eylemini ifade eder. Filtreleme ise önceden tanımlanmış kriterler (anahtar kelime, içerik türü, kategori vb.) doğrultusunda zararlı veya istenmeyen içeriğe erişimi otomatik olarak kısıtlayan bir süreçtir. Bu iki kavram, amaçları ve uygulama yöntemleri açısından farklılıklar göstermekle birlikte hukuki düzenlemeler ve teknolojik uygulamalar bağlamında sıklıkla iç içe geçmektedir.

5651 sayılı Kanun'da erişimin engellenmesi tanımlanırken filtreleme kavramı tanımlanmamıştır. 5651 sayılı Kanun m. 2/o'da erişimin engellenmesi, alan adından erişimin engellenmesi, IP adresinden erişimin engellenmesi, içeriğe (URL) erişimin engellenmesi ve benzeri yöntemler kullanılarak erişimin engellenmesi olarak tanımlanmaktadır.

Sosyal medya içeriğinin hacmi, son on yılda katlanarak artmıştır ve bu durum, etkili denetim ve yönetim için önemli zorluklar yaratmaktadır³¹³. 2022'deki bir çalışmaya göre günlük 500 milyon tweet, Instagram'a yüklenen 50 milyardan fazla fotoğraf ve YouTube'a her gün yüklenen 700.000 saatin üzerinde video gibi veriler, yalnızca insan gücüyle içerik denetiminin pratik olmaktan çıktığını göstermektedir³¹⁴. Bu muazzam ölçek ve ihlallerin aralıksız doğası karşısında yapay zekâ yaklaşımları arzu edilmektedir, hatta kaçınılmaz bir çözüm olarak görülmektedir³¹⁵.

Yapay zekânın bu bağlamdaki birincil işlevi, içerik denetiminde tanıma ve sınıflandırma görevlerini içermektedir. Bu, yapay zekânın belirli içerik türlerini (örneğin, nefret söylemi, terörist içerik) tanımlamasına ve kategorize etmesine olanak tanır. Yapay zekâ, otomatik yargılamalar yaparak doğrudan eylemde bulunabilir (örneğin, içeriği otomatik olarak kaldırmak) veya içeriği insan denetçilerin incelemesi için işaretleyebilir. Böylece ilgili uzmanlığa sahip denetçilere belirli içerik türlerini yönlendirerek verimliliği artırabilir³¹⁶. Örneğin, Mark Zuckerberg'e göre Meta'da kaldırılan nefret söyleminin %95'inden fazlası ve terörist içeriğin %98-99'u yapay zekâ tarafından tespit edilmektedir. Yapay zekâ ayrıca, belirli görüntüleri sınıflandırabilir ve dezenformasyon kampanyalarını, hesap yaşı, giriş konumu ve bilinen geçmiş olaylarla bağlantılar gibi dışsal faktörleri analiz ederek tespit edebilir.

İçerik denetiminde yapay zekânın benimsenmesinin ardındaki "ölçek gerekçesi", basit bir teknik zorunluluktan daha derin bir stratejik motivasyonu barındırmaktadır. Çevrimiçi içeriğin devasa hacmi gerçek bir zorluk olsa da

³¹³ Tarleton GILLESPIE, "Content Moderation, AI, and the Question of Scale", *Big Data & Society* 7, sy 2 (2020): 1, <https://doi.org/10.1177/2053951720943234>.

³¹⁴ Alex FEERST, "The Use of AI in Online Content Moderation", American Enterprise Institute, 2022, 2, <https://platforms.aei.org/wp-content/uploads/2022/09/The-Use-of-AI-in-Online-Content-Moderation.pdf>.

³¹⁵ GILLESPIE, "Content Moderation, AI, and the Question of Scale", 2.

³¹⁶ FEERST, "The Use of AI in Online Content Moderation", 6.

platformlar tarafından sürekli olarak bu durumun vurgulanması, otomasyona yönelik itici gücü haklı çıkaran bir hikâye olarak da işlev görmektedir³¹⁷. Bu hikâye, şirketlerin insan iş gücü maliyetlerini azaltmasına ve hesap verebilirliği insan karar vericilerden “opak” algoritmalara kaydırmasına olanak tanımaktadır.

Bu başlık altında yapay zekânın sosyal medyaya müdahalelerindeki rolünü, internet omurgası tabanlı engelleme, platform temelli engelleme, kurumsal engelleme, bireysel engelleme ve yapay zekânın sosyal etki operasyonlarındaki (sosyal teknikler) rolü açıklanmaya çalışılacaktır.

Yapay zekânın dezenformasyon oluşturmak (örneğin, deepfake’ler, propaganda) ve bu tür içerikleri tespit edip bunlarla mücadele etmek için kullanılması, birbirine bağlı madalyonun iki yüzü olarak görülebilir. Bu durum, yapay zekânın tarafsız bir teknoloji olmadığını aksine hem faydalı hem de kötü niyetli amaçlar için kullanılabilirlik yeteneklere sahip olduğunu ortaya koymaktadır. Yapay zekâ, dezenformasyonu tespit etme yeteneğini geliştirdikçe kötü niyetli aktörler de bu savunmaları aşmak için yapay zekâ odaklı yöntemlerini aynı anda güncellemeye başlamaktadır. Bu, dijital alanda sürekli bir “polis ve hırsız” dinamiğine yol açmaktadır³¹⁸.

Müdahale Türü	Birincil Aktörler	Temel Yapay Zekâ Mekanizması	Birincil Amaç	İlişkili Zorluklar
İnternet Omurgası Tabanlı Engelleme	İSS’ler Hükümetler	Derin Paket İncelemesi (DPI), Ağ trafiği için Makine	Ağ trafiği kontrolü içerik	Şifreli trafik sınırlamaları, kaynak yoğunluğu,

³¹⁷ GILLESPIE, “Content Moderation, AI, and the Question of Scale”, 2.

³¹⁸ FEERST, “The Use of AI in Online Content Moderation”, 8.

		Öğrenimi (ML)/Derin Öğrenme (DL)	filtreleme gözetim	gizlilik endişeleri
Platform Tabanlı Engelleme	Sosyal Medya Platformları	Doğal Dil İşleme (NLP), Bilgisayar Görüşü (CV), içerik sınıflandırma sı için ML	Topluluk standartları nı uygulama, içerik ölçeğini yönetme	Algoritmik önyargı, açıklanabilirli k eksiklikleri, düşmanca dinamikler, denetimde öznellik
Kurumsal Engelleme	Devletler	Büyük Dil Modelleri (LLM'ler), veri filtreleme, İnsan Geri Bildirimli Takviyeli Öğrenme (RLHF)	Devlet kontrolü, anlatı şekillendir me, muhalefeti bastırma	Sansürün görünmezliği , önyargının devamı, insan hakları erozyonu, hesap verebilirlik eksikliği
Bireysel Engelleme	Bireysel Kullanıcılar /Uygulama	Kişiselleştiril miş yapay zekâ, Dijital	Kullanıcı özerkliğini artırma, dijital refahı	Algoritmik kontrol, manipülasyo n potansiyeli,

	Geliştiriciler i	Refah uygulamaları	teşvik etme, gizlilik yönetimi	genellenebilir lik sorunları
Sosyal Teknikler	Kötü Niyetli Aktörler/D oğruluk Kontrolörler i/Araştırma cılar	NLP, Multimedya Analizi, Ağ Analizi, Üretken yapay zekâ	Dezenform asyon oluşturma/ tespit etme, kamuoyunu şekillendir me, etki	İçeriğin hacmi ve hızı, güven açıkları, üretken yapay zekânın karmaşıklığı

Şema 8: Yapay Zekâ Odaklı Sosyal Medya Müdahaleleri

A. PLATFORM TEMELLİ ENGELLEME

Platform temelli engelleme, sosyal medya platformları, arama motorları ve diğer çevrimiçi hizmetlerin kendi iç politikaları, kullanım şartları ve tabi oldukları mevzuat uyarınca uyguladıkları içerik kısıtlama ve denetim mekanizmalarını ifade eder³¹⁹. Bu tür platformlar, kullanıcı tarafından oluşturulan içeriğin kendi kurallarına yahut hukuki düzenlemelere uygunluğunu denetleyerek istenmeyen içeriği filtreleyebilir, kaldırabilir veya ilgili hesapları askıya alabilir.

Platformların en temel YZ uygulaması, zararlı veya yasaklanmış içeriklerin otomatik olarak tespiti ve kaldırılmasıdır. Doğal Dil İşleme (NLP) ve bilgisayarlı görü (*computer vision*) algoritmaları, metin, resim ve videolardaki nefret söylemi, şiddet içeren görseller, terör propagandası, dezenformasyon ve telif hakkı ihlallerini insan müdahalesine gerek kalmadan tarayarak işaretler veya doğrudan

³¹⁹ KAYA, *İnternet Hukuku*, 66.

kaldırır³²⁰. Bu sistemler, saniyede milyonlarca içeriği analiz etme kapasitesiyle manuel denetimin imkânsız olduğu bir ölçekte çalışır. Ancak bu otomasyon, önemli sorunları da beraberinde getirir. Yapay zekâ algoritmaları, kültürel detayları, hiciv veya ironiyi anlamakta zorlanabilir. Bu nedenle zararlı olmayan içerikleri yanlışlıkla sansürleyebilirken yeni veya karmaşık zararlı içerik türlerini gözden kaçırabilirler. Bu durum, “aşırı engelleme” (*over-blocking*) veya “yetersiz engelleme” (*under-blocking*) sorunlarına yol açabilir.

Platform temelli engellemenin en tartışmalı biçimlerinden biri, bir içeriği veya kullanıcı hesabını tamamen kaldırmak yerine, onun görünürlüğünü ve erişimini algoritmik olarak kısıtlamaktır. “Gölge yasaklama” (*shadow banning*) veya “görünürlük filtreleme” (*visibility filtering*) olarak da bilinen bu teknikte yapay zekâ algoritmaları, platformun politikalarını tam olarak ihlal etmeyen ancak “sınırdan” veya “istenmeyen” olarak kabul edilen içeriklerin haber akışlarında, arama sonuçlarında veya tavsiye motorlarında daha az gösterilmesini sağlar³²¹. Kullanıcı, içeriğinin yayılımının neden kısıtlandığını anlayamaz çünkü herhangi bir bildirim almaz. Bu durum, platformların şeffaflıktan uzak bir şekilde belirli fikir veya görüşleri sistematik olarak baskılamasına olanak tanır ve bir tür “yumuşak sansür” işlevi görür. Yapay zekâ, hangi içeriğin ne ölçüde bastırılacağına kullanıcı etkileşimi, içerik analizi ve diğer binlerce sinyali değerlendirerek karar verir, bu da süreci son derece karmaşık ve denetlenemez kılar.

Yapay zekâ, sadece içerikleri değil, aynı zamanda kullanıcı davranışlarını da analiz ederek hesap düzeyinde yaptırımlar uygular. Örneğin, spam yapan, tacizde bulunan, bot benzeri davranışlar sergileyen veya “koordineli özgün olmayan davranış” (*coordinated inauthentic behavior*) sergileyen hesap ağlarını tespit

³²⁰ Robert GORWA vd., “Algorithmic Content Moderation: Technical and Political Challenges in the Automation of Platform Governance”, *Big Data & Society* 7, sy 1 (2020): 3, <https://doi.org/10.1177/2053951719897945>.

³²¹ Ayrıntılı bilgi için bkz. Alessandro GALEAZZI vd., *Revealing The Secret Power: How Algorithms Can Influence Content Visibility on Social Media*, t.y., erişim 10 Eylül 2025, <https://arxiv.org/html/2410.17390v2>.

edebilir. Makine öğrenmesi modelleri, bu tür anormal davranış kalıplarını öğrenerek ilgili hesapları otomatik olarak askıya alabilir veya silebilir. Bu, platformların manipülatif aktörlere ve bot ordularına karşı savunmasında önemli bir araçtır. Ancak benzer şekilde, yanlış pozitifler (*false positives*) nedeniyle masum kullanıcıların hesaplarının da haksız yere kapatılmasına neden olabilir. Özellikle aktivist gruplar veya organize muhalif hareketler, platformların yapay zekâ sistemleri tarafından yanlışlıkla “koordineli özgün olmayan davranış” olarak etiketlenilmekte ve bu durum, sivil toplumun örgütlenme özgürlüğünü kısıtlayabilmektedir.

B. KURUMSAL ENGELLEME

Kurumsal engelleme, özel şirketler, eğitim kurumları, sivil toplum kuruluşları veya devlet daireleri gibi kurumların, kendi iç ağlarında (intranet) belirli sosyal medya platformlarına veya içerik türlerine erişimi kısıtlamasını ifade eder³²². Bu tür engellemelerin temel motivasyonları genellikle verimliliği artırmak, ağ güvenliğini sağlamak, kurum itibarını korumak veya yasal sorumluluktan kaçınmaktır. Yapay zekâ, bu alanda da kurumsal politikaların daha akıllı ve dinamik bir şekilde uygulanmasına olanak tanımaktadır.

Modern “Yeni Nesil Güvenlik Duvarları” (*Next-Generation Firewalls - NGFW*) ve “Birleşik Tehdit Yönetimi” (*Unified Threat Management - UTM*) sistemleri, yapay zekâ ve makine öğrenmesi algoritmalarını yoğun bir şekilde kullanır. Bu sistemler, sadece belirli web sitelerini engellemekle kalmaz, aynı zamanda ağ trafiğini derinlemesine analiz ederek çalışanların hangi uygulamaları ne kadar süreyle kullandığını tespit eder. Yapay zekâ, normal davranış kalıplarını öğrenir ve bu kalıpların dışına çıkan anormal aktiviteleri (örneğin, bir çalışanın mesai saatleri içinde aşırı sosyal medya kullanımı veya hassas kurumsal verileri

³²² KAYA, *İnternet Hukuku*, 65.

sosyal medya üzerinden paylaşma giriřimi) tespit ederek güvenlik yöneticilerini uyarabilir veya erişimi otomatik olarak engelleyebilir³²³.

Kurumlar, marka itibarını korumak için de yapay zekâ destekli sosyal medya izleme araçlarından yararlanır. Bu araçlar, kurumun veya ürünlerinin sosyal medyadaki yansımalarını sürekli olarak tarar. Müşteri şikayetleri, karalayıcı kampanyalar veya kurumla ilgili yayılan dezenformasyon, NLP algoritmaları tarafından anında tespit edilir. Kurumlar, bu tespitlere dayanarak kendi sosyal medya sayfalarındaki istenmeyen yorumları veya gönderileri yapay zekâ aracılığıyla otomatik olarak gizleyebilir veya silebilir. Bu, bir yandan kurumun dijital alandaki imajını korumasına yardımcı olurken diğer yandan eleştirel seslerin ve tüketici geri bildirimlerinin sistematik olarak bastırılması riskini de beraberinde getirir. Dolayısıyla yapay zekâ, kurumsal düzeyde hem iç disiplini hem de dış imaj yönetimini otomatize eden bir engelleme mekanizması olarak işlev görmektedir.

C. İNTERNET OMURGASI TEMELLİ ENGELLEME

İnternet omurgası temelli engelleme, en geniş kapsamlı ve teknik olarak en merkezi müdahale türlerinden biridir. Bu tür bir engelleme, genellikle devlet sşjeleri tarafından ulusal güvenlik, kamu düzeni veya siyasi istikrar gibi gerekçelerle İnternet Servis Sağlayıcıları (İSS) veya ülkenin internet ağ geçitleri (*gateway*) düzeyinde uygulanır. Temel amaç, belirli bir sosyal medya platformuna veya genel olarak internetin bir kısmına erişimi ülke çapında yavaşlatmak veya tamamen kesmektir³²⁴. Yapay zekâ, bu tür makro düzeydeki engellemelerin etkinliğini ve verimliliğini artırmada kritik bir rol oynamaktadır.

³²³ Ayrıntılı bilgi için bkz. Junyan LIANG ve Yoohwan KIM, "Evolution of Firewalls: Toward Securer Network Using Next Generation Firewall", 2022 *IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)*, 2022, 0752-59, <https://doi.org/10.1109/CCWC54503.2022.9720435>.

³²⁴ KAYA, *İnternet Hukuku*, 64.

