

T.C.

MARMARA ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

KAMU HUKUKU ANABİLİM DALI

KAMU HUKUKU BİLİM DALI

İNTERNET ŞİRKETLERİNİN İNSAN HAKLARI YÜKÜMLÜLÜKLERİ

Doktora Tezi

Ayşenur OCAK

İstanbul, 2024

T.C.

MARMARA ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

KAMU HUKUKU ANABİLİM DALI

KAMU HUKUKU BİLİM DALI

İNTERNET ŞİRKETLERİNİN İNSAN HAKLARI YÜKÜMLÜLÜKLERİ

Doktora Tezi

Ayşenur OCAK

Tez Savunma Jürisi

1. Tez Danışmanı: Prof. Dr. Osman CAN

2. Üye: Prof. Dr Abdullah Sezer

3. Üye: Doç. Dr. Demirhan Burak ÇELİK

4. Üye: Doç. Dr. Oya BOYAR

5. Üye: Dr. Öğr. Üyesi Volkan ASLAN

İstanbul, 2024

ÖZET

Dijitalleşme, ifade özgürlüğü ve bilgi edinme hakkı gibi temel hakları genişletirken çocuk istismarı, terör ve nefret söylemi gibi alanlarda yeni riskler de doğurmuştur. İnternet şirketlerinin bu riskleri yönetme ve kamusal alandaki rollerini düzenleme zorunluluğu, onları yalnızca ticari varlıklar değil, toplumsal sorumluluğa sahip aktörler haline getirmiştir. Temel hak ve özgürlükler üzerindeki etkilerinin artmasıyla birlikte, ulusal ve uluslararası düzeyde bu şirketlerin yükümlülüklerine yönelik birçok düzenleme ortaya çıkmıştır. Bu düzenlemeler çerçevesinde, şirketlere içerik yönetimi konusunda kapsamlı sorumluluklar getirilmiş; internet kullanıcılarının veya yetkili otoritelerin bildirimleri üzerine hukuka aykırı içeriklere müdahale etme yükümlülüğü getirilmiştir. Şirketler ayrıca, belirli içerik türlerinin internet ortamında yayılmasına karşı etkili önlemler almakla yükümlüdür. Hukukun üstünlüğü ilkesinin çevrimiçi ortamda sağlanabilmesi için, şirketler tarafından alınan kararlarda şeffaflık sağlanmalı ve internet kullanıcıları hem yönetim süreçleri hem de yönetim sürecine ilişkin kurallar konusunda bilgilendirilmelidir. Öte yandan, şirketlerin temel hak ve özgürlükleri sınırlayan kararlarının çeşitli mekanizmalar yoluyla denetlenebilir olması gerekmektedir. Bu bağlamda, yargısal denetimin yanı sıra şirketlerin iç denetim mekanizmalarının etkin şekilde işletilmesi önem taşımaktadır. İnternetin potansiyel riskleriyle mücadelede, internet şirketlerinin insan hakları risklerini sistematik bir şekilde değerlendirmesi ve yönetmesi büyük önem taşır. Bu yükümlülüklerin yerine getirilmesi, internet şirketlerinin insan hakları yükümlülüklerine ilişkin öngörülebilir, ölçülü ve tüm tarafların menfaatlerini gözetten bir yasal çerçevenin oluşturulmasını zorunlu kılmaktadır.

Anahtar Kelimeler: İnternet şirketleri, çevrimiçi platformlar, sosyal ağ sağlayıcılar, özen yükümlülükleri, Birleşmiş Milletler İş Dünyası ve İnsan Haklarına Dair Rehber İlkeler, Dijital Hizmetler Yasası, erişimin engellenmesi, içeriğin çıkarılması.

ABSTRACT

Digitalization has expanded fundamental rights such as freedom of expression and the right to access information, while also introducing new risks related to child exploitation, terrorism, and hate speech. The obligation of internet companies to manage these risks and regulate their roles within the public sphere has transformed them from mere commercial entities into actors with significant social responsibilities. With the increasing influence of internet companies on fundamental rights and freedoms, numerous initiatives at national and supranational levels have emerged to outline these companies' responsibilities. Through these regulations, companies have been assigned comprehensive duties in content management, requiring action on illegal content upon notification by users or authorities. Additionally, companies are obliged to take effective measures to prevent the dissemination of specific types of harmful content online. To uphold the rule of law in the online environment, transparency in decision-making by internet companies is essential, ensuring that internet users are regularly informed about both the rules governing the digital space and the processes underpinning its management. Furthermore, decisions made by companies that limit fundamental rights and freedoms should be subject to oversight through various mechanisms. Alongside judicial review, the implementation of internal oversight mechanisms within companies is crucial in this regard. In addressing the potential risks associated with the internet, it is vital for internet companies to systematically assess and manage human rights risks. Fulfilling these obligations necessitates the establishment of a legal framework that ensures predictability, proportionality, and the consideration of all stakeholders' interests regarding internet companies' human rights responsibilities.

Keywords: Internet companies, online platforms, social network providers, due diligence obligations, United Nations Guiding Principles on Business and Human Rights, Digital Services Act, access blocking, content removal.

İÇİNDEKİLER

ÖZET	i
ABSTRACT.....	ii
İÇİNDEKİLER	iii
KISALTMALAR CETVELİ.....	vi
GİRİŞ.....	1
I. Dijital Teknolojilerdeki Gelişmelerin İnsan Haklarının Konusu Bakımından Etkileri	4
A. Dijital İfade Özgürlüğü: Fırsatlar ve Riskler	8
B. Dijital Ortamda Gözetim ve Mahremiyet Hakkı	14
II. Dijital Teknolojilerdeki Gelişmelerin İnsan Haklarının Yükümlüsü Bakımından Etkileri	19
A. İnternet Şirketleri: Yeni Kamusal Alanın Güçlü Aktörleri.....	19
B. Hukukun Üstünlüğü ve İnsan Hakları Arasında İnternet Şirketleri	28

BİRİNCİ BÖLÜM

İNTERNET ŞİRKETLERİNİN İNSAN HAKLARI SORUMLULUKLARINA İLİŞKİN ULUSLARARASI STANDARTLAR

I. Birleşmiş Milletler Sistemi.....	42
A. Genel Olarak İş Dünyası Karşısında İnsan Haklarının Korunması	44
1. Küresel İlkeler Sözleşmesi	44
2. İş Dünyası ve İnsan Haklarına Dair Rehber İlkeler	48
3. Özel Sektörün Çocuk Hakları Üzerindeki Etkileri Konusunda Devletin Yükümlülüklerine Dair Genel Yorum 16.....	58
B. Özel Olarak İnternet Şirketlerinin İnsan Hakları Sorumlulukları	60
1. İfade Özgürlüğü Bakımından Özel Sektöre Uygulanabilir İlkeler	61
2. Özel Hayatın Korunması Bakımından Özel Sektöre Uygulanabilir İlkeler	71
II. Ekonomik İş Birliği ve Kalkınma Örgütü (OECD).....	76
A. OECD Çok Uluslu Şirketler Rehberi.....	76
B. Dijital Hizmet Sağlayıcılar İçin Rehber İlkeler	80

III. Uluslararası Çalışma Örgütü (ILO).....	81

İKİNCİ BÖLÜM

AVRUPA HUKUKUNDA İNTERNET ŞİRKETLERİ VE İNSAN HAKLARINA DAİR HUKUKİ ÇERÇEVE

I. Avrupa Konseyi	85
A. Gelişen Normatif Çerçeve: İnternet Platformları ve Sorumlulukları.....	88
1. İş Dünyası ve İnsan Hakları: Ortak Sorumluluk, Farklı Roller	89
2. İnternet Şirketlerinin Yükselen Rolü ve Artan Sorumlulukları	91
B. Avrupa İnsan Hakları Mahkemesi İçtihatlarında İnternet Platformlarının Hukuki Sorumluluğu.....	102
1. İçerik Yönetimi ve İfade Özgürlüğü	107
2. Kişisel Verilerin Korunması ve Gizlilik	127
II. Avrupa Birliği.....	148
A. İnternet Şirketlerinin Sorumluluklarına İlişkin Temel Rejim	150
1. E-Ticaret Direktifi.....	151
a. Aracı Hizmet Sağlayıcılar İçin Sorumluluktan Muafiyet Rejimi.....	151
b. Sorumluluktan Muafiyet Rejiminin Açmazları.....	156
2. Dijital Hizmetler Yasası.....	161
a. Dijital Hizmetler Yasasına Hâkim Olan İlkeler.....	166
b. Aracı Hizmet Sağlayıcılar İçin Sorumluluktan Muafiyet Rejimi.....	171
c. Özen Yükümlülükleri.....	177
B. Belirli Konulara Özgülenmiş Düzenlemeler	189
1. Genel Veri Koruma Tüzüğü	190
2. Dijital Tek Pazarda Telif Hakları ve Bağlantılı Haklara İlişkin Direktif.....	192
3. Terörist İçeriğin Çevrimiçi Yayılmasının Ele Alınmasına İlişkin Yönetmelik	196
4. Görsel-İşitsel Medya Hizmetleri Direktifi	200
5. Çocukların Cinsel İstismarı, Cinsel Sömürüsü ve Çocuk Pornografisiyle Mücadeleye İlişkin Direktif	202
C. Avrupa Birliği Adalet Divanı Kararlarında İnternet Şirketlerinin İnsan Hakları Yükümlülükleri	203
1. İçerik Yönetimi.....	203

2. Kişisel Veri Aktarımı	219
3. Unutulma Hakkı	221

ÜÇÜNCÜ BÖLÜM

TÜRK HUKUKUNDA İNTERNET ŞİRKETLERİNE İLİŞKİN MEVCUT HUKUKİ ÇERÇEVE VE ÖNERİLER

I. İnternet Şirketlerinin Sorumluluklarına İlişkin Temel Çerçeve.....	232
A. İçerik, Yer ve Erişim Sağlayıcıların Yükümlülükleri	235
1. Bilgilendirme Yükümlülüğü.....	235
2. Trafik Bilgilerini Saklama Yükümlülüğü.....	237
3. İçeriğinin Yayından Çıkarılması ve/veya Erişimin Engellenmesine İlişkin Yükümlülükler.....	238
B. Sosyal Ağ Sağlayıcıların Ek Yükümlülükleri	254
1. Temsilci Belirleme ve Bildirme Yükümlülüğü.....	256
2. İçerik Moderasyonuna İlişkin Yükümlülükler	258
3. Şeffaflık Yükümlülüğü.....	260
4. Veri Lokalizasyonu Yükümlülüğü	263
5. Bilgi Sağlama Yükümlülüğü	264
6. Çocuk Koruma Yükümlülüğü	267
7. Kriz Planı Oluşturma Yükümlülüğü	269
II. Belirli Konulara Özgülenmiş Düzenlemeler.....	269
A. Kişisel Verilerin Korunması Kanunu.....	270
B. Elektronik Ticaretin Düzenlenmesi Hakkında Kanun	276
III. Yeni Bir İnternet Kanunu İçin Öneriler	278
A. İçerik Moderasyonuna İlişkin Öneriler.....	280
B. Şeffaflık Yükümlülüğüne İlişkin Öneriler	287
C. Risk Yönetimine İlişkin Öneriler.....	290
SONUÇ	293
KAYNAKÇA	302

KISALTMALAR CETVELİ

AB	Avrupa Birlięi
ABAD	Avrupa Birlięi Adalet Divanı
ABD	Amerika Birleşik Devletleri
AEPD	İspanyol Veri Koruma Kurumu
AİHM	Avrupa İnsan Hakları Mahkemesi
AİHS	Avrupa İnsan Hakları Sözleşmesi
AYM	Anayasa Mahkemesi
BM	Birleşmiş Milletler
bkz.	bakınız
BTK	Bilgi Teknolojileri Kurumu
C.	Cilt
DSA	Digital Services Act
ECD	Electronic Commerce Directive
ed.	editör
GDPR	General Data Protection Regulation
HTTPS	Secure Hypertext Transfer Protocol
ICT	Information and Communication Technology
ILO	International Labour Organization
Ibid	Aynı yerde, aynı eserde
KVKK	Kişisel Verileri Koruma Kurumu
m.	madde
OECD	Organisation for Economic Co-Operation and Development
para.	paragraf
s.	sayfa
ss.	sayfa aralığı
S.	Sayı
TERREG	Regulation on Adressing the Dissemination of Terrorist Content Online
TİB	Telekomünikasyon İletişim Başkanlığı

UN	United Nations
UNGPs	United Nations Guiding Principles
URL	Uniform Resource Loader
vd.	ve diğerleri
VLOP	Very Large Online Platforms
VLOSE	Very Large Online Search Engine



GİRİŞ

2000 yılında yazdığı “*Fare Kılıçtan Daha Güçlüdür*” (*The Mouse is Mightier than the Sword*) başlıklı çalışmasında Lloyd Axworthy, internet teknolojilerindeki gelişmeler ile insan hakları ilişkisini şu şekilde ifade etmiştir: “... çoğu teknolojideki gibi iyi olduğu kadar kötü olma potansiyeli de vardır. Sunduğu tüm fırsatlar için karanlık bir taraf var... Bu nedenle, insan hakları ve internet sorununun bir parçası, bu teknolojinin kötüye kullanılmasının nasıl önleneceğidir.”¹ İnternet teknolojilerindeki gelişmelerin insan hakları üzerindeki etkisine, henüz video izlemek için YouTube’un, sosyal paylaşımında bulunmak için Twitter ve Facebook’un olmadığı; düşünce ve fikirlerin bloglarda yeni yeni ifade edilmeye başlandığı bir dönemde yapılan bu öngörülü vurgu, günümüzde her iki boyutuyla geçerliliğini sürdürmektedir.

Bilginin üretimi, depolanması, iletilmesi ve alınmasını kolaylaştıran dijital teknolojileri ifade eden bilgi ve iletişim teknolojileri toplumsal yaşamın tüm alanlarını olduğu gibi insan haklarını da dönüştürmüştür. Bu dönüşüm internet teknolojilerindeki gelişmelerle birlikte farklı boyutlar kazanmıştır. Bu noktada, insan hakları boyutuyla öne çıkan gelişmelerden biri de World Wide Web’in² gelişimidir. Başlangıçta, internet kullanımının Web 1.0 dönemi olarak da ifade edilen 1990’lı yıllarda internet, yalnızca birkaç sunucudan bilgi edinilebilmesi amacıyla hizmet etmekteydi. Bu bakımdan, Web 1.0 dönemi kullanıcıların pasif bir rol üstlendiği bir dönemdir. İlk defa 2004 yılında tanıtılan Web 2.0 teknolojisinin kullanılmaya başlamasıyla ise internet kullanıcılarının pasif konumdan aktif konuma geçerek aynı zamanda içerik de üretebildikleri bir dönem başlamıştır.³ Bu teknolojinin ayrıcalığı, katılımcı bilgi paylaşımını, etkileşimi ve iş birliğini kolaylaştıran ikinci nesil web tabanlı topluluklar, uygulamalar ve hizmetler sunması şeklinde ifade edilmektedir.⁴ İnternette yeni bir dönemi başlatan Web 2.0 teknolojisi; sosyal ağ hizmetleri (Facebook, Myspace, Twitter, LinkedIn vb.) video paylaşım siteleri (Flickr, YouTube, Digg gibi), barındırma hizmetleri gibi araçlarla ve

¹ Lloyd Axworthy, “The Mouse Is Mightier than the Sword”, **Human Rights and the Internet**, ed. Steven Hick, Edward F. Halpin, Eric Hoskins, London: Palgrave Macmillan UK, 2000, ss. 16-17.

² World Wide Web, Türkçe’ye Dünya Çapında Ağ olarak çevrilmiştir; ancak kavram orijinal şekliyle bilinirlik kazandığından çalışmada da bu şekilde kullanılmıştır.

³ John Lannon, **Human Rights and Information Communication Technologies: Trends and Consequences of Use: Trends and Consequences of Use**, IGI Global, 2012, s. xv.

⁴ Ibid., s. 11.

kullanıcı kaynaklı verilerle iletişimi tek taraflı olmaktan çıkarıp katılımcılığı sağladığı gibi, internete hiyerarşik ilişkilerin olmadığı, dinamik ve denetime tabi olmayan bir nitelik de kazandırmıştır.⁵

Web 1.0 ve 2.0'ın ardından internetin yeni neslinin Web 3.0 olacağı ifade edilmektedir. Halen gelişmekte olması dolayısıyla net bir tanımını yapmanın mümkün olmadığı Web 3.0'ün hedefinin Web'i daha kişiselleştirilmiş hale getirmek için bilginin makineler tarafından anlaşılmasını ve kullanılmasını sağlamak olduğu ifade edilmektedir. Bu sistemde, kullanıcıların sundukları içerik ve veriler anlamlandırılıp yorumlanarak yine kullanıcıların ihtiyaçları doğrultusunda kişiselleştirilmiş şekilde tekrar kullanıcıya sunulmaktadır. "Semantik Web" ya da "Anlamsal Web" olarak da adlandırılan bu Web'in belirleyici özelliği, kullanıcıların kişiselleştirilmiş bilgileri bulmasını, paylaşmasını ve birleştirmesini ve yoğun veri akışını etkili bir şekilde yönetmesini sağlayan farklı içerik bilgi uygulamaları ve sistemleri arasında bütünleştirici bir rol üstlenmesidir. Bu sistemde verinin ve bilginin iletilmesinde araçların rolünün azalacağı, kontrolün bireylerde olacağı öngörülmektedir.⁶

Bilgi ve iletişim teknolojilerindeki bu gelişmeler interneti, kullanıcıların kamusal profillerini oluşturabildikleri, kendilerini ifade edebildikleri, sosyal ya da politik tartışmalara katılabildikleri, ekonomik, kültürel ve idari faaliyetlere kolaylıkla erişebildikleri bir alana dönüştürmüştür. Bu gelişmeler, ifade özgürlüğü ve ifade özgürlüğü ile bağlantılı basın ve örgütlenme özgürlükleri yanında eğitim, sağlık, çalışma gibi haklar bakımından yeni fırsatlar yaratırken nefret ve şiddete teşvik biçimlerinin artmasına ve büyük miktarda verinin elde edilmesine yol açmıştır.

Öte yandan, bu gelişmeler demokrasinin gelişimi bakımından da hem bireysel hem kitlesel etkiler doğurmuştur. Örneğin, İran'da 2009 yılında başlayan demokrasi yanlısı protestolar ve 2011'de Tunus ve Mısır'daki Arap Baharı ayaklanmaları gücünü bu teknolojilerden almıştır. Bu yönüyle ele alındığında internetin, özellikle de Twitter ve Facebook gibi sosyal medya platformlarının, bazı toplumlara demokrasi için mücadele

⁵ Web 1.0 teknolojileri ile Web 2.0 teknolojilerinin karşılaştırması için bkz. Jane Bozarth, **Social Media for Trainers: Techniques for Enhancing and Extending Learning**, John Wiley & Sons, 2010, s. 12.

⁶ Maria Giannakaki, "The 'Right to Be Forgotten' in the Era of Social Media and Cloud Computing", **Human Rights and Risks in the Digital Era: Globalization and the Effects of Information Technologies**, IGI Global Scientific Publishing, 2012, s. 11.

edilebilme ve bazı durumlarda da bunu elde edebilme fırsatı sağladığını söylemek mümkündür.⁷ Bununla birlikte, karanlık yüzüne ışık tutulduğunda bu teknolojilerin hem insan hakları hem de demokrasiye yönelik yeni tehditler ortaya çıkardığı da görülmektedir. Myanmar'ın Rohingya'lara yönelik şiddet eylemleri ve sonrasında yaşananlar, internetin insan haklarına yönelik yıkıcı etkisini gösteren örneklerden biridir. Myanmar'da etnik ve dinsel bir azınlık grup olan Rohingya Müslümanlar uzun süre siyasi, ekonomik ve toplumsal baskılarla karşı karşıya kalmıştır.⁸ Bu baskıların şiddeti 2017'de sürdürülen operasyonlarla çok ciddi boyutlara ulaşmış ve bu baskılar sonucunda bir milyondan fazla Rohingya Bangladeş'e sığınmak zorunda kalmıştır.⁹ İnternetin söz konusu olaylardaki etkisi Birleşmiş Milletler Myanmar Bağımsız Uluslararası Gerçek Bulma Misyonu Başkanı tarafından da ortaya koyulmuştur. Buna göre, sosyal medya ifadesinin Facebook ile eş tutulduğu Myanmar'da Facebook, nefreti körükleyerek çatışmalara yol açan eylemlerin toplumda yayılmasında belirleyici rol oynamıştır.¹⁰ Yapılan açıklamalarda, Myanmar'da ordunun, sahte hesap kullanan ordu personelleri de dahil olmak üzere Facebook'ta Rohingya'ları hedef alan sistematik bir süreç yürüttüğü ve Facebook'un nefreti körükleyen ya da teşvik eden ifadelere yönelik yasaklayıcı politikalarının bu kriz sırasında yeterince uygulanmadığı; buna karşın şiddet olaylarına ilişkin içerik ve haberlerin ise sansürlendiği belirtilmektedir.¹¹

Bu konuda verilebilecek başka bir örnek de internetin demokratik seçimleri etkileme potansiyeline ilişkindir. 2016 yılından önce, 2016'da Amerika Birleşik Devletleri'nde meydana gelen başkanlık seçimi ve yine 2016'da İngiltere'de gerçekleşen Avrupa Birliği'nden ayrılma (Brexit) referandumunda, Facebook tarafından seçmenlerin verilerinin onların tercihlerinin etkilenmesi için kullanıldığı ve seçimlerin sonuçlarına

⁷ Sosyal medyanın Arap Baharı'ndaki rolünü rolüne ilişkin bilimsel veriler için bkz. Philip N. Howard vd., "Opening closed regimes: what was the role of social media during the Arab Spring?", Working Paper, 2011, https://deepblue.lib.umich.edu/bitstream/handle/2027.42/117568/2011_Howard-Duffy-Freelon-Hussain-Mari-Mazaid_PITPI.pdf?sequence=1%26isAllowed=y, (24.12.2024).

⁸ Birleşmiş Milletler'in 12.07.2022 tarihli raporunda bu olaylar insanlığa karşı suçlar olarak nitelendirilmektedir. Report of the Independent Investigative Mechanism for Myanmar, Human Rights Council, A/HRC/51/4, <https://iimm.un.org/wp-content/uploads/2022/08/A-HRC-51-4-E.pdf>, (24.12.2024).

⁹ Report of the Independent International Fact-Finding Mission on Myanmar, Human Rights Council, A/HRC/42/50, 8 August 2019, https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/42/50, (24.12.2024).

¹⁰ Tom Miles, "UN investigators cite Facebook Role in Myanmar Crisis, Reuters, 13 March 2018", 2018 <https://www.reuters.com/article/us-myanmar-rohingya-facebook/u-n-investigators-cite-facebook-role-in-myanmar-crisis-idUSKCN1GO2PN/>, (20.12.2024).

¹¹ "A Genocide Incited on Facebook, With Posts From Myanmar's Military-The New York Times", <https://www.nytimes.com/2018/10/15/technology/myanmar-facebook-genocide.html>, (22.10.2024).

etki edildiğine yönelik iddialar, internetin demokrasiye saldırdığı tartışmalarını beraberinde getirmiştir.¹²

İnternet ifade ve bilgi edinme özgürlüğünün sınırlarını genişletirken, çevrimiçi suçlar, çocuk istismarı ve terör gibi olgularla insan hakları ihlalleri riskini de artırmıştır. Bu noktada, internet şirketleri gibi özel aktörlerin rolü yeniden şekillenmektedir. Klasik insan hakları teorisinde devletler hakların korunmasında birincil yükümlüler olarak kabul edilse de internetin kamusal alanın önemli bir parçası haline gelmesiyle birlikte, bu alanda faaliyette bulunan özel sektörün de hakların korunmasına yönelik yükümlülükler üstlenmesi gerektiği tartışmaları güçlenmiştir. Günümüzde internete erişim, internet servis sağlayıcıları aracılığıyla gerçekleşmekte; bilgiye erişim, arama motorları tarafından kolaylaştırılmakta; sosyal yaşam ise çevrimiçi platformlar aracılığıyla yürütülmektedir. İçerikler merkezi olmayan bir şekilde üretilebilmekte ve dağıtılmakta; sınırların ötesinde kolektif eylemler gerçekleştirilebilmektedir. Bu noktada önemli olan; insan hakları ve demokrasinin gerçekleştirilmesi konusunda gittikçe artan rollerine rağmen bu potansiyeli sürdürme konusundaki kararın, büyük ölçüde kamu yararı öncelikleri olmayan internet şirketlerinin kararlarına bağlı olmasıdır.

I. Dijital Teknolojilerdeki Gelişmelerin İnsan Haklarının Konusu Bakımından Etkileri

Büyük veri, nesnelerin interneti, kuantum hesaplama, blok zincir teknolojisi ve karmaşık algoritmalar gibi yeni teknolojik gelişmeler insan hayatını pek çok yönden etkilemiştir. Bu etki alanlarından biri de insan haklarıdır.¹³

İnternet, verilerin saklanması ve erişilebilirliğini büyük ölçüde kolaylaştırdığı gibi, bireylerin kendilerini ifade etme imkanlarını artırarak bilgiye ulaşma ve bilgi ve düşüncelerin paylaşılması açısından vazgeçilemez bir nitelik kazanmıştır. Öte yandan, temel hak ve hürriyetlerin dijital alanda kullanılmasıyla birlikte, bu haklara yönelik yeni tehditler ortaya çıkmıştır. İnternet; pornografinin, kişilik haklarına saldırı niteliği taşıyan, nefret söylemi içeren ya da şiddete teşvik eden ifadelerin hızlı bir şekilde yayılmasına yol

¹² Karl Manheim, Lyric Kaplan, “Artificial Intelligence: Risks to Privacy and Democracy”, **Yale Journal of Law and Technology**, C. 21, S. 106, 2019, s. 142.

¹³ Bart Custers, “New Digital Rights: Imagining Additional Fundamental Rights for the Digital Era”, **Computer Law & Security Review**, C. 44, 2022, s. 1.

açtığı gibi, internet ortamında ifade edilen fikir ve düşüncelere yönelik filtreleme ya da engelleme gibi yeni müdahale türleri de ortaya çıkarmıştır. Bilgi teknolojilerindeki gelişmeler kişisel verilerin elde edilmesini ve işlenmesini büyük oranda kolaylaştırdığından özel hayata saygı hakkı bakımından kişisel verilerin otomatik olarak toplanması, bu verilerin bireylerin davranışlarının tahmin edilmesi, yönlendirilmesi ve değerlendirilmesi gibi amaçlarla kullanılması gibi etkiler doğurmuştur.¹⁴

Bilgi teknolojilerinin etkilediği haklardan biri de telif haklarıdır. İnsan Hakları Evrensel Bildirgesi'nin 27/2. maddesinde, "*Herkesin kendi yarattığı bilim, yazın ve sanat ürünlerinden doğan manevi ve maddi çıkarlarının korunmasına hakkı vardır.*" şeklinde düzenlenen bu hak, Avrupa İnsan Hakları Sözleşmesi'nin 1 Numaralı Protokolü'nün 1. maddesi kapsamında da korunmaktadır. Bu noktada, belgeler, müzikler, görsel ya da işitsel materyaller de dahil olmak üzere dijital içeriklere kolay ve kapsamlı bir erişim sağlayan bilgi teknolojileri; hak sahiplerine çoğaltma, dağıtma, yayma gibi konularda münhasır yetkiler veren telif hakları bakımından yeni sorunlar ortaya çıkarmıştır.¹⁵

Bilgi teknolojileri, yeni iş imkanlarının ve girişimlerin ortaya çıkması, rekabet ilişkilerinin farklılaşması, ürün ve hizmetlerin sunulması süreçlerinin otomatikleşmesi ya da çalışanlara yönelik denetim yollarının çeşitlenmesi gibi yeni fırsatlar ve zorluklar ortaya çıkardığından çalışma hakkını da etkilemektedir.¹⁶

Bilgi teknolojilerindeki gelişmelerin; mevcut hakları konu bakımından dönüştürmenin yanında, beraberinde getirdiği yeni fırsatlar ve risklerin bir sonucu olarak bazı hakların önemini artırdığı gibi diğer haklarla bağlantılı bazı hakların ayrı bir hak olarak ele alınması şeklinde bir etkisi de olmuştur. Örneğin, mahremiyetin korunması

¹⁴ Giovanni Sartor, "Human rights and information technologies", **The Oxford Handbook of Law, Regulation and Technology** (ed. R. Brownsword, E. Scotford, K. Yeung), Oxford University Press Oxford, 2017, s. 442.

¹⁵ Ibid., s. 446.

¹⁶ Ibid., s. 448.

amacıyla kabul edilen kişisel verilerin korunması hakkı, bilgi teknolojilerindeki gelişmelerin olumsuz etkilerine karşı kabul edilen yeni haklardan biridir.¹⁷

Öte yandan, insan hakları niteliği bakımından henüz üzerinde uzlaşa sağlanmamış olmakla birlikte, sınırlı bir şekilde kabul edilen ya da insan hakları niteliği tartışılmaya devam eden yeni haklar da bulunmaktadır. İlk kategoride yer alan haklar, internete erişim¹⁸ ve çevrimdışı olma haklarıdır. İkinci kategoride ise fikrini değiştirme hakkı, temiz bir sayfa (dijital) açma hakkı, verinin değerini bilme hakkı, temiz bir dijital çevrede yaşama hakkı gibi haklara yer verilmektedir.¹⁹

İnternette temel hak ve hürriyetlere yönelik tehditlerin artması bakımından dikkat çekici bir durum ise internetin insan hakları yükümlülükleri olan devlet ve özel kişiler için temel hak ve hürriyetlere müdahaleyi kolaylaştıran yeni araçlar sunmasıdır. İnternet kullanımının artmasıyla birlikte, devletler gittikçe artan şekilde internet erişimini kısıtlamaya, gelişmiş teknolojiler yoluyla internet kullanımını izlemeye, internet kullanımıyla bağlantılı yeni suç tiplerini düzenlenmeye başlamıştır.²⁰

Dijital ortam gerçekten de illegal davranışlar için çok geniş ve kolaylaştırıcı bir ortam yaratmıştır. Bu gelişmelerle birlikte büyük miktarda kişisel verinin özel hayatın gizliliği dikkate alınmaksızın toplanması ve işlenmesi, mevcut önyargıların algoritmalar yoluyla yansıtılıp yeniden üretilmesi, sosyal medya platformları aracılığıyla nefretin kolayca yayılması mümkün hale gelmiş; nefret söylemi ve çocuk pornografisinin yayılması, şiddete teşvik, telif hakkı ihlalleri, dolandırıcılık, kimlik hırsızlığı, kara para aklama gibi suç alanlarında yeni endişeler ortaya çıkmıştır.²¹

¹⁷ Oya Boyar, Sezen Kama Işık, “Dördüncü Kuşak Haklar ve Bilişim Teknolojilerinin Doğuşunda Mahremiyet Kavramına Karşılaştırmalı Bir Bakış”, **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, C. 25, S. 2, 2019, s. 606.

¹⁸ İnternete erişim, ilk defa 2011 yılında, Birleşmiş Milletler tarafından bir insan hakkı olarak tanımlanmıştır Frank La Rue, Un Secretary-General, UN Human Rights Council Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, “Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (A/HRC/17/27)”, UN, 16.05.2011, <https://digitallibrary.un.org/record/710170>, para. 17-27.

¹⁹ Custers, “New Digital Rights”, ss. 8-12.

²⁰ Wolfgang Benedek, Matthias C. Kettemann, **İfade Özgürlüğü ve İnternet**, Ankara, Adalet Bakanlığı, 2016, s. 6.

²¹ Council of Europe, “The Rule of Law on the Internet and in the Wider Digital World: Issue Paper”, Council of Europe Publ, 2014, s. 7, <https://rm.coe.int/16806da51c>, (10.08.2024).

Anlaşılabacağı üzere, söz konusu gelişmelerin insan hakları üzerindeki etkisi hakkın türüne göre farklılaşabilmekle birlikte, bu gelişmelerin hem güçlendirici hem de tehdit edici sonuçlarının olduğu söylenebilir.²² İnternet teknolojilerinin insan hakları bakımından sunduğu yeni fırsatlar yanında yeni sorunlar ortaya çıkarması bu alanda çeşitli girişimleri beraberinde getirmiştir.

Bu kapsamda ele alınabilecek kapsamlı çalışmalardan biri Dünya Bilgi Toplumu Zirvesi'dir. Birleşmiş Milletler ve Uluslararası Telekomünikasyon Birliği koordinasyonunda iki aşamalı şekilde gerçekleştirilmiş bu Zirve'nin ilk aşaması Aralık 2003'te Cenevre'de, ikinci aşaması ise Kasım 2005'te Tunus'ta yapılmıştır. Her iki aşamada da açıklanan ilkeler bildirgesinde bilgi ve iletişim teknolojilerinin kullanımı ve içerik oluşturulmasına ilişkin olarak insan hakları ve kişisel mahremiyet, düşünce, vicdan ve din özgürlüğü dahil olmak üzere başkalarının temel özgürlüklerine saygı duyulması gerektiği belirtilmiştir.²³

Aradan geçen on yılın sonunda, Aralık 2015'te Dünya Bilgi Toplumu Zirvesi'nin sonuçlarının uygulanması gözden geçirilmiş ve hazırlanan sonuç belgesi Birleşmiş Milletler Genel Kurulu'nda kabul edilmiştir. Bu kararda, *“insanların çevrimdışı olarak sahip olduğu hakların çevrimiçi olarak da korunması gerektiği”* hususu kabul edilmiş ve bilgi ve iletişim teknolojilerinin insan hakları üzerindeki olumlu ve olumsuz etkileri değerlendirilmiştir. Kararda, bilgi ve iletişim teknolojilerindeki gelişmelerin bilgiye erişim, ifade özgürlüğü ve toplanma ve örgütlenme özgürlüklerini sağlayarak insan haklarının uygulanmasını güçlendirme potansiyelini gösterdiği kabul edilmekle birlikte, bu teknolojilerin insan haklarına yönelik ciddi tehditlere yol açtığı belirtilerek devletlere ifade özgürlüğü, toplanma ve örgütlenme özgürlüğü ve özel hayatın gizliliği hakları bakımından her türlü önlemin alınması çağrısında bulunulmuştur.²⁴

²² Sartor, Giovanni, “Human Rights and Information Technologies”, **The Oxford Handbook of Law, Regulation and Technology**, Roger Brownsword, Eloise Scotford, and Karen Yeung (ed.), 2017, s. 425.

²³ WSIS, WSIS-03/GENEVA/DOC/4-E, Declaration of Principles Building the Information Society: A Global Challenge in the New Millennium, 12.12.2003; WSIS-05/TUNIS/DOC/6(Rev.1)-E, Tunis Agenda for Information Society 18.11.2005.

²⁴ United Nations General Assembly, A/RES/70/125, 1 February 2016.

A. Dijital İfade Özgürlüğü: Fırsatlar ve Riskler

Bilişim teknolojilerindeki gelişmeler bireyler için her türlü aktivitelerini gerçekleştirebildikleri fiziksel alanın dışında dijital yeni bir yaşam alanı ortaya çıkarmıştır. Günümüzde internetin siyasi, kültürel, sosyal ve ekonomik hayata tam katılım için vazgeçilmez bir araç haline gelmesi²⁵ göz önünde bulundurulduğunda, bu dijital yaşam alanının insan haklarının gerçekleştirilmesi bakımından da vazgeçilmez bir nitelik kazandığı söylenebilir. Bu yeni dijital yaşam alanı, bazı insan hakları bakımından bu hakların etkili bir şekilde kullanılmasını sağlayacak yeni fırsatları beraberinde getirmiştir. Bu haklardan en dikkat çeken, şüphesiz ifade özgürlüğüdür. İnternet, bireylerin kendilerini ifade etme imkanlarını artırmış; bilgiye ulaşılmasını, bilgi ve düşüncelerin paylaşılmasını kolaylaştırarak ifade özgürlüğü yönünden dönüştürücü bir etki yaratmıştır.

İfade özgürlüğünün tanımı ve koruma alanı güvence altına alındığı farklı hukuk düzenlerinde değişkenlik gösterebilmekle birlikte bu özgürlük; genel olarak düşünciyi açıklamak, açıklanan düşünciyi yaymak ve yayılan düşünceye ulaşmak şeklindeki eylemlerin bütününe kapsayan bir alan olarak kabul edilmektedir.

Çıkış noktası bireyin kamusal tartışmalara katılırken keyfi kısıtlamalara karşı korunması olan²⁶ ifade özgürlüğü; gerçeğin ortaya çıkarılabilmesi, bireyin entelektüel kapasitesini oluşturabilmesi ve karar alma süreçlerine etkili bir şekilde katılabilmesinin en temel araçlarından biri olarak kabul edilmektedir. Bütün bu yönleriyle birlikte ifade özgürlüğü, çoğulcu ve demokratik düzen için vazgeçilmez bir nitelik taşımaktadır.²⁷ İfade

²⁵ Frank La Rue, UN Secretary-General, UN Human Rights Council Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, “Promotion and Protection of the Right to Freedom of Opinion and Expression (A/66/290)”, 2011, <https://digitallibrary.un.org/record/710170>, para. 63.

²⁶ Rikke Frank Jørgensen, “Framing the Net: The Internet and Human Rights”, **Framing the Net**, Edward Elgar Publishing, 2013, s. 40.

²⁷ Eric Barendt, “Freedom of Expression”, **The Oxford Handbook of Comparative Constitutional Law**, ed. Michel Rosenfeld, András Sajó, Oxford University Press, 2012, Chapter 42; Handyside v. the United Kingdom, 57499/17, 74536/17, 80215/17, 9323/18, 16128/18, 25920/18 (ECtHR 07 Aralık 1976), para. 23.

özgürlüğü ayrıca, toplantı ve gösteri yürüyüşü düzenleme özgürlüğü, seçme ve seçilme hakkı gibi birçok hakkın gerçekleştirilebilmesi için de önem teşkil etmektedir.²⁸

1789 İnsan ve Yurttaş Hakları Bildirgesi'nde insanın sahip olduğu en değerli haklardan biri²⁹ olarak kabul edilen ifade özgürlüğü İnsan Hakları Evrensel Bildirgesi, Kişisel ve Siyasal Haklar Uluslararası Sözleşmesi ve Avrupa İnsan Hakları Sözleşmesi gibi insan haklarına ilişkin temel belgelerde güvence altına alınmıştır.³⁰

İfade özgürlüğünün bireysel ve toplumsal gelişmedeki rolü ulusal ve uluslararası yargı organlarının kararlarına da yansımıştır. Avrupa İnsan Hakları Mahkemesi, ifade özgürlüğünü, demokratik toplumların ilerlemesi ve her ferdin gelişimi için temel koşullardan birini oluşturduğu şeklinde nitelendirmektedir.³¹ Türk Anayasa Mahkemesi de benzer şekilde, ifade özgürlüğünün demokratik bir toplumun temel dayanaklarından ve demokratik toplumun gelişiminin ve her bireyin kendini gerçekleştirmesinin başlıca şartlarından birini oluşturduğunu ve toplumsal çoğulculuğa ancak her türlü fikrin serbestçe ifade edilebildiği özgür tartışma ortamında ulaşılabileceğini ifade etmektedir.³²

Amerikan Yüksek Mahkemesi kararlarında ifade özgürlüğü iki temel teoriye dayandırılmaktadır.³³ Bunlardan biri, ilk defa Yargıç Holmes tarafından savunulan fikirlerin serbest piyasası (*marketplace of ideas*) teorisidir.³⁴ Bu teori, gerçeğin en iyi

²⁸ Kevin Boyle, Sangeeta Shah, "Thought, Expression, Association and Assembly", **International Human Rights Law** (ed. Daniel Moeckli, Sangeeta Shah, David Harris, Sandesh Sivakumaran), OUP Oxford, 2014, s. 266; Oktay Uygun, **Devlet Teorisi**, İstanbul, On İki Levha, 2017, s. 590.

²⁹ 1789 İnsan ve Yurttaş Hakları Bildirgesi, m. 11.

³⁰ İnsan Hakları Evrensel Bildirgesi, m. 19: "Herkesin düşünce ve anlatım özgürlüğüne hakkı vardır. Bu hak düşüncelerinden dolayı rahatsız edilmemek, ülke sınırları söz konusu 205 İnsan Hakları Evrensel Beyannamesi olmaksızın, bilgi ve düşünceleri her yoldan araştırmak, elde etmek ve yaymak hakkını gerekli kılar." Kişisel ve Siyasal Haklar Uluslararası Sözleşmesi, m. 19: "*Herkesin, bir müdahale ile karşılaşmaksızın fikirlere sahip olma hakkı vardır. Herkes ifade özgürlüğü hakkına sahiptir; bu hak bir kimsenin ülke hudutlarıyla sınırlanmaksızın sözlü, yazılı veya basılı veya sanatsal ürün şeklinde veya kendi tercih ettiği başka bir iletişim vasıtasıyla her türlü bilgi ve düşünceyi arama, edinme ve ulaştırma özgürlüğünü de içerir.*" Avrupa İnsan Hakları Sözleşmesi, m. 10: "*Herkes ifade özgürlüğü hakkına sahiptir. Bu hak, kamu makamları tarafından müdahale edilmeksizin ve ulusal sınırlar dikkate alınmaksızın, görüş sahibi olma, bilgi ve düşünceleri edinme ve yayma özgürlüğünü içerir. Bu Madde devletlerin yayıncılığı, televizyon veya sinema işletmelerini izin alma koşuluna bağlamasını engellemez.*"

³¹ Jersild v. Denmark, 57891/17 (ECtHR [GC] 23 Eylül 1994) para. 31; Skalka v. Poland, 3019/04 (ECtHR 27 Mayıs 2003), para. 32.

³² Gülfidan Yıldırım Başvurusu, 2014/12290 (Anayasa Mahkemesi 19 Temmuz 2017), para. 32.

³³ Bilyana Petkova, "Privacy as Europe's First Amendment", **European Law Journal**, C. 25, S. 2, 2019, s. 146.

³⁴ Abrams v. United States, 250 U.S. 616 (1919), **Justia Law**, <https://supreme.justia.com/cases/federal/us/250/616/>, (22.10.2024).

testinin fikirlerin gücünden geçtiği ve hakikate ancak düşüncenin serbestçe ifade edildiği ve birbiri ile rekabet ettiği özgür bir ortamda ulaşılabileceği iddiasına dayandırılmaktadır. Yüksek Mahkemenin dayandığı diğer teori ise bireylerin, kendi düşüncelerini geliştirmede, arzu ettikleri fikirleri duyma ve söylemede özgür olmaları gerektiği savıyla açıklanan bireysel özerklik teorisidir.³⁵

Bilgi teknolojilerindeki gelişmeler, bireylerin kendilerini ifade etme imkanlarını artırarak bilgiye ulaşılmasını ve bilgi ve düşüncelerin paylaşılmasını kolaylaştırmıştır. Nitekim günümüzde ifade özgürlüğü internet özgürlüğü ile birlikte ele alınmaktadır. Örneğin, Avrupa İnsan Hakları Mahkemesi, Avrupa İnsan Hakları Sözleşmesi'nin 10. maddesinde düzenlenen ifade özgürlüğünü “*günümüz koşulları ışığında*” yorumlayarak interneti de kapsayacak şekilde kabul etmektedir.³⁶ Mahkeme'ye göre internet siteleri, erişilebilirlikleri ve çok sayıda veriyi saklamak ve yaymak konusundaki yeterlilikleri dolayısıyla, güncel bilgiye erişilmesine ve daha genel anlamda bilginin iletilmesinin kolaylaşmasına büyük oranda hizmet etmektedir.³⁷ Bu bakımdan, yeni demokrasilerde yeni mecralar yoluyla kullanılan ifade özgürlüğü “*demokrasinin oksijeni*”; internet de insanların içinde yaşadıkları, soluk aldıkları ve ifade özgürlüklerini kullandıkları atmosfer şeklinde nitelendirilmektedir.³⁸

Türk Anayasa Mahkemesi de kararlarında internetin ifade özgürlüğü bakımından vazgeçilemez bir nitelik kazandığını vurgulamaktadır. Mahkeme bu ilişkiyi bir kararında şu şekilde ortaya koymuştur: “*Çağımızın temel araçlarından biri olan internet, hayatın hemen her alanında etkin olarak kullanılmaktadır. Verilerin saklanması ve erişilebilirliğini büyük ölçüde kolaylaştıran internet, bilgiye ulaşma ve bilgi ve düşüncelerin paylaşılması açısından çok etkili ve yaygın bir yöntem olduğu gibi kişilerin haberleşme ve iletişim sağlaması için de vazgeçilmez niteliktedir. İnternetin modern demokrasilerde başta haberleşme hürriyeti ve ifade özgürlüğü olmak üzere temel hak ve özgürlüklerin kullanılması bakımından önemi tartışmasızdır.*” Anayasa Mahkemesi ayrıca, internetin ifade özgürlüğü bakımından öneminin bir sonucu olarak kamu gücünü

³⁵ Whitney v. California, 274 U.S. 357 (U.S. Supreme Court 16 Mayıs 1927).

³⁶ Stoll v. Switzerland, 69698/01 (ECtHR [GC] 10 Aralık 2007), para. 34.

³⁷ Times Newspapers Ltd v. the United Kingdom, 3002/03, 23676/03 (ECtHR 10 Mart 2009), para. 27.

³⁸ Benedek, Kettemann, *İfade özgürlüğü ve internet*, s. 6.

kullanan makamların ve mahkemelerin internet konusunda çok hassas davranmaları gerektiğini belirtmiştir.³⁹

İnternetin ifade özgürlüğüne ilişkin etkisi, bir yandan kullanımını artırma diğer yandan da kısıtlanmasını kolaylaştırma şeklinde iki yönlüdür.⁴⁰ İnternet, ifade özgürlüğüne yönelik müdahale alanlarının katlanarak artmasına yol açmıştır.⁴¹ İnternet kullanımındaki artışla birlikte, bu alanın kontrol edilmesine ilişkin olarak erişimin kısıtlanması ya da engellenmesi, gelişmiş teknolojiler yoluyla internet kullanımının izlenmesi, belli ifade biçimlerinin suç haline getirilmesi gibi giderek artan karşı tepkiler ortaya çıkmıştır.⁴²

İfade özgürlüğüne yönelik gittikçe artan bu müdahaleler, insan haklarının geleneksel yükümlüsü olan devletler dışında, internet yönetiminde belirleyici role sahip yeni aktörlerden de kaynaklanabilmektedir. Dolayısıyla, medya sahipleri, araçlar, internet servis sağlayıcıları ve benzerleri gibi özel yetkililerin işleyişlerinin; çevrimiçi ifade özgürlüğünün korunması bakımından önemli bir dönüşüm geçirmesi ihtiyacı doğmuştur. Bu dönüşüm, genel bir ifadeyle, özel aktörlerin çevrimiçi ifade özgürlüğüne yönelik yükümlülüklerinin ortaya koyulması şeklinde ifade edilebilir.⁴³

İnternetin ifade özgürlüğü bakımından vazgeçilmez bir nitelik kazanmasıyla ifade özgürlüğü ile bağlantılı bazı hakların önemi de artmıştır. İnternetin önemini artırdığı bu haklardan ilki, ifade özgürlüğünün kullanım biçimlerinden biri olarak kabul edilen anonimlik hakkıdır. İfade özgürlüğü bakımından anonimlik hakkının korunmasının değeri, bireyin kendisine herhangi bir siyasi veya toplumsal ayrımcılığa, damgalanmaya, toplumsal aşağılanmaya veya tecrit edilmesine yol açabilecek eylemlerden çekinmeden

³⁹ Ali Kıdık Başvurusu, 2014/5552 (AYM 26 Ekim 2017), para. 82.

⁴⁰ Benedek, Kettemann, *İfade özgürlüğü ve internet*, s. 7.

⁴¹ La Rue, Secretary-General, Expression, “Promotion and Protection of the Right to Freedom of Opinion and Expression”, 16.05.2011, para. 22-33.

⁴² Benedek, Kettemann, *İfade özgürlüğü ve internet*, s. 6.

⁴³ Bilgi ve iletişim teknolojilerindeki gelişmelerden önce de özel kişilerin ifade özgürlüğüne yönelik yükümlülükleri olduğu kabul edilmekteydi. Örneğin Avrupa İnsan Hakları Mahkemesi, bazı durumlarda, Devletin özel kişilerden gelen saldırılara karşı da ifade özgürlüğünü koruma pozitif yükümlülüğü bulunduğunu belirtmekteydi. Dink/Türkiye, 2668/07, 6102/08, 30079/08, 7072/09, 7124/09 (ECtHR 14 Eylül 2010) para. 106. Ancak, söz konusu gelişmeler büyük ölçüde özel şirketler tarafından yönetilen internetin ifade özgürlüğünün kullanımı bakımından öneminin artmasıyla birlikte, özel şirketlerin yükümlülüklerinin belirlenmesi de ayrı bir önem kazanmıştır. .

veya bunlardan kaçınmadan kamusal alanda özerkliğini kullanabilmesidir.⁴⁴ Anonimlik hakkı, siyasi katılım bakımından ayrıca önem teşkil etmektedir. Anonimlik, siyasi alana ilişkin müzakere ya da toplantılara katılan bireyi bunların kendisine karşı kullanılmasına karşı korur ve bireyin bu tür bir katılıma ilişkin karar verebilmesini de kolaylaştırır. Dolayısıyla bu hak, ifade özgürlüğü için gerekli olduğu gibi⁴⁵ bireyin siyasi özerkliğinin de ön koşuludur.⁴⁶

Birleşmiş Milletler Fikir ve İfade Özgürlüğü Özel Raportörü de anonimliği internette ifade özgürlüğü ile bağlantılı olarak ele almıştır. Özel Raportör 2011 Raporu'nda devletleri, bireylerin kendilerini isimsiz olarak ifade edebilmelerini sağlamaya ve gerçek isimle kayıt zorunluluğu gibi sistemlerden kaçınmaya davet etmiştir. Buna göre, bu hakkın suç işlenmesinin önlenmesi gibi sebeplerle sınırlanabileceği istisnai durumlarda, keyfi uygulamalara karşı yeterli güvence sağlanmalı ve uluslararası hukuka uygun hareket edilmelidir.⁴⁷

Bu kapsamda ele alınabilecek başka bir hak ise bilgi uçurma hakkıdır. Bilgi uçurma kavramı, ulusal veya uluslararası hukukun ihlali, yetkinin kötüye kullanılması, israf, dolandırıcılık veya çevreye, kamu sağlığına ya da kamu güvenliğine zarar verme gibi kamu yararını tehdit eden ya da buna zarar veren belirli bir durumun ifşa edilmesi olarak tanımlanabilmektedir. Bu kapsamda, ifade özgürlüğü ve halkın bilgi edinme hakkı ile bağlantılı olarak güvence altına alınan bilgi uçurma hakkının hesap verebilirlik ve demokrasi için kritik bir öneme sahip olduğu kabul edilmektedir.⁴⁸

Bilgi ve iletişim teknolojilerindeki gelişmelerin bilgi uçurma hakkına bakan yönü, ihbarcılara (*whistle-blower*) anonim olarak bilgi yayımlayabilecekleri yeni platformlar sunması ve internetin bu bilgileri uzun süre erişilebilir kılmasıdır. Nitekim WikiLeaks,

⁴⁴ Christina M. Akrivopoulou, "The Right to Public Privacy under Surveillance: CCTV Technology and the Myth of 'Public Security'", **Human Rights and Risks in the Digital Era: Globalization and the Effects of Information Technologies**, IGI Global Scientific Publishing, 2012, s. 29.

⁴⁵ Benedek, Kettemann, *İfade özgürlüğü ve internet*, s. 28.

⁴⁶ Akrivopoulou, "The Right to Public Privacy under Surveillance", s. 30.

⁴⁷ La Rue, Secretary-General, Expression, "Promotion and Protection of the Right to Freedom of Opinion and Expression", 16.05.2011, para. 84.

⁴⁸ Buna göre 60'dan fazla ülkede bilgi uçurma hakkı koruma altındadır. "Promotion and Protection of the Right to Freedom of Opinion and Expression (A/70/361)", United Nations, 08.09.2015, para. 27-28 <https://digitallibrary.un.org/record/805706>.

Globaleaks gibi kuruluşlar da anonim ihbarcılarını kendilerini riske atmadan bilgi sağlayabilmelerini sağlamak üzere kurulmuşlardır.⁴⁹

Belgeler, müzikler, görsel ya da işitsel materyaller de dahil olmak üzere dijital içeriklere kolay ve kapsamlı bir erişim sağlayan bilgi teknolojileri, hak sahiplerine çoğaltma, dağıtma, yayma gibi konularda münhasır yetkiler veren telif hakları bakımından telifli içeriklerin izin alınmaksızın karşıya yüklenebilmesi ve kullanıcılar tarafından indirilebilmesi gibi yeni sorunlar da ortaya çıkarmıştır.⁵⁰ Bu durum ayrıca, ifade özgürlüğü ile telif hakları arasında bir çatışma durumunun ortaya çıkmasına yol açmış ve dolayısıyla söz konusu haklar arasında somut olaya göre değişebilecek yeni bir denge kurulmasını zorunlu kılmıştır.

Avrupa İnsan Hakları Mahkemesi, *Neij ve Sunde Kolmissoppi/İsveç* kararında dünyanın en büyük dosya paylaşım sitelerinden olan “Pirate Bay” isimli internet sitesinin kurucularının ifade özgürlüğü ile telif hakkı sahiplerinin hakları arasında bir dengeleme yapmıştır. AİHM, söz konusu sitede telif hakları mevzuatına aykırı şekilde bulundurulmuş müzik, film, bilgisayar oyunu gibi paylaşımlar dolayısıyla kurucuların hapis cezası ile cezalandırılmasına ve tazminat ödemelerine karar vermiştir. Söz konusu hapis cezası ve tazminatın, başvuruların ifade özgürlüğüne bir müdahale niteliği taşıdığını belirten Mahkeme, siyasi yarar ya da kamu yararına ilişkin bir tartışmaya katkı sunan diğer ifade biçimlerine tanınan ifade özgürlüğü korumasından yararlanamayacağını ve böylesi durumlarda devletin takdir marjının oldukça yüksek olduğunu belirterek başvurunun açıkça dayanaktan yoksun olduğuna karar vermiştir.⁵¹

AİHM’in ifade özgürlüğü karşısında fikri mülkiyet hakkına öncelik veren bu yaklaşımının belirleyici noktası, ifadelerin siyasi ya da kamusal bir tartışmaya katkı sunup sunmadığıdır. Nitekim, Mahkeme daha sonra “myspace.com” ve “last.fm” internet sitelerinin telif hakları mevzuatına aykırı şekilde internet yayını yaptıkları gerekçesiyle engellenmesine ilişkin *Akdeniz/Türkiye* kararında, genel menfaati ilgilendiren bir konuya

⁴⁹ The Protection of Sources and Whistleblowers, Submission to the United Nations Special Rapporteur on the Right to Freedom of Opinion and Expression by Association for Progressive Communications (APC) 29.06.2015, s. 8, <https://www.apc.org/sites/default/files/APCSubmissionProtectionWhistleblowers.pdf>.

⁵⁰ Sartor, “Human rights and information technologies”, s. 446.

⁵¹ *Neij and Sunde Kolmissoppi v. Sweden*, 40397/12 (ECtHR 19 Şubat 2013).

ilişkin bir tartışmaya katılım söz konusu olduğunda dengelemenin farklı şekillerde olabileceğinin altını çizmiştir.⁵²

B. Dijital Ortamda Gözetim ve Mahremiyet Hakkı

Mahremiyet hakkı temel insan hakları metinlerinin büyük bir kısmında güvence altına alınmaktadır. Avrupa İnsan Hakları Sözleşmesi'nde özel ve aile hayatına saygı hakkı, İnsan Hakları Evrensel Beyannamesi ve Kişisel ve Siyasal Haklar Sözleşmesi'nde mahremiyet hakkı olarak yer verilen bu hakka ilişkin tüketici bir tanım yapılamamaktadır. Avrupa İnsan Hakları Sözleşmesi'nde bu hak; özel hayat, aile hayatı, konut ve haberleşme olmak üzere dört temel hakkı kapsayacak şekilde düzenlenmektedir. Bununla birlikte, bu haklar da sosyal ve ekonomik hayatı kapsayacak şekilde çok geniş hukuksal çıkarları güvence altına almaktadır.

Özel hayata saygı hakkı, bireyin fiziksel ve ruhsal bütünlüğünü korumanın yanında kişinin kendini gerçekleştirme ve başkalarıyla sosyal ilişkiler kurmasını sağlamakta ve bu yönüyle tüm insan haklarının başlangıcı ve demokrasinin de ön koşulu olarak görülmektedir.⁵³

Dijitalleşme sürecinde, iletişim, eğitim, sağlık gibi faaliyetlerin büyük bir kısmı ülkesel sınırları aşan sanal ortama taşınmıştır. Bu durum, internet kullanıcıların kişisel verilerinin küresel ölçekte işlenmesine ve dolayısıyla daha geniş bir gözetim riskine yol açmıştır. Bu bağlamda, kişisel verilerin korunması ve bireylerin mahremiyet haklarının güvence altına alınması günümüzün en önemli hukuki ve etik sorunlarından biri haline gelmiştir.⁵⁴ BM İnsan Hakları Konseyi'nin mahremiyet hakkına ilişkin 2014 yılındaki toplantısında da gözetim uygulamalarının, özel hayatın gizliliği, ifade ve düşünce özgürlüğü, toplanma özgürlüğü, aile hayatı ve sağlık hakları da dâhil olmak üzere insanların insan hakları üzerinde çok gerçek etkileri olabileceği belirtilerek bu endişeler

⁵² Akdeniz and Others v. Turkey, 20877/10 (ECtHR 11 Mart 2014), para. 26-28.

⁵³ Yaşar Salihpaşaoğlu, "Özel Hayatın Kapsamı: Avrupa İnsan Hakları Mahkemesi İçtihatları Işığında Bir Değerlendirme", *Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi*, C. 17, S. 3, 2013, s. 235.

⁵⁴ Big Brother Watch and Others v. The United Kingdom, 58170/13, 62322/14, 24960/15 (ECtHR [GC] 25 Mayıs 2021), para. 322.

paylaşmıştır. Bu toplantıda, dijital gözetim yoluyla toplanan bilgilerin muhalifleri hedef almak için kullanıldığını gösteren güvenilir raporlar olduğu ifade edilmiştir.⁵⁵

Bilgi teknolojileri, kişisel bilgilerin otomatik olarak toplanması, saklanması, işlenmesi, davranışları öngörme ve yönlendirme amacıyla kullanılması ya da bireylerin değerlendirilmesi yoluyla mahremiyet üzerinde olumsuz etkilere neden olabilmektedir. Bu teknolojiler, bireylerin çevrimiçi faaliyetlerini izlemek, davranışlarını analiz etmek ve hatta gelecekteki eylemlerini tahmin etmek için kullanılabilir. Bu sayede, farklı kaynaklardan elde edilen ve aynı bireylere ilişkin veriler bir araya getirilerek bireylerin profillerinin oluşturulması mümkün olabilmektedir. Söz konusu veriler, özel ve kamusal alanlarda, örneğin sağlık hizmetlerinde ya da finansal işlemlerde, ilgili kişilerin ihtiyaç ve ilgilerine uygun, bireyselleştirilmiş hizmetler sunulmasına yardımcı olacak şekilde kullanılabilir. Ancak, kişisel verilerin işlenmesi, bu verilerin olumsuz amaçlarla kullanılma riskine ve bireyler üzerinde caydırıcı bir etki yaratma tehlikesine de yol açmaktadır. Bu bilgilerin kolaylıkla paylaşılabilir ve saniyeler içinde yayılabilir olması, söz konusu etkileri daha da önemli hale getirmektedir.⁵⁶

Kullanıcı profilleri aracılığıyla ilgili kişilere olası özellikler, tutumlar ve ilgi alanları atfedilebilmekte; örneğin, beklenen satın alma davranışları, farklı reklam türlerine karşı tepkileri ya da yasadışı veya arzu edilmeyen davranışlara eğilimleri tahmin edilebilmektedir. Kişinin diğer bireylerle olan bağlantılarının analiz edilmesi, iletişim ya da sosyal ağların incelenmesi yoluyla elde edilen veriler aracılığıyla o kişinin tutumlarına ilişkin çıkarımlarda bulunulmasını da mümkün kılmaktadır. Bu yolla inşa edilen elektronik kimlikler, ilgili bireylerin yanlış veya yanıltıcı bir imajını sunabilmektedir.⁵⁷

Bu teknolojiler bilgilerin yayılımını kolaylaştırmak suretiyle bireylerin itibarını olumsuz etkileyebilecek, hatalı veya güncelliğini yitirmiş bilgilerin de kalıcı olarak erişilebilir durumda kalmasına neden olmaktadır. Öte yandan, dijital profillemeye yoluyla kişiler hakkında kredi değerliliği gibi çıkarımlar yapılabilen ve buna göre kararlar

⁵⁵ UN Office of the High Commissioner for Human Rights, “Summary of the Human Rights Council Panel Discussion on the Right to Privacy in the Digital Age, Report of the Office of the United Nations High Commissioner for Human Rights”, Panel Discussion on the Right to Privacy in the Digital Age (2014: Geneva), UN, 2014, s. 3, <https://digitallibrary.un.org/record/792327>.

⁵⁶ Sartor, “Human rights and information technologies”, s. 438.

⁵⁷ Ibid., s. 430.

alınabilmektedir. Bu bağlamda, bireylerin kendilerini sistemlerde gerçek özelliklerine veya tercih ettikleri imaja uygun şekilde temsil edebilme hakkını ifade eden “dijital kimlik hakkı” kabul edilmektedir.⁵⁸

Yapay zekâ teknolojilerindeki gelişmelerle birlikte, mahremiyet ve kişisel verilerin korunmasına yönelik süregelen riskler daha da ciddi boyutlara ulaşmış ve karmaşık bir hal almıştır. Ancak bu sistemlerin asıl ayırt edici yanı, sahip oldukları devasa veri ihtiyacı ve şeffaflıktan uzak doğalarıdır. Bu özellikler, kullanıcıların, hangi kişisel bilgilerinin toplandığını, bu bilgilerin nasıl kullanıldığını ve gerekli olduğunda nasıl düzeltilebileceğini ya da silinebileceğini kontrol etme imkanını daha da kısıtlamaktadır. Günümüzde, çevrimiçi ürün ve hizmetleri kullanan bireylerin hayatlarının birçok alanında dijital gözetimden kaçınması neredeyse imkânsız hale gelmişken, yapay zekâ sistemleri bu ortamdaki kullanıcı etkinliğini zayıflamasına yol açmıştır.⁵⁹

Bu gelişmeler uluslararası ve bölgesel düzeyde çok sayıda girişimi beraberinde getirmiştir. Veri koruma alanında ilk uluslararası düzenleme OECD tarafından 23 Eylül 1980 tarihinde kabul edilen “Özel Yaşamın Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeleri”dir. Bu düzenleme ile verilerin korunmasına ilişkin minimum standartları ifade eden şu ilkeler benimsenmiştir: i. veri toplamının sınırlılığı ilkesi, ii. veri kalitesi ilkesi, iii. belirli amaç ilkesi, iv. kullanımın sınırlılığı ilkesi, v. veri güvenliği ilkesi, vi. açıklık ilkesi, vii. bireyin katılımı ilkesi, viii. hesap verilebilirlik ilkesi.⁶⁰ Kişisel verilerin korunması ile ilgili uluslararası alanda yapılan ilk sözleşme ise, 28 Ocak 1981 tarihli ve 108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesidir.⁶¹ 1 Ekim 1985 tarihinde yürürlüğe giren Sözleşmenin temel amacı, her üye ülkede, uyruğu veya ikametgâhı ne olursa olsun gerçek kişilerin, temel hak ve özgürlüklerini ve özellikle kendilerini ilgilendiren kişisel nitelikteki verilerin otomatik yollarla işleme tabi tutulması karşısında özel yaşam haklarını güvence altına almaktır. Bu Sözleşme, teknolojik gelişmelerin kişisel verilerin

⁵⁸ Ibid., s. 441.

⁵⁹ Katharine Miller, “Privacy in an AI Era: How Do We Protect Our Personal Information?”, 18.03.2024, <https://hai.stanford.edu/news/privacy-ai-era-how-do-we-protect-our-personal-information>, (24.12.2024).

⁶⁰ “OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data”, 23 Eylül 1980, <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188>, (24.12.2024).

⁶¹ Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28.1.1981, <https://rm.coe.int/1680078b37>, (21.03.2023).

işlenmesinin yaygınlaştırması ve kolaylaştırmasının bir sonucu olarak güncellenmiş ve daha güçlü bir veri koruma mekanizması kurulmuştur.⁶²

Birleşmiş Milletler Genel Kurulu, 18 Aralık 2013 tarihinde Dijital Çağda Mahremiyet Hakkına ilişkin 68/167 sayılı Kararı kabul ederek dijital mahremiyetin insan hakları açısından önemini kabul etmiştir. Karar, dijital iletişimde mahremiyet hakkına saygı gösterilmesi gerektiğini teyit etmiş ve devletleri ihlallere son vermeye ve özellikle iletişimin gözetlenmesi ile ilgili olarak bu tür ihlalleri önlemek için yasal ve diğer tedbirleri almaya çağırıştır.⁶³

Avrupa İnsan Hakları Mahkemesi de 2010'lu yılların başında, internet üzerindeki içeriklerin ve iletişimin, özel hayata saygı başta olmak üzere, insan hakları ve özgürlüklerinin kullanılması ve bunlardan yararlanılması açısından yarattığı zarar riskinin basının yarattığı riskten daha yüksek olduğunu ortaya koymuş ve internet ortamında hakların ve özgürlüklerin korunmasını ve güçlendirilmesini güvence altına almak için teknolojiye özgü özelliklere uygun bir politikanın zorunluluğuna dikkat çekmiştir.⁶⁴ Mahkeme, suçla mücadelede biyometrik ve gözetim verilerinin ulusal veri tabanlarında saklanmasına ve yapay zeka kullanımına yönelik de önemli bir içtihat oluşturmuştur. Bu kapsamda, suç şüphesiyle yargılanıp beraat eden bireylerin biyometrik verilerinin saklanması⁶⁵ ve hafif bir suçtan hüküm giyen bir başvurucunun DNA, parmak izi ve fotoğraflarının kalıcı olarak saklanması⁶⁶ Sözleşme'nin 8. maddesine aykırı bulunmuştur. Mahkeme, özellikle yetkililerin bu tür veri tabanlarında yüz tanıma yazılımı kullanma planlarına vurgu yapmıştır. Toplu veri toplama faaliyetlerinin ele alındığı bir dizi davada ise AIHM, depolanan verilerin güvenliği, veri saklama süresi, toplanan verilerin kullanımı için mevcut teknoloji ve gözetim altındaki kişilerin izlendikleri konusunda bilgilendirilmiş olup olmadığı hususlarına özel önem vermiştir.⁶⁷

⁶² Convention 108 +, Convention for the protection of individuals with regard to the processing of personal data, Council of Europe, 18.05.2018, <https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1>, (20.9.2024).

⁶³ The right to privacy in the digital age A/RES/68/167, United Nations General Assembly, 2014, <https://documents.un.org/doc/undoc/gen/n13/449/47/pdf/n1344947.pdf>, (20.9.2024).

⁶⁴ Editorial Board of Pravoye Delo and Shtekel v. Ukraine, 33014/05 (ECtHR 05 Mayıs 2011), para. 63.

⁶⁵ S. and Marper v. the United Kingdom, 30562/04, 30566/04 (ECtHR [GC] 04 Aralık 2008).

⁶⁶ Gaughran v. the United Kingdom, 45245/15 (ECtHR 13 Şubat 2020).

⁶⁷ Roman Zakharov v. Russia, 47143/06 (ECtHR [GC] 04 Aralık 2015); Breyer v. Germany, 50001/12 (ECtHR 30 Ocak 2020); Big Brother Watch and Others v. the United Kingdom.

Avrupa Birliği'nde de söz konusu riskleri azaltmaya ya da ortadan kaldırmaya yönelik kapsayıcı bir çerçeve oluşturulmuştur. AB Veri Koruma Direktifi⁶⁸ 24 Ekim 1995 tarihinde kabul edilmiş ve uzun yıllar boyunca Avrupa Birliği içerisinde kişisel verilerin korunması ve işlenmesini düzenlemiştir. Teknolojik gelişmelerin hızla ilerlemesi ve kişisel verilerin hem özel şirketler hem de kamu otoriteleri tarafından faaliyetlerini sürdürmek için benzeri görülmemiş bir ölçekte kullanılmaya başlaması, Direktif ile kişisel verilerin korunması alanında yeterli ve etkili bir yeknesaklığın sağlanamaması, bazı üye ülkelerde diğerlerine göre daha yüksek veri koruma düzeylerinin benimsenmesi ve bu farklılıkların ülkeler arası kişisel verilerin transferi konusunda sıkıntılar yaratması gibi sebepler⁶⁹ kişisel verilerin korunması açısından daha kapsamlı önlemler alınması gerekliliğini ortaya çıkarmıştır. Bunun sonucunda, 2016 yılında, kişisel verilerin işlenmesiyle ilgili kapsamlı bir çerçeve sunan Genel Veri Koruma Tüzüğü kabul edilmiştir.⁷⁰ Avrupa Ekonomik Alanı ile iş yapan tüm kuruluşları kapsayan bu düzenleme, kişisel verilerin işlenmesi sürecine ilişkin olarak en yüksek gizlilik ayarlarının kullanılması, kişisel verilerin anonimleştirilmesi ve bu verilerin yasal bir dayanakla veya veri sahibinin açık rızası ile işlenebilmesine ilişkin yükümlülükler içermektedir.

Avrupa Birliği'nde, uzun süren müzakereler sonucunda 1 Ağustos 2024 tarihinde yürürlüğe giren Yapay Zekâ Yasası⁷¹ ise bu teknolojilerinin yol açtığı risklerin yönetilmesi bakımından oldukça önemlidir. Buna göre, yapay zekâ sistemlerinin tüm yaşam döngüsü boyunca mahremiyet hakkının ve kişisel verilerin korunmasının güvence altına alınması gerekmektedir. Bu bağlamda, kişisel verilerin işlendiği durumlarda, AB veri koruma hukukunda yer alan veri minimizasyonu, tasarım gereği ve varsayılan olarak veri koruma ilkeleri geçerlidir. Bu ilkelerle uyumu sağlamak adına sağlayıcılar tarafından verilerin anonimleştirilmesi ve şifrelenmesi yanında algoritmaların verilere taşınarak yapay zekâ

⁶⁸ European Parliament and Council of the European Union (1995), "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data", <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046>.

⁶⁹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), <https://eur-lex.europa.eu/eli/reg/2016/679/oj>, resital 6-10.

⁷⁰ Ibid.

⁷¹ 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), <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>.

sistemlerinin eğitilmesini sağlayan teknolojilerin kullanımını içeren önlemler alınabilecektir.⁷²

II. Dijital Teknolojilerdeki Gelişmelerin İnsan Haklarının Yükümlüsü Bakımından Etkileri

İnternetin günlük hayatın pek çok alanında yoğun bir şekilde kullanılmaya başlamasıyla birlikte, çevrimiçi ortamda insan haklarına ilişkin yeni gelişmeler yaşanmaya başlamıştır. Bunlardan biri de çevrimiçi ortamda, söz konusu hakların kullanılmasını mümkün kılan ve özel şirketler tarafından yönetilen çok sayıda yeni aktörün ortaya çıkmasıdır. Bu aktörlerden özellikle internet servis sağlayıcıları, yer sağlayıcıları, alan adı yazmanları, arama motorları ve sosyal medya platformları insan hakları üzerinde doğrudan bir etkiye sahiptir.⁷³

Şirketler internet üzerindeki faaliyetlerinde uluslararası insan hakları hukukuna aykırı müdahalelerde bulunabilir ya da kamu makamları veya üçüncü kişilerden kaynaklanabilecek müdahalelere ortak olabilirler. Bu kapsamda gündeme gelebilecek müdahalelere filtreleme, hizmet kesintisi, arama sonuçlarının manipülasyonu, arama sonuçlarının kaldırılması ya da dizinden çıkarılması, kullanıcı hesapların kapatılması, verilerin toplanması ve devletlerle paylaşılması gibi çeşitli örnekler vermek mümkündür. İnternet şirketlerinin internetin yönetilmesine ilişkin bu rolleri, özneleri devletler ve hükümetler olan insan hakları hukukunun şirketler için doğrudan uygulanabilir olmaması dolayısıyla sorunludur.⁷⁴ Bu sorun, internetin kamusal bir alan olarak nitelendirilmesi ve internet şirketlerinin kamusal bir görev icra etmeleri (A); buna karşın internet şirketlerinin önemli bir rol üstlendiği bu yeni kamusal alanda hukukun üstünlüğü ilkesi ve temel hak ve hürriyetler bakımından yeni risklerin ortaya çıkması (B) olarak açıklanabilir.

A. İnternet Şirketleri: Yeni Kamusal Alanın Güçlü Aktörleri

İlk defa siyaset bilimci Jürgen Habermas tarafından tartışmaya açılan kamusal alan kavramı, özellikle demokrasi bağlamında sıklıkla ele alınan bir kavram olmuştur.

⁷² Ibid., resital 69.

⁷³ Rebecca MacKinnon vd., **Fostering Freedom Online: The Role of Internet Intermediaries**, UNESCO, 2014, s. 21.

⁷⁴ “The Rule of Law on The Internet And in The Wider Digital World”, s. 9.

Habermas bu çalışmasında, kamu ve kamusal kavramlarının net olmadığını belirtmekle birlikte, kamusalığa ilişkin şu tespitleri yapmıştır: *“Şayet kapalı topluluklarinkinden farklı olarak herkese açık iseler toplantıları “kamusal” olarak adlandırıyoruz -tıpkı kamusal yerlerden veya kamusal binalardan söz ettiğim gibi. Ancak salt bu “kamusal binalar” lafı bile söz konusu binaların herkese açık oluşundan öte bir şeyi ifade ediyor; hatta bunların kamunun gidiş gelişine açık olmaları bile zorunlu değildir; bunlar devletin kurumlarını barındırırlar ve bizzat bu nitelikleri gereği kamusaldırlar. Devlet “kamu erki”dir. Bu sıfatını, kendi hukukuna tabi olanların ortak kamusal selametini sağlama görevine borçludur.”* Bu tespitiyle Habermas, herkese açık olmayı kamusalığin bir unsuru olarak ele almıştır. Kamusal binaların devletin kamu yararını sağlama görevi dolayısıyla kamu erki sıfatına sahip olmasının kamusalılık niteliğine işaret ettiğini belirten Habermas, kamusal binaların kamunun giriş çıkışına kapalı olsalar dahi bu özelliğe sahip olduklarını vurgular.

Habermas’ın kamusal alan tanımı, 1964 yılında yazdığı “Kamusal Alan” başlıklı makalesinde daha net bir çerçeveye oturmuştur. Buna göre, *“Kamusal alan kavramıyla her şeyden önce, toplumsal yaşamımız içinde, kamuoyuna benzer bir şeyin oluşturulabildiği bir alanı kastederiz. Bu alana tüm yurttaşların erişmesi garanti altına alınmıştır. Özel bireylerin kamusal bir gövde oluşturarak toplandıkları her konuşma durumunda, kamusal alanın bir parçası varlık kazanmış olur. Bu tür bir aradalık durumundaki bireylerin davranışları ne iş ve meslek sahiplerinin özel işlerini görürken yaptıkları davranışlara; ne de bir devlet bürokrasisinin yasal sınırlarına tabi anayasal bir düzenin üyelerinin davranışlarına benzer. Yurttaşlar ancak, genel yarara ilişkin meseleler hakkında kısıtlanmamış bir tarzda, yani toplanma, örgütlenme, kanaatlerini ifade etme ve yayınlama özgürlükleri garantilenmiş olarak tartışabildiklerinde kamusal bir gövde biçiminde davranmış olurlar.”*

Bu tanımda da vurgulandığı gibi, kamusal alanın belirleyici unsurları; herkese açık olma, herkesin erişebildiği bu alanda kamusal tartışmalara katılabilme ve bu tartışmalara katılırken bazı temel hak ve özgürlüklerinin güvence altına alınmış olmasıdır. Kamusal alana ilişkin bu tanımlayıcı unsurlar, kamusal alanı demokrasi için bir önkoşul haline getirmektedir.

Kamusal alan ifade, toplanma ve örgütlenme özgürlükleri üzerine inşa edildiğinden, internetin söz konusu özgürlükler bakımından etkileri, kamusal alana ilişkin yeni tartışmaları da beraberinde getirmiştir. Her gün milyarlarca insan tarafından kendilerini ifade etmek, tartışmak, eleştirmek, araştırmak, görüş ve içerik oluşturmak için kullanılan çevrimiçi platformlar bireyleri kamusal alanda daha aktif hale getirerek katılımcılığı artırmıştır. Dolayısıyla internet, *"bireylerin kendilerini birey olarak oluşturan anlam yaratma biçimlerine katılmak için adil bir fırsata sahip oldukları bir kültürü"*⁷⁵ ortaya çıkarabilme potansiyeli bakımından siyasi katılımın ötesinde, ilke olarak herkesin üretimine ve dağıtımına katılabileceği geniş katılımlı bir demokratik kültürün oluşmasını sağlamıştır.

Bu değişim interneti çok kısa bir süre içinde küresel kamu forumu haline getirmiştir.⁷⁶ Bu gerçek, covid salgınına yanıt olarak fiziksel kamusal alanların yaygın bir şekilde kapatılmasıyla daha da pekişmiştir.⁷⁷ Dünya çapında 5 milyardan⁷⁸ fazla kullanıcısıyla küresel bir nitelik taşıyan bu çevrimiçi alanın yönetimi yalnızca hükümetlere aittir.

Sosyal medya platformları, bireylerin kamusal tartışmalara girdiği günümüzün kamusal alanına ev sahipliği yapmaktadır. Şirketler, aynı zamanda, söylemin küratörleri⁷⁹ olarak hareket etmektedir.⁸⁰

İnternetin insan hakları bakımından derin bir değere sahip olması ve merkezi küresel kamu forumu haline gelmesiyle birlikte altyapı ve hizmetler üzerindeki kontrol,

⁷⁵ Jack M. Balkin, "Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society", **New York University Law Review**, S. 79, 2004, s. 40.

⁷⁶ "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (A/HRC/29/32)", United Nations, s. 5, <https://primarysources.brillonline.com/browse/human-rights-documents-online/promotion-and-protection-of-all-human-rights-civil-political-economic-social-and-cultural-rights-including-the-right-to-development;hrdhrd99702016149>, (22.10.2024).

⁷⁷ COVID-19 salgınına yanıt olarak toplum genelinde uygulanan "sokağa çıkma yasakları" ile birlikte, bu platformların yarattığı alanlar yalnızca yeni bir kamusal meydana değil, aynı zamanda dünya çapında birçok yerde fiilen tek kamusal meydana dönüşmüştür. Rebecca J Hamilton, "Governing the Global Public Square", **Harvard International Law Journal**, C. 62, S. 1, 2021, s. 159.

⁷⁸ <https://www.statista.com/statistics/617136/digital-population-worldwide/>

⁷⁹ Bir sanat terimi olarak "küratör", müze, kütüphane, sergi, hayvanat bahçesi vb.ni yöneten ve etkinliklerini düzenleyen yetkili kimseleri ifade etmektedir. <https://sozluk.gov.tr/>

⁸⁰ María José Segura, **Contemporary Threats to Human Rights in the Online Public Sphere**, (Doktora Tezi), University of Southern Denmark, 2017, s. 11.

büyük ölçüde şirketlerin eline geçmiştir.⁸¹ Böylece internet şirketleri kamusal alanın belirleyicisi haline gelmiştir.⁸²

Birleşmiş Milletler Özel Raportörü La Rue tarafından da belirtildiği gibi, internet hizmetlerinin özel şirketler tarafından işletildiği ve sürdürüldüğü göz önüne alındığında, özel sektör bireylerin ifade özgürlüğü ve bilgiye erişim hakları üzerinde eşi benzeri görülmemiş bir etki kazanmıştır.⁸³ Amerikan Yüksek Mahkemesi'nin dijital platformlara ilişkin bir kararında yargıç Thomas tarafından da bu hususa dikkat çekilmiştir. Yargıç Thomas, hem dijital platformların yarattığı ifade özgürlüğü alanını hem de hükümet yetkililerinin ifadeleri de dahil bu alanın kontrolünün birkaç özel kişinin kontrolünde olmasını, tarihte benzeri görülmemiş olarak nitelendirmiş ve bu konuyu hukuki olarak ele almanın kaçınılmaz olduğunu belirtmiştir.⁸⁴

Bu şirketler; özellikle “içerik düzenleme” araçları ve gizlilik uygulamalarına ilişkin olarak içeriğin kaldırılması, kullanıcı hesaplarının engellenmesi, kişisel verilerin toplanması, işlenmesi ya da üçüncü kişilerle paylaşılması gibi insan haklarının çevrimiçi kullanımı konusunda geniş bir takdir yetkisine sahiplerdir. Buna karşın, internet şirketlerinin bu yetkilerini şeffaflık, öngörülebilirlik, yasallık gibi hukuki sınırlar içerisinde kullanmalarını sağlayacak mekanizmalar henüz etkinleştirilmiş değildir.⁸⁵ Bunun bir sonucu olarak da çevrimiçi alana katılmak için bireyler; Google ve Facebook gibi çevrimiçi platformlarla etkileşimde bulunmalı ve ifade özgürlüğü, bilgi edinme özgürlüğü ve toplanma özgürlüğü gibi hak ve özgürlüklerini kullanmak için insan haklarının doğrudan yükümlüsü olmayan, yumuşak yönergeler ya da kurumsal sosyal sorumluluk esaslarıyla yönetilen bu şirketlere güvenmelidir.⁸⁶

⁸¹ Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, (A/HRC/29/32), para. 11.

⁸² Ioanna Tourkochoriti, “The Digital Services Act and the EU as the Global Regulator of the Internet”, **Chicago Journal of International Law**, C. 24, 2023, ss. 129-47.

⁸³ La Rue, Secretary-General, Expression, “Promotion and Protection of the Right to Freedom of Opinion and Expression”, 16.05.2011, para. 44.

⁸⁴ Thomas J, Concurring, Biden v. Knight First Amendment, 20-197 (U.S. Supreme Court U. S. (2021 593).

⁸⁵ Giovanni De Gregorio, “From Constitutional Freedoms to the Power of the Platforms: Protecting Fundamental Rights Online in the Algorithmic Society”, SSRN Scholarly Paper, Rochester, NY: Social Science Research Network, 2018, s. 66, <https://papers.ssrn.com/abstract=3365106>.

⁸⁶ Rikke Frank Jørgensen, “Human Rights and Private Actors in the Online Domain”, **New Technologies for Human Rights Law and Practice**, ed. Jay D. Aronson, Molly K. Land, Cambridge, Cambridge University Press, 2018, s. 243.

İnternet şirketlerinin insan haklarına ilişkin faaliyetlerin yoğun bir şekilde gerçekleştiği dijital ekosistemde sahip oldukları bu güç, yeni bir özelleştirme süreci olarak da değerlendirilebilmektedir. Buna göre, şirketlere ait medyanın sivil kamusal alan üzerinde hakim olması, devlet tarafından yerine getirilmesi gereken işlevlerin özel yüklenicilere yaptırılması, kamusal alanların alışveriş merkezlerine ve özel sektöre ait kent meydanlarına indirgenmesi gibi süreçlerde olduğu gibi, internet şirketleri tarafından yönetilen platformların artan kamusal niteliği de bir tür özelleştirme eğilimini yansıtmaktadır.⁸⁷ Bu durum da internet şirketlerinin insan hakları sorumluluklarının belirlenmesi, bu şirketlerin söz konusu sorumluluklar kapsamında neler yaptıkları ya da yapmaları gerektiği, ulusal ve uluslararası hukukta öngörülen sorumluluk rejimlerinin insan haklarının korunmasında yeterli olup olmadığı gibi sorunları gündeme getirmektedir.⁸⁸

İnternet şirketleri, kamusal alanın yönetimine olan etkileri, başka bir ifadeyle demokratik değerleri bakımından farklılaşabilmektedir. Buna ilişkin bir sınıflandırmada bu şirketler, mikro kapı bekçileri, otorite kapı bekçileri ve makro kapı bekçileri olarak ele alınmaktadır. Bu sınıflandırmaya göre makro kapı bekçileri, büyüklükleri, kapsamı ya da etkileri dolayısıyla bilgi üzerinde büyük bir kontrol yetkisine sahiplerdir ve diğerlerinden özellikle de interneti kullanmak isteyen kullanıcılar için kaçınılmaz bir nitelik taşımaları bakımından ayrılmaktadır. Bu tür şirketleri internet hizmet sağlayıcıları, mobil ağ sağlayıcıları ve büyük arama motorları şeklinde örneklendirmek mümkündür.⁸⁹

Otorite kapı bekçileri ise, makro kapı bekçilerine benzer şekilde, büyük miktarda bilgiyi kontrol edebilme potansiyeline sahip olmakla birlikte onlardan farklı olarak bu alanlarda kullanıcılar, interneti kullanmak için bu şirketlere bağlı değillerdir. Örneğin, Wikipedia, Facebook, Youtube gibi yüksek trafikli portallar ve internet siteleri bu kapsamdadır. Son olarak, ağ yöneticileri, uygulama ve içerik moderatörleri gibi siteleri ifade eden mikro kapı bekçileri ise, bilgi kaynakları olarak önemi daha az olmakla birlikte, demokratik öneme sahip tartışmaları kolaylaştırma potansiyeli olan şirketleri ifade etmektedir. Bu sınıflandırma, internet şirketlerinin sorumluluklarına ilişkin bir

⁸⁷ Ibid., s. 245.

⁸⁸ Ibid., s. 247.

⁸⁹ Emily Laidlaw, "A Framework for Identifying Internet Information Gatekeepers", **International Review of Law, Computers & Technology**, C. 24, S. 3, 2010, s. 271.

çerçeve sunmaktadır. Buna göre, internet şirketlerinin insan hakları yükümlülükleri, temel hak ve hürriyetler ile demokratik yaşamı etkileme güçleri oranında artmalıdır.⁹⁰

Gerçekten de internet, ifade özgürlüğü ve bilgiye erişim konularında yarattığı kolaylıkla demokrasi için vazgeçilmez bir hale gelmiştir. İnternete erişim, internet servis sağlayıcıları aracılığıyla gerçekleşmekte; bilgiye erişim, arama motorları tarafından kolaylaştırılmakta; sosyal yaşam ise çevrimiçi platformlar aracılığıyla yürütülmektedir. İçerikler merkezi olmayan bir şekilde üretilebilmekte ve dağıtılmakta; sınırların ötesinde kolektif eylemler gerçekleştirilebilmektedir. Bu noktada önemli olan; insan hakları ve demokrasinin gerçekleştirilmesi konusunda gittikçe artan rollerine rağmen bu potansiyeli sürdürme konusundaki kararın, büyük ölçüde kamu yararı öncelikleri olmayan internet şirketlerinin kararlarına bağlı olmasıdır.⁹¹

Çevrimiçi altyapı; ifade özgürlüğünü, gözetimi ve veri madenciliğini eş zamanlı olarak kolaylaştırmakta ve kontrol etmektedir. Başka bir ifadeyle, kişilerin birbirleriyle iletişim kurmak amacıyla güvendikleri teknoloji ve şirketler, aynı zamanda gözetim ve veri gücünü de elinde tutanlardır. 2009'dan bu yana çeşitli uluslararası girişimler⁹² sayesinde şirketler, mahremiyetin korunmasına ilişkin bazı önlemler almaya başlamışsa da şirketlerin kullanıcı verileri konusundaki iç işleyişleri halen şeffaf ve öngörülebilir değildir.⁹³

İnternetin kamusal nitelikteki faaliyetlerin yoğun bir şekilde gerçekleştirildiği bir alana dönüşmesiyle birlikte, ifade özgürlüğünün korunmasının mekânsal bazı ayrımlara dayandırıldığı Amerika Birleşik Devletleri'nde, çevrimiçi ifade özgürlüğüne

⁹⁰ Ibid., ss. 272- 274.

⁹¹ Jørgensen, "Human Rights and Private Actors in the Online Domain", s. 248.

⁹² Bu kapsamda önce çıkan girişimlerden biri de Global Network Initiative (www.globalnetworkinitiative.org)'dir.