Geleneksel engelleme yöntemleri genellikle belirli IP adreslerinin veya alan adlarının (DNS) kara listeye alınması gibi statik kurallara dayanıyordu. Ancak kullanıcıların Sanal Özel Ağ (VPN) veya Tor gibi anonimleştirici teknolojilerle bu engelleri aşması nispeten kolaydı. Yapay zekâ, bu noktada devreye girerek çok daha dinamik ve sofistike bir denetim mekanizması sunmaktadır. Özellikle Derin Paket İncelemesi (*Deep Packet Inspection* - DPI) teknolojileri, makine öğrenmesi algoritmaları ile entegre edildiğinde, internet trafiğinin içeriğini ve türünü yüksek bir doğrulukla analiz edebilir hale gelmiştir. Yapay zekâ destekli DPI sistemleri, şifrelenmiş olsa dahi VPN veya Tor trafiğine özgü kalıpları ve davranışları tanıyarak bu tür hizmetlerin kullanımını tespit edip yavaşlatabilir veya engelleyebilir. Bu sistemler, normal internet trafiği ile engellenmek istenen trafik türü arasında ayırım yapma yeteneğine sahip olduğu için yalnızca belirli bir sosyal medya platformunun trafiğini hedef alarak diğer internet hizmetlerinin etkilenmemesini sağlayabilir. Bu durum, müdahaleyi daha “cerrahi” ve tespiti daha zor hale getirir.

Derin Paket İncelemesi (DPI), hem paket başlığını hem de paket yükünü ayrıntılı olarak analiz ederek “ağ trafiğine tam görünürlük” sağlayan kritik bir teknolojidir. Bu yetenek, DPI’nın ağ güvenliği ve hükümet gözetimi gibi çeşitli uygulamalarda kullanılmasına olanak tanır. Süreç genellikle iki ana adımı içerir: “tanımlama” (gizli özellikleri keşfetmek için paketleri inceleme) ve “eylem” (örneğin, analiz için trafiği kaydetme veya güvenlik nedenleriyle paketleri ağdan düşürme). DPI, bilinen kötü amaçlı yazılım imzalarını tespit etmek ve saldırı sırası, saldırganın izlediği yol ve kullanılan teknikler dahil olmak üzere saldırı modellerini belirlemek için yaygın olarak kullanılmaktadır³²⁵.

Ayrıca yapay zekâ algoritmaları, ağ trafiğindeki anormallikleri gerçek zamanlı olarak tespit etme kapasitesine sahiptir. Örneğin, toplumsal bir olayın

³²⁵ DPI hakkında ayrıntılı bilgi için bkz. Merve ÇELEBİ vd., “A Comprehensive Survey on Deep Packet Inspection for Advanced Network Traffic Analysis: Issues and Challenges”, *Niğde Ömer Halisdemir Üniversitesi Mühendislik Bilimleri Dergisi* 12, sy 1 (2023): 1-29, <https://doi.org/10.28948/ngumuh.1184020>.

başlangıcında belirli bir sosyal medya platformuna yönelik trafikte ani bir artış yaşandığında, yapay zekâ sistemleri bu durumu potansiyel bir tehdit olarak etiketleyip otomatik olarak “bant genişliği daraltma” (*throttling*) sürecini başlatabilir. Bu, platformun tamamen engellenmesi yerine kullanılabilirliğini ciddi ölçüde azaltarak bilgi akışını yavaşlatmayı amaçlayan bir tekniktir. Kullanıcılar platforma erişebildiklerini zannetseler bile içeriklerin yüklenmemesi veya mesajların iletilmemesi gibi sorunlar yaşarlar. Bu durum, engellenmenin psikolojik etkisini de artırır ve kullanıcılar arasında belirsizlik oluşturur. Sonuç olarak yapay zekâ, internet omurgası düzeyindeki engellemeleri statik ve kolayca aşılabilir bir yöntem olmaktan çıkarıp öğrenen, adapte olan ve tespiti zor, dinamik bir kontrol mekanizmasına dönüştürmüştür.

D. BİREYSEL ENGELLEME

Bireysel engelleme ile kastedilen kişilerin bizzat başka kişilere yönelik yaptıkları engelleme değildir. Bireysel engelleme, bir kişinin internete erişiminin aşamalı olarak engellenmesini ifade eder. Buna “üç ihlal kuralı” (*Three Strikes Law*) da denmektedir. Buna göre kişiye farklı zaman dilimlerinde yapılan ikazlara rağmen söz konusu davranış terk edilmezse kişinin internet bağlantısı tamamen kesilmektedir³²⁶.

E. SOSYAL TEKNİKLER

Doğrudan içeriğe veya içeriğin yer aldığı platforma erişim teknik anlamda olmasa da dolaylı olarak engellenebilmektedir. Bu yönetime doktrinde “sosyal teknikler” adı verilmektedir. Bu tekniğe göre devletler, aldıkları bazı kararlar doğrultusunda potansiyel kullanıcının söz konusu platforma veya platformda yer alan içeriğe erişimini psikolojik olarak engellemektedir³²⁷. Örneğin, ilgili platformda oluşturulan içerik ticari bir kazanç sağlıyor ve devlet tarafından bu gibi

³²⁶ KAYA, *İnternet Hukuku*, 68.

³²⁷ KAYA, *İnternet Hukuku*, 91-92.

içerikler vergi gibi mali külfetlere tabi tutulması sebebiyle yahut paylaşımları dolayısıyla devletin nefesini ensesinde hisseden kullanıcı içeriğe erişmemeyi zorunlu olarak tercih edebilmektedir. Bunun gibi devletin aldığı kararlar, kişilerin ifade özgürlüğünü ihlal etmektedir.

Sosyal teknikler, ayrıca doğrudan içeriği veya erişimi engellemek yerine yapay zekâyı kullanarak sosyal medya üzerindeki kamusal tartışmayı ve algıyı manipüle etmeyi amaçlayan en sofistike ve sinsi müdahale yöntemleridir. Bu teknikler, engellemeden ziyade yönlendirme, saptırma ve boğma (*flooding*) prensiplerine dayanmaktadır.

Yapay zekâ, dezenformasyon ortamında “ikili bir rol” oynamaktadır: yanıltıcı içerik oluşturmak ve çeşitli tespit ve doğrulama sistemleri aracılığıyla dezenformasyonla mücadele etmek. Bu durum, dezenformasyon tehdidinin durağan olmadığını, yapay zekânın gelişmesiyle dinamik olarak geliştiğini göstermektedir. Dezenformasyonun tespiti için ileri yapay zekâ teknikleri kullanılmaktadır³²⁸.

II) SOSYAL MEDYAYA MÜDAHALE KONUSUNDAKİ YARGI KARARLARI

Sosyal medyada kullanıcılar (içerik sağlayıcılar) tarafından sağlanan içeriklerin yapay zekâ algoritmalarıyla nasıl müdahaleye maruz kaldıkları incelendikten sonra bu müdahalelerin temelde temas ettiği iki duruma ve bu durumlarla ilgili yargı kararlarına bakılması ve incelenmesi gerekmektedir.

Bu doğrultuda öncelikle ifade özgürlüğü kavramı ele alınacak ve sosyal ağ sağlayıcıların sosyal medyaya müdahalelerinin kullanıcıların ifade özgürlüğünü ihlal edip etmediği yargı kararları doğrultusunda açıklanacaktır. Devamında sosyal medyaya müdahalenin temelde temas ettiği ikinci durum olan hukuka

³²⁸ Bu teknikler hakkında ayrıntılı bilgi için bkz. Julia PUCZYŃSKA ve Youcef DJENOURI, “AI in Disinformation Detection”, *Applied Cybersecurity & Internet Governance* 3, sy 2 (2024): 211-32, <https://doi.org/10.60097/ACIG/200200>.

aykırı içerik kavramı incelenecek ve bu kavram ile ilgili yargı makamlarının kararları aktarılacaktır:

A. İFADE ÖZGÜRLÜĞÜ

İnsanlık, doğası gereği günümüze kadar kendini dış dünyaya çeşitli şekillerde yansıtmış, duygu ve düşüncelerini aktarmıştır. Bu aktarımlar zaman zaman önem kazanmış hatta savaş başlattığı gibi çağ da açıp kapatmıştır. Günümüze kadar gelen insanlık medeniyeti bu ifade edilişin tezahürüdür. 21. yüzyılda insanın kendini ifade etme, düşünce ve duygularını paylaşma biçimi, içeriği değişmekte ve gelişmektedir. İşte, bu noktadan hareketle insanı dönüştüren teknolojik gelişmelerin insanın dış dünyaya mührünü vurma biçimi olan ifade özgürlüğü bu başlık altında ele alınacaktır.

Öncelikle ifade özgürlüğünün ne anlama geldiği ortaya konmaya çalışılacak. Devamında unsurları ve keyfiliğe yol açmadan nasıl sınırlanabileceği ulusal ve uluslararası metinler ışığında açıklanacaktır.

1. Anlamı

Kişinin *sırf insan olduğu için sahip olduğu haklar* olarak tanımlanan insan hakları³²⁹ hukukta felsefe, sosyoloji gibi diğer sosyal bilimlerden farklı olarak ele alınmıştır. Örneğin, felsefe insan haklarının kaynağını, amacını ve nereye kadar gidebileceğini ele almakta iken sosyoloji insan haklarının toplumsal düzendeki yansımada ayna görevi üstlenmiştir. Hukuk ise bu alanların bir anlamda sentezi olmuş ve bu bilim dallarının birikimlerini belirli ölçülerde normatif yapıya kavuşturmuştur. Felsefi, sosyolojik ve hukuki incelemelere konu olan insan

³²⁹ İnsan hakları kavramı, “temel hak ve özgürlükler”, “kamu hürriyetleri” gibi kavramlardan ayırt edilmelidir. Ayrıca bkz. Kemal GÖZLER, *Anayasa Hukukunun Genel Esasları Ders Kitabı*, Güncellenmiş 14. Baskı (Ekin Yayınevi, 2022), 402-3; Oktay UYGUN, *Devlet Teorisi*, 5. Baskı (On İki Levha Yayıncılık, 2019), 484; Oktay UYGUN, *Kamu Hukuku İncelemeleri İnsan Hakları, Demokrasi, Hukuk Devleti, Egemenlik*, 2. Baskı (On İki Levha Yayıncılık, 2013), 7-8.

hakları³³⁰, elbette insanın geçmiş deneyimlerinden, acılarından ve sevinçlerinden çıkarılan derslerin bir kül halinde günümüze mirası olmuştur. İfade özgürlüğü de insan haklarının bu deneyimlerinde yer almıştır.

İfade özgürlüğü, insanların sosyal etkileşiminin temel yapı taşı olmuştur. “Kant'ın tabiri ile ifade özgürlüğü diğer tüm özgürlüklerin kalkanı konumundadır.”³³¹ Ayrıca insanın maddi ve manevi varlığını geliştirmesi için bir araç işlevi de görmektedir. İnsanlar (yazı, resim, fotoğraf vb.) çeşitli yollarla duygularını, düşüncelerini, tecrübelerini dış aleme yansıtır. İnsanoğlu sadece birikim yapmakla ve bunu dış aleme yansıtmakla kalmaz, diğer varlıklar tarafından bu birikimiyle fark edilmek ister. Böylece tek tek ortaya konan birikimler paylaşılır. Bu paylaşımlar da ifade özgürlüğünün kapsamı içinde yer alır. Nihayetinde genetik olarak birbirinden farklı olan insanın kendini dışa vurumu da farklılık arz etmekte, bir konu ya da durum üzerinde farklı şekillerde tepki verebilmektedir. Bu da müzakereyi doğurmakla kalmaz, hakikate daha fazla yaklaşılmasına vesile olur.³³²

İfade özgürlüğünün anlamını³³³ açıklamaya geçmeden önce bu terimin farklı şekillerde de ifade edildiğini belirtmek gerekir. Doktrinde birtakım yazarlar

³³⁰ İnsan haklarının doğal hukuk-pozitif hukuk görüşleri doğrultusunda tanımı için bkz. Abdurrahman EREN, *Anayasa Hukuku Dersleri Genel Esaslar - Türk Anayasa Hukuku*, Güncellenmiş 4. Baskı (Seçkin Yayıncılık, 2022), 462-70; GÖZLER, *Anayasa Hukukunun Genel Esasları Ders Kitabı*, 402; ayrıca bkz. UYGUN, *Devlet Teorisi*, 482-84; UYGUN, *Kamu Hukuku İncelemeleri İnsan Hakları, Demokrasi, Hukuk Devleti, Egemenlik*, 5-7.

³³¹ Yakup YILDIRIM, “Avrupa İnsan Hakları Mahkemesi Kararlarında İfade Özgürlüğü ve İtibarın Korunması Hakkı” (Doktora Tezi, Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, 2021), 16, <https://tez.yok.gov.tr/>.

³³² UYGUN, *Devlet Teorisi*, 581-82; UYGUN, *Kamu Hukuku İncelemeleri İnsan Hakları, Demokrasi, Hukuk Devleti, Egemenlik*, 130-31.

³³³ İfade özgürlüğünü açıklamak için geliştirilen “kendini geliştirme”, “gerçeklerin keşfedilmesi” ve “demokrasi” temelli teoriler için ayrıca bkz. YILDIRIM, “Avrupa İnsan Hakları Mahkemesi Kararlarında İfade Özgürlüğü ve İtibarın Korunması Hakkı”, 49-56.

düşünce özgürlüğü³³⁴ terimini kullanırken bazı yazarlar ise ifade hürriyeti³³⁵ veya ifade özgürlüğü³³⁶ terimini tercih etmektedirler. Biz bu terimler arasında birkaç nüans farkı dışında bir fark görmemekle birlikte belirtelim ki düşünce özgürlüğü kavramı daha çok “düşünce” ekseninde bir çerçeve çizmektedir. Bu yüzden açıklamalarımızı yaparken daha kapsamlı bir anlamı barındıran “ifade özgürlüğü” terimini kullanacağız^{337, 338}.

İfade özgürlüğünün anlam ve kapsamını belirlerken lafzi (gramatikal) anlamını vermekle konuya başlamak gerekir. Güncel TDK Sözlüğünde ifade³³⁹ “*anlatım, deyiş, söyleyiş, bir duyguyu yüz aracılığıyla anlatan belirtilerin, mimiklerin bütünü, tanık ve sanıkların olay hakkında yargı organlarına yaptıkları sözlü açıklama, dışa vurum*”, özgürlük ise “*herhangi bir kısıtlamaya, zorlamaya bağlı olmaksızın düşünme veya davranma, herhangi bir şarta bağlı olmama durumu, serbestî, her türlü dış etkiden bağımsız olarak insanın kendi iradesine, kendi düşüncesine dayanarak karar vermesi durumu, hürriyet*” olarak tanımlanmaktadır³⁴⁰. Bu iki tanımı birleştirirsek ifade özgürlüğü, “kişinin herhangi bir dış etkiye maruz kalmaksızın sözlü, yazılı, görsel şekillerde dış dünyada kendisini dışa vurumu” olarak tanımlanabilir.

³³⁴ Murat Volkan DÜLGER, *Bilişim Suçları ve İnternet İletişim Hukuku*, 9. Baskı (Seçkin Yayıncılık, 2022), 674, <https://www.turcademy.com/tr/kitap/bilisim-suclari-ve-internet-iletisim-hukuku-9789750275678>. Yazar ifade özgürlüğü kavramının düşünceyi dile getirmekle düşünce arasındaki bağı soyut olarak kopardığını ifade etmektedir.

³³⁵ ÖZTEKİN, *Teori ve Uygulamada Türk İnternet Hukuku*, 678 vd.

³³⁶ Ilgın MÜFTÜOĞLU, “Sosyal Medya ve İfade Özgürlüğü”, içinde *Bilişim Hukuku Güncel Sorunlar*, 1. Baskı, ed. Süleyman YILMAZ (Yetkin Yayınları, 2020), 149-59; UYGUN, *Devlet Teorisi*, 581-625; Şaban Cankat TAŞKIN, *İnternete Erişim Yasakları*, 1. Baskı (Seçkin Yayıncılık, 2016), 52 vd., <https://www.turcademy.com/tr/kitap/internete-erisim-yasaklari-9789750237874>; UYGUN, *Kamu Hukuku İncelemeleri İnsan Hakları, Demokrasi, Hukuk Devleti, Egemenlik*, 127-97; kavram farklılığına ilişkin ayrıntılı açıklamalar için bkz. Artun AVCI, *Türkiye’de İnternet ve İfade Özgürlüğü*, 1. Baskı (Legal Yayıncılık A.Ş., 2013), 45-58.