⁹³ Bu kapsamda şirketler aleyhine çeşitli süreçler yürütülmektedir. Örneğin, 2015 yılında Youtube Kids hakkında çocukların verilerini topladığı iddiasıyla yapılan şikâyet üzerine ABD Federal Ticaret Komisyonu tarafından çevrimiçi Çocuk Gizlilik Koruma Yasası (COPPA)'na aykırılık gerekçesiyle 170 bin dolar cezaya hükmedilmiştir. Bilgi için bkz. <https://www.cnbc.com/2019/09/04/youtube-to-pay-170-million-in-ftc-child-privacy-settlement.html>, (12.10.2021); Belçika Gizlilik Komisyonu tarafından Facebook aleyhine açılan dava da bu konuda verilebilecek başka bir örnektir. Bu davada Komisyon, çerezler sayesinde platform üyesi olmayan kullanıcıların dahi izlendiği ve izinleri olmaksızın verilerinin kaydedildiğini iddia etmiştir. Söz konusu davada yerel mahkeme, adı geçen uygulamaların durdurulmasına ve para cezasına hükmetmiştir. Bilgi için bkz. <https://globalfreedomofexpression.columbia.edu/cases/belgian-privacy-commission-v-facebook/>, (15.10.2021); Türk hukukunda da Kişisel Verileri Koruma Kurulu tarafından veri ihlali nedeniyle Facebook hakkında 11.04.2019 ve 18.09.2019 tarihlerinde iki farklı ceza kesilmiştir. Bilgi için bkz. <https://www.kvkk.gov.tr/Icerik/5450/2019-104> ve <https://kvkk.gov.tr/Icerik/5534/2019-269>.

uygulanacak rejime ilişkin önemli tartışmalar ortaya çıkmıştır. Bunun sebebi, Amerika Birleşik Devletleri’nde zaman, yer ve yöntem düzenlemelerinin anayasallığının “kamusal alan” düzenlemeleri üzerinde sürdürülüyor olmasıdır. Başka bir ifade ile kamu malı niteliğindeki bir mekânda gerçekleşen ifade özgürlüğü sınırlamalarında konuşmanın yapıldığı mekâna ilişkin tespit, sınırlamanın Anayasa’ya uygun olup olmadığı konusunda diğer tüm faktörlerden daha belirleyicidir.⁹⁴

Yüksek Mahkeme, *Hague v. Committee for Industrial Organization*⁹⁵ kararında, kamu mallarını *kamusal alanlar (public forum)* ve kamusal nitelikte olmayan alanlar (*nonpublic forum*) şeklinde iki temel kategoriye ayırmıştır. Buna göre devlet, kamusal alan teşkil eden mekanlarda, bakış açısına dayalı ayrımcılık yapmama ve ifade özgürlüğünün kullanılmasını kolaylaştırmakla yükümlüdür.⁹⁶ Bu ayırım, 1983 yılında verdiği *Perry Education Association v. Perry Local Educators’ Association*⁹⁷ kararıyla daha farklı bir boyut kazanmıştır. Bu kararda Mahkeme, kamusal alanları geleneksel kamusal alanlar (*traditional public forums*) ve belirlenmiş kamusal alanlar (*designated public forums*) şeklinde ikiye ayırmıştır.

Yüksek Mahkeme’ye göre geleneksel kamusal alanlar, “uzun süredir geleneklerle ya da devlet kurumları tarafından toplanmaya ve kamuya ilişkin meseleleri tartışmaya ayrılan yerler”i ifade etmiş⁹⁸; bu kategoriye sokaklar⁹⁹, parklar¹⁰⁰, kaldırımlar¹⁰¹ ve meydanlar¹⁰² gibi örneklerle somutlaştırmıştır.¹⁰³ Geleneksel kamusal alanlarda ifade özgürlüğü ancak zamana, yere ve şekle bağlı olarak ve çok istisnai durumlarda en az kısıtlayıcı yöntemler kullanılarak sınırlandırılabilir.¹⁰⁴ Belirlenmiş kamusal

⁹⁴ Matthew D. McGill, “Unleashing the Limited Public Forum: A Modest Revision to a Dysfunctional Doctrine”, *Stanford Law Review*, C. 52, S. 4, 2000, s. 932.

⁹⁵ *Hague v. Committee for Industrial Organization*, 307 U.S. 496 (U.S. Supreme Court 05 Haziran 1939).

⁹⁶ Dawn Nunziato, “From Town Square to Twittersphere: The Public Forum Doctrine Goes Digital”, *GW Law Faculty Publications & Other Works*, 2018, s. 29, https://scholarship.law.gwu.edu/faculty_publications/1368.

⁹⁷ *Perry Educ. Ass’n v. Perry Educators’ Ass’n*, 460 U.S. 37 (U.S. Supreme Court 23 Şubat 1983).

⁹⁸ *Hague v. Committee for Industrial Organization*.

⁹⁹ *Perry Educ. Ass’n v. Perry Educators’ Ass’n*.

¹⁰⁰ *Ibid.*

¹⁰¹ *United States v. Grace*, 461 U.S. 171 (U.S. Supreme Court 20 Nisan 1983).

¹⁰² *Capitol Square Review and Advisory Bd. v. Pinette*, 515 U.S. 753 (29 Haziran 1995).

⁶ Geleneksel kamusal alanların en önemli özelliklerinden biri de siyasi irade tarafından daha sonra kamusal alan statülerine son verilememesidir. Berke Özenç, “Toplantı ve Gösteri Yürüyüşü Özgürlüğü ve Mekân Yasakları”, *İstanbul Üniversitesi Hukuk Fakültesi Dergisi*, C. 73, S. 2, 2016, s. 92.

¹⁰⁴ Richard Moon, *The Constitutional Protection of Freedom of Expression*, University of Toronto Press, 2000, s. 148.

alanlar ise devlet tarafından kamusal ifade etkinliđi için açılan, devlete ait veya devlet tarafından kontrol edilen kamu mülkiyetinde bulunan yerleri ifade etmektedir.¹⁰⁵ Örneđin devlet okulları¹⁰⁶, üniversitelerin konferans salonları¹⁰⁷, devlet tarafından genel olarak ya da belirli bir konu için kiralanın özel mülkiyete konu tiyatrolar¹⁰⁸ devlet tarafından bu amaçla seçilebilir. Bir mekânın belirlenmiş kamusal alan olarak seçilmesinin ifade özgürlüğü bakımından etkisi, bu alanlarda ifade özgürlüğünü kullanmak isteyenlere yönelik ayrımcılığın yasak olmasıdır. Bir mekân genel amaçla kamusal alan olarak belirlenmiş ise hükümet söz konusu konuşmanın içeriğı ve/veya konusu veya ifade ettiğı bakış açısı temelinde ayrımcılık yapamaz. Belirli bir amaç için belirlenmiş kamusal alanlarda ise konu sınırlandırmaları tanımlandıktan sonra hükümet ifadeleri bu konularla sınırlandırabilir; ancak bu sınırlamanın ötesinde ayrımcılık yapılması yasaktır.¹⁰⁹ Dolayısıyla, sokaklar ya da parklar gibi geleneksel kamusal alanlar ve halka açık toplantılar gibi belirlenmiş kamusal alanlarda bireylerin ifade özgürlükleri en geniş korumaya sahiptir. Buna karşın kamusal olmayan alanlar ise, kamu malı niteliğine sahip olmakla birlikte, kamunun ifade özgürlüğü için tahsis etmediğı hapishaneler ya da askeri üsler gibi alanlardır.¹¹⁰

Kamusal alan-kamusal olmayan alan ayrımı esasen kamu mülkiyetindeki mallara ilişkindir. Kural olarak, özel kişilerin mülkiyetindeki alanlarda ifade özgürlüğünün sınırlandırılması konusunda mülkiyet sahiplerinin daha geniş bir yetkisi bulunmaktadır. Bununla birlikte, bazı durumlarda devlet tarafından kamusal alan olarak kullanılmak üzere tahsis edilen ve yönetilen özel mülkiyete konu mekanlar da kamusal alan olarak kabul edilebilmektedir.¹¹¹

Kamusal alan doktrininin süreç içerisindeki gelişimi, bu doktrinin internet ortamında uygulanabilirliğı konusunda da tartışmaları beraberinde getirmiştir. Bu

¹⁰⁵ Perry Educ. Ass'n v. Perry Educators' Ass'n.

¹⁰⁶ Madison Sch. Dist. v. Wisconsin Empl. Rel. Comm'n, 429 U.S. 167 (U.S. Supreme Court 08 Aralık 1976).

¹⁰⁷ Widmar v. Vincent, 454 U.S. 263 (U.S. Supreme Court 08 Aralık 1981).

¹⁰⁸ Southeastern Promotions, Ltd. v. Conrad, 420 U.S. 546 (1975), 420 U.S. 546 (U.S. Supreme Court 18 Mart 1975).

¹⁰⁹ Nunziato, "From Town Square to Twittersphere", s. 29.

¹¹⁰ Ibid.

¹¹¹ Southeastern Promotions, Ltd. v. Conrad, 420 U.S. 546 (1975) Bu davada, özel mülk olmakla birlikte belediye tarafından uzun süreli olarak kiralanın tiyatrun belirlenmiş kamusal alan teşkil ettiğine ve içerik sebebiyle tiyatrun yasaklanmasının Anayasa'ya aykırı olduğuna karar verilmiştir. .

kapsamda en dikkat çekici tartışmalardan biri, özel kişilerin sahibi olduğu ancak hükümet yetkilileri tarafından yönetilen sosyal medya hesaplarının bir kamusal alan olarak kabul edilip edilemeyeceğidir. Bu konu Amerika Birleşik Devletleri eski başkanı Donald Trump'ın başkan olduğu dönemde, Twitter hesabından bazı kullanıcıları engellemesi üzerine süregelen yargılamalarda da tartışılmıştır. Bu davalarda kullanıcılar engellendikleri için Başkan'ın tweetlerini göremedikleri, bu tweetleri cevaplayamadıkları, Başkan'ın tweetleriyle ilişkilendirilmiş yorum konularını görüntüleyemediklerini belirtirken Başkan Trump'ın temel argümanı ise hesabın kamusal alan olmadığı, engelleme özel bir davranış olduğu ve dolayısıyla Ek 1. maddenin uygulanamayacağıdır.

Bu kapsamda ilk olarak Amerika Birleşik Devletleri New York Güney Bölgesi Bölge Mahkemesi, hesaptaki "etkileşimli alanın" halka açık bir alan olduğunu ve bu alandan dışlanmanın anayasaya aykırı bakış açısı ayrımcılığı olduğunu tespit etmiştir. Karar, daha sonra Temyiz Mahkemesi tarafından da onanmıştır. Temyiz Mahkemesi bu sonuca ulaşırken Başkan'ın söz konusu engelleme kararını alırken özel kişi mi yoksa kamusal bir kişilik olarak mı hareket ettiği, engelleme kararının kullanıcıların bu alanda konuşamamalarına neden olup olmadığı, Twitter'ın kamusal alan teşkil edip etmediği, Başkan'ın engelleme kararının ayrımcılığa sebep olup olmadığı ve söz konusu hesabın hükümet söylemi teşkil edip etmediği hususlarında ayrıntılı değerlendirmelerde bulunmuştur. Bu değerlendirmeler neticesinde Mahkeme, Başkan'ın hesabının hükümete ulaşmak için kullanıldığı ve Twitter'ın etkileşimli özelliklerinin hesabı "sınırlama olmaksızın halkın erişimine açık" kıldığı gerekçesiyle halka açık bir forum oluşturduğuna karar vermiştir.¹¹²

Bu karar, daha sonra Amerika Yüksek Mahkemesi tarafından Trump'ın artık başkan olmaması sebebiyle bozulsada Yargıç Thomas, farklı gerekçesinde söz konusu tartışmaya ilişkin bazı değerlendirmelerde bulunmuştur. Yargıç Thomas, özel şirket olarak Twitter'ın sınırsız yetkili olduğu bir alanın kamusal alan olarak kabul edilmesinin "tuhaf" olduğunu belirtmiştir.¹¹³ Nitekim, Trump sadece bazı kullanıcıların kendisiyle etkileşimde bulunmasını engellerken söz konusu davanın görüldüğü sırada Trump'ın

¹¹² Knight First Amendment Institute at Columbia University v. Trump, 18-1691 (United States Court of Appeals 2 For the Second Circuit 2018).

¹¹³ Thomas J, Concurring, Biden v. Knight First Amendment de 2.

Twitter hesabı kalıcı olarak kapatılmış, dolayısıyla tüm Twitter kullanıcılarının kendisiyle etkileşim kurması engellenmişti. Bu tespitin ardından dijital platformların ifade özgürlüğünü kontrol etme gücüne dikkat çeken Yargıç Thomas, söz konusu gelişmelerle başa çıkmada özel kişilerin yükümlülüklerine ilişkin doktrinlere başvurulabileceğine işaret etmiştir.¹¹⁴

Kullanıcıların görüşlerini ifade ettikleri, bilgi alışverişinde bulundukları, kamusal tartışmalara katıldıkları internet ortamı da büyük ölçüde sınırlarının internet şirketleri tarafından belirlendiği özel mülk alanlarında gerçekleşmektedir. Dolayısıyla kamuya açık özel alanlar olarak görülen internet sitelerinde ya da platformlarda ifadenin korunması konusunda karar, bu “özel mülk” sahiplerinin takdirindedir. Bu durum, internetteki ifadeleri ek 1. maddenin sağladığı güvencelerden mahrum bırakmaktadır.¹¹⁵

Öte yandan, İletişim Ahlakı Yasası (Communication Decency Act [CDA]) da internet şirketlerine içerik düzenleme konusunda önemli bir güç sağlamaktadır. İletişim Ahlakı Yasası’nın; hizmet sağlayıcıları, kullanıcılarının üçüncü kişilerin yayınladıkları içerikten dolayı yayıncı olarak sorumlu tutulamamalarını güvence altına alan 230. maddesi, internet şirketlerine içeriği düzenleme konusunda geniş bir takdir yetkisi tanıyarak internet araçlarını üçüncü taraf içerikleri bakımından sorumluluktan muaf tutmaktadır. Buna göre şirketler, hukuka aykırı içeriği kaldırma ya da kaldırmama konusunda söz sahibi konumundadır. Bu bağışıklık, internet şirketlerini kişilik haklarına saldırı niteliği taşıyan ya da nefret içeren ifadeler de dahil olmak üzere üçüncü kişilerin eylemleri bakımından sorumlu tutulamamalarını sağladığından, kişilik haklarının korunması bakımından da sorun teşkil etmektedir.¹¹⁶

B. Hukukun Üstünlüğü ve İnsan Hakları Arasında İnternet Şirketleri

Kişisel özerkliğe saygı ve iktidar gücünün keyfi kullanımının dışlanması düşüncelerine dayanan hukukun üstünlüğü ilkesi; hukukun şeffaf, istikrarlı, öngörülebilir olmasını ve uyuşmazlıkların çözümüne ilişkin bağımsız ve tarafsız mekanizmaların

¹¹⁴ Ibid., s. 4.

¹¹⁵ Jørgensen, “Human Rights and Private Actors in the Online Domain”, s. 250.

¹¹⁶ Ibid.

varlığını gerektirmektedir.¹¹⁷ Kanun önünde eşit muameleyi sağlamanın, temel hak ve hürriyetleri korumanın, kamu makamlarının yetkilerini kötüye kullanmasını önlemenin ve karar alma organlarını hesap verebilir kılmanın bir ön koşulu olarak kabul edilen bu ilke, bu bakımdan bireyleri doğrudan etkilemektedir.¹¹⁸

Avrupa İnsan Hakları Mahkemesi de kendi dava hukukuna ilişkin olarak hukukun üstünlüğü kriterleri geliştirmiştir. Buna göre, temel haklar üzerindeki tüm kısıtlamalar net, kesin, kolay ulaşılır ve öngörülebilir yasal kurallara dayanmalı, meşru bir amaca hizmet etmeli, ilgili meşru amaçla orantılı olmalı ve bu şartların ihlal edildiği iddiasıyla başvurulabilecek etkili bir hukuk yolu bulunmalıdır. Bu kriterler, başka uluslararası insan hakları organları tarafından da benimsenmiştir.¹¹⁹

Anayasal bir kale olarak nitelendirilen¹²⁰ hukukun üstünlüğü ilkesi, herhangi bir anda iktidar dizginlerini ellerinde tutanların hukukla bağlı olmalarını gerektirir.¹²¹ Bu gereklilik dijital gelişmelerle birlikte ele alındığında, temel hak ve özgürlüklerle de doğrudan ilgili olan hukukun üstünlüğü ilkesinin çevrimiçi ortamda da güvence altında olup olmadığı sorusu gündeme gelmektedir. İnternet ve küresel dijital ortam büyük ölçüde özel şirketler tarafından yönetilmektedir.¹²²

Dijital çağın başlangıcında, internet şirketlerinin ortaya çıkışı sadece bir iş yapma özgürlüğü meselesi olarak ele alınmıştır. Böylece, bu yeni aktörler karşısında benimsenen temel yaklaşım, söz konusu özgürlüğü korurken aynı zamanda bunun olası kötüye kullanımını önlemektir. Dijital ortama minimum müdahale yaklaşımı, dijital gelişmeleri farklı bir boyuta taşımıştır. Çok büyük miktarlarda bilgi ve verinin işlenmeye başlamasıyla, mesele ekonomik olmaktan çıkmıştır. Piyasa ve otomatik karar alma teknolojilerinin karışımı, ekonomik özgürlüklerin kamu otoritelerine verilen yetkilerin

¹¹⁷ Robert Spano, “The Rule of Law as the Lodestar of the European Convention on Human Rights: The Strasbourg Court and the Independence of the Judiciary”, **European Law Journal**, C. 27, S. 1-3, 2021, s. 9.

¹¹⁸ Jeremy Waldron, “The Concept and the Rule of Law”, **Georgia Law Review**, C. 43, S.1, ss. 1–61.

¹¹⁹ “The Rule of Law on The Internet and in The Wider Digital World”, s. 10.

¹²⁰ Oreste Pollicino, “Digital Private Powers Exercising Public Functions: The Constitutional Paradox in the Digital Age and its Possible Solutions”, 15, 2021, s. 2, https://echr.coe.int/Documents/Intervention_20210415_Pollicino_Rule_of_Law_ENG.pdf, (19.7.2024).

¹²¹ Spano, “The Rule of Law as the Lodestar of the European Convention on Human Rights”, s. 3.

¹²² “The Rule of Law on The Internet and in The Wider Digital World”, s. 16.

kullanılmasına benzeyen bir şeye dönüşmesine yol açmıştır.¹²³ Tek bir devletin egemenliğiyle sınırlı olmayan dijital şirketler bir yandan temel hak ve özgürlüklerinin etkili bir şekilde kullanılmasını sağlarken diğer yandan anayasal ya da uluslararası sözleşmelerde devletler için öngörülen kurallara tabi olmaksızın bireysel ya da kitlesel insan hakkı ihlallerine yol açabilmekte, demokratik değerleri tehdit edebilmektedir.¹²⁴ İnternet şirketlerinin insan haklarının etkili bir şekilde kullanılabilmesi ya da ihlal edilebilmesindeki bu önemli rolü, bu şirketlerin insan hakları yükümlülüklerine ilişkin yani tartışmaları beraberinde getirmiştir.

Dijital alanda, özel aktörlerin ekonomik özgürlükleri iktidar biçimlerine dönüştüğünde, kamusal değerlerle çatışan özel standartlar ortaya çıkmaktadır.¹²⁵ Ekonomik çıkarların korunmasına hizmet eden bu özel standartlar, doğası gereği mahremiyete ve temel hak ve hürriyetlere zarar verebilmekte ve temel hak ve hürriyetlere yönelik kararlarda hesap verebilirliği engelleyebilmektedir. Bu bakımdan, internetin mahremiyet haklarını zayıflatarak ya da yok ederek, iletişim ya da örgütlenme özgürlüklerini kısıtlayarak hukukun üstünlüğünü zayıflatma ve keyfi müdahalelere yol açma potansiyeli yüksektir.¹²⁶

Belirtmek gerekir ki hizmet sağlayıcılar ile kullanıcılar arasındaki ilişki şirket ile tüketici arasında bir ilişkiye dayandığından, çevrimiçi ortam temel hak ve hürriyetlere yönelik müdahalelere karşı sağlanan bu güvencelerin büyük bir kısmından yoksundur. Bu tür özel kuruluşlar, örneğin, devlet sınırlamalarına uygulanan anayasal veya uluslararası hukuk kısıtlamalarına tabi olmaksızın ifade özgürlüğü ya da bilgiye erişime kısıtlamalar getirebilmekte ya da nefret söylemini yayabilmektedir.¹²⁷

Dijital ortamda internet şirketlerinin internetin yönetiminde geniş takdir yetkilerinin olması¹²⁸, söz konusu yönetimin tek taraflı olarak kolaylıkla değiştirilebilen ve kullanıcılara ne şekilde uygulanacağına ilişkin belirsizlikleri içeren hizmet koşulları

¹²³ Pollicino, “Digital Private Powers Exercising Public Functions”, s. 7.

¹²⁴ “The Rule of Law on The Internet and in The Wider Digital World”, S. 16.

¹²⁵ Pollicino, “Digital Private Powers Exercising Public Functions”, s. 3.

¹²⁶ “The Rule Of Law on The Internet and in The Wider Digital World”, s. 8.

¹²⁷ Ibid., s. 13.

¹²⁸ Jorgensen, bu takdir yetkisini anlatmak için tartışmaya açık da olsa, Google avukatlarının dünyada kimin konuşacağına karar verme konusunda herhangi bir devlet başkanı ya da yüksek mahkeme hakiminden daha fazla güce sahip olduklarını belirtmektedir. Jorgensen, “Human Rights and Private Actors in the Online Domain”, s. 246.

ya da kullanıcı sözleşmelerine dayanması, karar alma süreçlerinin şeffaf süreçlere dayanmaması ve alınan kararlara karşı bağımsız ve tarafsız itiraz mekanizmalarının olmaması hukukun üstünlüğü ilkesini aşındıran önemli sorunlardır.¹²⁹ Söz konusu hizmet koşulları, şirketlerin takdir yetkilerini oldukça geniş, sorumluluklarını ise dar tutmak üzere hazırlanmıştır. Örneğin, Facebook'un hizmet şartlarında kullanıcı hesaplarının kapatılmasının düzenlendiği 4/2. maddesi şu şekildedir: “*Kendi takdirimize bağlı olmak kaydıyla Topluluk Standartları başta olmak üzere Koşullarımızı veya İlkelerimizi açıkça, ciddi şekilde ya da sürekli olarak ihlal ettiğinizi belirlememiz halinde Meta Şirketi Ürünlerine erişiminizi durdurabilir veya kalıcı olarak engelleyebilir ve hesabınızı kalıcı olarak kapatabilir veya silebiliriz.*”¹³⁰ Bu kurallar, keyfi kararlara yönelik bir güvence içermediğinden hukukun üstünlüğü ilkesi ile bağdaşmamaktadır.

Nitekim, Suzor internet yönetimindeki bu sorunlara interneti “*Kuralsız (Lawless)*”¹³¹ olarak niteleyerek dikkat çekmektedir. Suzor’a göre internet şirketlerinin kullandıkları geniş takdir yetkileri, hukuk devletinde olması gereken yasal karar alma süreçlerinin antitezidir. Bir hukuk devletinde kanunlar, meşruluğunu anayasal sınırlara tabi olan demokratik kurumlar tarafından çıkarılmasından alırken, internet şirketlerinin karar alma süreçleri böyle bir meşruiyete dayanmamaktadır. Buna karşın, internet şirketleri ile kullanıcılar arasındaki ilişkinin bir tüketici işlemi olmanın ötesinde bu şirketler; bireylerin iletişim kurma, çalışma, öğrenme, eğlenme gibi çeşitli alanlarını bütün olarak elinde tutmakta ve bu yönüyle temel hak ve hürriyetlerin gerçekleştirilmesine ilişkin kararlar almaktadır.¹³²

İnternet şirketlerinin internet yönetimindeki söz konusu artan rolleri, başta mahremiyet hakları ve ifade özgürlüğü olmak üzere temel hak ve hürriyetlerin gerçekleştirilmesi bakımından bir dönüşümü beraberinde getirmiştir. Öyle ki, dijital ortamda internet şirketleri gerçek bir “Leviathan” olarak nitelendirilmektedir.¹³³

¹²⁹ Nicolas Suzor, “Digital Constitutionalism: Using the Rule of Law to Evaluate the Legitimacy of Governance by Platforms”, **Social Media + Society**, C. 4, S. 3, 2018, ss. 6-7.

¹³⁰ <https://tr-tr.facebook.com/legal/terms>

¹³¹ Nicolas P. Suzor, **Lawless: The Secret Rules That Govern our Digital Lives**, Cambridge, Cambridge University Press, 2019.

¹³² Ibid., s. 107.

¹³³ Timothy Garton Ash, **Free speech: Ten principles for a connected world**, Yale University Press., 2016, s. 1.

Başlıca sosyal medya platformları, kendi iç standartlarını ihlal eden içerikleri engellemek için insan (çalışanlar, yükleniciler ve ücretsiz kullanıcılar) ve yapay zekâ ("AI") karışımını kullanmaktadır. Platformlar bazı içerikleri henüz çevrimiçi ortamda görünmeden önce elemekte, diğer içerikleri ise göründükten sonra saniyeler ile yıllar arasında değişen bir zaman çizelgesinde kaldırmaktadır.¹³⁴ Öte yandan yine benzer gerekçelerle, kullanıcı hesapları hakkında geçici ya da kalıcı olarak kapatma kararı verebildiği gibi kullanıcılar tarafından oluşturulan içerikleri de kaldırabilmektedir.

Jack Balkin, şirketlerin ifade özgürlüğü bakımından yarattığı etkiyi “ifade özgürlüğü bir üçgendir” deyiimiyle ortaya koymaktadır. Bu kısa ifade aslında, ifade özgürlüğüne yönelik güvence ya da tehditleri de içeren düzenlemelerin, devletler ile bireyler arasında olduğu gibi ikili bir model olmaktan çıkıp üçüncü köşede sosyal medya şirketleri, geniş bant sağlayıcılar, arama motorları ya da elektronik ödeme sistemleri gibi hizmetleri sunan özel şirketlerin bulunduğu üçlü bir modele dönüşmesini net olarak anlatmaktadır. Söz konusu dönüşüm, en azından üç temel sorunu gündeme getirmektedir. Bunlardan ilki, devletlerin çevrimiçi ifade özgürlüğünün sınırlandırılmasına ilişkin olarak özel şirketlere baskı yapabilmesidir. İkinci sorun, devlet baskısından bağımsız olarak şirketlerin ifade özgürlüğü başta olmak üzere temel hak ve hürriyetleri ilgilendiren konularda gerekli süreçleri işletmeden, keyfi ve şeffaf olmayan kararlar alabilmeleridir. Son olarak, gerek devlet tarafından özel şirketlere baskı yapıldığı gerek özel şirketlerin kendi iç kararlarına göre hareket ettiği durumlarda, temel hak ve hürriyetleri etkilenen kullanıcılar için başvurulabilecek etkili bir merciinin olmaması söz konusu dönüşümün yol açtığı diğer bir önemli sorundur.¹³⁵

Burada önemli olan, kamusal alanın ayrılmaz bir parçası olmakla birlikte kamuya hesap verme yükümlülüğü olmayan büyük şirketlerin karar ve eylemlerinde nasıl bir özen göstermeleri gerektiğidir.

İnternet şirketleri, daha çok ekonomik çıkarların öne çıktığı kullanıcı sözleşmeleri ve şirket içi kurallar ile yönetilmektedir. Bir tüketici işlemi olarak düşünüldüğünde, bireylerin hizmet ya da ürünlere erişebilmeleri için şirketler tarafından sunulan hizmet koşulları ve kullanıcı kurallarına uymayı kabul etmeleri gerekmektedir. Söz konusu

¹³⁴ Hamilton, “Governing the Global Public Square”, s. 132.

¹³⁵ Jack M. Balkin, “Free Speech Is a Triangle”, *Columbia Law Review*, C. 118, 2018, s. 2011.

kurallara itiraz edilebilmesi mümkün olmadığından, bireyler temel hak ve hürriyetlerine yönelen potansiyel tehditleri daha en başından kabullenmek zorunda kalmaktadır. Bu tek taraflı ilişki, insan haklarının sınırlandırılması bakımından yeni bir rejim ortaya çıkarmaktadır. Bu yeni sınırlandırma rejiminde insan hakları, şirket kurallarına dayanılarak sınırlandırıldığı gibi söz konusu sınırlandırmada bir ölçülülük değerlendirilmesi de yapılmamaktadır. Ayrıca, şirket kuralları esas alındığında dahi esasında bu kurallara uygun olmayan bir sınırlama söz konusu olduğunda bu karara karşı itiraz etmenin etkili bir yolu bulunmamaktadır.

Bu kapsamda, CloudFlare isimli teknoloji şirketinin Nazi bağlantılı olduğunu düşündüğü Daily Stormer isimli internet sitesine hizmet vermeyi reddetmesi olayı, şirket kurallarından kaynaklanan insan hakları sınırlandırmalarındaki sorunların şirket yetkililerince de kabul edilmesi bakımından önemli bir örnektir. İnternet güvenliği, içerik dağıtımı, alan adı ve sunucu konularında hizmet veren CloudFlare şirketi, 2017 yılında, bir neo-Nazi sitesi olan Daily Stormer’ın hesabının kapatılmasına karar vermiştir. Şirket, söz konusu hesabın kapatılmasına ilişkin gerekçesinin Daily Stormer’ın ideolojisinin gizli destekçisi olmadıklarını göstermek olduğunu belirtmiştir. Söz konusu yasaklama kararının ardından, bazı şirket yetkilileri tarafından kararın keyfi bir karar olduğu ve aslında bunun tehlikeli olduğu belirtilmiştir. Şirketin üst düzey yöneticisi Matthew Prince, Daily Stormer özelinde bakıldığında pek çok kişinin bu sitenin kapatılması gerektiği konusunda kendisiyle hemfikir olduğunu düşündüğünü, buna karşın içerik kontrol mekanizmasına sahip olmanın kendisinin adalet kavramını altüst ettiğini belirtmiştir.¹³⁶ Zira, söz konusu karar alınırken şirketin hizmet vermeyi reddedeceği kuruluşlar hakkında bir standart olmadığı gibi kararın alınma usulüne dair herhangi bir güvence ya da itiraz mercii de bulunmamaktadır.

Kullanıcı sözleşmelerine aykırılık gerekçesiyle ifade özgürlüğünün sınırlanması konusunda dikkat çekici başka bir örnek de Amerika Birleşik Devletleri başkanlık seçimleri sonrasında 6 Ocak 2021 tarihinde, Donald Trump taraftarlarının seçim sonuçlarına karşı çıkmak amacıyla Kongre’ye saldırması üzerine, Youtube, Facebook, Twitter ve başkaca platformlar tarafından Trump’ın sosyal medya hesaplarının kapatılmasıdır. Söz konusu kapatma kararları kamuoyuna, kamu güvenliğine karşı

¹³⁶“Why We Terminated Daily Stormer”, **The Cloudflare Blog**, 16.08.2017, <https://blog.cloudflare.com/why-we-terminated-daily-stormer>, (1.10.2022).

olağanüstü bir durumla karşı karşıya kaldıkları¹³⁷, hesapla ilgili olarak devam eden şiddet potansiyelinden endişeli oldukları¹³⁸, hesabın kullanılmaya devam edilmesinin çok büyük riskleri olduğu¹³⁹ gerekçeleriyle birlikte duyurulmuştur.

Platform kurallarının ihlal edildiği gerekçesiyle ifade özgürlüğüne müdahalenin yakın tarihli bir örneği de Twitter'ın sahibi Elon Musk'ın kendi özel jetine ilişkin uçuş bilgilerinin paylaşılması üzerine aldığı yasaklama kararlarıdır. Musk, önce söz konusu bilgileri paylaşan kullanıcının, ardından da bu duruma ilişkin haberler yapan, aralarında The New York Times, Washington Post, CNN ve Voice of America muhabirlerinin de bulunduğu bazı gazetecilerin hesaplarını askıya almıştır. Herhangi bir uyarı yapılmaksızın, doğrudan geçici olarak askıya alınan hesaplarla ilgili yapılan tek açıklama, söz konusu hesapların Twitter kurallarını ihlal ettiği açıklamasıdır.¹⁴⁰ Çeşitli kesimler tarafından eleştirilen bu yasaklama kararları hakkında, Birleşmiş Milletler ve Avrupa Birliği yetkilileri de Twitter hesaplarından yaptıkları açıklamalarda, basın özgürlüğünün oyuncak olmadığı¹⁴¹, söz konusu keyfi kararların endişe verici olduğu ve bunlara karşı yaptırım uygulanabileceği¹⁴² açıklamalarıyla tepki göstermişlerdir. Söz konusu hesaplar, askıya alındıktan bir gün sonra, Musk tarafından Twitter'da düzenlenen anket sonrasında yeniden açılmıştır.¹⁴³ Elon Musk bu kararı başkalarının haklarının korunması için ifade özgürlüğüne müdahale olarak yansıtmıştır, ancak söz konusu karar kamu makamlarının keyfi kararlarına karşı öngörülen güvencelerden yoksundur. Herhangi bir yasal düzenlemeye dayanmayan ve bu bakımdan öngörülebilir olmayan yasaklama kararı; tweetlere erişimin engellemesi yerine, basın mensuplarının hesaplarının belirsiz bir süre için kapatılması dolayısıyla ölçülülük; karara karşı bir itiraz mekanizmasının mevcut olmaması dolayısıyla da etkili başvuru hakkı açısından sorunludur. Öte yandan,

¹³⁷ https://blog.twitter.com/en_us/topics/company/2020/suspension, (1.10.2022).

¹³⁸ <https://www.usatoday.com/story/tech/news/2021/01/26/youtube-ban-former-president-trumps-channel-remain-suspended/4265336001/>, (10.08.2022).

¹³⁹ <https://about.fb.com/news/2021/01/responding-to-the-violence-in-washington-dc/>, (11.8.2022).

¹⁴⁰ <https://www.theguardian.com/technology/2022/dec/17/elon-musk-reinstates-twitter-accounts-of-suspended-journalists>; <https://www.bbc.com/news/world-us-canada-63996061>, (11.08.2022).

¹⁴¹ https://twitter.com/MelissaFleming/status/1603763517642907655?ref_src=twsrc%5Etfw, (11.8.2022).

¹⁴² <https://twitter.com/verajourova/status/1603689440710369281>, (11.8.2022).

¹⁴³ Elon Musk ilk yaptığı ankette hesapların açılma zamanına ilişkin “şimdi, yarın, yedi gün sonra ve daha uzun süre” şeklinde dört farklı seçenek sunmuştur. Bu oylamada, oy veren kullanıcıların yüzde 38’i “daha uzun süre” seçeneği için oy kullanmıştır. Daha sonra seçenekleri “şimdi ve yedi gün sonra” şeklinde ikiye indirerek yeni bir anket düzenlemiştir. Bu ankette ise oy kullananların yüzde 58.7’si “şimdi”yi, %41.3’ü ise “yedi gün sonra”yı seçmiş ve nihayetinde hesaplar açılmıştır.

https://twitter.com/elonmusk/status/1603609466301059073?s=20&t=Kp0JPI0eSqLiBwMorUDE_g, (11.8.2024).

hesapların kapatılması gibi hesapların geri açılma süreci de ifade özgürlüğü ile çatışan haklar bakımından bir güvencesizliğe yol açmaktadır. Daha önce de belirtildiği üzere basın mensuplarının hesapları, Twitter’da düzenlenen bir anket sonucunda, yani Twitter kullanıcılarının kararıyla açılmıştır. Dolayısıyla bu örnekte, hangi ifade ve basın özgürlüklerinin kullanılacağına kullanıcıların takdirine kaldığı görülmektedir.

İnternet şirketlerinin insan haklarına ilişkin kararlarının ikinci boyutu, kamu makamlarından gelen talepler üzerine aldıkları kararlardır. Şirketlerin bu talepler üzerinde vereceği kararlar temel hak ve hürriyetlere yönelik güvenceleri ortadan kaldıracabileceği gibi, bu hak ve hürriyetlere devlet karşısında daha güçlü bir koruma da sağlayabilir. Örneğin, kamu makamlarından nefret içerdiği gerekçesiyle bir içeriğin kaldırılmasına yönelik talep olduğunda, internet şirketinin bu kararı uygulama ya da uygulamayı reddetme şeklinde iki seçeneği bulunmaktadır. Bu kararlardan ilki temel hak ve hürriyetler bakımından bir güvence teşkil ederken, ikinci durum temel hak ve hürriyetlere yönelik mevcut güvencelerin özel şirketler tarafından devre dışı bırakılması olarak görülebilir. Öte yandan, kamu makamlarının sansür olarak ifade edilebilecek talepleri söz konusu olduğunda; internet şirketlerinin kamu makamlarından gelen talepleri reddetmesi bir güvence, kabul etmesi ise bir risk olarak kabul edilebilir.

Bu konuda dikkat çeken kararlardan biri, Fransa’daki Yahoo! davasıdır.¹⁴⁴ Şirket merkezi Kaliforniya’da olan Yahoo! arama motoru, müzayede sitesi, kişisel web sayfası barındırma hizmetleri ve sohbet odaları dahil olmak üzere çeşitli internet web siteleri ve hizmetleri işleten bir internet servis sağlayıcısıdır. Söz konusu dava ise Yahoo!’nın müzayede sayfalarında satışa sunulan Naziliğe ilişkin eşyaları kaldırmayı reddetmesine ilişkindir.¹⁴⁵ Bu ret kararı üzerine açılan davada Yahoo!, hem Fransız mahkemesinin yargı yetkisine itiraz etmiş, hem de söz konusu ürünlerin alınması ya da satılması konusunda herhangi bir sorumluluğu olmadığını belirtmiştir.¹⁴⁶ Buna karşın Mahkeme, şirket hakkında para cezasına ve Nazilikle bağlantılı 1500’ü aşkın söz konusu eşyaya Fransız kullanıcıların erişimlerinin engellemesine kararı vermiştir. Bunun üzerine Yahoo!, Amerika Birleşik Devletleri Kuzey Kaliforniya Bölgesi Bölge Mahkemesi’nde yeni bir

¹⁴⁴ “LICRA et UEJF v. Yahoo! Inc., RG 05308 (May 22, 2000): Case Brief Summary”, **Quimbee**, , <https://www.quimbee.com/cases/licra-et-uejf-v-yahoo-inc>, (22.10.2024).

¹⁴⁵ Christine Duh, “Yahoo! Inc. v. LICRA”, **Berkeley Technology Law Journal**, C. 17, S. 1, 2002, s. 360.

¹⁴⁶ Marc H. Greenberg, “A Return to Lilliput: The LICRA v. Yahoo! Case and the Regulation of Online Content in the World Market”, **Berkeley Technology Law Journal**, C. 18, 2003, s. 1206.

dava açarak¹⁴⁷ söz konusu Fransız mahkeme kararının uygulanmasının Amerikan Anayasası'nın ihlali anlamına geleceğini ileri sürmüş ve Bölge Mahkemesi de bu yönde karar vermiştir.¹⁴⁸

Bu dava, internet şirketlerinin insan hakları yükümlülükleri bakımından yargı yetkisinden kaynaklanan önemli bir sorunu gün yüzüne çıkaran temel davalardan biri olarak kabul edilmektedir. Bununla birlikte karar, internet şirketlerinin yargı kararlarına karşı gelebilme potansiyelini de içeren güçlerini ve bunun temel hak ve hürriyetler açısından yol açabileceği sorunları da görünür kılmıştır.

İnternet şirketlerinin sahip oldukları bu potansiyelin başka bir yönü de kamu makamlarından gelen taleplere yönelik yaklaşımlarının hizmet verdikleri ülkeye göre değişebilmesidir. Şirketler, belli durumlarda, ulusal hukuktan kaynaklanan sorumluluktan kaçınmak amacıyla uluslararası insan hakları hukukuyla bağdaşmayan talepleri yerine getirebilmekte, böylece insan hakları ihlallerini kolaylaştıran bir işlev görebilmektedir. Örneğin Çin'de, 2005 yılında gazeteci Shi Tao'nun devletin gizli bilgilerini ifşa ettiği gerekçesiyle ve Yahoo! tarafından sağlanan e-posta bilgilerine dayanılarak on yıl hapis cezasına mahkûm edilmesi, şirketlerin bu konudaki yaklaşımlarının etkilerini ortaya koyması bakımından dikkat çekicidir. Olayın ardından Yahoo! yetkilileri, Amerika Birleşik Devletleri Kongresi tarafından gazetecinin mahkûmiyetinden sorumlu tutulmuş; kendilerinden tercihlerini neden bu yönde kullandıklarını açıklamaları istenmiştir. Bunun üzerine şirket yetkilileri yapacak bir şeylerinin olmadığını ve faaliyetlerini sürdürebilmek için buna mecbur olduklarını belirtmiş ve özür dilemişlerdir.¹⁴⁹ Bu noktada, Yahoo!'nın Çin'de 2013 yılı itibariyle e-posta hizmetlerine son verdiğini, 2021 yılı itibariyle de Çin pazarından tamamen çekildiğinin altı çizilmelidir.¹⁵⁰

¹⁴⁷ Dava, Fransa'daki davanın davacısı olan Licra topluluğuna karşı açılmıştır. Yahoo! Inc. v. La Ligue Contre Le Racisme Et, 145 F. Supp. 2d 1168 (N.D. Cal. 2001), 145 F. Supp. 2d 1168 (U.S. District Court for the Northern District of California 07 Haziran 2001).

¹⁴⁸ Duh, "Yahoo! Inc. v. LICRA", ss. 363-64.

¹⁴⁹ Elonnai Hickok, "Intermediary Liability and State Surveillance, Global Information Society Watch", <https://giswatch.org/en/communications-surveillance/intermediary-liability-and-state-surveillance>, (22.10.2024) ; Suzor, *Lawless*, s. 122.

¹⁵⁰ <https://www.bbc.com/news/technology-59136937>, (12.2.2021).

Doğrudan kamusal bir talep olarak değerlendirilemese devlet ve şirket arasındaki farklı ilişkiler de kullanıcıların hak ve hürriyetleri bakımından etki doğurabilmektedir. Buna ilişkin bir örnek, yakın tarihte Avustralya’da yaşanmıştır. Avustralya’da, internetin gazetecilik mesleği bakımından neden olduğu gerileme ve bu gerileme dolayısıyla yayın kuruluşlarından gelen şikayetler doğrultusunda hazırlanan bir yasa ile Facebook ve Google’a barındırdıkları içerikler dolayısıyla yayıncılara ödemeye yapma zorunluluğu getirilmiştir.¹⁵¹ Bu düzenleme sonrasında, yayıncılarla çeşitli görüşmeler yürüten Google’ın aksine, Facebook, Avustralyalı yayıncıların ve kullanıcıların Avustralya ve uluslararası haber içeriğini paylaşmalarını veya görüntülerini yasaklamaya karar vermiştir. Sonrasında, hükümetin geri adım atmasıyla başlayan müzakerelerle birlikte Facebook tarafından bu yasağa son verilmiş olsa da söz konusu yasaklama kararı, internet şirketlerinin gücünü ve insan haklarına yönelik potansiyel riski göstermesi bakımından önemlidir.¹⁵²

Bu çalışma, şirketlerin yalnızca ticari çıkarları değil, kamusal faydayı da göz önünde bulundurarak hareket etmeleri gerektiği önermesinden yola çıkmaktadır. İnternet şirketleri, dijital dönüşümün en güçlü aktörleri olarak, ifade özgürlüğü, bilgi edinme özgürlüğü gibi temel hakların korunmasında ve ihlalinde belirleyici bir rol oynamaktadırlar. Bu kapsamda, çalışma, internet hizmeti sunan tüm şirketleri değil, özellikle de ifade özgürlüğü ve bilgi edinme özgürlüğü üzerinde doğrudan etkisi olan, internet kamusal alanını şekillendiren şirketlere odaklanmaktadır. Bu tür şirketler, bilgi toplumu hizmetleri sağlayıcıları, sosyal ağ sağlayıcıları, internet araçları ve çevrimiçi platformlar gibi çeşitli kavramlarla ifade edilse de bu çalışmada kapsayıcı bir yaklaşımla "internet şirketleri" terimi tercih edilmiştir. Bu tercih, insan hakları alanında özel şirketlerin sorumluluklarının ele alındığı temel metinlerden olan Birleşmiş Milletler İş Dünyası ve İnsan Hakları Rehber İlkeleri’nde kullanılan terminoloji ile de uyumludur.

Bu kapsamda, çalışmanın birinci bölümünde, Birleşmiş Milletler, OECD ve ILO sistemlerinde, özel aktörler olan şirketlerin insan hakları yükümlülüklerinin nasıl ele alındığı değerlendirilmektedir. Birleşmiş Milletler İş Dünyası ve İnsan Hakları Rehber İlkeleri’nde şirketlerin insan haklarına saygı gösterme sorumluluğu, başkalarının insan

¹⁵¹ Pollicino, “Digital Private Powers Exercising Public Functions”, s. 1.

¹⁵² Giovanni De Gregorio, **Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society**, Cambridge: Cambridge University Press, 2022, s. 9.

haklarını ihlal etmekten kaçınmaları ve yaptıkları olumsuz insan hakları etkilerini ortadan kaldırmaları gerektiği şeklinde açıklanmaktadır. Bu sorumluluk tüm ticari şirketleri ve bazıları belirli bağlamlarda daha fazla dikkat gerektirse de uluslararası düzeyde kabul edilmiş tüm insan haklarını kapsamaktadır.

İkinci bölümde, Avrupa Konseyi ve Avrupa Birliği'ndeki gelişmeler incelenmektedir. Avrupa Konseyi'nde, ifade özgürlüğünün korunması, nefret söylemiyle ve şiddeti veya ayrımcılığı tahrik eden diğer içeriklerle mücadele edilmesi, internet kullanıcılarının kişisel verilerinin korunması ve çocuklara yönelik risklerin önlenmesi konusunda internet şirketlerinin yükümlülükleri ele alındığı çok sayıda tavsiye kararı bulunmaktadır. AİHM içtihadı da bu şirketlerin insan hakları üzerindeki etkileri ve devletin buna yönelik pozitif yükümlülükleri konusunda önemli bir bakış açısı sunmaktadır. Avrupa Birliği'nde ise 2000 yılında kabul edilen E-Ticaret Direktifinden 2022 yılında kabul edilen Dijital Hizmetler Yasası'na uzanan bir dönüşüm söz konusudur. E-Ticaret Direktifi'nin yirmi yıl önce kabulünden bu yana çevrimiçi platformlar dijital ekonomide kilit araçlara dönüşürken, aynı zamanda bilginin hem kaynağı hem de şekillendiricisi haline gelmiştir. Günümüzün arama motorları, sosyal medya ağları ve eticaret platformları, yalnızca hangi kullanıcıların ekosisteme katılabileceğini veya işlemlerin platform üzerinden nasıl gerçekleştirileceğini değil, aynı zamanda ilgili kullanıcıların hangi bilgileri alacağını da belirlemektedir. Bu dönüşümün bir sonucu olarak Dijital Hizmetler Yasası'nda, yenilikçiliği kolaylaştıran ve tüketicinin korunması ilkesi de dahil olmak üzere Avrupa Birliği Temel Haklar Şartında yer alan temel hakların etkin bir şekilde korunduğu güvenli, öngörülebilir ve güvenilir bir çevrimiçi ortam sağlanması amaçlanmıştır.

Son olarak üçüncü bölümde, Türk hukukundaki mevcut durum ele alınmaktadır. Bu kapsamda, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunu'nda yer alan erişimin engellenmesi ve içeriğin çıkarılması prosedürleri incelenmiştir. Çok sayıda değişikliğe uğrayan ve Anayasa Mahkemesi'nin çok sayıda ihlal ve iptal kararına konu olan Kanun, mevcut şekliyle internet ortamında temel hak ve özgürlüklerin etkili bir şekilde korunması amacını gerçekleştirirmede yetersiz kalmaktadır. 2020 yılında yapılan değişikliklerle, sosyal ağ sağlayıcıların insan hakları üzerindeki etkileri dikkate alınarak daha kapsamlı yükümlülüklerle tabi tutulması bu yolda atılmış önemli bir adımdır. Ancak

bu deęiřiklikler de ngrlebilirlik ve lllk ilkeleri bakımından eřitli sorunlar iermektedir. alıřmada, internet ortamında yarıřan hakların dengelenmesi, internet ynetiminde řeffaflıęın saęlanması ve internet ortamının yarattıęı risklerle etkili řekilde mcadele edilmesine ynelik neriler sunulmuřtur.



BİRİNCİ BÖLÜM

İNTERNET ŞİRKETLERİNİN İNSAN HAKLARI SORUMLULUKLARINA İLİŞKİN ULUSLARARASI STANDARTLAR

İnsan hakları hukuku doğası gereği devlet merkezlidir. Başka bir ifadeyle, insan hakları hukukunda birincil görev bireyler ya da şirketler gibi devlet dışı aktörlerde değil, devlettendir. Ancak devletin yükümlülüğün bir parçası da insan hakları hukukunun yatay etkisi olarak adlandırılan, özel kişilerin insan haklarını ihlal etmemesini sağlama görevidir. Böylece, insan hakları hukuku dikey ilişkiye (devletin bireye karşı yükümlülükleri) odaklanırken, özel taraflar arasındaki alanda ortaya çıkabilecek yatay etkiyi de kabul eder.

Geçtiğimiz on yıllık sürede insan hakları ve özel aktörler arasındaki ilişki insan hakları hukukunun önemli tartışma alanlarından biri olmuştur. Bu kapsamda sürdürülen çalışmalar bazı girişimlerin ortaya çıkması ve esnek hukuk kurallarının (*soft law*) benimsenmesi ile sonuçlanmıştır. Bu yönde atılmış en önemli adımlardan biri, Birleşmiş Milletler İnsan Hakları Konseyi'nin İş Dünyası ve İnsan Haklarına Dair Rehber İlkeleri¹⁵³ (UNGPs) onaylamasıdır. İş dünyası ile insan hakları ilişkisinin kurulması ve şirketlerin insan hakları yükümlülüklerine ilişkin küresel standartların ortaya koyulması bakımından bir dönüm noktası olarak kabul edilen Rehber İlkeler, şirketlerin sorumluluklarının sektörel olarak da ele alınması bakımından bir basamak tahtası işlevi görmüştür.

Örneğin, büyük internet şirketlerinin öncülüğünde oluşturulan ve yatırımcılar, akademik topluluklar ile sivil toplum kuruluşlarının katılımıyla uluslararası işbirliği organizasyonuna dönüşen Küresel Ağ Girişimi (*Global Network Initiative*), yatırımcı, sivil toplum ve akademik toplulukların deneyim ve uzmanlığından yararlanarak İfade Özgürlüğü ve Gizlilik İlkeleri'ni oluşturmuştur.¹⁵⁴ Bu ilkelere, ifade özgürlüğü ve

¹⁵³ Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework (HR/PUB/11/04), UN, 2011, https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinessshr_en.pdf. (2.11.2024)

¹⁵⁴ The GNI Principles, **Global Network Initiative**, <https://globalnetworkinitiative.org/gni-principles/>. (2.11.2024)

gizlilik ile ilgili olarak teknoloji şirketlerinin, ulusal yasalara uygun davranmanın ötesine geçen insan haklarına saygı gösterme yükümlülükleri olduğu kabul edilmiştir:

“Teknoloji şirketleri, faaliyet gösterdikleri her yerde geçerli yasalara uymalı ve uluslararası alanda tanınan insan haklarına saygı göstermelidir. Ulusal yasa, yönetmelik ve politikaların uluslararası standartlarla uyumlu olmaması durumunda, teknoloji şirketleri hükümet taleplerinin, yasaların veya düzenlemelerin olumsuz etkilerini mümkün olduğunca azaltmaya ya da bu etkilerle başka şekillerde başa çıkmaya çalışmalı ve uluslararası insan hakları ilkelerine en üst düzeyde bağlı kalmanın yollarını aramalıdır. Bu kapsamda, teknoloji şirketlerinin insan haklarına saygı gösterme çabalarını somut olarak ortaya koyabilmeleri de gereklidir.”¹⁵⁵

Avrupa Komisyonu da BM İş Dünyası ve İnsan Haklarına Dair Rehber İlkeleri uygulama konusunda BİT Sektörü Rehberi'ni yayınlamıştır. Rehber, ICT şirketlerinin insan hakları üzerinde doğrudan veya dolaylı olarak yaratabilecekleri olumsuz etkileri önlemeleri ve sorumluluklarını yerine getirmeleri için detaylı bir çerçeve sunmaktadır. Bu kapsamda, ICT sektöründe faaliyet gösteren şirketlere, veri güvenliği, gizlilik, bilgiye erişim gibi konular başta olmak üzere, insan hakları ihlallerini önlemek ve çözmek adına gerekli adımları nasıl atmaları gerektiğine dair önerilere yer verilmiştir. Bu öneriler arasında, risk analizi ve değerlendirme süreçleri; veri gizliliği ve güvenliği; şeffaflık; etkili başvuru mekanizmaları gibi öneriler öne çıkmaktadır.¹⁵⁶

BM Rehber İlkeler, Avrupa Konseyi'nin İnternet Kullanıcıları İçin İnsan Hakları Rehberi'nde de de referans alınan metinlerden biridir.¹⁵⁷ Bu doğrultuda, şirketlerin insan haklarına zarar vermekten veya bu zararları desteklemekten kaçınmaları ve bu tür etkilerin düzeltilmesi için çözüm sağlamaları veya çözüm süreçlerine katkıda bulunmaları

¹⁵⁵ Ibid., preamble.

¹⁵⁶ ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights, **European Commission**, (2013), <https://op.europa.eu/en/publication-detail/-/publication/ab151420-d60a-40a7-b264-adce304e138b>, (1.10.2023).

¹⁵⁷ Recommendation CM/Rec(2014)6 of the Committee of Ministers to Member States on a Guide to Human Rights for Internet Users, 16.04.2014, https://www.coe.int/en/web/freedom-expression/committee-of-ministers-adopted-texts/-/asset_publisher/aDXmrol0vvsU/content/recommendation-cm-rec-2014-6-of-the-committee-of-ministers-to-member-states-on-a-guide-to-human-rights-for-internet-users-adopted-by-the-committee-of-, (1.10.2023).

gerektiği kabul edilmiştir.¹⁵⁸ Ayrıca, özel sektör aktörlerinin şeffaflık ve hesap verebilirlik ilkelerine uygun hareket etmelerinin, sorumluluğu görünür hale getirme ve bu sorumluluğu etkin şekilde teşvik etmenin önemli bir yolu olarak vurgulanmıştır.¹⁵⁹

Ekonomik İş Birliği ve Kalkınma Örgütü (OECD) ile Uluslararası Çalışma Örgütü (ILO), şirketlerin insan hakları yükümlülüklerine ilişkin farklı ancak birbirini tamamlayan roller üstlenmektedir. OECD, Çok Uluslu Şirketler için Sorumlu İş Davranışı Rehberi¹⁶⁰ ve Dijital Hizmet Sağlayıcılar için Rehber İlkeler¹⁶¹ gibi araçlarla, şirketlere insan hakları, çalışma standartları, çevre ve yolsuzlukla mücadele konularında kapsamlı bir çerçeve sunar. Özellikle dijital hizmet sağlayıcılar için hazırlanan Rehber, çevrimiçi içerik yönetimi, veri gizliliği ve algoritmik şeffaflık gibi güncel konularda yol gösterici niteliktedir. ILO ise temel sözleşmeleri ve üçlü yapısı aracılığıyla, örgütlenme özgürlüğü, zorla çalıştırmanın yasaklanması, çocuk işçiliğinin önlenmesi ve ayrımcılıkla mücadele gibi çalışma hayatına özgü insan hakları standartlarını belirlemekte ve sosyal diyalogu teşvik etmektedir. Her iki kuruluş da şirketlerin tedarik zincirlerindeki insan hakları risklerini belirleme ve azaltma sorumluluğunu vurgulayarak, durum değerlendirme kavramını öne çıkarmaktadır. Bu sayede, BM, OECD ve ILO, şirketlerin insan hakları performansını iyileştirmelerine ve hesap verebilirliklerini artırmalarına katkı sağlayan önemli uluslararası aktörler olarak öne çıkmıştır.

I. Birleşmiş Milletler Sistemi

İnsan hakları ve özel şirketler arasındaki ilişkinin ortaya koyulması ve bu kapsamda özel şirketlerin insan hakları yükümlülüklerinin belirlenmesi konusunda küresel bir standart olarak kabul edilen Birleşmiş Milletler İş Dünyası ve İnsan Haklarına Dair Rehber İlkeler'de¹⁶² iş dünyasının insan hakları sorumlulukları sistematik bir şekilde ortaya konulmuştur. Bu ilkelerin benimsenmesi ve İnsan Hakları Konseyi'nin 16 Haziran 2011 tarih ve 17/4 sayılı kararıyla uygun bulunması, Birleşmiş Milletler bünyesinde bir süre devam eden çalışmaların sonucudur. Bu süreç, genel olarak üç aşamada ele

¹⁵⁸ Ibid., para. 54.

¹⁵⁹ Ibid., para. 27.

¹⁶⁰ OECD, **OECD Guidelines for Multinational Enterprises, 2011 Edition**, Paris, Organisation for Economic Co-operation and Development, 2011.

¹⁶¹ OECD Guidelines for Digital Service Providers, <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0389>, (23.10.2024).

¹⁶² "BM Guiding Principles".

alınmaktadır. Özel şirketlerin insan hakları ile ilişkilendirilmesinde ilk aşama, Ekonomik ve Sosyal Konsey'in, 1970'lerde Genel Sekreterlikten çok uluslu şirketlerin faaliyetlerinin insan haklarına etkileri üzerinde bir araştırma yapmasını talep etmesiyle başlamıştır. Bu aşamada, çeşitli girişimler söz konusu olmuşsa da bir sonuç elde edilemeden süreç son bulmuştur. İkinci aşamanın başlangıcı olarak kabul edilen 1990'lı yılların sonlardan itibaren ise çokuluslu şirketlerin insan haklarına etkileri konusunda daha yoğun çalışmalar sürdürülmüştür.¹⁶³ Bu kapsamda, 1999'da Birleşmiş Milletler Küresel Paktı (*UN Global Compact*) kurulmuş ve on temel ilke üzerinde anlaşılmıştır.¹⁶⁴

BM Küresel İlkeler Sözleşmesi; insan hakları, iş yaşamı, çevre ve yolsuzlukla mücadele alanlarında on evrensel ilkeyi daha iyi bir konuma ulaştırmak amacıyla işletmeleri, kurumları, sivil toplum kuruluşlarını ve hükümetleri bir araya getiren temel platformlardan birini temsil etmektedir. İş dünyası ve insan hakları arasındaki ilişki, belirtilen ilkeler dizisinin birinci ve ikinci maddelerinde düzenlenmiş ve iş dünyasının bu kapsamdaki sorumlulukları *ilan edilmiş insan haklarını desteklemek ve haklara saygı göstermek* ile *insan hakları ihlallerinin ortağı olmamak* şeklinde belirtilmiştir. Anlaşılabacağı üzere bu yükümlülükler; şirketlere insan haklarına ilişkin somut ve kapsamlı bir çerçeve sunmamakta, onları kurumsal sosyal sorumluluk çerçevesine göre, etki alanları dahilinde insan haklarından sorumlu kılmaktadır. Etki alanı kavramına ilişkin olarak net bir tanım olmasa da bu kavram bir şirketin belirli bir siyasi, sözleşmesel, ekonomik veya coğrafi yakınlığa sahip olduğu bireyleri kapsayacak şekilde kullanılmaktadır.¹⁶⁵ Ne var ki, tamamen gönüllülük esasına dayanan ve şirketlere ahlaki yükümlülükler getiren Küresel İlkeler Sözleşmesi, hukuken bağlayıcı bir niteliğe sahip olmaması ve kapsamının sınırlı olması dolayısıyla eleştirilmiştir.

İş dünyasının insan hakları üzerindeki etkilerine ilişkin üçüncü aşama, 2005 yılında İnsan Hakları Konseyi tarafından bu konuda bir uzman görevlendirme kararı alınması ve bu kapsamda Birleşmiş Milletler Genel Sekreterlik Özel Temsilcisi John G. Ruggie'nin görevlendirilmesiyle başlamıştır. Özel temsilci Ruggie, göreve başladığı 2005'ten 2011

¹⁶³ Özge Yucel Dericiler, "Şirketlerin İnsan Haklarına İlişkin Yükümlülüklerinin Niteliği ve Temellendirilmesi Sorunu: Saygı Gösterme Sorumluluğu Ne Yükler?", **Antalya Bilim Üniversitesi Hukuk Fakültesi Dergisi**, Cilt: 6, Sayı: 11, 2018, s. 60.

¹⁶⁴ Belirtilen ilkelere ilişkin ayrıntılı bilgi için bkz. <https://unglobalcompact.org/what-is-gc/mission/principles>.

¹⁶⁵ Jørgensen, "Human Rights and Private Actors in the Online Domain", s. 254.

yılına kadar BM İnsan Hakları Konseyi'ne BM Genel Kurulu'na ve İnsan Hakları Komisyonu'na iş dünyası ve insan haklarına ilişkin çok sayıda rapor sunmuştur.¹⁶⁶ Ruggie'nin yıllar süren çalışmaları, 2011 yılında Birleşmiş Milletler İş Dünyası ve İnsan Haklarına Dair Rehber İlkeler'in onaylanmasıyla sonuçlanmıştır.¹⁶⁷

A. Genel Olarak İş Dünyası Karşısında İnsan Haklarının Korunması

Birleşmiş Milletler bünyesinde iş dünyası ve insan hakları ilişkisi ve bu konuda devletlerin ve şirketlerin yükümlülükleri, Birleşmiş Milletler İş Dünyası ve İnsan Haklarına Dair Rehber İlkeler: BM Koruma, Saygı Gösterme ve Telafi Edici Çözüm Üretme Çerçevesinin Uygulanması başlıklı belgede kapsamlı bir şekilde ele alınmıştır. Bununla birlikte Rehber İlkeler, BM sistemi içerisinde farklı normatif gelişmelere zemin hazırlamıştır. Bu gelişmelerden biri de Birleşmiş Milletler Çocuk Hakları Komitesi'nin İş Sektörünün Çocuk Haklarına Etkileri Hakkında Devletin Yükümlülüklerine İlişkin 16 No'lu Genel Yorum'dur.¹⁶⁸ 16 No'lu Genel Yorum'da, BM Rehber İlkelere uygun olarak, devletlerin iş dünyasının çocuk haklarına olumsuz etkileri konusundaki yükümlülükleri belirlenmiş ve büyüklüğü, sektörü, yeri, sahipliği ve yapısı ne olursa olsun ulusal ve ulus ötesi tüm ticari kuruluşların bu kapsamda olduğu belirtilmiştir. Bununla birlikte bilgi ve iletişim teknolojilerinde yaşanan gelişmeler çocuk haklarını doğrudan etkilediğinden, Genel Yorum internet şirketlerinin sorumluluklarının belirlenmesinde önemlidir.

1. Küresel İlkeler Sözleşmesi

BM Küresel İlkeler Sözleşmesi (*UN Global Compact*), 2000 yılında Birleşmiş Milletler tarafından başlatılan ve işletmeleri insan hakları, çalışma standartları, çevre ve yolsuzlukla mücadele alanlarında evrensel ilkeleri benimsemeye teşvik eden bir kurumsal sürdürülebilirlik girişimidir. Bu sözleşme, iş dünyasının küresel sorunlara çözüm sunabilecek etkili bir güce sahip olduğu düşüncesinden hareketle, şirketlerin sadece kâr

¹⁶⁶ Özel Temsilci Ruggie'nin 2005-2011 tarihleri arasındaki çalışmaları hakkında ayrıntılı bilgi için bkz. <https://www.ohchr.org/en/special-procedures/wg-business/special-representative-secretary-general-human-rights-and-transnational-corporations-and-other>, (2.10.2024).

¹⁶⁷ Jørgensen, "Human Rights and Private Actors in the Online Domain", s. 254.

¹⁶⁸ General Comment No. 16 on State Obligations Regarding the Impact of the Business Sector on Children's Rights (CRC/C/GC/16), **Refworld**, 17.04.2013, <https://www.refworld.org/legal/general/crc/2013/en/102811>, (1.10.2024).

odaklı değil, aynı zamanda sosyal sorumluluklarını da göz önünde bulunduran bir yaklaşımla faaliyet göstermelerini amaçlamaktadır.

Küresel İlkeler Sözleşmesi, günümüzde, kurumsal sorumluluğa ilişkin sorunları çözebilme potansiyeli bakımından öne çıkmaktadır. Bu potansiyelin birkaç nedeni bulunmaktadır: (1) Küresel İlkeler Sözleşmesi, Sürdürülebilir Kalkınma Amaçları¹⁶⁹ ile uyum içinde olan belirli ilkeler kümesine odaklanmaktadır; (2) dünya genelinde en geniş kapsamlı çok paydaşlı sürdürülebilirlik girişimi olup, şu anda 25.000'den fazla katılımcıya sahiptir ve (3) işletmeleri kapsayarak geniş bir paydaş kitlesiyle büyük sorunların çözümüne katkıda bulunmayı amaçlamaktadır.¹⁷⁰

Küresel İlkeler Sözleşmesi uyarınca kurumsal sorumluluk en azından insan hakları, çalışma yaşamı, çevre ve yolsuzlukla mücadele alanlarında temel sorumlulukları karşılayacak şekilde faaliyet göstermek anlamına gelmektedir. Bu doğrultuda, belirtilen dört başlık altında, şirketlerin faaliyetlerine ilişkin on ilke kabul edilmiştir.¹⁷¹ Bununla birlikte, bu ilkelerin gerçekleştirilebilmesine yönelik de çeşitli girişimlerde bulunulmuştur. Örneğin, 2003 yılında, zorunlu bir “İlerleme Bildirimi” politikası kabul edilmiş, böylece katılımcıların on ilke bakımından ilerleme süreçlerini raporlamaları gerekliliği kabul edilmiştir. Bununla bağlantılı olarak ayrıca, 2005 yılından bu yana, raporlama yükümlülüğünü yerine getirmeyen katılımcılar listeden çıkarılmıştır. 2011 yılında ise, katılımcılara girişimin ilkelerinin nasıl uygulanacağına yönelik bir program hazırlanarak raporlama yükümlülüğüne ilişki ihmallerin önüne geçilmesi amaçlanmıştır.¹⁷²

Küresel İlkeler Sözleşmesi’nde insan hakları konusunda iki ilke yer almaktadır: i) iş dünyası uluslararası kabul görmüş insan haklarına saygı göstermeli ve bu hakları korumalıdır, ii) iş dünyası insan hakları ihlallerine ortak olmamalıdır.¹⁷³

¹⁶⁹ <https://www.globalcompactturkiye.org/surdurulebilir-kalkinma-amaclari>, (4.10.2024).

¹⁷⁰ Stefan Schembera, Alice Hengevoss, “Institutional Drivers of Responsible Innovation: The Impact of the UN Global Compact in the Digital Age”, s. 8, <https://papers.ssrn.com/abstract=3485060>, (11.11.2019).

¹⁷¹ The Ten Principles, UN Global Compact, <https://unglobalcompact.org/what-is-gc/mission/principles>, (22.10.2024). Sözleşme başlangıçta insan hakları, çalışma yaşamı ve çevre başlıkları ile olarak dokuz ilkedен oluşmuştur, onuncu ilke olan yolsuzlukla mücadele 2004 yılında eklenmiştir.

¹⁷² Schembera, Hengevoss, “Institutional Drivers of Responsible Innovation”, s. 10.

¹⁷³ The Ten Principles, UN Global Compact.

Bu ilkelerden saygı gösterme, iş dünyasının insan haklarını ihlal etmekten kaçınmak için gerekli özeni göstermesi ve dahil oldukları olumsuz insan hakları etkilerini ele alması gerektiği anlamına gelmektedir. İnsan haklarını koruma ilkesi ise saygı göstermenin ötesinde, insan haklarını desteklemek için harekete geçmeyi gerektirmektedir. Bu faaliyetler; ana iş alanında, stratejik sosyal yatırımlar veya hayırseverlik çalışmaları, kamu politikalarına yönelik savunuculuk veya çeşitli iş birlikleri yoluyla olabilecektir. Bu tür gönüllü eylemler, insan haklarına saygı gösterme yükümlülüğünü yerine getirmenin yerine değil, bu yükümlülüğe tamamlayıcı olarak gerçekleştirilmelidir. Söz konusu ilkeler yerine getirilirken kadınlar, çocuklar, engelliler, yerli halklar, göçmen işçiler, yaşlılar vb. dahil olmak üzere savunmasız grupların haklarına özel dikkat gösterilmelidir.¹⁷⁴

Küresel İlkeler Sözleşmesi'ne göre, iş dünyası tüm haklar üzerindeki potansiyel etkilerini göz önünde bulundurmalıdır. Bununla birlikte, mevcut veya potansiyel etkilerin çok ciddi olduğu ve/veya şirket ile suistimal arasında güçlü bir bağlantı olduğu durumlar özel değerlendirme yapılmasını gerektirmektedir. Sözleşme ile kurumsal sorumluluk, Devletlerin insan hakları yükümlülüklerinden bağımsız olarak kabul edilmektedir. Bununla bağlantılı olarak, ulusal yasaların uluslararası standartlarla çeliştiği durumlara ilişkin de bir rehberlik sunulmakta, şirketler uluslararası olarak tanınan insan hakları ilkelerine saygı göstermenin yollarını aramaya teşvik edilmektedir.¹⁷⁵

İnsan haklarına saygı gösterme eylemi, sadece etik bir sorumluluk değil, aynı zamanda bir iş meselesidir. Bir şirketin insan haklarına uygun hareket etmemesi, itibar kaybetmesine, sosyal lisansının tehlikeye girmesine, tüketici boykotlarına, yasal sorumluluk risklerine, yatırımcı ve iş ortaklarının olumsuz tepkilerine ve çalışanların moralinin düşmesine yol açabilecektir. Bütün bunlar, şirketler için ciddi bir risk ve maliyet potansiyeli teşkil etmektedir. Dolayısıyla insan haklarına duyarlı ve kapsayıcı iş modelleri, işletmelere yeni ürün ve hizmetler geliştirme, yeni pazarlara erişim sağlama ve faaliyet gösterdikleri toplumun değerli bir üyesi olma fırsatı sunmaktadır.¹⁷⁶

¹⁷⁴ UN Global Compact, principle 1.

¹⁷⁵ Ibid.

¹⁷⁶ Ibid.

İnsan hakları ihlallerine ortak olmama ilkesi ise şirketlerin, hükümetin, bireyin veya başka bir grubun neden olduğu bir insan hakları ihlaline karışmaktan kaçınmaları anlamına gelmektedir. Şirketlerin ilk ilkeye uygun olarak insan haklarına saygı gösterip bu hakları korumaları ve insan haklarına yönelik sistematik bir yönetim yaklaşımıyla hareket ikinci ilke bakımından insan haklarına ortak olma risklerini azaltmaktadır. Bununla birlikte, mevcut riskler her halükârda analiz edilmeli, önlenmeli ya da azaltılmalıdır.¹⁷⁷

Bir şirketin insan hakları ihlallerine ortaklığı genellikle iki unsurdan oluşmaktadır: i) şirketin ya da şirket temsilcisinin bir başkasının insan hakları ihlaline yardımcı olan bir eylemi ya da ihmali ve ii) şirketin bu eylemin insan hakları ihlaliyle bağlantılı olduğu bilgisine sahip olması. Buna göre şirketler, başkalarının insan hakları ihlallerini kolaylaştıran, meşrulaştıran, teşvik eden vb. eylemlerden ya da ihmallerden kaçınmalıdır. Bu ilke, şirketlere, yasal olarak sorumlu tutulabilecek hallerin ötesinde bir sorumluluk getirmekte ve yasal sorumlulukla bağlantılı olan sorumluluk hallerine ek olarak şirketin sistematik veya sürekli insan hakları ihlalleri karşısında sessiz veya eylemsiz kalması halini de içermektedir. Şirkete etik sorumluluk yükleyen bu ilke de aynı zamanda şirketin ticari olarak menfaatlerine de uygundur. Şirketler, insan hakları ihlallerine ortak olmama ilkesi uyarınca, etkili bir insan hakları politikası geliştirerek ve özen yükümlülüklerini yerine getirerek, insan hakları ihlalleriyle ilişkilendirilme risklerini azaltmaya yönelik tedbirler almalıdır. Bu kapsamda, uluslararası standartları takip edilmesi, insan hakları ihlallerin kınanması, etki alanlarındaki insan hakları sorunlarına yönelik farkındalık oluşturulması, risklerin analiz edilmesi, insan hakları etkilerinin değerlendirilmesi gibi adımlar atılabilir.¹⁷⁸

Küresel İlkeler Sözleşmesi, şirketlerin sosyal sorumluluğu önemsemesini sağlamak için farkındalık yaratsa da etkisi belirsizdir. Sözleşme, katılımcı şirketlerin taahhütlerine gerçekten uyup uymadığının takibi ve denetimine yönelik mekanizmalardan yoksundur. Öte yandan, gerçek bir sorumluluk üstlenmeyen şirketlerin imaj çalışmaları için kötüye kullanılabilir.¹⁷⁹ Buna rağmen, Küresel İlkeler

¹⁷⁷ UN Global Compact, principle 2.

¹⁷⁸ Ibid.

¹⁷⁹ Aakanksha Nath, Arpita Saha, "U.N. Global Compact: The Lifeline of Corporate Social Responsibility", SSRN Electronic Journal, 2008, ss. 27, 28, <https://papers.ssrn.com/abstract=1329289>, (1.8.2022).

Sözleşmesi, iş dünyasının insan hakları sorumluluklarına ilişkin önemli bir çerçeve sunmaktadır. Nitekim, Küresel İlkeler Sözleşmesi ile BM İnsan Hakları Yüksek Komiserliği Ofisi (OHCHR) tarafından yayımlanan ortak bir çalışmada, Rehber İlkeler'in Küresel İlkeler Sözleşmesi ile doğrudan ilgili olduğu belirtilmektedir. Buna göre, Rehber İlkeler, Küresel İlkeler Sözleşmesi'ne kavramsal ve operasyonel netlik sağlamak ve katılımcılara insan haklarına saygı gösterme sorumluluklarını yerine getirmelerini sağlamak için uygulamaları gereken politikalar ve süreçler konusunda yetkili bir çerçeve sunmaktadır.¹⁸⁰

2. İş Dünyası ve İnsan Haklarına Dair Rehber İlkeler

Birleşmiş Milletler'de, şirketlerin insan hakları sorumlulukları düzenleme çabaları 1970'li yıllara dayanmaktadır. Bu kapsamda 1973 ve yılında 1980'lerin başında çeşitli girişimlerde bulunulmuş; ancak bu girişimler başarısızlıkla sonuçlanmıştır. Devam eden çalışmalar sonucunda 2003 yılında, doğrudan şirketleri konu alan ve şirketlere insan haklarını teşvik etme, güvence altına alma, saygı gösterme ve koruma yükümlülüğü yükleyen bir taslak kabul edilmiştir. Şirketlerin insan hakları yükümlülüklerine ilişkin güçlü bir mekanizma sağlayan bu taslak, birçok sivil toplum kuruluşu tarafından memnuniyetle karşılanmışsa da devletlerin insan hakları sorumluluklarının iş dünyasına kaydırılmasının, insan haklarına, iş sektörüne ve kalkınma hakkına zarar vereceğine yönelik karşı görüşlerin etkisiyle kabul görmemiştir. 2005 yılında, özel temsilci John G. Ruggie şirketlerin insan hakları sorumluluklarının netleştirilmesi için görevlendirilmesiyle bu konuda önemli bir adım atılmıştır.¹⁸¹ Ruggie'nin şirketlerin insan haklarına saygı gösterme sorumluluğunu belirlediği "Koruma, Saygı Gösterme ve Telafi Edici Çözüm Üretme" çerçevesi¹⁸² 2008 yılında İnsan Hakları Konseyi tarafından kabul edilmiştir. 2011 yılında ise, bu çerçevenin kapsam ve içeriği detaylandırılarak 31 ilkeden oluşan Rehber İlkeler kabul edilmiştir.

¹⁸⁰ The UN Guiding Principles on Business and Human Rights: Relationship to UN Global Compact Commitments, 2011, https://d306pr3pise04h.cloudfront.net/docs/issues_doc%2Fhuman_rights%2FResources%2FGPs_GC+note.pdf, (12.9.2024).

¹⁸¹ Alex Newton, **The Business of Human Rights: Best Practice and the UN Guiding Principles**, Routledge, 2019, s. 43.

¹⁸² Protect, Respect and Remedy: A Framework for Business and Human Rights. Report of the Special Representative of the Secretary-General on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises, John Ruggie (A/HRC/8/5), United Nations, 07.04.2008, <https://digitallibrary.un.org/record/625292>, (10.7.2023).

Birleşmiş Milletler İş Dünyası ve İnsan Haklarına Dair Rehber İlkeler, şirketlerle bağlantılı insan hakları ihlallerinin önlenmesi, azaltılması ve telafi edilmesi için devletlerin ve şirketlerin uygulaması gereken bir dizi ilke sunmaktadır. Bu ilkeler, Birleşmiş Milletler'in şirketlerin insan haklarına nasıl saygı göstermeleri gerektiği konusundaki beklentilerini ilk kez açıklamıştır.

Rehber İlkeler, uzun bir süre şirketler ile insan hakları ilişkisini ahlaki boyutta ele aldığı ve şirketlere ilişkin bağlayıcı düzenlemelere yer verilmeyişi¹⁸³ dolayısıyla eleştirilmişse de günümüzde bu eleştiriler yerini söz konusu ilkelerin uygulamaya geçirilmesi konusunda neler yapılabileceği sorununa bırakmıştır.¹⁸⁴ Dolayısıyla, Rehber İlkeler her ne kadar bağlayıcı bir nitelik taşımasa da şirketler ve insan hakları ilişkisinin ele alındığı öncü bir metin olmasının yanında, somut olarak yapılabileceklerle dayanak olma bakımından da önem taşımaktadır. Bu bakımdan, İnsan Hakları Konseyi'nin Rehber İlkelerle dair beklentilerinin gerçekleştiği söylenebilir:

“Birleşmiş Milletler, dünyaya iradesini dayatabilecek merkezi bir komuta ve kontrol sistemi değildir; aslında, üye devletlerin verdiği yetkiler dışında bir “iradesi” yoktur. Ancak entelektüel liderlik yapabilir ve beklentiler ile hedefler koyarak öncülük edebilir. İnsan Hakları Konseyi, bu çerçeveyi destekleyerek, daha fazla detaylandırılmasını teşvik ederek ve ilgili tüm toplumsal aktörlerin

¹⁸³ Rehber İlkelerin yayınlanması sonrasında devam eden bu tartışmalar sürerken Ekvador, "çokuluslu şirketlerin ve diğer işletmelerin faaliyetlerini uluslararası insan hakları hukuku çerçevesinde düzenlemek için uluslararası hukuki bağlayıcılığı olan bir enstrüman geliştirmek" üzere Birleşmiş Milletler İnsan Hakları Konseyi'nde hükümetler arası çalışma grubu kurulmasını önermiştir. Cezayir, Benin, Burkina Faso, Çin, Kongo, Fildişi Sahili, Küba, Etiyopya, Hindistan, Endonezya, Kazakistan, Kenya, Fas, Namibya, Pakistan, Filipinler, Rusya Federasyonu, Güney Afrika, Venezuela ve Vietnam bağlayıcı olmayan mekanizmaların yetersiz olduğu gerekçesiyle bu öneriye destek verirken; Avusturya, Çek Cumhuriyeti, Estonya, Fransa, Almanya, İrlanda, İtalya, Japonya, Karadağ, Kore Cumhuriyeti, Romanya, Eski Yugoslavya Cumhuriyeti Makedonya, Büyük Britanya ve Kuzey İrlanda Birleşik Krallığı, Amerika Birleşik Devletleri bu öneriye karşı çıkmışlardır. Öneriye karşı çıkan devletlerin genel yaklaşımı, yeni bir sözleşmeye gerek olmadığı ve mevcut düzenlemeler ile etkili bir mekanizmanın kurulabileceği gerekçesine dayanmaktadır. Son olarak Arjantin, Botsvana, Brezilya, Şili, Kosta Rika, Gabon, Kuveyt, Maldivler, Meksika, Peru, Suudi Arabistan, Sierra Leone, Birleşik Arap Emirlikleri ise çekimser kalmışlardır. Human Rights Council, Elaboration of an international legally binding instrument on transnational corporations and other business enterprises with respect to human rights (A/HRC/RES/26/9), 14.07.2014, https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/26/9, (10.7.2023). UN Human Rights Council, Resolution 26/9 Elaboration of an international legally binding instrument on transnational corporations and other business enterprises with respect to human rights, UN Doc. A/HRC/RES/26/9, 14 July 2014.

¹⁸⁴ Özge Yücel Dericiler, **Uluslararası Esnek Hukuktan Bağlayıcı Hukuka: Şirketler ve İnsan Hakları**, On İki Levha, 2023, s. 69.

benimsemesini sağlayarak, iş dünyası ve insan hakları alanındaki yönetim boşluklarının kapatılmasına önemli bir katkıda bulunabilir.”¹⁸⁵

Küresel İlkeler Sözleşmesi’nde benimsenen *etki alanı* yaklaşımının aksine, Rehber İlkeler’de ticari faaliyetlerin mevcut ve potansiyel insan hakları etkilerine odaklanılmakta; bu etki Rehber İlkeler’de, *devletin insan haklarını koruma görevi, şirketlerin insan haklarına saygı gösterme sorumluluğu ve telafi edici çözüm üretme* şeklinde üç temel başlıkta ele alınmaktadır. Ruggie, bu üç temel ilkenin bir bütünün parçaları olduğunu ve sürdürülebilir ilerlemenin sağlanmasında birbirlerine desteklediklerini belirtmiş ve bu ilkelerin işlevlerini şu şekilde açıklamıştır: “*Devletin koruma görevi, çünkü devlet uluslararası insan hakları rejiminin tam merkezinde yer alır; şirketlerin saygı gösterme sorumluluğu, çünkü bu toplumun insan hakları konusunda iş dünyasından temel beklentisidir ve çözüm yoluna erişim, çünkü en uyumlu çabalar bile tüm istismarları önleyemez.*”¹⁸⁶ BM Rehber İlkeler, üç temel prensipten oluşmaktadır:¹⁸⁷

- Devletlerin uygun politikalar, düzenlemeler ve yargısal süreçler aracılığıyla, şirketler de dahil üçüncü tarafların insan hakları ihlallerine karşı koruma yükümlülüğü.
- Şirketlerin başkalarının haklarını ihlal etmemek için gereken özeni göstermesi ve kendi faaliyetlerinden kaynaklanan olumsuz etkileri ele almasını ifade eden insan haklarına saygı gösterme sorumluluğu.
- Mağdurların yargı yoluyla ya da yargı dışı mekanizmalarla etkili çözüm yollarına erişiminin sağlanması.

Bu prensipleri açıklamadan önce, Rehber İlkeleri daha iyi anlamak için bazı önemli özelliklerini belirtmek faydalı olacaktır. Buna göre Rehber İlkeler:

¹⁸⁵ “Protect, Respect and Remedy”, para. 107.

¹⁸⁶ Guiding Principles on Business and Human Rights: Implementing the United Nations ‘Protect, Respect and Remedy’ Framework. Report of the Special Representative of the Secretary-General on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises (A/HRC/17/31), United Nations, 21.03.2011, s. 4, <https://digitallibrary.un.org/record/705860>, (10.10.2023).

¹⁸⁷ Report of the Special Representative of the Secretary-General on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises, John Ruggie, para. 6.

- a) Şirketlerin büyüklüğü, sektörü, konumu, mülkiyeti veya yapısı ne olursa olsun, tüm devletler ve şirketler için geçerlidir. Ancak, tamamen gönüllü bir niteliğe sahiptirler.
- b) İşletmelerin tüm uluslararası tanınmış insan hakları üzerindeki etkisini kabul etmektedir.
- c) İnsan haklarının birbirinden ayrılamayacağını, yani bir tarafta doğru şeyler yapmanın diğer taraftaki zararları telafi etmeyeceğini vurgulamaktadır.
- d) Tüm sektörlerin insan haklarına saygı göstermek için anlamlı bir şekilde katılımını gerektirmektedir.
- e) Devletler veya işletmeler için yeni hukuki yükümlülükler yaratmadığı gibi mevcut herhangi bir hukuki yükümlülüğü de zayıflatmamaktadır.¹⁸⁸

Rehber İlkeler uyarınca Devletler, kendi topraklarında ve/veya yargı yetkilerinin olduğu yerlerde, ticari işletmeler dâhil üçüncü kişiler tarafından gerçekleştirilen insan hakları ihlallerine karşı koruma sağlamak¹⁸⁹ ve bu tür ihlallerin gerçekleşmesi halinde, hakları etkilenenlerin etkili telafi edici çözüme erişimlerini sağlamak için yargısal, idari, yasama veya diğer uygun yollarla gerekli adımları atmakla¹⁹⁰ yükümlüdür.

Devletlerin kendi bölgeleri ve yetki sınırları içinde ticari şirketler de dahil olmak üzere üçüncü tarafların insan hakları ihlaline karşı durmak şeklindeki görevi; etkili politikalar, yasalar, yönetmelikler ve hükümler yoluyla, bu ihlallerin önlenmesi, soruşturulması, cezalandırılması ve telafi edilmesi için uygun adımların atılmasını gerektirmektedir. Çözüm yollarına erişimi sağlama görevi ise kendi alanı ve/veya yetki alanı dahilinde iş dünyasıyla ilgili insan hakları ihlalleri gerçekleşen devletin, zarar gören tarafların etkili çözüm yollarına erişimini sağlamak için uygun adımları atmasını gerektirmektedir. Bu çözüm yolları adli, idari, yasal veya diğer uygun yollarla sağlanan çözümleri içermektedir.¹⁹¹

¹⁸⁸ Alex Newton, “Any volunteers? Challenges and opportunities for corporations implementing the responsibility to respect human rights.”, *Australian Journal of Corporate Law*, C. 28, S. 1, 2013, s. 74, doi:10.3316/agispt.20132379.

¹⁸⁹ “BM Guiding Principles”, ilke 1.

¹⁹⁰ “BM Guiding Principles”, ilke 25.

¹⁹¹ “Report of the Special Representative of the Secretary-General on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises, John Ruggie”, para. 25.

Rehber İlkeler’de insan hakları konusunda devletlerin yapması gerekenler yükümlülük olarak ele alınırken, ticari şirketlerin yapması gerekenler sorumluluk kavramı ile ifade edilmiştir. Şirketlerin insan haklarına saygı gösterme sorumluluğu, başkalarının insan haklarını ihlal etmekten kaçınmaları ve katkıda bulundukları olumsuz insan hakları etkilerini ele almaları anlamına gelmektedir. Devletler ile şirketler arasında açıkça bir fark oluşturmayı amaçlayan bu ayrım şirketlere yüklenen ödevin hukuki bir yükümlülük değil de ahlaki bir gereklilik olarak kabul edilmesiyle açıklanabilirse de¹⁹², Rehber İlkeler’de devletlerin yükümlülükleri ele alınırken yeni yasal yükümlülükler yaratılmadığına ilişkin açıklamaya yer verilmesi hususu göz önünde bulundurulduğunda, şirketler yanında devletler bakımından da çekimser bir duruşun tercih edildiğini söylemek mümkündür. Öte yandan, şirketlerle ilgili olarak katı bir yaptırım sistemine şüpheyile bakılması ve çeşitli çalışmalarda şirketlerin davranışlarının iç ve dış sosyal faktörlerin önemine dikkat çekilmesi de şirketler konusundaki bu yaklaşımı desteklemektedir.¹⁹³

Şirketlerin insan haklarına saygı gösterme sorumluluğu tüm ticari şirketleri ve bazıları belirli bağlamlarda daha fazla dikkat gerektirse de uluslararası düzeyde kabul edilmiş tüm insan haklarını kapsamaktadır. Öte yandan, şirketler yalnızca kendi ticari faaliyetleri bakımından değil iş ilişkisi içinde bulundukları şirketlerin faaliyetleri, ürünleri veya hizmetleri ile doğrudan bağlantılı olumsuz insan hakları etkilerini, bu etkilere katkıda bulunmasalar dahi, önlemek ve azaltmak için çaba harcamakla sorumludur.¹⁹⁴

Şirketlerin insan haklarına saygı gösterme sorumluluğu, Rehber İlkeler’in ikinci bölümünde ele alınmaktadır. 11-15. ilkelerde saygı gösterme sorumluluğuna ilişkin temel ilkeler; 16-24. ilkeler ise operasyonel ilkeler olarak sınıflandırılmıştır.