³³⁷ Aynı yönde: YILDIRIM, “Avrupa İnsan Hakları Mahkemesi Kararlarında İfade Özgürlüğü ve İtibarın Korunması Hakkı”, 9-12.

³³⁸ Aksi görüşte: DÜLGER, *Bilişim Suçları ve İnternet İletişim Hukuku*, 675-76.

³³⁹ AİHS m. 10 dışında kalan ifade biçimlerine ilişkin bkz. YILDIRIM, “Avrupa İnsan Hakları Mahkemesi Kararlarında İfade Özgürlüğü ve İtibarın Korunması Hakkı”, 56-91.

³⁴⁰ <https://sozluk.gov.tr/> (Son Erişim Tarihi: 08.12.2022).

İfade özgürlüğünün ulusal ve uluslararası metinlerdeki düzenlemesine de bakmak gerekir. İlk olarak İHEB m. 19’da herkesin düşünce ve ifade özgürlüğüne sahip olduğu ve bu hakkın herhangi bir kamu/özel müdahalesi olmaksızın, herhangi bir şekilde bilgi ve haber alma, verme ve arama özgürlüğünü kapsadığı belirtilmektedir. AİHS m. 10/1 c.2 ise bu özgürlüğün kapsamını şöyle belirlemiştir: *“Bu hak, kamu makamlarının müdahalesi olmaksızın ve ülke sınırları gözetilmeksizin, kanaat özgürlüğünü ve haber ve görüş alma ve de verme özgürlüğünü de kapsar.”* Diğer bir uluslararası sözleşme olan MSHS m. 19/2’de her türden fikrin ve haberin sınırlama olmaksızın sözlü, yazılı ya da basılı sanat şeklinde ya da kişinin seçeceği herhangi bir yolla alımının, iletiminin ve aranmasının özgürlük kapsamında yer aldığı belirtilmiştir. Nihayet, 1982 tarihli Anayasa m. 25-26’da da bu özgürlük pozitif bir temele oturtulmuştur. Buna göre herkes söz, yazı ve herhangi bir biçimde düşünce ve kanaatlerini herhangi bir kamu veya özel müdahalesi olmaksızın ifade etme özgürlüğüne sahiptir.

Ulusal ve uluslararası hukuki metinlere bakıldığında ifade özgürlüğünün akıl ve vicdan sahibi bir varlık olan insanın temel bir özgürlüğü ve hakkı olduğu anlaşılmaktadır. Böylece kişiler herhangi bir şey hakkında bilgi ve haber alma, arama, iletme hakkına sahip olmaktadır. Bu bağlamda maddi ve manevi anlamda gelişimlerini sürdürmekte, edinmiş oldukları bilgileri, tecrübeleri doğrulamakta ve değiştirebilme imkânına sahip olmaktadır³⁴¹.

İfade özgürlüğü insan varlığına içkin bir özelliktir. Dolayısıyla insanın düşünmemesi, düşündüklerini ifade etmemesi düşünülemez. Bu bağlamda bu özgürlük insan haklarının sınıflandırılmasında esas alınan bir ayrıma göre birinci

³⁴¹ ÖZTEKİN, *Teori ve Uygulamada Türk İnternet Hukuku*, 680.

kuşak haklar³⁴², diğer ayrımında negatif statü haklar³⁴³ arasında yer almaktadır. Buna göre ifade özgürlüğü devletin müdahale etmemesi gereken bir alan olması hasebiyle negatif statü haklar çerçevesinde ele alınmaktadır. Ancak edinilen tecrübeler ışığında AİHM'nin vermiş olduğu kararlarda devletin müdahale etmemesinin ifade özgürlüğünü tam anlamıyla korumadığı ve bu konuda devletin aktif bir rol almasının da gerektiği belirtilmiştir³⁴⁴.

2. Unsurları

Yukarıda ulusal ve uluslararası metinlerde ifade özgürlüğünün anlamına, içeriğine değinilmiş ve kişilerin varlıklarına içkin olan bu özgürlükle zıt fikir ve tecrübeleri görmeleri ve böylelikle kendilerini geliştirebilmelerinin sağlandığı belirtilmişti. Tam da bu noktada bu özgürlüğün -anamlı olmasını sağlayan- unsurlarına da değinmek faydalı olacaktır.

İHEB'de, AİHS'de ve MSHS'de ifade özgürlüğü, bir kanaate sahip olma, bilgiyi veya haberi alma, iletme ve arama üzerine inşa edilmiştir³⁴⁵. Doktrinde Yıldırım bu özgürlüğün unsurlarını görüş (kanaat) sahibi olma, bilgi ve fikir alma ile bilgi ve fikir verme olarak belirlerken³⁴⁶ Tanju ise Yıldırım'a ek olarak haber alma özgürlüğünü ve iletişim araçları özgürlüğünü³⁴⁷ de unsurlara dahil etmektedir.

³⁴² İnsan hakları öğretisinde bu ayrımın genel kabul gördüğü ve bu kabulün üç nedene dayandığı yönünde bkz. UYGUN, *Devlet Teorisi*, 497; Sezen KAMA IŞIK ve Oya BOYAR, "Dördüncü Kuşak Haklar ve Bilişim Teknolojilerinin Doğuşunda Mahremiyet Kavramına Karşılaştırmalı Bir Bakış", *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi* 25, sy 2 (2019): 603-5, <https://doi.org/10.33433/maruhad.667577>; ayrıca bkz. UYGUN, *Kamu Hukuku İncelemeleri İnsan Hakları, Demokrasi, Hukuk Devleti, Egemenlik*, 130.

³⁴³ MÜFTÜOĞLU, "Sosyal Medya ve İfade Özgürlüğü", 150.

³⁴⁴ UYGUN, *Devlet Teorisi*, 584-85; UYGUN, *Kamu Hukuku İncelemeleri İnsan Hakları, Demokrasi, Hukuk Devleti, Egemenlik*, 131-33.

³⁴⁵ MÜFTÜOĞLU, "Sosyal Medya ve İfade Özgürlüğü", 151 Yazar bunlara ek olarak "inanç özgürlüğü"nü de dahil etmektedir.

³⁴⁶ YILDIRIM, "Avrupa İnsan Hakları Mahkemesi Kararlarında İfade Özgürlüğü ve İtibarın Korunması Hakkı", 98.

³⁴⁷ Erhan TANJU, *AİHM Kararları Işığında İfade ve Basın Özgürlüğü*, Güncellenmiş 2. Baskı (Seçkin Yayıncılık, 2017), 187-89, <https://www.turcademy.com/tr/kitap/aihm-kararlari-isiginda-ifade-ve-basin-ozgurlugu-9789750241154>.

Kanaatimizce ifade özgürlüğü (1) Kanaat sahibi olma özgürlüğü, (2) Bilgi/haber alma özgürlüğü, (3) Bilgi/haber verme özgürlüğü ve (4) İletişim araçları özgürlüğü unsurlarından oluşmaktadır.

(1) Kanaat sahibi olma özgürlüğü: Kişinin dini, siyasi, kültürel, felsefi vb. alanlarda birikimlerine dayanarak fikir sahibi olabilmesidir. Bir kanaate sahip olabilmek için kişinin konu ile alakalı bilgilere erişme imkânının olması gerekir. Yani, bu özgürlüğün anlamlı olabilmesi için gerekli bilgileri barındıran araçlara ulaşımın serbest olması, kısıtlanmamış olması gerekir. Kişi bu araçlara ulaşarak yani bir araştırma yaparak bir kanaat oluşturmaktadır. Dolayısıyla ifade özgürlüğünün bu unsurunun olmaması ifade özgürlüğünü anlamsız kılacaktır.³⁴⁸ Bununla birlikte kişi sahibi olduğu kanaatini dış dünyaya yansıtmayabilir.

(2) Bilgi/haber alma özgürlüğü: Kişinin bir konu veya şey hakkında var olan bilgileri edinebilmesini ifade eder. Burada da kişinin bu özgürlükten faydalanabilmesi için ilgili bilgilere ulaşabilmesi gerekmektedir. Kişi bu bilgileri kamu veya özel kaynaklardan hiçbir müdahale olmaksızın edinebilmekte hatta AİHS m. 10'da belirtildiği üzere bunu ülke sınırlarıyla sınırlandırılmaksızın gerçekleştirebilmektedir.³⁴⁹ Bilgi alma özgürlüğünün kapsamı, verilmek istenen bilgiyi elde etmektir³⁵⁰.

(3) Bilgi/haber verme özgürlüğü: Kişinin sahip olduğu bilgiyi/haberi kamuya veya özel birkaç kişiye iletebilmesi, onlarla paylaşabilmesidir. Burada kişi önceden araştırdığı, edindiği bilgiyi/haberi olduğu gibi ya da kişisel süzgecinden geçirerek kanaatıyla dış dünyaya aksettirmektedir. Kanaat sahibi olmadan farkı, kişinin sahip olduğu bilgileri dış dünyaya yansıtmasıdır. Bu dışa yansıtma bazen

³⁴⁸ YILDIRIM, "Avrupa İnsan Hakları Mahkemesi Kararlarında İfade Özgürlüğü ve İtibarın Korunması Hakkı", 98-100.

³⁴⁹ YILDIRIM, "Avrupa İnsan Hakları Mahkemesi Kararlarında İfade Özgürlüğü ve İtibarın Korunması Hakkı", 101.

³⁵⁰ YILDIRIM, "Avrupa İnsan Hakları Mahkemesi Kararlarında İfade Özgürlüğü ve İtibarın Korunması Hakkı", 107.

çok güçlü olabilmektedir. Propaganda denilen bu yöntemde kişi veya daha çok kişiler topluluğu, sistematik bir şekilde diğer kişilerin sahip olduğu bilgi ve kanaatleri etkilemektedir³⁵¹.

(4) İletişim Araçları Özgürlüğü: Kişinin yukarıdaki özgürlükleri kullanırken hep baş ucu kitabı gibi yanında bulunması gerekli olan, bilgiye erişimini sağlayan, bilgiyi yaymasını sağlayan bir özgürlüktür. Dolayısıyla iletişim araçlarının olmaması, ifade özgürlüğünü bir masa olarak düşündüğümüzde bu masanın bir ayağının olmaması demektir. Geçmişten günümüze bilgiye erişimi sağlayan iletişim araçları olan kitap, gazete, dergi, televizyon ve radyonun önemi yadsınamaz. 21. yüzyılda ise artık bu kervana web 2.0 teknolojisinin getirisi olan Twitter, Facebook, Instagram, YouTube gibi sosyal medya uygulamaları da katılmış ve ifade özgürlüğünü de etkilemiştir³⁵².

3. Sınırlandırılması

İnsan hakları geçmişte yaşanan acı tecrübeler sonucu edinilmiş haklar olmakla birlikte keyfi bir biçimde de kullanılmamalıdır. Bu doğrultuda ulusal ve uluslararası hukuki metinlerde de bu durum dikkate alınarak bu hakları en az sınırlayacak ama keyfi bir uygulamaya da yer vermeyecek sınırlama sebepleri öngörülmüştür.

İfade özgürlüğü özelinde MSHS m. 19/3'te sınırlamanın gerekli olması ve kanunla yapılması şartıyla kişilerin şöhret ve itibarının korunması, ulusal güvenlik, kamu düzeni, kamu sağlığı ya da ahlak sebeplerine dayanılarak ifade özgürlüğünün sınırlandırılabilmesi belirtilmiştir.

AİHS m. 10/2'de ise bu özgürlüğün “kanunla” sınırlandırılabilmesi 10 hâl sayılmıştır: Ulusal güvenliğin korunması, ülke bütünlüğünün korunması, kamu

³⁵¹ Ayrıntılı bilgi için bkz. YILDIRIM, “Avrupa İnsan Hakları Mahkemesi Kararlarında İfade Özgürlüğü ve İtibarın Korunması Hakkı”, 120-21.

³⁵² Ayrıntılı bilgi için bkz. D. Sosyal Medya Platformlarının Yapay Zekâ Aracılığıyla İfade Özgürlüğünü Engellemesi.

güvenliğinin sağlanması, kamu düzeninin sağlanması, suç işlenmesinin önlenmesi, sağlığın korunması, ahlakın korunması, başkalarının şöhret ya da haklarının korunması, gizli bilgilerin açığa vurulmasının önlenmesi ve yargı organının otoritesinin ve tarafsızlığının sağlanması. Sözleşmede öngörülen bu sınırlama sebepleri ulusal makamlar tarafından ifade özgürlüğünü aşırı derece sınırlandıran bir şekilde uygulanabilir. Örneğin, kamu düzeni gerekçesiyle ülkedeki azınlık durumundaki görüşün “palazlanmasının” önü kamu düzeni açısından bir tehlike arz etmediği halde kesilebilir. Ancak bu takdir yetkisi de sınırsız değildir çünkü bir hak ihlali durumunda AİHM denetimine tabi tutulabilecektir³⁵³.

İfade özgürlüğünün sınırlandırılmasında AİHM ulusal makamlara verilen takdir yetkisinin kapsamını 3 tür parametre ekseninde ele almaktadır: (1) İfadenin konusu, (2) İfadenin yöneldiği kişi ya da kurum ve (3) İfadenin sahibi.

İfadenin konusu bakımından AİHM ırkçı düşünce açıklamalarının ve şiddete teşvik söylemlerinin sözleşme kapsamında olmadığını belirtmektedir. Dini konularda takdir yetkisi genişlerken siyasi konularda müdahale yetkisi azalmaktadır.

İfadenin yöneldiği kişi ya da kurum açısından AİHM’nin sınırlama yetkisinin en genişten en dar olana doğru sıralaması şu şekildedir:

³⁵³ UYGUN, *Devlet Teorisi*, 583.



Şema 9: AİHM’nin Sınırlama Yetkisi Sıralaması

İfade sahibi bakımından AİHM politikacı ve gazetecilerin ifade özgürlüklerine yapılan müdahaleleri katı yorumlamakta ve bu kişilerin bazı söylemlerinin doğal karşılanması gerektiğini ifade etmektedir³⁵⁴.

Nihayet Anayasa’da öngörülen sınırlamalara da değinmek gerekir. Genel olarak Anayasa’da öngörülen temel hak ve hürriyetler ilgili maddelerle birlikte Anayasa m. 13’te belirtilen genel sınırlama sebeplerine tabidir. Bu doğrultuda Anayasa m. 13 gereğince olağan dönemde³⁵⁵ temel hak ve özgürlüklerin sınırlandırılabilmesi için kanuni bir düzenleme olmalıdır. Ayrıca bu sınırlandırma, hakkın özünü zedelemekten Anayasa’nın sözüne ve ruhuna, ilgili maddedeki

³⁵⁴ UYGUN, *Devlet Teorisi*, 595-96.

³⁵⁵ Olağanüstü dönemlerde temel hak ve özgürlüklerin sınırlandırılması ve hatta durdurulması Anayasa m. 15’te öngörülen usul çerçevesinde gerçekleşecektir. Ayrıntılı bilgi için bkz. EREN, *Anayasa Hukuku Dersleri Genel Esaslar - Türk Anayasa Hukuku*, 647-61 Konunun kapsamının genişlememesi adına bu konuya burada değinmeyeceğiz.

sınırlama sebeplerine, demokratik toplum düzeninin gereklerine, laik cumhuriyetin gereklerine ve orantılılık ilkesine uygun olmalıdır³⁵⁶.

B. HUKUKA AYKIRI İÇERİK

Dijitalleşmenin 21. yüzyılda giderek yaygınlaşması, insanlık yararına faydalı uygulamaları beraberinde getirmişse de insanlık için faydalı olmayan hatta hukuka aykırı olan uygulamaları, iş ve eylemleri de getirmiştir. Bu çalışmanın ikinci bölümünde incelendiği üzere DSA da çevrimiçi ortamda yaygınlaşan dezenformasyonu, hukuka aykırı içeriği önlemek ve az önce incelenen ifade özgürlüğü gibi temel hak ve hürriyetleri korumak amacıyla ihdas edilmiştir.