Rehber İlkeler’e göre ticari şirketlerin insan haklarına saygı gösterme sorumluluğunu yerine getirmek için insan haklarını bilmeleri ve bu haklara saygı gösterdiklerini göstermeleri gerekmektedir. Bu da a. insan haklarına saygı gösterme sorumluluklarını yerine getirme taahhüdünü içeren bir politika benimsenmesi; b. insan hakları üzerindeki etkilerini belirlemek, önlemek, azaltmak ve ele almak için durum

¹⁹² Dericiler, *Uluslararası Esnek Hukuktan Bağlayıcı Hukuka*, s. 70.

¹⁹³ Claire Methven O’Brien, Sumithra Dhanarajan, “The Corporate Responsibility to Respect Human Rights: A Status Review”, **National University of Singapore**, C. Working Paper 2015/005, 2015, s. 4, https://law.nus.edu.sg/wp-content/uploads/2020/04/005_2015_Sumi-Dhanarajan.pdf, (10.11.2023).

¹⁹⁴ “BM Guiding Principles”, ilke 13, 14.

değerlendirme süreci işletilmesi ve c. neden oldukları veya katkıda bulundukları olumsuz insan hakları etkilerini gidermek için süreçler oluşturulması da dahil olmak üzere şirketlerin büyüklüklerine ve koşullarına uygun politikalar ve süreçler ile mümkündür.¹⁹⁵

Şirketlerin insan haklarına saygı gösterme sorumluluklarını yerine getirme taahhüdünü içeren politikaları, şirketin olumsuz insan hakları etkilerini tanımlama, önleme, hafifletme ve bunlarla nasıl hesap vereceğini belirlemelidir.¹⁹⁶ Ayrıca, şirketin tüm uluslararası insan hakları standartlarına saygı göstereceğine dair açık bir taahhüt içermelidir. Böylece şirketler yetkili birimler düzeyinde insan haklarına saygı duyacaklarını taahhüt etmiş olacaktır. Bu taahhüt:

- a) Şirketin en üst düzeyinde onaylanmalıdır;
- b) İlgili iç ve/veya dış uzmanlıklarla bilgilendirilmelidir;
- c) Şirketin personel, iş ortakları ve operasyonları, ürünleri veya hizmetleri ile doğrudan bağlantılı diğer taraflardan insan hakları ile ilgili beklentilerini belirtmelidir;
- d) Kamuya açık olmalı ve iç ve dış olarak tüm personele, iş ortaklarına ve diğer ilgili taraflara iletilmelidir;
- e) Şirket genelinde bu politikanın yerleşmesini sağlamak için gerekli operasyonel politika ve prosedürlere yansıtılmalıdır.¹⁹⁷

Saygı gösterme sorumluluğu kapsamında şirketlerin, olumsuz insan hakları etkilerini tespit etmek, önlemek, azaltmak ve nasıl ele alındığını açıklamak için insan hakları ile ilgili durum değerlendirmesi yapmaları gerekmektedir.¹⁹⁸ Durum değerlendirme sürecinin ilk adımı, ticari şirketin yapabileceği mevcut ve potansiyel olumsuz insan hakları etkilerinin yapısını tespit etmek ve değerlendirmektir. Şirketler ayrıca, faaliyetlerinin mevcut ve potansiyel etkilerine ilişkin söz konusu

¹⁹⁵ “BM Guiding Principles”, ilke 15.

¹⁹⁶ “BM Guiding Principles”, ilke 16.

¹⁹⁷ “BM Guiding Principles”, ilke 16.

¹⁹⁸ BM Rehber İlkeler’de, durum değerlendirme sürecini ifade etmek üzere *due diligence* kavramı tercih edilmiştir. Due diligence kavramı, durum değerlendirme sürecinden daha geniş bir sorumluluk ve yükümlülük çerçevesi sunan özen yükümlülüğünü de ifade ettiğinden kavramsal bir karışıklık söz konusudur. Bu karışıklığı ele alan Özge Yücel Dericiler, Rehber ilkelerde kavramın her iki anlama da gelecek şekilde kullanıldığını, sorumluluğun kapsamının somut olaya göre belirlenmesi gerektiği sonucuna ulaşmıştır. Dericiler, *Uluslararası Esnek Hukuktan Bağlayıcı Hukuka*, ss. 101-9.

değerlendirmenin bulgularını şirket politikalarına ve uygulamalarına uyarlamalı¹⁹⁹; şirketin insan hakları üzerindeki olumsuz etkilerini önlemede ne kadar etkili olduğunu takip etmeli²⁰⁰ ve durum değerlendirme süreci ve sonuçları hakkında kamuoyunu aydınlatmalıdır.²⁰¹ İnsan haklarına saygı gösterme konusundaki sorumluluk yalnızca belirli bir yargı alanında yürürlükte olanları değil, uluslararası düzeyde tanınan tüm insan haklarını kapsadığından, insan hakları konusundaki durum değerlendirmesi; asgari olarak, İnsan Hakları Evrensel Beyannamesi'nde sayılan tüm insan haklarına yönelik olmalıdır. Rehber İlkeler'e göre, durum değerlendirmesi:

- a. Şirketin kendi faaliyetleri aracılığıyla neden olabileceği veya katkıda bulunabileceği olumsuz insan hakları etkilerini, ya da iş ilişkileri aracılığıyla doğrudan bağlantılı olabilecek etkileri kapsamalıdır.
- b. Şirketin büyüklüğüne, ağır insan hakları etkileri riskine ve operasyonlarının doğasına ve bağlamına göre değişkenlik gösterecektir.
- c. İnsan hakları riskleri, şirketin operasyonları ve faaliyet bağlamı değiştikçe zamanla değişebileceğinden, sürekli olmalıdır.

Şirketler, durum değerlendirme sürecinde, insan hakları bakımından mevcut ya da potansiyel bir olumsuz etki tespit ettiklerinde, bu etkiyi sonlandırmak veya önlemek için gerekli adımları atmalıdır. Bu sorumluluk, şirketin neden olmamakla birlikte katkıda bulunduğu ya da katkıda bulunma ihtimalinin olduğu durumları da içermektedir. Bu kapsamda atılacak adımlar, şirketin olumsuz etkiyi giderme konusundaki gücünün derecesine göre değişebilecektir.²⁰² Şirketler ayrıca, uygun niteliksel ve niceliksel göstergeler ve geri bildirimlerle attıkları adımların etkililiğini de takip etmelidir.²⁰³

Anlaşılabacağı üzere, insan haklarına saygı gösterme sorumluluğu tamamen ve eşit olarak tüm ticari şirketler için geçerli olmakla birlikte, durum değerlendirme sürecine ilişkin sorumluluklar şirketin büyüklüğüne, ağır insan hakları etkileri riskine ve operasyonlarının doğasına ve bağlamına göre değişmektedir. Bu değişkenlik, 14. ilke de vurgulanmış; şirketlerin sorumluluklarını yerine getirmek için kullanacakları

¹⁹⁹ "BM Guiding Principles", ilke 19.

²⁰⁰ "BM Guiding Principles", ilke 20.

²⁰¹ "BM Guiding Principles", ilke 21.

²⁰² "BM Guiding Principles", ilke 19.

²⁰³ "BM Guiding Principles", ilke 20.

yöntemlerin boyutu ve karmaşıklığının, şirketin olumsuz insan hakları etkilerinin derecesine göre farklılık gösterebileceği kabul edilmiştir. Buna göre, durum değerlendirme sürecinin şirket daha büyükse, insan hakları riski daha fazlaysa veya ek yükümlülükler söz konusuysa daha sıkı bir şekilde uygulanması beklenmektedir. Öte yandan, daha az tartışmalı alanlarda faaliyet gösterebilecek küçük şirketler ya da işletmeler, Rehber İlkeler bakımından daha az sıkı uyum standardına tabidir.²⁰⁴

Bu noktada, internet şirketlerinin sorumluluklarına ilişkin küçük bir parantez açılabilir. BM Rehber İlkeler’de tüm şirketleri kapsayacak şekilde ortaya koyulan bu çerçeveye göre internet şirketleri, en azından insan haklarına saygı göstermekle ve şirketler için öngörülen somut adımları atmakla sorumludur.²⁰⁵ Bu sorumluluk öncelikle, internet şirketlerinin insan hakları ihlallerine ilişkin olarak bir politika taahhüdünde bulunmalarını ve faaliyetlerinin insan hakları üzerindeki etkilerini değerlendirmelerini gerektirmektedir. Örneğin, internet şirketleri tarafından hazırlanan hizmet koşulları bu kapsamda değerlendirilebilir. Kamuya açık olarak internet sitelerinde yer alması gereken bu metinlerde, internet şirketleri, hukuka aykırı içerikle ilgili politikalarını ve bu politikalar uyarınca alınabilecek kararları açıklamalıdır. Öte yandan, internet şirketleri, özellikle suç teşkil eden içeriklerle mücadele, veri gizliliğinin sağlanması, suç işlenmesinin önlenmesi ya da çocukların korunması gibi konulara ilişkin riskleri sürekli olarak değerlendirmeli ve bu riskleri azaltmaya yönelik tedbirler almalıdır.

Durum değerlendirme süreci, şeffaflık ve hesap verebilirlik ilkelerinin de gereği olarak, faaliyetleri olumsuz etkilere yol açan şirketlerin bu etkileri ele alma biçimlerine ilişkin olarak kamuoyunu aydınlatmalarını da gerektirmektedir. Bu sorumluluk, yüz yüze toplantılar, internet üzerinden görüşmeler, etkilenen paydaşlarla istişareler ve kamuya açık resmî raporlar da dâhil olmak üzere, çeşitli şekillerde yerine getirilebilir; ancak her halükârda uygun formatta ve sıklıkta, hedef kitlenin erişebileceği biçimde olmalıdır.²⁰⁶

²⁰⁴ Robert C. Blitt, “Beyond Ruggie’s Guiding Principles on Business and Human Rights: Charting an Embrasive Approach to Corporate Human Rights Compliance”, *Texas International Law Journal*, C. 48, S. 1, 2012, s. 48.

²⁰⁵ Birleşmiş Milletler tarafından ortaya koyulan bu prensiplerin internet şirketleri üzerindeki etkisi bu konudaki çalışmaların olduğu ilgili başlıklarda ele alınacağından burada genel olarak belirtilmekle yetinilmiştir.

²⁰⁶ “BM Guiding Principles”, ilke 21.

Son olarak, insan hakları ihlallerine neden olmaları ya da katkıda bulundukları durumlarda şirketler, bu olumsuz etkiyi azaltacak ya da ortadan kaldıracak telafi edici mekanizmalar başlatmakla sorumludur.²⁰⁷ Bununla birlikte internet şirketlerinin insan haklarına ilişkin sorumluluk alanı, yerine getirilen işlevin kamu işlevi olduğu hususu dikkate alındığında, diğer iş sektörlerine göre daha geniştir.²⁰⁸ Örneğin, çevrimiçi hizmet sağlayıcıları söz konusu olduğunda ek bir sorumluluk katmanı bulunmaktadır. Bu ihtimalde şirketin sorumluluğu sadece çalışanları ve toplulukla sınırlı olmayıp aynı zamanda doğrudan veya dolaylı olarak milyarlarca insanı da kapsamaktadır.²⁰⁹

Rehber İlkeler’de iş dünyası ve insan haklarına ilişkin olarak ortaya koyulan üçüncü temel prensip, telafi edici, çözüm mekanizmalarına erişim gerekliliğidir. Rehber İlkeler’de bu kapsamda hem devlete hem de ticari şirketlere yönelik ilkelere yer verilmiştir.²¹⁰

Buna göre devletler, iş bağlantılı insan hakları ihlaline karşı koruma görevinin bir parçası olarak, kendi bölgelerinde ve/veya yetki alanlarında bu tür ihlaller gerçekleştiğinde ve adli, idari, yasal ve diğer uygun araçları kullanarak, etkilenenlerin etkili çözümlere erişimini sağlamak için gerekli adımları atmak zorundadır. Rehber İlkeler’de bu mekanizmalar şu üç başlıkta ele alınmıştır: a) Devlet temelli yargısal mekanizmalar²¹¹, b) Devlet temelli yargı-dışı şikâyet mekanizmaları²¹², c) Devlet temelli olmayan şikâyet mekanizmaları.²¹³

Yargısal mekanizmalar, şirketlerden kaynaklanabilecek insan hakları müdahalelerine karşı telafi edici çözümlerin merkezinde yer almaktadır. Bu nedenle devletler, yargısal mekanizmalara başvurulmasını engelleyecek adımlardan kaçınmalı, mahkemelerin Devlet kurumlarından veya iş aktörlerinden gelecek ekonomik ve siyasi baskılardan bağımsız olmasını ve insan hakları savunucularının meşru ve barışçıl faaliyetlerinin engellenmemesini sağlamalıdır. Bununla birlikte, yargısal mekanizmaların

²⁰⁷ “BM Guiding Principles”, ilke 22.

²⁰⁸ “Report of the Special Representative of the Secretary-General on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises, John Ruggie”, s. 9.

²⁰⁹ Jørgensen, “Human Rights and Private Actors in the Online Domain”, s. 259.

²¹⁰ “BM Guiding Principles”, ilke 25-31.

²¹¹ “BM Guiding Principles”, ilke 26.

²¹² “BM Guiding Principles”, ilke 27.

²¹³ “BM Guiding Principles”, ilke 28.

gerekli ya da etkili olmadığı durumlarda yargı-dışı mekanizmalar da yargısal mekanizmaların tamamlanması ve eksiklerinin giderilmesi bakımından önem taşımaktadır. Rehber İlkeler’de, ulusal insan hakları kuruluşlarının bu açıdan önemli bir rolü olduğuna dikkat çekilmiştir.²¹⁴

Son olarak, devletler iş bağlantılı insan hakları zararları ile ilgilenen Devlet temelli olmayan şikâyet mekanizmalarına erişimi kolaylaştırmanın da yollarını aramalıdır. Devletler, kendilerinin sağladıkları mekanizmalar dışında ticari şirketler tarafından tek başına veya paydaşlarla birlikte yürütülen, bir sanayi derneği veya çok paydaşlı gruplar tarafından yürütülen mekanizmalar ya da bölgesel ve uluslararası insan hakları kuruluşları gibi alternatif çözüm mekanizmalarının geliştirilmesinde rol oynayabilirler ki bu mekanizmalar, erişim ve çözüm hızı, daha az masraf ve/veya ulus aşırı erişilebilirlik gibi avantajlar da sağlayabilir.²¹⁵

Öte yandan ticari şirketler, şikâyetlere erken safhada müdahale edilmesini ve doğrudan çözüm üretilmesini mümkün kılmak adına, ilgili ticari faaliyetlerden olumsuz yönde etkilenebilecek bireyler ve topluluklar için doğrudan erişilebilir nitelikte ve operasyonel düzeyde şikâyet mekanizmaları kurmalı veya bu mekanizmalara katılmalıdır. Bu şikâyet mekanizmaları, ticari şirketlerin insan haklarına saygı gösterme sorumluluğu açısından iki önemli görevi yerine getirmektedir. Bunlardan ilki, şirketin devam eden insan hakları durum değerlendirmelerinin bir parçası olarak, olumsuz insan hakları etkilerinin tespit edilmesine katkı sağlarlar. Bunu, şirketin faaliyetlerinden doğrudan etkilenenlerin olumsuz yönde etkilendiklerine veya etkileneceklerine inandıklarında, kaygılarını dile getirmeleri için bir kanal açarak yaparlar. Ticari şirketler, böylece şikâyetlerdeki eğilimleri ve örüntüleri analiz ederek, sistematik sorunları da tespit edebilir ve uygulamalarını bu doğrultuda uyarlayabilirler. İkinci olarak bu mekanizmalar, şikâyetlerin tespit edilmesinin ardından, ticari şirketler tarafından bunlara müdahale edilmesine ve olumsuz etkilerin erken safhada çözülmesine, dolayısıyla da zararların çoğalmasının ve şikâyetlerin büyümesinin önlenmesine de olanak sağlamaktadır.²¹⁶

²¹⁴ “BM Guiding Principles”, ilke 27.

²¹⁵ “BM Guiding Principles”, ilke 23-24.

²¹⁶ “BM Guiding Principles”, ilke 29.

Rehber İlkeler’de, devlet temelli olup olmadığına bakılmaksızın, yargı-dışı şikâyet mekanizmaları ile ilgili olarak, bu mekanizmaların etkililiğine ilişkin bazı kriterler belirlenmiştir. Bu kriterler, yargı-dışı şikâyet mekanizmaları ile ilgili önemli bir çerçeve sunmaktadır. Buna göre söz konusu mekanizmalar; kullanması hedeflenen tüm paydaş gruplarda güven uyandırmalı ve şikâyet süreçlerinin doğru uygulanması ile ilgili olarak hesap verebilir olmalı; mekanizmaları kullanması hedeflenen tüm paydaş gruplar tarafından bilinir olmalı ve belirli erişim engelleri ile karşılaşan kişilere gerekli desteği sağlamalı; her bir aşama için belirlenen süreleri açıklayarak, açık ve belli süreçleri ortaya koymalı ve süreç türleri, elde edilecek sonuçlar ve uygulamayı izleme yolları ile ilgili olarak net olmalı; mağdur taraflara, şikâyet sürecine makul, bilinçli ve saygılı bir şekilde girmeleri için gerekli olan bilgi, görüş ve uzmanlık kaynaklarına makul ölçülerde erişim imkanı sağlamanın yollarını bulmalı ve son olarak etkililiği ile ilgili güven oluşturmak ve tehlike altındaki kamu yararını gözetmek için şikâyetle bulunan tarafları, süreçle ilgili bilgilendirmeli ve mekanizmanın işleyişi hakkında yeterli bilgi paylaşımı yapmalıdır.²¹⁷

3. Özel Sektörün Çocuk Hakları Üzerindeki Etkileri Konusunda Devletin Yükümlülüklerine Dair Genel Yorum 16

BM İnsan Hakları Konseyi’nin 2011’de Rehber İlkeleri kabul etmesi üzerine Çocuk Hakları Komitesi, bu ilkeleri çocuk hakları açısından ele almayı amaçlayan bir çalışma başlatmıştır. Bu doğrultuda, 2013 yılında devletlerin, çocuk haklarını korumak adına şirketleri etkili bir şekilde düzenleme yükümlülüklerine odaklanan Genel Yorum 16 kabul edilmiştir.²¹⁸

Birleşmiş Milletler Çocuk Hakları Komitesi, ticari faaliyetlerin ve işlemlerin çocuk hakları yaklaşımıyla uyumlu olması açısından Devlet tarafından alınacak tüm kararların ve gerçekleştirilecek girişimlerin temeli olarak Sözleşme çerçevesinde dört genel ilke ortaya koymuştur. Bu ilkeler a) ayrımcılığa maruz kalmama, b) çocuğun üstün yararı, c) yaşama, hayatta kalma ve gelişme hakkı ve d) katılım hakkıdır.²¹⁹

²¹⁷ “BM Guiding Principles”, ilke 31.

²¹⁸ “General Comment No. 16 on State obligations regarding the impact of the business sector on children’s rights (CRC/C/GC/16)”, United Nations, 2013, <https://www2.ohchr.org/english/bodies/crc/docs/crc.c.gc.16.pdf>, (9.10.2024).

²¹⁹ General Comment No. 16, para. 12.

Ayrımcılığa maruz kalmama ilkesi devletlerin, iş yaşamıyla ilgili her tür yasal düzenlemenin, politikaların ve programların kasıtlı ya da kasıtsız olarak içerik ya da uygulama açısından çocuklara yönelik ayrımcılık yapmamasının sağlanmasını gerektirmektedir.²²⁰ Çocuğun üstün yararı ilkesi ise çocuklar üzerinde doğrudan ya da dolaylı etkisi olan ticari faaliyet ve işlemlere ilişkin her tür yasal, idari ve yargısal işlemde bu ilkeyi içselleştirip uygulama yükümlülüğünü ifade etmektedir.²²¹ Üçüncü ilke olan yaşama, hayatta kalma ve gelişme hakkı, ticari faaliyetlerin çocuğun fiziksel, zihinsel, manevi, ahlaki, psikolojik ve sosyal gelişimini kapsayan bütünsel gelişimi üzerindeki etkilerinin değerlendirilmesini ve bu konuda gerekli önlemlerin alınmasını gerektirmektedir.²²² Son olarak katılım hakkı da her çocuğun kendisini etkileyecek konularda görüşlerini serbestçe dile getirme ve çocuğu etkileyen herhangi bir adli veya idari kovuşturmada çocuğun ya doğrudan doğruya veya bir temsilci ya da uygun bir makam yoluyla dinlenmesini öngörmektedir.²²³

Buna göre, Devletler, şirketlerin çocuk haklarına zarar vermesini veya ihlallere katkıda bulunmasını önlemek için gerekli, uygun ve makul tüm önlemleri almakla yükümlüdür. Bu önlemler, şirketlerin çocuk haklarına etkisini belirleyen yasa ve düzenlemelerin çıkarılması, izlenmesi ve uygulanması ile ilgili politikaları içerebilecektir. Devletler, şirketlerin neden olduğu veya katkıda bulunduğu çocuk hakları ihlallerini soruşturmalı, yargılamalı ve telafi etmelidir. Dolayısıyla, bir devlet, işletmelerin neden olduğu çocuk hakları ihlalleri karşısında gerekli, uygun ve makul önlemleri almadığında ya da bu ihlalleri tolere ettiğinde veya iş birliği yaptığında, bu ihlallerden sorumlu kabul edilecektir.²²⁴

Genel Yorum 16 uyarınca Devletler, işletmelerin çocuk haklarına saygı göstermelerini sağlamak amacıyla çocuk haklarına yönelik özen yükümlülüğüne uygun hareket etmelidir. Bu yükümlülük, şirketlerin kendi faaliyetlerinin ve iş ilişkilerinin çocuk hakları üzerindeki etkilerini değerlendirme, önleme ya da azaltma sorumluluklarını güvence altına almaktadır. Özellikle, şirketlerin faaliyetleri veya faaliyet gösterdikleri sektör dolayısıyla çocuk hakları ihlalleri açısından yüksek riskin söz konusu olduğu

²²⁰ General Comment No. 16, para. 13, 14.

²²¹ General Comment No. 16, para. 15-17.

²²² General Comment No. 16, para. 18-20.

²²³ General Comment No. 16, para. 21-23.

²²⁴ General Comment No. 16, para. 28.

durumlarda, devletlerin daha katı bir özen süreci ve etkin bir izleme sistemi talep etmeleri gerekmektedir.²²⁵ Özen yükümlülüğü kapsamında ayrıca, büyük işletmelerin, çocuk haklarına yönelik etkilerini azaltmak adına uyguladıkları önlemleri kamuoyuna açıklamaları teşvik edilmeli, bazı durumlarda ise bu şeffaflık yükümlülüğü zorunlu hale getirilmelidir. Bu raporların, işletmeler arasında karşılaştırılabilir ve erişilebilir nitelikte olması sağlanarak, işletmelerin çocuklar üzerinde olumsuz etki yaratabilecek durumları önlemek için attıkları adımları içermesi gereklidir.²²⁶

Genel Yorum'da internet ve internetin çocuklar üzerindeki etkisine özel olarak dikkat çekilmiş; çocukların internet kullanırken siber zorbalık, ticaret ya da cinsel istismar ve sömürü gibi durumlara maruz kalabileceği gerekçesiyle dijital medyanın özellikle kaygı yarattığı belirtilmiştir. Bu bakımdan, çocukların internet ortamında karşılaşabilecekleri riskleri anlamaları ve bu durumlarla başa çıkabilmeleri için yaşlarına uygun güvenlik bilgisi sunulması gerekmektedir. Devletler, çocukları şiddet ve uygunsuz içeriklerden korumak amacıyla bilgi ve iletişim teknolojisi sektörünün uygun koruyucu önlemleri geliştirmesi ve uygulaması için sektörle iş birliği içinde olmalıdır.²²⁷

Her ne kadar Genel Yorum'da bütün bu ilkelerin gerçekleştirilmesi bakımından yükümlülük devletlere atfedilse de devletlerin koruma yükümlülüğü kapsamında ele alınan hususlar şirketlerin de saygı gösterme sorumluluğunun bir gereğidir. Nitekim, Genel Yorum'da da devletlerin, ticari kuruluşların çocuk haklarına saygı göstermelerini sağlayacak önlemleri alma yükümlülüklerini yerine getirmek için bu kuruluşlardan çocuk hakları etki değerlendirmesi yapmalarını istemeleri; ihlal risklerinin yüksek olduğu durumlarda ise etki değerlendirmesinin daha titiz ve ayrıntılı yapılmasını ve etkili bir izleme sistemi getirilmesini talep etmeleri gerektiği belirtilerek²²⁸ şirketlerin saygı duyma yükümlülüğünün de gerekleri ortaya koyulmuştur.

B. Özel Olarak İnternet Şirketlerinin İnsan Hakları Sorumlulukları

Birleşmiş Milletler sisteminde, şirketlerin insan hakları genel olarak ortaya koyulmakla birlikte, özel olarak internet şirketlerinin sorumluluklarına ilişkin bir çerçeveye

²²⁵ General Comment No. 16, para. 62.

²²⁶ General Comment No. 16, para. 65.

²²⁷ General Comment No. 16, para. 60.

²²⁸ General Comment No. 16, para. 62.

çizilmemiş, belirli sektörlerde insan haklarına yönelik daha ciddi riskler söz konusu olabileceği ve insan haklarına saygı gösterme sorumluluğunun çeşitli kriterlere göre daralıp genişleyebileceği belirtilmiştir. Söz konusu sorumluluk alanını belirleyen kriterlerden biri de şirketlerin olumsuz insan hakları etkilerinin derecesidir. Kural olarak şirketlerin büyüklüklerinin de bu sorumluluk alanında belirleyici olabileceği kabul edilmekle birlikte, insan haklarına etki derecelerine bağlı olarak bazı küçük ya da orta ölçekli şirketlerin de daha geniş önlemler alması gerekebilmektedir.

Bilgi ve iletişim teknolojileri sektörü faaliyetleri özellikle ifade özgürlüğü ve bu özgürlükle bağlantılı haklar ile mahremiyet/özel hayata saygı haklarını etkilemektedir. Nitekim internet şirketleri kendilerini tanımlarken ifade özgürlüğüne özellikle dikkat çekmektedir. Örneğin Google, şirketin tüm işlerinde “*insanların ifade özgürlüğü lehine bir önyargıya sahip olduğunu*” vurgulamaktadır.²²⁹ Facebook'un kurucusu Mark Zuckerberg de şirketin halka arz edilmesi sürecindeki bir açıklamasında, Facebook'un bir şirket olarak tasarlanmadığını belirttikten sonra platformun asıl amacına ilişkin olarak bireylere kazandırdıkları paylaşma gücü ile tahmin edilenden çok daha fazla sayıda insanın sesini duyurabilmesine imkan sağladığını ve bunun da hükümetleri doğrudan tüm insanların dile getirdiği konulara ve endişelere daha duyarlı hale getirmesini beklediklerini ifade etmiştir.²³⁰ Benzer şekilde Twitter da varlık nedeninin insanların özgür şekilde fikirlerini yayabilmesi olarak belirtmektedir.

Çalışmanın bu bölümünde, BM sisteminde, dijital ortamda internet şirketlerinin insan hakları yükümlülüklerine ilişkin gelişmelere odaklanılmaktadır. Bu gelişmeler, söz konusu şirketlerin faaliyetlerinin ağırlıklı olarak etkiledikleri ifade özgürlüğü (1) ve özel hayatın korunması hakkı (2) ile bağlantılı olarak ele alınacaktır.

1. İfade Özgürlüğü Bakımından Özel Sektöre Uygulanabilir İlkeler

Bilişim teknolojilerindeki gelişmeler, BM sisteminde özel sektör ile ifade özgürlüğü ilişkisini ele alan bir dizi çalışmayı beraberinde getirmiştir.

²²⁹ Jørgensen, “Human Rights and Private Actors in the Online Domain”, s. 262.

²³⁰ Facebook's Letter from Mark Zuckerberg, Full Text, **The Guardian**, (01.02.2012), Technology, <https://www.theguardian.com/technology/2012/feb/01/facebook-letter-mark-zuckerberg-text>, (1.05.2021).

İnsan Hakları Konseyi'nin 'İnternette İnsan Haklarının Geliştirilmesi, Korunması ve Kullanılması' başlıklı Kararı²³¹, bu kapsamda atılmış ilk adımlardan biri olarak kabul edilmektedir. Bu Karar ile, çevrim dışı hakların çevrim içi ortamda da korunması gerektiğini vurgulanmış; Devletlere, internete erişimi teşvik etme, kolaylaştırma ve bilgi ve iletişim olanaklarının geliştirilmesine yönelik uluslararası iş birliğini artırma çağrısında bulunulmuştur. Bu karar insan haklarının, özellikle de ifade özgürlüğünün sadece fiziksel dünyada değil dijital dünyada da yeri olduğunu teyit eden ilk BM kararı olması bakımından önemlidir. Bununla birlikte Karar, internet şirketlerine ilişkin özel bir değerlendirme içermemektedir.

Dijital gelişmelerin ifade özgürlüğüne etkileri ve bununla bağlantılı olarak özel aktörlerin rollerine ilişkin esaslı konular, BM Düşünce ve İfade Özgürlüğü Özel Raportörü David Kaye'nin 2016 yılındaki çalışmalarıyla kapsamlı olarak ele alınmıştır. Kaye, birinde ifade özgürlüğüne yönelik güncel zorlukları, diğerinde ise dijital çağda ifade özgürlüğü, devletler ve özel sektör ilişkisini ele aldığı iki rapor yayınlamıştır. İlkinde, ulusal güvenlik ve nefret söylemi gibi kavramlara getirilen geniş tanımlamaların devletlere ifade özgürlüğünün sınırlandırılması konusunda geniş bir takdir yetkisi sağladığına dikkat çekilmiştir.²³²

İkincisinde ise, ifade özgürlüğünde yönelik endişeler bağlamında devletler yanında özel sektör aktörleri de dikkate alınmış ve özel sektöre uygulanabilir ilkeler incelenmiştir.²³³

Kaye, Medeni ve Siyasi Haklar Sözleşmesi'nin 19. maddesinin üçüncü fıkrasına göre ifade özgürlüğüne yönelik bir sınırlama ancak sınırlamanın kanuna dayanması ve başkalarının haklarına veya itibarına saygı gösterilmesi veya ulusal güvenliğin veya kamu düzeninin veya kamu sağlığının veya ahlakın korunması için gerekli olması halinde hukuka uygun kabul edilebildiğini hatırlatarak bu kriterleri açıklamıştır. Buna göre, Gerekliklik kriteri bir sınırlamanın yararlı, makul, arzu edilir olmanın ötesine geçmesi ve

²³¹ "The promotion, protection and enjoyment of human rights on the Internet", United Nations, 2012.

²³² Promotion and protection of the right to freedom of opinion and expression (A/71/373), United Nations, 09.09.2016, <https://documents.un.org/doc/undoc/gen/n16/278/27/pdf/n1627827.pdf>, (1.5.2021).

²³³ Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (A/HRC/32/38), United Nations, 2016, <https://digitallibrary.un.org/record/842541>, (1.5.2021).

aynı zamanda bir orantılılık değerlendirmesini de kapsamasını gerekmektedir. İfade özgürlüğünün bu güvencelerin sağlanması, devletlerin hem ihlal etmekten kaçınmaya yönelik negatif yükümlülüklerini hem de bu hakların kullanılmasını sağlamaya yönelik pozitif yükümlülüklerini gündeme getirmektedir. Bu pozitif yükümlülükler, kamu makamlarının bireyleri özel kişilerin eylemlerinden korumak için adımlar atmasını gerektirebilir.²³⁴

Bununla birlikte Rapor'da, BM Rehber İlkelerin bilgi ve iletişim teknolojileri sektöründe faaliyet gösteren şirketlerin insan hakları sorumlulukları konusunda devletlerin yükümlülüklerinden bağımsız olarak küresel bir çerçeve sunduğuna da dikkat çekilmiştir. Buna göre, şirketler kendi faaliyetleri yoluyla olumsuz insan hakları etkilerine neden olmak veya katkıda bulunmaktan kaçınmalı, bu tür etkiler ortaya çıktığında durum değerlendirmesinde bulunmalı ve bu etkilere katkıda bulunmuş olmasalar da faaliyetleri, ürün ya da hizmetleriyle doğrudan bağlantılı etkiler ortaya çıktığında bu etkileri önlemeli veya azaltmalıdır.²³⁵

Kaye, BM Rehber İlkeler'de sunulan bu çerçeveyi dijital gelişmeler bağlamında değerlendirmiştir. Dijital ortamda, devletin içeriği kısıtlama veya kullanıcıların bilgilerine erişim taleplerine nasıl yanıt verileceğine ilişkin şirket içi kararlarda, hizmet şartlarının kabul edilmesinde, güvenlik ve mahremiyeti etkileyen tasarım ve mühendislik seçimlerinde ve belirli bir pazarda hizmet sağlama veya sonlandırma kararlarında insan haklarına ilişkin durum değerlendirmesi süreçleri ortaya çıkabilecektir. Kaye, Rehber İlkelerde öngörülen şeffaflık ve telafi edici çözüm yollarının sağlanmasına ilişkin sorumlulukları da bilgi ve iletişim teknoloji alanında faaliyet gösteren özel aktörlerle bağlantılı olarak ele almıştır.²³⁶

²³⁴ Ibid., para. 7, 8; General Comment No. 31 (2004) On the nature of the general legal obligation imposed on States Parties to the international covenant on civil and political rights, CCPR/C/21/Rev.1/Add. 13, 26 May 2004. Genel yorumda, Sözleşmedeki tüm haklar bakımından devletlerin bireyleri özel kişilerin ihlallerine karşı koruma yükümlülüğü kabul edilmekle birlikte, Sözleşme'nin bazı maddelerinde, pozitif yükümlülükler yükleyen belirli alanlar ayrıca düzenlenmektedir. Örneğin, 17. maddede yer alan özel hayatın gizliliği ile ilgili güvenceler hukuken koruma altına alınmalıdır. Benzer şekilde, 26. maddede de iş hayatı ya da konut edinme gibi gündelik hayatın temel konularında bireyler ayrımcılığa karşı korunmalıdır.

²³⁵ "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression", para. 10.

²³⁶ "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression", para 11.

Raporda, özel aktörlerin de içerisinde olduğu çok aktörlü bilgi ve iletişim sektörünün güncel sorunları tespit edilmiştir. Bu kapsamda, içerik düzenlemesi, gözetim ve dijital güvenlik, şeffaflık sorunları ele alınmış ve çözüm önerilerine yer verilmiştir.

Kaye, içerik düzenlemesine ilişkin olarak, devletlerin özel aktörler aracılığıyla internet içeriğine müdahalesi ve özel aktörlerin kamusal taleplere ne şekilde karşılık verdiği gibi çok sayıda soruna odaklanmıştır. İnternet ortamında oluşturulan ve barındırılan içeriklerin kapsamı her geçen gün artmaktadır. Blog yazıları, metin mesajları, fotoğraflar, videolar, sosyal medya paylaşımları gibi içerikler bu geniş ekosistemdeki içeriklerden yalnızca bir kaçıdır. Bu ekosistemin genişlemesiyle bağlantılı olarak söz konusu içerikler, gittikçe artan şekilde hem devlet hem de özel aktörlerin düzenlemelerine konu olmaktadır.²³⁷

İnternet içeriğinin düzenlenmesi, genellikle içerik düzenlemesi, özellikle karalama, küfür, taciz veya nefret söylemi, kışkırtma, fikri mülkiyet, müstehcenlik ve ahlaksızlık, terörizmin teşviki ya da övülmesi, ulusal güvenlik ve kamu güvenliği, çocukların korunması ve cinsiyete dayalı şiddetin önlenmesi gibi gerekçelere dayanmaktadır. Dijital gelişmelerle birlikte son zamanlarda, unutulma hakkı ve çoğulculuk ve çeşitlilik (örneğin, ağ tarafsızlığı) gibi sebepler de içerik düzenlenmesiyle bağlantılı olarak gündeme gelmiştir.²³⁸ Bu konuların neredeyse tamamında, içerik düzenleme, ifade özgürlüğü ile diğer haklar arasında denge kurulmasını da gerektiren bir faaliyete dönüşmektedir. Kaye, içerik düzenlemesine ilişkin bu faaliyetlerin büyük ölçüde şirketlerin politika ve kararlarıyla belirlendiğine dikkat çekmiştir.²³⁹

Raporda, hizmet şartları ya da topluluk kuralları, hangi içeriklerin yasaklandığına dair belirsiz ifadelerle yer verilmesi, kuralların uygulanmasındaki tutarsızlıklar ve içeriğin kaldırılması ya da hesabın kapatılmasına ilişkin itiraz mekanizmalarının olmaması gibi sebeplerle eleştirilmiştir.²⁴⁰ Bununla birlikte, platformların güncel kurallarında müdahale

²³⁷ “Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression”, para. 35-36.

²³⁸ “Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression”, para. 37.

²³⁹ “Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression”, para. 51.

²⁴⁰ “Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression”, para. 52.

edilen içerikler ya da kullanıcı hesapları bakımından itiraz mekanizmalarına yer verildiği ve kısıtlanan içeriklerin daha ayrıntılı olarak ele alındığı görülmektedir. Örneğin güncel topluluk kurallarında, *kamu yararı istisnaları* şeklinde ayrı bir kategori belirlenmiştir. Kamu yararı istisnaları, kural olarak topluluk standartlarına aykırı olmakla birlikte, kamu yararı değeri ile zarar riski kıyaslandığında kamu yararı niteliği ağır bastığı için izin verilen içerikler olarak tanımlanabilir. Twitter bu kategorideki içerikleri; kuralın ihlal edildiği, bununla birlikte yine de erişilebilir olmasına karar verildiği bilgisini içeren bir bildirimin arkasına yerleştirerek yayınlamaktadır.²⁴¹ Şirket kurallarındaki bu güncellemeler, içeriğe müdahale konusunda daha güvenceli bir sistem sağlasa da bu konuda artan talepler yeni sorunları da beraberinde getirmektedir. Çok çeşitli pazarlarda faaliyet gösteren araçlar, kaçınılmaz olarak "karmaşık değer yargıları", “kültürel hassasiyet ve çeşitlilik içeren sorunlar” ve "hukuk ihtilafı konusunda zor kararlar" ile karşı karşıya kalmaktadır.²⁴²

İnternet şirketlerinin içeriğe müdahalesi, sunulan hizmetin ve içeriklerin niteliğine bağlı olarak farklı şekillerde ortaya çıkabilir. İnternet servis sağlayıcıları, belirli anahtar kelimelere, web sayfalarına veya tüm web sitelerine erişimi engelleyebilir; alan adı kayıt şirketleri, devletlerin kara listesinde yer alan kişilerin taleplerini reddedebilir; sosyal medya şirketleri paylaşımları kaldırabilir veya hesapları askıya alabilir; arama motorları, yasa dışı içeriğe bağlantı veren arama sonuçlarını kaldırabilir. Bu müdahaleler meşru taleplere dayanabileceği gibi müdahalenin gerekçesi ve uygulanan yöntemin yasal veya korunan ifadenin kaldırılmasına da yol açma riskine bağlı olarak gereklilik ve orantılılık endişeleri ortaya çıkarabilmektedir.²⁴³

İnternet şirketlerinin içerik düzenlemeleri, ulusal düzenlemelerden ya da şirketlerin iç politika ve uygulamalarından kaynaklanabilir.²⁴⁴ Ulusal düzenlemeler bakımından internet şirketleri, tercih edilen rejimin türüne göre değişmekle birlikte, üçüncü kişilerin ya da devletlerin talepleri üzerine ve/veya herhangi bir yaptırımla karşı

²⁴¹ <https://help.twitter.com/en/rules-and-policies/public-interest>, (2.4.2021)

²⁴² “Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression”, para. 54.

²⁴³ “Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression”, para. 46.

²⁴⁴ Devlet düzenlemeleri aynı zamanda şirketlerin iç politika ve uygulamalarının hazırlanmasında ve bunların kapsamlarının belirlenmesinde de etkili olabilmektedir. Ancak yine de bu durumda müdahalenin kaynağı, devlet düzenlemeleri değil şirket içi kurallar olmaktadır.

karşıya kalmamak için bir talep olmaksızın içeriğe müdahale edebilirler. Bu talep bir yargı kararına dayanabileceği gibi yargı kararı olmaksızın da söz konusu olabilmektedir. Örneğin Avrupa Birliği Adalet Divanı'nın, *Google İspanya v. Mario Costeja González* davası²⁴⁵ sonrasında kurulan mekanizma ile “unutulma hakkı” başvurusu alan şirketler bu başvuruyu değerlendirerek içeriğe müdahale edip etmeme konusunda karar vermektedir.

Şirketlerin bir talep olmadan içeriğe müdahaleleri ise faaliyet izinlerinin bir gereği olarak ya da çalışanlarının güvenliğini tehlikeye atmamak veya yerel erişim engelleriyle karşılaşmamak gibi sebeplerle ihtiyatlı olmaya zorlanmalarından kaynaklanmaktadır.²⁴⁶ Bu kapsamda özellikle belirsiz yasal düzenlemeler, bu ihtiyatlılığı insan hakları aleyhine genişletebilmekte, bu da şirketlerin karar süreçlerinin insan hakları hukuku ile uyumlu olmayan şekilde sürdürülmesine yol açabilmektedir. Örneğin, Çin Halk Cumhuriyeti Siber Güvenlik Yasası'nın 12. maddesine göre kişi ve kuruluşlar, interneti kullanırken “kamu düzenini gözetmeli”, “interneti ulusal güvenliği, ulusal onuru ve ulusal çıkarları tehlikeye atacak faaliyetlerde bulunmak için kullanmamalı” ve “ekonomik veya sosyal düzeni bozmaya yönelik yanlış bilgiler oluşturmamalıdır.”²⁴⁷ Benzer şekilde, Nijerya'da hazırlanan yasa tasarısında “*herhangi bir ortamda*” herhangi bir kişi, grup veya hükümet kurumu hakkında “*kötü niyetle iftira atmak veya halkı aleyhlerine kışkırtmak amacıyla*” beyanda bulunmak yasaklanmaktadır.²⁴⁸

Diğer yandan, tasarım ve mühendislik tercihleri de şirketlerin içeriklere müdahalesine neden olabilmektedir. Platformların içeriği düzenleme, sınıflandırma ve sıralama biçimleri kullanıcıların kendi platformlarında hangi bilgilere erişip görüntülediklerini etkilemektedir. Örneğin platformlar, kullanıcı tercihlerinin algoritmik tahminlerini kullanır ve sonuç olarak bireylerin görebileceği reklamlara, sosyal medya

²⁴⁵ Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, Case C-131/12 (ECJ 13 Mayıs 2014).

²⁴⁶ İnternet şirketlerinin bu talepler karşısındaki yaklaşımı, bazı durumlarda devletler tarafından alınacak kararları da etkileyebilmektedir. Bu durum, özellikle bazı ülkelerde internetin tamamen kapatılması (shutdown) şeklinde, orantılılık ilkesi bakımından sorun oluşturabilecek uygulamaları beraberinde getirebilmektedir. “Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression”, para. 44.

“Translation: Cybersecurity Law of the People’s Republic of China (Effective June 1, 2017)”, **DigiChina**, (23.10.2024), <https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/> (2.10.2021).

²⁴⁸ “Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression”, para. 39.

beslemelerinin²⁴⁹ nasıl düzenlendiğine ve arama sonuçlarının görünme sırasına rehberlik etmektedir. Bu bakımdan, Kaye, özel kuruluşların platformlarını istedikleri gibi tasarlama ve kişiselleştirme özgürlükleri karşısında, tasarım ve mühendislik seçimlerinden kaynaklanan söz konusu etkilerin ifade özgürlüğü bakımından endişelere yol açtığını ifade etmiştir.²⁵⁰

Platformlara erişim sağlamak için kullanıcıların kabul etmesi gereken hizmet şartları ya da topluluk kuralları genellikle paylaşılabilecek içeriklere ilişkin kısıtlamalar içermektedir. Örneğin, hem Twitter Kurallarında hem de Facebook Topluluk Standartları'nda şiddet ya da küfür içeren ifadeler, çocukların cinsel istismarı, cinsel şiddet içeren paylaşımlar, intihara teşvik, başkalarının özel bilgileri, fikri mülkiyete konu içerikler gibi içeriklerin paylaşılması yasaklanmıştır.²⁵¹ Son zamanlarda, şirket politikalarında dezenformasyon ya da yanlış bilgilendirmenin önlenmesine yönelik kurallara da yer verilmekte, doğruluğu ve bütünlüğü zedelediğine karar verilen "yalan haberler" ve çeşitli aldatıcı uygulamalara yönelik olarak da içeriğe müdahale edilebilmektedir. Bu müdahale içeriğe yönelik etiketlerin uygulanması ya da uyarı verilmesinden içeriğin kaldırılması veya kullanıcı hesaplarının kapatılmasına kadar uzanabilmektedir.

Örneğin, Facebook yanıltıcı bilgilerin tespiti bakımından üçüncü taraf doğrulama programı kurmuştur.²⁵² Twitter da yakın bir zamanda, yanlış bilgilendirmeye karşı topluluk temelli bir yaklaşımı duyurmuştur.²⁵³ Sosyal medya platformlarının ötesinde, WhatsApp gibi mesajlaşma servisleri de kullanıcılarının özellikle hassas zamanlarda,

²⁴⁹ Sosyal medya beslemeleri, kullanıcıların sosyal medya platformlarında paylaşılan içerikleri görmelerini sağlayan akışlardır. Bu beslemeler, kullanıcıların takip ettikleri kişilerin, sayfaların veya grupların paylaşımlarını, gönderilerini ve etkinliklerini içerir. Sosyal medya platformları, kullanıcıların ilgisini çekebilecek içerikleri belirlemek için algoritmalar ve kullanıcının etkileşim geçmişinden yararlanır. Sosyal medya beslemeleri, kullanıcılara özelleştirilmiş bir deneyim sunmak için tasarlanmıştır. Algoritmalar, kullanıcının ilgi alanlarına, etkileşimlerine ve davranışlarına dayalı olarak içerikleri sıralar ve önerir. Bu şekilde kullanıcılar, en ilgi çekici ve ilgili içeriklere kolayca erişebilirler. Sosyal medya beslemeleri, genellikle gönderilerin zaman sıralamasına göre düzenlenir, ancak bazı platformlar algoritmalara dayalı olarak içeriği sıralar. Algoritmalar, kullanıcının etkileşim geçmişine, beğenilerine, yorumlarına, paylaşımlarına ve diğer faktörlere dayanarak içerikleri önceliklendirir ve kullanıcının ilgi alanlarına uygun olanları gösterir.

²⁵⁰ "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression", para. 55.

²⁵¹ <https://help.twitter.com/en/rules-and-policies/twitter-rules>, (10.10.2021).

²⁵² <http://www.facebook.com/journalismproject/programs/third-party-fact-checking>, (3.9.2021).

²⁵³ https://blog.twitter.com/en_us/topics/product/2021/introducing-birdwatch-a-community-based-approach-to-misinformation, (3.9.2021).

seimler gibi, mesajları sınırsız sayıda kiřiye iletmelerini sınırlamıştır.²⁵⁴ WhatsApp'ta, ilk gönderen kiřiden en az beř ileti uzaklařan mesajların farklı etiketlerle iletilmesi de yine bu amaçla geliştirilmiř bir araçtır. Böylece, kullanıcılar yanıltıcı olabilecek bilgilere karşı uyarılmaktadır.²⁵⁵

řirketler tarafından alınan bu önlemler genel olarak olumlu olsa da řirketlerin hizmet řartlarının tutarsız uygulanması, yetersiz çözüm mekanizmaları ve tedbirlerin etkinlięinin objektif olarak deęerlendirilmesini engelleyen řeffaflık ve verilere erişim eksiklięi gibi uzun süredir devam eden sorunlar dolayısıyla yanıltıcı bilginin yayılmasından kaynaklanan endişelere karşı yeterli bir yanıt sunmamaktadır. Dahası, platformlar küresel işletmeler olmalarına rağmen politikalarını tüm coęrafi bölgelere tutarlı bir řekilde uygulamamakta ve tüm yetki alanlarında insan haklarını aynı ölçüde korumamaktadır. Bu durum da farklı yetki alanlarında farklı insan hakları standartları ortaya çıkarmaktadır.²⁵⁶

Kaye, Rapor'un sonuç kısmında çeřitli önerilere yer vermektedir. İfade özgürlüęü ile ilgili olarak, řirketlerin faaliyetlerinin her ařamasında insan hakları standartlarını uygulamalarını tavsiye edilmektedir. řirketlerin bu řekilde kendi pozisyonlarını demokratik normlara saygı gösterecek ve otoriter taleplere karşı çıkacak řekilde belirlemeleri mümkün olabilecektir. Bunun için de řirketler en azından, internetin kullanımına ilişkin kuralları belirlemeli ve bu kuralların uygulanmasında řeffaflıęı mümkün olan en üst düzeyde saęlamalıdır.²⁵⁷

İnsan hakları deęerlendirme prosedürlerinin geliştirilmesi ve uygulanması da bu bakımdan önem taşımaktadır. İnternet řirketleri, insan hakları üzerindeki potansiyel etkilerini dikkate alan politikalar geliřtirmeli ve uygulamalıdır. Özel kuruluşların ifade özgürlüęü ve dięer temel hakları ilgilendiren politika, standart ve eylemlerinde mümkün

²⁵⁴ <https://faq.whatsapp.com/1053543185312573>. İlk olarak Hindistan'da uygulanmaya bařlayan ve daha sonra tüm dünyada uygulanabilir hale getirilen bu özellik, bir mesajın iletilmesini aynı anda beř sohbetle sınırlamaktadır. <https://tech.hindustantimes.com/tech/news/whatsapp-to-cap-message-forwarding-to-5-chats-globally-to-curb-rumours-story-T2kmTaZlm5ifpfGoKEPL9I.html>, (5.3.2021).

²⁵⁵ <https://faq.whatsapp.com/431498999157251>, (5.3.2021).

²⁵⁶ Disinformation and Freedom of Opinion and Expression-Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression A/HRC/47/25, **OHCHR**, para. 65, <https://www.ohchr.org/en/documents/thematic-reports/ahrc4725-disinformation-and-freedom-opinion-and-expression-report>, (23.10.2024).

²⁵⁷ "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression", para. 89.

olan en yüksek şeffaflığı sağlamaları da kritik önem taşımaktadır. İnsan hakları değerlendirmeleri, metodolojileri, yasal yükümlülüklerin yorumlanması ve bu değerlendirmelerin ticari kararlar üzerindeki ağırlığı bakımından şeffaf bir incelemeye tabi tutulmalıdır. Şeffaflık, içerik düzenlemesi bağlamı da dahil olmak üzere her alanda önemlidir ve hükümetlerin yayından kaldırma taleplerinin raporlanmasını da içermelidir.²⁵⁸

Kaye, 2018 yılında hazırladığı Rapor'da, şirketlerin sorumluluklarına ilişkin daha geniş bir çerçeve sunmuştur. Şirketlerin ulusal düzenlemeleri ya da kendi çıkarlarını değil uluslararası standartları esas almaları ve içerik standartlarını bu doğrultuda güncellemelerine yönelik vurgu dikkat çekicidir. Kaye, bu sorumluluğun gerekliliklerini şu şekilde ifade etmiştir:

*“İnsan hakları hukuku, şirketlere demokratik normları koruyan ve otoriter taleplere karşı koyan politikalar ve süreçler geliştirme araçları sunar. Bu yaklaşım, haklara dayalı kurallarla başlar, ürün ve politika geliştirme süreçlerinde titiz insan hakları etki değerlendirmeleri ile devam eder ve operasyonlar sırasında sürekli değerlendirme, yeniden değerlendirme ve anlamlı kamu ve sivil toplum danışmanlığı ile ilerler. İş Dünyası ve İnsan Haklarına Dair Rehber İlkeler ile sivil toplum, uluslararası kuruluşlar, Küresel Ağ İnisiyatifi ve diğerleri tarafından geliştirilen sektöre özgü yönergeler, tüm internet şirketlerinin benimsemesi gereken temel yaklaşımlar sunar.”*²⁵⁹

2018 yılında kabul edilen bir başka Rapor'da ise yapay zekâ teknolojilerinin ifade özgürlüğü ve bilgi ortamı üzerindeki etkilerine odaklanılmıştır.²⁶⁰ Bu doğrultuda, algoritmaların, insanlar gibi kültürel bağlamı değerlendirme, ironi tespit etme veya “aşırılık yanlısı” içerik ya da nefret söylemi gibi konuları doğru bir şekilde tanımlamak için gerekli olan eleştirel analizi yapma yeteneğine sahip olmadığı belirtilerek otomatik süreçlerin içerik düzenleme süreçlerini daha da zorlaştırabileceğine dikkat çekilmiştir. Bu

²⁵⁸ “Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression”, para. 87-89.

²⁵⁹ Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (A/HRC/38/35), UN, 2018, para. 70, <https://documents.un.org/doc/undoc/gen/g18/096/72/pdf/g1809672.pdf>, (21.10.2024).

²⁶⁰ Promotion and Protection of the Right to Freedom of Opinion and Expression (A/73/348), UN, 2018, <https://documents.un.org/doc/undoc/gen/n18/270/42/pdf/n1827042.pdf>, (21.10.2024).

teknolojiler, bilgi ve fikirlerin yayılması, medya çeşitliliği ve bağımsız sesler için uygun bir ortam yaratma amacına uygun olmayan bir internet yönetimine yol açabilecektir. Bu durum, özellikle şeffaflığa dair kaygıları da beraberinde getirmektedir. Otomatik süreçler ile yönlendirilen platformlarda, kullanıcılar “oyunun kurallarını” tam olarak bilmediklerinden bilginin yayılması, kısıtlanması ya da hedeflenmesine yönelik süreçleri anlamlandıramamaktadır.²⁶¹

Yapay zekâ teknolojilerine ilişkin bu tespitler, bu teknolojilerin tasarlanması, geliştirilmesi ve uygulanmasına yönelik birtakım önerileri de beraberinde getirmiştir. Buna göre²⁶²:

- a) Yapay zekâ teknolojilerinin geliştirilmesi ve kullanımı, insan hakları prensipleri temelinde yapılmalıdır.
- b) Şirketler, yapay zekâ sistemlerinin nasıl çalıştığı, hangi verileri kullandığı ve kullanıcıların haklarını nasıl etkileyebileceği konusunda şeffaf olmalıdır.
- c) Yapay zekâ sistemlerinde önyargı ve ayrımcılığın önlenmesi için gerekli önlemler alınmalıdır.
- d) Yapay zekâ sistemlerinin geliştirilme sürecinde sivil toplum kuruluşları ve diğer paydaşların görüşleri alınmalıdır.
- e) Yapay zekâ sistemleri geliştirilmeden önce insan hakları etkileri değerlendirilmeli ve bu değerlendirmelerin sonuçları kamuoyuyla paylaşılmalıdır.
- f) Yapay zekâ sistemlerinin neden olduğu olumsuz insan hakları etkilerinden zarar gören bireylerin etkili çözüm yollarına erişimi sağlanmalıdır.

Güncel çalışmalarda, şirketlerin insan haklarına ilişkin etkileri bakımından daha spesifik sorunların ele alındığı görülmektedir. 2019 yılında, nefret söylemi²⁶³; 2021 yılında ise dezenformasyon ve ifade özgürlüğü²⁶⁴ konusu ele alınmış, bu kapsamda şirketler için daha detaylı gereklilikler öngörülmüştür.

²⁶¹ Ibid., para. 27-32.

²⁶² Ibid., para. 65-70.

²⁶³ Promotion and protection of the right to freedom of opinion and expression (A/74/486), United Nations, 2019, <https://documents.un.org/doc/undoc/gen/n19/308/13/pdf/n1930813.pdf>, (21.10.2024).

²⁶⁴ Disinformation and freedom of opinion and expression. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Irene Khan (A/HRC/47/25), UN, 2021, <https://documents.un.org/doc/undoc/gen/g21/085/64/pdf/g2108564.pdf>, (20.10.2024).

Nefret söylemiyle mücadele kapsamında, şirketler insan hakları hukukuna uygun içerik politikaları oluşturmalarıdır. Bu politikalar, net, tutarlı ve uluslararası standartlara uygun olmalıdır. Bu kapsamda şirketler tarafından zararlı içeriklere ilişkin içerik düzenleme süreçleri işletilecektir. Bu süreçler, şeffaf ve orantılı olmalı; özellikle kullanıcı hesaplarının kapatılması veya içeriklerin kaldırılması gibi durumlarda insan denetimi mutlaka yapılmalıdır.²⁶⁵

Dezenformasyon ve ifade özgürlüğü ilişkisinin ele alındığı Rapor'da²⁶⁶, dijital teknolojilerin yanlış veya manipüle edilmiş bilginin çeşitli aktörler tarafından siyasi, ideolojik veya ticari amaçlarla daha önce hiç bilinmeyen bir ölçekte, hızla ve erişimde yaratılması, yayılması ve güçlendirilmesine yol açtığı ve bu durumun demokrasi ve insan hakları açısından önemli sonuçları olabileceği belirtilmektedir.²⁶⁷ Bu doğrultuda, dezenformasyonla mücadele konusundaki farklı yaklaşımlar ele alınmış; yetkililere içerik kaldırma konusunda geniş yetkiler veren ve şirketlere de bu kapsamda aşırı yükler yükleyen örneklerle ilişkin kaygılar ifade edilmiştir.²⁶⁸ Bu kapsamda şirketlere, kullanıcı haklarına duyarlı bir yaklaşım benimsemeleri, mevcut endişelere proaktif bir şekilde yanıt vermeleri ve internet kullanıcılarını güçlendirmeleri tavsiye edilmiştir.²⁶⁹ Bu, kullanıcıların kendi bilgi ve deneyimleri üzerinde daha fazla şeffaflık, kontrol ve seçenek sahibi olmalarının sağlanmasını gerektirmektedir. Şirketler ayrıca, algoritmalarının veya öneri sistemlerinin parametreleri hakkında kullanıcıya açık ve anlamlı bilgiler sunmalıdır. Bu sistemlerin farklı şekillerde çalışması güvence altına alınmalı ve kullanıcılara çevrimiçi deneyimlerini şekillendiren değişkenleri seçme imkânı tanınmalıdır. Son olarak, kullanıcılar için etkin başvuru mekanizmaları oluşturulmalı ve içerik türüne yönelik iç denetim mekanizmaları sağlanmalıdır.²⁷⁰

2. Özel Hayatın Korunması Bakımından Özel Sektöre Uygulanabilir İlkeler

Birleşmiş Milletler Sistemi'nde, özel hayata saygı hakkı da internet şirketlerinin değişen rolleri ve sorumlulukları bağlamında ele alınan konulardan biridir. Dijital

²⁶⁵ "Promotion and protection of the right to freedom of opinion and expression (A/74/486)", para. 58.

²⁶⁶ "Disinformation and freedom of opinion and expression. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (A/HRC/47/25)".

²⁶⁷ Ibid., para. 2.

²⁶⁸ Ibid., para. 57, 58.

²⁶⁹ Ibid., para. 95.

²⁷⁰ Ibid., para. 99, 101.

gelişmelerin en fazla aşındırdığı haklardan biri olan özel hayata saygı hakkının, BM sisteminde farklı boyutlarıyla ele alınması, bu hakkın korunabilmesi açısından önemlidir.

2013 yılında kabul edilen “Dijital Çağda Mahremiyet Hakkı” Kararı’nda, özel hayatın gizliliği hakkının kullanılmasının, ifade özgürlüğü ve müdahale olmaksızın kanaat sahibi olma hakkının gerçekleştirilmesi için önemli olduğunu ve demokratik bir toplumun temellerinden biri olduğu vurgulanmış ve dijital gelişmelerin hem devletlerin hem de şirketlerin insan haklarını ihlal veya istismar edebilecek izleme, dinleme ve veri toplama kapasitesini artırdığına dikkat çekilmiştir. Bununla birlikte Karar’da, yalnızca devletlere yönelik bir çağrıda bulunulmuştur.²⁷¹

2014 yılında kabul edilen bir başka Rapor’da ise, şirketlerin mahremiyet hakkı üzerindeki etkileri ayrı bir başlıkta ele alınmıştır.²⁷² Bu raporda, daha çok devletlerin, mahremiyet hakkına yönelik müdahalelerde şirketleri araçsallaştırmasına yönelik endişeler ifade edilmiştir. Raporda, devletlerin özel şirketlerden meşru amaçlarla kullanıcı verilerini sağlamasını talep edebileceği kabul edilmekle birlikte; bu taleplerin uluslararası hukuka aykırı bir talebe yanıt olarak ya da yeterli koruma önlemleri olmadan yerine getirilmesi halinde şirketlerin, devletlerin insan hakları ihlallerine ortak olma riskiyle karşı karşıya kalabileceğinin altı çizilmiştir.²⁷³ Bu risklerin insan hakları ihlallerine dönüşmemesi için internet şirketlerinin, faaliyetleri boyunca insan haklarına saygıyı içeren açık bir politika taahhüdü benimsemeleri tavsiye edilmiştir. Ayrıca, olumsuz etkilerin tespit edilmesi, ele alınması, önlenmesi ya da ve hafifletmesi yönelik durum değerlendirme politikaları da bulunmalıdır. Şirketler, hizmet şartlarının veya müşteri verilerini toplama ve paylaşma politikalarının kullanıcıların insan hakları üzerinde olumsuz bir etkiye yol açıp açmadığını değerlendirmelidir.²⁷⁴

Rapor’a göre, şirketler, uluslararası insan hakları standartlarına uymayan veri erişimi talepleriyle karşılaştıklarında, insan haklarının prensiplerini mümkün olan en üst düzeyde ele almalı ve bunu sürdürmelidir. Bu da, hükümet taleplerini mümkün olduğunca

²⁷¹ “The Right to Privacy in the Digital Age (A/RES/68/167)”.

²⁷² The Right to Privacy in the Digital Age Report of the Office of the United Nations High Commissioner for Human Rights (A/HRC/27/37), UN, 2014, para. 42-46 <https://documents.un.org/doc/undoc/gen/g14/088/54/pdf/g1408854.pdf>, (3.10.2023).

²⁷³ Ibid., para. 43.

²⁷⁴ Ibid., para. 44.

dar bir şekilde yorumlama, talebin kapsamı ve yasal temeli konusunda hükümetten açıklama isteme, veri taleplerine cevap vermeden önce mahkeme kararı talep etme ve kullanıcılarla riskler ve hükümet taleplerine uyum konusunda şeffaf bir şekilde iletişim kurma şeklinde pozisyonlar almayı gerektirebilir.²⁷⁵ Şirketlerin bu yöndeki davranışları; içerik kaldırma ve kullanıcı verilerine yönelik devlet taleplerinin hacmi ve bağlamı, bu tür taleplerin ele alınmasına yönelik süreçler ve ilgili yasa, politika ve yönetmeliklerin yorumuna ışık tuttuğu gibi kullanıcıların endişelerini dile getirebilmesi ve bilinçli kararlar verebilmeleri bakımından da önemlidir.

Raporda, BM Rehber İlkeler dikkate alınarak şirketlerin telafi edici çözüm üretme sorumlulukları da vurgulanmıştır. Bu sorumluluk, internet şirketlerinin olumsuz insan hakları etkisine neden olmaları veya katkıda bulunmaları durumunda, doğrudan çözüm sağlayarak veya meşru çözüm süreçleriyle iş birliği yoluyla tekrarlanmama ve düzeltilme garantilerini gerektirmektedir. Bu noktada, en erken aşamada düzeltmeyi mümkün kılmak için şirketler, operasyonel düzeyde şikâyet mekanizmaları oluşturmalıdır. Tazminat ve iade/eski hale getirme gibi unsurlara ek olarak şirketler, kullanıcılara hangi verilerin Devlet otoriteleriyle paylaşıldığı ve nasıl paylaşıldığı konusunda da bilgi vermelidir.²⁷⁶

2018 yılında, mahremiyet hakları kapsamında özellikle kişisel verilerin korunmasına ilişkin önemli bir çerçeve sunulmuştur.²⁷⁷ Bu doğrultuda, BM Rehber İlkeler’de öngörülen şirketlerin insan haklarını koruma sorumlulukları kapsamlı bir şekilde hatırlatılmış bu sorumluluklar kişisel verilerin korunmasına uyarlanmıştır. Buna göre, kullanıcı verisi toplayan ve saklayan şirketler kendi faaliyetlerinde kapsamlı insan hakları durum değerlendirmeleri yapmalı ve risk azaltmaya yönelik tedbirler almalıdır. Devletlerin bu verilere yönelik taleplerinde de mahremiyet ile insan haklarına zarar verme potansiyeline karşı gerekli önlemlerin alınması gerekmektedir. Öte yandan, dijital ortamda şeffaflık, toplanan kişisel verilerin türü, saklanma süresi, kullanım amacı ve paylaşılma koşulları hakkında bilgi sağlanmasını gerektirmektedir. Dolayısıyla şirketler, devletlerden gelen kullanıcı verisine erişim talepleri de dahil olmak üzere kullanıcı

²⁷⁵ Ibid., para. 45.

²⁷⁶ Ibid., para. 46.

²⁷⁷ “The right to privacy in the digital age Report of the United Nations High Commissioner for Human Rights (A/HRC/39/29)”, United Nations, 2018, <https://documents.un.org/doc/undoc/gen/g18/239/58/pdf/g1823958.pdf>, (4.10.2023).

verilerine ilişkin olarak yüksek düzeyde şeffaflık sağlamalıdır. Rapor'da, şirketler, ulusal yasaların bu tür bilgilerin açıklanmasını kısıtladığı durumlarda, sahip oldukları tüm etki gücünü kullanarak, bu bilgilerin serbest bırakılabilmesi için savunuculuk yapmaya teşvik edilmektedir.²⁷⁸

Mahremiyet haklarına ilişkin olarak, yapay zekâ sistemlerindeki gelişmeler de BM tarafından özel olarak ele alınmıştır. 2018 yılında, yapay zekâ destekli karar alma sistemlerinin temel hak ve özgürlükler üzerindeki etkilerinin ele alındığı Rapor'da bu sistemlerin mahremiyetin korunmasına ilişkin önemli yol açtığı belirtilmiştir.²⁷⁹ Bu teknolojilerin kullanıldığı veri toplama ve işleme süreçleri genellikle anonimleştirilmiş verilerden kişisel olarak tanımlanabilir bilgilere kadar değişkenlik gösterebilen geniş kapsamlı veri havuzlarına dayanmaktadır. Profillemeye, dijital parmak izi çıkarma ve veri brokerlerinden veri satın alma gibi yöntemlerle elde edilen veriler, bireyler hakkında dini inanç, sağlık durumu ve siyasi görüş gibi son derece hassas bilgileri ortaya çıkarabilmektedir. Bu durum, bireylerin mahremiyet haklarını ve rıza ilkesini ihlal ettiği için etik ve hukuki açıdan ciddi kaygılar uyandırmaktadır; zira bireylerin rızası olmadan elde edilen bu veriler, onların kontrolü dışında işlenmekte ve farklı amaçlarla kullanılmaktadır.²⁸⁰

Yapay zekanın etkilerinin ele alındığı bu Rapor'da, bu sistemlerin uluslararası veri koruma standartlarının temeli olan rıza, amaç sınırlaması, şeffaflık ve hesap verebilirlik ilkelerine de meydan okuduğunu vurgulanmıştır. Bu sistemlerde, mevcut veri kümeleri farklı bağlamlarda yeniden kullanılarak ve yeni veri kümeleri oluşturularak, bireylerin verileri üzerindeki denetimleri büyük ölçüde sınırlandırılmaktadır. Verilerin özgün bağlamlarından çıkarılması, güncelliğini yitirme veya doğruluğunun azalması riskini doğurmakta; bu durum, bireylerin verilerini düzeltme veya silme gibi temel haklarının kullanımını zorlaştırmaktadır. Anonimleştirme tekniklerinin yetersiz kaldığı alanlarda, yapay zekâ tabanlı sistemler bireylerin yaşamlarını derinden etkileyebilecek kararlar almakta; fakat bu kararlarda bireylerin etkin bir kontrol mekanizması bulunmamaktadır.²⁸¹

²⁷⁸ Ibid., para. 47.

²⁷⁹ "Promotion and protection of the right to freedom of opinion and expression (A/73/348)".

²⁸⁰ Ibid., para. 34.

²⁸¹ Ibid., para. 35.

2021’de ise, yapay zekâ sistemlerinin etkilerinin daha da sarsıcı bir hale gelmesiyle birlikte bu sistemlerin mahremiyet haklarına etkileri ayrı bir Rapor’da²⁸² ele alınmıştır. Rapor’da, bu sistemlerin yol açtığı mahremiyet endişeleri şu şekilde ifade edilmiştir:

“Yapay zekâ sistemleri, genellikle kişisel veriler de dahil olmak üzere büyük veri setlerine dayanır. Bu durum, geniş çaplı veri toplama, depolama ve işlemeyi teşvik etmektedir. Birçok şirket, mümkün olduğunca çok veri toplamak için hizmetleri optimize etmektedir. Örneğin, sosyal medya şirketleri gibi çevrimiçi şirketler, internet kullanıcıları hakkında büyük miktarda veri toplamaya ve bunlardan para kazanmaya dayanmaktadır. Nesnelerin İnterneti olarak adlandırılan şey hem işletmeler hem de Devletler tarafından kullanılan ve hızla büyüyen bir veri kaynağıdır. Veri toplama mahrem, özel ve kamusal alanlarda gerçekleşmektedir. Veri brokerları kişisel verileri elde etmekte, birleştirmekte, analiz etmekte ve sayısız alıcıyla paylaşmaktadır. Bu veri işlemleri, büyük ölçüde kamu denetiminden uzak olup mevcut yasal çerçeveler tarafından sadece sınırlı bir şekilde engellenmektedir. Sonuç olarak ortaya çıkan veri setleri büyüktür ve toplanan bilgiler daha önce görülmemiş boyutlardadır.

*Bu veri setleri, insanların özel hayatlarını şirketlere ve devletlere ifşa etmenin yanı sıra, bireyleri başka şekillerde de savunmasız hale getirmektedir. Veri ihlalleri milyonlarca insanın hassas bilgilerini defalarca ifşa etmiştir. Büyük veri setleri sayısız analiz biçimini ve verilerin üçüncü taraflarla paylaşılmasını mümkün kılmakta, bu da genellikle daha fazla mahremiyete yol açmaktadır.”*²⁸³

Raporda bu endişelerden yola çıkılarak, şirketlere yapay zekâ sistemlerinin insan haklarına olası etkilerini azaltmaya yönelik bir dizi önlem alması tavsiye edilmiştir. Buna göre, söz konusu sistemlerinin tasarım, geliştirme, dağıtım, satış ve işletme aşamalarında insan hakları özen yükümlülüğü süreçleri sistematik olarak sürdürülmelidir. Bu kapsamda düzenli ve kapsamlı insan hakları etki değerlendirmeleri yapılmalıdır. Bu konuda

²⁸² “The right to privacy in the digital age. Report of the United Nations High Commissioner for Human Rights (A/HRC/48/31)”, United Nations, 2021, <https://documents.un.org/doc/undoc/gen/g21/249/21/pdf/g2124921.pdf>, (5.8. 2024).

²⁸³ Ibid., para. 13, 14.

şeffaflık yükümlülükleri özel bir önem taşımaktadır. Bu bakımdan şirketler şeffaflığı, insan haklarına olan potansiyel veya gerçek etkileri ölçüsünde artırmalıdır.²⁸⁴

II. Ekonomik İş Birliği ve Kalkınma Örgütü (OECD)

1961 yılında kurulan ve halihazırda 37 devletin üye olduğu Ekonomik İş Birliği ve Kalkınma Örgütü ekonomik, sosyal ve yönetsel sorunları çözmek üzere oluşturulmuş bir örgüttür. Örgütün temel amaçları ekonomik büyüme, mali istikrar, ticaret ve yatırım, teknoloji, yenilik, girişimcilik ve kalkınma alanlarında işbirliği yoluyla refahın sağlanması ve yoksullukla mücadele konularında hükümetlere yardımcı olmak; ekonomik ve sosyal gelişme ile çevrenin korunması arasındaki dengeyi gözetmek, herkes için iş imkânı yaratılması ve sosyal eşitlik ile etkin ve sağlıklı bir yönetim gerçekleştirilmesini sağlamak; yeni gelişme ve sorunları anlamak ve bunlara çözüm üretmek konularında hükümetlere tavsiyelerde bulunmaktır.²⁸⁵

Bu amaçlar doğrultusunda, 1976 yılında OECD Çok Uluslu Şirketler Rehberi kabul edilmiştir. Uluslararası Yatırımlar ve Çok Uluslu Şirketler Deklarasyonu'nun bir parçası olan OECD Çok Uluslu Şirketler Rehberi'nde, çok uluslu şirketlere yönelik insan hakları ve çalışma ilişkilerini de kapsayan tavsiyelere yer verilmiştir. 1976 yılında kabul edilen ve sürekli gözden geçirilen Rehber'in 2011 yılında yapılan güncellemesinde²⁸⁶, internette ifade özgürlüğü de bir konu başlığı olarak yer almıştır. 2023 yılındaki son güncellemede ise veri toplama ve kullanma da dahil olmak üzere teknolojinin geliştirilmesi, finansmanı, satışı, lisanslanması, ticareti ve kullanımına ilişkin durum değerlendirme beklentileri Rehber'e dahil edilmiştir.²⁸⁷

A. OECD Çok Uluslu Şirketler Rehberi

1976 yılında yayımlanan Çok Uluslu Şirketler Rehberi'nde 2011 yılında yapılan güncellemede, şirketlerin insan hakları yükümlülükleri ilk defa hükümetler arası bir anlaşmayla ele alınmıştır. Bu güncellemede, Birleşmiş Milletler İş Dünyası ve Rehber

²⁸⁴ Ibid., para. 60, 61.

²⁸⁵ <https://www.oecd.org/about/document/oecd-convention.htm#Text>, (1.4.2021).

²⁸⁶ OECD Guidelines for Multinational Enterprises, **OECD**, 2011 Edition.

²⁸⁷ OECD Guidelines for Multinational Enterprises on Responsible Business Conduct, **OECD**, 2023 Edition, https://www.oecd.org/en/publications/oecd-guidelines-for-multinational-enterprises-on-responsible-business-conduct_81f92357-en.html, (23.12.2024).

İlkeler: "Koruma, Saygı Gösterme ve Telfi Edici Çözüm Üretme Çerçevesinin Uygulanması" ile uyumlu olan yeni bir insan hakları bölümüne yer verilmiş, devletlerin kendi yükümlölüklerini yerine getirme kabiliyetlerine ve/veya istekliliklerine bakılmaksızın insan haklarının hepsine saygı gösterilmesi gerektiğı açıkça belirtilmiştir. Ayrıca, şirketlerin bu sorumluluğı yerine getirmek için ihtiyaç duydukları sistemler şart koşularak hem kendi faaliyetleri hem de iş ilişkileri için durum değerlendirme süreçleri merkeze alınmıştır.²⁸⁸ Bu bölümde, şirketlerin insan hakları yükümlölükleri Birleşmiş Milletler Rehber İlkeler sistematığına uygun olarak ele alınmıştır. Buna göre;

“Devletler, insan haklarını korumakla yükümlüdür. Şirketlerin, uluslararası alanda tanınmış olan insan hakları ve faaliyet gösterdikleri ülkelerin uluslararası insan haklarına ilişkin yükümlölükleri ve diğer ilgili iç hukuk kuralları çerçevesinde,

- 1. İnsan haklarına saygı göstermeleri, başka bir deyişle insan hakları ihlallerinden kaçınmaları ve insan hakları üzerinde olumsuz etkilerde bulunabilecek durumlara müdahale etmeleri,*
- 2. Kendi faaliyetleri çerçevesinde insan haklarına olumsuz etkilerde bulunmaktan veya bunlara yol açmaktan kaçınmaları ve böyle durumlara karşılaştıklarında müdahale etmeleri,*
- 3. Kendileri doğrudan buna yol açmamış olsalar bile iş ilişkileri nedeniyle faaliyetleri, hizmet ve ürünleri ile doğrudan ilgili olan durumlarda, insan hakları üzerindeki olumsuz etkilerin önlenmesi ve hafifletilmesi için yollar aramaları,*
- 4. İnsan haklarına saygı prensibini benimsemeleri,*

²⁸⁸ John Gerard Ruggie, Tamaryn Nelson, “Human Rights and the OECD Guidelines for Multinational Enterprises: Normative Innovations and Implementations Challenges”, **Brown Journal of World Affairs**, C. 22, 2015, s. 105.

5. *Faaliyetlerinin içeriği, niteliği büyüklüğü ve insan hakları üzerinde yol açabilecekleri olumsuz etkilerin ciddiyeti dikkate alınarak insan hakları konusunda gerekli incelemeleri yapmaları,*

6. *İnsan hakları üzerinde olumsuz etkilere yol açabileceğini tespit ettikleri durumlarda, bu etkileri gidermek amacıyla meşru yollardan iş birliği yapmaları gerekmektedir.*"²⁸⁹

Rehber’de, devletlerin ve şirketlerin insan hakları yükümlülükleri bu çerçevede ele alındıktan sonra, söz konusu yükümlülüklerle ek olarak ayrıntılı açıklamalara yer verilmiştir. Rehberde göre devletlerin ilgili iç hukuk kurallarını yürürlüğe sokamaması, insan hakları ile ilgili uluslararası yükümlülüklerini yerine getirememesi ya da bu tür hukuk kuralları ve uluslararası yükümlülüklerle aykırı davranması şirketlerden insan haklarına saygı göstermesi beklentisini azaltmamaktadır. Bu bakımdan, iç hukuk kuralları ile uluslararası insan hakları arasında çatışmanın söz konusu olduğu ülkelerde, şirketlere iç hukuk kurallarını ihlal etmeden, mümkün olduğu ölçüde uluslararası alanda tanınmış insan hakları uygulamaları tavsiye edilmiştir.²⁹⁰

Şirketler, uluslararası alanda kabul görmüş hemen hemen tüm insan hakları üzerinde etkili olabilirler. Uygulamada, belli sektör ve ortamlarda bazı insan hakları diğerlerine göre daha çok risk altında olduğundan, bu haklar daha fazla ilgi odağındadırlar. Bazı insan haklarına yönelik bu eğilim Rehber’de 2011 yılında yapılan güncellemelerde de yer bulmuştur. Bu kapsamda, Rehber’de bilgi ve iletişim teknolojilerindeki ilerlemeler ve bu alanda faaliyet gösteren şirketlerin insan haklarına potansiyel etkileri göz önünde bulundurularak ifade özgürlüğünün korunmasına yönelik spesifik bir tavsiyeye yer verilmiştir. Rehberin “Genel Politikalar” başlıklı II. bölümünde şirketlerin, “*online ifade, toplanma ve örgütlenme özgürlüklerine saygı çerçevesinde, koşulları elverdiği ölçüde, uygun ortamlarda internet özgürlüğünün geliştirilmesine yönelik ortak çabaları desteklemeye*” teşvik edileceği belirtilmiştir.²⁹¹

²⁸⁹ “OECD Guidelines for Multinational Enterprises”, s. 31.

²⁹⁰ “OECD Guidelines for Multinational Enterprises”, s. 32.

²⁹¹ “OECD Guidelines for Multinational Enterprises”, s. 20.

Rehberin “Tüketici Menfaatleri” başlıklı VIII. bölümünün kişisel verilere ilişkin 6. paragrafında, şirketler için “*Tüketicinin mahremiyetine saygı gösterecek ve topladıkları, sakladıkları, işledikleri ve yayımladıkları kişisel verilerin gizliliğinin sağlanması için gerekli önlemleri alacaktır*” yükümlülüğüne yer verilmiş; bu maddenin açıklamasında ise söz konusu yükümlülük ile gerek internetin gerekse teknolojik ilerlemelerin etkisiyle şirketler tarafından toplanan kişisel verilerin ve bunların kullanımının giderek artmasının kişisel verilerin güvenlik ihlalleri de dahil olmak üzere özel hayat ihlallerine karşı korunmasının öneminin vurgulandığı belirtilmiştir.²⁹²

Rehber, son olarak 2023 yılında güncellenmiştir. 2011 yılından bu yana on yıllık bir deneyimi yansıtan bu versiyonun önsözünde, güncellenmenin toplumların ve işletmelerin karşılaştığı acil sosyal, çevresel ve teknolojik önceliklere yanıt verdiği belirtilmektedir.²⁹³ 2023 tarihli bu güncellemede, internet teknolojilerinde yaşanan gelişmeler de dikkate alınmış, bu kapsamda “Bilim ve Teknoloji” başlıklı IV. bölümün başlığı “Bilim, Teknoloji ve İnovasyon” olarak değiştirilmiş ve bu bölümde mahremiyete ve ifade özgürlüğüne ilişkin daha ayrıntılı yükümlülüklerle yer verilmiştir.

Bu kapsamda, söz konusu bölüme şirketlere yönelik şu iki madde eklenmiştir:

".... 6. Veri toplarken, paylaşırken ve kullanırken, veri erişimi ve paylaşımına ilişkin düzenlemelerin şeffaflığını artırmak önemlidir. Veri değeri döngüsü boyunca, rehberlere uyum sağlayan sorumlu veri yönetimi uygulamalarının benimsenmesi teşvik edilir. Bu uygulamalar, rehberlere uyum sağlayan davranış kurallarına, etik prensiplere, tüketici manipülasyonu ve baskısına karşı düzenlemelere, aynı zamanda gizlilik ve veri koruma normlarına uymayı içerir.

7. İşletmeler, kendi özel durumlarına göre, açık, özgür, küresel, uyumlu, güvenilir, erişilebilir, uygun maliyetli, güvenli ve dayanıklı bir İnternet'i teşvik etmek için uygun forumlarda iş birliği çabalarını desteklemelidir. Bu destek, ifade özgürlüğünü, barışçıl toplantı ve bir araya gelme haklarını çevrimiçi

²⁹² “OECD Guidelines for Multinational Enterprises”, s. 51.

²⁹³ “OECD Guidelines for Multinational Enterprises on Responsible Business Conduct”.

*ortamda destekleme prensipleriyle uyumlu olmalıdır. Tüm bunlar, Rehberlerde ele alınan konularla tutarlı bir şekilde yürütülmelidir."*²⁹⁴

Rehber’de ortaya konulan bu yükümlülüklerle ilgili olarak OECD tarafından yayımlanan Dijital Hizmet Sağlayıcılar İçin Rehber İlkeler’e²⁹⁵ de atıf yapılmakta ve bu ilkelerle uyumlu önlemler alınması gerektiği belirtilmektedir.

B. Dijital Hizmet Sağlayıcılar İçin Rehber İlkeler

Dijital Hizmet Sağlayıcılar İçin Rehber İlkeler’de dijital ortamda çocukları doğrudan veya dolaylı olarak etkileyebilecek eylemler bakımından dijital hizmet sağlayıcılara çocukların haklarının, güvenliklerinin ve çıkarlarının en iyi şekilde korunması için önerilere yer verilmiştir.

Dijital Hizmet Sağlayıcılar İçin Rehber İlkelerde söz konusu öneriler; tasarımda çocuk güvenliği, bilgi sağlama ve şeffaflık, gizlilik, veri koruma ve ticari kullanım, yönetim ve sorumluluk şeklinde dört başlıkta ele alınmıştır.

İlk olarak tasarımda çocuk güvenliği, çocuklar için uygun olmayan hizmet ve içerikler bakımından bu hizmet ve içeriklere erişimin engellenmesini ve çocukların erişebileceği ve kullanabileceği hizmetler bakımından ise güvenli ve faydalı bir dijital ortamın sağlanmasını gerektirmektedir. Öte yandan, ortaya çıkabilecek riskler bakımından uygulamaların sürekli olarak gözden geçirilerek güncellenmesi ve yasalar tarafından öngörülen yaş kısıtlamalarının uygulanması da güvenli tasarım yaklaşımının unsurları arasında ele alınmaktadır.²⁹⁶

İkinci olarak bilgi sağlama ve şeffaflık ilkesi, çocukların erişebileceği hizmetlerin sunulmasında dijital hizmet sağlayıcılara söz konusu hizmetlerin öz, anlaşılır, kolay erişilebilir, açık, sade ve yaşa uygun şekilde bilgi sağlanması olarak tanımlanmaktadır.²⁹⁷

²⁹⁴ “OECD Guidelines for Multinational Enterprises on Responsible Business Conduct”, s. 46.

²⁹⁵ “OECD Guidelines for Digital Service Providers”.

²⁹⁶ “OECD Guidelines for Digital Service Providers”, s. 1.

²⁹⁷ Ibid.

Rehber ilkelerde yer verilen veri koruma ve ticari kullanım başlığında, çocuklara dijital hizmetlerin sunulması sırasında kişisel veri toplama, işleme, paylaşma ve kullanma gerekliliği olması halinde dikkate alınması gereken hususlar ele alınmaktadır. Buna göre, böyle durumlarda, çocuklara ve onların ebeveynlerine kişisel verilerinin nasıl toplandığı, açıklandığı, erişilebilir hale getirildiği veya diğer şekillerde nasıl kullanıldığına dair bilgi sunulmalı; kişisel verilerin toplanması, kullanılması veya üçüncü taraflarla paylaşılması sadece çocuğun en iyi çıkarları doğrultusunda hizmetin sağlanmasıyla sınırlanmalı; çocuklara zarar verdiğine yönelik bulguların varlığı halinde veriler kullanılmamalı ve zorlayıcı bir nedenin varlığı ve çocukları zararlı etkilerden korumak için uygun önlemlerin alınmış olması hali dışında, çocukların profillerinin alınmasına izin verilmemelidir.²⁹⁸

Son olarak, yönetim ve sorumluluk konusunda dijital hizmet sağlayıcıların, hizmetlere erişen tüm çocukların çıkarlarını en iyi şekilde korumaya yönelik politika ve prosedürlerinin olması gerektiği belirtilmektedir. Bu başlık altında ayrıca, hizmet sağlayıcıların kendi politika ve prosedürleri yanında, bu amacı sağlamaya yönelik yerel politika, düzenleme veya yasalarla da uyumlu olmaları gerektiği vurgulanmıştır.²⁹⁹

III. Uluslararası Çalışma Örgütü (ILO)

1919 yılında adil çalışma koşullarının teşvik edilmesi, insan onurunun korunması ve iş dünyasının sürdürülebilir kalkınmaya katkıda bulunması amaçlarıyla kurulmuş olan Uluslararası Çalışma Örgütü, BM'nin bir ihtisas kuruluşudur. Örgüt, temel sözleşmeleri aracılığıyla örgütlenme özgürlüğü, zorla çalıştırmanın yasaklanması, çocuk işçiliğinin önlenmesi ve ayrımcılıkla mücadele gibi temel çalışma haklarını güvence altına almakta ve iş sağlığı ve güvenliği, sosyal güvenlik, ücretler ve çalışma saatleri gibi konularda da uluslararası standartlar belirlemektedir.

İş dünyası ve insan hakları ilişkisi söz konusu olduğunda, Birleşmiş Milletler İş Dünyası ve İnsan Haklarına Dair Rehber İlkeler ve OECD Çok Uluslu Şirketler Rehberi ile referans alınan bir diğer kaynak da ILO Çok Uluslu Şirketler ve Sosyal Politikaya

²⁹⁸ “OECD Guidelines for Digital Service Providers”, s. 2.

²⁹⁹ Ibid.

İlişkin İlkeler Üçlü Bildirgesi (Çokuluslu İşletmeler Bildirgesi)'dir.³⁰⁰ Bu Bildirge, uluslararası çalışma standartları temel alınarak insana yakışır iş, kapsayıcı ekonomik büyüme ve sürdürülebilir kalkınma bağlamında hükümetlere, sosyal ortaklara ve işletmelere çalışmayla ilgili insan hakları konusunda rehberlik sağlamak amacıyla 1977'de kabul edilmiş ve son olarak 2017 yılında güncellenmiştir. Bildirgede devletlerin ve işletmelerin insan haklarına ilişkin görev ve sorumluluklarının ana hatları belirlenirken Birleşmiş Milletler Rehber İlkeler'e atıfta bulunulmakta ve ticari faaliyetlerde işçi haklarının korunması ve bunlara saygı gösterilmesi söz konusu olduğunda bu görev ve sorumlulukların ne anlama geldiği daha açık bir şekilde ortaya koyulmaktadır. Buna göre şirketler, insan haklarına ilişkin kurumsal sorumlulukları uyarınca kendi faaliyetleri aracılığıyla olumsuz etki yaratmaktan veya bunlara katkıda bulunmaktan kaçınmalı ve böylesi etkilerin meydana gelmesi halinde bu etkileri ele almalı ve bu etkilere katkıda bulunmuş olmasalar dahi, iş ilişkileri aracılığıyla faaliyetleri, ürünleri veya hizmetleriyle doğrudan bağlantılı olan, insan hakları üzerindeki olumsuz etkileri önlemeli veya bunları hafifletmeye çalışmalıdır.³⁰¹

Çokuluslu İşletmeler Bildirgesi'nde çok uluslu şirketlerin faaliyet gösterdikleri ülkelerin genel politika amaçlarını bütünüyle dikkate almaları ve faaliyetlerinin ulusal hukuka uygun ve faaliyet gösterdikleri ülkenin kalkınma öncelikleri ve sosyal amaçları ve yapısı ile uyumlu olması gerektiği belirtilmektedir. Bu amaçla, çok uluslu işletmeler, hükümet ve uygun olduğu durumlarda ilgili ulusal işveren ve işçi örgütleri arasında istişareler gerçekleştirilmelidir.³⁰²

Çokuluslu İşletmeler Bildirgesi'nde çok uluslu şirketlerin yükümlülükleri istihdamın desteklenmesi, eğitim, çalışma ve yaşam koşulları, endüstriyel ilişkiler şeklinde dört başlıkta ele alınmıştır. Buna göre şirketler sosyal güvenlik sistemlerinin teşvik edilmesi, zorla ve zorunlu çalışma ve çocuk işçiliğinin etkili biçimde ortadan kaldırılması, fırsat ve muamele eşitliği ile istihdam güvenliğinin sağlanmasından sorumludur.³⁰³ Eğitim yükümlülüğü bakımından şirketlerden kendileri tarafından

³⁰⁰ Çokuluslu İşletmeler ve Sosyal Politikaya İlişkin İlkeler Üçlü Bildirgesi (MNE Bildirgesi), 03.03.2017, <https://www.ilo.org/tr/publications/cokuluslu-isletmeler-ve-sosyal-politikaya-iliskin-ilkeler-uclu-bildirgesi>.

³⁰¹ "Çokuluslu İşletmeler ve Sosyal Politikaya İlişkin İlkeler Üçlü Bildirgesi", s. 4.

³⁰² "Çokuluslu İşletmeler ve Sosyal Politikaya İlişkin İlkeler Üçlü Bildirgesi", s. 5.

³⁰³ "Çokuluslu İşletmeler ve Sosyal Politikaya İlişkin İlkeler Üçlü Bildirgesi", ss. 6-9.

istihdam edilen tüm seviyelerdeki çalışanlar için, uygun olduğu şekilde, işletmenin ihtiyaçlarını ve ülkenin kalkınma politikalarını karşılayabilmeleri amacıyla ilgili eğitimin verilmesini sağlamaları beklenmektedir. Şirketler, çalışma ve yaşam koşullarına ilişkin olarak ücretler, yan haklar, sağlık ve güvenlik hususlarında belli standartları sağlamalıdır. Son olarak, endüstriyel ilişkiler konusunda işçilerin örgütlenme özgürlüğü ve sendikalaşma ile toplu sözleşme yapma haklarına saygı göstermeli, bu hakları desteklemeli ve iş uyuşmazlıklarının çözümü konusunda etkili yöntemler sunmalıdırlar.³⁰⁴



³⁰⁴ “Çokuluslu İşletmeler ve Sosyal Politikaya İlişkin İlkeler Üçlü Bildirgesi”, ss. 6-16.

İKİNCİ BÖLÜM

AVRUPA HUKUKUNDA İNTERNET ŞİRKETLERİ VE İNSAN HAKLARINA DAİR HUKUKİ ÇERÇEVE

İnternet şirketlerinin insan hakları yükümlülükleri, küresel bir tartışma konusu olsa da Avrupa hukukunda önemli gelişmeler yaşanmaktadır. Özellikle Avrupa Birliği (AB) ve Avrupa Konseyi, internet şirketlerinin ifade özgürlüğü, mahremiyet, ayrımcılık yasağı gibi temel hakları koruma sorumluluğunu vurgulayan kapsamlı düzenlemeler ve standartlar geliştirmiştir.

İnternet şirketlerinin insan hakları yükümlülükleri bağlamında Avrupa Konseyi, doğrudan bu şirketlere yönelik özel bir düzenleme yapmamış olsa da ifade özgürlüğünün çevrimiçi korunmasına ilişkin çeşitli kararları ve Avrupa İnsan Hakları Mahkemesi (AİHM) içtihatları ile önemli bir rol oynamaktadır. Özellikle, ifade özgürlüğünün sınırlandırılması, nefret söylemi, özel hayatın gizliliği ve veri koruma gibi konularda AİHM kararları, internet şirketlerinin yükümlülüklerini belirlemede yol gösterici niteliktedir.

Avrupa Birliği'nde dijital hizmetlere yönelik hem tüm sektörleri kapsayan hem de sektörel düzenlemeler ortaya çıkmıştır. Avrupa Birliği'nde aracılardan sorumluluğuna ilişkin temel metin 2000/31/EC sayılı E-Ticaret Direktifi'dir. Direktif, aracılardan belli şartları yerine getirmeleri halinde sorumluluktan muaf tutmaktadır. Ancak bu muafiyet yalnızca içerik karşısında pasif role sahip araçlara ilişkindir. Günümüzde, internet araçlarının içerikler karşısında aktif bir tutum sergilemeleri ve Direktif'in dijital gelişmeler karşısındaki yetersizliği bir yandan AB'ye üye ülkelerde farklı yaklaşımların ortaya çıkmasına diğer yandan da yeni çalışmalar üzerinde yoğunlaşılmasına yol açmıştır. 2010'dan bu yana süren çalışmalar sonucunda, AB'de bir paradigma değişikliği olarak nitelendirilen Dijital Hizmetler Yasası ile Dijital Piyasalar Yasası şeklinde iki tasarı ortaya çıkmıştır. İnternet araçlarının sorumluluklarının da ele alındığı Dijital Hizmetler

Yasası, 27.10.2022 tarihinde Avrupa Birliği Resmî Gazetesi'nde yayımlanmış ve 16.11.2022 tarihinde yürürlüğe girmiştir.³⁰⁵

Bu bölümde, Avrupa Konseyi'nin çalışmaları ve AİHM içtihatları (I) ile Avrupa Birliği hukukunda (II) internet şirketlerinin insan hakları yükümlülükleri incelenecektir. Bu inceleme, internet şirketlerinin bölgesel düzeyde karşı karşıya kaldığı insan hakları sorunlarına ve bu sorunlara karşı geliştirilen çözüm mekanizmalarına ışık tutmayı amaçlamaktadır.

I. Avrupa Konseyi

Avrupa Konseyi'nde internet ortamında insan haklarının korunmasına yönelik çalışmalar, henüz internet kullanımının yaygınlaşmadığı dönemlere uzanmaktadır. Bu çalışmalar, internette insan hakları bakımından bir standart belirleme yanında uluslararası diyaloga değerli bir katkı oluşturmuştur. Tavsiye kararlar ve bildirilerde, internet yönetimine ilişkin genel ilkeler yanında devletlerin ve devlet dışı aktörlerin internet yönetimindeki sorumlulukları da ele alınmaktadır.

2003 yılında kabul edilen İnternette İletişim Özgürlüğüne İlişkin Bildiri'de³⁰⁶ internette ifade özgürlüğü ve bilgilerin özgürce dolaşımı esası kabul edilerek üye devletler için hepsi ifade özgürlüğü ile ilgili olan yedi prensip belirlenmiştir. Buna göre online içeriğe yönelik kısıtlamalar diğer içeriklere yönelik kısıtlamaların ötesine geçmemelidir; devletler internette yayınlanan içerikle ilgili olarak öz denetimi ve ortak düzenlemeyi teşvik etmelidir; devletler engelleme ya da filtreleme yoluyla internetteki bilgiler üzerinde önceden herhangi bir kontrol kurmamalıdır; devletler internet erişimini ayrımcı olmayan bir temelde desteklemelidir; internet üzerinden hizmet sunma özgürlüğü sağlanmalıdır; servis sağlayıcılarının internet içeriği üzerinde sadece sınırlı bir sorumluluğu olmalıdır ve kullanıcıların anonimlik yoluyla kimliklerini açıklamama kararına saygı duyulmalıdır. Bildiri'de servis sağlayıcıların sorumluluğuna ilişkin olarak, üye devletlerin hizmet sağlayıcılara, erişim sağladıkları, ilettikleri veya depoladıkları

³⁰⁵ 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, (2022), <https://eur-lex.europa.eu/eli/reg/2022/2065/oj>, (2.5.2023).

³⁰⁶ Declaration on Freedom of Communication on the Internet", Council of Europe, 28.05.2003, <https://rm.coe.int/16805dfbd5>, (2.5.2022).

internet içeriğini izleme ya da yasa dışı faaliyetlere işaret eden olguları veya koşulları aktif olarak arama gibi genel bir yükümlülük getirmemesini ve işlevleri ulusal hukuk tarafından tanımlandığı üzere bilgi iletmek veya internete erişim sağlamakla sınırlı olduğunda hizmet sağlayıcıların internetteki içerikten sorumlu tutulmamasını sağlaması gerektiği belirtilmektedir.³⁰⁷

2005 tarihli Bilgi Toplumunda İnsan Hakları ve Hukukun Üstünlüğü Bildirisi'nde, internetin giderek demokratik sürecin ayrılmaz bir parçası haline geldiği ve insan haklarının kullanılmasında daha geniş imkanlar sunabileceği ifade edilmiştir. Bildiride, ifade özgürlüğünün yanında internetin olumsuz etkilerinin daha görünür olduğu özel hayata saygı, adil yargılanma ile kanunsuz ceza olmaz ilkesi, mülkiyetin korunması, serbest seçimler ve toplanma özgürlüğü gibi diğer haklara da yer verilmiştir. Bildiride özel sektörün internet yönetimindeki etkisi kabul edilerek özel sektör aktörleri, hükümetler ve sivil toplumla işbirliği içinde, bilgi ve iletişim teknolojilerinin kötüye kullanımı veya yasadışı amaçlarla kullanımından kaynaklanan insan haklarına yönelik tehdit, risk ve kısıtlamaları önleme ve bunlara karşı koymak için önlemler almaya, bu teknolojiler aracılığıyla insan haklarının geliştirilmesi için davranış kuralları ile diğer öz düzenleme biçimlerini oluşturmaya ve bunların kapsamını daha da genişletmeye davet edilmektedir.³⁰⁸

Özel aktörlerin internet yönetimindeki etkileri, 2007 yılında kabul edilen Yeni Bilgi ve İletişim Ortamında İfade ve Bilgi Özgürlüğünün Desteklenmesine İlişkin Tavsiye Kararı'nda bir kez daha kabul edilmiştir.³⁰⁹ Buna göre, özel aktörler; i. evrilen etik rollerini ve sorumluluklarını kabul etmeli ve bunlarla ilgili anahtar eylem ve kararlarını, bireylerin haklarına ve özgürlüklerine etki eden konularda, gerektiğinde

³⁰⁷ Ibid., m. 6.

³⁰⁸ Declaration of the Committee of Ministers on human rights and the rule of law in the Information Society (CM(2005)56), Council of Europe, 13.05.2005, https://www.coe.int/t/dgap/goodgovernance/activities/public_participation_internet_governance/Declaration-on-Information-Society/011_DeclarationFinal%20text_en.asp, (2.5.2022).

³⁰⁹ Recommendation CM/Rec(2007)11 of the Committee of Ministers to member states on promoting freedom of expression and information in the new information and communications environment, 26.09.2007, [https://search.coe.int/cm/#{%22CoEIdentifier%22:\[%2209000016805d4d0e%22\],%22sort%22:\[%22CoEValidationDate%20Descending%22\]}](https://search.coe.int/cm/#{%22CoEIdentifier%22:[%2209000016805d4d0e%22],%22sort%22:[%22CoEValidationDate%20Descending%22]}), (4.3.2022).

gözden geçirme ve uyarlama konusunda işbirliği yapmalı ve ii. uygun olduğunda, yeni, açık, şeffaf ve hesap verebilir öz düzenleme biçimleri geliştirmelidir.³¹⁰

Bu hususlar aynı yıl kabul edilen İnternetin Kamu Hizmeti Olarak Değerini Geliştirmeye Yönelik Önlemler Hakkında Tavsiye Kararı'nda, internetin kamusal niteliğine de dikkat çekilerek yeniden ifade edilmiştir.³¹¹

2008 yılında kabul edilen İnternet Filtreleri ile İlgili Olarak İfade ve Bilgi Özgürlüğüne Saygının Geliştirilmesine Yönelik Önlemlere İlişkin Tavsiye Kararı'nda, özel aktörlerden kaynaklanabilecek ifade özgürlüğü kısıtlamaları “özel sansür” olarak nitelendirilmiş ve özel sansürün önlenmesi bakımından devletlere yönelik tavsiyelere yer verilmiştir. Buna göre özel aktörler, şeffaflığı özendirmek ve diğerlerinin yanı sıra bilgi alma ve verme hakkı ile ilgili olarak içerik ve hizmetlere erişimin engellenmesi ve bunların filtrelenmesi konusunda teknoloji ve hizmetlerin bireysel kullanıcılarına bilgi, rehberlik ve yardım sağlamak için ortak standartlar ve stratejiler geliştirmeye teşvik edilmelidir.³¹²

Avrupa Konseyi, 2011 yılında İnternet Yönetişim İlkelerine İlişkin Bildiri ile internet yönetişimine ilişkin on temel ilke kabul etmiş ve özel sektör aktörlerini de sorumluluklarını yerine getirirken bu prensipleri benimsemeye davet etmiştir. Buna göre özel sektör aktörleri, faaliyet ve işlemlerinin yanı sıra yeni teknoloji, hizmet ve uygulamaların tasarımı insan haklarını ve temel özgürlükleri tanımalı ve desteklemeli; teknik ve operasyonel konularda öncü rollerini sürdürürken, şeffaflığı sağlamalı ve kamu

³¹⁰ Ibid.

³¹¹ Recommendation CM/Rec(2007)16 of the Committee of Ministers to Member States on Measures to Promote the Public Service Value of the Internet, 07.11.2007, [https://search.coe.int/cm/#{%22CoEIdentifier%22:\[%2209000016805d4a39%22\],%22sort%22:\[%22CoEValidationDate%20Descending%22\]}](https://search.coe.int/cm/#{%22CoEIdentifier%22:[%2209000016805d4a39%22],%22sort%22:[%22CoEValidationDate%20Descending%22]}), (5.5.2022).

³¹² Recommendation CM/Rec(2008)6 of the Committee of Ministers to Member States on Measures to Promote the Respect for Freedom of Expression and Information with Regard to Internet Filters, 26.03.2008, https://www.coe.int/en/web/freedom-expression/committee-of-ministers-adopted-texts/-/asset_publisher/aDXmrol0vvsU/content/recommendation-cm-rec-2008-6-of-the-committee-of-ministers-to-member-states-on-measures-to-promote-the-respect-for-freedom-of-expression-and-informati, (5.5.2022).

politikası üzerinde etkisi olan eylemler için küresel topluma karşı hesap verebilir olmalıdır.³¹³

Buraya kadarki kısımda, Avrupa Konseyi'nin genel olarak çevrimiçi insan haklarının korunmasına ilişkin bildiri ve tavsiye kararları ele alınmıştır. Söz konusu belgelerde, çevrimdışı hakların çevrimiçi olarak da korunması gerektiği esas alınmış, çevrimiçi insan haklarının korunmasında devletler yanında özel aktörlerin de rollerine dikkat çekilmiştir. Bu noktada devletlere; özel aktörleri insan haklarına uygun hareket etmeleri konusunda teşvik etmeleri; özel aktörlere de öz düzenlemeler yoluyla şeffaf ve hesap verebilir şekilde davranmaları tavsiye edilmiştir. İlerleyen dönemde Konsey, özel aktörlerin internet yönetimindeki belirleyici rollerini dikkate alan ve doğrudan özel sektör aktörlerine yönelik tavsiye kararları da almıştır. Bu başlık altında, söz konusu kararlar ayrıca ve ayrıntılı olarak ele alınacaktır.

A. Gelişen Normatif Çerçeve: İnternet Platformları ve Sorumlulukları

İnternet yönetiminin çok paydaşlı yönü Avrupa Konseyi'nin erken dönem çalışmalarında dahi kabul edilmiştir. Bu kabulde birlikte internet yönetişimine ilişkin bildiri ve kararlarda, paydaşlardan biri olan özel aktörlere ilişkin olarak, hem özel aktörlerin hak ve özgürlüklerinin korunması hem de hak ve özgürlüklerin özel aktörlere karşı korunmasına yönelik hususlara yer verilmiştir. İnternetin gittikçe artarak kamusal hayatın merkezi haline gelmesiyle Konsey çalışmalarında, doğrudan özel aktörleri, yani internet şirketlerini konu alan ayrıntılı kararlar alınmaya başlanmıştır. Konsey çalışmalarında, mevcut insan haklarının ve temel özgürlüklerin gerek çevrimdışı (*offline*) gerek çevrimiçi (*online*) olarak eşit bir biçimde uygulanmasını sağlamak anlayışının etkisiyle teknolojik gelişmelerin insan haklarına etkisine yönelik çalışmaların yoğunluk kazandığı görülmektedir. Gittikçe artan bu ilginin temelinde internetin kamu hizmeti değeri taşıması yatmaktadır. İnsanlar, topluluklar, kamu yetkilileri ve özel kuruluşlar faaliyetleri için internete ihtiyaç duyarlar ve internet hizmetlerinin erişilebilir, ayırım gözetmeksizin ve makul bir ücret karşılığı sağlanabilir, emniyetli, güvenilir ve sürekli olması konularında geçerli bir beklentileri vardır. Dahası, hiç kimse interneti kullanırken

³¹³ Declaration by the Committee of Ministers on Internet Governance Principles, 21.09.2011, [https://search.coe.int/cm/#{%22CoEIdentifier%22:\[%2209000016805cc2f6%22\],%22sort%22:\[%22CoEValidationDate%20Descending%22\]}](https://search.coe.int/cm/#{%22CoEIdentifier%22:[%2209000016805cc2f6%22],%22sort%22:[%22CoEValidationDate%20Descending%22]}), (5.10.2022).

- Ticari işletmelerin insan hakları ihlallerine karşı koruma sağlamak için uygun adımların atılması,
- Tüm ticari işletmelerin, kendi ulusal yetki alanları dahilinde ve ötesinde, faaliyetleri boyunca insan haklarına saygı göstermesini teşvik edecek politika ve önlemlerin formüle edilmesi ve uygulanması,
- Bu tür suistimallerin kendi bölgelerinde ve/veya yetki alanlarında meydana gelmesi durumunda, etkilenenlerin etkili çözüme erişebilmesini sağlamak için uygun adımların atılması,
- BM Yol Gösterici İlkelerinin uygulanmasına ilişkin ulusal eylem planlarının geliştirilmesi hususlarında çağrıda bulunulmuştur.³¹⁶

2014 yılında kabul edilen Birleşmiş Milletler İş Dünyası ve İnsan Haklarına Dair Rehber İlkeler Hakkında Bakanlar Komitesi Bildirisi'nin ardından, Bakanlar Komitesi tarafından üye devletlere yönelik İnsan Hakları ve İş Dünyasına ilişkin CM/Rec (2016)3 Tavsiye Kararı kabul edilmiştir.³¹⁷ Bu Tavsiye Kararı'nın temel amacı, devletlerin "*iş ve insan hakları alanında küresel olarak kabul edilen BM İş ve İnsan Haklarına İlişkin İlkeleri etkili bir şekilde uygulamalarını*" sağlamaktır. Tavsiye Kararı'nda, devletin insan haklarını koruma yükümlülüğünün yanı sıra şirketlerin insan haklarına saygı yükümlülüğünü kolaylaştırabilecek eylem türlerine odaklanılmaktadır. Bu tür eylemler, devletlerin "*şirketlerin faaliyetlerinde insan haklarına ilişkin denetimleri uygulamalarını teşvik etmek veya gerektiğinde zorunlu kılmak için gereken tedbirleri uygulamalarını*" ve "*şirketlerin ilgili faaliyetlerde insan haklarına ilişkin denetimleri gerçekleştirmelerini*" içermektedir.³¹⁸ Devletler ayrıca, herkesin şirketlerin faaliyetlerinden kaynaklanan insan hakları ihlalleri konusunda mahkemelere ve çözümlere erişimini sağlamalıdır.³¹⁹

Tavsiye Kararı'nda, BM Rehber İlkeler'in Avrupa Konseyi'ne üye devletlerde etkili bir şekilde uygulanmasına yönelik kararlılık yeniden ifade edilmiş ve üye devletlere Tavsiye Kararı'nın ekinde belirtilen tavsiyeler ve ilkeler çerçevesinde mevzuatlarını ve uygulamalarını gözden geçirmeleri çağrısında bulunulmuştur. Yetmiş maddeden oluşan

³¹⁶ Ibid., para. 10.

³¹⁷ Recommendation CM/Rec(2016)3 of the Committee of Ministers to Member States, Council of Europe, <https://edoc.coe.int/en/fundamental-freedoms/7302-human-rights-and-business-recommendation-cmrec20163-of-the-committee-of-ministers-to-member-states.html>, (23.10.2024).

³¹⁸ Ibid., para. 20.

³¹⁹ Ibid., para. 31.

ekte, Birleşmiş Milletler Rehber İlkeler'in uygulanması, devletin insan haklarını koruma görevi, insan haklarına saygı konusunda kurumsal sorumluluğu etkinleştirmek için devlet eylemi, çözüm yollarına erişim ve işçiler, çocuklar, yerli haklar ile insan hakları savunucuları için ek korumalar hususlarında ayrıntılı tavsiyelere yer verilmiştir.³²⁰

2. İnternet Şirketlerinin Yükselen Rolü ve Artan Sorumlulukları

Avrupa Konseyi bünyesinde internet ortamında özellikle ifade özgürlüğü, bilgiye erişim, toplanma özgürlüğü, siber suçlardan korunma, özel hayatın korunması ve kişisel verilerin korunması haklarına yönelik çalışmalar dikkat çekmektedir.

Bu çalışmalardan ilk ikisi, 2008 yılında kabul edilen Çevrimiçi Oyun Sağlayıcıları İçin Kılavuz İlkeler³²¹ ile İnternet Servis Sağlayıcıları (ISP) İçin Kılavuz İlkeler'dir.³²² Çevrimiçi Oyun Sağlayıcıları İçin Kılavuz İlkeler'de, oyun tasarımcıları ve yayıncılarına özellikle çocukları hedef alırken şiddetin tasvir edilmesine, ırkçı veya yabancı düşmanı içeriğe ve uyuşturucu kullanımı gibi suç teşkil eden veya zararlı davranışları savunan içeriğe özel dikkat göstermeleri; çocukları ve gençleri hedef alan oyunlar başta olmak üzere, kullanıcılar tarafından oluşturulan içeriğin belirli bir süre kullanılmadığında otomatik olarak kaldırılması için mekanizmalar geliştirerek, şimdi veya daha sonraki yaşamlarında onurlarına, mahremiyetlerine ve güvenliklerine zarar gelmesini önlemeleri; oyuncular tarafından oluşturulan içeriğin kaldırılmadan önce polis ve/veya yetkili makamla irtibata geçilerek hukuka aykırılığının doğrulanması şeklinde tavsiyelerde bulunulmuştur. ISP'ler İçin Kılavuz İlkeler'de de, servis sağlayıcılara çocuklar başta olmak üzere, kullanıcıları internetin potansiyel riskleri konusunda bilgilendirmeleri; kullanıcıların mahremiyetini ve içeriğin gizliliğini korumak için uygun prosedürler ve teknolojiler oluşturmaları; yasalara uygun belirli ve meşru amaçlar için gerekli olmadıkça kullanıcılar hakkında bilgi toplamaktan veya saklamaktan kaçınmaları gibi hem kullanıcı haklarına saygı göstermeleri hem de bu hakları korumalarına yönelik tavsiyelerde bulunulmuştur. Kılavuz İlkeler'e göre örneğin, içerik ve trafik verilerinin izlenmesi ancak

³²⁰ "Recommendation CM/Rec(2016)3 of the Committee of Ministers to Member States, Council of Europe", ss. 8-27.

³²¹ Council of Europe, "Human Rights Guidelines for Online Games Providers", 2008, [https://rm.coe.int/16805a39d3#:~:text=Games%20designers%20and%20publishers%20are,the%20right%20to%20freedom%20of,\(5.12.2023\).](https://rm.coe.int/16805a39d3#:~:text=Games%20designers%20and%20publishers%20are,the%20right%20to%20freedom%20of,(5.12.2023).)

³²² Council of Europe, "Human Rights Guidelines for Internet Service Providers", 2008.

yasaların tanımladığı belli durumlarda ve meşru bir yetkili mercinin özel emriyle mümkün olabilmelidir. Öte yandan, ISP'ler tarafından yapılacak filtreleme ya da engelleme girişimleri meşru, orantılı ve şeffaf olmalıdır ve ancak içeriğin yasadışılığı teyit edildikten sonra yapılmalıdır.³²³

Avrupa Konseyi, bu kılavuzların yayımlanmasından birkaç yıl sonra, internet şirketlerinin insan hakları sorumluluklarını ele alan Bakanlar Komitesi'nin Üye Devletlere Arama Motorları Bağlamında İnsan Haklarının Korunmasına İlişkin Tavsiye Kararı³²⁴ ve Bakanlar Komitesi'nin Üye Devletlere Sosyal Ağ Hizmetlerinde İnsan Haklarının Korunmasına İlişkin Tavsiye Kararı³²⁵ yayımlamıştır.

Çıkış noktası, arama motorlarının bilgi toplumundaki rolleri olan Arama Motorları Bağlamında İnsan Haklarının Korunmasına İlişkin Tavsiye Kararı'nda arama motorlarının temel hak ve özgürlükler üzerindeki etkileri kapsamlı bir şekilde ele alınmış ve bu aktörlere yönelik detaylı tavsiyelerde bulunulmuştur. Tavsiye Kararı'nda arama motorlarının internet üzerindeki içeriğin erişilebilir kılınması ve internetin kamu için faydalı hale getirilmesi açısından önem taşıdığı, bu bakımdan arama motorlarının web üzerinde açık bir şekilde bulunan ve kitlelere ulaşması amaçlanan bilgileri serbestçe taramasına ve indekslemesine izin verilmesinin gerekli olduğu belirtilmiştir. Ayrıca, internet yönetiminin öne çıkan aktörlerinden olan arama motorlarının temel hak ve özgürlükler üzerindeki tehdit edici rolü de ele alınmış; bu noktada üye devletlere arama motorlarıyla ilgili olarak ifade özgürlüğü, bilgiye erişim ve diğer insan hakları ve temel

³²³ Ibid., m. 20.

³²⁴ Recommendation CM/Rec(2012)3 of the Committee of Ministers to Member States on the Protection of Human Rights with Regard to Search Engines, 04.04.2012, https://www.coe.int/en/web/freedom-expression/committee-of-ministers-adopted-texts/-/asset_publisher/aDXmrol0vvsU/content/recommendation-cm-rec-2012-3-of-the-committee-of-ministers-to-member-states-on-the-protection-of-human-rights-with-regard-to-search-engines-adopted-by, (12.10.2023).

³²⁵ Recommendation CM/Rec(2012)4 of the Committee of Ministers to Member States on the Protection of Human Rights with Regard to Social Networking Services, 04.04.2012, https://www.coe.int/en/web/freedom-expression/committee-of-ministers-adopted-texts/-/asset_publisher/aDXmrol0vvsU/content/recommendation-cm-rec-2012-4-of-the-committee-of-ministers-to-member-states-on-the-protection-of-human-rights-with-regard-to-social-networking-service, (12.10.2023).

özgürlüklerin korunmasına yönelik tutarlı stratejiler geliştirmeleri ve onları teşvik etmeleri tavsiye edilmiştir.³²⁶

Arama motorlarıyla ilgili önemli risklerden biri, kullanıcıların genellikle sınırlı sayıda baskın arama motorunu kullanma eğiliminde olmalarına bağlı olarak bilgi kaynaklarına ve çeşitliliğine erişimde haksız bir durumun ortaya çıkabilecek olmasıdır. Konsey bu noktada, arama motorlarından iş modelleri ya da karar alma süreçleri hakkında tam bir şeffaflık beklenmesinin rekabet açısından uygun olmayabileceğini değerlendirmekle birlikte devletlere arama motoru sağlayıcılarını; i) arama sonuçlarının seçilmesi ve sıralanmasına uygulanan genel kriterler ve süreçler konusunda şeffaflığı artırmaya, ii) arama sonuçları ile "kendi içerik" teklifleri de dahil olmak üzere her türlü ticari iletişim, reklam veya sponsorlu çıktılar arasında net bir ayrım yapmaya ve iii) arama motoru hizmetlerinin kamusal değer boyutu, arama motoru pazarının giderek yoğunlaşması ve arama sonuçlarının kötüye kullanılması, manipüle edilmesi ve kısıtlanması riski gibi konuları ele almak üzere arama motorları için dinamik pazar üzerine araştırmaya teşvik etme hususlarında tavsiyede bulunmaktadır.³²⁷

Tavsiye Kararı'nda, özel hayat ve kişisel verilerin korunması hakkı ayrı bir başlıkta ele alınmıştır. Bu başlık altında, büyük miktarda veriyi işleyen arama motorlarının dijital görüntüler, ses ve video içeriği gibi sesli ve görsel verilerin yaygınlaşmasıyla ayrı bir boyut kazandığı vurgulanmıştır. Tavsiye Kararı'nda, devletlerin arama motoru sağlayıcılardan kişisel veri toplamının en aza indirilmesini; saklama sürelerinin işlemenin meşru ve belirtilen amaçları için gerekli olan süreden daha uzun olmamasını; bireylerin kişisel verilerinin işlenmesi ve haklarını kullanmaları konusunda, veri konusuna uygun ve anlaşılır bir biçimde bilgilendirilmesini sağlamalarını talep etmeleri tavsiye edilmiştir. Ayrıca, kullanıcı verilerinin aktarılmasına ilişkin olarak da bu taleplerin uygun yasal prosedürlere dayanması, veriler kamu makamları veya özel taraflara ifşa edilmeden önce güçlü yasal güvenceler ve yasal süreç gerekliliklerine uyulması gerektiği belirtilmiştir.³²⁸

³²⁶ "Recommendation CM/Rec(2012)3 of the Committee of Ministers to Member States on the Protection of Human Rights with Regard to Search Engines", m. 7.

³²⁷ Ibid., m. 4.

³²⁸ Ibid., m. 11.

Tavsiye Kararı'nda ifade özgürlüğüne yönelik müdahale biçimlerinden olan filtreleme ve dizinden çıkarma hususlarına yönelik de önemli tespit ve tavsiyelere yer verilmiştir. Arama motorları web üzerindeki bilgilere serbestçe erişimin ön koşulu olarak kabul edildiğinden, arama motorları tarafından internet içeriğinin filtrelenmesi ve engellenmesi, sağlayıcıların ve kullanıcıların bilgi dağıtma ve bilgiye erişme haklarına yönelik risk teşkil etmektedir. Bu bakımdan, arama motorları bir yargı ya da yetkili makam kararı olmaksızın ağlarını ve hizmetlerini proaktif olarak izlemeye veya herhangi bir önleyici (*ex ante*) filtreleme veya engelleme faaliyeti yapmaya zorlanmamalıdır.³²⁹ Söz konusu müdahaleler şeffaf ve dar kapsamlı olmalı, sürekli olarak gözden geçirilmelidir. Belirli anahtar kelimeler için tüm arama sonuçlarının engellenmesi, arama motorları için öz ve ortak düzenleyici çerçevelere dahil edilmemeli veya teşvik edilmemelidir. Öz ve ortak düzenleyici rejimler, bireylerin ifade özgürlüğünü ve herhangi bir medya aracılığıyla bilgi, fikir ve içerik arama, alma ve verme hakkını engellememelidir.³³⁰

Sosyal Ağ Hizmetlerinde İnsan Haklarının Korunmasına İlişkin Tavsiye Kararı'nda ise ifade özgürlüğü ve özel hayata saygı haklarının korunmasına ilişkin tavsiyeler, bu defa sosyal ağ, yaygın ifadesiyle sosyal medya sağlayıcıları merkeze alınarak belirlenmiştir. Tavsiye Kararı uyarınca, bireyler arasındaki ifade ve iletişimin yanı sıra doğrudan kitle iletişiminin veya toplu iletişimin aracı olan sosyal ağ hizmetleri, insan haklarını mümkün kılmakta ve demokrasilerde katalizatör işlevi görmektedir. Bununla birlikte, ifade ve bilgi edinme özgürlüğünün yanı sıra özel hayat hakkı ve insan onuru, ayrımcı uygulamaları da barındırabilecek sosyal ağ hizmetlerinde tehdit altında olabilir. Bu bağlamda, sosyal ağ sağlayıcılarının insan hakları ve hukukun üstünlüğüne saygı göstermeleri gerektiği belirtilerek bu yönde bazı hedefler ortaya konulmuş; devletlere sosyal ağ hizmetleri sağlayıcıları ile iletişime geçerek belirtilen hedeflere uyulmasına katkıda bulunmak amacıyla öz ve ortak düzenleyici mekanizmalar oluşturmaları tavsiye edilmiştir.³³¹

³²⁹ Ibid., m. 13.

³³⁰ Ibid., m. 15, 16.

³³¹ "Recommendation CM/Rec(2012)4 of the Committee of Ministers to Member States on the Protection of Human Rights with Regard to Social Networking Services", m. 1-6.

Bu hedefler, Tavsiye Kararı'nda üç temel başlıkta ele alınmıştır: I. Kullanıcıların sosyal ağlarla başa çıkmasına yardımcı olmak için gereken temel bilgiler ve önlemler, II. Çocukların ve gençlerin zararlı içerik ve davranışlara karşı korunması, III. Kişisel veriler ve sosyal ağlara güven. Buna göre sosyal ağlarda kullanıcılar, paylaştıkları bilgilerin uygun şekilde işleneceğinden emin olmalı, bu bilgilerin kamuya açık mı yoksa özel mi olduğunu bilmeli ve bilgiyi kamuya açıklamayı seçmenin doğuracağı sonuçların farkında olmalıdır.³³² Öte yandan sosyal ağlar, çocuk ve gençlerin kişilik ve kimliklerinin gelişiminin ve tartışmalara ve sosyal etkinliklere katılımlarının bir parçası haline geldiğinden, bu gruplar kırılganlıkları dolayısıyla korunmalıdır.³³³ Tavsiye Kararı'nda bu yükümlülük çerçevesinde devletlere, sosyal ağ sağlayıcıların kullanıcılara hukuka aykırılık teşkil edebilecek içerikler hakkında bilgi sağlamalarını; Avrupa İnsan Hakları Sözleşmesi çerçevesinde uygunsuz olarak nitelendirilebilecek içerikler bakımından politikalar geliştirmelerini; söz konusu uygunsuz ve hukuka aykırı içeriklerin bildirilmesine yönelik erişilebilir mekanizmalar geliştirmelerini; siber zorbalık ve siber tacizin önlenmesine ilişkin etkili yöntemler geliştirmelerini temin etme tavsiye edilmektedir.³³⁴ Son olarak, kişisel veriler ve sosyal ağlarda güven hedefi bakımından sosyal ağ hizmet sağlayıcıların kişisel verileri, hangi meşru ve belirli amaçlarla topladırsa o amaçla sınırlı olarak, kesinlikle gerekli olduğu kadar ve mümkün olan en kısa süre için işlemleri gerektiği belirtilmektedir. Tavsiye Kararı uyarınca sosyal ağlar, gizlilik ve güvenlik önlemleri bakımından en iyi uygulamaları sağlamalı; kullanıcıların haklarını etkili bir şekilde kullanabilmelerini temin etmeli; hassas verilerin korunmasına özel olarak önem vermeli; kullanıcı verilerini, hukuka aykırı üçüncü taraf erişimlerine karşı korumalı; tasarım yoluyla gizlilik ilkesini uygulamalı; sosyal ağ kullanıcısı olmayanları kullanıcıların hukuka aykırı ya da kişilik haklarını ihlal eden eylemlerinden korumalı; kişisel verilerin kolluk görevi amacıyla işlenmesinde Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesine uygun hareket etmeli; kullanıcıları uygulanacak hukuk ve yargı yetkisi konusuna bilgilendirmeli ve son olarak kullanıcıların insan haklarına yönelik tehditler konusunda bilgi sahibi olmalarını ve gerektiğinde zararlarını tazmin edebilmelerini temin etmelidir.³³⁵

³³² Ibid., m. 3.

³³³ Ibid., m. 5,6.

³³⁴ Ibid., m. 10.

³³⁵ Ibid., m. 15.

Tavsiye kararlarının ardından Bakanlar Komitesi'nin 16 Nisan 2014 tarihli toplantısında kabul edilen İnternet Kullanıcıları İçin İnsan Hakları Rehberi'nde³³⁶ internette insan hakları ve internet şirketlerinin insan hakları sorumlulukları kapsamlı bir şekilde ele alınmıştır. Rehber'de internet şirketlerinin insan hakları sorumluluklarına ilişkin genel prensipler yanında internet bağlamında, pratikte hak ve özgürlüklerin neler olduğu, bu hak ve özgürlüklere nasıl bel bağlanabileceği ve bunların nasıl kullanılabilceği ve bunun yanı sıra, hukuksal yollara nasıl başvurulabileceğiyle ilgili bilgiler sunulmaktadır.

İnternet ortamında insan haklarının korunabilmesi internette hakların ve özgürlüklerin kullanılmasının değerlendirilmesini, düzenli aralıklarla gözden geçirilmesini ve yerine göre, söz konusu hak ve özgürlüklerin önündeki kısıtlamaların kaldırılmasını gerektirmektedir. Söz konusu kısıtlamalarda yasa ile öngörülme, demokratik bir toplumda geçerli bir amaca ulaşılması için gerekli olma ve bu geçerli amaçla orantılı olma şartları sağlanmalıdır.³³⁷

İnternet Kullanıcıları için İnsan Hakları Rehberi'ne göre internet, temel hak ve özgürlüklerin kullanımı ile demokrasiye katılımı önemli bir vasıta olduğundan herkesin internete erişim hakkı ve bu konuda ayırım gözetilmemesi sağlanmalıdır. Buna göre internet hizmet sağlayıcıları ya da online içerik ve hizmet sağlayıcıları gibi internet şirketleri, toplumsal cinsiyet, ırk, renk, dil, din veya inanç, siyasi veya diğer görüş, ulusal veya sosyal köken, ulusal bir azınlıkla bağlantı, mülk, doğum veya etnik köken, yaş veya cinsel yönelim gibi sebeplerle kullanıcılar arasında ayırım yapmamalıdır.³³⁸

Rehber'de, internet şirketlerinin ifade ve bilgi özgürlüğü bakımından insan haklarına saygı gösterme ve kullanıcı taleplerine cevap verecek mekanizmalar sağlama konusunda kurumsal sorumlulukları olduğu belirtilmektedir. Bununla birlikte, sosyal ağlar gibi online hizmet sağlayıcılarının içerikle ilgili politikaları nedeniyle belirli tür içerik ve davranışları kısıtlayabilecekleri, internet kullanıcıları tarafından yaratılan ve sağlanan içeriği sitelerinden kaldırabilecekleri, hatta hizmet koşullarına aykırılık

³³⁶ "Recommendation CM/Rec(2014)6 of the Committee of Ministers to Member States on a Guide to Human Rights for Internet Users".

³³⁷ Ibid., s. 1.

³³⁸ Ibid., s. 8.

gerekçesiyle kullanıcı hesaplarını kapatabilecekleri de kabul edilmektedir.³³⁹ Rehber’de bu kısıtlamalarla ilgili olarak söz konusu hizmet bakımından yasa dışı ya da uygunsuz içeriklerin neler olduğunu, bu içeriklerin varlığı halinde hangi önlemlerin alınabileceğini, muhtemel kısıtlamaların neler olduğu gibi hususlarda kullanıcıların bilgilendirilmesi gerektiğinin altı çizilmiştir. İçeriğin kaldırılması ve kullanıcı hesaplarının kapatılması bakımından, internet kullanıcılarına bu tedbirlerin hangi nedenlerle ve neye dayanılarak alındığı hususunda erişilebilir açık ve kesin bilgiler verilmelidir. Bu bilgilere söz konusu tedbirlere dayanak teşkil eden yasal hükümler ve tedbirin amacının orantılılığının ve geçerliliğinin değerlendirilmesinde kullanılan diğer unsurlar da dahildir. İnternet kullanıcıları aynı zamanda içeriğin kaldırılması ve/veya hesabın kapatılmasının makul bir süre içinde yargı denetimine tabi tutulmasını talep edebilmeli ve alınacak karara yetkili bir idari ve/veya yargı makamı nezdinde itiraz etme imkanına sahip olmalıdır.³⁴⁰

İnternet şirketleri, ifade özgürlüğü bakımından çevrimiçi içeriklerden de sorumludur. Nefret söylemiyle ve şiddeti veya ayrımcılığı tahrik eden diğer içeriklerle mücadele etme konusunda bir taahhütte bulunmaları, şirketlerin kurumsal sorumluluklarının bir parçası olarak kabul edilmektedir. İnternet servis sağlayıcıları ırkçı, yabancı düşmanı, Yahudi karşıtı, kadın düşmanı, cinsel olarak veya farklı bir temelde ayrımcılık içeren duyguların etkisiyle kullanılan ifadeler ve yayın sorumlularının verdikleri cevaplar konusunda dikkatli olmalı; internet kullanıcılarına yasa dışı sayılabilecek içerik veya görüş ve/veya davranışları bildirmeleri konusunda yardımcı olmalıdır.³⁴¹

Rehber’de özel olarak ele alınan bir diğer özgürlük toplanma, örgütlenme ve katılım özgürlüğüdür. Kullanıcılar internet ortamında topluluklar kurabilir, bunlara katılabilir ve interneti barışçıl protestolar için kullanabilirler. Dolayısıyla, internet şirketleri bu haklar bakımından da haksız kısıtlamalardan kaçınmalıdır.

İnternet ortamı, özel hayata yönelik farklı müdahale biçimlerini beraberinde getirdiğinden mahremiyet ve verilerin korunmasına ilişkin tasviyeler önem taşımaktadır. Rehber’de internet ortamında internet tarayıcıları, elektronik posta, mesajlar, internet

³³⁹ Ibid., s. 33.

³⁴⁰ Ibid., s. 34.

³⁴¹ Ibid.

üzerinden sesle iletişim protokolleri, sosyal ağlar, arama motorları ve “cloud” veri saklama hizmetleri gibi hizmetler sırasında kişisel verilerin düzenli aralıklarla işleme tabi tutulduğu ifade edildikten sonra özel şirketlerin, bu işleme faaliyeti sırasında belirli kurallara ve prosedürlere saygı gösterme yükümlülüğü olduğu belirtilmiştir. Buna göre, kişisel veriler sadece yasalar tarafından öngörüldüğünde veya ilgili kişinin rızasıyla işleme tabi tutulmalıdır. Kullanıcılar, hangi kişisel verilerin işleme tabi tutulduğu ve/veya üçüncü taraflara aktarıldığı; bu işlemin ne zaman, kimin tarafından ve ne amaçla yapıldığı konusunda bilgilendirilmelidir. Öte yandan kullanıcılar, önceden bilgilendirildikleri istisnai haller dışında gözetleme ve dinleme tedbirine maruz bırakılmamalıdır.³⁴²

Rehber’de, internet ortamında çocuk ve gençlere yönelik de bilgilendirmede bulunmaktadır. Bu kapsamda, çocuk ve gençlerin yasadışı online içerik ve davranışlar (örneğin online taciz) ve aynı zamanda yasa dışı olduğu iddia edilen içeriğin ilgili makamlara bildirilebileceği konusunda bilgilendirilmesi ve internette cinsel istismar ve tacizle ve diğer siber suçlarla ilgili olarak, fiziksel, zihinsel ve ahlaki sağlığa yönelik müdahalelere karşı korunmaları gerekliliği ortaya koyulmuştur.³⁴³

Son olarak, internet şirketlerinin internet kullanıcılarının etkili yasal yollara erişimine ilişkin sorumlulukları da ele alınmıştır. İnternet hizmet sağlayıcıları ya da online içerik ve hizmet sağlayıcıları gibi internet şirketleri internet kullanıcılarını kullanıcı hak ve özgürlükleri ile bunlara ilişkin yasal çözümler konusunda bilgilendirmelidir. Bu bilgilendirmeye, haklara müdahaleyle ilgili bildirim yapma ve şikâyetle bulunma ile hakların telafisi konusunda bilgiye kolayca erişim de dahildir.³⁴⁴

İnternet Kullanıcıları İçin İnsan Hakları Rehberi’nde internet şirketlerinin insan hakları sorumlulukları, bu şirketlerin rolleri bakımından herhangi bir ayırım yapılmaksızın genel olarak ele alınmıştır. Bununla birlikte, bazı internet şirketlerinin internetin yönetimindeki rolleri, bu şirketlerin sorumluluklarını diğerlerinden ayrı şekilde ele alınmasını gerektirmektedir. Bakanlar Komitesi’nin 2008 yılında kabul ettiği İnternet Aracılarının Rol ve Sorumluluklarına İlişkin Tavsiye Kararı’nın³⁴⁵ çıkış noktası da

³⁴² Ibid., s. 10.

³⁴³ Ibid., ss. 11-12.

³⁴⁴ Ibid., s. 12.

³⁴⁵ Recommendation CM/Rec(2018)2 of the Committee of Ministers to Member States on the Roles and Responsibilities of Internet Intermediaries”, Council of Europe, 07.03.2018,

internet aracılarının bu özel durumlarıdır. Nitekim, Tavsiye Kararı'nda öncelikle, internetin temel hak ve hürriyetler üzerindeki etkisi ve internet aracılarının internetin yönetimindeki rolleri üzerinde durulmuştur. Buna göre internet, halkın bilgi arama, alma ve verme yeteneğini geliştirerek, ifade özgürlüğü hakkı açısından özellikle önemli bir rol oynamıştır. Ayrıca, demokratik bir yönetimde toplanma ve örgütlenme özgürlüğü ve eğitim hakkı gibi Avrupa İnsan Hakları Sözleşmesi ve protokolleri tarafından korunan diğer hakların kullanılmasını ve bilgi ve kültüre erişimin yanı sıra kamusal ve siyasi tartışmalara katılımı sağlamaktadır.

İnternet Aracılarının Rol ve Sorumluluklarına İlişkin Tavsiye Kararı'nda internetin temel ve hak özgürlükler bakımından yarattığı olumsuz etkiye de dikkat çekmiştir. İnternet, mahremiyetle ilgili risklerin ve ihlallerin artmasına olanak tanımış ve özellikle cinsiyet, ırk ve din temelli olmak üzere, belirli taciz, nefret ve şiddete teşvik biçimlerinin yayılmasını teşvik etmiştir. Üstelik internetin yükselişi ve buna bağlı teknolojik gelişmeler, kamu düzeninin ve ulusal güvenliğin sürdürülmesi, suçun önlenmesi ve kanunların uygulanması ve fikri mülkiyet hakları da dahil olmak üzere başkalarının haklarının korunması açısından önemli zorluklar yaratmıştır. Özellikle, güvensizlik ve kafa karışıklığı yaratmak ve toplumdaki bölünmeleri keskinleştirmek için tasarlanmış, hedefli çevrimiçi dezenformasyon kampanyalarının demokratik süreçler üzerinde istikrarsızlaştırıcı etkileri de olabilir.³⁴⁶

Tavsiye Kararı'nda, internetin temel hak hürriyetler üzerindeki olumlu ve olumsuz etkileri ortaya koyulduktan sonra internet aracılarının internetin yönetimindeki belirleyici rolleri ele alınmış³⁴⁷ ve bu rolleri dolayısıyla insan haklarına ilişkin görev ve sorumluluklarının açıklığa kavuşturulmasını zorunlu olduğu belirtilmiştir. Ancak internet aracılara ilişkin bu düzenleyici çerçeve çok katmanlı ve dinamik bir yapıdadır. Tavsiye Kararı'nda belirtildiği gibi devletler, özel tarafların önemli kamu hizmeti değerine sahip

https://www.coe.int/en/web/freedom-expression/committee-of-ministers-adopted-texts/-/asset_publisher/aDXmrol0vvsU/content/recommendation-cm-rec-2018-2-of-the-committee-of-ministers-to-member-states-on-the-roles-and-responsibilities-of-internet-intermediaries, (10.10.2024).

³⁴⁶ Ibid., para. 3.

³⁴⁷ İnternet aracılarında bazıları kullanıcıları internete bağlar, bilgi ve verilerin işlenmesini sağlar veya kullanıcı tarafından oluşturulan içerik de dahil olmak üzere web tabanlı hizmetleri barındırır. Diğer bazı internet araçları ise bilgi toplama ve aramayı mümkün kılmakta; üçüncü taraflarca tasarlanan ve/veya işletilen içerik ve hizmetlere erişim sağlamak ve bunları barındırmakta ve indekslemektedir. Son olarak bazı internet araçları da görsel-işitsel hizmetler de dahil olmak üzere mal ve hizmetlerin satışını kolaylaştırmakta ve ödemeler dahil diğer ticari işlemleri mümkün kılmaktadır.

hizmetlerin sağlanmasında hayati bir rol üstlendiği internet ortamını düzenlemenin karmaşık zorluğuyla karşı karşıyadır. Söz konusu düzenleme görevi, internetin ve ilgili hizmetlerin küresel yapısı, araçların çeşitliliği, internet iletişiminin hacmi ve üretilme ve işlenme hızı nedeniyle daha da karmaşık hale gelmektedir. Araçların, bulut bilişim bağlamı da dahil olmak üzere birçok ülkede faaliyet göstermesi veya kullanılması nedeniyle eylemleri, farklı yargı bölgelerindeki çeşitli, bazen birbiriyle çelişen yasalar kapsamında da etkilere sahip olabilir.³⁴⁸

Bakanlar Komitesi, bu kapsamda internet araçlarının insan hakları sorumluluklarına ilişkin bir çerçeve çizmiş ve araçların sorumluluklarını insan haklarına ve temel özgürlüklere saygı, şeffaflık ve hesap verebilirlik, içerik denetimi, kişisel verilerin kullanımı ve etkili bir çözüme erişim olmak üzere beş başlıkta ortaya koymuştur.

Tavsiye Kararı'nda internet araçlarının büyüklükleri, sektörleri, işletme bağlamı, sahiplik yapısı veya doğası ne olursa olsun insan haklarına saygı göstermek ve yeterli önlem almakla sorumlu oldukları belirtilmiştir. Sorumluluğun kapsamı ise şu şekilde ortaya koyulmuştur: *“Araçların sorumluluklarını yerine getirme şekilleri, hizmetlerinin insan hakları üzerindeki etkisinin ciddiyetine göre değişebilir. İnternet araçlarının hizmetlerinin insan haklarına etkisinin daha büyük ve olası zararın daha fazla olduğu durumlarda, aracının hizmet şartlarını, toplum standartlarını ve ahlak kurallarını geliştirirken ve uygularken kullanmaları gereken önlemler de o kadar büyük olmalıdır. Bu önlemler, özellikle kötüye kullanım içeren dil ve görüntülerin, nefret ve şiddeti teşvik etmenin yayılmasını önlemeye yöneliktir.”*³⁴⁹

- a. Şeffaflık ve hesap verebilirlik:** İnternet araçlarına yönelik şeffaflık ve hesap verebilirlik sorumluluğu, kullanıcıların haklarını belirleyen tüm hizmet koşulları ve politikaları ile içerik denetimi ve kullanıcı verilerinin işlenmesi ve ifşa edilmesine ilişkin diğer tüm standartlar ve uygulamaların ve tüm bunlara ilişkin değişikliklerin açık, sade bir dille ve erişilebilir formatlarda kamuya açık olmasını gerektirmektedir. Bu sorumluluk kapsamında internet araçları hangi verilerin işlendiği, veri işlemenin ne kadar süreceği, hangi

³⁴⁸ “Recommendation CM/Rec(2018)2 of the Committee of Ministers to Member States on the Roles and Responsibilities of Internet Intermediaries”, para. 9.

³⁴⁹ Appendix, “Recommendation CM/Rec(2018)2 of the Committee of Ministers to Member States on the Roles and Responsibilities of Internet Intermediaries, s. 7.

kriterlerin kullanıldığı ve işleminin hangi amaçla gerçekleştirildiği gibi veri işleme tekniklerinin işleyişine ilişkin kamuya anlamlı bilgileri açık ve şeffaf bir şekilde sağlamalıdır. Aracılar, serbest ve açık bilgi ve fikir akışına yönelik tüm kısıtlamalar ve bu tür kısıtlamalara yönelik tüm taleplerin yanı sıra veri erişim ve düzenleme talepleri hakkında net, kolay erişilebilir ve anlamlı bilgiler sağlayan şeffaflık raporlarını da düzenli olarak yayınlamalıdır.

b. İçerik denetimi: İnternet araçlarının içerik denetimine ilişkin sorumlulukların iki boyutu bulunmaktadır. Bunlardan ilki, içerik denetimine ilişkin devlet talepleridir. Aracılar, bu tür talepler karşısında alacakları önlemleri en az kısıtlayıcı araçları kullanılarak uygulamalıdır. İkinci olarak aracılar, kendi içerik kısıtlama politikaları doğrultusunda içeriğe erişimi kısıtlarken bunu şeffaf ve ayrımcı olmayan bir şekilde yapmalıdır. İçeriğin herhangi bir şekilde kısıtlanması, en az kısıtlayıcı teknik araçlar kullanılarak gerçekleştirilmeli ve kısıtlamanın kapsamı ve süresi kesinlikle gerekli olanla sınırlı olmalıdır.

c. Kişisel verilerin kullanımı: İnternet araçları tarafından kişisel verilerin toplanması, saklanması, toplanması, uyarlanması, değiştirilmesi, bağlanması veya paylaşılması da dahil olmak üzere işlenmesi, belirli bir amaca veya başka bir meşru gerekçeye ilişkin olarak kullanıcının özgür, spesifik, bilgilendirilmiş ve açık rızasına dayalı olmalıdır. Ayrıca kullanıcıların kişisel verilerine erişme ve bunların düzeltilmesini, silinmesini ve engellenmesini isteme hakkının gereği olarak aracılar, işleminin tüm aşamalarında, özellikle bu tür bilgilerin çocuklara yönelik olduğu durumlarda, açık ve sade bir dil kullanarak onlara ilgili bilgileri sağlamalıdır. Aracılar; kişisel verilerin silinmesi hakkını hangi koşullar altında kullanabilecekleri, verilerin işlenmesine itiraz edebilecekleri ve kişisel verilerin işlenmesi için verilen rızayı geri çekebilecekleri ve bundan sonra tüm işlemlerin rızaya dayalı olarak gerçekleştirilebileceği koşullar konusunda da kullanıcıları açıkça bilgilendirmelidir. Aracıların kullanıcıların takip edilmesi ve profillerinin çıkarılmasına karşı da sorumlulukları bulunmaktadır. Buna göre aracılar, insan haklarını ihlal eden profil oluşturma ve dijital izleme tekniklerini kullanmamalı, kullanıcıları üçüncü şahıslar tarafından takip edilmekten ve profil oluşturmaktan korumaya çalışmalıdır.

Bu koruma sorumluluğu söz konusu faaliyetlerden veya bu karardan kaynaklanan hukuki sonuçlardan etkilenen kişilerin bu karara itiraz edebilmelerini de gerektirir. İnternet araçları kural olarak kişisel verileri üçüncü kişilere açıklamamakla da yükümlüdür. Tavsiye Kararı'nda bu yükümlülüğe ilişkin iki istisnaya yer verilmiştir: yasaların gerektirmesi ve yargı organları ya da kararları yargı denetimine tabi olan ve ifşanın yürürlükteki yasalar ve standartlarla tutarlı, demokratik bir toplumda gerekli ve izlenen meşru amaçla orantılı olduğunu tespit etmiş bağımsız idari otoriteler tarafından bu yönde bir talep olması.

d. Etkili bir çözüme erişim: Etkili bir çözüme erişim bakımından şikâyet mekanizmalarının ve bunlarının uygulanmasının internet aracısının boyutu, etkisi ve rolüne göre değişiklik gösterebileceği, ancak her halükârda ihlal iddiasının tarafsız ve bağımsız bir şekilde incelenmesine imkân sağlanması gerektiği kabul edilmektedir. Şikâyet mekanizmaları, geçerli usul güvencelerine uygun, erişilebilir, adil, haklarla uyumlu, şeffaf ve uygun maliyetli olmalı; şikâyet sahiplerinin yargı dahil olmak üzere bağımsız ulusal inceleme mekanizmaları yoluyla başvuruda bulunma fırsatlarını olumsuz etkilememelidir.

Avrupa Konseyi tarafından kabul edilen bu kılavuz ilkeler ve tavsiye kararlar ile internette insan haklarının korunması ve devlet ve devlet dışı aktörlere buna ilişkin çeşitli güçlüklerle başa çıkmalarına yardımcı olacak kapsamlı kurallar koyulması bir çözüme kavuşturulmuştur. Bu düzenlemeler, her ne kadar hukuki olarak bağlayıcı olmasalar da internet şirketlerinin insan hakları sorumlulukları bakımından belirleyici bir yorum oluşturmaları ve AİHM içtihadında da yol gösterici olmaları dolayısıyla önem arz etmektedir.

B. Avrupa İnsan Hakları Mahkemesi İçtihatlarında İnternet Platformlarının Hukuki Sorumluluğu

Avrupa İnsan Hakları Sözleşmesi'nin "İnsan Haklarına Saygı Yükümlülüğü" başlıklı 1. maddesinde hak ve özgürlükler "*Yüksek Sözleşmeciler Tarafından kendi yetki alanları içinde bulunan herkesin, bu Sözleşme'nin birinci bölümünde açıklanan hak ve*

özgürlüklerden yararlanmalarını sağlarlar.” şeklinde güvence altına alınmıştır. Bu maddede her ne kadar hak ve özgürlüklerin korunması konusunda devletlere bir çağrı yapılsa da³⁵⁰, sözleşmesel hakların ileri sürülebileceği muhataplar bakımından bir ayırım yapılmamıştır.³⁵¹ Bu madde, devlet dışındaki aktörleri insan haklarına ilişkin yükümlülüklerden bağışık tutmamaktadır. Zira, devletlerin Sözleşmeden kaynaklanan yükümlülüklerinden biri de diğer aktörlerin insan haklarına uygun davranmalarını sağlama yükümlülüğüdür. Buradan hareketle, şirketlerin insan hakları sorumluluklarını, devletlerin AIHS’nin normlarına uymak için şirketlerin davranışlarını düzenlemek amacıyla ortaya koydukları görevler olarak tanımlamak mümkündür.³⁵²

Şirketlerin insan haklarına ilişkin sorumluluklarına ilişkin iki farklı durumdan bahsedilebilir. Bunlardan ilki, Sözleşme kapsamında yapılan bir başvuruya konu ihlal iddiasının şirketlerin faaliyetlerinden kaynaklanması halidir. Bu durumda, şirketlere karşı doğrudan bir başvuru yapılamayacak olsa da hak ve özgürlükleri şirketlere karşı korumakla yükümlü olan devlete karşı başvuru yapılması mümkündür. Bu ihtimalde, Sözleşme’nin ihlal edildiğine hükmedilmesi; devletin, şirketlerin eylemlerini daha etkili bir şekilde düzenlemesini veya gelecekte benzer anlaşmazlıkları önleyecek bir yasa çıkarmasını gerektirebilir. İkinci ise şirketlerin devletin temsilcisi olarak hareket ederek hak ve özgürlükleri ihlal ettikleri durumlardır. Bu durum, bir şirketin doğrudan devlet tarafından yönetilmesi ya da devletin bazı fonksiyonlarının şirketler tarafından yerine getirilmesi halinde söz konusu olabilir.

Şirketlerin Sözleşme kapsamında insan haklarına saygı gösterme sorumlulukları, *“pozitif yükümlülükler”* kavramıyla sıkı bir ilişki içerisindedir. Buna göre, belirli insan haklarının etkili bir şekilde korunması, devletin *“müdahale etmeme”* yükümlülüğü yanında, devlet dışı aktörler arasındaki ilişkilere müdahale etmesini de gerektirebilmektedir.³⁵³ Dolayısıyla bu takdirde, devletin sorumluluğu temel hakları ihlal

³⁵⁰ AIHS’nin devletler yanında devlet dışındaki aktörlere yönelik de doğrudan yükümlülükler içerdiğine ilişkin değerlendirmeler için bkz. Alla Tymofeyeva, “Indirect Obligations of Business Entities under the European Convention of Human Rights”, *Zech Yearbook of Public and Private International Law*, C. 8, 2018, ss. 291-305.

³⁵¹ Oya Boyar, “Devletin Pozitif Yükümlülükleri ve Dolaylı Yatay Etki”, *İnsan Hakları Avrupa Sözleşmesi ve Anayasa (ed. Sibel İncoğlu)*, 2013, s. 61.

³⁵² Tymofeyeva, “Indirect Obligations of Business Entities under the European Convention of Human Rights”, s. 293.

³⁵³ ECHR, “Research Report: Positive Obligations on Member States under Article 10 to Protect Journalists and Prevent Impunity”, 2012, <https://policycommons.net/artifacts/1760336/research-report/2491983/>, (20.11.2023).

etmesinden değil, temel hakların garantörü olmasından kaynaklanmaktadır.³⁵⁴ Bu sorumluluğun sözleşmesel hakların üçüncü kişilerin müdahalelerinden korunması ve sözleşmesel hakların etkili biçimde kullanılmasının sağlanması şeklinde iki boyutu bulunmaktadır.³⁵⁵

AİHM içtihadında pozitif yükümlülüklerle ilişkin net bir tanımdan bahsetmek mümkün değildir. Aksine, Mahkeme bu yönde bir tanımlama yapmayı bilinçli olarak reddetmektedir. Bununla birlikte, belirli hak ve özgürlükler bakımından AİHM'nin, devletin pozitif yükümlülüklerin genel çerçevesini çizdiği söylenebilir. AİHM, ilk olarak eğitim hakkı ile ilgili olarak *Belçika Dil Hakları* davasında, Devletin bu hakkı sağlamak için pozitif bir yükümlülüğü olabileceğine karar vermiştir.³⁵⁶ Daha sonra Mahkeme, *Marckx/Belçika* davasında, Sözleşmenin 8. maddesinin amacının esasen bireyi kamu otoritelerinin keyfi müdahalesinden korumak olduğunu belirttikten sonra, devletin yükümlülüklerinin bu pozitif yönünü biraz daha detaylandırmıştır: “*Bununla birlikte, Devleti yalnızca bu tür müdahalelerden kaçınmaya zorlamaz: Bu öncelikle olumsuz taahhüdün yanı sıra, aile hayatına "saygı" duymanın etkili bir şekilde doğasında olan olumlu yükümlülükler de olabilir.*”³⁵⁷ X. ve Y./Hollanda davasında pozitif yükümlülüklerin kapsamı, “*bireylerin kendi aralarındaki ilişkiler alanı*”nı da kapsayacak şekilde genişletilmiştir.³⁵⁸ Mahkemenin pozitif yükümlülüklerle ilişkin içtihadı, bu kategoriye sürekli olarak yeni unsurlar eklenerek gelişmiştir. Bu çerçevede pozitif yükümlülüklerin karakteri, ulusal makamların bir hakkı güvence altına almak için gerekli tedbirleri alması, daha açık ifadesiyle ulusal makamların makul ve uygun tedbirler olarak bireyin haklarını koruması³⁵⁹ şeklinde ifade edilmektedir.³⁶⁰ Böylece, devletler

³⁵⁴ Cordula Dröge, “Positive Verpflichtungen der Staaten in der Europäischen Menschenrechtskonvention. Beiträge zum ausländischen öffentlichen Recht und Völkerrecht”, C. Band 159, 2003, <https://www.mpil.de/files/pdf2/beitr159.pdf>den aktaran Boyar, “Devletin Pozitif Yükümlülükleri ve Dolaylı Yatay Etki”, s. 54.

³⁵⁵ Boyar, “Devletin Pozitif Yükümlülükleri ve Dolaylı Yatay Etki”, s. 55.

³⁵⁶ Case “Relating to Certain Aspects of the Laws on the Use of Languages in Education in Belgium” v. Belgium, 1474/62; 1677/62; 1691/62; 1769/63; 1994/63; 2126/64 (ECtHR 23 Temmuz 1968).

³⁵⁷ Marckx v. Belgium, 62980/10, 57534/16, 60594/16, 61095/16, 65741/16, 1023/17, 1996/17 (ECtHR 13 Haziran 1979) para. 31.

³⁵⁸ X and Y v. the Netherlands, 8978/80 (ECtHR 26 Mart 1985), para. 23.

³⁵⁹ López Ostra v. Spain, 39666/16, 27733/21, 57905/21 (ECtHR 09 Aralık 1994), para. 55.

³⁶⁰ Jean-François Akandji-Kombe, “Positive Obligations under the European Convention on Human Rights”, **Human Rights Handbooks**, No. 7, 2007, s. 7.

"pozitif önlemler" alma yükümlülüğü kapsamında hakların, "özel kişilerin müdahalesi olmadan" özgürce kullanılabilmesini sağlamakla yükümlüdür.³⁶¹

Sözleşmesel bir hakka ilişkin olarak, pozitif bir yükümlülüğün var olup olmadığına karar verilirken, Sözleşme ile toplumun genel çıkarları ve bireyin çıkarları arasında ulaşılmaya çalışılan dengeye önem verilmesi gerektiği belirtilmekte ve bu tespitin Sözleşmeciler Devletlerde var olan farklı durumlara, modern toplumların idare edilmesi ile ilgili zorluklara, öncelikler ve kaynaklar hakkındaki seçimlere bağlı olarak değişkenlik göstereceği kabul edilmektedir.³⁶²

AİHM, pozitif yükümlülükler doktrini, *Editorial Board of Pravoye Delo ve Shtetel/Ukrayna* kararıyla internet alanına genişletmiştir.³⁶³ Bir gazetenin yazı işleri kurulu ve aynı gazetenin yazı işleri müdürü tarafından yapılan başvuruda, başvuru Ukrayna güvenlik kuvvetlerinin üst düzey memurlarının yolsuzluk ve başka yasadışı faaliyetlere karıştıklarını ve organize suçlarla bağlantılı olduklarını iddia eden imzasız bir mektubu bir internet sitesinden indirerek yayımladıkları gerekçesiyle kendilerine yaptırım uygulanmasından yakınmışlardır. AİHM, başvuru sahiplerinin tazminat ödeme ve özür yazısı yayınlamaya mahkûm edilmelerinin 10. madde ihlali olduğunu tespit etmiştir. Mahkemeyi bu sonuca ulaştıran sebeplerden biri de internetten elde edilen bilgileri kullanan gazeteciler için iç hukukta yeterli güvencelerin bulunmaması dolayısıyla başvuru sahiplerinin söz konusu yayının sonuçlarını öngörememiş olmasıdır.³⁶⁴ Bu nedenle, Sözleşme uyarınca devletler gazetecilerin internetteki ifade özgürlüğünü etkili bir şekilde korumak için ihtiyaç duyulan düzenleyici çerçeveyi sağlamak konusunda pozitif bir yükümlülüğe sahiptir.³⁶⁵

Buradan hareketle AİHS kapsamında, şirketlerin de insan hakları sorumlulukları olduğu kabul edilmelidir. Esasen AİHM, Avrupa Konseyi'nin şirketlerin insan haklarına ilişkin standart belirleme çabalarından çok önce de özellikle çevre davaları bağlamında pozitif yükümlülüklerin gereği olarak devletin şirketleri düzenleme görevlerini kabul

³⁶¹ Andrew Clapham, *Human Rights in the Private Sphere*, Oxford, New York: Oxford University Press, 1996, s. 345.

³⁶² *Gaskin v. The United Kingdom*, 10454/83 (ECtHR 07 Temmuz 1989) para. 42-46; *Ozgur Gundem v. Turkey*, 23144/93 (ECtHR 16 Mart 2000) para. 43.

³⁶³ *Editorial Board of Pravoye Delo and Shtetel v. Ukraine*, 33014/05 (ECtHR 05 Mayıs 2011).

³⁶⁴ *Editorial Board of Pravoye Delo and Shtetel v. Ukraine*, para. 66.

³⁶⁵ *Editorial Board of Pravoye Delo and Shtetel v. Ukraine*, para. 63.

etmiştir. Mahkeme, *Fadeyeva/Rusya* kararında devletin pozitif yükümlülüklerine atıfla kirlenici işletmenin yerel çevre standartlarını ihlal ederek faaliyet göstermesine rağmen Devletin kirlilikten etkilenen yerel halkın çıkarlarını dikkate alacak ve endüstriyel kirliliği kabul edilebilir seviyelere düşürecek etkili önlemler tasarladığı veya uyguladığına dair hiçbir bilgi bulunmadığını belirterek Sözleşmenin 8. maddesinin ihlal edildiğine hükmetmiştir.³⁶⁶

Avrupa İnsan Hakları Mahkemesi'ne göre ifade özgürlüğünün gerçek ve etkili bir biçimde kullanımı, yalnızca devletin her türlü müdahaleden imtina etme görevine bağlı olmayıp bireyler arası ilişkilere varıncaya kadar pozitif koruma tedbirlerinin alınmasını gerektirmektedir. AİHM, bu çerçevede gazete ve gazetecilerin ifade özgürlüklerinin devlet dışı aktörlerin müdahalelerinden korunmasına ilişkin bir dizi karar vermiştir.³⁶⁷

İnternet teknolojilerindeki gelişmeler ve internetin ifade özgürlüğü üzerindeki etkilerinin artmasıyla birlikte AİHM içtihadında da internette ifade özgürlüğüne yönelik gelişmeler yaşanmıştır.³⁶⁸ Mahkeme bir yandan, “*çevrimdışı olarak geçerli olan her şey çevrimiçi olarak da geçerlidir*” ilkesi ışığında temek hak ve özgürlüklerin internette de etkili şekilde korunmasının önemini ortaya koymakta, diğer yandan da internetin yarattığı güçlükleri dikkate alarak hak ve özgürlüklerin korunması ve güçlendirilmesi için internet politikasının teknolojiye özgü özelliklere uygun bir şekilde uyarlanmak zorunda olduğunu kabul etmektedir.³⁶⁹

Bu bölümde, AİHM'nin internet şirketlerinin insan hakları sorumluluklarıyla bağlantılı başvurular incelenerek bu şirketlerin insan haklarından sorumluluklarının şartları ve kapsamı belirlenmeye çalışılacaktır. İnternet şirketlerinin sorumluluklarının belirlenmesinde, Mahkeme'nin hem internetle bağlantılı içtihadı hem de devlet dışı aktörlerin Sözleşmesel yükümlülüklerine ilişkin içtihadı etkilidir. Bu bakımdan, başlığın odak noktası internet şirketlerinin sorumlulukları olmakla birlikte, Mahkeme'nin

³⁶⁶ *Fadeyeva v. Russia*, 4856/03, 69889/01, 23697/02, 69315/01, 72701/01 (ECtHR 09 Haziran 2005), para. 133, 134.

³⁶⁷ *Dink/Türkiye*, para. 106; *Ozgur Gundem v. Turkey* para. 42-46; *Gaşi and Others v. Serbia*, 24738/19 (ECtHR 06 Eylül 2022), para. 77-84 (Bu kararlar genellikle gazetecilerin üçüncü kişiler karşısında korunmasına ilişkindir.).

³⁶⁸ Ayrıntılı bilgi için bkz. Nina Vajic, Panayotis Voyatzis, “The Internet and freedom of expression: A ‘brave new world’ and the European Court of Human Rights’ evolving case law”, **Freedom of expression, essays in honour of Nicolas Bratza**, 2012, s. 395.

³⁶⁹ Editorial Board of *Pravoye Delo and Shtekel v. Ukraine*, para. 63.

çevrimiçi hakları yorumlayışı ve özel kişilerin sorumluluğuna ilişkin yaklaşımı da yer yer dikkate alınacaktır.

1. İçerik Yönetimi ve İfade Özgürlüğü

İnternet şirketlerinin kullanıcı içeriklerine ilişkin sorumlulukları, içeriklere müdahale etmekten kaynaklanan sorumluluklar ve içeriğe müdahale etmemekten kaynaklanan sorumluluklar şeklinde iki farklı kategoride ele alınabilir. İlk kategori, internet şirketlerinin, internet kullanıcılarının internet ortamındaki ifadelerini sınırlandırmasına ilişkindir. Bu sınırlama kullanıcı hesaplarının askıya alınması ya da kapatılması veya kullanıcılar tarafından oluşturulan içeriklerin filtrelenmesi gibi ifade özgürlüğüne aykırılık potansiyeli taşıyan eylemler şeklinde ortaya çıkabilir. İkinci kategori ise internet şirketlerinin, internet ortamındaki hukuka aykırı içerikleri önlememesine ilişkindir. Bu da hukuka aykırı içeriklerin tespitine ilişkin moderasyon ya da filtreleme vb. mekanizmaların sağlanmaması gibi kişilik haklarına aykırılık potansiyeli taşıyan eylemsizlik hallerinde söz konusu olabilir.

AİHM bugüne kadar bir internet şirketinin internet ortamındaki içeriğe müdahalesinden kaynaklanan sorumluluğuna ilişkin bir karar vermemiştir. Bununla birlikte, Mahkeme'nin şirket eylemlerinin ifade özgürlüğü kapsamında ele alındığı bazı kararları, internet şirketleri bakımından da yol gösterici nitelik taşımaktadır. Örneğin, *Tierfabriken/İsviçre* kararında AİHM, bir televizyon şirketinin bir derneğin reklamını konu bakımından uygun görmeyerek yayımlamayı reddetmesinin ifade özgürlüğünü ihlal ettiğine karar vermiştir.³⁷⁰ AİHM, öncelikle söz konusu şirketin özel hukuka tabi olduğunu ve reklam alıp almama konusunda sözleşme özgürlüğü olan bir taraf olduğunu belirtmiş ve AİHS'nin öngördüğü güvencelerin özel kişiler arasındaki ilişkilere genişletilmesi konusunda genel bir teori ortaya koymaktan özellikle kaçınmıştır.³⁷¹ Sonrasında ise televizyon şirketinin iç hukukta düzenlenen “siyasi reklam” yasağına dayanarak bu talebi reddettiğini belirterek, derneğin siyasi ifade özgürlüğünün yasaklanmasının devletin pozitif yükümlülükleri kapsamında sorumluluğunu

³⁷⁰ Vgt Verein Gegen Tierfabriken v. Switzerland, 24699/94 (ECtHR 28 Haziran 2001).

³⁷¹ Mahkemenin bu yaklaşımı şu ifadeden anlaşılmaktadır: “Mahkeme, Sözleşme güvencelerinin özel kişiler arasındaki ilişkilere ne ölçüde teşmil edilmesi gerektiğine dair genel bir teori geliştirmeyi gerekli görmek bir yana, arzu edilir bulmamaktadır.” Vgt Verein Gegen Tierfabriken v. Switzerland, para. 46.

gerektirebileceğini belirtmiştir.³⁷² Müdahalenin yasal bir dayanağı ve meşru bir amacı olduğunu kabul eden AİHM, demokratik toplumda gereklilik kriteri bakımından ayrıntılı değerlendirmelerde bulunmuş ve bireyin salt ticari çıkarının değil genel çıkarı etkileyen bir tartışmaya katılımının söz konusu olduğu durumlarda devletin takdir yetkisinin daralacağını ifade etmiştir. AİHM, yerel makamlar tarafından müdahalenin haklı çıkarılması için ileri sürülen genel gerekçelerin, özellikle başvuran derneğin durumu çerçevesinde yeterli bir şekilde ortaya koyulmadığını ve tüm İsviçre halkına ulaşmak isteyen başvuru derneğin ulusal televizyon programlarından başka aracı olmadığını göz önünde bulundurarak derneğin ifade özgürlüğünün ihlal edildiğine hükmetmiştir.³⁷³

Bu kararın ardından başvuru dernek, televizyon şirketinin yeni adı olan Publisuisse SA'ya televizyon reklamının yayınlanmasına ilişkin bir talepte bulunmuştur. Bu talep aynı zamanda, reklam yasağı konusunda hükümeti eleştiren bir yorumun ve AİHM'nin ilgili kararının da yayımlanmasını içermektedir. Başvuru, bu talebinin de reddedilmesi üzerine yeniden AİHM'ne başvurmuştur. AİHM, ulusal mahkemelerin AİHM'nin kararının artık geçerli olmadığına yönelik kararına ilişkin bir gerekçe sunmadıklarını belirterek oy çokluğuyla yeniden ifade özgürlüğünün ihlal edildiğine karar vermiştir.³⁷⁴ Karşı oy kullanan Yargıç Sajó, muhalif görüşünü “şirketin hak ve özgürlükleri”ne dayandırarak gerekçelendirmiştir. Bu gerekçe, ilerleyen yıllarda internet şirketleri bakımından da sıklıkla dile getirilen bir gerekçe olduğundan dikkat çekicidir:

“Özel kuruluşlara yüklenen reklam yayınlama yükümlülüğü, yayıncıların özel mülkiyet ve bilgi edinme menfaatlerine kısıtlamalar getirmektedir. ‘Zorunlu yayın’ kuralları ifade özgürlüğünün özüne dokunmaktadır. Değişen bir ortamda ‘taşıması zorunlu’ bir görevin dayatılması nedeniyle editöryal özgürlük zarar görebilir. Reklamların, hatta (ve özellikle) siyasi içerikli reklamların yayınlanmasının dayatılmasının, başkalarının ticari ve ifade çıkarları uğruna yayıncı/editörün ifade özgürlüğüne geniş kapsamlı bir müdahale olduğu göz önünde bulundurulduğunda, azami özen gösterilmesi gerekmektedir... Yayın yapma yükümlülüğü kendi başına, sadece konuşma hakkına bir müdahale

³⁷² Vgt Verein Gegen Tierfabriken v. Switzerland, para. 44-47.

³⁷³ Vgt Verein Gegen Tierfabriken v. Switzerland, para. 75-79.

³⁷⁴ Verein Gegen Tierfabriken Schweiz (VGT) v. Switzerland (No. 2), 32772/02 (ECtHR [GC] 30 Haziran 2009).

değildir; aynı zamanda bunun bir reklam olduğunun belirtilmesi, ilke olarak yayıncının pozisyonu ile yayınlanan reklamın bakış açısı arasında bir ayrım yapılmasına izin verse bile, aslında kısıtlanmış bir konuşma biçimidir.”³⁷⁵

Yargıç Sajo’ya göre editoryal bağımsızlığı sınırlamak şirketin hem mülkiyet hakkına hem de ifade özgürlüğüne müdahale teşkil edebilecektir. Bu tespit başlı başına bir sorun teşkil etmemektedir; çünkü çoğunluk görüşünde de “*pozitif bir yükümlülüğün var olup olmadığının belirlenmesinde, toplumun genel menfaatleri ile bireyin menfaatleri arasında kurulması gereken adil denge göz önünde bulundurulmalıdır*” denilerek şirketin de hak ve özgürlükleri kabul edilmiştir. Burada çoğunluk kararının ayırt edici yönü, somut başvuru bakımından, siyasi ifade özgürlüğüne ağırlık verilmesidir. Kamusal tartışmalara ve fikirlerin geniş kitlelere ulaştırılabilmesindeki etkileri dikkate alındığında söz konusu tespitlerin internet şirketleri bakımından da geçerli olacağı açıktır.

İnternet şirketlerinin kullanıcı içeriklerine müdahalesinden sorumluluğu konusunda yol gösterici nitelik taşıyan bir başka karar da *Appleby ve Diğerleri/Birleşik Krallık* kararıdır.³⁷⁶ Bu karar, internetin özellikle kamusal alan niteliği bakımından önemlidir. Başvuru, özel mülkiyete tabi bir alışveriş merkezinin girişinde bildiri dağıtmak için stant kurmaya çalışan başvuruçuların, şirket tarafından engellenmesinin başvuruçuların ifade özgürlüklerini ihlal edip etmediğine ilişkindir. AİHM, özellikle kamunun ilgisini çeken tartışmalarda ifade özgürlüğünün önemli olduğunu belirtmekle birlikte, somut başvuru bakımından şirketin mülkiyet hakkının da tehlikede olduğunun altını çizerek, yapılması gerekenin menfaatler arasında adil bir denge kurmak olduğunu ortaya koymuştur.³⁷⁷

Başvuruçuların temel argümanı, alışveriş merkezlerinin kamusal bir nitelik taşıdığı noktasında toplanmıştır:

“Mahkeme, başvuranların argümanlarını ve Amerika Birleşik Devletleri davalarına yapılan atıfları not etmiş ve alışveriş merkezlerinin, amaçları öncelikle özel ticari çıkarları takip etmek olsa da giderek artan bir şekilde,

³⁷⁵ Verein Gegen Tierfabriken Schweiz (VGT) v. Switzerland (No. 2), Dissenting Opinion of Judge Sajó,

³⁷⁶ Appleby and Others v. the United Kingdom, 61080/14 (ECtHR 06 Mayıs 2003).

³⁷⁷ Appleby and Others v. the United Kingdom, para. 40.

sınırları içinde yoğunlaşan çok sayıda faaliyetle toplanma yerleri ve etkinlik merkezleri olarak hizmet vermek üzere tasarlandığına dikkat çekmiştir. Sıklıkla, bireyler yalnızca alışveriş yapmaya davet edilmemekte, aynı zamanda vakit geçirmeye ve eğlenceden toplumsal, eğitimsel ve hayırsever etkinliklere kadar geniş bir yelpazedeki faaliyetlere katılmaya teşvik edilmektedir. Bu tür alışveriş merkezleri geleneksel şehir merkezinin özelliklerini taşıyabilir ve gerçekten de bu durumda, Galleries³⁷⁸ haritalarda şehir merkezi olarak işaretlenmiştir ve kamu hizmetlerini ve tesislerini ya içerir ya da bunlara yakındır. Sonuç olarak başvuranlar, alışveriş merkezinin, bireylerin ifade özgürlüğünü makul bir şekilde kullanma hakkını talep edebilecekleri "yarı kamusal" bir alan olarak görülmesi gerektiğini savunmuşlardır.”³⁷⁹

AİHM, somut başvuru bakımından, Amerika Birleşik Devletleri’nde kamuya açık özel mülkiyet alanlarında ifade özgürlüğüne ilişkin farklı yaklaşımlar olduğunu kabul etmekle birlikte, bu konuda henüz bir görüş birliği olmadığını belirtmiştir. Sonuç olarak, başvuranların söz konusu amaca ulaşmak için sahip olduğu alternatif yolları gerekçe göstererek ifade özgürlüğünün ihlal edilmediğine karar verse de internet şirketleri söz konusu olduğunda aksi kanaate varılmasını mümkün kılacak şu önemli tespitte bulunmuştur:

“...Bununla birlikte, mülkiyete erişimin engellenmesinin ifade özgürlüğünün etkili bir şekilde kullanılmasını engelleme etkisine sahip olduğu veya hakkın özünün yok edildiğinin söylenebildiği durumlarda Mahkeme, Devletin mülkiyet haklarını düzenleyerek Sözleşme haklarından yararlanılmasını koruması için pozitif bir yükümlülüğün ortaya çıkabileceğini göz ardı etmeyecektir. Belediyenin tamamının özel bir kuruluş tarafından kontrol edildiği bir şirket kasabası buna bir örnek olabilir.”³⁸⁰

Bu gözlem, hizmet kullanım şartları uyarınca herhangi bir nedenle –hatta hiçbir neden göstermeksizin– hizmet vermeyi durdurmakta özgür olan tekel benzeri internet servis sağlayıcılarının durumu açısından öğreticidir. Örneğin, Google’ın herhangi bir

³⁷⁸ Başvuru konusu alışveriş merkezinin bulunduğu alanın adı.

³⁷⁹ Appleby and Others v. the United Kingdom, para. 44.

³⁸⁰ Appleby and Others v. the United Kingdom, para. 47.

zamanda feshedebileceği Google mail hesapları ya da X'in askıya alabileceği sosyal medya hesapları bakımından AİHM'in kararında dışlamadığı ihtimal ortaya çıkabilir. Bu tür durumlarda, şirketlerin tekeli konumu açık bir şekilde ortaya konabilirse, internet şirketlerinin sorumluluğu söz konusu olabilir ve yetkili merciler söz konusu hizmetlere erişim sağlanmasını meşru bir şekilde şart koşabilir.³⁸¹

İnternet şirketlerinin içeriğe müdahale etmemekten kaynaklanan sorumluluklarına gelince, AİHM'in bu konuda içtihat oluşturacak kadar karar verdiği söylenebilir. AİHM içtihadında, internet şirketlerinin insan hakları yükümlülüklerine ilişkin olarak ortaya çıkan temel sorunlardan biri, internet servis sağlayıcıları ya da internet içerik sağlayıcıları gibi internet aracı şirketlerinin, kontrol ettikleri internet ortamında ortaya çıkan hak ihlallerinden sorumlu tutulup tutulamayacağıdır. Zira bu araçlar, internet ortamında yayılan içerikleri kaldırma ya da yayında tutma veya kullanıcı hesaplarını askıya alma hususlarında teknik araçlara sahip olduklarından kamusal nitelikli tartışmaların konularını sınırlama ve bu tartışmaların ne şekilde yürütüleceğini belirleme konularında benzersiz bir konuma sahiptir.³⁸²

İnternet araçlarına geçmeden önce AİHM içtihadında benzer durumdaki geleneksel medya aktörlerinin sorumluluk rejimini anlamak önemlidir. Geleneksel anlamda bir dergi sahibinin, derginin editörüne yazılan ve sert ifadeler içeren mektupları yayımlamaktan dolayı mahkûm edilmesinin Sözleşme'nin 10. maddesi kapsamında incelendiği *Sürek/Türkiye* kararı bu konuda dikkat çekici tespitleri barındırmaktadır.³⁸³ Mahkeme bu davada, mektupların içeriğini iddia edilen zulümlerin sorumlusu olarak gösterilenlere karşı köklü ve mantık dışı bir nefret uyandırarak bölgede daha fazla şiddete sebebiyet verebilecek nitelikte olduğunu değerlendirmiştir. Mektupların içeriğine ilişkin bu tespitten ardından Mahkeme, söz konusu mektup içerikleri bakımından dergi sahibinin sorumluluğunu da ele almıştır:

“Başvuranın bu mektuplarda bulunan görüşler ile şahsen bağlantılı olmadığı doğru olmasına rağmen, mektupların yazarlarına şiddet ve nefretin körüklenmesi için bir araç temin etmiştir. Mahkeme, başvurucunun dergi ile sadece ticari

³⁸¹ Benedek, Kettemann, *İfade özgürlüğü ve internet*, s. 17.

³⁸² Tarlach McGonagle, “The Council of Europe and Internet Intermediaries: A Case Study of Tentative Posturing”, **Human Rights In The Age Of Platforms**, The MIT Press, 2019.