İşte, çalışmanın bu adımında DSA’da vücut bulan “hukuka aykırı içerik” kavramı incelenecektir. Öncelikle bu kavramın anlamı ve unsurları üzerinde durulacak, devamında bu kavramın sınırlandırılması konusunda açıklamalar yapılacaktır.

1. Anlamı

DSA m. 3/h hükmüne göre hukuka aykırı içerik, *“kendiliğinden veya ürünlerin satışı ya da hizmetlerin sağlanması dahil olmak üzere bir faaliyetle bağlantılı olarak, Birlik hukukuna veya Birlik hukukuna uygun olan herhangi bir Üye Devlet hukukuna uymayan herhangi bir bilgi”* olarak tanımlanmaktadır. Bu tanım, ilgili hukukun kesin konusuna veya niteliğine bakılmaksızın uygulanır.

Bu geniş tanım, platformlar üzerinde ağır bir yük oluşturmakta ve DSA kapsamında küresel yıllık cirolarının %6’sına varan ciddi para cezalarından kaçınmak için “aşırı kaldırmaya” sevk etmektedir. Bu “Brüksel Etkisi”, küresel içerik denetimi politikalarının en katı AB ulusal yasalarına doğru kaymasına neden olabilir³⁵⁷.

³⁵⁶ Ayrıntılı bilgi için bkz. EREN, *Anayasa Hukuku Dersleri Genel Esaslar - Türk Anayasa Hukuku*, 596-636.

³⁵⁷ Dawn Carla NUNZIATO, “The Digital Services Act and the Brussels Effect on Platform Content Moderation”, *Chicago Journal of International Law* 24, sy 1 (2023): 3,

Hukuka aykırı içerik kavramı, çevrimdışı ortamdaki mevcut kuralları geniş ölçüde yansıtmayı amaçlamaktadır³⁵⁸. Bu, çevrimdışı dünyada hukuka aykırı olan bir şeyin, genellikle DSA kapsamında çevrimiçi olarak da hukuka aykırı kabul edileceği anlamına gelmektedir³⁵⁹. Ancak çevrimdışı hukuka aykırı olan çevrimiçi de hukuka aykırı olmalıdır ilkesi mantıksal bir temel sağlasa da uygulanması karmaşıktır. Dijital ortam, hızlı yayılma, küresel erişim, anonimlik ve algoritmik güçlendirme gibi benzersiz özelliklere sahiptir ve bu özellikler her zaman doğrudan çevrimdışı eşdeğerlere sahip değildir. Örneğin, “dezenformasyon” ve “bilgi manipülasyonu” DSA için merkezi endişe kaynakları olsa da birçok yargı alanında çevrimdışı olarak hukuka aykırı değildir. Bu durum, özellikle “zararlı ama yasal” içerik için bir tanım belirsizliği oluşturmaktadır³⁶⁰. Platformlar, sistemik risklerden kaçınmak veya kendi hizmet koşullarına uymak için bu tür içerikleri kaldırma baskısı hissedebilecektir.

DSA'nın tanımı, hukuka aykırı içerik, ürün, hizmet ve faaliyetlerle ilgili bilgileri kapsar. Bu kapsam, çeşitli içerik türlerini içermektedir:

- Hukuka aykırı nefret söylemi,
- Terör içeriği,
- Hukuka aykırı ayrımcı içerik,
- Çocuk cinsel istismarı görüntüleri,
- Özel görüntülerin rızasız paylaşımı,
- Çevrimiçi takip (*stalking*),

<https://cjl.uchicago.edu/print-archive/digital-services-act-and-brussels-effect-platform-content-moderation>.

³⁵⁸ Digital Services Act (DSA), Gerekçe 12.

³⁵⁹ Therese ENARSSON, “Navigating Hate Speech and Content Moderation Under the DSA: Insights from ECtHR Case Law”, *Information & Communications Technology Law* 33, sy 3 (2024): 388, <https://doi.org/10.1080/13600834.2024.2395579>.

³⁶⁰ Elena ABRUSCI, “The UK Online Safety Act, the EU Digital Services Act and Online Disinformation: Is the Right to Political Participation Adequately Protected?”, *Journal of Media Law* 16, sy 2 (2024): 454, <https://doi.org/10.1080/17577632.2024.2425551>.

- Uyumsuz veya sahte ürünlerin satışı,
- Telif hakkıyla korunan materyalin izinsiz kullanımı.

DSA kapsamındaki hukuka aykırı içerik tanımı, sadece içeriğin kendisi hukuka aykırı olduğunda değil, aynı zamanda hukuka aykırı bir faaliyetle ilişkili olduğunda da kapsamaktadır. Bu, tanımın genişliğini ve platformların sorumluluk alanının derinliğini gösterir.

DSA'da "açıkça" hukuka aykırı içerik kavramı da kullanılmaktadır. Bu kavram, herhangi bir derinlemesine analiz gerektirmeksizin sıradan bir kişi için bile içeriğin hukuka aykırı olduğunun açıkça anlaşıldığı durumları ifade eder. Bu kavram, özellikle hızlı kaldırma gereklilikleri (örneğin nefret söylemi için 24 saat kuralı)³⁶¹ bağlamında kritik öneme sahiptir çünkü bu durum genellikle otomatik tespit sistemlerinin kullanımını gerektirir.

DSA m. 23 uyarınca açıkça hukuka aykırı içeriğin sıkça sağlanması veya açıkça asılsız bildirimlerin/şikâyetlerin sıkça yapılması durumunda sosyal ağ sağlayıcılar, ilgili kişinin faaliyetlerini geçici olarak askıya alabilir. Bu, sistemin kötüye kullanılmasını önlemeyi amaçlayan bir tedbirdir.

DSA, bazı içerik türlerinin hukuka aykırı içerik olarak kabul edilmediğini de açıkça belirtir. Örneğin, bir potansiyel suçun görgü tanığı videosu, sadece hukuka aykırı bir eylemi tasvir ettiği için hukuka aykırı içerik olarak kabul edilmez, yeter ki bu videonun kaydedilmesi veya kamuya yayılması ulusal veya Birlik hukuku uyarınca hukuka aykırı olmasın³⁶².

DSA, "yanlış bilgi" (*misinformation*) ve "dezenformasyon" (*disinformation*) gibi kavramları açıkça tanımlamasa da bu terimlere atıfta bulunmakta ve özellikle risk değerlendirmeleri ve kriz müdahale mekanizmaları bağlamında bunlarla

³⁶¹ Digital Services Act (DSA), Gerekçe 87.

³⁶² Digital Services Act (DSA), Gerekçe 12.

mücadele etmeyi hedeflemektedir. Bu tür içerikler genellikle “zararlı içerik” (*harmful content*) kategorisine girer ve doğrudan yasalara aykırı olmayabilir³⁶³.

Kategori	Örnek İçerik Türleri	İlgili DSA Hükümleri Yasal Bağlam
İçeriğin Kendisi Hukuka Aykırı Olanlar	Hukuka Aykırı Nefret Söylemi	DSA m. 3/h, Üye Devlet Hukuku, AB Çerçeve Kararı 2008/913/JHA, DSA Beyanlar
	Terör İçeriği	DSA m. 3/h, AB Terör İçeriği Yayılımını Engelleme Tüzüğü (TERREG)
	Hukuka Aykırı Ayrımcı İçerik	DSA m. 3/h, AB Ayrımcılıkla Mücadele Hukuku
	Çocuk Cinsel İstismarı Görüntüleri	DSA m. 3/h, AB Çocuk İstismarı Direktifi
	Özel Görüntülerin Rızasız Paylaşımı	DSA m. 3/h, Ulusal Kişisel Veri Koruma Yasaları
	Çevrimiçi Takip (<i>Stalking</i>)	DSA m. 3/h, Ulusal Ceza Hukuku

³⁶³ ABRUSCI, “The UK Online Safety Act, the EU Digital Services Act and Online Disinformation: Is the Right to Political Participation Adequately Protected?”, 451.

	Telif Hakkıyla Korunan Materyalin İzinsiz Kullanımı	DSA m. 3/h, AB Telif Hakkı Direktifleri
Hukuka Aykırı Faaliyetlerle İlişkili Olanlar	Uyumsuz veya Sahte Ürünlerin Satışı	DSA m. 3/h, AB Tüketici Koruma Hukuku, Ürün Güvenliği Direktifleri
	Tüketici Koruma Hukukunu İhlal Eden Hizmetler	DSA m. 3/h, AB Tüketici Koruma Hukuku
	Hukuka Aykırı Konaklama Hizmeti Teklifleri	DSA m. 3/h, Ulusal Konaklama Yasaları
	Canlı Hayvanların Hukuka Aykırı Satışı	DSA m. 3/h, Ulusal Hayvan Refahı Yasaları
Hukuka Aykırı Olmayan Ancak Zararlı Olabilecekler	Dezenformasyon ve Yanlış Bilgi	DSA'nın ana maddelerinde doğrudan hukuka aykırı olarak tanımlanmaz ancak sistemik risk değerlendirmeleri ve kriz müdahale mekanizmalarında ele alınır

	Algı Yönetimi	DSA’da doğrudan hukuka aykırı olarak tanımlanmaz ancak sistemik risk değerlendirmelerinde ele alınır.
--	---------------	---

Şema 10: Hukuka Aykırı İçerik Örnekleri

2. Unsurları

Hukuka aykırı içerik kavramı, hukuki ve pratik açıdan önemli karmaşıklıklar içeren üç temel unsurdan meydana gelmektedir: (1) bilginin niteliği, (2) hukuka aykırılığın kaynağı ve (3) hukuka aykırılığın ortaya çıkış şekli.

DSA’nın tanımında yer alan “herhangi bir bilgi” ifadesi, kapsamı bilinçli olarak son derece geniş tutmaktadır. Bu ifade, düzenlemenin belirli bir teknoloji veya içerik formatıyla (metin, görsel, video vb.) sınırlı kalmasını engelleyerek gelecekte ortaya çıkabilecek yeni iletişim ve içerik türlerini de kapsamasını amaçlayan “teknoloji-nötr” bir yaklaşımdır. Bu genişlik, platformların sorumluluğunun yalnızca kullanıcı tarafından oluşturulan bariz içeriklerle sınırlı olmayıp aynı zamanda reklamlar, ürün listelemeleri, hizmet teklifleri ve hatta kullanıcı profilleri gibi ticari faaliyetlerle ilişkili bilgileri de içermektedir. Bu durum, DSA’nın sadece ifade özgürlüğü bağlamındaki içerikleri değil, aynı zamanda tüketici hakları, ürün güvenliği ve hukuka aykırı ticaret gibi çok daha geniş bir yasal alanı düzenleme hedefini ortaya koymaktadır.

Hukuka aykırı içerik tanımının en çok tartışılan ve en karmaşık unsurunu, hukuka aykırılığın kaynağını belirleyen çift referanslı yapısı oluşturmaktadır. Tanım, içeriğin “Birlik hukukuna veya Birlik hukukuna uygun olan herhangi bir üye devlet hukukuna” aykırı olmasını yeterli görmektedir. Bu yapı, önemli hukuki sonuçlar doğurur:

- ETD’den Ayrışma: Bu yaklaşım, ETD’nin temelini oluşturan ve hizmet sağlayıcının yerleşik olduğu ülkenin hukukunun uygulanmasını öngören “menşe ülke” ilkesinden (*country of origin principle*) önemli bir sapmadır. DSA ile birlikte platformlar, artık yalnızca kendi yerleşik oldukları ülkenin değil, hizmet sundukları her bir AB üyesi ülkenin ilgili ulusal yasalarına uymakla yükümlü hale gelmiştir.
- Hukuki Belirsizlik ve Parçalanma (*Fragmentation*): Platformların 27 farklı üye devletin potansiyel olarak birbirinden farklı ulusal yasalarını (örneğin, farklı nefret söylemi, hakaret veya dezenformasyon tanımlarını) takip etme ve uygulama zorunluluğu, ciddi bir hukuki belirsizlik ve uygulama yükü oluşturacaktır. Bir içeriğin bir ülkede yasal iken diğerinde hukuka aykırı sayılabilmesi, platformların yeknesak bir içerik politikası uygulamasını güçleştirecektir.
- “En Düşük Ortak Payda” Riski ve “Brüksel Etkisi”: Ağır para cezalarıyla karşılaşma riskinden kaçınmak isteyen küresel platformlar, tüm AB için en kısıtlayıcı ulusal yasayı standart olarak benimseme eğilimine girebilecektir. Bu “en düşük ortak payda” (*lowest common denominator*) yaklaşımı, ifade özgürlüğü üzerinde genel bir “caydırıcı etki” (*chilling effect*) oluşturma potansiyeli taşır.

DSA, bir bilginin hukuka aykırı sayılabilmesi için iki alternatif yol öngörmektedir:

- İçeriğin Kendiliğinden Hukuka Aykırı Olması: Bu kategori, bilginin içeriğinin doğası gereği hukuka aykırı olduğu durumları kapsar. En net örnekler arasında terör propagandası, çocuk cinsel istismar materyalleri veya Birlik düzeyinde tanımlanmış hukuka aykırı nefret söylemi yer alır. Bu tür içerikler, bağlamdan büyük ölçüde bağımsız olarak varlıkları ve yayılmaları itibarıyla hukuka aykırıdır.
- Hukuka Aykırı Bir Faaliyetle İlişkili Olması: Bu kategori, DSA’nın getirdiği önemli bir genişlemedir. Burada içeriğin kendisi yasal olabilir

ancak hukuka aykırı bir eylemi, ürünü veya hizmeti konu aldığı için hukuka aykırı hale gelir. Örneğin, sahte veya tehlikeli bir ürünün satışına yönelik bir ilan, telif hakkı ihlaliyle elde edilmiş bir eserin hukuka aykırı kopyasını sunan bir bağlantı veya lisanssız bir konaklama hizmeti teklifi bu kapsama girer. Bu unsur, platformları yalnızca zararlı ifadeleri değil, aynı zamanda hukuka aykırı ticaret ve haksız rekabet gibi ekonomik faaliyetleri de denetlemekle sorumlu kılarak onları dijital pazarın düzenlenmesinde daha aktif bir role zorlamaktadır.

3. Sınırlandırılması

DSA, çevrimiçi ortamda hukuka aykırı içeriğin etkin bir şekilde ele alınması ile kullanıcıların temel hak ve özgürlüklerinin korunması arasında karmaşık bir denge kurmayı hedeflemektedir. Bu denge, özellikle ifade özgürlüğü, bilgi edinme hakkı, orantılılık ve gereklilik ilkeleri çerçevesinde şekillenmektedir.

DSA, hukuka aykırı içeriğin kaldırılması ve kullanıcıların temel haklarının, özellikle ifade özgürlüğü ve bilgi edinme hakkının korunması arasında bir denge kurmayı amaçlar. Ancak DSA'nın hukuka aykırı içerik tanımının genişliği ve üye devlet yasalarına atıfta bulunması, ifade özgürlüğü üzerinde "en düşük ortak payda" sansürüne yol açabilecektir.

DSA'nın hukuka aykırı içeriği herhangi bir üye devlet hukukuna bağlayan geniş tanımı ve ağır para cezaları, platformları "aşırı kaldırmaya" (*over removal*) teşvik eden güçlü bir mekanizma oluşturmaktadır³⁶⁴. Bu durum, "Brüksel Etkisi" olarak bilinen bir olguya yol açabilir³⁶⁵. Zira AB düzenlemeleri küresel standartları

³⁶⁴ TURILLAZZI vd., "The Digital Services Act: An Analysis of Its Ethical, Legal, and Social Implications", 94.

³⁶⁵ NUNZIATO, "The Digital Services Act and the Brussels Effect on Platform Content Moderation", 122.

fiilen belirleyebilir. Bu, DSA'nın ifade özgürlüğü üzerindeki etkisinin AB sınırlarının ötesine geçtiği anlamına gelmektedir.