³⁸³ *Sürek v. Turkey* (No. 1), 26682/95 (ECtHR [GC] 08 Temmuz 1999).

açından bağlı olduğu ve editoryal sorumluluğu bulunmadığı gerekçesi ile mektupların içeriğine ilişkin her türlü cezai sorumluluktan muaf tutulması gerektiği iddialarını kabul etmemektedir. Başvuran mal sahibi olup bu konumu itibarıyla derginin yazı işleri yönetimini şekillendirme hakkına sahiptir. Bu nedenle, derlemenin editoryal ve gazetecilik personelinin kamuoyuna bilgi toplama ve yayma konusunda üstlendiği ve çatışma ve gerginlik durumlarında daha da büyük önem kazanan ‘görev ve sorumluluklara’ dolaylı olarak tabi olmuştur.’³⁸⁴

AIHM’nin dergi sahibini üçüncü taraf içeriğinden sorumlu tutmasının Sözleşme’ye aykırı olmadığına ilişkin bu içtihadında belirleyici olan husus, dergi sahibinin derginin yazı işleri yönetimini şekillendirebileceğine ilişkin tespittir. Bu tespit, internet ortamında üçüncü kişiler tarafından yayımlanan içerikler bakımından şu soruyu gündeme getirmektedir: İnternet ortamındaki içerikleri şekillendirme hakkına sahip olan, dahası internet ortamını bütünüyle kontrol edebilen internet şirketleri de üçüncü taraf içeriklerinden sorumlu tutulacak mıdır? Bu soruya AIHM içtihadı çerçevesinde cevap aramadan önce interneti, geleneksel medyadan ayıran birtakım farklılıkların altını çizmek gerekir. Her şeyden önce, yeni medyanın içerik hacmi geleneksel medyanın çok üzerinde olduğundan içeriği yayınlanmadan önce modere etmek internet araçları bakımından orantısız yükümlülükleri beraberinde getirebilir. İnternet araçları, sahipleri oldukları sitelerin editörleri olarak da değerlendirilemezler. Son olarak, internetin bilgi ve fikirlerin akışındaki etkisi de internet araçlarına yüklenecek sorumluluklar bakımından dikkate alınması gereken bir farklılıktır. AIHM’nin internet şirketlerinin sorumluluklarına ilişkin içtihadında bu farklılıkların yansımaları görülmektedir.

AIHM internet araçlarının üçüncü taraf içeriklerinden sorumluluğunu *Delfi AS/ Estonya* kararında ayrıntılı olarak ele almıştır.³⁸⁵ Başvurucu Delfi AS, Estonya’nın en büyük haber portallarından biri olup kendi haber makalelerini yayınlayan ve okuyucuları da bu haberlere yorum yapmaya davet eden bir internet portalıdır.³⁸⁶ Başvurucu, portalda

³⁸⁴ Sürek v. Turkey (No. 1), para. 63.

³⁸⁵ Delfi AS v. Estonia, 64569/09 (ECtHR [GC] 16 Haziran 2015).

³⁸⁶ Mahkeme, daha sonra, portalın bu niteliğini kararını gerekçelendirirken vurgulamaktadır. Mahkeme, dava konusu Delfi’nin “kullanıcıların herhangi bir konuda fikirlerini özgürce ortaya koydukları ve forum yöneticisinin herhangi bir girdi ile tartışmayı yönlendirmediği bir internet tartışma forumu veya bülten tahtası ya da platformu sağlayan herhangi bir içerik sunmadığı ve içerik sağlayıcısının bir internet sitesi

bir feribot şirketine ilişkin olarak yayımlanan makalenin altında feribot şirketinin sahibine karşı tehdit ve hakaret içeren yorumlardan dolayı -ilgilinin talebi üzerine söz konusu yorumları kaldırmış olmasına rağmen- hukuken sorumlu tutulmasından yakınmaktadır. Başvurucu, üçüncü kişilerin ifade özgürlüğünü kullanımı üzerinde önleyici sansür politikası uygulaması konusunda kendisine dayatılan yükümlülüğün, aynı zamanda kendi ifade, yani üçüncü kişiler tarafından oluşturulan ve yayınlanan bilgileri yayma özgürlüğünü de ihlal ettiğini ileri sürmüştür. AİHM, Avrupa Konseyi ve Avrupa Birliği'nin konuya ilişkin belgelerini dikkate alarak üç aşamalı testi uygulamıştır.

Müdahalenin yasayla öngörülmüş olması kriteri bakımından AİHM, iç hukukta internet araçlarının sorumluluğuna ilişkin özel bir düzenleme olmamasına rağmen genel hükümlerin ilgili içtihat ile birlikte, bir medya yayıncısının medya yayınında yapılan hakaret içerikli her tür açıklamadan sorumlu olduğunu açıklığa kavuşturduğuna ve müdahalenin yasayla öngörülmüş olduğuna kanaat getirmiştir. Söz konusu müdahalenin başkalarının şöhret ve haklarının korunması meşru amacına dayandığını belirten AİHM, demokratik bir toplumda gereklilik kriteri bakımından ayrıntılı bir incelemeye geçmiştir. Bu inceleme -söz konusu içeriklerin küçük düşürücü ya da yasaya aykırı olduğuna ilişkin taraflar arasında herhangi bir anlaşmazlık olmadığından- başvurusunun söz konusu yorumlardan sorumlu tutulmasının ifade özgürlüğüne yönelik orantısız bir müdahale teşkil edip etmediğine ilişkindir.

Şirket tarafından yapılan savunmada; portalda yayımlanan makalenin içeriğinde herhangi bir haksızlık olmadığı ve hakaret içeren ifadelerin makalenin altında yazılan yorumlarda yer aldığı, şirketin ilgili kişiden gelen bildirim üzerine aynı gün yorumu kaldırdığı, söz konusu içeriklerden yorumların sahiplerinin sorumlu tutulması gerektiği ve şirketin sorumlu tutulmasının araçların sınırlı sorumluluğunun kabul edildiği Avrupa Birliği hukukuna da uygun olmayacağı iddiaları ileri sürülmüştür.³⁸⁷ Büyük Daire ise öncelikle söz konusu başvurunun gelişen teknolojik yenilikler bağlamında Mahkeme'ye yapılan ilk başvuru olduğundan hareketle internetin doğasına ilişkin tespitlerde bulunmuş, internetin ifade özgürlüğü bakımından emsalsiz bir platform olma ve bu platformun nefret söylemi ve şiddete teşvik eden söylemler de dahil olmak üzere,

ya da bir blogu hobi olarak işleten sıradan bir kişi olduğu bir sosyal medya platformu" olmadığına dikkat çekmiştir. Delfi AS v. Estonia, para. 116.

³⁸⁷ Delfi AS v. Estonia, para. 80.

karalayıcı ve açıkça hukuka aykırı olan diğer türdeki konuşmaların daha önce hiç olmadığı kadar hızlı şekilde dünya çapında yayılabilmesine neden olma şeklinde iki boyutunu ortaya koymuştur. Böylece Mahkeme, internet yönetiminin geleneksel medya yönetiminden farklı olabileceğini de kabul etmiştir:

*“Mahkeme, internetin kendine özgü yapısı nedeniyle, üçüncü taraflarca oluşturulan içerikle ilgili olarak Sözleşme’nin 10. maddesi çerçevesinde bir internet haber portalına yüklenecek ‘görev ve sorumlulukların’ geleneksel bir yayıncının görev ve sorumluluklarından bir dereceye kadar farklılık gösterebilir.”*³⁸⁸

Mahkeme, bu değerlendirmesiyle her ne kadar yeni medyayı geleneksel medyadan ayırsa da başvurucunun ekonomik menfaatlerle internet haber portalı işleten bir medya yayıncısı olduğu tespitiyle, somut dava bakımından Delfi’nin rolünü basılı medya yayıncılarına yakın şekilde değerlendirmiştir. Nitekim, basılı medyaya yönelik iç hukuk düzenlenmeleri de aynı gerekçeyle, yasayla öngörülmüş olma şartı bakımından yeterli görülmüştür.³⁸⁹ Mahkeme, aynı yaklaşımını, yayıncı sorumluluğu bakımından da devam ettirmiş görünmektedir.

Bu noktada, şirketin tehdit, hakaret, müstehcen ifadeler veya küfür içeren ya da kine, şiddete ya da yasadışı eylemlere teşvik eden yorumlarla ilgili olarak otomatik filtreleme ile uyar-kaldır sistemi şeklinde iki mekanizma olduğunu tespit etmekle birlikte otomatik filtreleme sisteminin yeterince başarı sağlamaması ve yorumların uyarı beklenmeden derhal kaldırmaya yönelik tedbirler alınmaması³⁹⁰ gerekçeleriyle Sözleşme’nin 10. maddesinin ihlal edilmediğine hükmetmiştir. Mahkemenin bu gerekçelendirmesi, internet şirketleri bakımından yeni bir sorunu beraberinde getirmiştir: Bir internet şirketi olan Delfi, söz konusu yorumun yayımlanmasını engellemediği için

³⁸⁸ Delfi AS v. Estonia, para. 113.

³⁸⁹ Delfi AS v. Estonia, para. 128.

³⁹⁰“Sonuç olarak, başvuran şirketin portalında yayınlanan yorumlar üzerinde önemli ölçüde denetleme uyguladığının kabul edilmesi gerektiğine yönelik yukarıda belirtilen hususlar dikkate alındığında Mahkeme, başvuran şirkete, nefret söylemi içeren ve şiddete teşvik eden ve bu nedenle açıkça hukuka aykırı olan yorumların yayınlanır yayınlanmaz hemen kaldırılmasına yönelik bir yükümlülük getirmenin, ilke olarak, şirketin ifade özgürlüğüne orantısız müdahale teşkil etmeyeceğini değerlendirmiştir.” para. 159. AİHM’in, herhangi bir uyarı ya da bilgi sahibi olup olmamaya bakılmaksızın üçüncü taraf içeriğinden sorumluluğu kabul eden bu anlayışı, araçlara sistematik ve proaktif bir izleme sorumluluğu yüklediğinden, kararın en tartışmalı yönlerinden biri olmuştur McGonagle, “The Council of Europe and Internet Intermediaries”, s. 235.

mi, yoksa engellemediği gibi daha sonra da kaldırmadığı için mi sorumlu tutulmuştur? Mahkeme, Delfi AS kararında, bu soruyu cevapsız bırakmıştır.³⁹¹

AİHM daha sonra, internet servis sağlayıcılarının sorumluluğu ve yükümlülüğü sorunlarını *Magyar Tartalomsgátlatók Egyesülete and Index.hu Zrt/Macaristan* davasında yeniden değerlendirmiştir.³⁹² Biri internet içerik sağlayıcıları öz denetim kurulu, diğeri bir internet haber portalı olan iki başvuru tarafından yapılan başvuru, iki emlak sitesinin aldatıcı uygulamalarının eleştirildiği bir görüşün yayınlanmasının ardından, internet sitelerinde paylaşılan kaba ve hakaret içerikli yorumlar konusundaki sorumluluklarına ilişkindir. Başvuru, Delfi AS başvurusu ile başvurunun konusu bakımından olduğu gibi, başvuru sahiplerinin aldıkları tedbirler bakımından da benzerlik göstermektedir. Delfi AS’de olduğu gibi bu başvuruda da a) her iki başvuru da portalların genel koşullarında, başkalarının haklarına zarar veren yasa dışı yorumların yasak olduğunu ve yorumlardan yazarlarının sorumlu olduğunu belirtmişlerdir, b) her iki başvuru sahibinin de hukuka aykırı yorumlara ilişkin olarak uyar-kaldır sistemleri mevcuttur ve c) ikinci başvuru -internet haber portalı- portalındaki yorumları kısmi olarak takip eden bir ekip kurmuştur.

AİHM de Delfi AS kararında olduğu gibi burada da, başvuru sahiplerinin konumuna ilişkin bir tespitle birlikte, ifade özgürlüğüne etkilerini belirtmiştir: “Mahkeme, hem *birinci başvuru sahibinin internet servis sağlayıcılarının kendi kendini düzenleyen bir kuruluşu olarak, hem de ikinci başvuru sahibinin büyük bir haber portalı olarak ifade haklarının kullanımına olanak tanıyan bir forum sağladığını ve halkın bilgi ve fikirleri iletebilmesini sağladığını belirtir.*”³⁹³ Mahkeme, internet portallarının da çeşitli görev ve sorumlulukları olması gerektiğini yinelemiş, ancak internetin özel doğası nedeniyle bu

³⁹¹ Mahkemenin bu tavrı mutabık görüşteki yargıçlar tarafından da eleştirilmiştir: “7. Bu nedenle bize göre, bir haber portalını kullanıcı tarafından oluşturulan yorumların yayınlanmasını ‘engellemediği’ için sorumlu bulmak, portalın her türlü hukuka aykırı yoruma yönelik sorumluluktan kaçınması için kullanıcı tarafından oluşturulan bütün yorumları tek tek ön denetlemeye tabi tutması anlamına gelecektir. Bu durum, uygulamada, haber portalının Sözleşme’nin 10. maddesi ile güvence altına alınan ifade özgürlüğüne orantısız bir müdahaleye yol açabilir. 8. İkinci olarak, Mahkeme Sözleşme’nin 10. maddesinin ihlal edilmediği yönünde karar vermesine yol açan temel ilkeleri açık bir şekilde belirtmeliydi. Mahkeme bunun yerine, davaya özgü gerekçeler benimsemiş ve bununla birlikte ilgili ilkeleri sonraki içtihatla daha açık bir şekilde geliştirilmeye bırakmıştır. 9. Bize göre, Mahkeme mevcut dava gibi bir davanın değerlendirilmesine ilişkin ilkeleri daha açık bir şekilde belirtme imkânını kullanmalıydı.” Delfi as v. Estonia Joint Concurring Opinion Of Judges Raimondi, Karakas, De Gaetano And Kjølbrot, para. 7-9.

³⁹² Magyar Tartalomsgátlatók Egyesülete and Index.hu Zrt v. Hungary, 22947/13 (ECtHR 02 Şubat 2016).

³⁹³ Magyar Tartalomsgátlatók Egyesülete and Index.hu Zrt v. Hungary para. 61.

görevler ve sorumlulukların özellikle üçüncü taraf içerikleri konusunda geleneksel bir yayıncıdan farklılık gösterebileceğinin altını çizmiştir.³⁹⁴

Sonuç olarak bakıldığında, *MTE and Index.Hu Zrt* kararında, Delfi AS kararının aksine ve belki de söz konusu kararın eleştirel sonuçlarından dolayı AİHM, internet araçlarının çevrimiçi kamuoyunda tartışmayı teşvik etmedeki rollerine üstünlük tanımıştır.³⁹⁵ Öyle ki Mahkeme, başvuru sahipleri “özgür medyanın kahramanları”³⁹⁶ olarak nitelendirmiş, internet portallarının üçüncü taraf içeriklerinden sorumlu tutulmasının, bu portalları örneğin yorum alanını tamamen kapatmaya zorlayarak, portalın yorum ortamı üzerinde öngörülebilir olumsuz etkilere neden olabileceğine dikkat çekmiştir.³⁹⁷ AİHM, Delfi AS’dan açık bir şekilde ayrılan bu kararı şu şekilde gerekçelendirmektedir:

*“Ancak, bu dava farklıdır. İncelenen yorumlar, saldırgan ve kaba olmasına rağmen (yukarıdaki 12 ve 14. paragraflara bakınız), açıkça yasa dışı bir konuşma oluşturmamıştır ve kesinlikle nefret söylemi veya şiddeti teşvik etmiş değildir. Dahası ikinci başvuru sahibi, ekonomik çıkarlara sahip olarak kabul edilmesi gereken büyük bir medya kuruluşunun sahibidir, birinci başvuru ise bilinen böyle bir çıkarı olmayan kâr amacı gütmeyen internet servis sağlayıcılarının öz düzenleyen bir derneğidir.”*³⁹⁸

“Elbette ki üçüncü tarafların kullanıcı yorumları nefret söylemi şeklinde ve bireylerin fiziksel bütünlüğüne doğrudan tehditler şeklinde ortaya çıkarsa başkalarının ve toplumun hakları ve çıkarları, Sözleşme taraflarını, belirli bir süre içinde açıkça yasa dışı yorumları kaldırmamışlarsa, internet haber portallarına sorumluluk yüklemeye yetkili kılabilir. Ancak, mevcut durum böyle ifadeler içermemektedir.”

³⁹⁴ Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary, para. 62.

³⁹⁵ Bu iki kararın karşılaştırmalı değerlendirmesi için bkz. Marta Maroni, “A Court’s Gotta Do, What a Court’s Gotta Do. An Analysis of the European Court of Human Rights and the Liability of Internet Intermediaries Through Systems Theory”, *EUI Working Papers*, 2019; Benedek Wolfgang, Matthias C. Kettemann, “Freedom of Expression and the Internet”, Council of Europe, Updated and Revised 2nd Edition.2020, ss. 139-41.

³⁹⁶ Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary, para. 88.

³⁹⁷ Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary, para. 86.

³⁹⁸ Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary, para. 64.

Anlaşılabacağı üzere AİHM, söz konusu başvurudaki değişen yaklaşımının gerekçesini yorumların içeriğindeki farklılık ile açıklamaktadır. AİHM her ne kadar, başvuru kuruluşların amacı bakımından da farklılaştığına dikkat çekmek istese de “kâr amacı gütmeme” niteliği yalnızca ilk başvuru için geçerlidir; ikinci başvuru olan Index.Hu Zrt, Delfi AS gibi kâr amacı güden bir şirkettir. Dolayısıyla, kâr amacı güdüp gütmemenin sorumluluğun belirlenmesinde esaslı bir kriter olduğunu söylemek mümkün görünmemektedir. MTE and Index.Hu Zrt kararında, internet servis sağlayıcısına yönelik muameledeki farklılığı haklı kılan tek husus içeriğin açıkça hukuka aykırı olmamasıdır.³⁹⁹

İnternet araçlarının üçüncü taraf içeriklerinden sorumluluğunda içeriğin bu belirleyici etkisi, daha sonra *Pihl/İsveç*⁴⁰⁰ kararında da onaylanmıştır. İnternet araçlarının ifade özgürlüğünün ihlal edildiği iddiasına ilişkin önceki başvurulardan farklı olarak Pihl/İsveç başvurusunda başvuru kişi, üçüncü taraflarca hakkında yorum yapılmasına aracılık eden bir web sitesi sahibinin söz konusu içeriklerden sorumlu tutulmamasının özel hayata saygı hakkını ihlal ettiğini iddia etmiştir.⁴⁰¹ Söz konusu yorumlarda başvuru, bir Nazi partisine dahil olmakla ve esrar bağımlısı olmakla itham edilmiştir.

Pihl/İsveç davası bakımından da yorumların içeriği kararda belirleyici olmuştur. AİHM; yorumun, saldırgan olmasına rağmen nefret söylemi veya şiddeti kışkırtma düzeyine ulaşmadığını göz önüne alarak, iç hukuk mahkemelerinin takdir yetkisi içinde hareket ettiklerine ve başvuranın 8. madde uyarınca hakları ile web sitesi sahibinin 10. madde uyarınca ifade özgürlüğüne arasında adil bir denge sağladıklarına karar vermiştir.⁴⁰²

AİHM, Pihl/İsveç kararında da söz konusu web sitesi sahibinin kâr amacı gütmeyen bir dernek olduğunun altını çizse de daha önce de belirttiğimiz gibi MTE and

³⁹⁹ Oreste Pollicino, “Judicial Protection of Fundamental Rights in the Transition from the World of Atoms to the Word of Bits: The Case of Freedom of Speech”, **European Law Journal**, 2019, s. 160, <https://papers.ssrn.com/abstract=3371697>.

⁴⁰⁰ Pihl v. Sweden, 74742/14 (ECtHR 07 Şubat 2017).

⁴⁰¹ AİHM, Sözleşme’nin 8. ve 10. maddeleri bakımından özel hayata saygı hakkı ve ifade özgürlüğünün eşit saygıyı hak ettiğini ve başvurunun bu iki hakkın öznelinden hangisi tarafından yapıldığının bir fark yaratmayacağını belirtmektedir. Buna göre her iki durumda da takdir marjı, ilke olarak aynı olmalıdır ve bu iki hak arasındaki dengeleme işleminin ulusal makamlar tarafından Mahkeme’nin içtihadında belirtilen kriterlere uygun olarak yapıldığı durumlarda, Mahkeme’nin kendi görüşünü yerel mahkemelerin görüşünün yerine koyması için güçlü nedenler gerekmektedir. Bu yaklaşım, devletlerin internet şirketlerinin insan hakları sorumluluklarına ilişkin pozitif yükümlülükleri bakımından da genel bir prensibi ortaya koymaktadır. Pihl v. Sweden, para. 27.

⁴⁰² Pihl v. Sweden, para. 37.

Index.Hu Zrt kararı bu amacın söz konusu sorumlulukların belirlenmesinde belirleyici olmadığını göstermektedir. Ayrıca, AIHM bu davada Delfi AS kararındaki yaklaşımını da gerekçelendirerek, araçların sorumluluğuna ilişkin ilgili yorumun yayında kaldığı sürenin de önemli olduğuna dikkat çekmiştir. Buna göre Delfi AS kararında şikâyet konusu yorumlar ancak altı hafta sonra kaldırılmışken Pihl/İsveç kararında ilgili yorum dokuz gün sonra siteden kaldırılmıştır.⁴⁰³ AIHM'in bu yaklaşımının, yorumun yürürlükte kaldığı süre arttıkça kişilik haklarına aykırılığın da artacağı çıkarımına dayandığı anlaşılmaktadır. Ne var ki internet araçlarının sorumluluklarını belirlerken önemli olan, kişilik haklarına aykırı yorumun yayınlandığı süre değil, internet aracısının söz konusu yorumla ilgili olarak uyar-kaldır mekanizmasını gerekli ve yeterli şekilde işletip işletmediğidir. Her iki başvuruda da hakkında ilgili kişinin uyarısı üzerine yorumlar bir gün içerisinde kaldırılmıştır. Dolayısıyla Pihl/İsveç davasında yorumun daha kısa süre yayında kalmasının nedeni, başvurucunun uyar-kaldır mekanizmasını erkenden işletmesidir. Mahkeme'nin bu gerekçelendirmesi, dolaylı da olsa, internet araçlarına herhangi bir uyarı almadan yorumları kontrol etme şeklinde bir sorumluluk yükleyebilecek niteliktedir.

Nitekim, Pihl kararından aylar sonra verilen *Tamiz/Birleşik Krallık*⁴⁰⁴ kararında da internet aracısının uyar-kaldır mekanizmasını etkili bir şekilde işletip işletmediği, aracının sorumluluğunun belirlenmesine ilişkin tartışma konusu yapılan hususlardan biri olmuştur. Bu başvuruda da başvuru, Google Inc.'e ait bir blog barındırma hizmeti olan "Blogger.com" tarafından barındırılan bir blogda yayımlanan kendisiyle ilgili ve fotoğrafının yer aldığı bir yazının yorumlar bölümünde yer alan yorumların, kişilik haklarını ihlal ettiğini iddia etmiştir. AIHM, yorumların saldırgan olduğunu kabul etmekle birlikte belli bir seviyede kalması (*vulgar abuse*), ilgilinin uyarısı üzerine çeşitli adımlar atması ve Google Inc. gibi bilgi toplumu hizmet sağlayıcıların (*ISSP'lerin*) çok çeşitli siyasi, sosyal ve kültürel konularda bilgiye erişimi ve tartışmayı kolaylaştırmada oynadıkları önemli rolü göz önünde bulundurarak ulusal mahkemelerin ifade özgürlüğü ile özel hayata saygı hakkı arasında adil denge kurduklarına karar vermiştir.⁴⁰⁵

⁴⁰³ Pihl v. Sweden, para. 32.

⁴⁰⁴ Tamiz v. The United Kingdom, 3877/14 (ECtHR 19 Eylül 2017).

⁴⁰⁵ Tamiz v. The United Kingdom, para. 90.

Tamiz/Birleşik Krallık kararında, Pihl/İsveç kararında ima edilen görüşün aksine, yorumların yayında kaldığı süre değil, internet aracısının yorumla ilgili olarak uyar-kaldır mekanizmasını gerekli ve yeterli şekilde işletip işletmediği hususu üzerinde durulmuştur. Başvurucu, içeriğin kaldırılması sürecinin dört ay sürdüğünü ve bu süreçte yorumların itibarı üzerinde ciddi ve olumsuz bir etkisi olduğunu ileri sürmüştü de AİHM, internet şirketinin sorumluluğunu belirlerken başvurucunun farklılaşan beyanları üzerinden uyarının hangi tarihte yapıldığını netleştirmeye yönelik bir çaba içerisine girmiştir.⁴⁰⁶

Aracı sorumluluğuna ilişkin ilerleyen süreçte verdiği *Hoiness/ Norveç*⁴⁰⁷ kararında da AİHM, internet şirketinin uyar-kaldır sisteminin etkililiğine dikkat çekmiştir. Dava konusu Hegnar Online'ın o zamana kadar bünyesine dahil olduğu Hegnar Media AS şirketi, herhangi birinin uygunsuz bulabileceği forum yorumlarını şikâyet etmeyi kolaylaştıran bir yaklaşım benimsemiştir: i) her bir gönderinin yanında şirketi uyarmak için tıklanabilecek bir bağlantı ("uyarı düğmesi") bulunuyordu ve şirket bu tür şikâyetler aldığı anda bu durum, genellikle yorumun silinmesiyle sonuçlanmaktaydı; ii) şirketin forum kurallarını ihlal eden yorumları kendi inisiyatifleriyle kaldıran moderatörleri de bulunmaktaydı; iii) ilgili kişinin mail gibi alternatif yöntemlerle de uyarıda bulunabilmesi ve yorumları kaldırtabilmesi mümkündü.⁴⁰⁸ Somut başvuruda çevrimiçi haber portalı Hegnar Online tarafından işletilen tartışma forumunda yayınlanan karalayıcı yorumlardan biri, forum moderatörleri tarafından kendi inisiyatifleri ile, diğer iki yorum ise başvurucunun uyarısı üzerine yalnızca on üç dakika sonra kaldırılmıştır. AİHM, forum yöneticisi tarafından alınan önlemlerin ve başvurucunun bildirimlerine verilen yanıtları bir bütün olarak değerlendirerek yerel mahkemelerin, başvuranın 8. madde kapsamındaki hakları ile haber portalı ve tartışma forumlarının sunucusunun 10. madde kapsamındaki ifade özgürlüğü hakkı arasında bir denge kurmaya çalışırken takdir marjları dahilinde hareket ettiklerini tespit etmiştir.⁴⁰⁹

Her ne kadar doğrudan internet şirketlerini konu almasa da AİHM'nin *Sanchez/Fransa* kararı, şirketlerin insan hakları sorumlulukları da dahil internet yönetimi

⁴⁰⁶ Kararda, başvuru Google Inc'ye bildirimde bulunduktan sonra kendisiyle ilk defa iki ay sonra iletişim kurulduğunu iddia etmiştir. Ancak AİHM, ulusal yargılama süreçlerinde başvurucunun bu konuda herhangi bir itirazda bulunmadığına ve bu yönde bir delil de sunmadığına dikkat çekerek, ulusal mahkemelerin bu konudaki bulgularına itiraz edilemeyeceğini belirtmiştir. *Tamiz v. The United Kingdom*, para. 33, 65, 88.

⁴⁰⁷ *Hoiness v. Norway*, 43624/14 (ECtHR 19 Mart 2019).

⁴⁰⁸ *Hoiness v. Norway*, para. 21.

⁴⁰⁹ *Hoiness v. Norway* para. 73-75.

ve sosyal medya hesabı kullanımına ilişkin önemli bir karardır.⁴¹⁰ Karar, AİHM'in Avrupa Birliği'nde online içeriğe ilişkin kabul edilen güncel metinlerin de yansımalarını içermektedir. Sanchez/Fransa kararının konusu, bir politikacı ve parlamento seçimlerinde aday olan Bay Sanchez'in, Facebook "duvarında" siyasi rakiplerinden biri hakkında yaptığı paylaşımına yapılan üçüncü taraf yorumlarından dolayı adli para cezasına mahkûm edilmesinin ifade özgürlüğünü ihlal edip etmediğidir. Söz konusu paylaşım yapılan çok sayıda yorumdan ikisinde, Bay Sanchez'in hakkında paylaşım yaptığı siyasi rakibi FP ve partneri Leila T ile Müslümanlara yönelik aşağılayıcı ifadeler yer verilmiştir.⁴¹¹

AİHM, başvuruyu incelerken üçüncü taraf içeriklerinden sorumluluğu ayrı bir başlık olarak ele almıştır. AİHM, Delfi AS kararından itibaren, üçüncü taraf içeriklerine ilişkin başvurularda şu unsurları göz önünde bulundurduğunu belirtmiştir: ilk olarak, yorumların bağlamı; ikinci olarak, başvuran şirketin iftira içeren yorumları önlemek veya kaldırmak için uyguladığı önlemler; üçüncü olarak, başvuran şirketin sorumluluğuna alternatif olarak yorumların gerçek yazarlarının sorumluluğu ve dördüncü olarak, iç hukuk süreçlerinin başvuran şirket bakımından sonuçları.⁴¹² Somut başvuru bakımından özellikle yorumların bağlamı ve söz konusu yorumlar karşısında alınan önlemlere ilişkin tespitler dikkat çekicidir.

Öncelikle, yorumların bağlamı bakımından AİHM, mevcut siyasi ve sosyal iklimi göz önünde bulundurarak seçimler bağlamında, ırkçı ve yabancı düşmanı söylemin etkisinin daha büyük ve daha zararlı hale gelebileceğini belirtmiş; yorumların içeriklerini, genel tonlarını, bazı ifadelerin şiddeti ve argo kullanılan dilin ahlaki olmayan özelliklerini öne sürerek nefret söylemi oluşturduklarını tespit etmiştir. Mahkeme, yorumların bağlamı bakımından ayrıca, internet ortamında Facebook "duvarının" konumunu belirlemeye çalışmıştır:

⁴¹⁰ Sanchez v. France, 45581/15 (ECtHR [GC] 15 Mayıs 2023).

⁴¹¹ Söz konusu yorumlarda, *Bay Sanchez'in siyasi rakibi FP ve ortağı Leila T'ye ve Müslümanlara yönelik, şehri Cezayir'e çevirdikleri, kebab salonu ve cami olmayan bir sokak kalmadığı, şehrin merkezinde nargile barları ve örtülü kadınlar olduğu, Müslümanlar tarafından yıllardır uyuşturucu ticareti yapıldığı, okulların önünde "beyaz insanlara" taş attıkları, şehrin güvensizlik başkenti olduğu...* ifadeleri yer almaktadır. Sanchez v. France, para. 15.

⁴¹² Sanchez v. France, para. 163.

“Mahkeme, davacının Facebook ‘duvarının’, hükümetin iddiasının aksine, ‘ticari amaçlarla işletilen büyük, profesyonel olarak yönetilen bir İnternet haber portalı’ ile karşılaştırılamayacağını belirtmektedir. Yukarıda belirtilen Delfi AS kararında (§ 116) belirtildiği gibi, üçüncü taraf yorumlarının yayınlanabileceği ‘İnternet’teki diğer forumlar’ kategorisine girdiğine şüphe yokken, mevcut davanın kendine has özellikleri, Mahkeme’yi bu soruya, Sözleşme’nin 10 § 2 maddesi anlamında, sosyal medyayı siyasi amaçlarla, özellikle de seçim hedeflerine ulaşmak için, internette kullanıcıların tepkilerinin ve yorumlarının yayınlanabileceği kamuya açık forumlar açarak kullanmaya karar verdiklerinde siyasetçilere atfedilmesi gereken ‘görev ve sorumluluklar’ ışığında yaklaştırmaya sevk etmektedir. Davacı sadece özel bir kişi değildi ve kendisi bu hesabı yerel meclis üyesi, siyasi amaçlarla ve bir seçim bağlamında kullandığını belirtmiştir. Mahkeme ayrıca, davacının sadece siyaset alanında profesyonel olmadığını, aynı zamanda dijital hizmetler alanında da bir miktar uzmanlığa sahip olduğunu not eder...”⁴¹³

Anlaşılabileceği üzere AİHM, başvurucunun Facebook duvarının bir internet portalı olarak nitelendirilemeyeceğini belirtmekle birlikte bir siyasetçi tarafından ve siyasi amaçlarla kullanıldığını göz önünde bulundurarak “platform sağlayıcısının hiçbir içerik sunmadığı ve içerik sağlayıcısının web sitesini veya blogu bir hobi olarak işletebilecek özel bir kişi olabileceği bir sosyal medya platformu” olarak da değerlendirilemeyeceğini ortaya koymuştur.⁴¹⁴ AİHM bu noktada, hesap sahibinin yorumlara ilişkin görev ve sorumluluklarını belirlerken; profesyonel kuruluşlardan farklı olarak başvurucunun otomatik filtreleme ya da tüm yorumları etkili bir şekilde izleme gibi araçları olmadığını kabul etmekle birlikte her bir aktörün objektif durumuna göre sorumluluk derecesinin belirlenmesi gerektiğini, aksinin (bir muafiyet tanınımının) kötüye kullanımı teşvik etme veya kolaylaştırma riski taşıyabileceğini ifade etmiştir.⁴¹⁵

AİHM ikinci olarak, başvuran tarafından alınan önlemlere ilişkin değerlendirmeye geçmiştir. AİHM, her ne kadar somut davada platformun kendisine yönelik bir hak ihlali iddiasında bulunulmamışsa da söz konusu değerlendirmeyi yaparak

⁴¹³ Sanchez v. France, para. 180.

⁴¹⁴ Sanchez v. France, para. 179.

⁴¹⁵ Sanchez v. France, para. 185.

internet şirketlerinin açıkça hukuka aykırı içerikler bakımından sorumluluklarını bir kez daha hatırlatmıştır:

“Mahkeme ilk olarak, ister kullanıcıları için bir sosyal ağ oluşturan ve sağlayan profesyonel bir kuruluş olarak hareket eden ev sahibinin kendisi (bu durumda Facebook) tarafından, ister platformu kendi makalelerini veya görüşlerini yayınlamak için kullanan ve diğer kullanıcıların yorumlarını eklemesine izin veren hesap sahibi tarafından yapılsın, zarar gören bir tarafça herhangi bir bildirim yapılmamış olsa bile, açıkça hukuka aykırı yorumları mümkün olduğunca çabuk tespit etmek ve makul bir süre içinde silinmelerini sağlamak için asgari düzeyde bir sonradan moderasyon veya otomatik filtrelemenin arzu edileceğinden şüphe edilemeyeceğini gözlemlemektedir.”⁴¹⁶

Yukarıdaki değerlendirmesiyle AİHM, açıkça hukuka aykırı üçüncü taraf içerikler söz konusu olduğunda, bu içeriklerin yayımlanmasında etkili olan tüm aktörlerin söz konusu içeriklere ilişkin görev ve sorumluluklarının olduğunu ortaya koymuştur. Somut dava bakımından, hesabını tüm kamunun erişimine açan ve ulusal düzeyde tanınan bir politikacı olan başvurucunun sorumluluk derecesinin, sözlerinin kapsamı ve ağırlığı ile sosyal medya platformlarına etkili bir şekilde müdahale etmek için sahip olduğu kaynaklar dolayısıyla, özel bir kişi ya da yerel bir figüre göre daha ağır olacağı değerlendirilmiştir.⁴¹⁷

AİHM, *Zöchling/Avusturya*⁴¹⁸ kararında da Delfi AS ve Sanchez/Fransa kararlarındaki içtihadını sürdürerek, internet şirketlerinin üçüncü taraf içeriklerinden sorumluluğunu özellikle içeriğin niteliği ile başvuru tarafından alınan önlemleri dikkate alarak belirlemeye çalışmıştır. Bu başvuru, Delfi AS ve Sanchez/Fransa kararlarından farklı olarak bir internet haber portalının yayıncısının, kullanıcıların yorumlarındaki nefret söyleminden sorumlu tutulmasının reddedilmesine ilişkin bir şikayetle ilgilidir.⁴¹⁹ Başvurucu, internet şirketi tarafından portalda yayımlanan ve

⁴¹⁶ Sanchez v. France, para. 190.

⁴¹⁷ Sanchez v. France, para. 201.

⁴¹⁸ Zöchling v. Austria, 4222/18 (ECtHR 05 Eylül 2023).

⁴¹⁹ AİHM, ifade özgürlüğü ile kişilik haklarının karşı karşıya geldiği durumlarda başvurunun, saldırgan bir makalenin yayıncısı tarafından 10. madde kapsamında mı yoksa makalenin konusu olan kişi tarafından 8. madde kapsamında mı yapıldığına göre sonuçlanmaması gerektiğini, her iki durumda da takdir yetkisinin aynı olması gerektiğini belirtmektedir. Axel Springer Ag v. Germany, 39954/08 (ECtHR [GC] 07 Şubat

başvurucunun fotoğrafını da içeren bir makalenin altındaki yorumlar dolayısıyla tazminat talebinde bulunmuş; ancak tazminat talebi Temyiz Mahkemesi tarafından internet şirketinin başvurucunun talebi üzerine söz konusu yorumu sildiği, bunun ötesinde tüm yorumları izleme gibi bir yükümlülüğü olmadığı, sonuç olarak şirketin özen yükümlülüğüne uygun davrandığı gerekçesiyle başvurucunun talebini reddetmiştir. AİHM, somut davada olduğu gibi açıkça nefret söylemi ve şiddete teşvik içeren yorumlar söz konusu olduğunda internet portallarına daha geniş sorumluluklar yüklenebileceğini, bunun da çatışan menfaatler arasında bir dengeleme yapılmasını gerektirdiğini belirtmiştir:

“Mevcut davada Temyiz Mahkemesi, şirketin portalında hakaret içeren içeriği önlemek veya bu tür içeriği kaldırmak için uygulayacağı olası önlemleri değerlendirmemiştir. Bölge Ceza Mahkemesi'nin, başvuran hakkındaki saldırgan yorumların Eylül 2015'ten bu yana şirketin portalında yayınlanan makaleler altında tekrar tekrar yayınlandığı ve böylece şirketin daha fazla suç işleyebileceğini öngörebileceği yönündeki tespitini dikkate almamıştır. Mahkeme, hukuka aykırı yorumları yasaklamak yerine kullanıcıları ‘istenmeyen’ yorumlar olduğu konusunda bilgilendirmenin tek başına nefret söylemini önlemeye yönelik etkili bir tedbir olarak görülüp görülemeyeceğini değerlendirmemiştir.”⁴²⁰

Bu değerlendirmeye birlikte AİHM, internet şirketlerinin kural olarak üçüncü taraf içeriklerini izleme yükümlülükleri olmadığını göz ardı etmemekle birlikte bu şirketlerin özen yükümlülükleri (*due diligence*) olduğunu yinelemiş ve çatışan menfaatler arasında herhangi bir dengeleme yapılmaması dolayısıyla özel hayata saygı hakkı bakımından usule ilişkin yükümlülüklerin yerine getirilmediğine ve Sözleşmenin 8. maddesinin ihlal edildiğine karar vermiştir.

Buraya kadarki kısımda incelenen Delfi AS/Estonia, MTE and Index.Hu Zrt/ Macaristan, Pihl/ İsveç, Tamiz/Birleşik Krallık, Hoiness/Norveç, Sanchez/Fransa ve Zöchling/Avusturya kararları birlikte değerlendirildiğinde, internet aracı şirketlerinin

2012), para. 87; Von Hannover v. Germany (no. 2), 40660/08, 60641/08 (ECtHR [GC] 07 Şubat 2012) para. 106; Mosley v. the United Kingdom, 48009/08 (ECtHR 10 Mayıs 2011), para. 111.

⁴²⁰ Zöchling v. Austria, para. 13.

üçüncü taraf içeriklerinden sorumluluğuna ilişkin bazı tespitlerde bulunmak ve söz konusu sorumluluğun kapsamını belirlemek mümkün görünmektedir. Buna göre söz konusu sorumluluğun kapsamına ilişkin ikili bir ayırım yapılması mümkündür: a) nefret söylemi ve şiddete teşvik niteliğindeki üçüncü taraf içerikleri, b) nefret söylemi ve şiddete teşvik içermemekle birlikte saldırgan, kaba vb. nitelikteki üçüncü taraf içerikleri.

AIHM, ilk kategori bakımından, Delfi AS kararından itibaren internet aracı şirketlerinin üçüncü taraf içeriklerinden sorumlu tutulabilmesi konusunda devletlerin geniş bir takdir marjı olduğunu ifade etmektedir. Nitekim internet araçlarının ifade özgürlüklerinin öne çıkarıldığı sonraki kararlarda AIHM, Delfi AS kararının, yorumların niteliği bakımından farklılaştığını ve bu farklılığın da aracı şirkete, ilgili kişinin uyarısı beklenmeksizin içeriğe müdahale de dahil daha kapsamlı bir sorumluluk yüklediğini açıkça ortaya koymuştur. Sanchez/Fransa kararında, Delfi AS'den farklı olarak, söz konusu sorumluluklarının gereklerini yerine getirmeyen aracıya cezai yaptırım uygulanmasının da ifade özgürlüğüne aykırılık teşkil etmediğine karar vermiştir.⁴²¹ Nefret söylemi ve şiddete teşvik içermemekle birlikte saldırgan, kaba vb. nitelikteki üçüncü taraf içerikleri bakımından ise AIHM, somut davaya göre farklı kriterler geliştirse de prensip olarak internet şirketlerini ya da kâr amacı gütmeyen araçları uyar-kaldır mekanizmasını etkili bir şekilde işlettikleri sürece hukuka aykırı içeriklerden sorumlu tutmamakta ve aksinin araçlar üzerinde caydırıcı etkiye yol açabileceğini kabul etmektedir.

AIHM *Magyar Jeti Zrt / Macaristan* kararında⁴²² ise internet şirketlerinin üçüncü taraf içeriklerinden sorumluluğu farklı bir bağlamda ele alınmıştır. İnternet şirketlerinin yayınlarında yer alan köprülerden (hyperlink) sorumlu tutulup tutulamayacağına ilişkin bu karar, Mahkeme'nin üçüncü taraf içerikleri bakımından yukarıda belirtilen yaklaşımının devamı niteliğinde olsa da internet ortamında köprülere ilişkin önemli değerlendirmeler içermektedir:

“Ayrıca, İnternet'in halkın haber ve bilgiye erişimini artırmadaki rolünü akılda tutarak Mahkeme, köprülerin amacının, başka sayfalara ve web kaynaklarına yönlendirerek, İnternet kullanıcılarının birbirine bağlı bir ağda bulunan

⁴²¹ Päivi Korpisaari, “From Delfi to Sanchez – when can an online communication platform be responsible for third-party comments? An analysis of the practice of the ECtHR and some reflections on the Digital Services Act”, **Journal of Media Law**, C. 14, S. 2, 2022, s. 370.

⁴²² *Magyar Jeti Zrt v. Hungary*, 11257/16 (ECtHR 04 Aralık 2018).

malzemelere gidip gelmesine izin vermek olduğunu belirtir. Köprüler, bilgileri birbirine bağlayarak erişilebilir hale getirip İnternet'in sorunsuz çalışmasına katkıda bulunur.

Köprüler, genel olarak, kullanıcıları yalnızca İnternet'in başka bir yerinde bulunan içeriğe yönlendirdiklerinden dolayı, bir raporlama tekniği olarak, geleneksel yayınlama eylemlerinden farklıdır. Bağlantılı ifadeleri izleyiciye sunmazlar veya içeriğini iletmezler, yalnızca okuyucuların başka bir web sitesinde malzeme olduğunu fark etmelerine hizmet ederler.

Köprüleri bilgi yayma eylemlerinden ayırt eden bir başka özelliği, bilgilere bir köprü aracılığıyla atıfta bulunan kişinin, köprüünün erişim sağladığı ve bağlantı oluşturulduktan sonra değiştirilebilecek web sitesinin içeriği üzerinde kontrol sahibi olmamasıdır - Köprüünün aynı kişi tarafından kontrol edilen içeriğe işaret etmesi doğal bir istisnadır. Ayrıca, köprüünün arkasındaki içerik, zaten onu yönlendirdiği web sitesinde ilk yayıncı tarafından kullanıma sunulmuş ve kamuya sınırsız erişim sağlanmıştır.

Sonuç olarak, köprülerin özelliklerini göz önüne alarak Mahkeme, yerel mahkemelerin köprü göndermeyi karalayıcı ifadelerin yayılmasıyla eşdeğer tutan, bu içeriğin kendisinden otomatik olarak sorumluluğunu gerektiren yaklaşımına katılamaz. Mahkeme bunun yerine, bir köprü yayınlamanın, 10. madde perspektifinden haklı olarak böyle bir sorumluluğa yol açıp açmayacağının sorununun, her durumda bir dizi unsur dikkate alınarak bireysel bir değerlendirme yapılmasını gerektirdiğini düşünmektedir.

Mahkeme, başvuru şirketin köprüünün yayıncısı olarak sorumluluğunu analizinde aşağıdaki hususları özellikle ilgili olarak belirler: (i) gazeteci itiraz edilen içeriği onayladı mı; (ii) gazeteci itiraz edilen içeriği tekrarladı mı (onaylamadan); (iii) gazeteci sadece itiraz edilen içeriğe bir bağlantı mı ekledi (onaylamadan veya tekrarlamadan); (iv) gazeteci itiraz edilen içeriğin karalama içerdiğini veya başka şekilde yasadışı olduğunu biliyor muydu ya da kendisinden bilmesi beklenebilir

*miydi? (v) gazeteci iyi niyetle hareket etti mi, gazetecilik etiklerine saygı duydu mu ve sorumlu gazetecilikte beklenen özeni gösterdi mi?*⁴²³

İnternet şirketlerinin bir üçüncü taraf içeriği olarak köprülerden sorumluluğunun ilk defa incelendiği bu kararda, söz konusu sorumluluğun değerlendirilmesinde beş sorudan oluşan bir test önerilmektedir. Somut başvuru bakımından AİHM, bu soruların tamamına olumsuz yanıtlar vererek bu şartlar altında makale yazarına ya da yayıncıya objektif sorumluluk yüklemenin onları değişken içeriği üzerinde hiçbir kontrolleri olmayan malzemelere köprü vermekten tamamen kaçınmaya zorlayabileceğine ve internetteki bilgi akışında öngörülebilir olumsuz sonuçlara yol açabileceğine dikkat çekmiştir.

AİHM, bu kararda da Delfi AS kararında ortaya koyduğu temel prensipten sapmamaya çalışmış, kararını gerekçelendirirken aracının yönlendirdiği köprünün içeriğine de dikkat çekmiştir. Böylece AİHM, söz konusu içeriğin bir politikacı hakkında olduğunu da göz önüne alarak *“gazetecinin, sağladığı erişime rağmen içeriğin tartışmalı olabileceğini, ancak muhtemelen siyasi partilere yönelik eleştirilerin hoşgörü sınırları içinde kalacağını ve bu nedenle yasa dışı olmayacağını makul bir şekilde varsayabileceğini”* düşünmüştür. Buna göre içeriğin nefret söylemi ya da şiddete teşvik gibi açıkça hukuka aykırı olduğu durumlarda ifade özgürlüğü ile özel hayata saygı hakkı arasında kurulacak dengenin farklı bir sonucu olabileceğini; ancak, diğer üçüncü taraf içeriklerine kıyasla köprülerin -içeriğinin daha sonradan aracının bilgisi dışında değişebileceği hususu da dikkate alındığında- daha sınırlı bir sorumluluk rejimine tabi tutulacağını söylemek mümkündür.⁴²⁴

⁴²³ Magyar Jeti Zrt v. Hungary, para. 73-77.

⁴²⁴ Karar’da, köprülere ilişkin olarak yer verilen uluslararası hukuk içtihatları da bu görüşü desteklemektedir. AİHM’in bu kapsamda atıfta bulunduğu kararlardan biri, Kanada Yüksek Mahkemesi’nin Crookes v. Newton kararıdır. (2011, SCC 47, [2011] 3.S.C.R. 269) Bu kararda, Kanada Yüksek Mahkemesi, hakaret içeren materyale köprü oluşturma hakkı hakaret içeren ifadelerin yayınlanması anlamına gelip gelmediği konusunu ele almış, bir kişinin sadece üçüncü taraf bir web sitesine veya hakaret içeren bir belgeye köprü yayınlayarak bir kişiyi karalayamayacağına karar vermiştir. Mahkemenin görüşü tam olarak şu şekildedir: *“Köprüler özünde referanslardır ve diğer ‘yayın’ eylemlerinden temelde farklıdır. Köprüler ve referansların her ikisi de bir şeyin var olduğunu bildirir, ancak içeriğini kendileri bildirmezler... Bir köprü, kendi başına asla atıfta bulunduğu içeriğin ‘yayınlanması’ olarak görülmemelidir. ... Yalnızca bunu yapan kişi veya kuruluş, köprü bağlantısı verilen materyaldeki içeriği, hakaret içeren içeriği gerçekten tekrarlayacak şekilde sunduğunda, bu içerik söz konusu kişi veya kuruluş tarafından ‘yayınlanmış’ olarak kabul edilmelidir.”* AİHM, Federal Alman Anayasa Mahkemesi’nin bir kararına da atıfta bulunmuştur. Buna göre, Federal Alman Anayasa Mahkemesi, 15 Aralık 2011 tarihli ve 1 BvR 1248/11 sayılı telif hakkının ihlal edildiği iddiasına ilişkin kararında, çevrimiçi bir makaleye köprü

2. Kişisel Verilerin Korunması ve Gizlilik

AİHM, kişisel verilerin korunması meselesini ilk defa *Leander/İsveç* kararında ele almış ve bir kamu otoritesi tarafından bir bireyin kişisel verilerinin depolanmasının, ulusal güvenliğin korunması amacına dayandığı gerekçesiyle Sözleşme'nin 8. maddesine aykırılık teşkil etmediğine karar vermiştir.⁴²⁵ Bilgi ve iletişim teknolojilerindeki gelişmelerin gözetim, iletişim, dinleme ve veri saklama araçları üzerindeki etkileriyle birlikte AİHM; kişisel verilerin toplanması⁴²⁶, saklanması⁴²⁷, kullanılması⁴²⁸, ifşa edilmesi⁴²⁹ ve silinmesine⁴³⁰ ilişkin çok çeşitli başvuruları karara bağlamıştır.

AİHM'nin kişisel verilerin korunmasına ilişkin içtihadı özellikle, kişisel verilerin kamu kurumları tarafından kaydedilmesi ve verilerin çeşitli amaçlarla kullanılmasına ilişkindir. Söz konusu başvurularda örneğin, suç isnadı altındaki kişilerin iletişiminin izlenmesi ve kolluk birimleri ya da adli makamlarla paylaşılması; biyometrik ya da tıbbi verilerin veya adli sicil kayıtlarının devlet arşivlerinde tutulması; kaydedilen kişisel verilere erişimin engellenmesi suretiyle kişisel verilerin korunması hakkının ihlal edildiği iddia edilmektedir.

AİHS'nin 8. maddesinin amacı esasen bireyi kamu makamlarının keyfi müdahalelerine karşı korumak olmakla birlikte, özel hayata saygı hakkının güvence altına

eklenmesinin Alman Anayasası kapsamında korunduğuna işaret etmiştir. Federal Anayasa Mahkemesi, başka bir web sitesine yönlendiren bir köprü yerleştirmenin, bunu yapan kişi veya kuruluşun web sitesinin içeriğini otomatik olarak kendi görüşü haline getirmedeğini vurgulamıştır. Federal Alman Anayasa Mahkemesi ayrıca, hukuka aykırı içeriğe sahip bir web sitesinin zaten bir internet arama motoru aracılığıyla çok kolay bir şekilde bulunabileceğini, dolayısıyla bu içeriğe bağlantı vermenin ayrıca bir ihlal teşkil etmeyeceğini belirtmiştir. Federal Alman Anayasa Mahkemesinin bu kararı, köprülerle ilgili yeni bir tartışma konusu ortaya çıkarmaktadır: Aracıların üçüncü taraf içerikleri bakımından ifade özgürlüğü ile kişilerin unutulma hakkı arasında nasıl bir dengeleme yapılacaktır? Zira Mahkeme, söz konusu bağlantıya arama motoru üzerinden kolayca erişilebilmesini, araçların söz konusu içeriğe ilişkin köprülerden sorumlu tutulmamalarının bir gerekçesi olarak kabul etmiştir. Ancak, unutulma hakkı kapsamında arama motorlarında liste dışı bırakılan URL'ler söz konusu olduğunda araçların sorumluluğunun kapsamı değişebilecektir. Ibid., para. 30.

⁴²⁵ *Leander v. Sweden*, 9248/81 (ECtHR 26 Mart 1987).

⁴²⁶ *Taylor-Sabori v. the United Kingdom* (dec.), 11782/85 (ECtHR 29 Mayıs 2001); *Uzun v. Germany*, 35623/05 (ECtHR 02 Eylül 2010); *L.h. v. Latvia*, 52019/07 (ECtHR 29 Nisan 2014).

⁴²⁷ *S. and Marper v. the United Kingdom*; *B.B. c. France*, 5335/06 (ECtHR 26 Ocak 2006); *Khelili c. Suisse*, 16188/07 (ECtHR 18 Ekim 2011).

⁴²⁸ *Shimovolos v. Russia*, 30194/09 (ECtHR 21 Haziran 2011).

⁴²⁹ *Peck v. the United Kingdom*, 60898/00 (ECtHR 28 Ocak 2003); *Panteleyenkov v. Ukraine*, 11901/02 (ECtHR 29 Haziran 2006); *Sõro v. Estonia*, 22588/08 (ECtHR 03 Eylül 2015).

⁴³⁰ *Valenzuela Contreras v. Spain*, 34724/14, 58208/14, 21969/15, 23735/16, 23740/16, 65993/16, 14118/17 (ECtHR 30 Temmuz 1998); *Gaughran v. the United Kingdom*, 45245/15 (ECtHR 13 Şubat 2020).

alınması, Devlet'e bu tür müdahalelerden kaçınma şeklindeki negatif yükümlülüğe ek olarak, pozitif yükümlülükler de yüklemektedir. Bu yükümlülükler bireylerin kendi aralarındaki ilişkiler alanında özel hayata saygıyı güvence altına almak için tasarlanmış tedbirlerin kabul edilmesini gerektirmektedir. Söz konusu yükümlülüklerin sağlanmasına ilişkin araçların seçimi, ilke olarak, devletin takdir yetkisi dahilinde olmakla birlikte; temel değerlerin ve özel yaşamın temel yönlerinin tehlikede olduğu durumlarda, vahim eylemlere karşı etkili caydırıcılık, etkili ceza hukuku hükümleri gerektirebilmektedir.⁴³¹ Kişisel verilerin korunmasına ilişkin pozitif yükümlülükler, şüphesiz, bireyler ve internet şirketleri arasındaki ilişkileri de kapsamaktadır. Bu da kişisel veriler üzerindeki etkileri gittikçe artan internet şirketlerine karşı da kişisel verilerin korunması hakkının güvence altına alınmasını gerektirmektedir. AİHM içtihadında, internet şirketlerinin bu kapsamdaki sorumluluklarının özellikle kişisel verilerinin ifşası ve kişisel verilerin silinmesine ilişkin olarak gündeme geldiği görülmektedir.

Devletin internette kişisel verilerin korunmasına ilişkin pozitif yükümlülükleri ilk defa *K.U./Finlandiya*⁴³² kararında, kişisel verilerin ifşası bağlamında ele alınmıştır. Bu başvuru, 12 yaşındaki bir çocuğun isim, doğum tarihi, fotoğraf ve fiziksel özellikleri gibi verilerinin internet ortamında cinsel içerikli bir reklamda yayınlanması ve reklamı verenin kimliğinin yürürlükte olan mevzuat nedeniyle internet servis sağlayıcısından alınamaması ile ilgili olarak Devletin Sözleşme'nin 8. maddesinden kaynaklanan pozitif yükümlülüklerinin ihlal edilip edilmediğine ilişkindir. Dolayısıyla netleştirilmesi gereken asıl mesele, Devletin internet servis sağlayıcılarından, bir çocuğu pedofillerin hedefi haline getiren bir web sitesinde -rızası olmadan- onun hakkında bilgi yayınlayan özel bir kullanıcının kimliğini açıklamasını talep edip edemeyeceğidir. AİHM, bu bakımdan hükümetin, mevzuatta söz konusu eylemlerin suç olarak düzenlendiği ve ayrıca hizmet sağlayıcıya yönelik olarak da hem ceza hem de tazminat sorumluluğu işletilebileceğine ilişkin savunmalarından tatmin olmamıştır.⁴³³ Mahkemeye göre bir suçun mevzuatta düzenlenmiş olması, gerçek suçluyu tespit etmek ve onun yargılanmasını sağlamak mümkün olmadıkça ancak sınırlı bir caydırıcı etkiye sahiptir. Tazminat sorumluluğuna gelince, Mahkeme somut dava bakımından bu giderimi de yeterli görmemiştir:

⁴³¹ August v. the United Kingdom (dec.), 32848/06 (ECtHR 21 Ocak 2003).

⁴³² K.U. v. Finland, 2872/02 (ECtHR 02 Aralık 2008).

⁴³³ K.U. v. Finland, para. 47,48.

“Hem kamu yararı hem de fiziksel veya psikolojik refahlarına karşı işlenen suçların mağdurlarının çıkarlarının korunmasının, gerçek suçlunun tespit edilmesini ve adalete teslim edilmesini -mevcut davada bu başvuranın adına reklamı veren kişidir- ve mağdurun kendisinden maddi tazminat almasını sağlayan bir hukuk yolunun mevcut olmasını gerektirdiği açıktır.”⁴³⁴

AIHM, kararı gerekçelendirirken, internette ifade özgürlüğü ile mahremiyet haklarına ilişkin de temel bir kural ortaya koymuştur. Buna göre internet kullanıcılarının kendi mahremiyetleri ile ifade özgürlüklerine saygı gösterileceğine dair bir güvenceye sahip olması öncelik arz etse de, bu güvence mutlak olamaz ve zaman zaman düzensizliğin veya suçun önlenmesi veya başkalarının hak ve özgürlüklerinin korunması gibi diğer meşru zorunluluklara boyun eğmelidir.⁴³⁵ Mahkeme, somut başvuruda, ulusal hukukta bu yarışan menfaatleri dengelemek için bir çerçevenin mevcut olmadığını tespit etmiş ve Sözleşme’nin 8. maddesinin ihlal edildiğine karar vermiştir. Mahkeme bu karardan sonra da internet şirketlerinin kullanıcı verilerinin ifşasına ilişkin sorumluluklarını farklı bağlamlarda ele alma fırsatı bulmuştur.

Örneğin, *Standard Verlagsgesellschaft mbH/Avusturya* kararında⁴³⁶ başvuru şirket, sahibi olduğu platformda iki politikacıya karşı yayımlanan yorumların sahiplerinin kimliklerini ifşa etmeye zorlanmasının ifade özgürlüğünü ihlal ettiğini iddia etmiştir. AIHM öncelikle, ulusal hukuk yargılamasında da tartışmalı noktalardan biri olan internet portalının hak ve sorumlulukları bakımından bir basın kuruluşu olarak değerlendirilip değerlendirilemeyeceği hususunu ele almıştır. Buna göre başvuran şirket, söz konusu yorumların yazarlarının gazetecilik kaynakları oluşturduğu ve bu nedenle kimliklerinin korunduğunu iddia ederken yerel mahkemeler ise, herhangi bir gazetecilik faaliyetinin söz konusu olmaması nedeniyle, başvuran şirketin kullanıcı yorumlarıyla ilgili olarak editoryal gizliliğe başvuramayacağına hükmetmiştir.⁴³⁷ Hükümet de buna paralel olarak, başvuran şirketin aynı anda hem araçlara tanınan sorumluluk muafiyetinden hem de yayıncılara kaynaklarıyla ilgili olarak tanınan güvencelerden yararlanamayacağını ileri sürmüştür.⁴³⁸ Hükümet ayrıca,

⁴³⁴ K.U. v. Finland, para. 47.

⁴³⁵ K.U. v. Finland, para. 49.

⁴³⁶ *Standard Verlagsgesellschaft MbH v. Austria* (No. 3), 39378/15 (ECtHR 07 Aralık 2021).

⁴³⁷ *Standard Verlagsgesellschaft MbH v. Austria* (No. 3), para. 69.

⁴³⁸ *Standard Verlagsgesellschaft MbH v. Austria* (No. 3), para. 58.,

internet şirketinin içeriklerden sorumlu tutulmadığını, içerikleri silmeye de zorlanmadığını belirterek şirketin haklarına bir müdahaleden söz edilemeyeceğini iddia etmiştir. AİHM, bu iddiaları, yarışan menfaatleri de dikkate alarak ayrıntılı bir şekilde değerlendirmiş ve başvurucunun basın özgürlüğüne müdahale edildiğine karar vermiştir:

“...Mahkeme, çevrimiçi yorumların yazarlarının verilerini ifşa etme yükümlülüğünün, onları tartışmaya katkıda bulunmaktan vazgeçirebileceğinden ve dolayısıyla genel olarak forumlarda paylaşım yapan kullanıcılar arasında caydırıcı bir etkiye yol açabileceğinden şüphe duymamaktadır. Bu durum, dolaylı olarak, başvuran şirketin bir medya şirketi olarak basın özgürlüğü hakkını da etkilemektedir. Başvuran şirket, gazetecilik çalışmaları hakkındaki tartışmaları ilerletmek amacıyla kullanıcıları makaleleri hakkında yorum yapmaya davet etmektedir. Bu amaca ulaşmak için yorum sahiplerinin kullanıcı adı kullanmalarına izin verir; kayıt üzerine, kullanıcılar verilerinin kamuya açık olarak görülmeyeceği ve yalnızca yasaların gerektirmesi halinde ifşa edileceği konusunda bilgilendirilir. Forum kuralları belirli içeriklerin kabul edilmeyeceğini ve yorumların bir anahtar kelime sistemi tarafından taranacağını, manuel incelemeye tabi tutulabileceğini ve kurallara uygun olmadıkları takdirde silineceğini belirtir.

Mahkeme, İnternet'te bilginin yayılmasının kolaylığı, kapsamı ve hız ile bu tür bilgilerin bir kez ifşa edildikten sonra kalıcılığının, geleneksel medyaya kıyasla hukuka aykırı söylemin etkilerini önemli ölçüde artırabileceğini gözden kaçırmamaktadır. Bu nedenle, Sözleşme'nin internette mutlak bir anonimlik hakkı sağlamadığı konusunda Hükümet ile hemfikirdir.

Mahkeme aynı zamanda, internet kullanıcılarının kimliklerinin ifşa edilmemesindeki menfaatlerini de göz önünde bulundurmaktadır. Anonimlik uzun zamandır misillemelerden veya istenmeyen dikkatlerden kaçınmanın bir aracı olmuştur. Bu nedenle, özellikle internet de dahil olmak üzere, görüşlerin,

fikirlerin ve bilgilerin serbestçe akışını önemli bir şekilde teşvik edebilmektedir. Dolayısıyla, dolaylı olarak bir medya şirketinin çıkarlarına da hizmet edebilir.

Mahkeme, internette farklı derecelerde anonimliğin mümkün olduğunu gözlemlemektedir. Bir internet kullanıcısı, doğrulanmamış veya bir tür doğrulamaya tabi olabilecek bir hesap veya iletişim verileri aracılığıyla bir hizmet sağlayıcı tarafından tanımlanabilirken, daha geniş bir kamuoyu için anonim olabilir. Bir hizmet sağlayıcı, kullanıcıları için geniş ölçüde anonimliğe de izin verebilir; bu durumda kullanıcıların kendilerini hiç tanıtmaları gerekmez ve yalnızca İnternet erişim sağlayıcıları tarafından tutulan bilgiler aracılığıyla sınırlı ölçüde- izlenebilirler. Bu tür bilgilerin yayınlanması genellikle soruşturma veya yargı makamları tarafından bir tedbir kararı gerektirecek ve kısıtlayıcı koşullara tabi olacaktır. Yine de bazı durumlarda failerin tespit edilmesi ve kovuşturulması için gerekli olabilir”⁴³⁹

AIHM, müdahalenin kanunla öngörülmesi ve meşru bir amaca dayanması kriterleri bakımından bir tartışma olmadığını belirterek, demokratik toplumda gereklilik incelemesine geçmiştir. Bu incelemede, Devletin pozitif yükümlülüklerinin bir gereği olarak, kullanıcı verilerinin açıklanıp açıklanmayacağına karar verilmeden önce Sözleşme'nin 8. ve 10. maddeleri bakımından çatışan menfaatlerin tartılması gerektiğini; somut davada bu yükümlülüğün bir yandan davacıların itibarlarını koruma hakkını, diğer yandan da başvuran şirketin, yazarların kişisel verilerini ve fikirlerini kamuya açık bir şekilde ifade etme özgürlüklerini korumadaki rolü ile birlikte basın özgürlüğü hakkını içerdiğini belirtmiştir. AIHM'e göre ulusal mahkemeler, söz konusu yorumların siyasi bir tartışmanın parçası olduğunu ve bir yandan söz konusu yorumların yazarları ile bu yazarları korumaya çalışan başvuran şirketin çıkarları, diğer yandan da davacıların çıkarları arasındaki dengeyi göz önünde bulundurmamışlardır.⁴⁴⁰

AIHM K.U. /Finlandiya kararında, internet şirketinin çocuğun menfaatlerini ihlal eden kullanıcı kimliğini ifşa etmesini sağlayacak etkili bir mekanizmanın kurulmamış olmasını Sözleşme'nin 8. maddesine aykırı bulurken; *Standard Verlagsgesellschaft mbH / Avusturya* kararında ise internet şirketinin kullanıcı kimliğini paylaşmaya zorlanmasının

⁴³⁹ Standard Verlagsgesellschaft MbH v. Austria (No. 3), para. 74-77.

⁴⁴⁰ Standard Verlagsgesellschaft MbH v. Austria (No. 3), para. 95.

ifade özgürlüğüne aykırı olduğuna karar vermiştir. Bu iki kararın, internet şirketlerinin bireylerin mahremiyetlerinin korunmasına ilişkin sorumluluğuna ilişkin birtakım sonuçları bulunmaktadır. Öncelikle, kural olarak internet şirketleri, internet kullanıcılarının anonimliğine saygı göstermek ve bunu korumakla görevlidir. *Standard Verlagsgesellschaft mbH/Avusturya* kararında, her ne kadar başvuru internet şirketinin basın özgürlüğü çerçevesinde ele alınsa da, somut başvuru bakımından adil şekilde dengelenmesi gereken haklardan birinin de “yorum yazarlarının çıkarları” olduğu ortaya koyulmuştur.⁴⁴¹ Ayrıca Mahkeme, başvuru şirketin hak sahipliğini ortaya koyarken anonimliğin, başvuran şirketin kendi imkanlarıyla savunamaması halinde etkili olmayacağını, kimliklerinin hukuk mahkemelerinde ifşa edilmesi halinde kullanıcıların anonimliklerini kendilerinin savunmasının zor olacağını belirterek, internet şirketlerinin kullanıcıların haklarını koruma işlevini de dikkate almıştır.⁴⁴² Kararda araçların, kullanıcıların kimlik bilgilerinin ve anonimliğinin korunmasına ilişkin yükümlülüklerini düzenleyen hukuki metinlere yapılan atıflar⁴⁴³ da kararın internet şirketlerinin sorumluluklarına bakan yönünü ortaya koymaktadır. Söz konusu kararlardan çıkarılacak diğer sonuç ise internet şirketlerinin suçun önlenmesi veya başkalarının hak ve özgürlüklerinin korunması gibi istisnai bazı durumlarda kullanıcı içeriklerini yetkili otoritelerle paylaşmakla yükümlü olabileceğidir.

Kullanıcı kimliklerinin açıklanmasının iki farklı boyutunu ortaya koyan bu kararlar aynı zamanda bazı yeni sorunları da gündeme getirmektedir: Örneğin, internet şirketlerinin birbirinin tam karşısı iki farklı eylemde bulunmasını gerektiren bu sorumluluğun belirlenmesinde hangi kriterler esas alınacaktır? Kullanıcı verilerinin korunması ile başkalarının hak ve özgürlükleri arasındaki dengelemede dikkate alınacak hususlar nelerdir? Kullanıcı verilerinin paylaşılmasının gerekli olduğu durumlarda, paylaşımın sınırları ne olmalıdır?

⁴⁴¹ *Standard Verlagsgesellschaft MbH v. Austria* (No. 3), para. 94.

⁴⁴² *Standard Verlagsgesellschaft MbH v. Austria* (No. 3), para. 78.

⁴⁴³ Kararda, Avrupa Birliği ve Avrupa Konseyi’nin çeşitli karar ve bildirimlerinde yer alan anonimlik ve kullanıcı verilerinin korunmasına ilişkin şu düzenlemelere yer verilmiştir:

“2.4. *Kişisel verilerin kullanılması*

2.4.1. *Aracılar, yasalar gerektirmedikçe veya adli bir makam ya da kararları yargı denetimine tabi olan ve işinin yürürlükteki yasalar ve standartlarla tutarlı, demokratik bir toplumda gerekli ve izlenen meşru amaçla orantılı olduğunu tespit eden diğer bağımsız idari makamlar tarafından talep edilmedikçe kişisel verileri üçüncü bir tarafa ifşa etmemelidir.*” “Recommendation CM/Rec(2018)2 of the Committee of Ministers to Member States on the Roles and Responsibilities of Internet Intermediaries”.

AIHM'nin önünde kullanıcı verilerinin kamu otoriteleriyle paylaşılmasına ilişkin, yukarıda örneklendirilen sorunları da içeren önemli bir başvuru bulunmaktadır. Telegram tarafından Rusya aleyhine yapılan başvuru⁴⁴⁴, Rusya Federal Güvenlik Servisi'nin *"terörle ilgili faaliyetlerden şüphelenilen Telegram kullanıcılarıyla ilgili olarak 12 Temmuz 2017'den bu yana yapılan iletişimin deşifre edilmesini"* kolaylaştıracak teknik bilgileri ifşa etmesine ilişkin talebini kullanıcılarının ifade özgürlüğünün korunmasının önemi gerekçesiyle yerine getirmeyen internet şirketi hakkında para cezasına hükmedilmesinin ve iletişim uygulamasının kapatılmasının ifade özgürlüğüne aykırı olup olmadığına ilişkindir. Başvuruda Telegram tarafından ileri sürülen iddialar özetle şu şekildedir: i. söz konusu talebe dayanak yasa hükmü; kullanıcılar arasındaki gizliliğin sınırlarına ilişkin net bir çerçeve sunmadığı, ilgisiz kişilerin gizliliklerini güvence altına almadığı, şirketin söz konusu talebi yerine getirmesine ilişkin bir süre tanımadığı, kullanıcıların verilerinin açıklanmasına ilişkin bir yargı kararı gerektirmediği için kanunilik şartını taşımamaktadır, ii. başvuru hakkında verilen kararlarda, yarışan menfaatler arasında (bir tarafta terörle mücadele ve kamu güvenliğinin sağlanması, diğer tarafta ise internet hizmeti kullanıcılarının özel yaşam hakları ve ifade özgürlüğü ile başvuran şirketin bilgi yayma özgürlüğü) bir dengeleme yapılmamıştır, iii. uygulamanın kapatılması kararı, hukuka aykırı ve orantısızdır. AIHM'de derdest durumda olan bu başvuru, şirketlerin kişisel verilerinin korunmasına ilişkin sorumlulukları bakımından önemli noktalara ışık tutacak niteliktedir.⁴⁴⁵

İnternet şirketlerinin kişisel verilerin korunması hakkına ilişkin sorumlulukları bakımından AIHM içtihadında dikkat çeken diğer konu da kişisel verilerin silinmesi, daha bilinen ifadesiyle unutulma hakkına ilişkindir. AIHM'nin kişisel verilerin silinmesi

⁴⁴⁴ Telegram Messenger Llp and Telegram Messenger Inc. v. Russia (communicated), 13232/18 (ECtHR 29 Ekim 2020).

⁴⁴⁵ Rusya'da Telegram mesajlaşma uygulamasının engellemesi sürecinde, yasağın atlatılması için kullanıldığı iddia edilen Google, Amazon Web Services, Digital Ocean, Microsoft ve Hetzner gibi büyük bulut hizmetlerinin IP adresleri de dahil olmak üzere yaklaşık 20.000.000 IP adresine erişim engellenmiştir. Bu kapsamda yasak uygulanan diğer internet şirketlerden bazıları arasında çevrimiçi faaliyetlerini sona erdirmeye noktasına gelmiştir. Örneğin, OOO Zhivaya Fotografiya isimli şirket, kendisine de uygulanan yasağa ilişkin olarak AIHM'e başvuruda bulunmuştur. Başvuru, AIHM'de derdest durumdadır. OOO Zhivaya Fotografiya v. Russia (communicated), 48932/19 (ECtHR 15 Haziran 2020); Benzer şekilde Private Networks LP şirketi tarafından yapılan başvuru da kullanıcılara Telegram Messenger platformundaki yasaklı bilgilere ve kanallara erişim sağladığı iddiasıyla tgvpn.com sitesinin de erişime engellenmesine ilişkin olup derdest haldedir. Private Networks Lp v. Russia (communicated), 4945/20 (ECtHR 01 Eylül 2020).

hakkına ilişkin bu kararları, internet şirketlerinin kullanıcı verilerini silme yükümlülüklerinin çerçevesini ortaya koymaktadır.

Unutulma hakkını, veri öznesinin belli koşullar altında kendisi ile ilgili kişisel verilerin fazla gecikmeksizin kalıcı olarak silinmesini veri sorumlusundan temin etme hakkı olarak tanımlamak mümkündür.⁴⁴⁶ AİHM’ne göre unutulma hakkı, bireyin mevcut algılanma şeklini etkileyen geçmiş bilgilerinin silinmesini veya değiştirilmesini ya da bunlara erişimin sınırlandırılmasını elde etme menfaatine dayanmaktadır.⁴⁴⁷ Dolayısıyla bu hak, şartları oluştuğunda internet şirketlerine kişisel verilerin korunmasına ilişkin sorumluluklar yüklemektedir. Bu sorumluluğun kapsamının ve sınırlarının belirlenmesi de şüphesiz, ifade özgürlüğü ile özel hayata saygı hakkı arasında adil bir denge kurulmasını gerektirmektedir.

AİHM, "unutulma hakkı" kavramının birçok yönü bulunduğunu ve halen inşa aşamasında olduğunu kabul etmektedir. Bu gelişim sürecine ilişkin, unutulma hakkının ilk olarak daha önce ifşa edilmiş adli nitelikteki bilgilerin basın tarafından yeniden yayınlanması bağlamında ortaya çıktığını tespit etmiştir. Hakkın bu yönüne dair başvurularda AİHM, unutulma hakkı kavramına açıkça atıfta bulunmaksızın somut başvurunun özelliklerini dikkate alarak karar vermiştir.⁴⁴⁸ Unutulma hakkının yeni bir yönü, haber makalelerinin dijitalleştirilmesi bağlamında ortaya çıkmış ve ilgili gazetelerin web sitelerinde yaygın bir şekilde yayılmasıyla sonuçlanmıştır.⁴⁴⁹ Bu yayılmanın etkisi, web sitelerinin arama motorları tarafından listelenmesiyle eş zamanlı

⁴⁴⁶ Kalıcı olarak silme hakkı (“unutulma hakkı”), “1. Veri öznesinin kendisi ile ilgili kişisel verilerin fazla gecikmeksizin kalıcı olarak silinmesini veri sorumlusundan temin etme hakkı bulunur ve aşağıdaki hâllerden birinin geçerli olması durumunda, veri sorumlusu kişisel verileri fazla gecikmeksizin kalıcı olarak silmekle yükümlüdür.” “Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC”, (18.05.2024), <https://eur-lex.europa.eu/eli/reg/2016/679/oj>.

⁴⁴⁷ Hurbain v. Belgium, 57292/16 (ECtHR [GC] 04 Temmuz 2023), para. 191.

⁴⁴⁸ Österreichischer Rundfunk v. Austria, 35841/02 (ECtHR 07 Aralık 2006) para. 68, 69. Mediengruppe Österreich GmbH v. Austria, 37713/18 (ECtHR 26 Nisan 2022), para. 68-70.

⁴⁴⁹ AİHM, unutulma hakkının bu “yeni” yönüne ilişkin olarak, ulusal yargılamalarda hakkın ne şekilde ele alındığına ilişkin bazı aktarımlarda bulunmuştur: “*Bu yeni bağlamda özel hayata saygı hakkına ek olarak, ulusal mahkemeler ve yetkililer, bazı hukuk sistemlerinde bağımsız bir hak haline gelen kişisel verilerin korunması hakkından destek almaktadır (bkz. İngiltere ve Galler Yüksek Mahkemesi ve İspanya Anayasa Mahkemesi’nin bulguları -sırasıyla yukarıdaki 102. ve 107. paragraflar). Farklı bir yaklaşıma göre haber yayıncılarının basın makalelerini değiştirme taleplerine ilişkin özel durumda, "unutulma hakkı" yalnızca kişilik hakkının korunmasına dayandırılabilir; bu nedenle kişisel verilerin korunmasıyla bağlantılı olan bilgisel kendi kaderini tayin hakkından ayırt edilmelidir.*”

olarak artmıştır. Bu tür durumlarda mesele, bilginin yeniden ortaya çıkarılması değil, çevrimiçi ortamda bulunmaya devam etmesidir.⁴⁵⁰

AİHM içtihadında, haber makalelerinin dijitalleştirilmesine ilişkin olarak son zamanlarda bir içtihat gelişiminin olduğu söylenebilir. Bu kapsamda AİHM, hem dijital arşivlerde saklanan orijinal haber makalelerinin kaldırılması veya değiştirilmesi taleplerini, hem de internet gazeteleri tarafından yayınlanan makalelerin indeksten çıkarılmasına ilişkin başvuruları karara bağlamıştır.

İlk kategoride yer alan başvuruları AİHM, başlarda unutulma hakkına atıfta bulunmaksızın başvurucuların itibarlarının korunmasıyla ilgili olarak ele alsa da, hakkın gelişim sürecine paralel olarak sonradan unutulma hakkı kavramına da değinmeye başlamıştır.⁴⁵¹ Bu kategoride ele alınabilecek ilk karar, *Węgrzynowski ve Smolczewski/Polonya* kararıdır.⁴⁵² İki avukatın, itibarlarını zedeleyen bir gazete makalesinin gazetenin internet sitesinde kamunun erişimine açık olmaya devam etmesinin özel hayata saygı ve itibarın korunması haklarını ihlal ettiği iddiasıyla yapılan söz konusu başvuruda AİHM, Sözleşme'nin 8. maddesinin ihlal edilmediğine karar vermiştir. Bu kararda AİHM'nin dikkat çeken değerlendirmelerinden biri de geçmişte bireysel itibarlara yönelik haksız olduğu sonucuna varan yayınların tüm izlerini kamusal alandan kaldırarak tarihi yeniden yazma görevinin yargı makamlarına ait olmadığını kabul etmesi olmuştur.⁴⁵³ *Fuchsmann/Almanya başvurusunda*⁴⁵⁴ da AİHM, uluslararası bir iş adamı olan başvurucunun, Haziran 2001'de New York Times'ın internet baskısında yayınlanan ve altın kaçakçılığı, zimmete para geçirme ve Rus organize suç örgütleriyle bağlantılı olmakla suçlandığı bir makaleye ilişkin tedbir talebinin reddedilmesinin Sözleşme'nin 8. maddesini ihlal etmediğine karar vermiştir. Kararda, özellikle makalenin kamu yararını ilgilendiren bir tartışmaya katkıda bulunduğu; başvuranın medya sektöründe uluslararası alanda faaliyet gösteren bir Alman işadamı olması nedeniyle makaleye belirli bir ilgi olduğu; yeterli olgusal temelinin olduğu; gazetecinin gazetecilik görev ve sorumluluklarına tam olarak uyduğu; makalenin polemik yaratacak ifade ve imalardan uzak olduğu; yayılan bilgilerin esas olarak başvuranın mesleki yaşamıyla ilgili

⁴⁵⁰ Hurbain v. Belgium, para. 195.

⁴⁵¹ M.L. and W.W. v. Germany, 60798/10, 65599/10 (ECtHR 28 Haziran 2018).

⁴⁵² Węgrzynowski and Smolczewski v. Poland, 33846/07 (ECtHR 16 Temmuz 2013).

⁴⁵³ Węgrzynowski and Smolczewski v. Poland, para. 65.

⁴⁵⁴ Fuchsmann v. Germany, 71233/13 (ECtHR 19 Ekim 2017).

olduğu ve makalenin Almanya'daki sonuçlarının sınırlı olduğu hususları belirleyici olmuştur.⁴⁵⁵ Unutulma hakkı kavramının ilk defa açıkça zikredildiği *M.L. ve W.W./Almanya* kararında da AİHM, yine Sözleşme'nin 8. maddesinin ihlal edilmediğine karar vermiştir. Ancak, kararda unutulma hakkına ilişkin bazı değerlendirmelerde bulunulmuştur. Bu başvurunun konusu, ünlü bir aktörü öldürme suçuyla haklarında müebbet hapis cezasına hükmedilen başvuruçuların, mahkumiyetlerine ilişkin bilgilerin çeşitli medya kuruluşlarının internet sitelerinden kaldırılmamasının AİHS'nin 8. maddesine aykırılık teşkil edip etmediğine ilişkindir. Başvuruçular, M.L. ve W.W. üvey kardeşler olup mahkumiyetlerinin ardından ilk olarak 1994'te, ardından 2000 ve 2004'te yeniden yargılanmak için birçok talepte bulunmuşlar ve talepleri reddedilmiştir. M.L. ve W.W. sırasıyla 2007 ve 2008 yıllarında denetimli serbestlikle serbest bırakılmışlardır. Başvuruçular 2007 yılında, *Der Spiegel Online*, *Deutschlandradio* ve *Mannheimer Morgen* şeklindeki üç medya kuruluşuna karşı, sırasıyla 1991-1993, 2000 ve 2001 tarihlerinde haklarındaki yayınlara ilişkin olarak üç farklı dava süreci başlatmıştır.

Deutschlandradio tarafından yapılan yayınla ilgili olarak başvuruçuların isimlerinin anonim hale getirilmesi talebiyle açtıkları davada Hamburg Bölge Mahkemesi, başvuranların mahkumiyetlerinden bu kadar uzun bir süre sonra artık eylemleriyle yüzleşmemelerinin, kamunun başvuranların bu eylemlere katılımı hakkında bilgilendirilmesindeki menfaatinden daha ağır bastığına karar vermiştir. Hamburg İstinaf Mahkemesi, internetteki materyallerin genellikle kullanıcılar için kalıcı olarak erişilebilir hale getirildiği, bu bilgilerin açıkça eski olduğu gerçeğinin sonucu değiştirmedığı, bu durumun tahliye edilmek üzere olan başvuruçuların topluma entegre olmaları ve yeniden sosyalleşmeleri bakımından risk teşkil ettiği ve bu sebeplerle radyo istasyonunun başvuruçuların haklarına yapılan müdahaleden sorumlu olduğunu belirterek kararı onamıştır. Radyo istasyonunun başvurusu üzerine Federal Temyiz Mahkemesi ise doğru haberlerin kişilik haklarını ihlal edebileceğini, örneğin haberin yayılmasının önemli bir etkiye sahip olması veya haberin ilgili kişiyi damgalaması ve bu nedenle sosyal olarak izole etme etkisine sahip olması durumunda, neden oldukları zararın halkın gerçeği bilme menfaatinden daha ağır bastığını belirterek unutulma hakkını kabul etmekle birlikte; davanın sıradan suç davranışlarının kapsamının ötesine geçtikçe kamuoyunun bu konuda bilgilendirilmesinde o kadar büyük çıkar olduğunu ve İstinaf Mahkemesinin radyo

⁴⁵⁵ Fuchsmann v. Germany, para. 35-52.

istasyonunun ifade özgürlüğü hakkını ve radyo istasyonunun misyonunun bir parçasını oluşturan halkın bilgilendirilme menfaatini yeterince dikkate almadığını belirterek temyiz talebini kabul etmiştir.⁴⁵⁶

Der Spiegel Online’a karşı açılan dava bakımından da Hamburg Bölge Mahkemesi, portalda yer alan ve başvuruçuların geçmişlerini anlatan ve yargılanma süreçlerindeki fotoğrafları da içeren beş makaleye kamunun erişiminin kısıtlanmasına karar vermiş ve bu karar İstinaf Mahkemesi tarafından onanmış ise de Temyiz Mahkemesi benzer gerekçelerle kararı bozmuştur.⁴⁵⁷ Son olarak, 2001 tarihli Mannheimer Morgen gazetesine karşı açılan davada da başvuruçuların talepleri Hamburg Bölge Mahkemesi tarafından kabul edilmiş ve bu karar İstinaf Mahkemesi tarafından da onanmıştır; ancak gazete tarafından yapılan temyiz başvurusunun kabul edilmesiyle bu karar da bozulmuştur.⁴⁵⁸

AIHM, Avrupa Konseyi ve Avrupa Birliği düzenlemeleri ile Avrupa Birliği Adalet Divanı’nın içtihadını ortaya koyduktan sonra, Sözleşme’nin 8. maddesinin bireylere bilgilisel kendi kaderini tayin hakkı sağladığını, ancak bu hakkın devreye girebilmesi için kişinin itibarına yönelik saldırının şu üç şartı taşıması gerektiğini belirtmiştir: i. belirli bir ciddiyet seviyesine ulaşması, ii. kişinin özel hayata saygı hakkından faydalanmasına engel teşkil etmesi, iii: kişinin kendi eylemlerinin öngörülebilir bir sonucu olarak ortaya çıkmaması.⁴⁵⁹

Mahkeme, bu tespitin ardından, basının fikir ve bilgileri kamuoyuna aktarma ve somut dava bakımından asıl önem arz eden *daha önce bildirilmiş haberleri içeren arşivleri muhafaza etmek ve bunları kamunun erişimine sunmak gibi ikincil ancak yine de değerli* rollerini açıklamıştır. Buna göre arşivler, özellikle halkın kolayca erişebildiği ve genellikle ücretsiz olmaları nedeniyle eğitim ve tarihi araştırmalar için önemli bir kaynak teşkil etmektedir. Buna karşın, internet sitelerinin özellikle bilgi saklama ve iletme kapasitesi bakımından başta özel hayata saygı hakkı olmak üzere, insan hak ve özgürlüklerinin kullanılması ve bunlardan yararlanılması bakımından oluşturduğu zarar riski, basının oluşturduğundan kesinlikle daha yüksektir. Dolayısıyla somut davada

⁴⁵⁶ M.L. and W.W. v. Germany, para. 12-26.

⁴⁵⁷ M.L. and W.W. v. Germany, para. 30-38.

⁴⁵⁸ M.L. and W.W. v. Germany, 40-44.

⁴⁵⁹ M.L. and W.W. v. Germany, para. 88.

olduğu gibi yarışan haklar söz konusu olduğunda da bu haklar arasında kamu yararını ilgilendiren bir tartışmaya katkı, ilgili kişinin tanınmışlık derecesi, haberin konusu, kişinin geçmişteki tutum ve davranışları, yayının içeriği, şekli ve sonuçları ve varsa, fotoğrafların çekildiği koşullar dikkate alınarak bir dengeleme yapılması gerekmektedir.⁴⁶⁰ Ancak bu noktada, bilginin silinmesine ilişkin talebin muhatabının da dengelemede önem arz ettiğini belirtmek gerekmektedir. AİHM bu bakımdan; faaliyeti genellikle ifade özgürlüğünün korunmasının amaçlandığı şeyin merkezinde yer alan bilginin orijinal yayıncısı ile temel menfaati ilgili kişi hakkındaki ilk bilgiyi yayınlamak değil, özellikle bu kişi hakkında mevcut herhangi bir bilginin tanımlanmasını kolaylaştırmak ve bu bilginin doğruluğunu tespit etmek olan arama motorları arasında ayırım yapmıştır. Nitekim, somut başvurunun da içeriklerin internet portallarında erişime açıldıkları zamanki değil, bu raporların uzun bir süre sonra ve özellikle de başvuranların cezaevinden tahliye edilmeleri beklenen tarih yaklaşırken erişime açık olmalarının hukuka uygun olup olmadığının sorgulanması bakımından özellik arz ettiğini belirtmiştir. Dolayısıyla, incelenmesi gereken husus, söz konusu raporların erişime açılmasının kamu yararını ilgilendiren bir tartışmaya katkıda bulunup bulunmadığı değil, katkıda bulunmaya devam edip etmediğidir.⁴⁶¹

Mahkeme somut başvuruda söz konusu haberlerin medya kuruluşlarının internet sitelerinde yer almasının, aradan geçen yıllar nedeniyle azalmamış olan kamu yararına ilişkin bir tartışmaya katkıda bulunmaya devam ettiğini; her ne kadar cinayeti işlemiş olmalarından ve sonraki yargılama sürecinden kaynaklansa da anonimlik taleplerinde bulundukları sırada kamuoyu tarafından bilinmeyen özel kişiler olmadıklarını; mahkumiyetleri sonrasında birkaç kez yeniden yargılanma talebinde bulundukları ve buna ilişkin olarak basınla temasa geçerek kamuoyunun bilgilendirilmesi talebinde bulunduklarından unutulma hakkı elde etme konusunda yalnızca sınırlı bir meşru beklentiye sahip olduklarını; söz konusu yayınlardan bazılarının erişimin ücretli olmasını da göz önünde bulundurarak yayınların yayılma kapsamının sınırlı olduğunu ve son olarak fotoğrafların on üç yıl öncesine ait olmaları dolayısıyla kişilerin tanınma

⁴⁶⁰ M.L. and W.W. v. Germany, para. 95; Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland, 931/13 (ECtHR [GC] 27 Haziran 2017) para. 136.

⁴⁶¹ M.L. and W.W. v. Germany, para. 99.

olasılıklarını azalttığını değerlendirerek Sözleşme'nin 8. maddesinin ihlal edilmediğine karar vermiştir.⁴⁶²

Anlaşılaçağı üzere AİHM, *Węgrzynowski ve Smolczewski/Polonya, Fuchsmann/Almanya ve M.L. ve W.W./Almanya* kararlarına konu dijital arşivlerde saklanan haber makalelerinin kaldırılması veya değiştirilmesi taleplerini, ifade özgürlüğü ile özel hayata saygı hakları arasında denge kurulmasına ilişkin mevcut içtihatlar doğrultusunda ele almıştır. Her üç durumda da Mahkeme, ifade ve basın özgürlüğüne ağırlık veren ulusal yargı organlarının kararlarına katılmıştır. İkinci kategoride yer alan, yani internet gazeteleri tarafından yayınlanan bir makalelerin indeksten çıkarılmasına ilişkin olarak ise AİHM'in arama motorlarının etkisiyle gittikçe artan bu talepler konusunda yeni bir bakış açısı geliştirdiğini söylemek mümkündür.

AİHM bu yeni bakış açısını ilk defa, bir internet gazetesinin genel yayın yönetmeninin, 2008 yılında bir restoranda çıkan kavgayı konu alan ve bu bağlamda açılan ceza davasının ayrıntılarını veren bir makaleyi gazetesinin internet sitesinde bulundurmaktan sorumlu tutulmasının ifade özgürlüğüne aykırı olup olmadığına ilişkin *Biancardi/İtalya* kararında ortaya koymuştur.⁴⁶³ Başvurucu, makalede adı geçenler tarafından makalenin internetten kaldırılmasına ilişkin 6 Eylül 2010 tarihli talep sonrasında herhangi bir şey yapmamakla birlikte, hakkında dava açılması üzerine makaleyi 23 Mayıs 2011 tarihinde indeksten çıkarmıştır. Böylece, açılan davanın makalenin kaldırılmasına ilişkin kısmı konusuz kalmıştır. Ancak, adli işlemlere ilişkin olması bakımından hassas veriler içeren söz konusu makalenin bildirimine rağmen kaldırılmaması dolayısıyla başvuru hakkında tazminata hükmedilmiştir.

AİHM, öncelikle somut başvurunun şu sebeplerle farklılık arz ettiğini ve bu nedenle de yeni bir yaklaşım gerektirdiğini⁴⁶⁴ ortaya koymuştur:

“Bu nedenle, mevcut davayı karakterize eden iki temel özellik vardır: Birincisi, çevrimiçi makalenin internette kaldığı süre ve bunun söz konusu bireyin itibarına saygı gösterilmesi hakkı üzerindeki etkisidir; ikinci özellik ise söz

⁴⁶² M.L. and W.W. v. Germany, para. 97-115.

⁴⁶³ Biancardi v. Italy, 77419/16 (ECtHR 25 Kasım 2021).

⁴⁶⁴ Biancardi v. Italy, para. 63.

konusu veri sahibinin niteliği ile ilgilidir -yani siyasi veya kamusal bir figür olarak kamusal bir bağlamda hareket etmeyen özel bir birey. Gerçekten de tanınmış olsun ya da olmasın herhangi bir kişi bir internet aramasının konusu olabilir ve kişisel verilerine internet üzerinden erişimin devam etmesi nedeniyle hakları zarar görebilir."⁴⁶⁵

AIHM böylece, somut dava bakımından şu hususlara özen gösterilmesi gerektiğini ifade etmiştir: (i) makalenin çevrimiçi tutulduğu sürenin uzunluğu; (ii) söz konusu verilerin hassasiyeti ve (iii) başvurana uygulanan yaptırımın ağırlığı.⁴⁶⁶

Süre unsuru bakımından AIHM, başvuru konusu makalenin gazeteye bildirim sonrasında sekiz ay boyunca çevrimiçi kaldığını ve kolayca erişilebilir olduğunu tespit etmiştir. Başvurucunun, ulusal yargı organları tarafından karar verildiği tarihte makaleye konu kişi hakkındaki ceza yargılamasının devam ettiğine ilişkin argümanları, makalenin olay tarihinden itibaren güncellenmemesi dolayısıyla kabul görmemiştir.⁴⁶⁷ Verilerin niteliği bakımından makalenin konusunun ceza yargılamasına ilişkin olduğunu belirten AIHM, hassas verilerle ilgili bilgilerin yayınlandığı koşulların, bilgi yayma hakkı ile veri sahibinin özel hayatına saygı gösterilmesi hakkı arasında denge kurulurken dikkate alınması gereken bir faktör olduğuna dikkat çekmiştir. Son olarak, başvuru hakkında hükmedilen tazminatın somut dava bakımından aşırı olmadığına karar vermiştir. Böylece AIHM, başvurucunun ifade özgürlüğüne müdahalenin haklı olduğu sonucuna ulaşmıştır.⁴⁶⁸ Biancardi/İtalya kararı, unutulma hakkının ilgili içeriğin internetten kaldırılmaksızın indeksten çıkarılmasına ilişkin ilk karar olması ve yalnızca internet arama motoru sağlayıcılarından değil, aynı zamanda somut başvuruda olduğu gibi internet üzerinden erişilebilen gazetelerden de belgelerin indeksini kaldırmalarının talep edilebileceğinin kabul edilmesi bakımından bir dönüm noktası olarak kabul edilebilir. Karar ayrıca, internet şirketlerinin indeksten çıkarma tedbirini geç uygulamadan da sorumlu tutulabileceğini teyit etmiştir.

⁴⁶⁵ Biancardi v. Italy, para. 62.

⁴⁶⁶ Biancardi v. Italy, para. 64.

⁴⁶⁷ Biancardi v. Italy, para. 65.

⁴⁶⁸ Biancardi v. Italy, para. 67-71.

AIHM'in *Hurbain/Belçika* kararı ise unutulma hakkının bugüne kadar en kapsamlı şekilde ele alındığı karardır.⁴⁶⁹ *Hurbain/Belçika* kararı, *Biancardi/İtalya* kararında indeksten çıkarmaya ilişkin olarak ortaya koyulan yeni bakış açısının, dijital arşivde tutulan orijinal haber içeriğinin değiştirilmesine dair olarak da uygulanması bakımından bir dönüm noktası olmasını yanında; unutulma hakkı başvuruları bakımından yarışan hakların dengelenmesine ilişkin yeni kriterlerin benimsenmesi, dolayısıyla unutulma hakkına dair taleplerin doğrudan muhatabı olan internet şirketlerinin sorumluluklarıyla ilgili yeni bir çerçeve sunması bakımından da önem arz etmektedir.

Belçika'nın önde gelen gazetelerinden biri tarafından yapılan bu başvuruda başvuru gazete, 1974 yılına ilişkin bir haberin, daha sonra gazetenin online arşivinde de yer alması üzerine haberde adı geçen kişinin açtığı davada dijital içerikte anonimleştirme yapılmasına ve tazminat ödenmesine karar verilmesinin ifade özgürlüğüne aykırılık teşkil ettiğini ileri sürmüştür. Söz konusu haber, ölümcül bir trafik kazasına ilişkin olup doktorluk mesleğini icra eden G.'nin tam adını içermektedir. G. hakkında bu olayla bağlantılı olarak iki yıl hapis cezasına hükmedilmiş, ancak cezası ertelenmiştir.⁴⁷⁰

AIHM, değerlendirmesine mevcut başvurunun şu iki açıdan ayırt edici olduğunu tespit ederek başlamıştır: i. başvuru internet sitesinde çevrimiçi olarak yayınlanan makalenin anonimleştirilmesine ilişkindir, ii. başvuru, başvuru gazetenin fiziksel baskısında 1994 yılında yayınlanan bir makalenin arşivlenmiş versiyonunun 2008 yılında çevrimiçi olarak yayınlanması ve erişilebilir olmaya devam etmesiyle ilgilidir.⁴⁷¹ Bu tespitin ardından AIHM, daha önce *Biancardi/İtalya* kararında kabul ettiği ayrımı, terminolojik olarak da şu şekilde tanımlamıştır:

“Genel olarak, ‘unutulma hakkı’ uygulamada arama motoru operatörleri veya haber yayıncıları tarafından alınabilecek çeşitli tedbirlere yol açabilir. Bunlar ya arşivlenmiş bir makalenin içeriğiyle (örneğin, makalenin kaldırılması, değiştirilmesi veya anonimleştirilmesi) ya da bilginin erişilebilirliğine getirilen sınırlamalarla ilgilidir. İkinci durumda, erişim sınırlamaları hem arama

⁴⁶⁹ *Hurbain v. Belgium*.

⁴⁷⁰ *Hurbain v. Belgium*, para. 13.

⁴⁷¹ *Hurbain v. Belgium*, para. 173.

motorları hem de haber yayıncıları tarafından uygulanabilir. Açıklık ve tutarlılık açısından Mahkeme bu kararda, arama motoru operatörleri tarafından alınan tedbirleri ifade etmek için "listeden çıkarma" (delisting) terimini ve söz konusu makalenin arşivlendiği web sitesinden sorumlu haber yayıncısı tarafından alınan tedbirleri ifade etmek için 'indeksten çıkarma'(de-indexing) terimini kullanacaktır.”⁴⁷²

AIHM’in erişim sınırlamalarının hem arama motorları hem de haber yayıncıları tarafından uygulanabilir olduğuna ilişkin bu tespiti, beraberinde ilgili içeriğin yayılmasında etkili olan bu iki aktör bakımından sorumluluk ilişkisinin ne olduğuna dair bir sorunu gündeme getirmektedir. AIHM, Hurbain/ Belçika kararında bu ilişkiyi şu şekilde ortaya koymuştur:

“...veri sahiplerinin arama motorları karşısındaki haklarını kullanmak için önceden veya eş zamanlı olarak orijinal web sitesiyle iletişime geçme zorunluluğu bulunmamaktadır; zira bunlar, her biri kendi meşruiyet temeline sahip ve bireyin hakları ve menfaatleri üzerinde farklı etkileri olan iki farklı işleme şeklidir... Aynı şekilde, bir haber sitesinin yayıncısına karşı açılan bir davanın incelenmesi, önceden yapılan bir yayından kaldırma talebine bağlı kılınamaz. Mahkeme'nin görüşüne göre arama motoru operatörlerinin faaliyetleri ile haber yayıncılarının faaliyetleri arasındaki bu ayrım, Mahkeme'nin unutulma hakkı iddiasına dayalı olarak halkın bilgi alma hakkı da dahil olmak üzere ifade özgürlüğüne yönelik herhangi bir müdahaleyi incelerken önemini korumaktadır.”⁴⁷³

AIHM bu başvuruda, ifade özgürlüğü ile dijital basın arşivlerinin korunması ve özel hayata saygı hakkı ile unutulma hakkı ilişkisine dair kapsamlı değerlendirmelerde bulunmuştur. Buna göre internet arşivlerinin bütünlüğü ilkesi; arşivlerin genel bir kural olarak gerçek, güvenilir ve eksiksiz kalmalarını gerektirmektedir. Öte yandan, teknoloji ve iletişim araçlarındaki gelişmelerle birlikte gittikçe daha fazla kişi "unutulma hakkı" olarak bilinen hak kapsamında çıkarlarını korumaya çalışmaktadır. Bu çerçevede AIHM, geçmişte yayınlanan ve sonrasında da internette kalmaya devam eden bilgilerin

⁴⁷² Hurbain v. Belgium, para. 175.

⁴⁷³ Hurbain v. Belgium, para. 208.

potansiyel etkilerini ortaya koyarak bir bakıma unutulma hakkının arka planında yatan hukuki değerleri açığa çıkarmıştır:

“Yayınlanan ve bir süredir internette mevcut olan kişisel bilgilerin, ilgili kişinin kamuoyu tarafından nasıl algılandığı üzerinde geniş kapsamlı olumsuz bir etkiye sahip olabileceği açıktır. Ayrıca, başka zararlı etkilerin ortaya çıkma riski de bulunmaktadır: Birincisi, bilgilerin bir araya getirilmesi ki bu ilgili kişinin bir profilinin oluşturulmasına yol açabilir ve ikincisi, eğer bilgiler bir bağlama oturtulmazsa, bu, başka bir kişi hakkındaki çevrimiçi bir makaleye başvuran bir bireyin gerçeğin parçalanmış ve çarpıtılmış bir resmini elde etmesi anlamına gelebilir. Dahası, belirli bir isimle bağlantılı aramaların gerçek sıklığından bağımsız olarak, bir kişiyle ilgili bilgilerin çevrimiçi olarak yayınlanmasının bir başka olası sonucu da o kişi için herhangi bir zamanda beklenmedik bir şekilde geçmişiyile tekrar karşılaşma tehdidi ve bunun sonucunda ortaya çıkan korkudur.”⁴⁷⁴

Hurbain/Belçika kararında AİHM, unutulma hakkının caydırıcı etkisini de değerlendirmiştir. Şöyle ki, ilgili kişinin talebi üzerine bir makalenin çevrimiçi olarak erişilebilir olmaya devam etmesinin hukuka uygunluğunu daha sonraki bir aşamada, söz konusu tüm menfaatlerin tartılması suretiyle gözden geçirme yükümlülüğü, basının gelecekte haberleri çevrimiçi arşivlerinde tutmaktan kaçınması veya böyle bir talebe konu olması muhtemel makalelerdeki kişiselleştirilmiş unsurları çıkarması riskini beraberinde getirmektedir. Bununla birlikte AİHM’ne göre içerik sağlayıcıların, yalnızca ilgili kişinin bu yönde açık bir talepte bulunması halinde, ifade özgürlüğü ve özel hayata saygı açısından menfaatleri değerlendirmeleri ve tartmaları gerekmektedir. Bu tespit, unutulma hakkının muhatabı olan internet şirketlerinin sorumluluğuna ilişkin bir sınır konulması bakımından önemli olmakla birlikte, söz konusu caydırıcı etkiye ilişkin kaygıları gidermeye yetmemektedir. Her ne kadar ilgili kişi talepte bulunduğunda, arşivlenen makalenin çevrimiçi olarak erişilebilir olmaya devam etmesinden kaynaklanan saldırının ciddiyetini kanıtlamakla yükümlü olsa da⁴⁷⁵ internet şirketlerinin ilgilinin talebi üzerine yarışan menfaatleri değerlendirme ve bunları tartma şeklindeki sorumlulukları, şirketlerin herhangi bir yaptırımla karşı karşıya kalmamak için talebi kabul etme şeklinde olağan bir

⁴⁷⁴ Hurbain v. Belgium, para. 192.

⁴⁷⁵ Hurbain v. Belgium, para. 209, 210.

sonucu beraberinde getirmektedir. Bu, ifade özgürlüğünün ağır bastığı durumlarda dahi söz konusu olabilecek bir ihtimaldir.

AİHM, ilk defa Biancardi/İtalya kararında ifade ettiği unutulma hakkının yeni bir yaklaşımı gerektirdiğine ilişkin görüşünü Hurbain/Belçika kararında yinelemiş, eşit değerdeki çeşitli hakların dengelenmesinde aşağıdaki kriterlerin dikkate alınması gerektiğini kabul etmiştir: (i) arşivlenen bilginin niteliği; (ii) olayların üzerinden ve ilk ve çevrimiçi yayından bu yana geçen süre; (iii) bilginin güncel değeri; (iv) unutulma hakkını talep eden kişinin tanınırlığı ve olaylardan bu yana davranışları; (v) bilginin çevrimiçi ortamda bulunmaya devam etmesinin olumsuz yansımaları; (vi) dijital arşivlerdeki bilginin erişilebilirlik derecesi; ve (vii) tedbirin ifade özgürlüğü ve daha spesifik olarak basın özgürlüğü üzerindeki etkisi.⁴⁷⁶

AİHM, bu kriterleri daha sonra somut başvuruya uygulamıştır. Buna göre başvurucunun anonimleştirilmesini talep ettiği içerik, hassas veri olarak kabul edilen ceza yargılamasına ilişkindir. İlk defa 1984 yılında basılı olarak yayınlanan başvuru konusu makale, 2008 yılında dijital olarak da yayınlanmış ve anonimlik talebinin yapıldığı 2010 yılına kadar aradan on altı yıl geçmiştir. AİHM, güncellik kriteri bakımından ulusal yargı organlarının olaylardan yirmi yıl sonra kamuya mal olmamış bir kişinin kimliğinin, karayolu güvenliğine ilişkin kamusal bir tartışmaya sadece istatistiksel bir katkı sağladığına, makalenin kamu yararına katkıda bulunmadığına, tarihsel bir öneme de sahip olmadığına yönelik kararlarına katıldığını belirtmiştir. Tanınırlık kriterine gelince, “medya spotlarının dışında kalma gerçeği, bir kişinin itibarının korunması lehine ağırlık kazanabilir” görüşünü kabul eden AİHM, doktor olan başvurucunun kamuoyunun ilgisini çeken biri olmadığına ve sonraki davranışlarında da medyanın ilgi odağı olmaktan imtina ettiğine dikkat çekmiştir. Mahkeme; içeriğin olumsuz etkilerini ayrıntılı bir şekilde ele alarak söz konusu makalenin başvurucunun ad ve soyadına dayalı basit bir aramayla hemen ortaya çıktığının, bunun başlı başına psikolojik bir etki doğurduğunun ve doktor olan başvurucunun itibarına ciddi şekilde zarar verme ve başvurucunun topluma entegre olmasını engelleme olasılığı olduğunun altını çizmiştir. Bu bakımdan AİHM, ulusal yargı organlarının dijital arşivlerin “sanal adli sicil kaydı”na dönüşmemesine ilişkin yaklaşımını onaylamıştır. AİHM, erişilebilirlik kriterine ilişkin olarak, arşivlenen

⁴⁷⁶ Hurbain v. Belgium, para. 205.

makalenin erişilebilirlik derecesinin, yani kısıtlama olmaksızın ve ücretsiz olarak erişilebilir olup olmadığının veya erişimin abonelerle sınırlı olup olmadığının veya başka bir şekilde kısıtlanıp kısıtlanmadığının da önemini belirtmiş ve somut başvurudaki yüksek erişilebilirlik derecesinin başvurucuya zarar verdiğine kanaat getirmiştir. Son olarak, tedbirin ifade ve basın özgürlükleri üzerindeki etkisi AİHM tarafından oldukça ayrıntılı şekilde değerlendirilmiştir. Bu kapsamda, kararda internetin kişilerin itibarı ve hakları üzerindeki olumsuz etkileri karşısında alınabilecek çeşitli tedbirler olduğu belirtilerek, içerikler üzerinde farklı etkileri olan internet şirketleri için bir yol haritası çizilmiştir.

Buna göre arama motorları tarafından uygulanabilecek tedbirler şu şekildedir:

- a. arama sonuçlarının, söz konusu web sitesinin bağlantısının sonuçlar listesinde daha az belirgin bir konumda görünecek şekilde yeniden düzenlenmesi
- b. bağlantının arama motorunun dizininden kaldırılması yoluyla tamamen veya kısmen listeden çıkarılması (yalnızca ilgili kişinin adına dayalı aramalarla ilgili olarak)⁴⁷⁷

Web sitesi yayıncıları tarafından alınabilecek tedbirler çok daha çeşitlidir:

- a. dijital arşivde saklanan bir metnin tamamının veya bir kısmının kaldırılması
- b. metinde atıfta bulunulan kişinin bilgilerinin anonim hale getirilmesi
- c. metne bir not eklenmesi, yani dijital düzeltme yoluyla (bilgilerin yanlış ya da eksik olduğu durumlarda)
- d. makalenin web sitesinin dahil olduğu arama motorunun indeksinden çıkarılması

⁴⁷⁷ Hurbain v. Belgium para. 241.

- e. makalenin, arama motoru operatörlerine verilen erişim kodları veya arama programlarının belirli yerleri taramasını engelleyen direktifler temelinde harici arama motorları tarafından tamamen veya kısmen (yalnızca ilgili kişinin adına dayalı aramalarla ilgili olarak) indeksten çıkarılmasının sağlanması.⁴⁷⁸

Somut başvuruda makalede adı geçen kişinin başlıca endişesi makalenin internet aramaları sonucunda adı ve soyadı temel alınarak görüntülenmesi olduğundan, başvurucudan makalenin anonimleştirilmesini ve alternatif olarak gazetenin iç arama motorundan makalenin indeksten çıkarılmasını istemiştir. Yargılama sonucunda makalenin dijital versiyonda anonimleştirilmesine karar verilmiştir. Sonuç olarak AİHM, makalenin tam şeklinin basılı olarak da gazete arşivlerinde kalacak olmasını göz önünde bulundurarak, makalenin elektronik versiyonunun anonimleştirilmesinin Sözleşme'nin 10. maddesi anlamında kesinlikle gerekli olanla sınırlı ve orantılı olduğuna karar vermiştir.⁴⁷⁹

AİHM'nin çok kapsamlı bir şekilde ele aldığı ve gazetecilik faaliyetleri kapsamında yasal olarak yayınlanan ve bir haber kuruluşunun web sitesinde arşivlenen bilgilerin kaldırılması veya değiştirilmesinin sözleşmeye aykırı olmadığına kabul edildiği bu davada, kararın kendisinde olduğu gibi karşı oylarda da önemli hususlara dikkat çekilmiştir. Karşı oylarda, çoğunluk görüşüne iki temel eleştiri yöneltilmiştir.

Bunlardan ilki, “*Medyanın gelecekte, neredeyse kalıcı şekilde, orijinal olarak yasal bir biçimde yayınlanan makalelerde sonradan değişiklik yapmasının gerekli olduğu bir duruma izin vermek istiyor muyuz?*” sorusuyla ileri sürülen caydırıcı etkiye ilişkindir. Karşı oy yazısında, buna izin vermenin olası sonuçlarına dair şu ihtimallere dikkat çekilmiştir:

“Bu davada Büyük Daire'nin görevi, çevrimiçi basın arşivlerine ve aynı zamanda genel olarak medya arşivlerine ne tür bir değer atfedilmesi gerektiğini belirlemektir. Medyanın gelecekte, neredeyse kalıcı şekilde, orijinal olarak yasal bir biçimde yayınlanan makalelerde sonradan değişiklik yapmasının gerekli

⁴⁷⁸ Hurbain v. Belgium, para. 241.

⁴⁷⁹ Hurbain v. Belgium, para. 256.

olduğu bir duruma izin vermek istiyor muyuz? Sonuçları ne olurdu? Özellikle, medyanın önceden yayınlanmış materyalin içeriğini değiştirmeye zorlanacağı yönünde sürekli bir tehditle karşı karşıya kalması durumunda, olayları aktarırken çok daha fazla kısıtlama sergilemek zorunda kalacağına inanıyorum. Ayrıca, masraflı mahkeme süreçlerinden ve bu yargılamalarda kaybeden tarafta olma riskinden kaçınmak amacıyla, arşivlenen bilgilerin değiştirilmesine ilişkin talepleri kabul etme yönünde güçlü bir teşvike sahip olacaklardır.”⁴⁸⁰

İkinci eleştiri ise çoğunluğun, söz konusu içerikler üzerinde söz sahibi olan farklı aktörler arasında ayırım yapılmamasına ilişkindir:

“Unutulmamalıdır ki, günümüzde ‘unutulma hakkı’ olarak adlandırılan tartışmanın parametrelerini belirleyen ve giderek artan özel hayatın gizliliği taleplerini tetikleyen şey, öncelikle arama motorlarının bilgiyi erişilebilir kılma gücüdür. Bu arama motorları olmasaydı tartışmanın çerçevesi tamamen farklı olurdu. Dolayısıyla bu gerçeğin altını çizmek ve özellikle arama motorlarının unutulma hakkı iddialarına yanıt ararken ilk başvurulacak adres olması gerektiğini vurgulamak gerekiyor.”⁴⁸¹

Görüleceği üzere karşı oylarda unutulma hakkına değil, unutulma hakkının kapsamına bir karşı çıkış söz konusudur. Dijital basın arşivlerine müdahalenin olası sonuçlarına ve sorunun ortaya çıkışı bakımından arama motorlarının etkisine yapılan özel vurgular, kişilik hakları ve itibara yönelik dijital teknolojik gelişmelerin yol açtığı risklere yönelik alternatif tedbir arayışına işaret etmektedir.

Sorunun merkezinde bulunan internet araçları söz konusu olduğunda, alınacak tedbirler de her halükârda ilgili içeriğin listelenmesine ilişkin olacağından, şirketlerin bu yöndeki talepleri karşılayacak mekanizmalar kurması gerektiği söylenebilir. İçeriğin yayıncısı durumunda olan internet şirketleri bakımından ise alınacak tedbirler

⁴⁸⁰ Hurbain v. Belgium, Dissenting Opinion of Judge Ranzoni Joined By Judges Kūris, Grozev, Eicke And Schembri Orland, para. 5.

⁴⁸¹ Hurbain v. Belgium, Dissenting Opinion of Judge Ranzoni Joined By Judges Kūris, Grozev, Eicke And Schembri Orland, para. 7.

çok daha çeşitli olduğundan, bu şirketlerin insan hakları sorumlulukları kapsamında zorlu bir dengeleme faaliyeti yürütmeleri beklenmektedir.

II. Avrupa Birliği

Avrupa Birliği'nde internet şirketlerinin insan haklarına ilişkin sorumlulukları, internetin henüz geniş bir kullanıcı kitlesine ulaşmadığı yıllardan bu yana düzenlemelere konu olmuştur. 1996-2000 yılları arasında yeni internet servislerinin ortaya çıkması ve beraberinde internet kullanıcı sayısının yüzde 64 oranında artarak 16 milyondan 513 milyona yükselmesiyle bu çalışmalar da hız kazanmıştır. 1996-2000 yılları arasında özellikle erişim sağlayıcılar (*access providers*) ve yer sağlayıcılar (*host service providers*) internetin yönetimindeki kilit rol oynamaktaydı. 2000-2010 yılları arasında teknolojinin gelişmesi ve internet kullanımının katlanarak artmasıyla arama motorları, sosyal medya platformları ve e-ticaret platformları gibi yeni aktörler internet yönetiminde belirleyici hale gelmiştir. Böylece ticari çıkarlar, devletlerin rolü ve bireysel haklar gibi konulara ilişkin tartışmalar da artmıştır. Günümüzde ise bu konular, internet, yapay zekâ ve blok zinciri gibi dönüştürücü teknolojilerin de ekosisteme eklenmesiyle çok daha karmaşık bir hal almıştır.

Avrupa Birliği'nde internetin gelişimine paralel olarak, ele alınan sorunlar ve bu sorunların ele alınış şekli de değişmiştir. Başlangıçta ekonomik bir yaklaşımla “tüketicilerin korunması” amacıyla başlayan endişelere; çocukların, kişisel verilerin, telif haklarının, ifade özgürlüğünün korunması gibi başka endişeler de eklenmiştir. Böylece Birlik hukukunda, üye devletlere yönelik çok sayıda tavsiye niteliğinde tebliğ, karar ve görüş ortaya çıkmıştır. Ayrıca, internetin karmaşıklaşan yapısı karşısında üye devletlerde ortak bir yaklaşımı sağlamak üzere çeşitli düzenlemeler kabul edilmiştir.

İnternet şirketlerinin insan hakları sorumluluklarının ele alındığı erken dönem düzenlemelerde, hukuka aykırı ve zararlı içeriğin etkilerine ilişkin artan toplumsal kaygılar ile ifade özgürlüğü arasındaki dengenin öz düzenleme (*self-regulation*) yoluyla ele alınması teşvik edilmiştir. Böylece, üye devletlerdeki yaygın yaklaşımın⁴⁸² takip

⁴⁸² Protection of Minors and Human Dignity in Audiovisual and Information Services-Consultations on the Green Paper. Commission Staff Working Paper. (SEC (97) 1203), 1997, <https://aei.pitt.edu/1164/>; “Interim Report on Initiatives in EU Member States with Respect to Combating Illegal and Harmful Content on the

edilmesi amaçlanmıştır. Buna göre ortak sorunlarla karşılaşan sektörün kendi kendini düzenleyen kurumları, özellikle teknik çözümlerle ilgili yaklaşımlarını faydalı bir şekilde koordine edebilecektir. Ayrıca, merkezi olmayan internet ortamında internet kullanıcıları da öz düzenlemede önemli rol oynayacaktır.⁴⁸³

Öz düzenlemeden ortak düzenlemeye geçiş, başka bir ifadeyle AB'nin internet düzenlemesine müdahil olması; internet kullanıcılarının güven arayışlarını karşılayarak internette kullanıcı sayısını artırma ve ticaretin serbestçe akabileceği bir alan oluşturma hedefinin bir sonucudur. Dolayısıyla, AB'nin internetteki yasadışı ve zararlı içeriği düzenlemesinin arkasında ekonomik bir motivasyon bulunmaktadır. Bu motivasyonla 1996 yılından bu yana, kamuoyunda artan endişelerin bir sonucu olarak internet içeriğinin düzenlenmesini içeren çeşitli AB girişimleri harekete geçirilmiştir.⁴⁸⁴

AB Konseyi ve Avrupa Komisyonu tarafından başlatılan bu girişimlerde, öz düzenlemenin önemi vurgulanmakla birlikte AB'nin öz düzenleme konusunda gerekli koordinasyonu sağlaması, bu alandaki en iyi uygulamaların paylaşımını teşvik etmesi ve kolaylaştırması, Avrupa'nın kültürel ve dilsel çeşitliliğini dikkate alarak filtreleme, derecelendirme, izleme ve gizliliği artırıcı teknik konularda araştırmayı desteklemesi ve internet içeriği için yasal sorumluluk konusunu daha fazla değerlendirmesi istenmiştir.⁴⁸⁵ Bu kapsamda, özellikle şu üç hedef üzerinde durulmuştur: güvenli ortam yaratma, içerik filtreleme ve derecelendirme sistemleri geliştirme ve farkındalık artırma.⁴⁸⁶ Ayrıca, çocukların hukuka aykırı ve zararlı içerikten korunması konusunda da daha özel hedefler

Internet", 4.7.1997, <https://cordis.europa.eu/article/id/8553-illegal-and-harmful-content-on-the-internet-member-states-initiatives>, (14.10.2023).

⁴⁸³ Commission of the European Communities, "Illegal and Harmful Content on the Internet" (Communication), COM(96) 487, s. 14.

⁴⁸⁴ J Bonnici, C.N.J. de Vey Mestdagh, CNJ, "Right Vision, Wrong Expectations: The European Union and Self-Regulation of Harmful Internet Content", **Information & Communications Technology Law**, C. 14, 2005, s. 136,137.

⁴⁸⁵ Resolution of the Council and of the Representatives of the Governments of the Member States, Meeting within the Council of 17 February 1997 on Illegal and Harmful Content on the Internet, (1997), <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A41997X0306>, (14.10.2023).

⁴⁸⁶ Decision No 276/1999/EC of the European Parliament and of the Council of 25 January 1999 Adopting a Multiannual Community Action Plan on Promoting Safer Use of the Internet by Combating Illegal and Harmful Content on Global Networks, (1999), [http://data.europa.eu/eli/dec/1999/276\(1\)/oj/eng](http://data.europa.eu/eli/dec/1999/276(1)/oj/eng), (14.10.2023).

ortaya koyulmuştur.⁴⁸⁷ Böylece AB, internetin düzenlenmesi konusunda alanı şirketlere bırakmakla birlikte ortak ilkeler belirleyerek onları kontrol etmeye çalışmıştır.

Öz düzenlemeyi önceleyen bu yaklaşımla, henüz gelişme aşamasında olan internetin gelişimini sektöre uğratmamak amaçlanmıştır.⁴⁸⁸ Bu tercih aynı zamanda, AB'nin öz düzenleme ile zararlı içeriğin ortak bir tanımının yapılacağı, zararlı içeriğe yönelik ortak bir çözüm yolu geliştirileceği ve şeffaf ve hesap verebilir bir düzenleme sistemi kurulacağı beklentilerini yansıtmaktadır.⁴⁸⁹

2000 yılında kabul edilen ve üye ülkeler için bağlayıcı nitelik taşıyan E-Ticaret Direktifi'nde (ECD) de benzer şekilde öz düzenlemenin önemi vurgulanmıştır.⁴⁹⁰ Ancak Direktif'te, öz düzenlemeler yanında ortak düzenleme çabaları da teşvik edilmiştir. E-Ticaret Direktifi, tüm bilgi toplumu hizmetlerine uygulanan yatay bir çerçeve direktifidir. ECD'nin kabul edilmesinden bu yana, sektörel kurallarla da yatay temel rejimi tamamlamaya yönelik tedbirler alınmıştır.⁴⁹¹

A. İnternet Şirketlerinin Sorumluluklarına İlişkin Temel Rejim

Avrupa Birliği hukukunda, internet şirketlerinin insan hakları sorumluluklarını düzenleyen temel bir yatay rejim oluşturmuştur. Bu rejim, temel hakların dijital ortamda korunmasını amaçlayan ve farklı sektörlere uygulanabilen genel ilkeler ve kuralları bütünüdür.

⁴⁸⁷ Council Recommendation of 24 September 1998 on the Development of the Competitiveness of the European Audiovisual and Information Services Industry by Promoting National Frameworks Aimed at Achieving a Comparable and Effective Level of Protection of Minors and Human Dignity (98/560/EC), **OJ L**, Council of the European Union, 24.09.1998, <http://data.europa.eu/eli/reco/1998/560/oj/eng>, (14.10.2023).

⁴⁸⁸ Committee on Women's Rights Annexed to Report on the Commission proposal for a Council Decision adopting a Multiannual Community Action Plan on promoting safe use of the Internet (Report of the Committee on Civil Liberties and Internal Affairs rapporteur Mr Gerhard Schmid (A4-0234/98), 09.06.1998, s. 32.

⁴⁸⁹ AB'nin bu beklentilerine yönelik eleştiriler için bkz. Bonnici, de Vey Mestdag, CNJ, "Right Vision, Wrong Expectations", s. 147.

⁴⁹⁰ 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'), C. 178 OJ L § (2000), <http://data.europa.eu/eli/dir/2000/31/oj/eng>, (23.12.2024).

⁴⁹¹ Alexandre De Streel, Martin Husovec, "The E-Commerce Directive as the Cornerstone of the Internal Market", **European Union**, 2020.

Bu rejimin önemli yapı taşlarından ikisi, E-Ticaret Direktifi (ECD) ve Dijital Hizmetler Yasası'dır (DSA). E-Ticaret Direktifi, çevrimiçi hizmet sağlayıcıların hukuka aykırı içerikten sorumluluktan muafiyetlerine ilişkin için genel bir çerçeve sunarken; DSA sorumluluk muafiyetleri yanında, özellikle büyük çevrimiçi platformların sorumluluklarını ve yükümlülüklerini düzenlemektedir. Bu iki düzenleme birlikte, kullanıcıların temel haklarının dijital ortamda korunmasını amaçlayan bir sistem oluşturmaktadır. Bu bölümde, E-Ticaret Direktifi ve Dijital Hizmetler Yasası uyarınca, internet şirketlerinin insan hakları sorumluluklarına ilişkin temel yatay rejim ele alınacaktır.

1. E-Ticaret Direktifi

Avrupa Birliği hukukunda internet şirketlerinin insan hakları sorumlulukları, ilk defa kapsamlı şekilde 2000 yılında kabul edilen E-Ticaret Direktifi'nde ele alınmıştır. E-Ticaret Direktifinin kabulü ile Birlik, uyumunu yüksek düzeye çıkarmayı, küçük ve orta ölçekli işletmeler için dijital ekonomiyi teşvik etmeyi ve dijital pazarda tüketicilerin daha yüksek güvenini ve hukuki belirliliği sağlamayı amaçlamıştır. Bu nedenle Direktif, üçüncü bir tarafça sağlanan yasadışı içeriği barındıran veya ileten “bilgi toplumu hizmeti”⁴⁹² sağlayıcılarının belirli koşullar yerine getirildiğinde sorumluluklardan muaf tutulması yaklaşımını esas almıştır. Direktif, hizmet sağlayıcılar için genel bir sorumluluk rejimi sağlamamakta, bunun yerine hizmet sağlayıcıların AB hukuku kapsamında sorumlu tutulmayacağı özel kurallar, yani güvenli limanlar getirmektedir.⁴⁹³

a. Aracı Hizmet Sağlayıcılar İçin Sorumluluktan Muafiyet Rejimi

Bilgi toplumunun gelişmesinde büyük etkisi olan E-Ticaret Direktifi, tüm sektörler yatay olarak, çeşitli şekillerde çevrimiçi hizmetlerin geliştirilmesine ve işleyişine olanak tanıyan bir koşullu sorumluluk çerçevesi getirmiştir. Direktif'in sorumluluk rejimine ilişkin amaçları, iç pazarın işleyişini kolaylaştırmak, sınır ötesi hizmetlerin gelişimini artırmak ve aracı olarak hareket eden hizmet sağlayıcıların sorumluluğuna ilişkin ulusal hükümlerin uyumlaştırılması yoluyla rekabetin bozulmasını

⁴⁹² “ECD”, resital 17, 18.

⁴⁹³ Tambiama Madiega, **Reform of the EU Liability Regime for Online Intermediaries: Background on the Forthcoming Digital Services Act : In Depth Analysis**, LU: Publications Office, 2020, s. 1.

ortadan kaldırmaktır.⁴⁹⁴ Bu kapsamda hizmet sağlayıcılar, belli koşullar altında, “basit iletim (*mere conduit*)”, “ön belleğe alma (*caching*)” ve “barındırma (*hosting*)” hizmetleri bakımından üçüncü tarafların yasadışı davranışları için sorumluluktan korunmaktadır.⁴⁹⁵

Sorumluluk rejimine geçmeden önce bu rejimi anlaşılır kılacak bazı kavramların ve rejimin genel niteliklerinin açıklanması önemlidir.

Öncelikle, E-Ticaret Direktifi’nin öngördüğü sorumluluk sistemini bir kusur sorumluluğu olarak nitelendirmek mümkündür. Bir hizmet sağlayıcının sorumluluğu belirlenirken genelde iki model üzerinde durulmaktadır. Bunlardan ilki olan objektif sorumluluk sisteminde (*strict liability system*) hizmet sağlayıcı, yasa dışı içerik üzerinde herhangi bir bilgisi veya kontrolü olmasa bile sorumlu tutulur. Öte yandan, kusurlu sorumluluk sisteminde (*with-fault liability system*) hizmet sağlayıcı, yalnızca platformlarında yasa dışı içeriğe bilerek izin vermesi veya bu içeriğe karşı önlem almaması halinde sorumludur. İlki, teknik ve ekonomik açıdan hizmet sağlayıcılara orantısız bir yük yükleme potansiyeli taşıdığından E-Ticaret Direktifi’nde; sorumluluğun, başkalarının haklarının kasıtlı olarak ihlal edilmesi halinde ortaya çıkacağı ikinci sistem tercih edilmiştir. Hizmet sağlayıcının kusurlu davranışı ise gerçek bilgi (*actual knowledge*) ve zımni bilgi (*constructive knowledge*) şeklinde iki farklı seviyede ele alınmaktadır. Gerçek bilgi seviyesinin arandığı hallerde hizmet sağlayıcı, ancak internette birinin haklarını ihlal eden bir materyal olduğunu biliyorsa sorumlu tutulacaktır. İkinci seviye olan zımni bilgi seviyesi ise hizmet sağlayıcının internette birinin haklarının ihlal edildiğine ilişkin ipuçlarına sahip olduğu ya da bunu öngörmesinin beklenebileceği durumlarda sorumluluğu gündeme getirmektedir.⁴⁹⁶ Her iki bilgi seviyesine de atıfta bulunan E-Ticaret Direktifi’nde, bilginin seviyesi sorumluluğun belirlenmesinde rol oynamaktadır. Buna göre hizmet sağlayıcının cezai sorumluluğu için gerçek bilgi gerekliken tazminat taleplerine ilişkin hukuki sorumluluk için zımni bilgi yeterlidir.⁴⁹⁷

⁴⁹⁴ Pablo Baistrocchi, “Liability of Intermediary Service Providers in the EU Directive on Electronic Commerce”, **Santa Clara High Technology Law Journal**, C. 19, S. 1, 2003, s. 112.

⁴⁹⁵ Maria Lilla Montagnani, Alina Trapova, “New Obligations for Internet Intermediaries in the Digital Single Market-Safe Harbors in Turmoil?”, **Journal of Internet Law**, C. 22, S. 7, 2019, s. 3.

⁴⁹⁶ Rosa Julia Barcelo, “Liability for on-line intermediaries: A european perspective”, **European Intellectual Property Review**, C. 20, S. 12, 1998, s. 457.

⁴⁹⁷ “Impact Assessment Report Annexes Accompanying the Document Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC’ (SWD(2020) 348) Part 2/2”, 15.12.2020, s. 157.

ECD'nin bir başka özelliği ise Direktif'te düzenlenen sorumluluktan muafiyet koşullarının sorumluluk için pozitif bir temel teşkil etmemesidir. Bu koşullar, hizmet sağlayıcının hangi durumlarda sorumlu tutulacağını değil, yalnızca sorumluluğun uygulanamayacağı durumları belirlemeye yöneliktir. Dolayısıyla ECD, sorumluluğun kendisini değil, sorumluluğun yokluğunu uyumlaştırmaktadır. Ayrıca bu sorumluluk rejimi, yatay (*horizontal*) ve tarafsızdır (*neutral*). Bu ilkeler uyarınca sorumluluk muafiyetleri; bilginin kaynağı, ilgili hukuk alanı, sorumluluğun nitelendirilmesi veya tam olarak birincil veya ikincil sorumluluk olup olmadığına bakılmaksızın neyin yasadışı sayıldığını belirlemeden, her türlü yasadışı içeriğe uygulanır.⁴⁹⁸ Bu yaklaşım AB mevzuatının; çevrimiçi araçları, koşullar yerine getirildiğinde, telif hakkı ve ticari marka ihlalleri, hakaret, yanıltıcı reklam, haksız ticari uygulamalar, haksız rekabet, yasadışı içerik yayınları vb. dahil olmak üzere üçüncü taraf eylem ve işlemlerinden doğacak her türlü sorumluluktan muaf tuttuğu anlamına gelmektedir. Yatay yaklaşım, sorumluluk kurallarının tasarlanmasında söz konusu farklı menfaatler arasında bir denge kurulmasını gerektirdiğinden hizmet sağlayıcıların sorumluluklarına ilişkin düzenlemelerde hem internette bilginin yasadışı kullanımının önlenmesi hem de AB temel haklarına (örneğin ifade özgürlüğü, kişisel verilerin korunması, mülkiyet hakları, iş yapma özgürlüğü vb.) saygı gösterilmesinin sağlanması amaçlanmıştır.⁴⁹⁹

ECD'de araçların sorumluluklarına ilişkin hükümler, Direktif'in "Aracı Hizmet Sağlayıcıların Sorumluluğu" başlıklı dördüncü kısmında dört maddede düzenlenmiştir. Buna göre hizmet sağlayıcıları için öngörülen sorumluluktan muafiyet rejimi, "*basit iletim, ön belleğe alma, barındırma*" faaliyetlerine yönelik bilgi toplumu hizmetleri bakımından, içerik üzerinde bilgi ve kontrol sağlanmaması koşuluyla, sorumluluktan muaf olacakları güvenli limanların sağlanması şeklinde ifade edilebilir.

Basit iletim (*mere conduit*) faaliyetinin düzenlendiği 12. madde; bir hizmet sağlayıcısının, hizmetin bir iletişim ağı üzerinden bilgi iletimini veya iletişim ağına erişim sağlanmasını içermesi durumunda, sağlayıcının iletilen bilgi için sorumlu olmadığını belirtmektedir. Bu muafiyet; sağlayıcının iletimi başlatmaması, iletimin alıcısını seçmemesi ve iletimde yer alan bilgiyi seçmemesi veya değiştirmemesi, başka bir

⁴⁹⁸ "Impact Assessment 2", s. 163.

⁴⁹⁹ Madiega, *Reform of the EU Liability Regime for Online Intermediaries*, s. 4.

ifadeyle iletişimde pasif bir rol üstlenmesi⁵⁰⁰ şartına bağlıdır. Maddede, basit iletim faaliyeti için öngörülen bu muafiyetin üye devletlerin hukuk sistemleri doğrultusunda, mahkeme veya idari otoritenin, hizmet sağlayıcıdan ihlali sonlandırmasını veya önlemesini talep etme olasılığını etkilemeyeceği belirtilerek muafiyet sınırlandırılmıştır.

Direktif'in 13. maddesi, *hizmetin alıcısı tarafından sağlanan bilgilerin bir iletişim ağına iletilmesi durumunda hizmet sağlayıcının, yalnızca bilginin başka alıcılara istekleri üzerine daha etkin bir şekilde iletilmesini sağlamak amacıyla gerçekleştirdiği bilginin otomatik, ara ve geçici depolanması faaliyetlerinden sorumlu tutulmamasını gerektirmektedir. Ön belleğe alma (caching) faaliyetine ilişkin bu muafiyet; hizmet sağlayıcının bilgiyi değiştirmemesi, bilgiye erişimin koşullarına uygun davranması, bilginin güncellenmesine ilişkin kurallara uyumlu olması, bilginin kullanımına ilişkin veri elde etmek için endüstri tarafından yaygın olarak tanınan ve kullanılan yasal teknoloji kullanımına müdahale etmemesi, iletimin başlangıç kaynağından kaldırıldığı veya erişimin engellendiği veya bir mahkeme ya da idari otorite tarafından bu tür bir kaldırma veya engelleme emri verildiğini öğrendiğinde bilgiye erişimi engellemesi koşullarına bağlıdır. Basit iletim faaliyetine benzer şekilde, ön belleğe alma faaliyetine ilişkin muafiyet de bir mahkeme veya idari otoritenin, hizmet sağlayıcısından bir ihlalin önlenmesi veya sonlandırılması talebinde bulunabilmesi olasılığını da etkilememektedir.*

Barındırma (*hosting*) faaliyetine ilişkin muafiyet ise hizmetin bir alıcısı tarafından sağlanan bilgilerin depolanmasını içeren bir hizmetinin sağlandığı durumlarda, hizmet sağlayıcısının, hizmetin bir alıcısının talebi üzerine depolanan bilgilerden sorumlu olmaması şeklinde düzenlenmiştir. Hizmet sağlayıcının barındırma faaliyetine ilişkin sorumluluktan muafiyeti de hizmet sağlayıcının yasa dışı faaliyet veya bilgiler hakkında gerçek bilgiye sahip olmaması ve tazminat taleplerine ilişkin olarak yasa dışı faaliyet veya bilgilerin açıkça görülebileceği olgu veya durumların farkında olmaması veya bu tür bir bilgi veya farkındalık elde ettiğinde, bilgiyi kaldırmak veya bilgiye erişimi engellemek için hızlı bir şekilde hareket etmesi koşullarıyla kabul edilmiştir.⁵⁰¹

⁵⁰⁰ Benoît Frydman, Ludovic Hennebel, Gregory Lewkowicz, "Co-regulation and the rule of law", **Governance, Regulation and Powers on the Internet**, ed. Cécile Méadel, Eric Brousseau, Meryem Marzouki, Cambridge: Cambridge University Press, 2012, s. 141.

⁵⁰¹ "ECD", m. 14.

Barındırma faaliyetleri, muafiyetin koşulları bakımından basit iletim ve ön belleğe alma faaliyetlerinden önemli ölçüde ayrılmaktadır. Bir barındırma hizmeti sağlayıcısı, barındırdığı hukuka aykırı olduğu iddia edilen faaliyetin ya da bilginin bilgisini edinir ya da farkına varırsa ancak bu içeriği kaldırmak ya da erişimi engellemek için hızlı bir şekilde hareket etmesi halinde sorumluluktan muaf olabilmektedir. Her ne kadar Direktif'te açıkça belirtilmemiş olsa da barındırma faaliyetine ilişkin muafiyetin bu koşulu, devletler tarafından ele alınması beklenen veya öz düzenlemeye bırakılan örtülü bir "uyar-kaldır (*notice and takedown*)" prosedürünü işaret etmektedir.⁵⁰² Barındırma faaliyetleri bakımından da üye devletlerin bir mahkeme veya idari otoriteleri aracılığıyla ihlalin önlenmesi veya sonlandırılması talebinde bulunabilmeleri mümkündür.

Resital 42'ye göre, hizmet sağlayıcıların muafiyeti; teknik, otomatik ve pasif nitelikteki faaliyetler için geçerli olup sağlayıcının aktif olarak hareket ettiği durumları kapsamamaktadır:

*“Bu Direktif'te yer alan sorumluluk muafiyetleri, yalnızca bilgi toplumu hizmet sağlayıcısının faaliyetinin, sadece iletimi daha verimli hale getirmek amacıyla, üçüncü taraflarca kullanıma sunulan bilgilerin iletildiği veya geçici olarak depolandığı bir iletişim ağının işletilmesi ve bu ağa erişim sağlanmasına ilişkin teknik süreçle sınırlı olduğu durumları kapsamaktadır; bu faaliyet yalnızca teknik, otomatik ve pasif niteliktedir ve bu da bilgi toplumu hizmet sağlayıcısının iletilen veya depolanan bilgiler hakkında ne bilgisi ne de bu bilgiler üzerinde kontrolü olduğu anlamına gelmektedir.”*⁵⁰³

Basit iletim ve ön belleğe alma faaliyetleri bakımından hizmet sağlayıcılar çoğunlukla pasif bir role sahiptir ve ilettikleri kullanıcı içeriği hakkında ya hiç bilgi sahibi değildir ya da sınırlı bilgiye sahiptir. Basit iletim hizmeti sağlayıcılar, iletimi başlatmadıkları, alıcıyı seçmedikleri veya iletimde yer alan bilgileri seçmedikleri veya değiştirmedikleri sürece ilettikleri içerikten sorumlu değildir. Ön belleğe alma faaliyeti sağlayıcıları da bilgi iletimini daha verimli hale getirmek için uyguladıkları otomatik, ara ve geçici bilgi depolamasından sorumlu değildir. Buna karşın barındırma hizmeti

⁵⁰² Frydman, Hennebel, Lewkowicz, “Co-regulation and the rule of law”, s. 141,142.

⁵⁰³ “ECD”, resital 42.

sağlayıcılar, barındırdıkları içerik üzerinde daha fazla kontrole sahip olarak daha aktif bir rol oynarlar. Bu nedenle daha sıkı yükümlülöklere ve muafiyet koşullarına tabilerdir.

E-Ticaret Direktifi'nde sorumluluk muafiyetleri yanında, internet şirketleri için öngörölen diğler bir güvenli liman da genel izleme yükümlölüğü yasağıdır. Bu yasak Direktif'in 15. maddesinde *“Üye Devletler, 12, 13 ve 14. maddeler kapsamındaki hizmetleri sağlarken, ilettikleri veya sakladıkları bilgileri izlemek için veya yasadışı faaliyeti gösteren olguları veya koşulları aktif olarak araştırmak için genel bir yükümlölük getiremez.”* şeklinde ve kesin bir dille ifade edilmiştir. Böyle bir yükümlölük; sağlayıcıların ağıları üzerinden akan tüm bilgileri kontrol etmek ve denetlemek zorunda kalmaları anlamına geleceğinden ve bu durumda da hizmetlerin gerçekçi ve ticari bir şekilde sunulmasını neredeyse imkânsız hale getireceğinden, bu güvencenin Direktif'in temel taşlarından biri olduğı söylenebilir.

Direktif'in bu hükümlerinden, internet şirketlerinin sorumluluklarına ilişkin iki temel çıkarımda bulunmak mümkündür. Bunlardan ilkine göre basit iletim, ön belleğle alma, barındırma hizmetleri bakımından internet şirketleri genel bir izleme yükümlölüğü altında değildir. Bununla birlikte şirketlerin, kendi inisiyatifleri ile böyle bir sorumluluk üstlenebilecekleri açıktır. İkinci olarak, şirketler yine sayılan hizmetler bakımından ilgili maddelerde belirtilen koşulları sağladıkları sürece sorumluluktan muaftır.

E-Ticaret Direktifi'nde, sorumluluk muafiyetleri için öngörölen koşullar dışında, hizmet sağlayıcılara bir yükümlölük yüklenmemiştir. Ancak, üye devletler tarafından belirli yasadışı faaliyet türlerinin tespit edilmesi ve önlenmesine yönelik özen yükümlölüklerinin belirlenmesi mümkündür.⁵⁰⁴

b. Sorumluluktan Muafiyet Rejiminin Açmazları

E-Ticaret Direktifi, uygulamada hukuki belirlilik sağlamadığı ve bunun bir sonucu olarak üye devletlerde farklı pratiklere yol açtığı, çevrimiçi hizmet sağlayıcılar ile kullanıcıların hak ve çıkarlarını dengelemediğı gerekçeleriyle eleştirilmiştir.

⁵⁰⁴ “ECD”, resital 48.

Bu eleştiriler dört başlıkta toplanmaktadır. Buna göre Direktif, bilgi toplumu hizmetleri kavramı ile ortaya koyulan çerçevenin yeni tür çevrimiçi hizmetleri kapsayıp kapsamadığına; sorumluluktan muafiyetin koşulları, başka bir ifadeyle güvenli limana giden yolların neler olduğuna; bazı sağlayıcılar için öngörülen “uyar-kaldır” mekanizmasının işleyişine ve araçların korunmasına ilişkin net bir çerçeve sunmamaktadır.

İlk eleştiri bakımından eleştirinin çıkış noktası; ECD resital 17’de bilgi toplumu hizmetlerinin, uzaktan, elektronik araçlarla, hizmet alıcısının bireysel talebi üzerine ve normalde ücret karşılığı sunulan hizmetler olarak tanımlanmasıdır. Sorumluluk muafiyetini “*normalde ücret karşılığında sağlanan*” hizmetler için geçerli kılan bu tanımın; “*reklamlarla desteklenen faaliyetler*”, “*tamamen ücretsiz modeller*” ve “*freemium*⁵⁰⁵ *modeller*” için geçerli olup olmadığı açık değildir. Bu husus, örneğin Fransa’da, Wikimedia Vakfı Davası’nda da gündeme gelmiş ve Paris Temyiz Mahkemesi, Wikimedia Vakfı’nın ücretsiz hizmet sunmasına rağmen barındırma hizmet sağlayıcısı olduğunu belirterek Vakıf lehine karar vermiştir.⁵⁰⁶ Avrupa Birliği Adalet Divanı ise, “*‘bilgi toplumu hizmetleri’ kavramının, hizmet sağlayıcısının alıcı tarafından değil, bir web sitesinde yayınlanan reklamlardan elde edilen gelirle ücretlendirildiği çevrimiçi bilgi hizmetlerinin sağlanmasını kapsadığı şeklinde yorumlanması gerektiği*”ni kabul ederek hizmetin alıcısına ücretsiz sunulmasına rağmen, platformun reklam yoluyla gelir elde ettiğine dikkat çekerek ekonomik bir faaliyetin varlığını aramıştır.⁵⁰⁷ Bu belirsizlik, Direktifin kapsamının ulusal düzeyde farklılaşması yanında, ulusal mahkemeler ile Adalet Divanı arasında da uyumsuzlukları beraberinde getirmiştir.

İkinci olarak, Direktif’te sorumluluktan muafiyetin koşullarına ilişkin kavramlar da net bir şekilde açıklanmamıştır. Direktifin 13. ve 14. maddelerine göre güvenli liman muafiyetinden faydalanabilmek için servis sağlayıcının, ilgili içeriğin hukuka aykırılığı hakkında “*gerçek bilgi edinmesi*” veya “*hukuka aykırı faaliyetlerin veya bilgilerin açıkça görüldüğü olguların veya koşulların farkında olması*” üzerine ilgili içeriği kaldırmak ya

⁵⁰⁵ Kavram, daha fazla özellik için satın alma opsiyonu sunan ücretsiz modelleri tanımlamaktadır.

⁵⁰⁶ Michelle Paulson and Jacob Rogers, “Victory in France: Court Rules in Favor of the Wikimedia Foundation”, *Diff*, 20.06.2016, <https://diff.wikimedia.org/2016/06/20/france-legal-victory/>, (10.5.2023).

⁵⁰⁷ Sotiris Papasavvas v. O Fileleftheros Dimosia Etairia Ltd., Takis Kounnafi, Giorgos Sertis, **Global Freedom of Expression**, (13.03.2024), <https://globalfreedomofexpression.columbia.edu/cases/sotiris-papasavvas-v-o-fileleftheros-dimosia-etairia-ltd-takis-kounnafi-giorgos-sertis/>, (2.10.2024).

da içeriğe erişimi engellemek için “hızlı” hareket etmesi beklenmektedir. Direktif’te hizmet sağlayıcılar belirli hallerde hukuka aykırı içerikten sorumlu tutulmalarına rağmen, hukuka aykırı (*illegal content*) içeriğin kapsamı ve istisnaları belirlenmemiştir. Dolayısıyla telif hakkı, ticari marka ve ticari sırların çevrimiçi ihlalleri; sahtecilik ve internet üzerinden izinsiz dağıtım; tüketici hakları, mahremiyet, iftira ve hakaret yasası ihlalleri; veri koruma ihlalleri; nefret söylemi ve şiddete teşvik ve çocukların cinsel istismarı ve özel cinsel görüntülerin rıza olmadan ifşa edilmesi dahil olmak üzere çok çeşitli içerik kategorileri bu kapsamda ele alınmıştır. Buna karşın, Direktif’te hukuka aykırı olmamakla birlikte zararlı içerik (*harmful content*), bütünüyle sorumluluk rejimi kapsamı dışında bırakılmıştır.⁵⁰⁸

Hukuka aykırı içerikle ilgili olarak dikkat çeken diğer bir eksiklik de hukuka aykırı içerikten sorumluluk ile içeriğe aktif müdahale etmeme şartı arasındaki bağlantının doğru bir şekilde kurulamamasıdır. Söz gelimi, Direktif’te önbellege alma faaliyeti bakımından muafiyet, hizmet sağlayıcının iletme “*aktif olarak müdahale etmemesi*” şartıyla kabul edilmiştir. Bu düzenlemeye göre hizmet sağlayıcının zorunlu olarak aktif davrandığı/davranması gerektiği hallerde de -örneğin aracının yasal yükümlülükleri dolayısıyla çocuk pornografisine erişimi kısıtlamayı amaçlayan filtreler getirmesi- hizmet sağlayıcı iletme aktif olarak müdahale ettiği için paradoksal bir şekilde artan sorumluluk riskiyle karşı karşıya bırakılmıştır.⁵⁰⁹

Sorumluluğun koşullarına ilişkin bu belirsizlikler, güvenli limanlara nasıl ulaşılacağına ilişkin belirsizlikleri de beraberinde getirmiştir.⁵¹⁰ Bu çerçevenin yorum yoluyla belirlenmeye çalışılması ise yasal parçalanmaya ve Direktifin amacının tam tersi şekilde uyumsuzluğa yol açmıştır.⁵¹¹

Direktif’te eleştirilen üçüncü husus, Direktifin 14/1-b maddesinde hizmet sağlayıcılar için örtülü şekilde öngörülen “uyar-kaldır (*notice and takedown*)” mekanizmasının uygulanmasına ilişkin net bir tutumun olmamasıdır. 21. maddede yer

⁵⁰⁸ Madiega, *Reform of the EU Liability Regime for Online Intermediaries*, s. 10.

⁵⁰⁹ Rikke Frank Jørgensen vd., “ICT And Human Rights”, **The Danish Institute For Human Rights Denmark’s National Human Rights Institution**, 2017, s. 31.

⁵¹⁰ Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions (COM(2015) 192 final). A Digital Single Market Strategy for Europe’, 2015, s. 12.

⁵¹¹ Rikke Frank Jørgensen vd., “ICT And Human Rights”, s. 30.

alan “uyar-kaldır” mekanizması bakımından yeni düzenlemelere ihtiyaç duyulacağına ilişkin ima, esasen bunun bir tercih olduğunu göstermektedir. Ne var ki bu durum, “uyar-kaldır” mekanizmasının üye devletlerde farklı şekillerde uygulanmasına yol açmış; bu heterojenlik prosedürde daha fazla çeşitliliğe neden olarak Direktif’in dijital uyum hedefine zarar vermiştir. Ortak bir bildirim ve kaldırma sisteminin olmaması hem kullanıcılar hem de hizmet sağlayıcılar bakımından hukuki belirsizliği artırmanın yanında, hukuka aykırı içerik iddiasıyla talep alan hizmet sağlayıcıların sorumluluktan kaçınmak için bir tür sansür organı haline dönüşmeleri riskini beraberinde getirmiştir.⁵¹² Bu durum, özellikle de içeriğin yasadışı ya da zararlı olmadığı kanıtlanmışsa geçerlidir. Sonuç olarak, söz konusu rekabet halindeki menfaatleri dengeleyen açık ve detaylı bir mekanizma oluşturulmalıdır.⁵¹³ Öte yandan, otomatik içerik düzenleme sistemlerinin de uygulanmaya başlamasıyla ortaya çıkan şeffaflık, hesap verebilirlik ve usul süreçlerine ilişkin endişeler mevcut sorunları daha da derinleştirmiştir.⁵¹⁴

Son olarak, Direktif’in önemli eksiklerinden biri de Direktif’te güvenli liman hükümleriyle araçların sorumluluğu ele alınmasına rağmen araçları içeriğin kaldırılması veya içeriğe erişimin engellenmesi gibi tedbirlerle ilgili davalardan koruyacak düzenlemelerin olmamasıdır. Nitekim koruyucu hükümler, Üye Devletlerin araçlardan içerik kaldırma veya erişimi engelleme prosedürleri uygulamalarını veya hukukun uygulanmasında aktif rol oynamalarını talep etmelerini engelleyememiştir.⁵¹⁵

Sonuç olarak, dünya nüfusunun yüzde 7’sinden daha azının internet kullanıcısı olduğu 2000 yılında⁵¹⁶ kabul edilen E-Ticaret Direktifi tarafından belirlenen çevrimiçi araçlar için sorumluluktan muafiyet rejimi, dijital hizmetler pazarının hızlı gelişimini de yeterince ele almamıştır.

2016 yılına gelindiğinde, dijital hizmetlere ilişkin yeni bir ana akım düşünce yayılmaya başlamıştır. Avrupa Birliği Adalet Divanı’nın (ABAD) “unutulma hakkını” kabul etmesiyle arama motorlarının bireylere karşı sorumluluğuna ilişkin baskılar

⁵¹² Baistrocchi, “Liability of Intermediary Service Providers in the EU Directive on Electronic Commerce”, s. 131.

⁵¹³ Ibid., s. 123.

⁵¹⁴ Sander Sagar, Thomas Hoffman, “Intermediary Liability in the EU Digital Common Market-From the E-Commerce Directive to the Digital Services Act”, IDP. **Internet, Law and Politics E-Journal**, No. 34.

⁵¹⁵ Rikke Frank Jørgensen vd., “ICT And Human Rights”, s. 31.

⁵¹⁶ <https://data.worldbank.org/indicator/IT.NET.USER.ZS>, (20.12.2024)

artmıştır. Öte yandan, Facebook'un Myanmar'da içerik denetimini ihmal etmesi, sağlayıcıların daha az kazançlı pazarlarda kronik olarak yetersiz yatırım yapmasının ciddi risklerini ortaya çıkarmıştır. 2016 ABD seçimleri öncesinde sosyal medyada içerik denetimine ilişkin iddialar, internet şirketlerinin sorumluluklarına ilişkin tartışmaları daha ciddi boyutlara taşımıştır. Avrupa'da göç krizi yaşanırken de nefret söyleminin hızla yayılmasıyla platformlar üzerindeki dikkatler artmıştır. Bütün bu gelişmeler, internet şirketleri ve insan hakları ilişkilerinde öz düzenlemenin yetersizliğini ve yeni bir ortak düzenleme ihtiyacını ortaya çıkarmıştır.⁵¹⁷

Bu kapsamda, E-Ticaret Direktifi yanında Görsel İşitsel Medya Hizmetleri Direktifi⁵¹⁸ ya da Dijital Ortak Pazar Direktifi⁵¹⁹ gibi ek düzenleyici önlemler alınmaya çalışılsa da bu ek çerçeveler E-Ticaret Direktifi ile uyumlulukları açısından çeşitli hukuki zorluklar ortaya çıkarmıştır. Ayrıca, AB Üye Devletleri'nin dijital hizmetler pazarını düzenlemek için kendi ulusal mevzuatlarını kabul etmeleri, AB içinde sınır ötesi dijital hizmetler sağlama konusunda hukuki parçalanma ve belirsizliği artırmıştır. Böylece, aracı sorumluluğu meselesi sürekli olarak tartışma konusu olmuştur.

Bu belirsizlikler ve zorluklar, Avrupa Birliği Adalet Divanı'nın Direktifin sorumluluk sistemi hakkında kesin yorumlar sağlayamaması dolayısıyla⁵²⁰ yargı yoluyla da aşılamamıştır.⁵²¹ Böylece internet servis sağlayıcıları, ifade özgürlüğü hakkını ve hizmetlerinin alıcıları tarafından sunulan çevrimiçi içeriğin dolaşımını korumak yerine, kendileri için daha az maliyetli bir yol seçerek özel anlaşmalar, mahkeme dışı uzlaşmalar ve talep üzerine işaretlenen içeriği kaldırarak otosansür yoluyla kendi haklarını aktif

⁵¹⁷ Martin Husovec, "Rising above Liability: The Digital Services Act as a Blueprint for the Second Generation of Global Internet Rules", **Berkeley Technology Law Journal**, C. 38, 2023, ss. 883-920.

⁵¹⁸ Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the Coordination of Certain Provisions Laid down by Law, Regulation or Administrative Action in Member States Concerning the Provision of Audiovisual Media Services, ss. 1-24, <https://eur-lex.europa.eu/eli/dir/2010/13/oj>, (5.12.2024).

⁵¹⁹ Directive (EU) 2019/ 790 of the European Parliament and of the Council of 17 April 2019 on Copyright and Related Rights in the Digital Single Market and Amending Directives 96/9/EC and 2001/29/EC, ss. 92-125.

⁵²⁰ Avrupa Birliği Adalet Divanı'nın ilgili kararları, aşağıda II/C başlığı altında ele alınmaktadır.

⁵²¹ Sophie Stalla-Bourdillon, "Internet Intermediaries as Responsible Actors? Why It Is Time to Rethink the E-Commerce Directive as Well", **The Responsibilities of Online Service Providers**, ed. Mariarosaria Taddeo, Luciano Floridi, Law, Governance and Technology Series, Cham: Springer International Publishing, 2017, C. 31, ss. 275-93. Christina Angelopoulos, "Beyond the Safe Harbours: Harmonising Substantive Intermediary Liability for Copyright Infringement in Europe", **Intellectual Property Quarterly**, 2013-3, 2013, ss. 253-74; En Fernández-Díez Ignacio Garrote, "Comparative analysis on national approaches to the liability of Internet intermediaries for infringement of copyright and related rights", WIPO, 2014, <https://www.wipo.int/publications/en/details.jsp?id=4145&plang=E>, (8.10.2024).

olarak korumaya yönelmiştir. Bütün bunlar da nihayetinde, dijital hizmet sağlayıcılarının sorumluluğuyla ilgili mevcut AB yasal çerçevesini uyumlaştırmayı ve gözden geçirmeyi amaçlayan Dijital Hizmetler Yasası'nın hazırlanmasına yol açmıştır.⁵²²

2. Dijital Hizmetler Yasası

E-Ticaret Direktifi'nin yirmi yıl önce kabulünden bu yana çevrimiçi platformlar dijital ekonomide kilit araçlara dönüşürken, aynı zamanda bilginin hem kaynağı hem de şekillendiricisi haline gelmiştir. Günümüzün arama motorları, sosyal medya ağları ve e-ticaret platformları, yalnızca hangi kullanıcıların ekosisteme katılabileceğini veya işlemlerin platform üzerinden nasıl gerçekleştirileceğini değil, aynı zamanda ilgili kullanıcıların hangi bilgileri alacağını da belirlemektedir. Dolayısıyla, daha önce pasif ve tarafsız aracı konumuyla tanımlanan platformlar artık aktif dijital alan ortakları olarak nitelendirilmektedir.⁵²³

Aradan geçen süre içerisinde platformlar, video paylaşım sitelerinde telif hakkı ile korunan eserlerin yasadışı dağıtımı, e-ticaret platformlarında sahte ürünlerin satışı veya sosyal medya platformlarında nefret söylemi ve şiddeti öven içeriklerin yayılması gibi yasadışı faaliyetler için bir “fırsat” yaratmıştır. Platformların, dezenformasyonun yayılmasındaki etkileri de giderek artan bir endişeye yol açmıştır.

Dijital alandaki bu gelişmeler, dijital alanda hukukun üstünlüğünün sağlanması ve temel hak ve özgürlüklerin korunmasına yönelik hukuki çalışmaların tetikleyicisi olmuştur. Bunun sonucunda Avrupa Birliği'ne üye devletlerde, yasadışı içerik, çevrimiçi yanıltıcı bilgi veya diğer toplumsal riskleri konu alan ulusal yasa hazırlıkları ortaya çıkmıştır. Farklı ulusal yasaların iç piyasayı olumsuz etkileme potansiyeli ise konunun Birlik düzeyinde ele alınması ihtiyacını ortaya çıkarmıştır. Bu doğrultuda, 19 Ekim 2022 tarihinde Dijital Hizmetler Yasası (DSA) kabul edilmiştir.⁵²⁴

⁵²² Sagar, Hoffman, “Intermediary Liability in the EU Digital Common Market-From the E-Commerce Directive to the Digital Services Act”, ss. 3-4.

⁵²³ Miriam Buiten, “The Digital Services Act: From Intermediary Liability to Platform Regulation”, JIPITEC, C. 12, S. 5, 2021, ss. 361-380.

⁵²⁴ 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, (2022), <https://eur-lex.europa.eu/eli/reg/2022/2065/oj>, (2.5.2023).

Her ne kadar çıkış noktalarından biri piyasanın işleyişini korumak ve iyileştirmek olsa da DSA'nın temel amacı; yenilikçiliği kolaylaştıran ve tüketicinin korunması ilkesi de dahil olmak üzere Avrupa Birliği Temel Haklar Şartında yer alan temel hakların etkin bir şekilde korunduğu güvenli, öngörülebilir ve güvenilir bir çevrimiçi ortam sağlamaktır.⁵²⁵ Bu kapsamda, özellikle büyük sosyal medya platformları ve çevrimiçi pazar yerleri için, hukuka aykırı içeriğin denetimi bakımından belirli özen yükümlülükleri ve uyar-kaldır mekanizmaları oluşturularak, sorumluluk alanları ve hesap verebilirlik araçları net bir şekilde belirlenmektedir. DSA'da otomatik filtreleme araçları da ele alınarak bu araçların risk değerlendirmesindeki yükümlülükleri artırılmakta; çok büyük çevrimiçi platformlar uygun risk yönetimi ve denetim sistemleri oluşturmaya zorlanmaktadır.⁵²⁶ Bu yönüyle DSA, Avrupa Birliği'nin "Dijital Anayasası" olarak da anılmaktadır.⁵²⁷

E-Ticaret Direktifi bağlamında, DSA'nın Direktifi yürürlükten kaldırmak yerine sadece bazı hükümlerini değiştirdiğinin altını çizmek gerekir. Başka bir deyişle DSA, mevcut mevzuatı ilga etmemekte, onlarla birlikte var olmaktadır.⁵²⁸ Böylece, DSA ile E-Ticaret Direktifi ve halihazırda uygulamaya konulmuş diğer daha yeni sektöre veya konuya özgü araçların tamamlanması amaçlanmaktadır.

Genel olarak ifade etmek gerekirse DSA, E-Ticaret Direktifi'nin üç temel esası olarak kabul edilen; i) sorumluluktan muafiyet, ii) menşei ülke ilkesi, iii) genel izleme yükümlülüğü yasağı prensiplerini korumakla birlikte, değişen koşulları göz önünde bulundurarak bu ilkelere yeni bir biçim kazandırmaktadır.

⁵²⁵ Ibid., m. 1(1).

⁵²⁶ Sagar, Hoffman, "Intermediary Liability in the EU Digital Common Market-From the E-Commerce Directive to the Digital Services Act", s. 6.

⁵²⁷ Avrupa Parlamentosu üyesi ve Yeşiller/EFA (Avrupa Özgür İttifakı) Grubu İç Pazar ve Tüketicinin Korunması Komitesi gölge raportörü Alexandra Geese, DSA'nın kabulüne ilişkin şu yorumda bulunmuştur: "Avrupa için dijital bir anayasanın vadesi çoktan geçmişti. Avrupa Parlamentosu DSA ile ilgili üçlü müzakerelere güçlü bir konumla giriyor: Facebook ve Google gibi teknoloji devleri artık dijital ekosistemimiz üzerindeki kontrolü tekeline alamamalı. Bu yasayla AB, ifade özgürlüğünü korurken sistemik risklerle de mücadele etmeyi başarıyor. Platformlar, kullanıcılarının ifadelerinden değil, kendi davranışlarından sorumlu hale gelir." "European Parliament Votes on Constitution for the Internet", **Greens/EFA**, (23.10.2024), <https://www.greens-efa.eu/en/article/press/european-parliament-votes-on-constitution-for-the-internet>.

⁵²⁸ Miriam Buiten, "The Digital Services Act: From Intermediary Liability to Platform Regulation", 2021, s. 11.

İlk olarak DSA’da E-Ticaret Direktifi’nin sorumluluk rejimi korunmakla birlikte, çevrimiçi platformların yasadışı içeriği nasıl kaldıracağı ayrıntılı olarak ele alınmıştır. Sorumluluk rejiminin korunmasının arka planında, Avrupa Birliği Adalet Divanı’nın (ABAD) mevcut kurallara ilişkin bir içtihat geliştirmiş olması ve gelişen içtihadın birçok yeni hizmet türünün ortaya çıkmasına ve gelişmesine yardımcı olması⁵²⁹; sorumluluktan muafiyet yerine araçlara daha fazla hukuki risk yüklemenin kullanıcıların ifade özgürlüğüne zarar verebilme ihtimali; sorumluluk rejiminin değiştirilmesinin yeni işletmeler için çok maliyetli olacağı; sorumluluk muafiyetleri için gerekli standardın düşürülmesinin çevrimiçi ortamda güvenlik ve güveni etkileyeceği gibi çok çeşitli nedenler bulunmaktadır.⁵³⁰

İkinci olarak, E-Ticaret Direktifi’nde yer alan ve bir çevrimiçi platformun yalnızca kurulu olduğu üye devletin sorumluluk rejimine tabi olmasını ifade eden menşe ülke ilkesi (*country-of-origin principle*) de DSA’da korunmuştur. Bununla birlikte, bilgi toplumu hizmet sağlayıcılara yönelik önemli hususların birçoğu DSA’da ayrıntılı şekilde ve Avrupa düzeyinde ele alınması, yani ulusal hukuklara farklılaşabilecekleri çok sınırlı alan bırakılması bu ilkenin pratikteki önemini azaltmıştır.⁵³¹

Üçüncü olarak, ECD’de olduğu gibi DSA’da da aracı hizmet sağlayıcılara yönelik genel izleme yükümlülüğü yasağı, belli durumlarda özel izleme yapma yükümlülüğü getirilebileceği istisnasıyla kabul edilmiştir. ECD Resital 47’den farklı olarak, DSA Resital 30’da ulusal otoriteler tarafından getirilebilecek özel izleme yükümlülüklerinin Birlik hukukuna ve içtihadına uygun olması gerektiğinin altı çizilmiştir. Böylece, Avrupa Birliği Adalet Divanı’nın özel izleme yükümlülüğüne ilişkin yorumlarının geçerliliği onaylanmıştır.

DSA’da bu temel ilkelere yeni bir biçim kazandırılması yanında, hizmet sağlayıcılara yönelik yeni yükümlülüklerle de yer verilmiştir. Bu, araçların E-Ticaret Direktifi’nin sağladığı sorumluluk muafiyetini kaybetmediği, ancak ek yükümlülüklerle

⁵²⁹ “DSA”, resital 16.

⁵³⁰ “Impact Assessment Accompanying the Document Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC” (SWD(2020) 348) Part 1/2”, 15.12.2020, s. 48, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020SC0348>.

⁵³¹ Folkert Wilman, “The Digital Services Act (DSA) An Overview”, SSRN Scholarly Paper, Rochester, NY, 16.12.2022, s. 3.

tabi olduğu anlamına gelir.⁵³² Başka bir deyişle, Dijital Hizmetler Yasası ile hizmet sağlayıcıların kullanıcı tarafından oluşturulan içeriğe ilişkin sorumluluğu büyük ölçüde aynı kalırken, karar alma ve dijital hizmetleri tasarlama süreçlerinde dikkate almaları gereken hususlar değişmektedir.⁵³³ Bildirim ve eylem sistemi kapsamında yasadışı çevrimiçi içerikle mücadele, platformların içerik engelleme veya kaldırma kararlarına itiraz etmelerine olanak tanıyan dahili şikayet mekanizmalarının kurulması ve çok büyük çevrimiçi platformlar ile çok büyük arama motorlarına yönelik kapsamlı görevler buna örnektir. Bu yenilikler, hizmet sağlayıcılar için öngörülebilirliği artırırken, kullanıcıların da ifade özgürlüğü ve bilgi edinme hakları bakımından daha güvenceli bir ekosistem sağlamaktadır. Bu sistemler, çevrimiçi platform kullanıcılarının ifade özgürlüğü ve bilgi edinme haklarını kullanmalarını garanti eder.⁵³⁴

Dijital Hizmetler Yasası, yasanın adında belirtilenin aksine, tüm dijital hizmetleri değil, aracı hizmetler olarak nitelendirilen ve temelde kullanıcılar tarafından oluşturulan içeriğin iletilmesini ve depolanmasını içeren hizmetleri konu almaktadır.⁵³⁵ Yasanın kapsamını, sağlayıcılar değil de hizmetler belirlemektedir. Dolayısıyla, birden fazla hizmet sunan hizmet sağlayıcıların, hizmetlerinden bazılarının DSA kapsamında olması ve diğerlerinin olmaması (ya da hizmetlerin kapsam dahilinde olduğu durumlarda, DSA'da yer alan farklı kurallara tabi olmaları) mümkündür.

Ayrıca, hizmet sağlayıcının yerleşik olduğu ülkenin de DSA'nın uygulanabilirliğinde bir önemi bulunmamaktadır. Önemli olan, söz konusu hizmetin AB'de sunulup sunulmadığıdır. Bir aracı hizmet sağlayıcının Birlik ile “önemli bir bağlantısı” varsa AB’de hizmet sunduğu kabul edilmektedir. DSA’da şu üç halde hizmet sağlayıcı ile Birlik arasında önemli bir bağlantı olduğu kabul edilmektedir:⁵³⁶ i) hizmet sağlayıcının Birlikte bir kuruluşunun olması; ii) hizmet sağlayıcının Birlikte bir kuruluşu olmasa da bir veya daha fazla üye devletteki hizmetin alıcısı sayısının bu ülkelerin

⁵³² Andrej Savin, “The EU Digital Services Act: Towards a More Responsible Internet”, **Copenhagen Business School, CBS Law Research Paper No. 21-04**, 2021, s. 5.

⁵³³ Husovec, “Rising above Liability”, s. 898.

⁵³⁴ Ibid.

⁵³⁵ Sadece aracılık hizmetlerini değil daha genel bir ifadeyle bilgi toplumu hizmetlerini konu alan E- Ticaret Direktifi bu bakımdan DSA’dan daha kapsamlıdır. Bu direktif DSA’nın kabul edilmesinden sonra da varlığını sürdürdüğünden bu düzenlemeler arasında genel hüküm (*lex generalis*)- özel hüküm (*lex specialis*) ilişkisi kurulabilir. Wilman, “The Digital Services Act (DSA) - An Overview”, ss. 2, 3.

⁵³⁶ “DSA”, resital 8.

nüfusuna oranla önemli olması; iii) faaliyetlerin bir veya daha fazla üye devlete yönelik olarak hedeflenmesi.⁵³⁷

DSA’da hizmet sağlayıcılara yönelik düzenlemelerin iki boyutu vardır. Bunlardan biri, hizmet sağlayıcıların sorumluluk rejimine; diğeri ise özen yükümlülüklerine ilişkindir. Belirtmek gerekir ki özen yükümlülükleri, sorumluluk muafiyetinden bağımsız olarak düzenlenmiştir. Teklif aşamasında, her ne kadar özen yükümlülüğünün sorumluluktan muafiyetin bir şartı olarak düzenlenmesi ileri sürülmüşse de bu öneri kabul edilmemiştir. Önerinin kabul edilmemesi, yani özen yükümlülüğünün bağımsız olarak öngörülmesinin gerekçesi, Etki Değerlendirmesi Raporu’nda özen yükümlülüğün etkili kılınması ve kamu otoritelerinin iş yükünün artırılmaması amaçları vurgulanarak şu şekilde açıklanmıştır:

“Özen yükümlülüğünü sorumluluk muafiyetinin bir şartı olarak yapılandırmak, uyumluluğun nihayetinde gönüllü olacağı anlamına gelir. Bu durumda, aracı hizmet sağlayıcı kurallarına uymak için yalnızca ‘teşvik edilecek’, ‘zorunlu kılınmayacaktır.’ Aracı, ulusal veya AB mevzuatına göre mahkeme tarafından sorumlu tutulmayacağını veya uyumluluğun maliyetinin potansiyel yaptırımlardan daha düşük olabileceğini değerlendirerek bir risk hesaplaması yapabilir. Bazı durumlarda, özellikle tazminat davalarının gerçekçi bir tehdit olmadığı durumlarda, aracılardan muafiyet koşullarına uyma teşviki sınırlı olabilir. Ancak, aracılardan ilgili gerekliliklere uyup uymama seçeneği bırakılmamalı ve bu amacı gerçekleştirmek için bağımsız yükümlülükler getirilmelidir.

Ek olarak, özen yükümlülüğüne uyum, daha sistematik bir denetime tabidir ve sorumluluğu veya muafiyetini belirlemek için ceza ve hukuk davalarında yapılan olay ve durum değerlendirmelerinin ötesinde bir soruşturma içerir. Sorumluluk muafiyetlerini genel özen yükümlülüğüne dayalı bir şartlılığa dahil etmek, mahkemeler ve idari makamlar için haksız bir yük oluşturur.”⁵³⁸

⁵³⁷ Örneğin, bir uygulamanın ulusal uygulama mağazasında bulunmasından, söz konusu Üye Devlette kullanılan bir dilde yerel reklam veya ilan verilmesinden veya söz konusu Üye Devlette genel olarak kullanılan bir dilde müşteri hizmetleri sunulmasından kaynaklanabilir. Ibid., resital 8.

⁵³⁸ “Impact Assessment 2”, ss. 165-166.

DSA’da hizmet sağlayıcılar dışında üye devletlere yönelik de ayrıntılı yükümlülükler yer verilmiştir. Bu bölümde, çalışma kapsamının dışına çıkmadan, yalnızca internet şirketleri için öngörülen yükümlülükler ele alınacak, şirketlerin hukuka uygun hareket etmelerini sağlama ve kullanıcıların temel hak ve özgürlüklerini korumaları konusunda üye devletler için öngörülen yükümlülükler yer verilmeyecektir. Bu yükümlülükleri daha anlaşılır kılmak amacıyla, yükümlülükler geçmeden önce DSA’ya hâkim olan temel ilkeler ortaya koyulacaktır.

a. Dijital Hizmetler Yasasına Hâkim Olan İlkeler

Dijital Hizmetler Yasası, AB’nin dijital ortamda kullanıcıları ve temel hakları korumaya yönelik uzun süreli çabalarının bir sonucudur. Bu kapsamda, Komisyon tarafından yıllar boyunca çok çeşitli paydaşlarla (dijital hizmet sağlayıcılar, diğer işletmeler, akademi, kamu makamları, sivil toplum kuruluşları ve vatandaşlar dahil), çok sayıda görüşme gerçekleştirilmiştir.

Bu görüşmelerde, genel olarak E-Ticaret Direktifi’nde yer alan çeşitli hususların dijital gelişmeler ışığında güncellenmesi gerektiği kabul edilmekle birlikte sorumluluk muafiyeti ve genel izleme yasağı başta olmak üzere, Direktif’in temel prensiplerinin bugün hala geçerli olduğu ve DSA’ya aktarılması gerektiği fikri de desteklenmiştir.⁵³⁹ Böylece, platform yönetimine ilişkin düzenlemelerin ortak zemininde, öte yandan bireyler, toplum ve şirketlere yönelik yeni riskleri de dikkate alan bir metin inşa edilmiştir.

DSA’nın kapsamlı yapısı pek çok konuya ilişkin çok çeşitli çıkarımlar yapmayı mümkün kılarsa da düzenlemelerin geneline yansıyan bazı genel ilkeleri özel olarak öne çıkarmaya engel teşkil etmemektedir. Bu noktada DSA’nın dayandığı temel ilkeleri, i. sorumluluk yerine hesap verebilirlik, ii. asimetrik yaklaşım (*asymmetrical approach*) iii. düzenlemelerin yataylığı (*horizontality of regulations*), iv. sorumluluğun paylaşılması, v. kullanıcıların yetkilendirilmesi ve vi. ekosistem çözümleri⁵⁴⁰ şeklinde altı başlıkta ele almak mümkündür.

⁵³⁹ Ilaria Buri, Joris van Hoboken, “‘The Digital Services Act (DSA) Proposal: A Critical Overview’: Discussion Paper”, 2021, s. 6, <https://dare.uva.nl/search?identifier=d51d31c3-cfef-4034-b04a-c353f4ac07ea>, (10.06.2024).

⁵⁴⁰ Husovec, “Rising above Liability”, s. 909.

i. Sorumluluk yerine hesap verebilirlik ilkesi, hizmet sağlayıcıların sorumluluk rejimine ilişkindir. DSA, hizmet sağlayıcıların hukuka aykırı üçüncü taraf içerikleri bakımından suç ortağı olarak ele alındığı düzenlemelerin ötesine geçmiş, yargı organlarının tam sorumluluk ya da tam muafiyet ikilemine son vermiştir. Bunu yaparken, bir yandan E- Ticaret Direktifinde öngörülen muafiyetleri benimsemekte, diğer yandan da kullanıcıların içeriklerinin denetlenmesi veya diğer genel risklerin yönetilmesi için kullanılan sistem ve prosedürlerin işleyişini iyileştirmeyi amaçlayan özen yükümlülükleri (*due diligence*) öngörmektedir.⁵⁴¹

ii. Asimetrik yaklaşım ise DSA'nın, platformların büyüklüğüne ve yarattığı risklere göre farklı yükümlülükler öngören sistematığını ifade etmektedir. DSA'da çevrimiçi ortamda temel hakların korunması amacıyla kabul edilen özen yükümlülükleri; aracı hizmet sağlayıcılar, barındırma sağlayıcıları, çevrimiçi platformlar ve çok büyük çevrimiçi platformlar (VLOPs) ile çok büyük arama motorları (VLOSEs) arasında ayırım yapan kademeli bir yapıda ele alınmıştır.

Bu yapı, her biri farklı hizmetleri düzenleyen dört yatay katmana sahip bir piramidi andırmaktadır. Bu piramidin en alt ve en geniş katmanında tüm aracılık hizmetleri için geçerli olan temel yükümlülükler; ikinci katmanda, hizmet alıcısı tarafından ve onun talebi üzerine sağlanan bilgilerin depolanmasından oluşan barındırma hizmetleri için geçerli yükümlülükler; üçüncü katmanda “çevrimiçi platformlar” ile ilgili yükümlülükler ve en üstte ise çok büyük çevrimiçi platform ve çok büyük arama motoru sağlayıcıları için yükümlülükler yer almaktadır.⁵⁴² Piramitte yukarı doğru çıkıldıkça, giderek daha az sayıda sağlayıcı kategorisi için geçerli olan ve giderek sıkılaştan yükümlülükler ortaya çıkmaktadır.

Barındırma hizmetlerinin özel bir alt kategorisi olan çevrimiçi platformlar, kullanıcıların bilgilerinin depolanması yanında kamuya yayılmasını da sağladıklarından, barındırma hizmetleri için öngörülenlere ek bazı yükümlülüklerle daha tabi kılınmıştır. Bu yapılırken, şirketlere aşırı yük yüklenmemesi konusunda da özen gösterilmiştir. Taraflar arasında denge kurmayı amaçlayan bu yaklaşım uyarınca, çevrimiçi platformlara yönelik sınırlandırıcı ve negatif bir tanımlama yapılmıştır. Buna göre hizmet alıcıları tarafından

⁵⁴¹ Ibid.