C. İFADE ÖZGÜRLÜĞÜ VE HUKUKA AYKIRI İÇERİK AÇISINDAN VERİLEN KARARLAR

Çalışmanın bu bölümünde ifade özgürlüğü ve hukuka aykırı içerik teorik açıdan incelendikten sonra uygulamada bu kavramların nasıl vücut bulduğu açıklanması gerekmektedir. Bu doğrultuda bu iki kavramla ilgili olan mahkeme kararlarına yer verilecektir.

Öncelikle AB Adalet Divanı'nın DSA öncesi dönemde verdiği iki karara bakmak gerekmektedir: *Peterson v Google/YouTube* ve *Elsevier v Cyando* (C-682/18 ve C-683/18). 22 Haziran 2021 tarihli bu kararlar³⁶⁶, DSA öncesi dönemde çevrimiçi platformların kullanıcılar tarafından yüklenen telif hakkı ihlal eden içerikten sorumluluğunu ele almıştır. Avrupa Adalet Divanı, bir video paylaşım veya dosya barındırma platformunun işletmecisinin, telif hakkı ihlali durumunda içeriğe erişim sağlamaya platformu kullanıma sunmanın ötesinde katkıda bulunmadıkça “kamuya iletim” yapmadığına hükmetmiştir.

Sorumluluk, işletmecinin platformunda hukuka aykırı içeriğin bulunduğu dair *belirli bilgiye* sahip olması ve derhal kaldırmaması veya erişimi engellememesi durumunda ortaya çıkar. Ayrıca genel bilgiye rağmen işletmecinin telif hakkı ihlallerine etkili bir şekilde karşı koymak için makul ölçüde özenli bir işletmeciden beklenen *uygun teknolojik önlemleri* uygulamaması durumunda da sorumluluk doğabilir. Mahkeme, platformun finansal modelinin hukuka aykırı içerik paylaşımını teşvik edip etmediğini de değerlendirmiştir.

Peterson ve *Elsevier* kararları, DSA'dan önce verilmiş olsa da aracı sorumluluğu ve hukuka aykırı içerik, özellikle telif hakkı ihlali konularında temel

³⁶⁶ *Peterson v Google/YouTube* ve *Elsevier v Cyando* (C-682/18 ve C-683/18) kararları için bkz. <https://curia.europa.eu/juris/document/document.jsf?text=&docid=243241&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=5112081>

ilkeler belirlemiştir. Platformların rolü “nötr” (teknik, otomatik, pasif) ise sorumlu tutulmadığı ancak “belirli bilgiye” sahip olmaları veya “uygun teknolojik önlemleri” uygulamamaları ya da finansal modellerinin hukuka aykırı içeriği teşvik etmesi durumunda bu muafiyeti kaybettikleri temel fikri, DSA’nın sorumluluk muafiyetlerini ve özen yükümlülüklerini doğrudan etkilemiştir. Bu “aktif rol” kriteri³⁶⁷, DSA’nın bildirim ve eylem mekanizmalarının ve güvenilir işaretleyici kavramının doğrudan yasama yanıtlarıdır. DSA’nın VLOP’lar ve VLOSE’ler için getirdiği daha sıkı kurallar, platformları hukuka aykırı içeriği yönetmede “aktif bir rol” üstlenmeye itmekte, böylece yalnızca barındırma hizmeti sağlayıcılarından beklenen “tarafsızlık” ilkesinin ötesine geçmektedir.

DSA sonrası dönemde ise AB Komisyonu ile Amazon arasındaki dava (C-639/23 P(R)) dikkat çekmektedir. 27 Mart 2024 tarihli bu karar, Avrupa Komisyonu’nun Amazon Store’u VLOP olarak belirlemesi ve Amazon’un bu karara karşı aldığı ihtiyati tedbir başvurusunu ele almıştır³⁶⁸. Dava, özellikle DSA m. 39 uyarınca reklam deposunun kamuya açık hale getirilmesi yükümlülüğü etrafında dönmüştür. Mahkeme, Genel Mahkeme’nin tarafların dinlenmesi ilkesini ihlal ettiğini tespit etmiş ve Amazon’un gizli ticari bilgilerinin açıklanmasıyla ciddi ve telafisi imkânsız zarara uğrayabileceği yönündeki argümanını kabul etmiştir. Ancak Mahkeme, AB yasama organının (kamu yararı) çıkarlarının Amazon’un (ticari sırların ifşası) çıkarlarından üstün olduğuna karar vermiştir.

AB Komisyonu/Amazon davası, DSA uygulamasının pratik zorluklarını, özellikle de düzenleyici şeffaflık hedefleri (DSA m. 39’da düzenlenen reklam deposu) ile temel haklar (iş yapma özgürlüğü ve mahremiyet) arasındaki dengeyi göstermektedir. AB Adalet Divanı’nın, ticari sırların ifşasından kaynaklanan ciddi

³⁶⁷ İpek ÇEVİK, “Avrupa Birliği Dijital Hizmetler Yasası’nın Değerlendirmesi”, *Yıldırım Beyazıt Hukuk Dergisi*, sy 2 (2023): 394-95, <https://doi.org/10.33432/ybuhukuk.1273986>.

³⁶⁸ AB Komisyonu v. Amazon C-639/23 P(R) kararı için bkz. <https://curia.europa.eu/juris/document/document.jsf?text=&docid=284262&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=5112081>.

ve telafisi imkânsız zararı kabul etmesine rağmen AB yasama organının kamu yararı hedeflerini Amazon'un ticari çıkarlarına üstün tutma kararı, DSA uygulamasında güçlü bir duruş sergilemektedir. Bu karar, DSA'nın platform iş modellerini daha fazla hesap verebilirlik ve şeffaflık yönünde temelden yeniden şekillendirme hedefini vurgulamakta, ticari gizliliğin bile bu hedeflere tabi olabileceğini göstermektedir. Bu durum, platformların gelecekte DSA yükümlülüklerine ekonomik veya temel haklar gerekçesiyle itiraz ettiği davalar için bir emsal teşkil edecektir.

Öte yandan Avrupa Komisyonu, DSA'nın temel uygulama gerekliliklerine uymadıkları gerekçesiyle Çek Cumhuriyeti, İspanya, Kıbrıs, Polonya ve Portekiz'i AB Adalet Divanı'na sevk etmiştir³⁶⁹. Bu ülkelerin, DSA'nın merkezi bir unsuru olan ulusal Dijital Hizmet Koordinatörlerini (DSC) atayamadıkları veya yetkilendiremedikleri ve platformlara DSA kurallarını ihlal etmeleri durumunda ceza uygulama için gerekli yasal çerçeveyi oluşturamadıkları belirtilmiştir.

Komisyonun beş üye devleti uyumsuzluk nedeniyle AB Adalet Divanı'na sevk etmesi, önemli bir uygulama zorluğunu ortaya koymaktadır: uygulamanın ulusal yetkililere (DSC'ler) bağımlılığı. Üye devletlerin gerekli uygulama altyapısını kuramaması, DSA'nın AB genelinde tek tip uygulanmasını tehlikeye atmaktadır. DSC'lerin atanmasındaki ve ceza çerçevelerinin oluşturulmasındaki gecikmeler ve başarısızlıklar, "katmanlı sorumluluklar" yaklaşımının önemli engellerle karşılaştığını ve potansiyel olarak AB genelinde düzensiz uygulamalara yol açabileceğini göstermektedir. Bu durum aynı zamanda AB Komisyonu'nun, üye devletleri mahkemeye vermeyi gerektirse bile yasanın tek tip uygulanmasını sağlama konusundaki kararlılığını göstermektedir.

AB Adalet Divanı tarafındaki yargısal gelişmelerden sonra AIHM tarafındaki gelişmelere bakmak gerekmektedir. Bu kapsamda Delfi AS/Estonya,

³⁶⁹ <https://digital-strategy.ec.europa.eu/en/news/commission-decides-refer-czechia-spain-cyprus-poland-and-portugal-court-justice-european-union-due?>

Magyar Tartalomszolgálatók Egyesülete/Macaristan, Sanchez/Fransa ve Zöchling/Avusturya kararları incelenecektir.

Delfi AS v Estonya kararı³⁷⁰, çevrimiçi bir haber sitesinin “açıkça hukuka aykırı” kullanıcı yorumlarından (nefret söylemi veya şiddete teşvik dahil) sorumlu tutulmasının ifade özgürlüğünü ihlal etmediğini belirlemiştir. Bu karar, çevrimiçi haber sitelerinin yorum bölümleri üzerindeki kontrolü nedeniyle sorumlu tutulabileceğini ima etmiştir.

Sanchez v Fransa kararı³⁷¹, bir Facebook kullanıcısının nefret dolu üçüncü taraf yorumlarını silmemesi nedeniyle cezai sorumluluğa tabi tutulduğu ilk davadır. Mahkeme, tüm ilgili aktörler arasında “sorumluluğun paylaşılması” gerektiğini vurgulamış ve “açıkça hukuka aykırı” yorumlar için bildirim olmasa bile minimum düzeyde sonraki denetim veya otomatik filtrelemenin arzu edilebilir olduğunu belirtmiştir³⁷².

AİHM’nin *Sanchez* ve *Delfi* kararlarında belirtilen minimum düzeyde sonraki denetim veya otomatik filtreleme yaklaşımı, DSA’nın genel izleme yasağıyla potansiyel bir çatışma meydana getirmektedir. Bu durum, platformların, özellikle de VLOP’ların, yasal sorumluluktan kaçınmak ve hızlı kaldırma gerekliliklerini (örneğin 24 saat kuralı) karşılamak için daha proaktif içerik denetim mekanizmaları geliştirmesi gerektiği anlamına gelebilir³⁷³.

DSA, genel izleme yükümlülüğünü açıkça yasaklasa da AİHM’nin *Sanchez* ve *Delfi* gibi kararları, açıkça hukuka aykırı içerik için belirli düzeyde proaktif tespitin arzu edilebilir olduğunu düşündürmektedir. Bu durum, platformlar üzerinde, özellikle de sistemik risk yükümlülükleri olan VLOP’lar ve VLOSE’ler üzerinde, nefret söylemi veya çocuk cinsel istismarı materyali gibi ciddi hukuka aykırı içerikler için bir tür sürekli tarama yapma baskısı oluşturmaktadır. Bu,

³⁷⁰ Karar için bkz. [https://hudoc.echr.coe.int/fre#{%22itemid%22:\[%22001-155105%22\]}](https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-155105%22]}).

³⁷¹ Karar için bkz. <https://hudoc.echr.coe.int/eng?i=001-224928>.

³⁷² ENARSSON, “Navigating Hate Speech and Content Moderation Under the DSA”, 393.

³⁷³ ENARSSON, “Navigating Hate Speech and Content Moderation Under the DSA”, 393.

DSA'nın açık yasağının sınırlarını belirsizleştirebilir ve platformların daha ileri düzey otomatik araçlar kullanmasına yol açabilir.

AB Adalet Divanı ve AİHM uygulamasından sonra AB üyesi devletlerdeki ilgili kararlara bakılması gerekmektedir. Bu kararlardan ilki, Hollanda Amsterdam Bölge Mahkemesi tarafından görülen *Applicant/Twitter* (ECLI:NL:RBAMS:2024:3980) davasıdır³⁷⁴. 5 Temmuz 2024 tarihli bu karar, X (eski adıyla Twitter) platformunun bir kullanıcının hesabına uyguladığı “gölge yasaklama” (*shadow banning*) ve arama kısıtlamalarıyla ilgilidir. Mahkeme, gölge yasaklamanın DSA m. 17 (gerekçe beyanı) kapsamına girdiğine ve bu nedenle platformun kısıtlamaların nedenlerine ilişkin bir gerekçe sunması gerektiğine hükmetmiştir. Bu karar, platformların içerik denetimi kararlarında şeffaflık ve gerekçelendirme yükümlülüğünün önemini göstermektedir.

Applicant/Twitter davası, DSA m. 17'nin doğrudan uygulanmasını göstermekte ve platformların içerik denetimi kararları için gerekçe sunma zorunluluğunu pekiştirmektedir. Mahkemenin gölge yasaklamanın bu kapsama girdiğine hükmetmesi, DSA'nın platformların içerik denetimi uygulamaları üzerindeki somut etkisini ortaya koymaktadır. Bu durum, platformların şeffaflık ve hesap verebilirlik konusunda daha fazla çaba göstermesini gerektirmekte, kullanıcıları güçlendirmekte ve platformların opak denetim uygulamalarını sınırlayabilecektir.

Diğer bir üye devlet olan Almanya'nın 2017'de yürürlüğe giren Ağ Yaptırım Kanunu (NetzDG)³⁷⁵, sosyal medya platformlarında nefret söylemi ve yalan haberlerle mücadele etmeyi amaçlayan öncü bir ulusal düzenlemedir. NetzDG, açıkça hukuka aykırı içeriğin 24 saat içinde, daha belirsiz içeriğin ise 7 gün içinde kaldırılmasını zorunlu kılmıştır.

³⁷⁴ Karar için bkz. <https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RBAMS:2024:3980>.

³⁷⁵ Kanun metni için bkz. <https://www.gesetze-im-internet.de/netzdg/BjNR335210017.html>.

DSA, NetzDG gibi ulusal yasaları uyumlu hale getirmeyi hedeflemiş ve NetzDG'nin büyük ölçüde DSA tarafından yürürlükten kaldırılmasına yol açmıştır. Ancak, NetzDG'nin getirdiği şeffaflık raporlama ve şikâyet prosedürleri gibi bazı unsurlar DSA'ya ilham vermiştir.

Belçika'da izleme tabanlı reklamların hukuka aykırı olduğuna dair mahkeme kararı³⁷⁶, DSA'nın reklam şeffaflığı ve kişisel veri kullanımına ilişkin hükümlerinin uygulama alanını göstermektedir.

PROBLEMİN ÇÖZÜMÜ: DENGİ

Bu çalışma kapsamında önceki bölümlerde sosyal medya ve yapay zekâ olguları hem teknik hem de hukuki zeminde incelenmiştir. Bu inceleme sonucunda hem 5651 sayılı Kanun hem DSA hem de AI Act ile uyumlu bir model önerilmektedir. Modelin ismi, DENGİ'dir (Dijital Etkileşimde Norm ve Güvence Ekosistemi).

Mevcut sosyal medya içerik denetim sistemlerinin temel kusuru, teknolojik bir soruna salt teknolojik bir çözümle (bağlamdan kopuk yapay zekâ ile) yaklaşımlarıdır. Bu yaklaşım, hukukun temel ilkelerini ve toplumsal gerçeklikleri göz ardı etmektedir. Bunun sonucunda ifade özgürlüğünü sistematik olarak ezen, “yanlış pozitif” kararlarla hukuka uygun ifadeleri cezalandıran ve kullanıcıyı yabancılaştıran, şeffaflıktan uzak bir “kara kutu” sistemidir.

Burada sunulan mimari, bu sığ bakış açısını reddetmektedir. Sorunu “farklı yasal ve kültürel bağlamlarda ifade özgürlüğü ile çevrimiçi güvenliği, teknolojik verimlilikle nasıl dengeleyebiliriz?” şeklinde yeniden tanımlamaktadır. Çözüm daha akıllı bir algoritma değil, bu algoritmayı hukuki güvencelerle donatan, şeffaf süreçlerle yöneten ve toplumsal katılımı merkeze alan entegre bir ekosistemidir.

DENGİ ile dört temel noktanın uyumlu olması hedeflenmektedir:

³⁷⁶ Resmî karar metni için bkz. <https://www.iccl.ie/wp-content/uploads/2025/05/Arrest-Marktenhof-14-05-2025.pdf>.

- **Hukuki Denge:** Bu, en temel dengedir. Önerilen model, bir yanda Anayasa ve uluslararası sözleşmelerle korunan ifade özgürlüğü ile diğer yanda 5651 sayılı Kanun, DSA, AI Act gibi düzenlemelerin ve toplumsal beklentilerin gerektirdiği kamu güvenliği ve birey haklarının korunması arasındaki hassas çizgide yürümelidir. DENGİ, bu iki temel değeri birbirine feda etmeden orantılı ve adil bir denge noktası bulmayı amaçlamaktadır.
- **Teknolojik Denge:** Yapay zekânın ölçek ve hız avantajı ile insan zekânının detay, empati ve bilgelik kapasitesi arasında denge kurulmalıdır. Yapay zekâ, milyonlarca içeriği saniyeler içinde tarayarak ilk elemeyi yapmalı ve “bilirkişi” raporunu sunmalıdır. Ancak nihai karar, özellikle “gri alanlarda” her zaman bir insanın denetimine bırakılmalıdır.
- **Kültürel Denge:** Modelin en yenilikçi yönlerinden biri, küresel platformların tek tip kuralları ile yerel kültürel ve dilsel gerçeklikler arasında bir denge kurmasıdır.
- **Operasyonel Denge:** Tamamen insana dayalı denetim çok pahalı, tamamen yapay zekâyâ dayalı denetim ise hatalı ve güvensizdir. Önerilen model maliyetleri düşürürken kullanıcı güvenliğini ve memnuniyetini artırarak platformun uzun vadeli sağlığını güvence altına almayı hedeflemektedir.