⁵⁴² Wilman, “The Digital Services Act (DSA) - An Overview”, s. 3.

sağlanan bilgileri onların talebi üzerine depolamakla kalmayıp aynı zamanda bu bilgileri hizmet alıcılarının talebi üzerine kamuya yayan yer sağlayıcı hizmetleri sağlayıcıları olarak tanımlanmalıdır. Bununla birlikte, bir hizmet alıcısının talebi üzerine bilgiyi depolayan ve halka yayan barındırma hizmetleri bu faaliyetin, başka bir hizmetin önemsiz ve sadece ek bir özelliği olmaması, nesnel ve teknik nedenlerle söz konusu hizmet olmadan kullanılamaması ve bu özelliğin diğer hizmete entegre edilmesi DSA'nın uygulanmasını önlemek için bir araç olmaması şartlarıyla çevrimiçi platform olarak kabul edilmektedir. Bu tanıma göre bir hizmetin bilgi depolama ve yayma özelliği, başka bir hizmetin önemsiz ve sadece ek bir özelliği olursa ya da hizmet, nesnel ve teknik nedenlerle ana hizmetten ayrılabilirse veya bu özelliğin eklenmesi yasadan kaçınmak için bir araç olarak kullanılmışsa çevrimiçi platform olarak sayılmayacaktır.⁵⁴³ Bu tanıma göre çevrimiçi bir platformun ayırt edici unsuru; verilen hizmetin, esasında kullanıcıların bilgilerinin kamuya yayılması olmasıdır.

Örneğin, kullanıcıların ürünlerini satmalarına ve satın almalarına olanak tanıyan bir e-ticaret platformu kullanıcıların ürün yorumlarını ve puanlarını da barındırabilir. Bu yorum ve puanlama sistemi, platformun temel işlevi için gerekli olmadığından ve teknik olarak da platformdan ayrılabilir olduğundan "çevrimiçi platform" olarak sayılmamaktadır. Dolayısıyla, bu kapsamda olmayan hizmet sağlayıcılar, çevrimiçi platformlar için bu kısımda sayılan ek yükümlülöklere tabi değildir.⁵⁴⁴

Çok büyük çevrimiçi platformlar ve çok büyük arama motorlarının yükümlölükleri ise -alt katmanlardakilere göre daha fazla aktif kullanıcılarının olmasının bir sonucu olarak- kamusal tartışmada, bilginin çevrimiçi olarak erişilebilir kılınmasında,

⁵⁴³ “Sosyal ağlar veya tüketicilerin tüccarlarla mesafeli sözleşmeler yapmasına olanak tanıyan çevrimiçi platformlar gibi çevrimiçi platformlar, yalnızca hizmet alıcıları tarafından sağlanan bilgileri onların talebi üzerine depolamakla kalmayıp aynı zamanda bu bilgileri hizmet alıcılarının talebi üzerine kamuya yayan yer sağlayıcı hizmetleri sağlayıcıları olarak tanımlanmalıdır. Bununla birlikte, aşırı geniş yükümlölükler getirmekten kaçınmak amacıyla, yer sağlayıcı hizmet sağlayıcıları, kamuya yaymanın yalnızca başka bir hizmetle özünde bağlantılı olan küçük ve tamamen yardımcı bir özellik veya asıl hizmetin küçük bir işlevselliği olduğu ve bu özellik veya işlevselliğin objektif teknik nedenlerle diğer veya asıl hizmet olmadan kullanılmadığı ve bu özellik veya işlevselliğin entegrasyonunun bu Tüzüğün çevrimiçi platformlara uygulanan kurallarının uygulanabilirliğini atlatmak için bir araç olmadığı durumlarda çevrimiçi platformlar olarak değerlendirilmemelidir.” “DSA”, resital 13.

⁵⁴⁴ DSA’da, çevrimiçi platform tanımına uymakla birlikte mikro ve küçük ölçekli nitelikteki işletmeler de bu kısımda sayılan yükümlölüklerden muaf tutulmuştur. Bununla birlikte, 2003/361/EC sayılı Tavsiye Kararı’nda mikro ya da küçük işletme olarak nitelendirilmesine rağmen DSA’nın 33. maddesine göre, “çok büyük çevrimiçi platform (VLOP)” olarak kabul edilen platformlar bu muafiyetten istisna tutulmuştur. “DSA”, m. 19(2).

bilgi, görüş ve fikirlerin kamuya yayılmasındaki ayırt edici rolleri dolayısıyla daha da kapsamlıdır. Bu noktada, bir çevrimiçi platformun ya da arama motorunun hangi durumda “çok büyük” sayılacağı hususu netleştirilmelidir. Bu eşik DSA’da, “*Birlik içinde aylık ortalama aktif hizmet alıcı sayısı 45 milyona eşit veya daha fazla olmak*”⁵⁴⁵ şeklinde nicel bir kriter esas alınarak belirlenmiştir. DSA uyarınca bu kategoride yer alan hizmet sağlayıcılar, Komisyon tarafından pazar ve teknolojik gelişmeleri dikkate alan bir metodoloji ile tespit edilecek ve yayınlanacaktır.⁵⁴⁶

DSA’da, çok büyük çevrimiçi platformlar ile çok büyük çevrimiçi arama motorları belirlenirken hizmetin niteliği ya da etkisi yerine, aktif kullanıcı sayısına odaklanılarak; sahip oldukları çok sayıda kullanıcı sayesinde toplum üzerindeki geniş etki uyandırabilen ve yine aynı sebeple, hukuka aykırı ve zararlı içeriğin yayılmasında daha ciddi risk teşkil eden hizmet sağlayıcıların yükümlülüklerinin artırılması ve böylece internetteki genel güvenliğin ve kullanıcı haklarının korunması amaçlanmaktadır.

Katmanlar arasındaki ilişki, başka bir ifadeyle DSA kapsamındaki yükümlülükler, bir katmandaki belirli bir hizmet piramidinin başka katmanındakilerle örtüştüğü sürece kümülatiftir. Örneğin, çok büyük bir çevrimiçi platform, sadece bu tür hizmetlere ilişkin özel yükümlülüklerle değil, aynı zamanda çevrimiçi platformlar, barındırma hizmetleri ve genel olarak aracılık hizmetlerine ilişkin yükümlülüklerle de uymak zorundadır.⁵⁴⁷

iii. Yatay düzenleme ilkesi, DSA’nın tüm sektörleri kapsayacak şekilde AB’de tüm hukuk sistemine yayılarak temel beklentiler oluşturmasını ifade etmektedir. Hizmet sağlayıcıların yükümlülüklerinin sektörel olarak ele alınması da bir alternatiftir; ancak sektörel düzenlemeler, günümüzün çevrimiçi yönetişiminin ortaya çıkardığı risklerin ve yasal süreç zorluklarının kapsamlı bir şekilde ele alınmasında yetersiz kalmaktadır.

⁵⁴⁵ “DSA”, resital 75, 76.

⁵⁴⁶ Avrupa Komisyonu, çok büyük çevrimiçi platformlar ve arama motorlarını belirlediği ilk kararında, aylık en az 45 milyon aktif kullanıcıya ulaşan on yedi platform ve iki arama motoru olmak üzere on dokuz çok büyük şirket belirlemiştir. Söz konusu karara göre bu şirketler şu şekilde kategorize edilebilir: Sosyal medya: Instagram, LinkedIn, Pinterest, Snapchat, TikTok, Twitter, Facebook, YouTube; Pazar yerleri: Alibaba AliExpress, Amazon Store, Booking.com, Google Shopping, Zalando; Uygulama mağazaları: Apple AppStore, Google Play; Diğer: Google Haritalar, Wikipedia; Arama motorları: Bing, Google Arama. “DSA: Very Large Online Platforms and Search Engines”, Text, **European Commission-European Commission**, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2413, (23.10.2024).

⁵⁴⁷ Wilman, “The Digital Services Act (DSA)-An Overview”, s. 3.

DSA’da, sektörel düzenleme yerine yatay düzenlemenin tercih edilmesinde dört temel sebep etkili olmuştur: E-Ticaret Direktifi doğası gereği yataydır ve revizyonu da yatay bir yaklaşım gerektirmektedir; (ii) belirlenen riskler ve sorunlar sistemiktir ve sektörler arası toplumsal kaygılara yol açar; (iii) sektöre özgü mevzuat tutarsızlıklara ve belirsizliklere yol açabilir; ve (iv) yalnızca yatay kurallar tüm hizmet türlerinin ve tüm yasadışı içerik kategorilerinin kapsanmasını sağlar.⁵⁴⁸ Yasa’nın bu niteliği, sektörel düzenlemelere engel olmamakla birlikte sektörel düzenlemelerin de yatay bir yaklaşımla DSA ile etkileşime girmelerini gerektirir. Bu yönüyle DSA, *dijital medeni haklar bildirgesi* olarak görülebilir. DSA’nın yataylığı, yalnızca kurallara uyan şirketler ve bireyler için faydalı olmakla kalmayıp aynı zamanda sistemde oyun oynanmasını da engellemektedir. Kuralların yataylığı yalnızca kurallara uyan şirketler ve bireyler için faydalı değil aynı zamanda “düzenleyici arbitraj” olarak ifade edilen farklı düzenlemelerin veya yasal çerçevelerin sunduğu farklı avantajlardan yararlanmak için bir anlaşmazlığı veya durumu kasıtlı olarak belirli bir düzenlemeye tabi tutma girişiminin de önüne geçmektedir.⁵⁴⁹

Yatay düzenleme, farklı menfaat gruplarının veya değerlerin çatıştığı konularda daha iyi bir denge sağlanması bakımından da avantaj sağlamaktadır. Çevrimiçi ortamda örneğin, çocukları korumak için yetişkinlerin özgürlüklerinin kısıtlanması ya da nefret söylemi ile mücadele için ifade özgürlüğünün sınırlandırılması gerekebilir. Yatay düzenleme, çevrimiçi ortamı kontrol edenlere her iki alanı da kapsayan yetkiler tanıyarak bu gibi durumlarda denge kurulmasına olanak tanımaktadır.⁵⁵⁰

iv. Sorumluluğun paylaşılması ilkesi, çevrimiçi ortamda sorumluluğun tek bir aktöre yığılması yerine kendini korumak isteyen herkesin kendisi için bir şeyler yapması, üzerine düşeni yerine getirmesi gerekliliğini ifade etmektedir. Nitekim E-Ticaret Direktifinde olduğu gibi DSA’da da “genel izleme yükümlülüğü yasağı”nın kabul edilmesi, tam da sorumluluğun paylaşılması prensibinin bir sonucudur. Bu kapsamda mağdurlar veya temsilcilerden, hizmet sağlayıcılara hukuka aykırı içerik hakkında

⁵⁴⁸ “Impact Assessment I”, s. 48.

⁵⁴⁹ Husovec, “Rising above Liability”, s. 912.

⁵⁵⁰ Ibid., s. 913.

bildirimde bulunmaları veya yetkililere başvurmaları; hizmet sağlayıcılardan da bildirimler veya yargı kararı ya da idari kararları üzerine harekete geçmeleri beklenir.

v. Kullanıcıların yetkilendirilmesi ilkesi, sorumluluğun paylaşılması ilkesinin de bir gereği olarak, çevrimiçi ortamda sorumluluk üstlenmesi veya risk paylaşması beklenen kullanıcıların söz konusu riskleri yönetebilmeleri için güçlendirilmeleri anlamına gelmektedir. DSA kapsamında kullanıcılar, kendi deneyimlerini şekillendirebilme, şirketlerin kararlarına itiraz edebilme, hatalı kararlar dolayısıyla tazminat talebinde bulunabilme, ebeveyn kontrol araçlarına sahip olma gibi yöntemlerle güçlendirilmişlerdir. Ancak, kullanıcılar ne kadar güçlendirilirse güçlendirilsin şirketlerin sorumluluktan tamamen kurtulmaları söz konusu değildir, kullanıcıların yetkilendirilmesinin esas amacı onları risk yönetim süreçlerine dahil etmektir.⁵⁵¹

vi. Ekosistem çözümleri ilkesi ise herkesin çözümün bir parçası olması gerektiğini vurgulamaktadır. DSA öncesinde çevrimiçi ortama ilişkin düzenlemelerde sağlayıcılar üzerine yoğunlaşarak ekosistemdeki diğer oyunculara yeterince dikkat edilmemesine karşın, DSA’da dijital ekosistem merkeze alınmaktadır. Bunu yaparak DSA, yasaların doğal olarak sadece öngörebileceği ve teşvik edebileceği ancak inşa edemeyeceği toplumsal yapılara büyük ölçüde güvenmektedir. Tehditleri analiz eden yerel kuruluşlar, içerik üreticilerine yardımcı olan tüketici grupları ve araştırmacı toplulukları gibi bu yapılar, DSA'nın araçlarına hayat veren yapılardır.⁵⁵²

b. Aracı Hizmet Sağlayıcılar İçin Sorumluluktan Muafiyet Rejimi

Dijital Hizmetler Yasası’nda, E-Ticaret Direktifinde bulunan sorumluluk rejimi büyük ölçüde korunarak, aracı hizmet sağlayıcılara (basit iletim, önbelleğe alma ve barındırma hizmetleri sağlayıcıları) hizmetin türüne göre değişen koşullar altında sorumluluk muafiyetleri tanınmıştır.

Buna göre aracı hizmet sağlayıcılar, basit iletim hizmetleri bakımından iletimi başlatmadıkları, iletimin alıcısını seçmedikleri ve iletimde yer alan bilgileri seçmedikleri

⁵⁵¹ Ibid., ss. 913, 914.

⁵⁵² Ibid., s. 919.

ya da deęiřtirmedikleri;⁵⁵³ önbellege alma hizmeti bakımından ise bilgileri deęiřtirmedikleri, bilgiye erişim koşullarına uydukları, bilgileri güncelledikleri, teknolojinin yasal kullanımına müdahale etmedikleri ve iletimin ilk kaynağındaki bilgilerin ağdan kaldırıldığı veya bunlara erişimin devre dıřı bırakıldığı ya da adli veya idari bir makamın bu tür bir kaldırma veya devre dıřı bırakma emri verdiği konusunda gerçek bilgi edinmesi üzerine depoladığı bilgileri kaldırmak veya bunlara erişimi devre dıřı bırakmak için hızlı bir şekilde hareket ettikleri sürece⁵⁵⁴ sorumluluktan muaftır.

Benzer şekilde barındırma hizmetleri bakımından da sağlayıcı, hukuka aykırı faaliyet veya bilgi hakkında gerçek bilgiye (*actual knowledge*) sahip olmaması ve tazminat talepleriyle ilgili olarak, hukuka aykırı faaliyet veya bilgilerin açık olduđu durum veya koşulların farkında (*awareness*) olmaması ya da (b) sağlayıcının, bu tür bir bilgiyi edinmesi veya durumun farkına varmasından sonra, bilgiyi kaldırmak veya bilgiye erişimi engellemek için süratle hareket etmesi koşuluyla, kullanıcı içeriklerinden sorumlu tutulamayacaktır.⁵⁵⁵

E- Ticaret Direktifi'nden DSA'ya aktarılan bu yaklaşım, hem kuralların sağladığı yasal kesinlik açısından hizmet sağlayıcıları hem de temel hakların korunması açısından kullanıcıları korumayı amaçlamaktadır. Sağlayıcıların, genel olarak ya da şüphe üzerine deęil de hukuka aykırı faaliyet ya da içerik hakkında bilgi veya farkındalık elde ettiğinde harekete geçmelerini gerektiren bu yaklaşımla sorumluluk riskleri sınırlandırılmaktadır. Çünkü ilk ihtimal, kullanıcıların temel hakları (özellikle ifade özgürlüğü ve kişisel verilerin korunması) üzerinde olumsuz etkilere yol açma ve hizmet sağlayıcılara aşırı yük getirme potansiyeli taşımaktadır.⁵⁵⁶ İkinci ihtimalin taşıdığı bazı kullanıcıların zarar görebilme potansiyeli ise hizmetler aracılığıyla paylaşılan yasadışı içerikten zarar gören kişilerin (hakaret mağdurları, telif hakkı sahipleri, istismara uğrayan çocukların temsilcileri, vb) temel haklarını koruyabilmeleri için çeşitli çözüm ve itiraz mekanizmalarına erişebilir kılınmalarıyla, özellikle de ihtiyati tedbir kararlarıyla -büyük ölçüde- bertaraf edilebilecektir.

⁵⁵³ "DSA", m. 4.

⁵⁵⁴ "DSA", m. 5.

⁵⁵⁵ "DSA", m. 6.

⁵⁵⁶ Wilman, "The Digital Services Act (DSA)-An Overview", s. 5.

Aracı hizmet sağlayıcıların sorumluluktan muafiyet şartlarına geçmeden önce söz konusu muafiyet şartlarının niteliğini anlamak önemlidir. Muafiyet şartlarının sağlanması, hizmet sağlayıcıların kullanıcılar tarafından oluşturulan içerikten sorumlu tutulmamalarının bir gereğidir; ancak bu şartların sağlanmaması aracı hizmet sağlayıcıların içerikten sorumlu tutulmaları için yeterli değildir. Aracı hizmet sağlayıcılarının hangi hallerde ne şekilde sorumlu tutulacakları Birlik ya da ulusal düzeyde ayrıca düzenlenmesi gereken bir konudur. Dolayısıyla, şartların sağlanmadığı ve bu nedenle sorumluluk muafiyetine dayanılmadığı durumlarda, sağlayıcının sorumlu olup olmadığı ilgili hukuk uyarınca ayrıca belirlenecektir.

DSA’da aracı hizmet sağlayıcıların sorumluluktan muafiyet rejimleri korunmakla birlikte, muafiyet rejimine ilişkin bazı yenilikler de söz konusudur. Bu yenilikler arasında, “pasif faaliyet” prensibinden “tarafsız faaliyet” prensibine geçiş ve “gerçek bilgi” ya da “farkındalık” sahibi olma kriterinin somutlaştırılması özellikle önem arz etmektedir.

E-Ticaret Direktifi’nde “pasif faaliyet”⁵⁵⁷ kriteri olarak yer verilen bu şart, DSA’da “tarafsız faaliyet” prensibi olarak değiştirilmiştir. Buna göre bir aracı hizmet sağlayıcı, hizmet alıcısı tarafından sağlanan bilgilerin sadece teknik ve otomatik olarak işlenmesi suretiyle tarafsız bir şekilde sunduğu takdirde DSA’da öngörülen sorumluluk muafiyetinden yararlanabilecek, bu bilgiler hakkında bilgi sahibi olmasını veya bu bilgiler üzerinde kontrol sahibi olmasını sağlayacak türden aktif bir rol oynadığı durumlarda muafiyet söz konusu olmayacaktır. Dolayısıyla, bilginin hizmet alıcısı tarafından değil de aracı hizmet sağlayıcısı tarafından sağlandığı -sağlayıcının editoryal sorumluluğu altında geliştirildiği durumlar da dahil- durumlarda da aracı hizmet sağlayıcı muafiyetten yararlanamayacaktır.⁵⁵⁸

DSA, sorumluluktan muafiyetinin kapsamı ve sınırları bakımından net bir ayrımı beraberinde getiren “tarafsız faaliyet” prensibine ilişkin net bir çerçeve sunmamaktadır. Nitekim Dijital Hizmetler Yasası Etki Değerlendirmesi Raporu’nda; etiketleme, indeksleme, arama işlevleri sağlama veya içerik seçme gibi kullanıcı dostu hizmet

⁵⁵⁷ “ECD”, resital 42.

⁵⁵⁸ “DSA”, resital 18.

sunulmasını sağlayan çok çeşitli otomatik faaliyetlerin de aktif rol üstlenme olarak kabul edilebileceği riskine dikkat çekilmiştir.⁵⁵⁹

DSA, bir aracının hangi durumlarda aktif rol üstlenmiş sayılacağına ilişkin belirsizliği tam anlamıyla gidermiş olmasa da bu konuda iki hususa açıklık getirmiştir.

Bunlardan ilki, 7. maddede güvence altına alınan “iyi niyetli ve özenli hareket etme”⁵⁶⁰ halidir. E-Ticaret Direktifi, hizmet sağlayıcıları bir yandan hukuka aykırı içerikle mücadele etme konusunda teşvik ederken, diğer yandan da onları hukuka aykırı içerikle mücadele ederken “aktif rol üstlenen” durumuna düşme riskiyle karşı karşıya bırakmaktaydı. Daha basit ifadeyle, hizmet sağlayıcıların hukuka aykırı içerik kapsamında iyilik yapması engellenmekte, sağlayıcıların cesaretleri kırılmaktaydı.⁵⁶¹

Hukuka aykırı içerikle mücadelede caydırıcı etki yaratabilecek bu paradoksal durum, hukuki belirsizliğin önlenmesi ve hizmet sağlayıcıların yasa dışı içeriğe karşı gönüllü olarak harekete geçmelerinin önünün kesilmemesi amacıyla DSA’da ortadan kaldırılmıştır.⁵⁶² Buna göre araçların iyi niyetle ve özenli bir şekilde; a) yasadışı içeriği tespit etmek, tanımlamak ve kaldırmak veya bunlara erişimi engellemek amacıyla kendi inisiyatifiyle gönüllü olarak araştırmalar yapması veya diğer önlemleri alması ya da b) Birlik hukuku ve Birlik hukukuna uygun ulusal hukukun gereklilikleri de dahil olmak üzere, DSA’da belirtilenler de dahil, Birlik hukukunun ve ulusal hukukun gerektirdiği önlemleri alması, onları aktif rol üstlenen durumuna düşürmeyecek ve dolayısıyla sorumluluk muafiyetlerinden yararlanmalarına engel teşkil etmeyecektir.

Bununla birlikte, bu gerekliliklerin platformlar tarafından içeriğin aşırı izlenmesini veya denetlenmesini teşvik etme riskini önlemede yeterli olup olmadığı belirsizdir. DSA’da yasadışı içeriği tespit etmek için alınabilecek önlemlere de açıklık getirilerek bu risk azaltılmaya çalışılmıştır. Buna göre sağlayıcılar iyi niyetle ve özenli bir şekilde hareket etmekle kalmamalı, aynı zamanda objektif, ayrımcı olmayan ve orantılı tedbirler almalıdır. Buna ek olarak, yasal içeriğin haksız yere kaldırılmasına karşı da

⁵⁵⁹ “Impact Assessment 2”, s. 159.

⁵⁶⁰ Doktrinde bu düzenleme, ihtiyacı olanlara yardım etmek için eylemde bulunan bir kişiyi anlatan “İyi Samiriyeli” meseline atıfla sık sık “Good Samaritan Clause” olarak anılmaktadır.

⁵⁶¹ Wilman, “The Digital Services Act (DSA)-An Overview”, s. 6.

⁵⁶² “DSA”, resital 26.

güvenceler sağlamalıdır. Bu faaliyetlerin otomatik araçlar kullanılarak yürütüldüğü durumlarda ise sağlayıcılardan “ilgili teknolojinin hata oranını mümkün olan azami ölçüde sınırlamak için yeterince güvenilir olmasını” sağlamak amacıyla “makul önlemler alması” beklenmektedir. Kullanımı gittikçe artan algoritmik modellerin hata oranını dikkate alan bu düzenleme olumlu olmakla birlikte, muğlak yapısı itibariyle farklı uygulamalara yol açabilecek niteliktedir.⁵⁶³ Son olarak, gönüllük esasının araçlar tarafından yükümlülükleri dolanmak amacıyla kullanıldığı durumlarda sağlayıcılar, iyi niyetli ve özenli hareket etmiş sayılamayacağından bu muafiyetlerden yararlanamayacaktır.⁵⁶⁴

İkinci olarak, aracı hizmet sağlayıcılarının hukuka aykırı faaliyetleri gerçekleştirmek üzere kullanıcılarla iş birliği yapmaları hali de DSA’da açıkça tarafsız olmayan faaliyet olarak nitelendirilerek muafiyet kapsamı dışında tutulmuştur. Örneğin *“sağlayıcının, amacının yasadışı faaliyetleri kolaylaştırmak olduğunu veya hizmetlerinin bu amaca uygun olduğunu açıkça belirtmek suretiyle, hizmetini yasadışı faaliyetleri kolaylaştırmak temel amacıyla sunduğu haller”*⁵⁶⁵ bu kapsamdadır.

DSA’daki bu somutlaştırma çabalarına rağmen aracı hizmet sağlayıcıların sorumluluklarının tarafsız faaliyet prensibi üzerinden belirlenmesine yönelik eleştiriler sürmektedir. Bu eleştirilerde özellikle, tarafsız olmak/aktif rol oynamak ayrımının iş modellerinin gereği olarak içerik moderasyonu yapan ve yapay zekâ destekli moderasyon sistemleriyle yönetilen günümüz çevrimiçi platformlara uygun olup olmadığı sorgulanmaktadır.⁵⁶⁶

DSA’nın aracı hizmet sağlayıcıların sorumluluktan muafiyetine ilişkin getirdiği bir başka yenilik de “gerçek bilgi” ya da “farkındalık” sahibi olma kriterine ilişkindir. E-Ticaret Direktifine göre hizmet sağlayıcıların sorumluluk muafiyetinin şartlarından biri de yasadışı faaliyetlere ilişkin gerçek bilgi ya da farkındalık elde ettiğinde onu kaldırmak ya da engellemek için harekete geçmeleri idi. Bu gerekliliğe rağmen Direktif’te, içeriği kaldırma yükümlülüğünü tetikleyen bir ihlal hakkında hangi noktada “gerçek bilgi (*actual*

⁵⁶³ Florence G’sell, “The Digital Services Act (DSA): A General Assessment”, **Content Regulation in the European Union–The Digital Services Act, Trier Studies on Digital Law 1**, 2023, s. 8.

⁵⁶⁴ “DSA”, resital 26.

⁵⁶⁵ “DSA”, resital 20.

⁵⁶⁶ Buiten, “The Digital Services Act”, 2021, ss. 14-15.

knowledge)" ya da "farkındalık (*awareness*)" edinmiş sayılacağı netleştirilmemişti. DSA'da bu hususa açıklık getirilerek bir aracının, "*basiretli bir tacirin yasa dışı olduğu iddia edilen içeriği makul bir şekilde tespit etmesine, değerlendirmesine ve uygun olduğu hallerde buna karşı harekete geçmesine olanak tanıyacak kadar kesin ve yeterli bir şekilde kanıtlanmış olması*" halinde, yani yeterince kesin ve yeterince kanıtlanmış (*sufficiently precise and adequately substantiated*) bildirimlerle⁵⁶⁷ gerçek bilgi ya da farkındalık elde edebileceği kabul edilmiştir.

Her halükârda, yasadışı içerik veya faaliyetlere ilişkin genel bir bilgi ya da farkındalık yeterli değildir; bilgi "spesifik (*specific*)" içerik veya faaliyetlerle ilgili olmalıdır.⁵⁶⁸ Hemen belirtmek gerekir ki sağlayıcının, hizmetine yüklenen bilgileri otomatik olarak indekslemesi, bir arama işlevine sahip olması veya hizmet alıcılarının profillerine veya tercihlerine dayanarak bilgi önermesi, platformda gerçekleştirilen yasa dışı faaliyetler veya platformda depolanan yasa dışı içerik hakkında "spesifik" bilgi sahibi olduğunun kabul edilmesi için yeterli değildir.⁵⁶⁹

Sorumluluktan muafiyet rejimi kapsamında, son olarak, DSA'da aracı hizmet sağlayıcılara yönelik kullanıcıların bilgilerini izleme ya da yasa dışı faaliyetlere işaret eden olgu ya da durumları aktif olarak araştırma yönünde genel yükümlülük getirme yasağı da korunmuştur. Yasağın aynı şekilde kabul edilmesinin gerekçesi, Dijital Hizmetler Yasası Etki Değerlendirme Raporu'nda şu şekilde açıklanmıştır:

"Bu hüküm, çevrimiçi dünyada temel haklar dengesinin temelini oluşturmaktadır. Üye Devletlerin, kullanıcıların ifade özgürlüğünü ve bilgi alma özgürlüğünü orantısız bir şekilde sınırlayabilecek veya hizmet sağlayıcılara aşırı yük getirebilecek ve dolayısıyla iş yapma özgürlüklerine gereksiz yere müdahale edebilecek genel yükümlülükler getirmemesini sağlar. Ayrıca, çevrimiçi gözetimi

⁵⁶⁷ Hizmet sağlayıcılar, bildirimlerin bu nitelikte sunulabilmesi için gerekli tedbirleri almalı ve bildirimlerin şu unsurları içermesini sağlamalıdır: (a) kişi veya kuruluşun söz konusu bilginin neden yasa dışı içerik olduğunu iddia ettiğine dair yeterince kanıtlanmış bir açıklama; (b) tam URL veya URL'ler gibi bu bilgilerin tam elektronik konumunun açık bir göstergesi ve gerektiğinde içeriğin türüne ve belirli barındırma hizmeti türüne uyarlanmış yasadışı içeriğin tanımlanmasını sağlayan ek bilgiler; (c) 2011/93/EU sayılı Direktifin 3 ila 7. Maddelerinde atıfta bulunulan suçlardan birini içerdiği düşünülen bilgiler hariç olmak üzere, bildirim gönderen kişi veya kuruluşun adı ve e-posta adresi; (d) Bildirimi gönderen kişi veya kuruluşun, bildirimde yer alan bilgi ve iddiaların doğru ve eksiksiz olduğuna dair iyi niyetli inancını teyit eden bir beyan. "DSA", m. 16.

⁵⁶⁸ Wilman, "The Digital Services Act (DSA)- An Overview", dipnot 25.

⁵⁶⁹ "DSA", resital 22.

sınırlandırır ve kişisel verilerin ve mahremiyetin korunmasında olumlu etkileri vardır. Böylesine orantısız bir yüke izin verilmesi, muhtemelen çok sayıda hatalı kaldırma işlemine ve kişisel veri ihlaline yol açarak kapsamlı davalara neden olacaktır. Genel izleme yükümlülüklerinde değişiklik yapılmasına yönelik seçenekler değerlendirilmiş ve daha sonra burada açıklanan haklar dengesi ile uyumadığı için göz ardı edilmiştir.”⁵⁷⁰

c. Özen Yükümlülükleri

Dijital Hizmetler Yasası’nda çevrimiçi hizmet sağlayıcılara yönelik düzenlemelerin ikinci boyutu, çevrimiçi hizmet sağlayıcıların yükümlülüklerine ilişkindir. Daha önce de ifade edildiği gibi bu yükümlülükler, sorumluluk muafiyetinin bir şartı olarak değil, ondan bağımsız olarak düzenlenmiştir.⁵⁷¹

Çevrimiçi hizmet sağlayıcıların bu yükümlülükleri, DSA’nın “Şeffaf ve Güvenli Bir Çevrimiçi Ortam İçin Özen Yükümlülükleri” başlıklı üçüncü bölümünde (Chapter III) oldukça ayrıntılı bir şekilde ele alınmıştır. Madde başlığında her ne kadar doğrudan insan hakları yükümlülükleri olarak ifade edilmese de temel haklara yönelik vurgulardan bu yükümlülüklerin insan hakları yükümlülükleri olduğu açıkça anlaşılmaktadır.

DSA, aracı hizmet sağlayıcılarının sorumlu ve özenli davranmasının güvenli, öngörülebilir ve güvenilir bir çevrimiçi ortamın sağlanması ve ifade ve bilgi edinme özgürlüğü, iş yapma özgürlüğü, ayrımcılık yasağı, tüketicinin korunması başta olmak üzere temel hakların korunması için gerekli olduğuna yönelik tespitle başlamaktadır.⁵⁷² Dolayısıyla, DSA’da hizmet sağlayıcılar için öngörülen yükümlülüklerle Avrupa Birliği Temel Haklar Şartında güvence altına alınan hak ve özgürlüklerin etkin bir şekilde korunması amaçlanmıştır.⁵⁷³

Öte yandan hizmet sağlayıcılar, özen yükümlülükleri kapsamında alacakları tedbirler sırasında da temel haklar konusunda dikkatli olmalıdır. DSA’da öngörülen tedbirleri tasarlarken, uygularken ve yürürlüğe koyarken, keyfi ve ayrımcı olmayan bir

⁵⁷⁰ “Impact Assessment 1”, s. 48.

⁵⁷¹ “DSA”, resital 41.

⁵⁷² “DSA”, resital 3.

⁵⁷³ “DSA”, resital 9, m. 1(1).

şekilde hareket etmeli ve Şart'ta yer alan temel haklar da dahil olmak üzere –özellikle de ifade özgürlüğü⁵⁷⁴- hizmet alıcılarının haklarını ve meşru menfaatlerini dikkate almalıdır.

Örneğin, tüm aracı hizmet sağlayıcılar, asgari olarak, Birleşmiş Milletler İş Dünyası ve İnsan Haklarına Dair Rehber İlkeler gibi insan haklarının korunmasına yönelik ilgili uluslararası standartları dikkate almalıdır. Çok büyük çevrimiçi platformların sağlayıcıları ise özellikle medya özgürlüğü ve çoğulculuk dahil olmak üzere ifade ve bilgi özgürlüğüne gereken özeni göstermelidir.⁵⁷⁵

DSA'da yorum yöntemi olarak da temel hakları esas alan bir yaklaşım benimsenmiştir. Çatışma konusu olabilecek haklar da dahil birçok temel hak ve özgürlüğün birlikte ele alınmasını gerektiren pek çok durumda DSA, ifade ve bilgi edinme özgürlüğü ile medya özgürlüğü ve çoğulculuğu da dâhil olmak üzere, temel haklara uygun olarak yorumlanmalı ve uygulanmalıdır. Bu da orantılılık ilkesine uygun olarak, ilgili haklar arasında adil bir denge kurulmasını gerektirmektedir.⁵⁷⁶

Çalışmanın bu bölümünde söz konusu yükümlülükler, nitelikleri dikkate alınarak a) içerik denetimine ilişkin yükümlülükler ve b) risk yönetimine ilişkin yükümlülükler şeklinde iki kategoride ele alınacaktır. Her iki yükümlülüğün kapsamı da hizmet sağlayıcının büyüklüğüne ve yerine getirdiği faaliyetin türüne göre şekillenmektedir.

aa) İçerik Yönetimine İlişkin Yükümlülükler

Aracı hizmet sağlayıcıların DSA kapsamındaki özen yükümlülüklerinin ilk ayağını, içerik yönetimine ilişkin yükümlülükler oluşturmaktadır. İçerik yönetimi DSA'da şu şekilde tanımlanmıştır:

“Otomatik olsun ya da olmasın, aracı hizmet sağlayıcıları tarafından üstlenilen, özellikle hizmet alıcıları tarafından sağlanan hukuka aykırı içeriği veya kendi hizmet koşullarına uygun olmayan bilgileri tespit etmeyi, tanımlamayı ve ele almayı amaçlayan, söz konusu yasa dışı içeriğin veya bu bilgilerin mevcudiyetini, görünürlüğünü ve erişilebilirliğini etkileyen, bunların alt sıralara düşürülmesi

⁵⁷⁴ “DSA”, resital 90.

⁵⁷⁵ “DSA”, resital 47.

⁵⁷⁶ “DSA”, resital 153.

(demotion), değersizleştirilmesi⁵⁷⁷ (demonetisation), erişiminin engellenmesi veya kaldırılması gibi alınan önlemler veya bir alıcının hesabının kalıcı olarak kapatılması veya askıya alınması gibi hizmet alıcılarının bu bilgileri sağlama kabiliyetini etkileyen faaliyetler”⁵⁷⁸

Bu tanımdan da anlaşıldığı üzere, içerik yönetiminin amacı hukuka aykırı ya da hizmet koşulları uyarınca uygunsuz içeriklerin tespit edilmesi, tanımlanması ve ele alınmasıdır. Bu kapsamda hizmet sağlayıcıların gerekli ve orantılı tedbirleri alması gerekmektedir. Hizmet sağlayıcılar tarafından alınabilecek tedbirler; içeriğin alt sıralara düşürülmesi, maddi olarak değersizleştirilmesi erişiminin engellenmesi veya kaldırılması gibi hukuka aykırı ya da uygunsuz içeriğin veya bilginin mevcudiyetini, görünürlüğünü ve erişilebilirliğini etkileyen, dolayısıyla doğrudan içeriğe yönelik olabileceği gibi; kullanıcı hesabının feshedilmesi veya askıya alınması gibi hizmet alıcılarının bu bilgileri sağlama kabiliyetini etkileyen, dolayısıyla içerik sahibine yönelik de olabilir.⁵⁷⁹ Bu tedbirlerin otomatik ya da otomatik olmayan şekillerde uygulanması DSA kapsamında bir fark yaratmamaktadır.

Aracı hizmet sağlayıcıların içerik yönetimine ilişkin yükümlülüklerini tetikleyen içerikler hukuka aykırı ya da hizmet koşullarınca uygunsuz içeriklerdir. Dolayısıyla, yükümlülüklerin neler olduğuna geçmeden önce, hukuka aykırı ve uygunsuz içeriklerin neler olduğu açıklığa kavuşturulmalıdır.

⁵⁷⁷ İnternet kullanıcılarının, YouTube veya Instagram (daha az olarak Facebook) gibi platformlarda para kazanabilecekleri iş modellerinden biri de platformun sunduğu programlar aracılığıyla para kazancı elde etmesidir. Bu programlar, reklam verenlerin içerik boyunca veya içeriğin üzerine çeşitli biçimlerde (örneğin, bannerlar, multimedya klipleri) reklam görüntülemelerine izin verir. İçerik yönetimi kapsamında platformlar (genellikle sosyal medya platformları), tek taraflı olarak, içerik oluşturucu/etkili kişinin gelir akışına erişimini engelleyebilir. Bu tedbir, kullanıcının yalnızca belirli videolar için potansiyel geliri kaldırıldığından, çok katı bir tedbir olarak değerlendirilmemektedir. İnternet kullanıcılarının, YouTube veya Instagram (daha az olarak Facebook) gibi platformlarda para kazanabilecekleri iş modellerinden biri de platformun sunduğu programlar aracılığıyla para kazancı elde etmesidir. Bu programlar, reklam verenlerin içerik boyunca veya içeriğin üzerine çeşitli biçimlerde (örneğin, bannerlar, multimedya klipleri) reklam görüntülemelerine izin verir. İçerik yönetimi kapsamında platformlar (genellikle sosyal medya platformları), tek taraflı olarak, içerik oluşturucu/etkili kişinin gelir akışına erişimini engelleyebilir. Bu tedbir, kullanıcının yalnızca belirli videolar için potansiyel geliri kaldırıldığından, çok katı bir tedbir olarak değerlendirilmemektedir. Nicolo Zingales, “Demonetization – Glossary of Platform Law and Policy Terms”, 17.12.2021, <https://platformglossary.info/demonetization/>.

⁵⁷⁸ “DSA”, m. 3(1)/t.

⁵⁷⁹ “DSA”, m. 3(1)/t.

DSA’da hukuka aykırı içerik kavramı, çevrimdışı ortamın genel dinamiklerini yansıtacak şekilde, yani yasadışı içerikle birlikte yasadışı ürün, hizmet ve faaliyetlerle ilgili bilgileri de kapsayacak şekilde ele alınmaktadır:

“Bu kavram özellikle, biçimi ne olursa olsun, yürürlükteki yasalar uyarınca ya yasadışı nefret söylemi veya terörist içerik ve yasadışı ayrımcı içerik gibi kendisi yasadışı olan ya da yasadışı faaliyetlerle ilgili olması nedeniyle yürürlükteki kuralların yasadışı kıldığı bilgileri ifade edecek şekilde anlaşılmalıdır. Örneğin, çocukların cinsel istismarını gösteren görüntülerin paylaşılması, özel görüntülerin rıza dışı paylaşımı, çevrimiçi takip, uygun olmayan veya sahte ürünlerin satışı, tüketiciyi koruma yasasını ihlal eden ürünlerin satışı veya hizmetlerin sağlanması, telif hakkıyla korunan materyallerin izinsiz kullanımı, konaklama hizmetlerinin yasa dışı olarak sunulması veya canlı hayvanların yasa dışı olarak satılması verilebilir.”⁵⁸⁰

Hizmet koşullarına uygun olmayan içerikler ise kısaca, aracı hizmet sağlayıcılar tarafından sunulan hizmete ilişkin olarak yasaklanan içerikler olarak tanımlanabilir. Hizmet sağlayıcılar, kullanıcı sözleşmeleriyle çevrimiçi içeriği, hukuka aykırı içeriğin ötesinde kısıtlamayı tercih edebilirler, ancak bu yöndeki tercihlerini keyfî ve ayrımcı olmayacak şekilde uygulamalıdır.

DSA uyarınca hem uygunsuz içerikler hem de hukuka aykırı içeriklerin belirlenmesi aracı hizmet sağlayıcılara bırakılmıştır. Bununla birlikte, söz konusu içeriklerin belirlenmesine ilişkin detaylı yükümlülükler yer verilerek hizmet sağlayıcıların yetkileri sınırlandırılmıştır. Dolayısıyla DSA, içerik denetiminin esasına ilişkin unsurların belirlenmesinde platformlara bir alan tanırken, bu alanı usul kurallarıyla çevrelemiştir. Şeffaflığı, belirliliği ve öngörülebilirliği sağlamaya yönelik bu sınırlandırmalar, bir bakıma çevrimiçi ortamda hukukun üstünlüğünün korunmasının da ön koşuludur.

⁵⁸⁰ “DSA”, resital 12.

Daha önce de belirtildiği gibi DSA’da hizmet sağlayıcıların yükümlülükleri onların büyüklükleri ve etkileri dikkate alınarak belirlendiğinden, içerik yönetimine ilişkin yükümlülükler de buna göre değişkenlik göstermektedir.

Piramidin en geniş katmanında yer alan “tüm aracı hizmet sağlayıcılar”, içerik yönetimine ilişkin kuralları hizmet koşullarında belirtmek ve içerik denetimine ilişkin düzenli şeffaflık raporları sunmakla yükümlüdür. Bu kapsamda içerik yönetimi amacıyla kullanılan tüm politika, prosedür, tedbir ve araçların yanı sıra, dahili şikâyet mekanizmalarına ilişkin bilgiler de dahil olmak üzere içerik yönetimine ilişkin kurallar ve bu kurallardaki değişikliklerin kullanıcılara önceden açıklanması gerekmektedir. Ayrıca, hizmet koşullarında belirlenen yaptırımların uygulanması sırasında ifade özgürlüğü, medya özgürlüğü ve çoğulculuğu başta olmak üzere tüm tarafların hakları ve meşru menfaatleri göz önünde bulundurularak özenli, objektif ve orantılı bir şekilde hareket edilmelidir. Dolayısıyla, hizmet koşullarının geriye dönük olarak değiştirilmesi ya da mevcut hizmet koşullarında dayanağı olmayan geçmişe etkili (*ex post facto*) yaptırımların uygulanması mümkün değildir.⁵⁸¹

Tüm aracı hizmet sağlayıcıların, içerik denetimine ilişkin temel yükümlülüklerinden biri de şeffaflık raporlama yükümlülüğüdür. Hizmet sağlayıcılar, yılda en az bir kere, makine tarafından okunabilir bir formatta ve kolay erişilebilir bir şekilde, ilgili dönem boyunca gerçekleştirdikleri her türlü içerik denetimine ilişkin açık ve kolay anlaşılır raporları kamuoyuyla paylaşmalıdır.⁵⁸²

Yükümlülükler piramidinde, zeminin bir üstündeki katmanda barındırma hizmeti sağlayıcıları için ek yükümlülükler yer almaktadır. Barındırma hizmeti sağlayıcılarının içerik yönetimine ilişkin ek yükümlülükleri kısmında, özellikle hukuka aykırı içeriğe ilişkin bildirim ve bildirim sonrası süreçler üzerinde durulmaktadır. Buna ilişkin en önemli hususlardan biri, E-Ticaret Direktifi’nde uyar-kaldır (*notice and takedown*) olarak nitelendirilen mekanizmanın, DSA’da bildirim ve eylem (*notice and action*) olarak karşılık bulmasıdır. Bu değişiklik, pratikte çok önemli bir değişiklik öngörmemekte, daha ziyade bu mekanizmalar için üye devletlerin farklı mekanizmaları arasında bir uyum

⁵⁸¹ Husovec, “Rising above Liability”, s. 901.

⁵⁸² “DSA”, m. 15.

sağlamaktadır.⁵⁸³ Bu kapsamda DSA’da söz konusu bildirim sistemlerinin kullanıcı dostu, erişilebilir ve yeterince kesin ve yeterince kanıtlanmış bildirimlerin sunulmasını kolaylaştıracak nitelikte olması gerektiği belirtilmiş, ayrıca bu nitelikteki bir bildirim sisteminin taşıması gereken unsurlar da detaylı olarak belirtilmiştir. Barındırma hizmeti sağlayıcıların, bu bildirimleri özenli, keyfi olmayan, tarafsız şekilde ve zamanında ele almaları gerekmektedir.⁵⁸⁴

Bildirim ve eylem mekanizması kapsamında barındırma hizmeti sağlayıcıları, söz konusu bildirimler üzerine içeriğin kaldırılması, içeriğe erişimin devre dışı bırakılması veya içeriğin öneminin azaltılması şeklinde içeriğin görünürlüğünün azaltılması; ödemelerin askıya alınması, feshedilmesi veya başka bir şekilde kısıtlanması; hizmet sunumunun tamamen veya kısmen askıya alınması veya sonlandırılması; hizmet alıcısının hesabının askıya alınması veya feshedilmesi şeklinde çok çeşitli eylemlerde bulunabilirler. Her halükârda karardan etkilenen hizmet alıcılarına; kararın kapsamı, süresi, karara dayanak olgular ve yasal mevzuat ve karara karşı başvurulabilecek itiraz mekanizmaları hakkında açık ve net bilgilerin yer aldığı bir gerekçe beyanı sunulmalıdır.⁵⁸⁵ Böyle bir gerekçe beyanı, ilgili kullanıcının kısıtlama getiren kararı anlaması ve isterse buna itiraz edebilmesi için önemlidir.

Barındırma hizmeti sağlayıcılara yönelik bir başka ek yükümlülük de bir suç işlendiğinde, işlenmekte olduğunda ya da işlenmesi ihtimalinin varlığı halinde bu durumu kolluk kuvvetleri veya adli makamlara bildirme ve bu kapsamda gerekli desteği sağlama yükümlülüğüdür.⁵⁸⁶ Bu yükümlülük geçmiş, devam eden veya muhtemel suçları kapsamı bakımından geniş olmakla birlikte, yalnızca bir veya daha fazla kişinin hayatına veya güvenliğine yönelik tehdit içeren suçlarla sınırlıdır. Barındırma hizmet sağlayıcıları, genel olarak herhangi bir suçla ilgili bildirim yükümlülüğü altında değildir.

Piramidin üçüncü katmanında, çevrimiçi platformlar için ek yükümlülükler yer almaktadır. İçerik yönetimi açısından çevrimiçi platformlar, diğerlerine ek olarak ayrıca şu yükümlülüklerle tabidir:

⁵⁸³ Buiten, “The Digital Services Act”, 2021, s. 18.

⁵⁸⁴ “DSA”, m. 16(6).

⁵⁸⁵ “DSA”, m. 17(1).

⁵⁸⁶ “DSA”, m. 18.

- Hizmet alıcıların haksız kararlara karşı itiraz edebilmelerini sağlamak,⁵⁸⁷
- Bildirim-eylem süreçleri bakımından güvenilir işaretçilerin bildirimlerini öncelikli ele almak,⁵⁸⁸
- DSA'nın 15. maddesinde, tüm araçlar için öngörülen şeffaflık raporlama yükümlülüğüne ek olarak, alternatif uyuşmazlık çözüm mekanizmaları ve çözüm mekanizmalarının kötüye kullanılmasına ilişkin bilgileri de raporlamak,⁵⁸⁹
- Çevrimiçi arayüz tasarımlarında aldatıcı veya manipülatif uygulamalardan kaçınmak,⁵⁹⁰
- Çevrimiçi reklamlar bakımından kullanıcılarına reklam şeffaflığı sağlamak, kullanıcıların içeriklerini ticari iletişim olarak etiketlemelerine izin vermek ve hassas kişisel verileri reklam hedeflemede kullanmamak,⁵⁹¹
- Öneri sistemi kullanmaları halinde, önerilerin nasıl çalıştığını kullanıcılara açıklayarak ve onlara önerileri etkileyen faktörleri kontrol etme imkânı vererek şeffaflık sağlamak⁵⁹² ve
- Çocuklar tarafından erişilebilen hizmetlerde, yüksek düzeyde gizlilik, emniyet ve güvenliğini sağlamak⁵⁹³

DSA'ya göre bildirim ve eylem mekanizmaları, hizmet alıcılar tarafından ya da güvenilir işaretçiler tarafından işletilebilir. Güvenilir işaretçiler, güvenilir bildirimler sunmak için gerekli uzmanlığa ve tarafsızlığa sahip olduklarını gösteren ve bu nedenle talepleri üzerine yetkili ulusal makamlar tarafından resmi olarak güvenilir işaretleyiciler olarak atanan kuruluşlardır. Çevrimiçi platformlar, yasa dışı veya uygunsuz içeriklerin daha etkin bir şekilde tespit edilip kaldırılmasının sağlanması için tasarlanmış bu sistem kapsamında aldıkları bildirimleri öncelikli olarak ele almakla yükümlüdür.⁵⁹⁴

Çevrimiçi platformlar için öngörülen ek yükümlülüklerde, bildirim-eylem mekanizmaları kapsamında alınan kararlara karşı başvurulabilecek itiraz mekanizmaları

⁵⁸⁷ "DSA", m. 20, 21.

⁵⁸⁸ "DSA", m. 22(1).

⁵⁸⁹ "DSA", m. 24.

⁵⁹⁰ "DSA", m. 25(1).

⁵⁹¹ "DSA", m. 26.

⁵⁹² "DSA", m. 27.

⁵⁹³ "DSA", m. 28.

⁵⁹⁴ "DSA", m. 22.

geniş yer tutmaktadır. Hizmet alıcılar, bu kararlara karşı dahili şikâyet mekanizmalarını (*internal complaint-handling system*) işletebilecekleri gibi, kendi üye devletlerinin ulusal makamına şikâyetle bulunabilirler ya da anlaşmazlığı alternatif uyuşmazlık çözüm (*out-of-court dispute settlement*) organına sunmayı da seçebilirler. Çevrimiçi platformlar, bir yandan dahili şikâyet mekanizması kurarak hizmet alıcıların kolay ve hızlı şekilde harekete geçebilmelerini sağlamak diğer yandan da alternatif uyuşmazlık yöntemlerini kullanabilmeleri konusunda hizmet alıcılara destek olmakla yükümlüdür. Buna göre söz konusu dahili itiraz sistemi kolay ve erişilebilir olmalı, kullanıcılara altı aydan az olmamak üzere itiraz süresi tanınmalı ve yeterince kesin ve yeterince kanıtlanmış şikâyetlerin sunulması mümkün kılınmalıdır. Çevrimiçi platformlar ayrıca, hizmet alıcılarının alternatif uyuşmazlık çözümüne erişim imkanına ilişkin bilgilerin çevrimiçi arayüzlerinde kolayca erişilebilir, açık ve kullanıcı dostu olmalarını sağlamakla yükümlüdür.⁵⁹⁵

Çevrimiçi platformlar ayrıca, söz konusu bildirim ve şikâyet mekanizmalarının kötüye kullanılmasına karşı da önlem almakla yükümlüdür. DSA’da hizmet alıcılar tarafından “sıklıkla, açıkça yasadışı içerik sağlanması” ve “bildirim ve eylem mekanizmaları ile dahili şikâyet sistemleri kapsamında sıklıkla, açıkça asılsız bildirim ve şikâyetle bulunulması” iki farklı kötüye kullanım şekli olarak kabul edilmiştir. Her iki durumda da platformların, kötüye kullanımda bulunanların taleplerini, önceden bildirimde bulunarak askıya alması gerekmektedir. Bu, DSA’nın sağlayıcıların yasadışı içerikle ilgili olarak proaktif bir şekilde hareket etmesini gerektirdiği birkaç durumdan biridir, ancak bu durumda “yaptırım” yasadışı içerikten ziyade kullanıcıyı hedef almaktadır.⁵⁹⁶

Bu tür askıya alma kararları, ifade ve bilgi edinme özgürlüğü üzerinde olumsuz etki doğurabilecek potansiyeldedir. Bu nedenle çevrimiçi platformlar, kendi hüküm ve koşullarında kötüye kullanıma ilişkin politikalarını açık ve ayrıntılı bir şekilde belirtmeli ve kötüye kullanım teşkil eden davranışlar ile bu davranışların tespit edilmesi halinde uygulanacak askıya alma yaptırımına ilişkin açıklamalarda bulunmalıdır.⁵⁹⁷ Ayrıca, bir talebin kötüye kullanım teşkil edip etmediğine karar verirken vaka bazında, özenli ve

⁵⁹⁵ “DSA”, m. 20.

⁵⁹⁶ Wilman, “The Digital Services Act (DSA)-An Overview”, s. 9.

⁵⁹⁷ “DSA”, m. 23(4).

tarafsız bir şekilde inceleme yapılması gerekmektedir.⁵⁹⁸ Böylece, çevrimiçi platformlara hukuka aykırı içerikle mücadele etme yükümlülüğü yüklenirken hizmet alıcıların ifade ve bilgi alma özgürlükleri de güvencesiz bırakılmamıştır.

Çevrimiçi platformlar, şeffaflık raporlama bakımından da ek yükümlülükler altındadır. Bu kapsamda, çevrimiçi platformların raporlarında DSA'nın 15. maddesinde tüm aracı hizmet sağlayıcılar için öngörülenlere ek olarak; a) 21. maddede belirtilen alternatif uyuşmazlık çözüm yollarına giden uyuşmazlık sayısı, uyuşmazlık çözümünün sonuçları, uyuşmazlık çözüm prosedürlerinin tamamlanması için gereken ortalama süre ve uyuşmazlık sonucunun uygulanma oranı ve b) 23. madde uyarınca açıkça yasadışı içerik sağlanması, açıkça asılsız bildirimler sunulması ve açıkça asılsız şikayetler sunulması nedeniyle uygulanan askıya alma sayılarına da yer verilmelidir.⁵⁹⁹

DSA'da yer alan bu detaylı düzenlemelerle piyasa tarafından tek taraflı olarak belirlenerek kullanıcılara dayatılan kuralların yerini, hizmet alanlara güven veren öngörülebilir ve şeffaf süreçler almıştır. Bu süreçler, çevrimiçi hak ve özgürlüklere yönelik tehditleri bütünüyle ortadan kaldırmamakla birlikte, içerik denetiminin daha özenli sürdürülmesi konusunda önemli bir güvence teşkil etmenin yanında, denetim süreçlerinin iyileştirilmesi konusunda şirketler üzerinde bir baskı unsuru da teşkil etmektedir.⁶⁰⁰

bb) Risk Yönetimine İlişkin Yükümlülükler

Dijital dönüşüm ve dijital hizmetlerin artan kullanımı, bu ekosistemde hem kullanıcılar hem de toplum için yasadışı faaliyetlerin yayılmasından temel hakların ihlaline varan yeni riskler ortaya çıkarmıştır. Günümüzde çevrimiçi platformlar; tasarım tercihleri, çevrimiçi kullanıcı güvenliği, kamuoyu ve söylemin şekillendirilmesi ve çevrimiçi ticaret üzerinde güçlü bir etkiye sahip olduklarından, etkili düzenleme ve

⁵⁹⁸ “DSA”, m. 23(3).

⁵⁹⁹ “DSA”, m. 24.

⁶⁰⁰ DSA'nın usul kuralları, çeşitli yazarlar tarafından, "batan bir gemiden su almak için çay kaşığı kullanmaya" benzediği için genel sorunları çözmeyen gereksiz bir "süreç tiyatrosu" olarak eleştirmektedir. Bu eleştiriler için bkz. DSA'nın usul kuralları, çeşitli yazarlar tarafından, "batan bir gemiden su almak için çay kaşığı kullanmaya" benzediği için genel sorunları çözmeyen gereksiz bir "süreç tiyatrosu" olarak eleştirmektedir. Bu eleştiriler için bkz. Evelyn Douek, “Content Moderation as Systems Thinking”, *Harvard Law Review*, C. 136, S. 2, 2022.

yaptırımların yokluğunda riskleri ve neden oldukları toplumsal ve ekonomik zararı etkili bir şekilde azaltmadan oyunun kurallarını belirlemektedir.⁶⁰¹

Çevrimiçi ortamın platformların ellerine bırakıldığı senaryo, özellikle hukuka aykırı faaliyetlerin yayılmasına ilişkin ciddi riskler içermektedir. Bunlar, çocuk cinsel istismarı materyalleri, terörist içerikler, yasa dışı nefret söylemi ve bireyleri hedef alan yasa dışı reklamlar, fikri mülkiyet haklarını ihlal eden içerikler vb. gibi yasa dışı içeriklerin yayılmasından ya da tehlikeli mallar, güvenli olmayan oyuncaklar, yasadışı ilaçlar, taklitler, dolandırıcılıklar gibi tüketicilerin korumasını ihlal eden uygulamalardan kaynaklanabilir. Bu riskler kendi başına insan haklarının korunması bakımından kaygı verici olmaya yetse de çevrimiçi ortamın riskleri, hukuka aykırı faaliyetlerin yayılmasının çok daha ötesindedir.

Bu riskler platformların sistemlerinin, çoğu zaman koordineli saldırılar ve gerçek olmayan davranışlar yoluyla, belirli mesajların veya davranışların çevrimiçi olarak güçlendirilmesi için manipüle edilmesiyle de bağlantılı ortaya çıkabilir.⁶⁰² Bu tür davranışlar, örneğin, çocuklar başta olmak üzere kullanıcıların şiddete veya kendine zarar vermeye teşvik edilmesine, komplo teorilerine, temel sağlık konuları ya da siyasi süreçlerle ilgili dezenformasyon için platform sistemlerinin kasıtlı olarak kötüye kullanılmasına yol açabilir. Algoritmik tavsiyeler veya “karanlık tasarımlar (*dark patterns*)” yoluyla pazaryerlerindeki tüketici tercihleri ya da satıcıların tüketicilere ulaşma kabiliyetleri de değiştirilebilir.⁶⁰³

Gittikçe artan bu riskler, DSA’da risk yönetimine ilişkin kapsamlı yükümlülükleri beraberinde getirmiştir. Buna göre çevrimiçi platformlar, kalabalıkları bir araya getirmenin yarattığı riskleri analiz etmek ve gerekirse bu risklere müdahale etmekle yükümlüdür. Yükümlülüklerin kapsamı ise yine büyük gücün beraberinde büyük sorumluluklar getireceği prensibi doğrultusunda, çevrimiçi platformların büyüklüklerine göre⁶⁰⁴ değişmektedir. Mikro ve küçük nitelikteki platformlar, risk yönetimi

⁶⁰¹ “Impact Assessment 1”, s. 12.

⁶⁰² “Impact Assessment 1”, s. 12.

⁶⁰³ “Impact Assessment 2”, s. 16.

⁶⁰⁴ Çok büyük platformlar ve çok büyük arama motorları ise DSA’nın 33. maddesinde, 45 milyondan fazla aktif kullanıcıya hizmet veren çevrimiçi platformlar veya arama motorları olarak tanımlanmış ve Komisyon’un bu şirketleri belirleyerek isimlerini yayımlayacağı belirtilmiştir. Commission Recommendation of 6 May 2003 Concerning the Definition of Micro, Small and Medium-Sized Enterprises

sorumluluğuna sahip değilken orta ve büyük ölçekli platformlar içerik yönetimiyle bağlantılı sınırlı yükümlülüklerle tabidir. Çok büyük platformlar ve çok büyük arama motorları ise kapsam ve etki bakımından daha küçük platformların neden olduklarından farklı toplumsal risklere neden olabildiğinden⁶⁰⁵, genel risk yönetimi kapsamında daha geniş yükümlülük altındadır.⁶⁰⁶

Orta ve büyük ölçekli çevrimiçi platformlar, ürün tasarımlarının küçükleri nasıl koruduğunu ve karanlık modeller olarak da bilinen manipülatif ve agresif uygulamalara karşı nasıl koruduklarını düşünmelidir. Çok büyük çevrimiçi platformlar ve arama motorlarının ise bunlara ek olarak, hizmetlerinin tasarımından, işleyişinden ve kullanımından kaynaklanan sistemik riskleri değerlendirmeleri⁶⁰⁷ ve belirledikleri sistemik riskleri temel haklara saygılı bir şekilde ve özenle azaltmak için gerekli önlemleri almaları gerekmektedir.⁶⁰⁸

Bu doğrultuda, VLOP ve VLOSE'lar hizmetlerinin ve ilgili sistemlerinin tasarımından veya işleyişinden ya da hizmetlerinin kullanımından kaynaklanan her türlü sistemik riski özenle tespit ve analiz etmek, ardından bu risklere yönelik gerekli tedbirleri almakla yükümlü kılınmıştır. Bu tespit ve analizlerde, platformların yasa dışı içeriğin yayılması; insan onuru, özel hayata saygı, kişisel verilerin korunması, ifade ve bilgi özgürlüğü, ayrımcılık yasağı, çocuk ve tüketici hakları gibi temel haklara olumsuz etkisi ve kamu sağlığı, küçükler, sivil söylem, seçim süreçleri ve kamu güvenliği üzerinde olumsuz etkilere neden olma potansiyeli gibi hususlar değerlendirilmelidir. Platformların yükümlülükleri risk değerlendirmesiyle bitmemekte, ayrıca makul, iyi niyet ve etkili risk azaltma tedbirleriyle söz konusu tedbirlerin temel haklar üzerindeki etkilerini de dikkate alarak bu riskleri hafifletmeleri gerekmektedir.⁶⁰⁹

(Text with EEA Relevance) (Notified under Document Number C(2003) 1422), European Commission, 06.05.2003, <http://data.europa.eu/eli/reco/2003/361/oj/eng>, (5.10.2024). Çok büyük platformlar ve çok büyük arama motorları ise DSA'nın 33. maddesinde, 45 milyondan fazla aktif kullanıcıya hizmet veren çevrimiçi platformlar veya arama motorları olarak tanımlanmış ve Komisyon'un bu şirketleri belirleyerek isimlerini yayımlayacağı belirtilmiştir.

⁶⁰⁵ "DSA", resital 76.

⁶⁰⁶ Husovec, "Rising above Liability", ss. 899-900.

⁶⁰⁷ "DSA", resital 76.

⁶⁰⁸ "DSA", resital 86.

⁶⁰⁹ Platformların alabileceği olası tedbirler, DSA'da örnekleme yoluyla sayılmıştır. Buna göre bu tedbirler şunları içerebilir: "(a) Çevrimiçi arayüzleri de dahil olmak üzere hizmetlerinin tasarımını, özelliklerini veya işleyişini uyarlamak; (b) Hizmet şartlarını ve uygulanmasını uyarlamak; (c) Belirli yasa dışı içerik

Birlik'te veya Birlik'in önemli bir bölümünde kamu güvenliğine veya kamu sağlığına yönelik ciddi bir tehdide yol açan olağanüstü koşulların ortaya çıkması halinde, Komisyon tarafından VLOP ve VLOSE'lara yönelik bazı ek yükümlülükler de getirebilir. DSA'da kriz müdahale mekanizması olarak ifade edilen bu yükümlülük kapsamında platformlardan, hizmetlerinin söz konusu tehdide etkilerini değerlendirmeleri; varsa, bu katkıyı ortadan kaldırmak ya da sınırlandırmak için tedbir almaları; mevcut etkiler ve alınan tedbirler konusunda Komisyon'a rapor sunmaları talep edilebilecektir.⁶¹⁰

VLOP ve VLOSE'lar kendilerini, en az yılda bir kez bağımsız denetime tabi tutmakla yükümlüdür. Bu denetim kapsamında, platformların özen yükümlülükleri ve davranış kurallarına uygunlukları değerlendirilmeli ve denetimleri gerçekleştiren kuruluşların her bir denetim için ayrı bir denetim raporu oluşturması sağlanmalıdır. DSA'ya göre söz konusu denetim sonucunda olumsuz bir durumun ortaya çıkması ihtimalinde ise platformların bu olumsuzluğu ortadan kaldırmaya yönelik tedbir alma yükümlülükleri başlamaktadır. Buna göre platformlar ya denetim raporu uyarınca gerekli tedbirleri uygulamalı ya da bunu yapmama nedenlerini gerekçelendirerek aldıkları alternatif önlemleri belirtmelidir.⁶¹¹

türleriyle ilgili bildirimlerin işleme alınma hız ve kalitesini ve uygun olduğu durumlarda, özellikle yasa dışı nefret söylemi veya siber şiddetle ilgili olarak, bildirilen içeriğin hızlı bir şekilde kaldırılması veya içeriğe erişimin engellenmesi de dahil olmak üzere içerik denetleme süreçlerini uyarlamak ve ilgili karar alma süreçlerinin ve içerik denetleme için tahsis edilen kaynakları uyarlamak; (d) Önerileri de içeren algoritmik sistemlerini test etmek ve uyarlamak; (e) Reklam sistemlerini uyarlamak ve sağladıkları hizmet ile bağlantılı olarak reklamların sunumunu sınırlandırmayı veya ayarlamayı hedefleyen önlemler almak; (f) Özellikle sistemik riskin tespiti ile ilgili olarak faaliyetlerinin herhangi birinin iç süreçlerini, kaynaklarını, testlerini, dokümantasyonunu veya denetimini güçlendirmek; (g) Madde 22 uyarınca güvenilir işaretçilerle işbirliğini başlatmak veya ayarlamak ve Madde 21 uyarınca mahkeme dışı uyuşmazlık çözüm organlarının kararlarının uygulamak; (h) Sırasıyla 45. ve 48. maddelerde atıfta bulunulan davranış kuralları ve kriz protokolleri aracılığıyla diğer çevrimiçi platform sağlayıcıları veya çevrimiçi arama motorları ile işbirliğini başlatmak veya ayarlamak; (i) Hizmet alıcılarına daha fazla bilgi vermek için farkındalık artırıcı önlemler almak ve çevrimiçi arayüzlerini uyarlamak; (j) Yaş doğrulama ve ebeveyn kontrol araçları, reşit olmayanların istismarı bildirmelerine veya uygun şekilde destek almalarına yardımcı olmayı amaçlayan araçlar dahil olmak üzere çocuk haklarını korumaya yönelik hedefli tedbirler almak; (k) Mevcut kişilere, nesnelere, yerlere veya diğer varlıklara veya olaylara kayda değer ölçüde benzeyen ve bir kişiye gerçek veya doğru gibi görünen oluşturulmuş veya manipüle edilmiş bir görüntü, ses veya video oluşturup oluşturmadığına bakılmaksızın bir bilgi ögesinin çevrimiçi arayüzlerinde sunulduğunda belirgin işaretlerle ayırt edilebilir olmasını sağlamak ve ayrıca hizmet alıcılarının bu tür bilgileri belirtmelerini sağlayan kullanımı kolay bir işlevsellik sağlamak.” “DSA”, m. 35(1).

⁶¹⁰ “DSA”, m. 36(1).

⁶¹¹ “DSA”, m. 37.

VLOP ve VLOSE’lar, öneri sistemleri⁶¹² ve çevrimiçi reklamların kullanımına ilişkin olarak online çevrimiçi platformlar için öngörülenlere ek bazı şeffaflık yükümlülüklerine tabidir. Bu ek şeffaflık yükümlülükleri, öneri sistemleri bakımından, profil oluşturmaya dayanmayan en az bir seçenek sunulmasını; çevrimiçi reklamlar bakımından da reklamlar, reklam verenler ve hedef kitle hakkındaki bilgilerin -kişisel veri içermeyecek şekilde- toplanarak kamuoyunun erişimine açık hale getirilmesini gerektirmektedir.

VLOP ve VLOSE’ların, şeffaflık raporlama yükümlülüğü kapsamında diğer hizmet sağlayıcılara kıyasla daha sık ve daha kapsamlı rapor yayınlamaları gerekmektedir.⁶¹³ DSA uyarınca VLOP ve VLOSE’lar, ilgili otoritelerin DSA’da öngörülen yükümlülüklerin izlenmesi ve değerlendirilmesi için gerekli olan verilere erişimini sağlamakla da yükümlüdür.

B. Belirli Konulara Özgülenmiş Düzenlemeler

E-Ticaret Direktifi, dijital hizmetler bakımından temel ilkelerin ele alındığı yatay bir yasal çerçeve sağladığından, bu Direktif’te tüm yasadışı faaliyet türleri ayrı ayrı ele alınmamıştır. E-Ticaret Direktifi sonrasında çevrimiçi araçlara yönelik mevzuat, belirli hukuka aykırı faaliyet türlerini esas alan yatay ve dikey düzenlemelerle gelişmiştir. Dikey düzenlemelerde söz konusu hukuka aykırı faaliyet türlerine özgü özel sorumluluk rejimleri öngörülmüştür.⁶¹⁴ Bu özel sorumluluk rejimleri, çeşitli menfaatler arasında “adil bir denge sağlanması” amacı bakımından daha elverişli olduğundan, günümüz internetinin gerçekleriyle daha uyumludur.⁶¹⁵

Belirli konuların özel olarak ele alındığı bu düzenlemelerde, hukuka aykırı tüm içerik türlerine yönelik yükümlülükler yer verilmediği gibi hesap verilebilirlik ve şeffaflık ya da bunların mekanizmaları hedef sektörle sınırlı kalmaktadır. Dolayısıyla bu düzenlemelerin kapsamı, hem daha özel içerik türlerine (örneğin telif hakkı ihlalleri,

⁶¹² Öneri sistemleri, kullanıcıların ilgi alanlarını ve davranışlarını analiz ederek, onlara ürün, hizmet, içerik veya bilgi önerisinde bulunan sistemleri ifade etmektedir. Bu sistemler, kullanıcıların geçmişteki aramalarına, satın aldıkları ürünlere, izledikleri videolara veya beğendikleri gönderilere bakarak, onların ilgisini çekebilecek yeni ürünler veya içerikler önerir.

⁶¹³ “DSA”, m. 42(1,2).

⁶¹⁴ “Impact Assessment 2”, s. 86.

⁶¹⁵ Christina Angelopoulos, Stijn Smet, “Notice-and-Fair-Balance: How to Reach a Compromise between Fundamental Rights in European Intermediary Liability”, *Journal of Media Law*, C. 8, S. 266, 2016.

terörist içerikler, çocukların cinsel istismarı veya yasadışı nefret söylemi) hem de söz konusu içerikler bakımından yalnızca belli hizmet türlerine odaklanması açısından sınırlıdır.⁶¹⁶

1. Genel Veri Koruma Tüzüğü

İnternet teknolojilerindeki gelişmelerin önemli etkiler ortaya çıkardığı alanlardan biri de kişisel verilerdir. Günümüzde kişiler, kişisel verilerini giderek daha fazla kamusal ve küresel erişime sunmaktadır. Öte yandan teknolojik gelişmeler, özel şirketlerin faaliyetlerini sürdürmek için kişisel verileri benzeri görülmemiş bir ölçekte kullanmalarına ve aktarmalarına imkân tanımıştır. Teknolojinin değişen doğası karşısında, Genel Veri Koruma Tüzüğü ile kişisel verilerin korunmasına ilişkin olarak yeni haklar geliştirilmiş ve internet şirketlerine kapsamlı yükümlülükler yüklenmiştir. Tüzüğün, kişisel verilerin serbestçe akışını sağlamak ve özel hayatın gizliliğini korumak başta olmak üzere gerçek kişilerin temel hak ve özgürlüklerinin korunması şeklinde iki temel amacı bulunmaktadır.

Tüzükte kişisel verilerin işlenmesinde yer alan iki farklı aktöre atıfta bulunmaktadır: veri sorumluları ve veri işleyenler. Bu ayrım, farklı aktörlerin farklılaşan yükümlülüklerinin belirlenmesinde önemli bir rol oynamaktadır. Veri sorumluları, kişisel verilerin kullanımına ilişkin kararları alan taraftır. Verileri "tek başına veya başkalarıyla birlikte" muhafaza eder ve ne şekilde kullanılacağına karar verirler.⁶¹⁷ Bu nedenle, daha kapsamlı ve sıkı kurallara uymak zorundadırlar. Veri işleyenler ise kişisel verileri muhafaza etmekle birlikte verilerin kullanımı konusunda veri sorumlusunun talimatlarını takip ederler.

Bu bağlamda, yalnızca kullanıcılar tarafından ağ üzerinden gönderilen bilgilerin iletimiyle sınırlı kaldıkları sürece internet servis sağlayıcıları genellikle Direktif kapsamının dışında kalmaktadır. Ancak barındırma hizmeti sağlayıcılar, sosyal medya platformları ve arama motorları için durum daha karmaşıktır. Bu hizmet sağlayıcılar,

⁶¹⁶ "Impact Assessment 1", s. 30.

⁶¹⁷ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), m. 4(7), <https://eur-lex.europa.eu/eli/reg/2016/679/oj>, (24.10.2024).

ağlarında üçüncü şahıslar tarafından oluşturulan verileri kendi amaçları doğrultusunda işledikleri zaman söz konusu veri işleme faaliyeti için veri sorumlusu olarak kabul edilmektedir. Buna karşın, kullanıcılar tarafından yayınlanan verilerle ilgili olarak, “işleme amaçlarını ve araçlarını belirleyip belirlemediklerine” ve dolayısıyla kontrolör veya işlemci olarak nitelendirilmeleri gerekip gerekmediğine karar vermek için somut duruma göre bir değerlendirme yapılması gerekmektedir.⁶¹⁸

Veri sorumlusu niteliğindeki çevrimiçi hizmet sağlayıcılar; işlemenin adil ve hukuka uygun olmasını, verilerin şeffaf bir şekilde ve meşru amaçlarla toplanmasını ve başka amaçlarla işlenmemesini, bu amaçlarla ilgili olarak yeterli, ilgili ve aşırı olmamasını, doğru olmasını ve güncel tutulmasını sağlamaktan sorumludurlar.⁶¹⁹ Çocukların verileri söz konusu olduğunda işleme faaliyetleri velayet sorumluluğu bulunan kişinin rızasını gerektirdiğinden, veri sorumlusunun mevcut teknolojiyi dikkate alarak çocuk üzerinde velayet sorumluluğu bulunan kişi tarafından rıza veya izin verildiğini doğrulamak için makul çaba sarf etmesi gerekmektedir.⁶²⁰

Tüzük kapsamında veri sorumlusu, verileri toplanan bireylere, verilerinin toplanması ve işlenmesine ilişkin gerekli bilgileri açık, şeffaf, anlaşılabilir ve erişilebilir bir biçimde sağlamak zorundadır.⁶²¹ Daha da önemlisi, veri sahibinin talebi üzerine ve gerekli şartların sağlanması halinde veri sorumlusunun, ilgili verilerin düzeltilmesini ya da silinmesini sağlaması gerekmektedir. Bununla birlikte Tüzükte ifade özgürlüğü ile ilgili belli durumlara yer verilerek bu durumlarda kişisel verilerin silinmesine ilişkin yükümlülüklerin gerekli olduğu ölçüde uygulanmayabileceği belirtilmiştir.⁶²²

Tüzük tarafından ele alınan bir diğer önemli konu da sınır ötesi veri akışları ile ilgilidir. Tüzüğün 25. maddesi uyarınca AB içerisinde toplanan verilerin, ancak üçüncü ülkenin verilerin yeterli düzeyde korunmasını sağlaması halinde bu tür bir aktarıma izin verilmektedir.⁶²³

⁶¹⁸ Louise Timmermans, “The Role of Internet Intermediaries In the Protection of Freedom of Expression and Personal Data: Human Rights in a Digital Age”, 2017, ss. 32, 33, <https://doi.org/20.500.11825/594>.

⁶¹⁹ “General Data Protection Regulation”, m. 5(1).

⁶²⁰ “General Data Protection Regulation”, m. 8.

⁶²¹ “General Data Protection Regulation”, m. 13, 14.

⁶²² “General Data Protection Regulation”, m. 18.

⁶²³ “General Data Protection Regulation”, m. 44.

Veri sorumluları, veri sahiplerinin verilere erişim ve verilerin işlenmesine itiraz etme haklarının daha etkili kullanılmasını sağlamakla da yükümlüdür. Bu yükümlülükler arasında; işleme faaliyetlerinin kayıtlarının tutulması⁶²⁴, işleme güvenliğini sağlamak üzere gerekli tedbirlerin alınması⁶²⁵ veya öngörülen veri işlemenin kişisel verilerin korunması üzerindeki etkisinin değerlendirilmesinin üstlenilmesi⁶²⁶ gibi yükümlülükler yer almaktadır.

Genel Veri Koruma Tüzüğü ile kabul edilen bu yükümlülükler göz önünde bulundurulduğunda, yükümlülüklerinin kullanıcıların ifadelerinden daha ziyade kullanıcı davranışlarına ilişkin depolanan verilerin şirketler tarafından toplanması ve kullanmasıyla ilgili olduğu anlaşılmaktadır. Bu kapsamda şirketler tarafından verilerin kaydedilme ve saklanma biçimlerine ilişkin mühendislik çalışmaları yapılması, kullanıcı arayüzü tasarımlarının düzenlenmesi, veri koruma etki değerlendirmeleri hazırlanması gibi çok çeşitli adımların atılmasını gerektirebilecektir.⁶²⁷

2. Dijital Tek Pazarda Telif Hakları ve Bağlantılı Haklara İlişkin Direktif

Son yıllarda çevrimiçi içerik pazarının işleyişinde önemli değişiklikler yaşanmıştır. Çevrimiçi içerik paylaşım hizmetleri, kullanıcıları tarafından yüklenen içeriğe erişim sağlamaları dolayısıyla, çevrimiçi içeriğe erişimin ana kaynağı haline gelmiştir. Çevrimiçi platformlar, kültürel ve yaratıcı eserlere daha geniş erişim sağlanmasının ve bu sektörlerde yeni iş modelleri geliştirilmesinin önemli bir yoludur, ancak telif hakkı korumalı içeriklerin kullanıcılar tarafından izinsiz yüklenmesine ve yayılmasına yol açabildiğinden ifade özgürlüğü ve telif hakları arasında bir gerilime neden olmaktadır.

Belirli bilgi toplumu hizmetleri, normal kullanımlarının bir parçası olarak, kullanıcıları tarafından yüklenen telif hakkıyla korunan içeriğe veya diğer konulara kamunun erişimini sağlamak üzere tasarlanmıştır. 2019/790 sayılı Dijital Tek Pazarda

⁶²⁴ “General Data Protection Regulation”, m. 30.

⁶²⁵ “General Data Protection Regulation”, m. 32.

⁶²⁶ “General Data Protection Regulation”, m. 35.

⁶²⁷ Daphne Keller, “The Right Tools: Europe’s Intermediary Liability Laws and the EU 2016 General Data Protection Regulation” **European Private Law eJournal**, 2017, s. 318.

Telif Hakları ve Bağlantılı Haklara İlişkin Direktif'te⁶²⁸ (Telif Hakları Direktifi), bu belirli hizmetlere odaklanan bir özel sorumluluk rejimi öngörülmüştür:

*“Direktif kapsamındaki hizmetler; temel amacı ya da temel amaçlarından biri, doğrudan ya da dolaylı olarak, daha geniş bir izleyici kitlesini çekmek amacıyla, kategorilere ayırmak ve hedefli tanıtım yapmak da dahil olmak üzere, düzenlemek ve tanıtmak suretiyle, kullanıcıların telif hakkı ile korunan büyük miktarda içeriği yüklemelerini ve paylaşımlarını sağlamak ve depolamak olan hizmetlerdir. Bu tür hizmetler; kullanıcıların bu faaliyetten kar elde etmek amacıyla büyük miktarda telif hakkı korumalı içeriği yüklemelerini ve paylaşımlarını sağlamaktan başka bir ana amacı olan hizmetleri içermemelidir.”*⁶²⁹

Buna göre telif hakkı korumalı içeriklerin yüklenmesi ve paylaşılmasına odaklanan ve bu içeriklerden kar elde etmeyi amaçlayan çevrimiçi platformlar, Direktifte öngörülen özel sorumluluk rejimine tabi olacaktır. Bir çevrimiçi içerik paylaşım hizmeti sağlayıcısının büyük miktarda telif hakkı korumalı içeriği depolayıp depolamadığının ve bu içeriğe erişim sağlayıp sağlamadığının değerlendirilmesi ise, somut duruma göre, hizmetin hedef kitlesi ve hizmet kullanıcıları tarafından yüklenen telif hakkı korumalı içerik dosyalarının sayısı gibi unsurlar göz önünde bulundurularak belirlenecektir.⁶³⁰ Temel amacı farklılaşan ya da kâr amacı gütmeyen çevrimiçi hizmet sağlayıcılar ile temel amacı telif hakkı korsanlığı yapmak veya bunu kolaylaştırmak olan hizmet sağlayıcılar ise Direktif kapsamının dışında tutulmuştur.⁶³¹

Temel amacı telif hakkı korumalı içeriklerin yüklenmesi ve paylaşılması olmayan hizmet sağlayıcılar ile kâr amacı gütmeyen hizmet sağlayıcıların Direktif kapsamı dışında bırakılması, bu hizmet sağlayıcıların sorumluluktan muafiyet koşulları bakımından Telif Hakları Direktifinde öngörülen özel rejime tabi olmamalarını ifade etmektedir. Bununla birlikte, bu hizmet sağlayıcılar genel sorumluluk rejimi olan DSA'ya, ya da başkaca özel sorumluluk rejimlerine tabi olabilir. Öte yandan, sağladıkları hizmetlerle telif hakkını

⁶²⁸ Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (Copyright Directive), 17.5.2019, <https://eur-lex.europa.eu/eli/dir/2019/790/oj>, (23.12.2024)

⁶²⁹ “Copyright Directive”, resital 62.

⁶³⁰ “Copyright Directive”, m. 17(5).

⁶³¹ “Copyright Directive”, resital 62.

teşvik eden hizmet sağlayıcıların Telif Hakları Direktifi'nin kapsamı dışında bırakılması ise onları bütünüyle sorumluluk rejiminin dışına çıkarma ve sorumluluk muafiyetlerinden yararlandırmama amacına yöneliktir.

Telif Hakları Direktifi'nin 17. maddesinde, çevrimiçi içerik paylaşım platformlarının sorumluluk rejimi, yetkiye dayanan kullanım ve yetkisiz kullanım şeklinde iki aşamalı olarak düzenlenmiştir. Buna göre, kural olarak, bir çevrimiçi içerik paylaşım hizmet sağlayıcısı, telif hakları ile korunan içerikleri kamuya iletmek veya kamunun erişimine sunmak için hak sahiplerinden buna ilişkin yetki almalıdır.⁶³² Bu yetki örneğin, adil ve her iki taraf arasında makul bir denge sağlayan bir lisans sözleşmesi imzalanması şeklinde olabilir.⁶³³ Bu durumda, platformda ticari amaç gütmeyen ve faaliyetleri esaslı bir kazanç yaratmayan kullanıcılar da bu kapsamda değerlendirilecektir. Başka bir ifadeyle, platformun hak sahibi tarafından yetkilendirilmesi kullanıcıların da yetkilendirildiği anlamına gelecek ve bu içerikler bakımından ayrıca yetki alınmasına gerek kalmayacaktır.

Herhangi bir yetkilendirme yapılmaması halinde, çevrimiçi içerik paylaşım hizmeti sağlayıcıları özel bir sorumluluk rejimine tabi olacak ve ; (a) *yetki almak için gerekli tüm çabayı gösterdiğini; (b) telif hakkı sahiplerinin kendilerine sunduğu ilgili ve gerekli bilgilerle belirli eserlerin ve diğer materyallerin kullanılamamasını sağlamak için sektörün yüksek profesyonel özen standartlarına uygun olarak gerekli tüm çabayı gösterdiğini ve her durumda; (c) hak sahiplerinden yeterince kanıtlanmış bir bildirim alındıktan sonra derhal harekete geçerek bildirilen eserlere veya diğer materyallere erişimi engellemek veya web sitelerinden kaldırmak için hızlı bir şekilde hareket ettiğini ve bunların gelecekte de yüklenmesini önlemek için (b) bendi uyarınca gerekli tüm çabayı gösterdiğini* kanıtlamadıkları sürece, telif hakkı ile korunan eserlerin ve diğer materyallerin kamuya sunulması da dahil olmak üzere, kamuya yetkisiz olarak iletilmesi eylemlerinden sorumlu olacaktır.⁶³⁴

Buna göre ikinci aşama olarak hizmet sağlayıcılar, sorumluluktan muafiyetten yararlanabilmek için telif hakkı ile korunan eserin hizmetlerinde yer almaması adına en

⁶³² "Copyright Directive", m. 17(1).

⁶³³ "Copyright Directive", resital 61.

⁶³⁴ "Copyright Directive", m. 17(4).

iyi çabayı göstermekle yükümlüdür. En iyi çabanın gösterilip gösterilmediği değerlendirilirken, sektörel en iyi uygulamalar ve ilgili tüm gelişmeler ışığında atılan adımların etkililiği ve orantınlılığı dikkate alınmalıdır. Bu da hizmetin büyüklüğü, gelecekteki potansiyel gelişmeler de dahil olmak üzere mevcut araçlara ilişkin olarak teknolojinin gelişen durumu ve bu tür araçların maliyeti gibi ilgili tüm gelişmelerin özel olarak göz önünde bulundurulmasını gerektirmektedir. Hizmet sağlayıcılar tarafından atılan her türlü adım, izlenen hedefler açısından etkili olmalı, ancak izinsiz eserlerin ve diğer konuların erişilebilirliğini önleme ve durdurma amacına ulaşmak için gerekli olanın ötesine geçmemelidir.⁶³⁵

Direktif'te ön görülen bu özel sorumluluk rejimi, önce lisans sonra filtre rejimi olarak tanımlanabilir. Her ne kadar 17. maddede açıkça ifade edilmese de hizmet sağlayıcıların korunan materyalin kullanılmamasını sağlamak için en iyi çabayı gösterme yükümlülüğü, filtreleme sistemlerinin kullanılmasını gerektirmektedir. Çünkü yüklenen içeriği, içerik tanıma araçlarına başvurmadan “kullanılmamasını sağlamanın” veya “gelecekte yüklenmesini önlemenin” çok sınırlı yolları vardır.⁶³⁶ Aslında diğer tek yöntem geçmiş veya şüpheli telif hakkı ihlallerinden yola çıkarak hareket edilmesidir, ancak bu yöntem de aynı derecede etkili değildir. Dolayısıyla Direktif, fiilen çevrimiçi içeriğin yayınlanmadan önce otomatik araçlarla filtrelenmesini zorunlu hale getirmiştir.⁶³⁷

Hizmet sağlayıcıların en iyi çabayı gösterme yükümlülükleri, doğrudan çevrimiçi içeriğe müdahaleyi gerektirdiğinden, ifade özgürlüğü ve kişisel verilerin korunması haklarını da etkilemektedir. Bu bakımdan Direktif'te, yarışan haklar arasında denge kurulmasına ilişkin net bir tutum söz konusudur. Resital 70'de, genel bir ifadeyle, hizmet sağlayıcılar tarafından atılacak adımlarda hak ihlaline neden olmayan içeriğe ve bu hizmetleri hukuka uygun şekilde kullanan kullanıcıların haklarına müdahale edilmemesi gerektiği belirtilmiştir.⁶³⁸ Öte yandan Direktif'te, alıntı, eleştiri, inceleme, karikatür, parodi amacı taşıyan kullanımlar, telif hakkına yönelik korumanın istisna ve sınırları olarak kabul edilmiştir. Bu tür içerikler bakımından hak sahibi tarafından bir

⁶³⁵ “Copyright Directive”, resital 66.

⁶³⁶ Republic of Poland v European Parliament and Council of the European Union Republic of Poland v European Parliament and Council of the European Union, Case C-401/19 (ECJ 26 Nisan 2022), para. 54.

⁶³⁷ Martin Husovec, “Mandatory Filtering Does Not Always Violate Freedom of Expression: Important Lessons from Poland v Council and European Parliament (C-401/19)”, **Common Market Law Review**, C. 60, S. 1, 2023, s. 178.