DENGİ mimari yapısı 4 ana katmandan oluşmalıdır: teknolojik çekirdek, usuli çerçeve ve platform yönetimi, yönetim, şeffaflık ve hesap verilebilirlik ve yetkili kullanıcı ve toplumsal katılım.

Katman 1: Teknolojik Çekirdek

Bu katman, deyim yerindeyse DENGİ’nin “motoru”dur. Bu katman sayesinde yapay zekâ, “infazcı” olmaktan çıkarak kültürel yetkinliğe sahip bir “bilirkişi” niteliğini haiz olmaktadır. Bu katman 4 alt modülden oluşmalıdır:

Modül 1: Akıllı Sınıflandırma

Bu modül, sosyal medya platformuna yüklenen her içeriği ilk karşılayan yerdir. Gelen içeriği denetim önceliğine göre metin, görsel ve ses analiziyle “siyasi tartışma”, “dini metin”, “mizah/hiciv”, “sanatsal ifade”, “kişisel görüş”, “haber metni” gibi sınıflandırır. Her kategoriye atanmış varsayılan bir risk ve hassasiyet puanı bulunur. Örneğin "hiciv" olarak etiketlenen bir içerik, sonraki modülde daha farklı parametrelerle incelenir.

Modül 2: Kültürel Bağlam

Bu modül ise sistemin kalbi olarak nitelenebilir. Akıllı sınıflandırma motorundan geçen “belirsiz” veya “hassas” olarak işaretlenen içerikleri derinlemesine analiz eder. Bu modül, Türkiye Türkçesine özel, zengin bir veri setiyle eğitilmiş bir Büyük Dil Modelini (LLM) temel almalıdır. Bu dil modelinin veri seti rastgele kaynaklardan seçilmemeli ve en azından şunları içermelidir:

- Türk Edebiyatı Klasikleri ve modern eserler.
- TDK Atasözleri ve Deyimler Sözlüğü.
- TBMM tutanakları (siyasi dilin analizi için).
- Yargıtay kararları (hakaret, nefret söylemi gibi hukuki kavramların metin içi karşılıkları için).
- Anonimleştirilmiş ve izinli sosyal medya verileri.
- Diyanet tarafından onaylanmış temel dini metinler ve tefsirler (dini ifadelerin yanlış yorumlanmasını önlemek için).

Modül 3: Şeffaf Raporlama ve Açıklanabilir Yapay Zekâ (XAI)

Bu modül ile önceki başlıklarda ifade edildiği üzere “kara kutu” sorunu çözülmek istenmektedir. Bu modül, bir içerik hakkında neden olumsuz bir karar eğilimi oluştuğunu insan tarafından okunabilir bir formatta raporlar. Örnek bir rapor çıktısı şöyle olmalıdır:

- İçerik ID: 892374

- Potansiyel İhlal: Topluluk Kuralları - Nefret Söylemi (%78 olasılık)
- Tetikleyici Unsurlar: “hain” (%60 katkı), “hesap verecekler” (%18 katkı)
- Bağlamsal Not (Modül 2’den): İçerik, bir siyasi parti liderinin konuşmasından alıntıdır. Bağlam: Siyasi Eleştiri.
- Öneri: İnsan denetimine sevk edilsin. Düşük öncelikli.

Şeffaflık, denetimle anlam kazanır. İlgili sosyal ağ sağlayıcı ve/veya yapay zekâ sağlayıcısı, yerleştiricisi, dağıtıcısı, DENGİ’nin anonimleştirilmiş verilerini ve modellerini, gizlilik anlaşmaları çerçevesinde bağımsız akademisyenlerin ve sivil toplum kuruluşlarının denetimine açmalıdır. BTK, Yapay Zekâ Ofisi gibi düzenleyici kurumlar, bu veriler üzerinden “algoritmik denetim” yaparak platformların yasalara uyumunu ve sistemik riskleri daha etkin bir şekilde izleyebilir. Bu, DSA’ya ve AI Act’e uygundur.

Modül 4: İnsan Destekli Karar Sistemi

Bu modül ile insan denetçilerin en verimli ve doğru kararı verebilmesi için bir web arayüzü sunulmalıdır. Denetçinin ekranında şu unsurlar yer almalıdır:

- Orijinal içerik.
- Modül 3’ten gelen XAI raporu.
- Kullanıcının geçmişteki benzer içeriklerinin durumu (anonimleştirilmiş).
- Tek tıkla karar seçenekleri: “Onayla (Zararsız)”, “Etiketle (Hassas İçerik)”, “Kaldır (Kural İhlali)”, “Üst Kurula Sevk Et”.

Verilen her insan kararı, sistemin kendini geliştirmesi için geri besleme (*feedback loop*) olarak kullanılır ve Modül 2’deki LLM’nin sürekli olarak daha akıllı hale gelmesini sağlar (*Reinforcement Learning from Human Feedback - RLHF*).

Bu katmanın çalışma prensibi şöyle olmalıdır:

1. İçerik yüklenir.
2. Modül 1, içeriği tarar. Bariz spam/hukuka aykırı ise karantinaya alır, değilse risk/konu kategorisine göre etiketleyip Modül 2’ye gönderir.

3. Modül 2, kültürel ve anlamsal analiz yapar.
4. Modül 3, analizi bir skor ve anlaşılır bir rapora dönüştürür.
5. Karar Mantığı: Risk Skoru $< \%20$ ise içerik otomatik onaylanır. Risk Skoru $> \%85$ ise içerik doğrudan Modül 4'teki insan denetçinin önüne düşer. $\%20 < \text{Risk Skoru} < \%85$ ise "Gri Alan" olarak işaretlenir ve insan denetçiye sunulur.
6. İnsan denetçi, Modül 4 arayüzünü kullanarak nihai kararı verir. Bu karar, kullanıcıya XAI raporuyla birlikte bildirilir.
7. Verilen karar, gelecekteki kararların isabet oranını artırmak için sisteme geri beslenir.

Katman 2: Usuli Çerçeve ve Platform Yönetimi

Bu katmanda yukarıdaki süreç sonunda oluşan teknik veri, kullanıcılar için adil ve şeffaf bir platform sürecine dönüştürülür. Burada kullanıcı, içeriğinin kaldırılmasına önce itiraz etmektedir. Bu itiraz, sistemin farklı bir parametre setiyle içeriği yeniden analiz etmesini tetiklemelidir. Kullanıcının itirazı devam ediyorsa yukarıda bahsedilen XAI raporu uzman denetçiye gönderilmelidir. Bu doğrultuda denetçi algoritmanın neyi neden işaretlediğini görmelidir. Bu, denetçi kararının verimini ve doğruluğunu artıracaktır. Bu sürecin devam etmesi durumunda ise ilgili sosyal ağ sağlayıcıdan bağımsız olarak oluşturulan hakem kurulları hem sistemin ürettiği raporu hem de kullanıcının savunmasını dikkate alarak karar vermelidir.

Katman 3: Yönetişim, Şeffaflık ve Hesap Verilebilirlik

Bu katmanda 5651 sayılı Kanun gibi düzenlemeler kapsamında platformların yayımlamak zorunda olduğu şeffaflık raporları, DENGİ sayesinde çok daha anlamlı hale gelir. Platformlar sadece "10.000 içerik nefret söylemi nedeniyle kaldırıldı" demek yerine, DENGİ'den elde edilen anonimleştirilmiş verilerle "Kaldırılan içeriklerin $\%30$ 'unda "x" kelimesi, $\%20$ 'sinde "y" görseli tetikleyici oldu. İtiraz edilen kararların $\%15$ 'i insan denetçiler tarafından "hiciv"

bağlamı nedeniyle geri çevrildi” gibi derinlemesine analizler sunabilir. Bu, BTK, DHK, ADHK gibi kurumların “algoritmik denetim” yapabilmesini sağlayacaktır.

Katman 4: Yetkili Kullanıcı ve Toplumsal Katılım

Bu katmanda bir kullanıcının içeriği kaldırıldığında kendisine DENGİ’nin ürettiği basitleştirilmiş XAI raporu sunulur. “İçeriğiniz, “...” ifadesinin nefret söylemiyle ilişkilendirilme olasılığının yüksek bulunması nedeniyle incelenmek üzere işaretlenmiştir” gibi bir bildirim, cezalandırıcı bir dilden ziyade eğitici bir rol üstlenir. Bu, kullanıcıların platform kurallarını, dijital dünyanın örf ve adetini ve ahlakını daha iyi anlamasına yardımcı olur.

Herkes için tek bir doğru akış oluşturmak yerine kontrolün kullanıcıya devredilmesi gerekir. Kullanıcıya gelişmiş filtreleme araçları sunarak görmek istemedikleri içerik türlerini (örneğin, siyasi tartışmalar, şiddet içeren haberler) kendi hassasiyet eşiklerine göre yönetmeleri sağlanmalıdır. Bu, sorumluluğu dağıtır ve platformu daha kişisel bir alan haline getirir.

SONUÇ

21. yüzyılın toplumsal yaşamını ve dinamiklerini derinden etkileyen ve bu çalışmanın temelini oluşturan iki oyun değiştirici olgu olan sosyal medya ve yapay zekânın etkileşimi, çok katmanlı ve karmaşık bir hukuki çerçeve içerisinde incelenmiştir. Bu çalışma, söz konusu iki olgunun teknik, kavramsal ve hukuki boyutlarını bir araya getirerek bu etkileşimin temel hak ve özgürlükler, özellikle de ifade özgürlüğü üzerindeki yansımalarını ve bu alandaki hukuki düzenleme çabalarını bütüncül bir yaklaşımla ele almayı hedeflemiştir.

Çalışmanın birinci bölümünde, sosyal medya ve yapay zekâ olgularının kavramsal ve tarihsel temelleri atılmıştır. Bu bölümde sosyal medya, Web 1.0’ın tek yönlü yapısından Web 2.0 ile gelen çift yönlü etkileşime ve Web 3.0’ın getirdiği yeni olanaklara uzanan bir çizgide incelenmiştir. Türkiye özelinde, sosyal medya ekosistemini oluşturan içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı, toplu kullanım sağlayıcı ve 7253 sayılı Kanun ile hukukumuza giren sosyal ağ sağlayıcı gibi sùjelerin 5651 sayılı Kanun kapsamındaki tanımları ve sorumlulukları

detaylandırılmıştır. Paralel olarak yapay zekâ, tarihsel gelişim süreci, makine öğrenmesi ve derin öğrenme gibi alt dalları ile ele alınmıştır. Yapay zekânın hukuki niteliği üzerine yapılan tartışmalarda onu basit bir eşya veya Roma hukukundaki köle statüsüne indirgeyen yaklaşımların doğuracağı hukuki açmazlara dikkat çekilmiş ve *Ekici* tarafından önerilen “entegre kişilik” statüsünün en isabetli çözüm olacağı kanaatine varılmıştır. Bununla birlikte doktrinde ve hukuki düzenlemelerde henüz uzlaşa sağlanmadığı için yapay zekânın içerik sağlayıcı olarak kabul edilmesi mümkün olmadığı ifade edilmiştir.

İkinci bölümde, AB’nin bu alandaki öncü düzenlemeleri olan Dijital Hizmetler Kanunu (DSA) ve Yapay Zekâ Kanunu (AI Act), çalışmanın ana ekseninde incelenmiştir. DSA’nın, 2000 tarihli ETD’nin yetersiz kalması üzerine ihdas edildiği ve çevrimiçi platformlar için kademeli bir sorumluluk rejimi getirdiği ortaya konulmuştur. Bu rejimde, tüm sosyal ağ sağlayıcılar için irtibat noktası belirleme, şeffaf hizmet şartları sunma gibi temel yükümlülükler öngörülmektedir. Ayrıca aylık 45 milyondan fazla aktif kullanıcıya sahip Çok Büyük Çevrimiçi Platformlar (VLOP) için sistemik risklerin değerlendirilmesi ve azaltılması, bağımsız denetim ve araştırmacılara veri erişimi sağlama gibi çok daha sıkı ek yükümlülükler getirilmiştir. AI Act ise yapay zekâ sistemlerini potansiyel risk seviyelerine göre sınıflandıran “risk temelli bir yaklaşım” benimsemektedir. Bu yaklaşıma göre sosyal puanlama gibi temel haklara açık tehdit oluşturan sistemler “kabul edilemez risk” kategorisinde yasaklanmış, istihdam ve eğitim gibi hassas alanlarda kullanılanlar “yüksek riskli” kabul edilerek katı kurallara tabi tutulmuş, “deepfake” gibi içerik üreten sistemler “sınırlı riskli” sayılarak şeffaflık yükümlülüğüne bağlanmış ve spam filtreleri gibi uygulamalar ise “minimal riskli” görülerek büyük ölçüde düzenleme dışı bırakılmıştır.

Çalışmanın üçüncü ve son bölümünde ise yapay zekânın sosyal medya içeriklerine yönelik teknik müdahale biçimleri ve bu müdahalelerin hukuki yansımaları ele alınmıştır. Yapay zekânın, platformların devasa içerik hacmiyle başa çıkabilmesi için “ölçek gerekçesi” ile kaçınılmaz bir araç haline geldiği ifade edilmiştir. Müdahale türleri, platformların içerik denetimi ve “gölge yasaklama”

gibi pratiklerini içeren “platform temelli engelleme”, devletlerin Derin Paket İncelemesi (DPI) gibi teknolojilerle internet trafiğini kontrol ettiği “internet omurgası temelli engelleme”, “bireysel engelleme” ve “sosyal teknikler” olarak sınıflandırılmıştır. Bu müdahalelerin hukuki sonuçları, ifade özgürlüğü ve hukuka aykırı içerik kavramları ekseninde, Avrupa İnsan Hakları Mahkemesi (AİHM), AB Adalet Divanı ve ulusal mahkeme kararları ışığında incelenmiştir. İncelenen kararlar, AİHM’nin “açıkça hukuka aykırı” içerikler için platformlardan proaktif bir denetim beklemesi (Delfi ve Sanchez kararları) ile DSA’nın genel izleme yasağı arasındaki potansiyel çatışmayı, DSA’nın gerekçe gösterme yükümlülüğünün “gölge yasaklama” gibi şeffaf olmayan uygulamalara dahi uygulanabilir olduğunu (Applicant/Twitter kararı) ve DSA’nın etkinliğinin üye devletlerin Dijital Hizmetler Koordinatörlerini (DSC) ataması gibi uygulama adımlarını zamanında atmasına bağlı olduğunu göstermiştir.

Bu çalışma, 5651 sayılı Kanun kapsamındaki sosyal ağ sağlayıcı yükümlülükleri ile DSA’nın getirdiği rejimi karşılaştırmıştır. Her iki düzenlemenin de yurt dışı kaynaklı sağlayıcılara temsilci atama, raporlama ve resmi/bireysel başvurulara yanıt verme gibi ortak yükümlülükler getirdiği görülmektedir. Ancak DSA, VLOP’lar için getirdiği sistemik risk yönetimi, temel haklara “gereken özeni gösterme” zorunluluğu ve AB genelinde koordineli bir denetim mekanizması kurması gibi hususlarla çok daha derinlikli ve hak temelli bir çerçeve sunmaktadır. 5651 sayılı Kanun, daha çok belirli suç kataloglarına odaklanırken DSA daha geniş bir “hukuka aykırı içerik” tanımı ve “zararlı ama yasal” içeriklerin meydana getirdiği toplumsal risklerle de mücadele etmeyi hedeflemektedir.

Bu çalışma, yapay zekâ ve sosyal medya olgularını teknik, toplumsal ve hukuki boyutlarıyla bir arada ele alarak bu alandaki temel hukuki düzenlemeler olan 5651 sayılı Kanun, DSA ve AI Act’i ortak bir süzgeçten geçirerek literatüre katkı sağlamıştır. Gelineen noktada hukuki düzenlemeler, ETD’nin “sorumsuzluk” temelli yaklaşımından uzaklaşarak şeffaflık, hesap verebilirlik, risk yönetimi ve kullanıcı haklarını merkeze alan proaktif bir modele evrilmektedir. Yapay zekânın

içerik denetimindeki rolü kaçınılmazdır ancak bu otomasyonun keyfilğe ve orantısız kısıtlamalara yol açma riski bulunmaktadır. Bu bağlamda DSA, platformları kullandıkları yapay zekâ araçları hakkında şeffaf olmaya zorlayarak uygulama katmanını düzenlerken AI Act, en manipülatif sistemleri yasaklayıp diğerlerine şeffaflık yükümlülüğü getirerek temel teknolojinin kendisini düzenlemektedir. 5651 sayılı Kanun ise bu yönde atılmış bir adım olmakla birlikte AB'nin kapsamlı ve hak temelli modeline kıyasla daha dar bir çerçevede kalmaktadır.

Bu tezde çözüm olarak “DENGİ (Dijital Etkileşimde Norm ve Güvence Ekosistemi)” adlı model önerilmiştir. Modelin temel amacı, sosyal medya ve yapay zekâ etkileşiminde dört temel noktada uyum sağlamaktır. Model hukuki düzeyde ifade özgürlüğü ile kamu güvenliği arasındaki hassas dengeyi gözetmektedir. Teknolojik olarak yapay zekânın işlem gücü ile insanın bağlamsal anlama ve empati yeteneğini birleştiren hibrit bir yaklaşım önerilmektedir. Kültürel anlamda küresel platform standartlarını yerel dilsel ve toplumsal normlarla uyumlu hale getirirken operasyonel olarak ise maliyet etkinliği ile süreçlerin adaleti arasında en uygun dengeyi kurmayı hedeflemektedir. Bu çok boyutlu denge arayışı, DENGİ modelini hem teorik olarak sağlam hem de pratik olarak uygulanabilir bir çerçeve olarak konumlandırmaktadır.

Modelin mimari yapısı, bu felsefeyi hayata geçiren dört katmanlı bir sistem üzerine kuruludur. Sistemin motoru olan “Teknolojik Çekirdek” katmanı, içerikleri akıllıca sınıflandıran, Türkiye Türkçesinin kültürel ve dilsel derinliğine vakıf bir Büyük Dil Modeli (LLM) ile bağlamsal analiz yapan ve kararlarını “Açıklanabilir Yapay Zekâ (XAI)” raporlarıyla şeffaf hale getiren modüllerden oluşur. Bu katman, bariz ihlalleri ve zararsız içerikleri otonom olarak yönetirken özellikle “gri alan” olarak tanımlanan hassas ve belirsiz vakaları tecrübeli insan denetçilerin önüne gerekçeli raporlarla sunar. İnsan denetçilerin verdiği nihai kararlar, sistemi sürekli olarak eğiten bir geri besleme döngüsü (RLHF) oluşturarak modelin zamanla daha isabetli ve adil kararlar almasını sağlayacaktır.

Bu yapı, yapay zekâyı bir “infazcı” olmaktan çıkarıp insanın karar verme sürecini destekleyen yetkin bir “bilirkişi” konumuna taşıyacaktır.

Teknolojik çekirdeğin üzerinde inşa edilen diğer katmanlar ise modelin yönetsel ve toplumsal etkisini tamamlar. “Usuli Çerçeve ve Platform Yönetimi” katmanı, kullanıcılara şeffaf itiraz mekanizmaları sunarak adil yargılanma hakkını dijital alana taşır. “Yönetişim, Şeffaflık ve Hesap Verilebilirlik” katmanı, platformların düzenleyici kurumlara ve kamuoyuna yüzeysel istatistikler yerine derinlemesine analitik veriler sunmasını sağlayarak “algoritmik denetim” imkânı tanır. Son olarak “Yetkili Kullanıcı ve Toplumsal Katılım” katmanı, kullanıcılara içeriklerinin neden işaretlendiğini açıklayan eğitici bildirimler göndererek cezalandırıcı bir yaklaşımdan onarıcı ve öğretici bir diyaloga geçişi mümkün kılar. Sonuç olarak DENGİ modeli, sadece bir içerik denetim aracı olmayıp kullanıcılar, sosyal ağ sağlayıcılar ve düzenleyici otoriteler arasında güvene dayalı, şeffaf ve hesap verilebilir bir dijital ekosistem imkânı sunmaktadır.

KAYNAKÇA

- 11.10.2023 Tarihli ve E. 2020/76, K. 2023/172 Sayılı Kararı, No. 2020/76 (Anayasa Mahkemesi 11 Ekim 2023).
- 15.11.2017 Tarihli ve 2015/76 E., 2017/153 K. Sayılı Kararı, No. 2015/76 (Anayasa Mahkemesi 15 Kasım 2017).
- 29.05.2014 tarihli ve 2014/4705 Başvuru Numaralı Kararı, No. 2014/4705 (Anayasa Mahkemesi 29 Mayıs 2014).
- ABRUSCI, Elena. “The UK Online Safety Act, the EU Digital Services Act and Online Disinformation: Is the Right to Political Participation Adequately Protected?” *Journal of Media Law* 16, sy 2 (2024): 440-67. <https://doi.org/10.1080/17577632.2024.2425551>.
- AKKURT, Sinan Sami. *Sosyal Medyada Gerçekleşen İhlaller Karşısında Kişilik Hakkının Korunması*. 3. Baskı. Seçkin Yayıncılık, 2023.
- AKKURT, Sinan Sami. “Yapay Zekânın Otonom Davranışlarından Kaynaklanan Hukuki Sorumluluk”. *Uyuşmazlık Mahkemesi Dergisi*, sy 13 (2019): 39-59. <https://doi.org/10.18771/mdergi.581875>.
- AKSOY, Ecem. *Yapay Zeka’nın Sorumluluk Hukukundaki Konumu Ve Büyük Veri İle İlişkisi*. 1. Baskı. Seçkin Yayıncılık, 2022.
- AKYASAN BİRSEN, Gönül. *Sosyal Medyada Paylaşılan İçerik Nedeniyle Kişilik Hakkı İhlalleri*. 1. Baskı. Seçkin Yayıncılık, 2020.
- ARF, Cahit. “Makine Düşünebilir Mi ve Nasıl Düşünebilir?” *Atatürk Üniversitesi - Üniversite Çalışmalarını Muhite Yayma ve Halk Eğitimi Yayınları Konferanslar Serisi No: 1*, Atatürk Üniversitesi, 1959, 91-103. <https://www.mbkaya.com/hukuk/cahit-arf-makine-dusunebilir-mi-orjinal.pdf>.
- AVCI, Artun. *Türkiye’de İnternet ve İfade Özgürlüğü*. 1. Baskı. Legal Yayıncılık A.Ş., 2013.
- BACAKSIZ, Pınar ve SÜMER, Seda Yağmur. *Robotlar, Yapay Zeka ve Ceza Hukuku*. 1. Baskı. Ankara: Adalet Yayınevi, 2021.

- BERNERS-LEE, T. J., CAILLIAU, Robert ve GROFF, Jean-François. “The World-Wide Web”. *Computer Networks and ISDN Systems* 25, sy 4 (1992): 454-59. [https://doi.org/10.1016/0169-7552\(92\)90039-S](https://doi.org/10.1016/0169-7552(92)90039-S).
- BEUC. “The Digital Services Act Proposal: BEUC Position Paper”. 2021. https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-032_the_digital_services_act_proposal.pdf.
- Bilgi Teknolojileri ve İletişim Kurumu. “Sosyal Ağ Sağlayıcı Hakkında Usul ve Esaslar (2023/DK-İD/119)”. R.G. 32150, 01 Nisan 2023. <https://www.resmigazete.gov.tr/eskiler/2023/04/20230401-13.pdf>.
- BLOSSOM, John. *Content Nation: Surviving and Thriving as Social Media Changes Our Work, Our Lives, and Our Future*. 1. Baskı. Wiley Publishing, Inc., 2009.
- BOYD, Danah M. ve ELLISON, Nicole B.. “Social Network Sites: Definition, History, and Scholarship”. *Journal of Computer-Mediated Communication* 13, sy 1 (2007): 210-30. <https://doi.org/10.1111/j.1083-6101.2007.00393.x>.
- BOZKURT YÜKSEL, Armağan Ebru. *Buluşçu Yapay Zekâ ve Patent Hukuku*. 1. Baskı. Aristo Yayınevi, 2020.
- BOZKURT YÜKSEL, Armağan Ebru. *Yapay Zekâ, Endüstri 4.0 ve Robot Üreticiler Hukuki Bakış*. 1. Baskı. İstanbul: Aristo Yayınevi, 2019.
- BOZKURT YÜKSEL, Armağan Ebru ve BAK, Başak. “Yapay Zekâ”. İçinde *Futurist Hukuk*, 1. Baskı., 111. İstanbul: Aristo Yayınevi, 2018.
- BUIJS, Doris. “The Digital Services Act and the Implications for News Media and Journalistic Content (Part 1)”. DSA Observatory, 2022. <https://dsa-observatory.eu/2022/09/29/digital-services-act-implications-for-news-media-journalistic-content-part-1/>.
- BURI, Ilaria ve VAN HOBOKEN, Joris. “The Digital Services Act (DSA) Proposal: A Critical Overview”. Institute for Information Law (IViR), 2021. https://dsa-observatory.eu/wp-content/uploads/2021/11/Buri-Van-Hoboken-DSA-discussion-paper-Version-28_10_21.pdf.

CHANDER, Anupam. “When the Digital Services Act Goes Global”. *Berkeley Technology Law Journal* 38, sy 3 (2023): 1067-88.
<https://papers.ssrn.com/abstract=4606282>.

CHOUDHURY, Nupur. “World Wide Web and Its Journey from Web 1.0 to Web 4.0”. *International Journal of Computer Science and Information Technologies* 5, sy 6 (2014): 8096-100.
<https://ijcsit.com/docs/Volume%205/vol5issue06/ijcsit20140506265.pdf>

CILLIERS, Francois Quintin. “The Role and Effect of Social Media in the Workplace”. *Northern Kentucky Law Review* 40, sy 3 (2013): 567-92.

CSERNATONI, Raluca. “The EU’s AI Power Play: Between Deregulation and Innovation”. *Carnegie Europe*, 2025.
<https://carnegieendowment.org/research/2025/05/the-eus-ai-power-play-between-deregulation-and-innovation?lang=en>.

ÇEKİN, Mesut Serdar, BERKTAŞ, Ahmet Esad ve AKINCI, Muhammed Furkan. *Veri Hukuku*. 1. Baskı. On İki Levha Yayıncılık, 2023.

ÇELEBİ, Merve, ÖZBİLEN, Alper ve YAVANOĞLU, Uraz. “A Comprehensive Survey on Deep Packet Inspection for Advanced Network Traffic Analysis: Issues and Challenges”. *Niğde Ömer Halisdemir Üniversitesi Mühendislik Bilimleri Dergisi* 12, sy 1 (2023): 1-29.
<https://doi.org/10.28948/ngumuh.1184020>.

ÇEVİK, İpek. “Avrupa Birliği Dijital Hizmetler Yasası’nın Değerlendirmesi”. *Yıldırım Beyazıt Hukuk Dergisi*, sy 2 (2023): 387-419.
<https://doi.org/10.33432/ybuhukuk.1273986>.

DENİZ ÇELİK, Kübra. *Sosyal Medya Kullanımının İş Sözleşmesine Etkisi*. 1. Baskı. On İki Levha Yayıncılık, 2019.

DINUCCI, Darcy. “Fragmented Future”. *Print Magazine*, 1999.

EUROPEAN PARLIAMENT ve COUNCIL OF THE EUROPEAN UNION. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in

particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), L 178 OJ § (2000).
<http://data.europa.eu/eli/dir/2000/31/oj/eng>.

EUROPEAN PARLIAMENT ve COUNCIL OF THE EUROPEAN UNION.
Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 Laying down a Procedure for the Provision of Information in the Field of Technical Regulations and of Rules on Information Society Services, OJ L 241 § (2015).
<http://data.europa.eu/eli/dir/2015/1535/oj/eng>.

DOĞAN, Erdem. *Yapay Zekanın Hukuki Statüsü ve Sorumluluğu*. 1. Baskı. Seçkin Yayıncılık, 2022.

DÜLGER, Murat Volkan. *Bilişim Suçları ve İnternet İletişim Hukuku*. 9. Baskı. Seçkin Yayıncılık, 2022. <https://www.turcademy.com/tr/kitap/bilisim-suclari-ve-internet-iletisim-hukuku-9789750275678>.

EBERS, Martin. "Truly Risk-Based Regulation of Artificial Intelligence: How to Implement the EU's AI Act". *Stanford Law School*, sy EU Law Working Papers No: 101 (2024). <https://law.stanford.edu/publications/no-101-truly-risk-based-regulation-of-artificial-intelligence-how-to-implement-the-eus-ai-act/>.

EDOSOMWAN, Simeon, PRAKASAN, Sitalaskshmi Kalangot, KOUAME, Doriane, WATSON, Jonelle ve SEYMOUR, Tom. "The History of Social Media and its Impact on Business". *The Journal of Applied Management and Entrepreneurship* 16, sy 3 (2011).

EKİCİ, Şerafettin. *Bilişim ve Teknoloji Hukuku*. Güncellenmiş 2. Baskı. Seçkin Yayıncılık, 2023.

EKİCİ, Şerafettin. "New Proposed Personality Model for Artificial Intelligence: Integrated Personality". *Bilişim Hukuku Dergisi* 7, sy 1 (2025): 311-63. <https://doi.org/10.55009/bilisimhukukudergisi.1686538>.

ENARSSON, Therese. "Navigating Hate Speech and Content Moderation Under the DSA: Insights from ECtHR Case Law". *Information &*

Communications Technology Law 33, sy 3 (2024): 384-401.
<https://doi.org/10.1080/13600834.2024.2395579>.

EREN, Abdurrahman. *Anayasa Hukuku Dersleri Genel Esaslar - Türk Anayasa Hukuku*. Güncellenmiş 4. Baskı. Seçkin Yayıncılık, 2022.

EUROPEAN COMMISSION. “Communication from the Commission Guidelines on Prohibited Artificial Intelligence Practices”. 2025. <https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act>.

EUROPEAN COMMISSION. “Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions AI Continent Action Plan”. 2025. <https://digital-strategy.ec.europa.eu/en/library/ai-continent-action-plan>.

EUROPEAN COMMISSION. “Communication to the Commission - Approval of Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online”. 2025. <https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-protection-minors>.

EUROPEAN PARLIAMENT. “Regulating Dark Patterns in the EU: Towards Digital Fairness”. 2025. [https://www.europarl.europa.eu/RegData/etudes/ATAG/2025/767191/PRS_ATA\(2025\)767191_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2025/767191/PRS_ATA(2025)767191_EN.pdf).

EUROPEAN PARLIAMENT. “Resolution of 16 February 2017 with Recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL))”. 2017. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017IP0051>.

EUROPEAN PARLIAMENT ve COUNCIL OF THE EUROPEAN UNION. “Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU)

2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)”. 2024. <http://data.europa.eu/eli/reg/2024/1689/oj/eng>.

FEERST, Alex. “The Use of AI in Online Content Moderation”. American Enterprise Institute, 2022. <https://platforms.aei.org/wp-content/uploads/2022/09/The-Use-of-AI-in-Online-Content-Moderation.pdf>.

GAHNTZ, Maximilian ve PERSHAN, Claire. “Action Recommended: How the Digital Services Act Addresses Platform Recommender Systems”. *Verfassungsblog*, 2023. <https://dx.doi.org/10.17176/20230227-185115-0>.

GALEAZZI, Alessandro, PAUDEL, Pujan, CONTI, Mauro, DE CRISTOFARO, Emiliano ve STRINGHINI, Gianluca. *Revealing The Secret Power: How Algorithms Can Influence Content Visibility on Social Media*. t.y. Erişim 10 Eylül 2025. <https://arxiv.org/html/2410.17390v2>.

GILLESPIE, Tarleton. “Content Moderation, AI, and the Question of Scale”. *Big Data & Society* 7, sy 2 (2020). <https://doi.org/10.1177/2053951720943234>.

GORWA, Robert, BINNS, Reuben ve KATZENBACH, Christian. “Algorithmic Content Moderation: Technical and Political Challenges in the Automation of Platform Governance”. *Big Data & Society* 7, sy 1 (2020). <https://doi.org/10.1177/2053951719897945>.

GOSZTONYI, Gergely, GYETVÁN, Dorina ve KOVÁCS, Andrea. “Theory and Practice of Social Media’s Content Moderation by Artificial Intelligence in Light of European Union’s AI Act and Digital Services Act”. *European Journal of Law and Political Science* 4, sy 1 (2025): 33-42. <https://doi.org/10.24018/ejpolitics.2025.4.1.165>.

GÖÇMEN, İlke. *Avrupa Birliği Hukukunun Temelleri*. Gözden Geçirilmiş ve Güncellenmiş 2. Baskı. Seçkin Yayıncılık, 2023.

- GÖZLER, Kemal. *Anayasa Hukukunun Genel Esasları Ders Kitabı*. Güncellenmiş 14. Baskı. Ekin Yayınevi, 2022.
- GÜÇLÜTÜRK, Osman Gazi. *Yapay Zekâ ve Verinin Kullanımı*. 1. Baskı. On İki Levha Yayıncılık, 2022.
- HELDT, Amélie Pia. “EU Digital Services Act: The White Hope of Intermediary Regulation”. İçinde *Digital Platform Regulation: Global Perspectives on Internet Governance*, editör Terry FLEW ve Fiona R. MARTIN. Palgrave Global Media Policy and Business. Palgrave Macmillan, 2022. https://doi.org/10.1007/978-3-030-95220-4_4.
- HOLST, Luca, MAYER, Valentin, LÄMMERMANN, Luis, URBACH, Nils ve WENDT, Domenic. “The Impact of the EU AI Act’s Transparency Requirements on AI Innovation”. Conference paper presented de 19th International Conference on Wirtschaftsinformatik. 2024. <https://www.fim-rc.de/Paperbibliothek/Veroeffentlicht/4979/id-4979.pdf>.
- INITIATIVE FOR APPLIED ARTIFICIAL INTELLIGENCE. “AI Act: Risk Classification of AI Systems from Practical Perspective”. 2023. <https://aai.frb.io/assets/files/AI-Act-Risk-Classification-Study-appliedAI-March-2023.pdf>.
- IŞIK, Alper. *İnternet Aktörleri ve Egemenliğin Değişen Boyutları*. Güncellenmiş 2. Baskı. On İki Levha Yayıncılık, 2025.
- JAPKOWICZ, Nathalie ve STEFANOWSKI, Jerzy. “A Machine Learning Perspective on Big Data Analysis”. İçinde *Big Data Analysis: New Algorithms for a New Society*, editör Nathalie JAPKOWICZ ve Jerzy STEFANOWSKI, 16:1-31. Studies in Big Data. Springer International Publishing, 2016. https://doi.org/10.1007/978-3-319-26989-4_1.
- KAMA IŞIK, Sezen ve BOYAR, Oya. “Dördüncü Kuşak Haklar ve Bilişim Teknolojilerinin Doğuşunda Mahremiyet Kavramına Karşılaştırmalı Bir Bakış”. *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi* 25, sy 2 (2019): 602-23. <https://doi.org/10.33433/maruhad.667577>.

- KARA KILIÇARSLAN, Seda. “Yapay Zekânın Hukuki Statüsü ve Hukuki Kişiliği Üzerine Tartışmalar”. *Yıldırım Beyazıt Hukuk Dergisi*, sy 2 (2019): 363-89. <https://doi.org/10.33432/ybuhukuk.599224>.
- KARADENİZ, Salih. “Avrupa Birliği Yapay Zekâ Kanunu’nun Risk Grupları ve İlgililerin Yükümlülükleri Bağlamında İncelenmesi”. *Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi* 29, sy 1 (2025): 307-66. <https://doi.org/10.34246/ahbvuhfd.1541455>.
- KARADENİZ, Salih. *Blokzincir Teknolojisi ile Gerçekleştirilen Merkeziyetsiz Otonom Organizasyonların (DAO’ların) Hukuki Niteliği*. 1. Baskı. Adalet Yayınevi, 2024.
- KAYA, Mehmet Bedii. *Avrupa Birliği P2B Tüzüğü: Aracı Hizmet Sağlayıcılar ve Arama Motorları İçin Adil ve Şeffaf Platform Kuralları*. 1. Baskı. On İki Levha Yayıncılık, 2022.
- KAYA, Mehmet Bedii. *İnternet Hukuku*. 2. Baskı. İstanbul: On İki Levha Yayıncılık, 2021.
- KAYA, Mine. *Elektronik Ortamda (Elektronik Haberleşme - İnternet - Sosyal Medya) Kişilik Hakkının Korunması*. 1. Baskı. Seçkin Yayıncılık, 2015.
- KAYIHAN, Şaban. *Ticari İşletme Hukuku*. Gözden Geçirilmiş ve Güncellenmiş 7. Baskı. Seçkin Yayıncılık, 2021.
- KAYNAK BALTA, Büşra. *Fikir ve Sanat Eserleri Kanunu Kapsamında Eser Kavramı ve Yapay Zeka Ürünleri*. 1. Baskı. Seçkin Yayıncılık, 2021.
- KNIGHT-GEORGETOWN INSTITUTE. “Systemic Risk Assessment under the Digital Services Act”. 2025. <https://kgi.georgetown.edu/research-and-commentary/systemic-risk-assessment-under-the-digital-services-act/>.
- LEERSSEN, Paddy, VAN DUIN, Anna, TOEPOEL, Iris ve VAN HOBOKEN, Joris. *Pathways to Private Enforcement of the Digital Services Act*. Institute for Information Law, University of Amsterdam, 2025. <https://dsa-observatory.eu/2025/06/05/report-pathways-to-private-enforcement-of-the-digital-services-act-dsa/>.

- LIANG, Junyan ve KIM, Yoohwan. "Evolution of Firewalls: Toward Securer Network Using Next Generation Firewall". *2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)*, 2022, 0752-59. <https://doi.org/10.1109/CCWC54503.2022.9720435>.
- M. KAPLAN, Andreas ve HAENLEIN, Michael. "Rulers of The World, unite! The Challenges and Opportunities of Artificial Intelligence". *Business Horizons* 63, sy 1 (2020): 37-50. <https://doi.org/10.1016/j.bushor.2019.09.003>.
- M. KAPLAN, Andreas ve HAENLEIN, Michael. "Users of The World, unite! The challanges and opportunities of Social Media". *Business Horizons* 53, sy 1 (2010): 59-68. <https://doi.org/10.1016/j.bushor.2009.09.003>.
- MAMALI, Kübra Sıla. *Dijital Hizmetler Yasası ve AB E-Ticaret Direktifi Kapsamında İnternette Hizmet Sağlayıcıların Hukuka Aykırı İçerikten Sorumluluğu*. 1. Baskı. Hukuk Yayınları Dizisi 3492. Seçkin Yayıncılık, 2023.
- MCCARTHY, John, L. MINSKY, Marvin, ROCHESTER, Nathaniel ve E. SHANNON, Claude. "A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence". *AI Magazine* 27, sy 4 (2006): 12-14. <https://ojs.aaai.org/index.php/aimagazine/article/view/1904/1802>.
- MOTI, Zahra, SENOL, Asuman, BOSTANI, Hamid vd. *Targeted and Troublesome: Tracking and Advertising on Children's Websites*. 2023. <https://doi.org/10.48550/arXiv.2308.04887>.
- MÜFTÜOĞLU, Ilgın. "Sosyal Medya ve İfade Özgürlüğü". *İçinde Bilişim Hukuku Güncel Sorunlar*, 1. Baskı, editör Süleyman YILMAZ. Yetkin Yayınları, 2020.
- NASU, Hitoshi. "Artificial Intelligence and the Obligation to Respect and to Ensure Respect for IHL". *İçinde Ensuring Respect for International Humanitarian Law*, editör Eve MASSINGHAM ve Annabel MCCONNACHIE. Taylor & Francis Group, 2020.

- NUNZIATO, Dawn Carla. “The Digital Services Act and the Brussels Effect on Platform Content Moderation”. *Chicago Journal of International Law* 24, sy 1 (2023): 115-28. <https://cjil.uchicago.edu/print-archive/digital-services-act-and-brussels-effect-platform-content-moderation>.
- O'REILLY, Tim. “What is Web 2.0: Design Patterns and Business Models for the Next Generation of Software”. *Communications & Strategies*, sy 1 (2007): 17-37. <https://papers.ssrn.com/abstract=1008839>.
- ÖZKAN, Işıl. *Avrupa Birliği Kamu Hukuku: Brexit Sonrası Değişikliklerle*. Güncellenmiş 3. Baskı. Seçkin Yayıncılık, 2022.
- ÖZTEKİN, Alp. *Teori ve Uygulamada Türk İnternet Hukuku*. Güncellenmiş 2. Baskı. Seçkin Yayıncılık, 2023.
- PAQUET, Eric, VIKTOR, Herna ve GUO, Hongyu. “Data Mining in Finance: Current Advances and Future Challenges”. İçinde *Big Data Analysis: New Algorithms for a New Society*, editör Nathalie JAPKOWICZ ve Jerzy STEFANOWSKI, 16:159-75. Studies in Big Data. Springer International Publishing, 2016. https://doi.org/10.1007/978-3-319-26989-4_7.
- PUCZYŃSKA, Julia ve DJENOURI, Youcef. “AI in Disinformation Detection”. *Applied Cybersecurity & Internet Governance* 3, sy 2 (2024): 211-32. <https://doi.org/10.60097/ACIG/200200>.
- QUINTAIS, João Pedro, APPELMAN, Naomi ve FATHAIGH, Ronan Ó. “Using Terms and Conditions to apply Fundamental Rights to Content Moderation”. *German Law Journal* 24, sy 5 (2023): 881-911. <https://doi.org/10.1017/glj.2023.53>.
- EUROPEAN PARLIAMENT ve COUNCIL OF THE EUROPEAN UNION. 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), L 277 OJ § (2022). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R2065>.

- SALIM, Sara, TURNBULL, Benjamin ve MOUSTAFA, Nour. “Data analytics of social media 3.0: Privacy protection perspectives for integrating social media and Internet of Things (SM-IoT) systems”. *Ad Hoc Networks* 128, sy 102786 (2022). <https://doi.org/10.1016/j.adhoc.2022.102786>.
- SHAHI, Gautam Kishore, TESSA, Benedetta, TRUJILLO, Amaury ve CRESCI, Stefano. *A Year of the DSA Transparency Database: What it (Does Not) Reveal About Platform Moderation During the 2024 European Parliament Election*. 2025, 1-12. <https://arxiv.org/pdf/2504.06976v1>.
- SİNGİL, Nesrin. “Yapay Zekâ ve İnsan Hakları”. *Public and Private International Law Bulletin* 42, sy 1 (2022): 121-58. <https://10.26650/ppil.2022.42.1.970856>.
- TANJU, Erhan. *AIHM Kararları Işığında İfade ve Basın Özgürlüğü*. Güncellenmiş 2. Baskı. Seçkin Yayıncılık, 2017. <https://www.turcademy.com/tr/kitap/aihm-kararlari-isiginda-ifade-ve-basin-ozgurlugu-9789750241154>.
- TAŞKIN, Şaban Cankat. *İnternete Erişim Yasakları*. 1. Baskı. Seçkin Yayıncılık, 2016. <https://www.turcademy.com/tr/kitap/internete-erisim-yasaklari-9789750237874>.
- TURGUT, Cemile. *Kişilik Hakkının Bir Görünümü Olarak Unutulma Hakkı*. 1. Baskı. On İki Levha Yayıncılık, 2021.
- TURILLAZZI, Aina, TADDEO, Mariarosaria, FLORIDI, Luciano ve CASOLARI, Federico. “The Digital Services Act: An Analysis of Its Ethical, Legal, and Social Implications”. *Law, Innovation and Technology* 15, sy 1 (2023): 83-106. <https://doi.org/10.1080/17579961.2023.2184136>.
- TÜZGEN, Abdurrahman Hamza. *Türk Hukukunda Sosyal Medya Reklamları*. 1. Baskı. On İki Levha Yayıncılık, 2023.
- UYGUN, Oktay. *Devlet Teorisi*. 5. Baskı. On İki Levha Yayıncılık, 2019.
- UYGUN, Oktay. *Kamu Hukuku İncelemeleri İnsan Hakları, Demokrasi, Hukuk Devleti, Egemenlik*. 2. Baskı. İstanbul: On İki Levha Yayıncılık, 2013.

- VAN DE KERKHOF, Jakob. “Article 22 Digital Services Act: Building Trust with Trusted Flaggers”. *Internet Policy Review* 14, sy 1 (2025). <https://doi.org/10.14763/2025.1.1828>.
- VAN DE KERKHOF, Jakob ve GOANTA, Catalina. “Shadowbanned on X: The DSA in Action”. *European Journal of Risk Regulation* 16, sy 1 (2025): 352-59. <https://doi.org/10.1017/err.2024.81>.
- VAN DIJK, Jan A. G. M. *The Network Society: Social Aspect of New Media*. Second Edition. SAGE Publications Ltd, 2006.
- WERNICK, Alina ve MEDING, Kristof. *Beware! The AI Act Can Also Apply to Your AI Research Practices*. 2025. <https://arxiv.org/html/2506.03218v1>.
- WILMAN, Folkert. *The Digital Services Act (DSA) - An Overview*. 2022, 1-21. <https://dx.doi.org/10.2139/ssrn.4304586>.
- YAN, Enliang, SONG, Jialin, LIU, Chaonan, LUAN, Jingmin ve HONG, Wenxue. “Comparison of Support Vector Machine, Back Propagation Neural Network and Extreme Learning Machine for Syndrome Element Differentiation”. *Artificial Intelligence Review* 53, sy 4 (2020): 2453-81. <https://doi.org/10.1007/s10462-019-09738-z>.
- YASAMAN, Zeynep. *Türk ve Avrupa Birliği Hukukunda İnternette Marka Hakkının İhlali*. 1. Baskı. On İki Levha Yayıncılık, 2020.
- YEŞİLTUNA, Oğuzhan. *Hakikat ya da Neticeler: İfade Özgürlüğü Bağlamında Çevrimiçi Bilgi Çarpıtmayla Mücadele*. 1. Baskı. On İki Levha Yayıncılık, 2023.
- YILDIRIM, Yakup. “Avrupa İnsan Hakları Mahkemesi Kararlarında İfade Özgürlüğü ve İtibarın Korunması Hakkı”. Doktora Tezi, Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, 2021. <https://tez.yok.gov.tr/>.
- YILMAZ, Süleyman ve ERKAN, Vehbi Umut. “Sosyal Medya Hesaplarının Miras Yoluyla İntikal Edip Edemeyeceği Sorusunun Kişisel Verileri Koruma Hukuku Kapsamında İncelenmesi”. *İnönü Üniversitesi Hukuk Fakültesi Dergisi* 11, sy 2 (31 Aralık 2020): 567-86. <https://doi.org/10.21492/inuhfd.789817>.

YILMAZTEKİN, Hasan Kadir. *Yapay Zekanın Eser Sahipliği*. 1. Baskı. Adalet Yayınevi, 2021.

YUSUFOĞLU BİLGİN, Fülürya. *Dijital Piyasalarda Yer Sağlayıcıların Hukuki Sorumluluğu (Marka, Telif Hakkı ve Haksız Rekabet Kapsamında)*. 1. Baskı. On İki Levha Yayıncılık, 2022.

ZHAN, Yuanzhu, XIONG, Yu ve XING, Xinjie. “A conceptual model and case study of blockchain-enabled social media platform”. *Technovation*, 2022, 1-8. <https://doi.org/10.1016/j.technovation.2022.102610>.