⁶³⁸ “Copyright Directive”, resital 66.

yetkilendirme yapıp yapılmadığına bakılmaksızın bir hak ihlalinin bahsedilemeyeceği gibi⁶³⁹, hizmet sağlayıcıların etkili şikâyet ve çözüm mekanizmalarını işleterek, hizmetlerin bu tür özel amaçlarla kullanılmasını güvence altına almaları gerekmektedir.⁶⁴⁰

Direktif uyarınca çevrimiçi içerik paylaşım hizmeti sağlayıcıları, atacakları adımlar konusunda hak sahiplerine karşı şeffaf olmakla yükümlüdür. Söz konusu sorumluluktan muafiyet rejimi çerçevesinde çok çeşitli eylemler gerçekleştirilebileceğinden, hak sahiplerinin talebi üzerine, üstlenilen eylemlerin türü ve bunların gerçekleştirilme şekli hakkında hak sahiplerine yeterli bilgi sağlanmalıdır.⁶⁴¹

Son olarak, Direktif'te genel izleme yükümlülüğü açıkça yasaklandığından, sorumluluktan muafiyet koşulları kapsamında genel izlemeye yol açacak uygulamalardan kaçınılmalıdır.

3. Terörist İçeriğin Çevrimiçi Yayılmasının Ele Alınmasına İlişkin Yönetmelik

İnternet hizmet sağlayıcıları, bir yandan dijital ekonominin gelişmesine katkıda bulunurken diğer yandan da ifade özgürlüğü ile bağlantılı haklar başta olmak üzere temel hak ve hürriyetlerin daha etkili kullanılmasını sağlar. Ne var ki bu hizmetler, terör grupları ve destekçileri tarafından kendi mesajlarını yaymak, taraftar toplamak ve terör eylemlerini kolaylaştırmak için kötüye kullanılmaya da müsaittir. Bu bakımdan, söz konusu içerikler çevrimiçi ortamda bireylerin radikalleşmesinde bir katalizör görevi görmektedir.

Bu kapsamda Avrupa Birliği hukukunda, terörist içeriğin çevrimiçi ortamda yayılmasına karşı çeşitli düzenlemeler ortaya çıkmıştır. Terörle Mücadeleye İlişkin 2017/541 sayılı Direktifte Üye Devletler, kişileri terör suçu işlemeye açıkça teşvik eden çevrimiçi içeriklerin yayılmasını önlemekle yükümlü kılınmıştır. Bu kapsamda öncelikle internette terörle mücadelenin en etkili yolu olan içeriğin kaldırılması yolu denenmeli, ancak bunun mümkün olmaması halinde terörist içeriğe erişim engellenmelidir.⁶⁴² Her iki

⁶³⁹ "Copyright Directive", m. 17(7).

⁶⁴⁰ "Copyright Directive", resital 70.

⁶⁴¹ "Copyright Directive", resital 68.

⁶⁴² Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on Combating Terrorism and Replacing Council Framework Decision 2002/475/JHA and Amending Council Decision 2005/671/JHA, resital 22, <https://eur-lex.europa.eu/eli/dir/2017/541/oj>, (23.10.2024).

durumda da alınacak tedbirler, şeffaf prosedürler takip edilerek ve orantılılık, gereklilik ve kullanıcıların temel hakları göz önünde bulundurularak belirlenmeli, hatalı kararlara karşı etkili başvuru yolları sağlanmalıdır.⁶⁴³

Çevrimiçi terörist içerikle mücadelede Üye Devletlere yükümlülükler yükleyen bu Direktif sonrasında, bu içerikler bakımından doğrudan barındırma hizmet sağlayıcıların yükümlülüklerinin ele alındığı Terörist İçeriğin Çevrimiçi Yayılmasının Ele Alınmasına İlişkin 2021/784 sayılı Tüzük kabul edilmiştir. Çevrimiçi terörist içeriğin kaldırılmasına ilişkin son derece hızlı bir rejim öneren Tüzük, bir yandan kullanıcıların ve hizmet sağlayıcıların haklarının korunmasına yönelik güvenceler sağlarken diğer yandan kamu güvenliğinin korunmasına katkıda bulunmayı amaçlamaktadır.⁶⁴⁴ Bu amaç bakımından barındırma hizmet sağlayıcıların özel toplumsal sorumlulukları olduğu kabul edilmektedir:

*“Merkezi rolleri ve sundukları hizmetlerle bağlantılı teknolojik imkân ve kabiliyetleri ışığında yer sağlayıcı hizmet sağlayıcıların, açık ve demokratik bir toplumda bilgi ve fikir alma ve verme özgürlüğü de dâhil olmak üzere ifade özgürlüğünün temel önemini göz önünde bulundurarak, hizmetlerini teröristler tarafından kötüye kullanılmaktan korumak ve hizmetleri aracılığıyla çevrimiçi olarak yayılan terörist içeriğin ele alınmasına yardımcı olmak konusunda özel toplumsal sorumlulukları vardır.”*⁶⁴⁵

Hizmet sağlayıcıların bu özel toplumsal sorumlulukları, üye devletler tarafından verilen içeriğin kaldırılması kararları ya da hizmet sağlayıcıların terörist içeriğe ilişkin özen yükümlülüklerinden kaynaklanabilmektedir.⁶⁴⁶

⁶⁴³ “Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on Combating Terrorism and Replacing Council Framework Decision 2002/475/JHA and Amending Council Decision 2005/671/JHA”, m. 21.

⁶⁴⁴ Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on Addressing the Dissemination of Terrorist Content Online (TERREG), <https://eur-lex.europa.eu/eli/reg/2021/784/oj>, 23.10.2024.

⁶⁴⁵ “TERREG”, resital 5.

⁶⁴⁶ Eugénie Coche, “Countering Terrorism Propaganda Online Through TERREG and DSA: A Battlefield or a Breath of Hope for Our Fundamental Human Rights?.”, **Moura Vicente, D., de Vasconcelos Casimiro, S., Chen, C. (eds) The Legal Challenges of the Fourth Industrial Revolution**, Law, Governance and Technology Series, V. 57, Springer, 2023, s. 315.

Buna göre hizmet sağlayıcılar, üye devletlerin yetkili otoriteleri tarafından terörist içeriğin kaldırılmasına ya da bu içeriğe erişimin engellenmesine ilişkin bir karar verilmesi halinde, gecikmeyi haklı çıkaracak nesnel olarak gerekçelendirilebilir teknik veya operasyonel nedenler göstermedikleri sürece, mümkün olan en kısa sürede ve her halükârda söz konusu kararın alınmasından itibaren bir saat içinde tüm üye devletlerde terörist içeriği kaldırmak ya da içeriğe erişimi engellemekle yükümlüdür. Bu kapsamda hizmet sağlayıcılar, uygulanacak tedbirlerin niteliği ve zamanı konusunda üye devletlere bilgi vermekle yükümlüdür. Ayrıca, kaldırma kararının gereklerinin, mücbir sebepler ya da fiili imkansızlıklar veya hizmet sağlayıcıdan kaynaklanmayan hatalar sebebiyle yerine getirilememesi halinde, söz konusu gerekçeler ortadan kalkar kalmaz gerekli tedbirlerin alınması gerekmektedir.⁶⁴⁷

Üye devletler tarafından verilen kararların yerine getirilmesinden başka hizmet sağlayıcılar, terörist içeriklere ilişkin olarak hem hizmet koşullarında gerekli düzenlemeleri yapmak hem de bir takım özel önlemler almakla da yükümlüdür. Bu kapsamda örneğin,

- Terör içeriklerinin tespit edilmesi ve hızlı bir şekilde kaldırılması ya da bu içeriklere erişimin engellenmesi için yeterli personel veya teknik araç bulundurulması,
- Kullanıcıların terör içeriklerini kolayca bildirmesi için mekanizmalar oluşturulması,
- Kullanıcıların terör içerikleri konusunda farkındalığının artırılması için çeşitli mekanizmalar kurulması gibi çeşitli önlemler alınması mümkündür.⁶⁴⁸

Tüzük'te bu şekilde bazı önlemlere yer verilmiş olsa da hangi önlemlerin alınacağı hususu hizmet sağlayıcıların inisiyatifine bırakılmıştır. Ancak bu önlemler her halükârda, (a) hizmetlerin terör içeriklerine maruz kalma seviyesini azaltmada etkili, (b) hedefe yönelik ve orantılı olmalı; (c) ifade özgürlüğü, bilgi edinme hakkı, özel hayatın gizliliği ve kişisel verilerin korunması gibi temel haklar gözetilerek ve (d) ayrımcı olmayan bir şekilde uygulanmalıdır. Ayrıca, teknik önlemlerin tercih edilmesi halinde olası hataların

⁶⁴⁷ “TERREG”, m. 3(7).

⁶⁴⁸ “TERREG”, m. 3(7).

önüne geçmek ve terörist içerik olmayan diğer materyallerin kaldırılmasının önüne geçmek amacıyla insan gözetimi ve doğrulama yoluyla güvence sağlanmalıdır.⁶⁴⁹ Örneğin, hizmet sağlayıcılar filtreleme sistemlerini kullanmak zorunda değildir, ancak hizmetlerinin terörist içeriğin yayılması amacıyla kötüye kullanılmasını etkili bir şekilde ele almak için uygun ve gerekli olduğunu düşünmeleri halinde kendi inisiyatifleri ile bu sistemleri kullanmaya karar verebilirler.⁶⁵⁰ Bu tür araçları kullanmayı tercih ettiklerinde buna ilişkin güvenceleri sağlamaları ve buna ilişkin yeterli kapasiteye sahip olup olmadıklarını raporlamaları gerekmektedir.⁶⁵¹

Tüzük'te, başta ifade özgürlüğü olmak üzere temel hak ve özgürlükler arasındaki olası çatışmaların çözümüne yönelik de çeşitli güvencelere yer verilmiştir.⁶⁵² Buna göre hizmet sağlayıcılar, alınan önlemlere ve çevrimiçi meşru ifadelerin hatalı bir şekilde kaldırılmasına ilişkin yıllık şeffaflık raporları yayınlamalıdır. Öte yandan, içeriğin kaldırılmasına karar verilmesi halinde bunu kullanıcıya bildirmeli ve kaldırma kararına itiraz edilebilmesi için gerekli belgeleri sağlamalıdır.⁶⁵³ Hizmet sağlayıcılar, kullanıcı dostu şikâyet mekanizmaları kurarak şikayetlerin hızlı bir şekilde ele alınmasını sağlamakla da yükümlüdür. İçeriğin hatalı bir şekilde kaldırıldığının anlaşılması halinde ise kaldırılan içeriğin mümkün olan en kısa sürede eski durumuna döndürülmesi gerekmektedir.⁶⁵⁴

Sonuç olarak terörist içerik bakımından öngörülen bu rejimin, güvenli liman rejimine kıyasla hizmet sağlayıcılar için daha sıkı kurallar getirdiği açıktır. Bu yönüyle Tüzüğün güvenli liman rejiminde bir erozyona yol açtığı, bu bakımdan yatay rejimin sonunu getirdiği ileri sürülmektedir.⁶⁵⁵ Ancak, çevrimiçi ortamdaki geniş içerik yelpazesi göz önünde bulundurulduğunda, mevcut ve potansiyel sorunlarla mücadelenin yatay ve sektörel yaklaşımların birlikte ele alınmasını gerektirdiği sonucuna varılabilir. Bu bakımdan, çevrimiçi terörist içerikle mücadelede yatay ve dikey yaklaşımların birlikteliği

⁶⁴⁹ “TERREG”, m. 5(3).

⁶⁵⁰ “TERREG”, resital 25.

⁶⁵¹ “TERREG”, resital 24.

⁶⁵² Coche, “Countering Terrorism Propaganda Online Through TERREG and DSA: A Battlefield or a Breath of Hope for Our Fundamental Human Rights?”, ss. 319-24.

⁶⁵³ “TERREG”, m. 11.

⁶⁵⁴ “TERREG”, m. 10.

⁶⁵⁵ Philippe Jougoux, **Facebook and the (EU) Law: How the Social Network Reshaped the Legal Framework**, Cham: Springer International Publishing, 2022, C. 48, s. 172.

hem kapsanan içerik türü hem de prosedürel güvenceler ve yükümlülükler açısından tamamlayıcı bir işlev görmektedir.⁶⁵⁶

4. Görsel-İşitsel Medya Hizmetleri Direktifi

Avrupa Birliği hukukunda internet hizmet sağlayıcılarının insan haklarına ilişkin yükümlülüklerinin ele alındığı sektörel düzenlemelerden biri de 2018/1808 sayılı Direktif'tir.⁶⁵⁷ Direktif, doğrudan hizmet sağlayıcılara yönelik olmasa da Üye Devletler üzerinden video paylaşım platformlarına genel kamuoyunun, özellikle de gençlerin giderek daha fazla eriştiği görsel-işitsel içerikler bakımından yükümlülükler yüklenmektedir.

Her ne kadar video paylaşım platformu hizmetlerinde sunulan içeriğin önemli bir kısmı video paylaşım platformu sağlayıcısının editoryal sorumluluğu altında olmasa da içeriğin, yani programların, kullanıcı tarafından oluşturulan videoların ve görsel-işitsel ticari iletişimlerin organizasyonunu, otomatik araçlar veya algoritmalar da dahil olmak üzere belirlediklerinden, bu sağlayıcıların küçükleri fiziksel, zihinsel veya ahlaki gelişimlerine zarar verebilecek içerikten korumak için uygun önlemleri almaları gerekmektedir.⁶⁵⁸

Resital 45'e göre kullanıcıların, özellikle de reşit olmayanların giderek daha fazla görsel-işitsel içerik tüketmesi, video paylaşım platformlarıyla bağlantılı olarak yeni zorluklar ortaya çıkarmakta ve bu platformlarda sunulan zararlı içerik ve nefret söylemi giderek artan bir şekilde endişe yaratmaktadır. Dolayısıyla, küçükleri ve genel kamuoyunu bu tür içeriklerden korumak için bu konularda orantılı kuralların belirlenmesi önem arz etmektedir.⁶⁵⁹ Bu noktada, video paylaşım hizmet sağlayıcılara yönelik düzenlemelerin genel izleme yasağına uygun olması, herhangi bir ön kontrol önlemine

⁶⁵⁶ Coche, "Countering Terrorism Propaganda Online Through TERREG and DSA: A Battlefield or a Breath of Hope for Our Fundamental Human Rights?", s. 318.

⁶⁵⁷ "Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 Amending Directive 2010/13/EU on the Coordination of Certain Provisions Laid down by Law, Regulation or Administrative Action in Member States Concerning the Provision of Audiovisual Media Services (Audiovisual Media Services Directive) in View of Changing Market Realities", (2018), <http://data.europa.eu/eli/dir/2018/1808/oj/eng>, (16.11.2024).

⁶⁵⁸ "Audiovisual Media Services Directive", resital 47.

⁶⁵⁹ "Audiovisual Media Services Directive", resital 45.

veya içeriğin yükleme filtrelemesine yol açmaması gerektiğinin altını çizmek gerekmektedir.⁶⁶⁰

Bu kapsamda Direktifin 28b maddesinde, platformların çocukları ve genel kullanıcı kitlesini hukuka aykırı ve zararlı içerikten korumak için almaları gereken önlemler net bir şekilde belirlenmiştir. Buna göre, video paylaşım platformu sağlayıcılarının, çocukları, fiziksel, zihinsel veya ahlaki olarak gelişimlerini etkileyebilecek içerikler bakımından gerekli önlemleri almaları gerekmektedir. Hizmet sağlayıcıların ayrıca genel olarak, şiddete veya nefrete teşvik içeren ya da suç teşkil eden içeriklere ilişkin olarak da gerekli tedbirleri almakla yükümlüdür.⁶⁶¹

Direktife göre uygun tedbirlerin; söz konusu içeriğin niteliği, yol açabileceği zarar, korunacak kişi kategorisinin özellikleri ve video paylaşım platformu sağlayıcıları ile içeriği oluşturan veya yükleyen kullanıcıların hakları ve meşru menfaatleri ile genel kamu yararı ışığında belirlenmesi gerekmektedir. Bu kapsamda hizmet sağlayıcılar tarafından içeriklere yaş sınırlaması ya da ebeveyn kontrol sistemleri getirme, kullanıcıların içerik bildirme mekanizmalarını kullanmasına imkân sağlama, şeffaf raporlama prosedürleri oluşturma ve gerektiğinde içerik kaldırma gibi önlemler alınabilmektedir. Ayrıca Direktif, üye devletleri video paylaşım platformlarının kendi düzenleme çabalarını teşvik etmeye ve kullanıcıların dijital okuryazarlık becerilerini geliştirmeye yönlendirmektedir. Direktif, kişisel verilerin korunması hakkı bakımından da hizmet sağlayıcılara açık bir yükümlülük yüklemektedir. Buna göre video paylaşım hizmetleri tarafından toplanan veya başka şekilde oluşturulan reşit olmayanlara ait kişisel veriler, doğrudan pazarlama, profil oluşturma ve davranışsal hedefli reklamcılık gibi ticari amaçlarla işlenmeyecektir.⁶⁶²

⁶⁶⁰ “Audiovisual Media Services Directive”, m. 28b(3).

⁶⁶¹ Federico Galli, Andrea Loreggia, Giovanni Sartor, “The Regulation of Content Moderation”, **The Legal Challenges of the Fourth Industrial Revolution**, ed. Dário Moura Vicente, Sofia De Vasconcelos Casimiro, Chen Chen, Law, Governance and Technology Series, Cham: Springer International Publishing, 2023, C. 57, s. 80.

⁶⁶² “Audiovisual Media Services Directive”, m. 28b(1).

5. Çocukların Cinsel İstismarı, Cinsel Sömürüsü ve Çocuk Pornografisiyle Mücadeleye İlişkin Direktif

Yeni teknolojilerin ve internetin gittikçe artan kullanımı çocukların cinsel istismarı ve çocuk pornografisini de artırmıştır. Bu durum, çocukların cinsel istismarı ve çocuk pornografisi gibi ciddi cezai suçlar, suçluların kovuşturulması süreçleri ve çocuk mağdurların korunması hususlarında kapsamlı bir yaklaşım gerektirmiştir. Direktif, çocukların cinsel istismarı ve sömürüsünün ciddi biçimlerini suç haline getirmekte ve cezaları artırmaktadır. Ayrıca, ağırlaştırıcı koşullar getirmekte ve yargı yetkisi ve suçluların iadesi konularını ele almaktadır. Çocukların cinsel sömürüsüne ilişkin bir suç olarak cezalandırılacak davranışlar (bir bilgisayar sistemi aracılığıyla gerçekleştirilsin ya da gerçekleştirilmesin) arasında; çocuk pornografisi üretimi, çocuk pornografisinin dağıtımı, yayılması ya da iletilmesi; teklif edilmesi ya da başka bir şekilde yapılması yer almaktadır.⁶⁶³

Direktif'te, esas olarak cezai tedbirler ele alınmış olsa da içerik sınırlamasına ilişkin olarak da bazı tedbirlere yer verilmiştir. Buna göre çocuk pornografisi içeren veya yayan web sitelerine karşı şu tedbirlerin alınması gerekmektedir:

“Üye devletler, kendi topraklarında barındırılan çocuk pornografisi içeren veya yayan web sayfalarının derhal kaldırılmasını sağlamak için gerekli tedbirleri alacak ve kendi toprakları dışında barındırılan bu tür sayfaların kaldırılmasını sağlamak için çaba göstereceklerdir.

Üye Devletler, kendi topraklarındaki İnternet kullanıcılarına yönelik çocuk pornografisi içeren veya yayan web sayfalarına erişimi engellemek için tedbirler alabilirler. Bu tedbirler şeffaf usullerle belirlenmeli ve özellikle kısıtlamanın gerekli ve orantılı olanla sınırlı olmasını ve kullanıcıların kısıtlamanın nedeni hakkında bilgilendirilmesini sağlamak üzere yeterli güvenceler sağlamalıdır. Bu güvenceler aynı zamanda adli telafi imkanını da içermelidir.”⁶⁶⁴

⁶⁶³ Andrej Savin, **EU Internet Law**, Third Edition Edward Elgar Publishing, 2020, s. 384.

⁶⁶⁴ Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on Combating the Sexual Abuse and Sexual Exploitation of Children and Child Pornography, and Replacing

Direktif'in bu hükmü uyarınca üye devletlerin, çocuk pornografisi içeren veya yayan web sitelerinin kaldırılmasını veya bunlara erişimin engellenmesini sağlamak için gerekli tüm tedbirleri alması gerekmektedir. Bu da hizmet sağlayıcıların, söz konusu içerikler bakımından çeşitli önlemler almasını gerektirmektedir. Direktif bu kapsamda son kullanıcıların haklarının dikkate alınmasını ve bu önlemlere ilişkin yeterli güvencelerin sağlanmasını gerektirmektedir; ancak buna ilişkin bir rehberlik sağlamamaktadır.⁶⁶⁵

C. Avrupa Birliği Adalet Divanı Kararlarında İnternet Şirketlerinin İnsan Hakları Yükümlülükleri

Avrupa Birliği Adalet Divanı'nın internet şirketleri ve insan hakları ilişkisini ele aldığı içtihadı çoğunlukla dijital araçların sorumluluğu, sosyal medya yayınları ve kişisel verilerin korunması, platform veri işleme uygulamaları ve tüketiciyi koruma kanununun sosyal medya ortamındaki veri koruma kurallarıyla etkileşimi ile ilgili davalarda geliştirilmiştir.

Dijital araçların sorumluluğu, Dijital Hizmetler Yasasıyla güncellenmeden önce, E-Ticaret Direktifi kapsamında belirlenmekteydi. Bu kapsamda, belirli araçlara, belli koşulları sağlamaları halinde, kullanıcıların yasadışı davranışlarından kaynaklanan ikincil sorumluluktan sınırlı bir muafiyet tanınmıştır. Ayrıca, Direktifin 15. maddesinde Üye Devletlerin dijital araçlara ilettikleri veya depoladıkları bilgileri izleme veya yasa dışı faaliyete işaret edebilecek gerçekleri veya durumları aktif olarak arama konusunda genel bir yükümlülük getirilmemesi öngörülmüştür. Araçların sorumluluktan muafiyetine ilişkin bu hususlar, Dijital Hizmetler Yasası'nda benzer şekilde düzenlenmiştir.

1. İçerik Yönetimi

2010'lu yıllarda ABAD, özellikle de fikri mülkiyet hakkıyla bağlantılı bir dizi davada, hizmet sağlayıcıların içerik denetimi konusundaki yükümlülüklerini ele almıştır.

Council Framework Decision 2004/68/JHA, m. 25. <https://eur-lex.europa.eu/eli/dir/2011/93/oj>, (23.10.2024).

⁶⁶⁵ "Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on Combating the Sexual Abuse and Sexual Exploitation of Children and Child Pornography, and Replacing Council Framework Decision 2004/68/JHA", resital 47.

Bu kararlarda söz konusu yükümlölüklerin yerine getirilmesi ve bu kapsamda yarışan hak ve menfaatler arasında denge kurulmasına ilişkin önemli gelişmeler yaşanmıştır. Bu kararlarda, söz konusu yükümlölükler ile bağlantılı olarak Direktif'in 15. maddesinde düzenlenen genel izleme yükümlölüğü yasağına ilişkin önemli tespitler yapılmıştır. Böylece, izin verilen ve izin verilmeyen izleme yükümlölüklerinin yelpazesi de açıklığa kavuşturulmuştur.⁶⁶⁶

Avrupa Birliği Adalet Divanı içtihadında, E-Ticaret Direktifi ile ilgili olarak hizmet sağlayıcıların insan hakları yükümlölükleri temel olarak iki şekilde gündeme gelmiştir. Bunlardan ilki, Direktif'in 12 (3), 13 (2) ve 14 (3) maddeleri uyarınca, bir mahkeme veya idari makamın kararı üzerine, hukuka aykırı içeriğin kaldırılması ya da erişimin engellenmesi de dahil hukuka aykırı içerikten kaynaklanan ihlali sona erdirmeye veya önleme yükümlölüğüdür.⁶⁶⁷ Basit iletim, ön belleğe alma ve barındırma hizmet sağlayıcılara, sorumluluktan muafiyet koşullarını sağlamalarına rağmen, yetkili otoriteler aracılığıyla bu şekilde yükümlölükler getirilmesi mümkündür.⁶⁶⁸ Üye devletlerin hukuk sistemleri uyarınca alınabilecek bu kararların Birlik hukukuna da uygun olması gerekmektedir.⁶⁶⁹

İnsan hakları yükümlölüklerinin gündeme geldiği ikinci durum ise, barındırma hizmet sağlayıcıların hukuka aykırı içerik hakkında gerçek bilgi veya farkındalık elde etmesi üzerine hukuka aykırı içeriğin kaldırılması veya erişimin engellenmesi için ivedilikle harekete geçme yükümlölüğüdür. Diğerler hizmet sağlayıcılarından farklı olarak barındırma hizmet sağlayıcıları, hizmet alıcıları tarafından ve onların talebi üzerine sağlanan bilgileri depoladıkları ve bazen büyük ölçekte olmak üzere diğer alıcıların bunlara erişimine izin verdikleri için hukuka aykırı içerikle mücadelede özel bir rol oynamaktadır.⁶⁷⁰ Bu bakımdan, barındırma hizmeti sağlayıcıların, bu yönde bir yargı kararı ya da idari karar olmaksızın da hukuka aykırı içeriği kaldırmaları ya da erişimi engellemeleri gerekebilmektedir. Direktifin 14(1) maddesinde, sorumluluktan muafiyetin şartları arasında düzenlenen bu yükümlölüğün yerine getirilmemesi, barındırma hizmet

⁶⁶⁶ Giancarlo Frosio, Christophe Geiger, "Taking Fundamental Rights Seriously in the Digital Services Act's Platform Liability Regime", *European Law Journal*, C. 29, S. 1-2, 2023, s. 38.

⁶⁶⁷ "ECD", resital 45; "DSA", resital 25.

⁶⁶⁸ Tobias Mc Fadden v Sony Music Entertainment Germany GmbH, Case C-484/14 (ECJ 15 Eylül 2016), para. 56-59, 79.

⁶⁶⁹ "DSA", resital 25.

⁶⁷⁰ "DSA", resital 50.

sağlayıcının muafiyetten yararlanmasına engel teşkil edecektir.⁶⁷¹ Dolayısıyla, içerik yönetimine ilişkin yükümlülükler sunulan hizmetin niteliğine göre farklılık göstermektedir.⁶⁷²

Dijital araçlar, kendi incelemeleri veya kendilerine yapılan bildirimler yoluyla yasadışı faaliyetlerden haberdar olabilirler. Kullanıcılar tarafından yapılan bildirimler yeterince ayrıntılı ya da sağlam delillerle desteklenmemiş olabileceğinden, söz konusu bildirimler hizmet sağlayıcıları otomatik olarak sorumluluktan muafiyet kapsamından çıkarmamaktadır. Bununla birlikte, platformun yasadışılığına ilişkin bir bildirim alması, özenli bir platformun kendisine iletilen bilgilere dayanarak yasadışı faaliyeti tespit edip edemeyeceği değerlendirilirken dikkate alınacaktır.⁶⁷³

ABAD, bu kritere ilişkin olarak, hizmetlerin yasadışı amaçlar için de kullanıldığına dair genel bir farkındalığın ya da soyut bir bilginin yeterli olmadığını; E Ticaret Direktifi'nin lafzı, amacı ve genel bağlamından bunun belirli yasadışı bilgi ve faaliyetlere yönelik olduğunun anlaşıldığını ifade etmiştir. Buna göre, bir çevrimiçi içerik paylaşım platformu işletmecisinin, o platforma yüklenen içeriği otomatik olarak indekslemesi, platformun arama fonksiyonuna sahip olması ve kullanıcıların profil veya tercihlerine göre video önermesi de platformun söz konusu içerikten sorumlu tutulması için yeterli bir gerekçe değildir.⁶⁷⁴

ABAD, platformların hukuka aykırı içeriklerin paylaşılması ve yayılması konusunda vazgeçilmez bir rol oynadığını kabul etmektedir. Gerçekten de platformlar olmasaydı, pek çok hukuka aykırı içeriğin internette paylaşılması imkânsız ya da çok daha karmaşık olurdu.⁶⁷⁵ Bununla birlikte, internetin ifade özgürlüğü ve bağlantılı diğer özgürlükler açısından taşıdığı özel önem dikkate alınarak adil bir dengenin aranması

⁶⁷¹ “ECD”, m. 14(1); “DSA”, resital 22, m.6.

⁶⁷² Dijital Hizmetler Yasası resital 5'te bu kapsam şu şekilde ifade edilmiştir: “*Bu Yasa, özellikle aracı hizmet sağlayıcılarına ve özellikle de 'basit iletim', 'önbelleğe alma' ve 'barındırma' hizmetleri olarak bilinen hizmetlerden oluşan aracı hizmetlere uygulanmalıdır; zira bu hizmetlerin, esasen her türlü meşru ve sosyal açıdan faydalı amaçlar için kullanımının katlanarak artması, yasadışı veya başka türlü zararlı bilgi ve faaliyetlerin aracılığı ve yayılmasındaki rollerini de artırmıştır.*”

⁶⁷³ L'Oréal SA and Others v eBay International AG and Others, Case C-324/09 (ECJ 12 Temmuz 2011), para. 122; Frank Peterson v Google LLC and Others and Elsevier Incv Cyando AG, Joined Cases C-682/18 and C-683/18 (ECJ 22 Haziran 2021), para. 115.

⁶⁷⁴ Bu tespit, DSA resital 22 ile yasal bir zemine kavuşmuştur.

⁶⁷⁵ Frank Peterson v Google LLC and Others and Elsevier Incv Cyando AG, ECJ 22 Haziran 2021, para. 77.

gerektiği açıktır.⁶⁷⁶ Bu adil denge arayışında, platformun eylemlerinin sonuçları hakkında tam bilgi sahibi olarak "kasıtlı" hareket edip etmediği de dikkate alınması gereken önemli bir noktadır.⁶⁷⁷

Bir kapsamda, örneğin, platformun yasadışı içeriğin varlığını bilmesine (veya bilmesi gerekmesine) rağmen, platformundaki telif hakkı ihlallerine inandırıcı ve etkili bir şekilde karşı koymak için, özenli bir platformdan beklenebilecek makul ölçüde teknolojik önlemleri uygulamaya koymaması; platformun kamuya hukuka aykırı olarak iletilen korumalı içeriğin seçilmesine katılması; platformda bu tür içeriğin hukuka aykırı paylaşımı için özel olarak tasarlanmış araçlar sağlanması; ve operatörün, örneğin kullanıcılarını platform aracılığıyla korunan içeriği yasadışı olarak kamuya iletmeye teşvik eden bir finansal model benimseyerek bu tür bir paylaşımı bilerek teşvik etmesi gibi hallerde kasıtlı hareket ettiği kabul edilebilecektir.⁶⁷⁸

Bu noktada, platformun içeriğin yasa dışı olarak kullanıma sunulduğunun "genel anlamda" farkında olmasının, tek başına kasıtlı bir davranış olarak değerlendirilemeyeceğinin altı tekrar çizilmelidir. Ancak, hak sahibinden bildirim alan platformun yasa dışı içeriği kaldırmak veya erişimi engellemek için hızlı bir şekilde harekete geçmemesi durumunda bu değerlendirme farklı olacaktır.⁶⁷⁹

Telif hakkıyla korunan eserlerin bir video paylaşım platformu olan *YouTube'a* ve bir dosya barındırma ve paylaşım platformu olan *Uploaded'a* izinsiz yüklenmesine ilişkin *Youtube/Cyando*⁶⁸⁰ kararında ABAD, bir platformun yasadışı içerikten hangi hallerde sorumlu tutulabileceğine; başka bir açıdan bakıldığında, bir platformu sorumluluktan

⁶⁷⁶ Nitekim, Youtube/Cyando davasında da başsavcı bu hakların önemine atıfta bulunmuştur: "... bu platformları kullananların temel hakları göz ardı edilemez. Bunlar arasında, ... ifade ve bilgi edinme özgürlüğü de yer almaktadır; bu madde, kanaat sahibi olma ve bilgi ve fikir alma ve yayma özgürlüğünü de kapsamaktadır. Hem Adalet Divanı'nın hem de Avrupa İnsan Hakları Mahkemesi'nin içtihatlarından internetin bu açıdan özel bir öneme sahip olduğu açıkça görülmektedir. Daha spesifik olarak ikinci mahkeme, YouTube'un bireylerin bu özgürlüğü kullanmasında önemli bir araç olduğuna hükmetmiştir. Bu durum, ... YouTube gibi çevrimiçi platformları kullanarak eserlerini çevrimiçi olarak paylaşan çok sayıda insan göz önüne alındığında, ifade özgürlüğüyle yakından bağlantılı olan sanat özgürlüğü için de geçerlidir." Opinion of Advocate General Saugmandsgaard Øe delivered on 16 July 2020. Frank Peterson v Google LLC and Others and Elsevier Inc. v Cyando AG., (ECJ 2018), para. 241.

⁶⁷⁷ Frank Peterson v Google LLC and Others and Elsevier Inc. v Cyando AG, ECJ 22 Haziran 2021, para. 78, 80, 83.

⁶⁷⁸ Frank Peterson v Google LLC and Others and Elsevier Inc. v Cyando AG, para. 84.

⁶⁷⁹ Frank Peterson v Google LLC and Others and Elsevier Inc. v Cyando AG, para. 85.

⁶⁸⁰ Frank Peterson v Google LLC and Others and Elsevier Inc. v Cyando AG, para. 85.

muaf tutulabilmesi için hangi yükümlülükleri yerine getirmesi gerektiğine ilişkin somut tespitlere yer vermiştir. Bu kapsamda Youtube'un platform kullanıcıları tarafından platformuna yüklenen içeriğin oluşturulmasına veya seçilmesine müdahale etmediği ve bu içeriği yüklenmeden önce görüntülemediği veya izlemediği; bu içeriğin otomatik olarak bu platforma yüklendiği; YouTube'un kullanıcılarını, hizmet şartlarında ve bir dosya her yüklendiğinde, telif hakkı ile korunan içerik yayınlamanın yasak olduğu konusunda açıkça bilgilendirdiği; bir videonun hak sahibi tarafından bildirilmesi nedeniyle engellendiği durumlarda, videoyu yükleyen kullanıcının, ihlallerin tekrarlanması durumunda hesabının engelleneceği konusunda uyarıldığı; YouTube'un, platformundaki telif hakkı ihlallerini önlemek, sona erdirmek ve içeriği kontrol etmek için çeşitli teknolojik önlemleri uygulamaya koyduğu; ve platformun finansal modelinin, yasadışı içerik paylaşımı yapılması ya da bunun teşvik edilmesine dayanmadığı hususlarının altını çizmiştir. Birleştirilen davalardan diğerine konu Uploaded bakımından da Mahkeme, içeriğin platform tarafından oluşturulmadığı, seçilmediği, görüntülenmediği veya kontrol edilmediği ve platformunun kullanım koşullarında kullanıcıların, bu platform aracılığıyla telif haklarını ihlal etmelerinin yasak olduğu konusunda bilgilendirildiğine dikkat çekmiştir.⁶⁸¹

ABAD, söz konusu platformlara ilişkin nihai değerlendirmenin başvuran mahkemenin görevi olduğunu belirtmişse de ayrıntılı bu tespitleriyle platformların kullanıcıların yasadışı olarak telif hakkı ihlali yapmasına aktif olarak aracılık etmediğini, dolayısıyla hukuka aykırı içeriklere ilişkin sorumluluktan muaf olduklarını ima etmiştir.⁶⁸²

Daha önce de ifade edildiği üzere, hizmet sağlayıcılar, kullanıcı bildirimleri yerine yetkili organlar eliyle de hukuka aykırı içeriğe müdahale etmeye zorlanabilir. E-Ticaret Direktifi'nin 12(3), 13(2) ve 14(3) maddelerine göre, güvenli liman korumaları, bir mahkeme veya idari makamın, üye devletlerin hukuk sistemlerine uygun olarak, farklı türden kararlar alınmasını engellemektedir. Bununla birlikte, yetkili organlar tarafından verilecek bu kararlarda da hizmet sağlayıcıların hakları ile internet

⁶⁸¹ Frank Peterson v Google LLC and Others and Elsevier Incv Cyando AG, para. 97.

⁶⁸² Frank Peterson v Google LLC and Others and Elsevier Incv Cyando AG, para. 102.

kullanıcılarının yarışan hak ve menfaatleri arasında adil bir denge kurulması önem arz etmektedir.

ABAD, yetkili otoritelerin hizmet sağlayıcılara yönelik kararlarının kapsamının ele alındığı ilk davalardan biri, çevrimiçi pazaryerlerinden eBay’de, Fransız kozmetik şirketi olan L’Oréal’in, sahte ürün satışlarına ilişkin *L’Oréal v. eBay*⁶⁸³ davasıdır. ABAD, bu davada hizmet sağlayıcılardan mevcut ihlalleri sona erdirmeleri yanında, gelecekteki ihlallerin önlenmesine yönelik olarak da karar alınabileceğini kabul etmiştir. Bu kararlar etkili, orantılı, caydırıcı olmalı ve meşru ticaretin önünde engel oluşturmamalıdır.⁶⁸⁴ Ayrıca, E-Ticaret Direktifi’nin 15. maddesi uyarınca, ilgili çevrimiçi hizmet sağlayıcısından istenen tedbirler, tüm müşterilerin bütün verilerinin aktif bir şekilde izlenmesini gerektirmemelidir.⁶⁸⁵

Hizmet sağlayıcıların, mevcut ihlalleri sona erdirmeye ve gelecekteki ihlalleri önleme yükümlülükleri *Telekabel Wien*⁶⁸⁶ kararında yarışan tüm menfaatleri de kapsayacak şekilde ele alınmıştır. Bir internet erişim sağlayıcısına telif haklarını ihlal eden içeriğe sahip web sitelerine erişimin engellenmesini emreden bir kararının uygulanmasıyla ilgili bu davada, ABAD, hizmet sağlayıcıya karşı bu yönde bir karar alınıp alınamayacağını değerlendirmiştir.

Hizmet sağlayıcılara bu konuda bir yükümlülük yüklenmesi, onları önemli bir maliyet teşkil edebilecek, faaliyetlerinin organizasyonu üzerinde önemli bir etkiye sahip olabilecek veya zor ve karmaşık teknik çözümler gerektiren tedbirler almaya mecbur bıraktığından hizmet sağlayıcıların iş yapma özgürlüğünü etkilemektedir. Bu bakımdan, hizmet sağlayıcılar, hedeflenen amaca ulaşmak için alacakları tedbirleri belirleme konusunda serbest bırakılmıştır. Bununla birlikte, hizmet sağlayıcılar her halükârda, internet kullanıcılarının temel hakkı olan bilgi edinme özgürlüğünü dikkate almakla yükümlüdür:

⁶⁸³ L’Oréal SA and Others v eBay International AG and Others.

⁶⁸⁴ L’Oréal SA and Others v eBay International AG and Others, para. 144; Frank Peterson v Google LLC and Others and Elsevier Incv Cyando AG, ECJ 22 Haziran 2021, para. 141.

⁶⁸⁵ Frank Peterson v Google LLC and Others and Elsevier Incv Cyando AG, para. 139.

⁶⁸⁶ UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH and Wega Filmproduktionsgesellschaft mbH, Case C-314/12 (ECJ 27 Mart 2014).

*“Bu bağlamda, internet servis sağlayıcısı tarafından alınan tedbirler, üçüncü bir tarafın telif hakkı veya bağlantılı bir hakkı ihlaline son vermeye hizmet etmeleri, ancak bu şekilde sağlayıcının hizmetlerini yasal olarak bilgiye erişmek için kullanan internet kullanıcılarını etkilememeleri anlamında, kesinlikle hedefe yönelik olmalıdır. Aksi takdirde, sağlayıcının bu kullanıcıların bilgi edinme özgürlüğüne müdahalesi, izlenen amaç ışığında haksız olacaktır.”*⁶⁸⁷

L'Oréal davasındaki sonuçları yineleyen ABAD, tedbirlerin *"üçüncü bir şahsın telif hakkı ihlalini sona erdirmeye hizmet etmesi, ancak aynı zamanda internet kullanıcılarının yasal bilgilere erişmesini kesinlikle engellememesi"* gerektiğini teyit etmiştir. Buna göre, çatışan hak ve menfaatler arasında adil bir dengenin sağlanabilmesi için, hizmet sağlayıcılar tarafından alınan tedbirler, (i) [...] internet kullanıcılarını, yasal olarak erişilebilir bilgilere erişme imkanından gereksiz yere mahrum bırakmamalı ve (ii) [...] korunan konuya yetkisiz erişimi önleme etkisi yaratmalı veya en azından bunu başarmayı zorlaştırmalı ve fikri mülkiyet hakkını ihlal ederek kendilerine sunulan konuya erişen internet kullanıcılarını ciddi şekilde caydırmalıdır. Dolayısıyla, telif hakkına konu içeriğin engellenmesinin diğer ilgili haklar üzerinde orantısız bir etkisi olacaksa; korunan içeriğin engellenmesi yerine erişimin "zorlaştırılması" ve ihlallerin "ciddi şekilde caydırılması" telif hakkı sahipleri için yeterli koruma olarak kabul edilebilecektir.⁶⁸⁸

Telif hakkı sahibi ile internet kullanıcılarının hakları arasında denge kurulmasına ilişkin bir başka dava da McFadden v. Sony Music kararıdır.⁶⁸⁹ ABAD Telekabel Wien kararına atıf yaparak, hizmet sağlayıcının alacağı tedbirler konusunda serbest bırakılmasının adil dengenin sağlanmasına katkıda bulunduğunu belirttikten sonra; somut davada olduğu gibi alınacak önlemlerin sınırlı olduğu durumlarda da, seçme hakkının, hizmet sağlayıcısına bırakılmasının gerekip gerekmediği sorununa odaklanmıştır.⁶⁹⁰

⁶⁸⁷ UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH and Wega Filmproduktionsgesellschaft mbH, para. 56.

⁶⁸⁸ Martin Senftleben, Christina Angelopoulos, “The Odyssey of the Prohibition on General Monitoring Obligations on the Way to the Digital Services Act: Between Article 15 of the E-Commerce Directive and Article 17 of the Directive on Copyright in the Digital Single Market”, 2020, s. 17, <https://papers.ssrn.com/abstract=3717022>.

⁶⁸⁹ Tobias Mc Fadden v Sony Music Entertainment Germany GmbH.

⁶⁹⁰ Tobias Mc Fadden v Sony Music Entertainment Germany GmbH, para. 84-86.

Somut başvuruda, wifi hizmeti sunmaktan ibaret bir hizmet sağlayan Mc Fadden'in söz konusu yargı kararı uyarınca üç farklı önlem alınabileceği öngörülmektedir: i. tüm iletişimin incelenmesi, ii. bağlantının sona erdirilmesi ve iii. şifre ile koruma sağlanması. Buna göre, tüm iletişimin incelenmesi, en başta genel izleme yükümlülüğü yasağına aykırı olduğundan; bağlantının sona erdirilmesi ise, internet erişimi sağlamaktan ibaret bir ekonomik faaliyet sürdüren bir hizmet sağlayıcının iş yapma özgürlüğüne ciddi bir müdahale teşkil edeceğinden çatışan hak ve menfaatler arasında adil bir denge sağlamamaktadır.⁶⁹¹ Şifre ile koruma ise, hak sahibinin fikri mülkiyetinin korunması hakkı, bir iletişim ağına erişim hizmeti sağlayan bir sağlayıcının iş yapma özgürlüğü ve kullanıcıların bilgi edinme özgürlüğü arasında adil bir denge sağlayabilecektir. ABAD, sevk eden Mahkeme gibi tek bir önlemin alınabileceği hallerde dahi, hizmet sağlayıcıların yükümlülüklerini yerine getirirken alacakları teknik önlemleri seçmekte özgür olduklarını kabul etmiştir.⁶⁹²

Hizmet sağlayıcıların söz konusu yükümlülükleri, E-Ticaret Direktifi'nin 15. maddesinde yasaklanan genel izleme yükümlülüğü ile sıkı bir ilişki içerisindedir. Zira, genel izleme yükümlülüğü yasağı, hizmet sağlayıcıların yükümlülüklerinin doğal bir sınırını teşkil etmektedir. Dolayısıyla, izleme yükümlülükleri bakımından hangi tedbirlerin meşru olup hangilerinin olmadığı konusunun açıklığa kavuşturulması gerekmektedir.

İzleme yükümlülüğü, kısaca, hizmet sağlayıcıların ilettikleri ya da depoladıkları bilgileri izlemeleri yükümlülüğünü ifade etmektedir. E-Ticaret Direktifi'nin 15. maddesi, Üye Devletlerin internet araçlarına, Direktifin 12-14. maddeleri kapsamındaki faaliyetlerle ilgili olarak, ilettikleri veya depoladıkları bilgileri izlemek için genel bir yükümlülük veya yasadışı faaliyetlere işaret eden olguları veya koşulları aktif olarak araştırmak için genel bir yükümlülük getirmesini engellemektedir.

E-Ticaret Direktifi'nde öngörülen genel izleme yasağı temel olarak beş nedene dayandırılmaktadır.⁶⁹³ Her şeyden önce, henüz emekleme aşamasında olan çevrimiçi

⁶⁹¹ Tobias Mc Fadden v Sony Music Entertainment Germany GmbH, para. 87-89.

⁶⁹² Tobias Mc Fadden v Sony Music Entertainment Germany GmbH, para. 101.

⁶⁹³ Toygar Hasan Oruc, "The Prohibition of General Monitoring Obligation for Video-Sharing Platforms under Article 15 of the E-Commerce Directive in Light of Recent Developments: Is It Still Necessary to

aracilar, hizmetleri aracılığıyla iletilen devasa bilgi miktarını aktif ve doğru bir şekilde izlemek için teknik kapasiteye sahip değildir. Ayrıca, çevrimiçi araçların, pasif faaliyetleri bakımından bu tür bir izleme yükümlülüğü altında bırakılması hakkaniyetli olmayacağı gibi; bu tür bir yükümlülük AB'de gelişmekte olan çevrimiçi ticaret sektörü üzerinde caydırıcı etki de yaratabilecektir. Öte yandan, genel izleme yükümlülüğü, araçların yasadışı içeriklerden haberdar olmalarını sağlayarak sorumluluk riskini de artıracaktır. Son olarak, bu yükümlülük kapsamında otomatik sistemlerin kullanılması ya da araçların sorumluluktan kaçınma eğilimiyle hareket etmesi meşru içeriklerin de aşırı engellenmesi riski taşımaktadır.⁶⁹⁴ Dolayısıyla, genel izleme yükümlülüğü yasağı, hizmet sağlayıcıların iş yapma özgürlüğü; internet kullanıcılarının ise ifade özgürlüğü⁶⁹⁵ ve kişisel verilerinin korunması hakları ile bağlantılıdır.

E- Ticaret Direktifi'nin 15. maddesinde yalnızca genel nitelikteki yükümlülüklerle ilişkin bir izleme yükümlülüğü yasaklandığından, bu madde hizmet sağlayıcılara belirli bir durumda izleme yükümlülüğü getirilmesine engel teşkil etmemektedir. Direktif'te izleme yükümlülüğüne ilişkin bu ayrıma yer verilmekle birlikte, meşru görülen ve görülmeyen bu yükümlülüklerin kapsamı açıklığa kavuşturulmamıştır. Bu belirsizlik nedeniyle, genel izleme yükümlülüklerinin özel izleme yükümlülüklerinden nasıl ayırt edileceği, başka bir ifadeyle internet şirketlerine hangi durumlarda izleme yükümlülüğü getirilebileceği sorusu ABAD tarafından ele alınmıştır.

ABAD E-Ticaret Direktifi'nin 15(1) maddesinin nasıl yorumlanacağı konusuna ilk kez 2011 yılındaki *L'Oréal v. eBay* kararında değinmiş ve 15. maddesi uyarınca, ilgili çevrimiçi hizmet sağlayıcısından istenen tedbirlerin, tüm müşterilerin bütün verilerinin aktif bir şekilde izlenmesini gerektirmemesi gerektiğini ortaya koymuştur. Daha sonra

Maintain It?", **Journal of Intellectual Property, Information Technology and Electronic Commerce Law**, C. 13, 2022, s. 178.

⁶⁹⁴ Toygar Hasan Oruç, "The Prohibition of General Monitoring Obligation for Video-Sharing Platforms under Article 15 of the E-Commerce Directive in Light of Recent Developments: Is It Still Necessary to Maintain It?", 2022, s. 179.

⁶⁹⁵ ABAD 2010'lu yıllarda, filtreleme sistemleri ile bağlantılı olarak, çevrimiçi olarak iletilen veya depolanan içeriğin izlenmesine yönelik genel bir yükümlülüğün, hukuka uygun içeriği engelleme potansiyeli dolayısıyla, ifade özgürlüğü ve bilgi edinme özgürlüğüne zarar verebileceğine dikkat çekmiştir. Evangelia Psychogiopoulou, "The CJEU as a Fundamental Rights Adjudicator in Social Media Cases", **Social Media, Fundamental Rights and Courts**, kitap editörü Evangelia Psychogiopoulou, Federica Casarosa London: Routledge, 2023, s. 27, doi:10.4324/9781003207085-3.

*Scarlet Extended*⁶⁹⁶ ve *Netlog*⁶⁹⁷ kararlarında, bu yasak daha kapsamlı şekilde ele alınmıştır

Mahkeme *Scarlet Extended* kararında, fikri mülkiyete konu elektronik dosyaların tanımlanması için hizmet sağlayıcılardan hizmetleri aracılığıyla geçen tüm elektronik iletişimleri filtrelemeleri için önleyici bir sistem kurmalarının istenmesinin genel izleme yasağına aykırı olduğu kabul ederken; *Netlog* kararında ise sosyal ağ platformlarının, müzikal ve sesli görsel çalışmaların yasadışı kullanımını önlemek için tüm kullanıcıları kapsayan genel bir filtreleme sistemi kurmasının gerekliliğini reddetmiştir.⁶⁹⁸

İçerik yönetimi ilişkin davalarda, temel mesele çatışan haklar arasında adil bir denge kurulmasıdır. *Scarlet Extended* ve *Netlog* kararlarında, aralarında denge kurulması gereken bu haklar hizmet sağlayıcıların iş yapma özgürlükleri, hak sahiplerinin fikri mülkiyet hakları ve kullanıcıların haklarıdır. Genel izleme yükümlülüğü yasağına aykırı olarak, hizmet sağlayıcılardan filtreleme sistemi kurmalarının beklenmesi, hizmet sağlayıcıların iş yapma özgürlüğünü ciddi bir şekilde ihlal edeceği gibi, kullanıcıların da çeşitli haklarına zarar verecektir. Filtreleme sisteminin kurulması, tüm içeriğin sistematik olarak analiz edilmesini ve ağdaki yasadışı içerikleri gönderen kullanıcıların IP adreslerinin toplanmasını ve tanımlanmasını gerektireceğinden, kişisel verilerin korunması hakkını ihlal edecektir. Öte yandan hukuka aykırı içerik ile hukuka uygun içerik arasında yeterli ayırım yapamama riski taşıyan bu sistemler, hukuka uygun iletişimin engellenmesine yol açarak potansiyel olarak bilgi edinme özgürlüğüne de zarar verebilecektir.⁶⁹⁹

Böylece ABAD, hizmet sağlayıcılara, (1) önleyici bir tedbir olarak; (2) masrafları yalnızca kendisine ait olmak üzere; (3) kullanıcılar arasında ayırım gözetmeksizin ve 4) sınırsız bir süre için; (5) sunucularında depolanan bilgileri filtreleyecek bir filtreleme

⁶⁹⁶ *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, Case C-70/10 (ECJ 24 Kasım 2011).

⁶⁹⁷ *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV*, Case C-360/10 (ECJ 16 Şubat 2012).

⁶⁹⁸ Rikke Frank Jørgensen vd., “ICT And Human Rights”, s. 14.

⁶⁹⁹ *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* para. 47-53; *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV*, para. 48-51.

sistemi kurmaya zorlanmasının genel izleme yükümlülüğü anlamına geleceğine ve AB hukuku ile uyumsuz olduğuna karar vermiştir.⁷⁰⁰

Bu yasak özel izleme yükümlülüğü ile ilgili olmadığı gibi hizmet sağlayıcıların proaktif davranışlar benimsemesini de engellememektedir. *L'Oréal v. eBay* kararında ABAD, ticari marka ihlallerine ilişkin olarak, çevrimiçi pazar yerinde, ihlal konusu ticari markaları taşıyan malların satışına yönelik genel ve kalıcı bir yasaklamanın söz konusu olamayacağını belirtirken; (1) aynı satıcı tarafından, (2) aynı markayla ilgili olarak ve (3) aynı türden daha fazla ihlalin önlenmesi için talimat verilebileceğini belirterek olaya özgü ve sınırlı özel izleme yükümlülüğünü kabul etmiştir.⁷⁰¹

*Glawischnig-Piesczek*⁷⁰² kararında, ABAD'ın, özel izleme yükümlülüğünün sınırlarını daha da genişlettiği görülmektedir. 2016 yılında Avusturya'da anonim bir Facebook kullanıcısının Avusturyalı bir siyasetçi olan Eva Glawischnig-Piesczek aleyhinde bir makale ve karalayıcı bir yorum paylaşmasıyla ortaya çıkan bu davada, ABAD tarafından yorumlanması beklenen hususlardan biri de Direktifin 15. maddesi uyarınca, bir yer sağlayıcıya karşı alınan tedbirin aynı ifadeler ve/veya eşdeğer içeriğe sahip beyanları kapsayıp kapsamayacağıdır.

Mahkeme, ilk olarak, E-Ticaret Direktifi, Resital 47'ye de atıfta bulunarak söz konusu yasağın yalnızca genel izleme yükümlülükleri için geçerli olduğunu açık bir şekilde ifade etmiştir:

*“Bu bağlamda, her ne kadar Madde 15(1) üye devletlerin ev sahibi sağlayıcılara ilettikleri veya depoladıkları bilgileri izlemek için genel bir yükümlülük veya yasadışı faaliyeti gösteren olguları veya koşulları aktif olarak araştırmak için genel bir yükümlülük getirmelerini yasaklasa da bu direktifin 47. maddesinden de anlaşılacağı üzere, böyle bir yasak 'belirli bir durumda' izleme yükümlülükleriyle ilgili değildir.”*⁷⁰³

⁷⁰⁰ Eleonora Rosati, “The Role, Responsibility and Liability of Online Intermediaries under EU IP Law”, **Handbook of Fashion Law**, Cahapter 7, 2024, s. 8.

⁷⁰¹ *L'Oréal SA and Others v eBay International AG and Others*, para. 141.

⁷⁰² *Eva Glawischnig-Piesczek v Facebook Ireland Limited*, Case C-18/18 (ECJ 03 Ekim 2019).

⁷⁰³ *Eva Glawischnig-Piesczek v Facebook Ireland Limited*, para. 34.

Mahkeme, daha sonra, 15. madde kapsamında yasaklanmayan özel izleme yükümlülüğünün, üye devlette yargı yetkisine sahip bir mahkeme tarafından incelenen ve değerlendirilen, değerlendirmeyi takiben yasadışı olduğu ilan edilen belirli bir bilgiye ilişkin olabileceğini belirtmiştir:

“Bir sosyal ağın, barındırma sağlayıcı tarafından depolanan bilgilerin farklı kullanıcıları arasında hızlı bir şekilde akışını kolaylaştırdığı göz önüne alındığında, yasadışı olduğu düşünülen bilgilerin daha sonra bu ağın başka bir kullanıcısı tarafından yeniden üretilmesi ve paylaşılması konusunda gerçek bir risk bulunmaktadır.

Bu koşullarda, söz konusu barındırma sağlayıcının ilgili menfaatlerin daha fazla zarar görmesini engellemesini sağlamak amacıyla, yargı yetkisine sahip mahkemenin, söz konusu barındırma sağlayıcıdan, içeriği daha önce yasadışı ilan edilen içerikle aynı olan depolanmış bilgilere erişimi engellemesini veya bu bilgilerin depolanmasını kimin talep ettiğine bakılmaksızın bu bilgileri kaldırmasını talep edebilmesi meşrudur. Özellikle, söz konusu bilgilerin içeriğinin aynı olduğu göz önünde bulundurulduğunda, bu amaçla verilen tedbir kararı, barındırma sağlayıcıya, depoladığı bilgileri genel olarak izleme yükümlülüğü veya 2000/31 sayılı Direktif’in 15(1) maddesinde öngörüldüğü üzere, yasa dışı faaliyeti gösteren olguları veya koşulları aktif bir şekilde araştırma yükümlülüğü getirdiği şeklinde değerlendirilemez.”⁷⁰⁴

ABAD’ın bu yaklaşımı, hukuka aykırı olduğuna karar verilen bir bilgi ile esasen aynı olmakla birlikte, kullanılan kelimeler veya bunların kombinasyonu nedeniyle farklı görünmesinin yol açabileceği riskin ortadan kaldırılabilmesi; başka bir ifadeyle yargı organları tarafından verilen hukuka aykırılık kararlarının etkisizleştirilmesinin önüne geçilmesi bakımından önemlidir. Aksi takdirde, hukuka aykırı içerik hakkındaki kararının etkileri, daha önce yasadışı ilan edilenlerden neredeyse hiç farklı olmayan mesajların saklanmasıyla kolayca aşılabılır ve bu da ilgili kişinin mağduru olduğu

⁷⁰⁴ Eva Glawischnig-Piesczek v Facebook Ireland Limited, para. 36,37.

davranışa son vermek için birden fazla dava başlatmak zorunda kalmasıyla sonuçlanabilir.⁷⁰⁵

Özel izleme yükümlülüğü, hizmet sağlayıcılara hukuka aykırı içerikle eşdeğer içerikte bilgileri izleme ve filtreleme yükümlülüğü de yükleyebilmektedir. Bu da eşdeğer bilginin ne olduğuna ilişkin önemli bir sorunu beraberinde getirmektedir. ABAD, bu noktada, menfaatler arasında denge kurulması gerekliliğine dikkat çekerek, özel izleme yükümlülüğü kapsamında barındırma sağlayıcılara aşırı yük getirilmemesi gerektiğini ifade etmektedir.⁷⁰⁶ Dolayısıyla, yetkili bir mahkeme tarafından eşdeğer içeriklere ilişkin bir karar verildiğinde; kararda, daha önce tespit edilen ihlalle ilgili kişinin adı, bu ihlalin tespit edildiği koşullar ve yasadışı olduğu ilan edilen içeriğe eşdeğer içerik gibi belirli unsurlara yer verilmesi önemlidir. Söz konusu eşdeğer içeriğin ifadelerindeki farklılıklar, yasadışı ilan edilen içerikle karşılaştırıldığında, her halükârda, ilgili yer sağlayıcının söz konusu içeriğe ilişkin bağımsız bir değerlendirme yapmasını gerektirecek şekilde olmamalıdır.⁷⁰⁷ Bu kararlar, hukuka aykırı içeriğin kolaylıkla yeniden üretilebilmesinin yol açacağı riskin azaltılması amaçlanmıştır. Öte yandan, eşdeğer içeriğin unsurları belirlenerek servis sağlayıcılara aşırı yük yüklemekten kaçınılmıştır.

Özel izleme yükümlülüğü, otomatik filtreleme sistemlerinin kullanılması gerektireceğinden, karar bu yönüyle ifade özgürlüğüne yönelik endişelere yol açmıştır. Teknolojinin mevcut durumu ve içerikler değerlendirilirken bağlamın dikkate alınması ihtiyacı göz önüne alındığında eşdeğer içerik tespitinin nasıl doğru bir şekilde yapılabileceği konusu belirsizliğini korumaktadır.⁷⁰⁸

Kişilik haklarını ihlal eden bir içerikle ilgili olarak genel izleme yükümlülüğü yasağının kapsamını daraltan bu içtihadın, telif haklarını ihlal eden içeriklere de uygulanıp uygulanamayacağı da tartışmaların başka bir boyutunu oluşturmaktadır. Bir görüşe göre, ABAD'ın, *Scarlet Extended* ve *Netlog* kararlarında, gelecekteki ihlallerin önlenmesi bağlamında önleyici izleme ele alınırken, tüm içeriğin izlenmesini gerektirecek böyle bir uygulamanın sorunlu olduğunun vurgulaması ve *Mc Fadden*

⁷⁰⁵ Eva Glawischnig-Piesczek v Facebook Ireland Limited, para. 41.

⁷⁰⁶ Eva Glawischnig-Piesczek v Facebook Ireland Limited, para. 44.

⁷⁰⁷ Eva Glawischnig-Piesczek v Facebook Ireland Limited, para. 45.

⁷⁰⁸ Frosio, Geiger, "Taking Fundamental Rights Seriously in the Digital Services Act's Platform Liability Regime", s. 39.

kararında da hizmet sağlayıcılar tarafından alınabilecek önlemlere ilişkin olarak tüm içeriğin izlenmesi seçeneğinin en baştan dışarıda bırakması, genel izleme yükümlülüğüne yönelik mevcut yorumun telif hakları söz konusu olduğunda uygulanmayacağını göstermektedir.⁷⁰⁹

Buna karşı çıkan diğer görüşe göre ise, belirli hak ihlallerini izleme yükümlülüğünü 'genel' izleme olarak kabul etmek, bu tür filtrelemeyi mümkün kılan teknolojik gelişmeleri göz ardı etmek ve AB yasama organını belirli yasadışı içerik türleriyle mücadele etmek için yararlı bir araçtan mahrum bırakılmak anlamına gelecektir. Oysa, Glawischnig kararıyla birlikte Mahkemenin genel izleme yükümlülüğü tanımı değişmiştir. Bu kapsamda, hizmet sağlayıcıların bağımsız bir değerlendirme yapmasını gerektirmeyecek “belirli” bir içeriğin izlenmesi özel izleme teşkil ettiğinden, telif haklarına ilişkin hak ihlallerinin önlenmesi için de otomatik filtreleme sistemleri kullanılabilecektir.⁷¹⁰

Hizmet sağlayıcılar tarafından otomatik filtreleme araçları kullanılması hususu, yakın zamanda *Republic of Poland v. Parliament and Council*⁷¹¹ davasında kapsamda bir şekilde ele alınmış ve çevrimiçi içerik paylaşım hizmeti sağlayıcıların, Dijital Tek Pazarda Telif Hakları Direktifi⁷¹² uyarınca, telif hakları ile korunan içeriğin korunması

⁷⁰⁹ João Pedro Quintais, Christina Angelopoulos, “YouTube and Cyando, Joined Cases C-682/18 and C-683/18 (22 June 2021): Case Comment (HvJ EU 22 Juni 2021, YouTube En Cyando)”, 2022, ss. 9-10.

⁷¹⁰ Opinion of Advocate General Saugmandsgaard Øe, “Republic of Poland v European Parliament and Council of the European Union. Action for annulment – Directive (EU) 2019/790 – Article 17(4), point (b), and point (c), in fine – Article 11 and Article 17(2) of the Charter of Fundamental Rights of the European Union – Freedom of expression and information – Protection of intellectual property – Obligations imposed on online content-sharing service providers – Prior automatic review (filtering) of content uploaded by users. Opinion of Advocate General Saugmandsgaard Øe delivered on 15 July 2021. Republic of Poland v European Parliament and Council of the European Union., Case C-401/19 (ECJ 2019), para. 111-115.

⁷¹¹ Republic of Poland v European Parliament and Council of the European Union, Case C-401/19 (ECJ 26 Nisan 2022). *Republic of Poland v. Parliament and Council* davası, bilgi toplumu hizmet sağlayıcılar arasında özel bir kategori teşkil eden çevrimiçi içerik paylaşım hizmeti sağlayıcılarının telif hakkı ile korunan içeriğin hukuka aykırı paylaşılmasından sorumluluğuna ilişkindir. ‘Çevrimiçi içerik paylaşım hizmeti sağlayıcı’ ana amacı veya ana amaçlarından biri kullanıcıları tarafından yüklenen, düzenlediği ve kâr elde amacıyla tanıttığı, büyük miktarda telif hakkı ile korunan eserler veya korunan bağlantılı hak konularını depolamak ve kamunun erişimine arz etmek olan bir bilgi toplumu hizmeti sağlayıcısıdır. Dijital Tek Pazarda Telif Hakları Direktifi’nin (2019/790) 17. maddesinde, bu nitelikteki hizmeti sağlayıcılara özel bir sorumluluk rejimi öngörülmüştür. Hizmet sağlayıcıların, hukuka aykırı içerikten sorumluluğunu genişleten bu düzenleme ifade özgürlüğünü daralttığı gerekçesiyle eleştirilmiştir.

⁷¹² Direktife göre, bir eserin hak sahibinin eserin paylaşılmasına ilişkin izninin olmadığı durumlarda çevrimiçi içerik paylaşım hizmeti sağlayıcılar, E-Ticaret Direktifinde de öngörülen hukuka aykırılığı bildirilen içeriğe erişimi engellemek veya içeriği kaldırmak için hızlı bir şekilde hareket etme yükümlülüğüne ek olarak; ayrıca bu içeriğin erişilemezliğini ve gelecekte yüklenmesini önlemek için yüksek endüstri mesleki özen standartlarına uygun olarak ellerinden gelen çabayı göstermeleri gerekmektedir. “Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019

bakımından, otomatik tanıma ve filtreleme sistemlerinin de kullanılmasını gerektirebilecek özel sorumluluk rejimine tabi kılınmalarını⁷¹³ ifade özgürlüğü açısından değerlendirmiştir. Mahkeme, AİHM içtihadına da atıfla, internetin “bireylerin ifade ve bilgi edinme özgürlüğü haklarını kullandıkları başlıca araç” haline geldiğini, bunun da “erişilebilirlik” ve “büyük miktarda bilgiyi depolama ve iletme kapasitesi” ile kolaylaştırıldığını vurgulamıştır.⁷¹⁴ Mahkeme ayrıca, bir ön inceleme ve ön filtreleme gerektirebilecek söz konusu rejimin, çevrimiçi içeriğin yayılmasına yönelik önemli bir aracı kısıtlayabileceğini ve dolayısıyla ifade özgürlüğüne yönelik bir sınırlama teşkil edebileceğini de kabul etmiştir. Bununla birlikte, ABAD’a göre, hizmet sağlayıcıların filtreleme sistemlerinin kullanmaya zorlanması, otomatik olarak ifade özgürlüğünü ihlal etmemektedir. Dolayısıyla, izin verilen ve verilmeyen filtreleme sistemlerinin birbirinden ayırt edilmesi önemlidir. Buna göre, bir filtreleme sisteminin ifade özgürlüğü ile bağdaştırılabilmesi için filtreleme sistemi, a. filtreleme sistemi yasadışı içeriği engellemek için tasarlanmalı, yasadışı ve yasal içerik arasında doğru bir şekilde ayırım yapabilmeli⁷¹⁵; b. bu sistem, yasadışı olmayan içerikleri yanlışlıkla engelleme riskini azaltmak için insan müdahalesine ihtiyaç duymamalı, otonom olarak karar verme yeteneğine sahip olmalı⁷¹⁶; c. kullanıcıların ifade ve bilgi edinme özgürlüklerini yasal içeriğin hatalı veya haksız bir şekilde engellediği durumlara karşı koruyan çeşitli usuli güvenceler sağlanmalı⁷¹⁷; d. hizmet sağlayıcıların, bu kapsamda, hizmet etkili ve hızlı şikayet ve telafi mekanizmaları oluşturmaları sağlanmalı⁷¹⁸ ve e. kullanıcıların, uyuşmazlıkların tarafsız bir şekilde çözülmesini sağlayan mahkeme dışı telafi

on Copyright and Related Rights in the Digital Single Market and Amending Directives 96/9/EC and 2001/29/EC”, (2019), <https://eur-lex.europa.eu/eli/dir/2019/790/oj>.

⁷¹³ Direktifin 17(4) maddesinde düzenlenen dava konusu düzenlemeye göre, çevrimiçi içerik paylaşım hizmeti sağlayıcıları; (a) Yetki almak için gerekli tüm çabayı gösterdiğini; (b) Telif hakkı sahiplerinin kendilerine sunduğu ilgili ve gerekli bilgilerle belirli eserlerin ve diğer materyallerin kullanılamamasını sağlamak için sektörün yüksek profesyonel özen standartlarına uygun olarak gerekli tüm çabayı gösterdiğini ve her durumda; (c) Hak sahiplerinden yeterince kanıtlanmış bir bildirim alındıktan sonra derhal harekete geçerek bildirilen eserlere veya diğer materyallere erişimi engellemek veya web sitelerinden kaldırmak için hızlı bir şekilde hareket ettiğini ve bunların gelecekte de yüklenmesini önlemek için (b) bendi uyarınca gerekli tüm çabayı gösterdiğini kanıtlamadıkları sürece, telif hakkı ile korunan eserlerin ve diğer materyallerin kamuya sunulması da dahil olmak üzere, kamuya izinsiz olarak iletilmesi eylemlerinden sorumlu olacaktır. Bu kapsamda, hizmet sağlayıcılar hak sahiplerinden yetki almak, bir yetki alınmamışsa içeriğin yayılmaması konusunda en iyi çabayı göstermekle yükümlüdür. Dolayısıyla 17. maddenin öngördüğü rejim; önce lisans, sonra filtre rejimi olarak tanımlanabilir. Husovec, “Mandatory Filtering Does Not Always Violate Freedom of Expression”, s. 176.

⁷¹⁴ Republic of Poland v European Parliament and Council of the European Union, ECJ 26 Nisan 2022, para. 46.

⁷¹⁵ Republic of Poland v European Parliament and Council of the European Union, para. 86.

⁷¹⁶ Republic of Poland v European Parliament and Council of the European Union, para. 90, 91.

⁷¹⁷ Republic of Poland v European Parliament and Council of the European Union, para. 93.

⁷¹⁸ Republic of Poland v European Parliament and Council of the European Union, para. 94.

mekanizmalarına ve etkili yargı yollarına erişimi sağlanmalıdır.⁷¹⁹ Sonuç olarak, 17. maddede öngörülen rejim varlığını sürdürse de geçerliliği, kullanıcılarının ifade ve bilgi edinme özgürlüğünü güvence altına alan güvencelerin sıkı bir şekilde uygulanmasına bağlıdır.⁷²⁰

Buna göre, önleyici otomatik filtreleme yalnızca yasadışı içeriği '*kesin olarak hedeflediğinde*' mümkündür. Yasal ve yasadışı içerikleri "*yeterince ayırt edemeyen*", filtreleme sistemleri diğer güvencelerin sağlanıp sağlanmadığına bakılmaksızın, güvenilir değildir. Dolayısıyla, kesin hedef prensibi, filtreleme sistemlerinin anayasallık sınırı olarak kabul edilebilir.

ABAD güncel kararlarında, hizmet sağlayıcıların hukuka aykırı içerikle ilgili yükümlülüklerini ele alırken "yüksek sektörel mesleki özen standartlarına" uygun olarak elinden gelen çabayı göstermeleri gerektiğinden bahsetmektedir. Bu değerlendirme, göz en iyi sektörel uygulamaların ve hizmetin büyüklüğü, gelecekteki potansiyel gelişmeler de dahil olmak üzere mevcut araçlara ilişkin olarak teknolojinin gelişen durumu ve hizmetler için bu tür araçların maliyeti gibi ilgili tüm gelişmelerin göz önünde bulundurulmasını gerektirmektedir. Bu kapsamda, hizmet sağlayıcılar tarafından atılacak her türlü adım, izlenen hedefler açısından etkili olmalı, ancak izinsiz eserlerin ve diğer konuların erişilebilirliğini önleme ve durdurma hedefine ulaşmak için gerekli olanın ötesine geçmemelidir.⁷²¹

Bu yapılırken, farklı hak ve menfaatler arasında internetin ifade ve bilgi edinme özgürlüğü açısından taşıdığı özel önem dikkate alınarak adil bir denge kurulması gerektiğini belirtmektedir.⁷²²

⁷¹⁹ Republic of Poland v European Parliament and Council of the European Union, para. 95.

⁷²⁰ João Pedro Quintais, "Between Filters and Fundamental Rights: How the Court of Justice saved Article 17 in C-401/19-Poland v. Parliament and Council", **Verfassungsblog**, 2022, <https://verfassungsblog.de/filters-poland/>, (12.10.2024).

⁷²¹ Republic of Poland v European Parliament and Council of the European Union, ECJ 26 Nisan 2022, para. 4.

⁷²² Frank Peterson v Google LLC and Others and Elsevier Incv Cyando AG, Joined Cases C-682/18 and C-683/18 (ECJ 22 Haziran 2021), para. 65.

2. Kişisel Veri Aktarımı

Genel Veri Koruma Tüzüğü'nün 44-50. maddelerinde, sınır ötesi veri akışlarına ilişkin kapsamlı düzenlemelere yer verilmiştir. Buna göre, AB içerisinde toplanan kişisel verilerin üçüncü ülkelere aktarımı; ancak aktarımın yapılacağı ülkede yeterli düzeyde korumanın sağlanması koşuluyla yapılabilecektir.

ABAD 2015 yılında *Schrems*⁷²³ davasında bu konuda önemli bir karar vermiştir. Dava, bir AB vatandaşının, Edward Snowden'ın ABD istihbarat servislerinin faaliyetlerine ilişkin ifşaatlarının ardından, İrlanda Veri Koruma Otoritesine şikâyetle bulunması ve bu şikâyetin reddedilmesi sonrasında İrlanda Yüksek Mahkemesi tarafından ABAD'a ulaşmıştır. Bu kapsamda ABAD, ABD-AB arasında veri aktarımını konu alan "Güvenli Liman" Kararının⁷²⁴ ve Facebook'un İrlanda'daki yan kuruluşu tarafından ABD'de bulunan sunuculara veri aktarımının Veri Koruma Direktifi⁷²⁵ ile uyumlu olup olmadığına karar vermek durumundaydı. Mahkeme, 'yeterli düzeyde koruma' kavramının bir tanımının bulunmadığına dikkat çekmekle birlikte; bu koruma düzeyinin, temel hak ve özgürlüklerin AB içinde güvence altına alınana eşdeğer düzeyde korunmasını gerektirdiğini belirtmiştir.⁷²⁶ Bu prensip göz önünde bulundurularak yapılan değerlendirmede, özel hayata saygı temel hakkının AB düzeyinde korunmasının, kişisel verilerin korunmasına ilişkin istisnaların ve sınırlamaların yalnızca kesinlikle gerekli olduğu sürece uygulanmasını gerektirdiğine⁷²⁷; oysa Güvenli Liman Kararı'nda, ulusal güvenlik, kamu yararı veya kolluk kuvvetleri tarafından gerekçelendirilen ve veri kaygılarına üstün gelen müdahalelere izin verildiği⁷²⁸ tespit edilmiştir. Böylece Mahkeme, söz konusu Güvenli Liman Kararı'nı geçersiz kılmıştır.

⁷²³ Maximillian Schrems v Data Protection Commissioner, Case C-362/14 (ECJ 06 Ekim 2015).

⁷²⁴ "Commission Decision of 26 July 2000 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the Safe Harbour Privacy Principles and Related Frequently Asked Questions Issued by the US Department of Commerce", European Commission, <https://www.europeansources.info/record/2000-520-ec-commission-decision-of-26-july-2000-pursuant-to-directive-95-46-ec-of-the-european-parliament-and-of-the-council-on-the-adequacy-of-the-protection-provided-by-the-safe-harbour-privacy-pri/>, (12.10.2024).

⁷²⁵ 95/46/EC sayılı Veri Koruma Direktifi, Genel Veri Koruma Tüzüğü ile yürürlükten kaldırılmıştır; ancak Genel Veri Koruma Tüzüğünde olduğu gibi, Veri Koruma Direktifinin 25. maddesinde de üçüncü ülkede yeterli güvencelerin sağlanması koşuluyla veri aktarımı yapılabileceği belirtilmektedir.

⁷²⁶ Maximillian Schrems v Data Protection Commissioner, para. 73-74.

⁷²⁷ Maximillian Schrems v Data Protection Commissioner, para. 92.

⁷²⁸ Maximillian Schrems v Data Protection Commissioner, para. 86.,

Güvenli Liman Kararı'nın iptal edilmesinin ardından ortaya çıkan boşluk ve belirsizlik yeni bir düzenleme ihtiyacı ortaya çıkarmış ve 2016 yılında, ABD ve AB "Avrupa-ABD Gizlilik Kalkanı" (*Privacy Shield*) adlı yeni bir veri aktarım mekanizması üzerinde anlaşmıştır.⁷²⁹ Veri koruma aktivisti Schrems, "Gizlilik Kalkanı" veri aktarım mekanizmasının da AB veri koruma standartlarını karşılamadığını ve Avrupalıların verilerinin ABD'de Ulusal Güvenlik Ajansı (NSA) tarafından gözetim altında tutulabileceğini ileri sürmüş ve dava yeniden ABAD'ın önüne gelmiştir.⁷³⁰ Bu kapsamda ABAD, Gizlilik Kalkanı'nın GDPR'a uygun olup olmadığını incelemiştir. Buna göre, Gizlilik Kalkanı, ABD'ye aktarılan veriler için yeterli düzeyde koruma sağlasa da ulusal güvenlik ve kamu yararı gereklerine veya Amerika Birleşik Devletleri'nin iç mevzuatına dayalı olarak temel haklara müdahaleye olanak sağlamaktadır.⁷³¹

ABAD'a göre, eşdeğerlik testinde, veri aktarımına ilişkin olarak, orantılılık kriterinin ve GDPR'ın 45(2)(a) maddesi uyarınca bireylerin etkili denetim yollarına başvuru ile idari ve adli tazminat talep etme haklarının da göz önünde bulundurulması gerekmektedir.

Kişisel verilerin korunmasına ilişkin olarak orantılılık kriteri, kişisel verilerin korunmasına ilişkin istisnaların ve sınırlamaların yalnızca kesinlikle gerekli olduğu ölçüde uygulanması anlamına gelmekte ve müdahaleyi gerektiren mevzuatın, ilgili tedbirin kapsamını ve uygulanmasını düzenleyen ve asgari güvenceler getiren açık ve kesin kurallar koymasını gerektirmektedir. Özellikle, bu tür verilerin işlenmesini öngören bir tedbirin hangi durumlarda ve hangi koşullar altında kabul edilebileceği belirtilmeli ve böylece müdahalenin kesinlikle gerekli olanla sınırlı kalması sağlanmalıdır. Kişisel verilerin otomatik işleme tabi tutulduğu durumlarda bu tür güvencelere duyulan ihtiyaç daha da artmaktadır.⁷³² Gizlilik Kalkanı, istihbarat amacıyla toplu gözetim konusunda

⁷²⁹ "Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the EU-U.S. Privacy Shield (Notified under Document C(2016)4176) (Text with EEA Relevance)", (2016), http://data.europa.eu/eli/dec_impl/2016/1250/oj/eng, (12.10.2024).

⁷³⁰ Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, Case C-311/18 (ECJ 16 Temmuz 2020).

⁷³¹ Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, para. 163-165.

⁷³² Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, para. 176.

açık ve kesin kurallar içermediği için orantılılık kriteri bakımından eşdeğer bir koruma düzeyi sağlamamaktadır.⁷³³

ABAD, veri aktarımına ilişkin değerlendirmede, etkili idari ve adli giderimin var olup olmadığının belirlenmesinin özellikle önemli olduğunu işaret etmektedir. Zira, GDPR'ın 116. maddesinden de anlaşılacağı üzere, veri sahipleri, üye devletlerin idari ve adli makamlarının, veri sahiplerinin bu şekilde aktarılan verilerinin söz konusu üçüncü ülkede hukuka aykırı olarak işlendiği iddiasına dayanan şikayetlerini ele almada yetersiz olduğunu görebilir ve bu da onları söz konusu üçüncü ülkenin ulusal makamlarına ve mahkemelerine başvurmak zorunda bırakabilir. Kararda Gizlilik Kalkanı'nda, bir ombudsmanlık mekanizmasına yer verilmiş olduğu belirtilmişse de bu kurumun yürütmeden bağımsız ve bağlayıcı karar alma yetkisine sahip olmaması dolayısıyla etkili bir giderim sağlamadığı kabul edilmiş⁷³⁴ ve Güvenli Liman Kararı gibi, Gizlilik Kalkanı kararının da geçersiz olduğuna hükmedilmiştir.

ABAD'ın, ABD'deki koruma seviyelerinin AB'de mevcut olanlarla eşleşmediğine ilişkin bu tespitleri, internet şirketlerinin veri aktarımına ilişkin sorumluluklarını doğrudan etkilemektedir. Buna göre, iki ülke arasında veri taşıyan internet şirketleri tarafından bu koşullar altına veri aktarımı yapılması AB hukukunu ihlal edeceğinden, İnternet şirketlerinin veri aktarımının yasal ve adil bir şekilde gerçekleştiğini ve veri sahiplerinin haklarının korunmasını sağlamak için daha fazla sorumluluk almalarını gerekmektedir.

3. Unutulma Hakkı

Unutulma hakkı, bir birey tarafından geçerli bir talepte bulunulması halinde kişisel verilerin arama motoru sonuçlarından kaldırılması hakkını ifade etmektedir. GDPR'da her ne kadar silme hakkı (*right to erasure*) ile aynı anlama gelecek şekilde kullanılsa da, Avrupa Birliği Adalet Divanı tarafından silme hakkından türetilen bu hak

⁷³³ Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, para. 180.

⁷³⁴ Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, para. 195.

diğerinden verinin silinmesi değil görünmez hale getirilmesini konu alması bakımından farklılaşmaktadır.⁷³⁵

GDPR'ın "silme hakkı" başlıklı 17. madde başlığında, parantez içerisinde unutulma hakkına yer verilse de bu maddede yalnızca silme hakkı düzenlenmiştir. Unutulma hakkı, GDPR'nin öncülü olan AB Veri Koruma Direktifi kapsamındaki silme hakkının ABAD tarafından Google İspanya v. AEPD davasında⁷³⁶ yorumlanmasıyla ortaya çıkmıştır.

Bir İspanyol vatandaşı, ismiyle arama yapıldığında, arama sonuçlarında 16 yıl önceki sosyal güvenlik borçlarının tahsili için yapılan işlemlerle bağlantılı bir gayrimenkul ihalesine atıfta bulunan iki gazete makalesinin çıkmasına ilişkin bu dava öncesinde, başvuru ilgili gazete ve Google İspanya aleyhine İspanyol Veri Koruma Kurumu'na (AEPD) şikâyetle bulunmuştur. Bunun üzerine AEPD, söz konusu bilgilerin yayınlanmasının hukuka uygun olduğu görüşünü benimsemiş ve gazete ile ilgili şikâyeti reddederken Google İspanya ve Google Inc.'ye yönelik şikâyeti kabul etmiştir. Google Inc.'nin bu karara karşı ulusal yüksek mahkemede itiraz etmesi üzerine, Yüksek Mahkeme Avrupa Hukuku'nun yorumlanmasının davanın karara bağlanmasıyla ilgili olduğunu tespit etmiş ve davayı ABAD'a havale etmiştir.

ABAD, arama motoru faaliyetlerinin, arama motoru tarafından değiştirilip değiştirilmediği sorusundan bağımsız olarak, 95/46 sayılı Avrupa Veri Koruma Direktifi hükümleri kapsamında "kişisel verilerin işlenmesi" teşkil ettiğine karar vermiştir. ABAD'a göre arama motoru operatörü, kişisel verilerin bu şekilde işlenmesi bakımından bir "kontrolör"dür.⁷³⁷ ABAD, kontrolör tarafından kişisel verilerin işlenmesinin, kontrolörün bir üye devlet topraklarındaki bir kuruluşunun "faaliyetleri bağlamında" gerçekleştirilmesi halinde, Avrupa Veri Koruma Kanunu'nun, Avrupa Birliği (AB) dışında bulunan kuruluşlar için de geçerli olduğunu açıklamıştır.

⁷³⁵ Daniel J. Solove, "The Limitations of Privacy Rights", *Notre Dame Law Review*, C. 98, S. 3, 2022, s. 982.

⁷³⁶ Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, Case C-131/12 (ECJ 13 Mayıs 2014).

⁷³⁷ Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, para. 32.

Google v. İspanya davasında, veri işleme, yani üçüncü taraflara ait web sitelerinin bilgi veya verilerinin indekslenmesi ve depolanması, Google İspanya'nın ana şirketi olan ABD merkezli Google Inc. tarafından gerçekleştirilmiştir.⁷³⁸ Arama sonuçlarının bireyler üzerindeki etkisi, şirketlerin ekonomik menfaatleri, internet kullanıcılarının bilgi edinme hakları gibi çatışan farklı menfaatleri göz önünde bulunduran ABAD, bu menfaatlerin çeşitli kriterler ışığında ele alınması gerektiği sonucuna varmıştır:

“Bu müdahalenin potansiyel ciddiyeti ışığında, bu tür bir motorun operatörünün bu işlemde sahip olduğu ekonomik çıkarla gerekçelendirilemeyeceği açıktır. Bununla birlikte, bağlantıların sonuç listesinden çıkarılmasının, söz konusu bilgilere bağlı olarak, bu bilgilere erişmekle potansiyel olarak ilgilenen internet kullanıcılarının meşru menfaatleri üzerinde etkileri olabileceğinden, ana davada söz konusu olan gibi durumlarda, özellikle bu menfaat ile veri sahibinin Şart'ın 7. ve 8. maddeleri kapsamındaki temel hakları arasında adil bir denge aranmalıdır. Veri sahibinin bu maddeler tarafından korunan haklarının, genel bir kural olarak, internet kullanıcılarının bu menfaatini geçersiz kıldığı doğru olmakla birlikte, bu denge, belirli durumlarda, söz konusu bilginin niteliğine ve veri sahibinin özel hayatı için hassasiyetine ve kamunun bu bilgiye sahip olma menfaatine, özellikle de veri sahibinin kamu hayatında oynadığı role göre değişebilen bir menfaate bağlı olabilir.”⁷³⁹

Buna göre unutulma hakkı, verilerin yetersiz, ilgisiz veya aşırı olduğu durumlarda, arama motorlarının üçüncü taraf web sayfalarına bağlantıları kaldırmasını gerektirmektedir. Bu hak verilerin silinmesini gerektirmediğinden verilerin yer aldığı web siteleri ya da arama motorları bu verileri silmek değil; kişilerin isimlerine yönelik arama sonuçlarında ifşa etmemekle yükümlüdür. Arama motorlarının bu yükümlülüğü, veri sahipleri ve internet kullanıcılarının yarışan hak ve menfaatleri arasında denge kurulmasını gerektirmektedir. Kural olarak, veri sahibinin Şart'ın 7. ve 8. maddeleri ile korunan hakları, internet kullanıcılarının meşru menfaatlerine üstün gelse de, bu dengenin özellikle de bilginin niteliği, veri sahibinin özel hayatı açısından hassasiyeti, kamunun bu bilgiye sahip olma menfaati, veri sahibinin kamu hayatında oynadığı rol gibi her

⁷³⁸ Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, para. 46.

⁷³⁹ Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, para. 81.

bir vakanın ilgili koşullarına bağlı olabileceği belirtilmelidir.⁷⁴⁰ Bu kapsamda, veri sahibinin kamu hayatında bir rol oynadığı durumlarda, ifade ve bilgi edinme özgürlüğü hakkı, özel hayat ve kişisel verilerin korunması haklarının önüne geçebilirken; bu ilişki, en azından, referansın kaldırılması talebinde atıfta bulunulan bilgilerin bir kısmının - bir bütün olarak içerikle ilgili olarak önemsiz olmayan - yanlış olduğunun kanıtlandığı durumlarda her halükarda tersine dönmektedir. Böyle bir durumda, bilgilendirme hakkı ve bilgilendirilme hakkı dikkate alınamaz, çünkü bu tür bilgileri yayma ve bu bilgilere erişme hakkını içeremezler.⁷⁴¹

Unutulma hakkının kapsamı içeriğe referans veren bağlantının kaldırılmasıyla sınırlı değildir. Bu hak, ayrıca, makaleyi gösteren küçük resimler şeklinde görüntülenen fotoğrafların kaldırılmasını da gerektirebilmektedir. İfade ve haber alma özgürlüğü şüphesiz fotoğrafların yayınlanmasını da kapsamakla birlikte, fotoğraflar bir kişi veya ailesi hakkında özellikle kişisel ve hatta mahrem bilgileri aktarabildiğinden, özel hayatın gizliliğinin korunması bu bağlamda özel bir önem kazanmaktadır. Ayrıca, ilgili kişiye ilişkin internette bulunan tüm bilgiler isme göre yapılan bir aramada toplanabileceğinden, küçük resimler daha yoğun bir müdahaleye yol açabilecektir.⁷⁴²

Bu doğrultuda, bir arama motoru operatörü, bir kişinin adı temelinde gerçekleştirilen bir görsel aramanın sonuçlarından, o kişiyi temsil eden küçük resimler şeklinde görüntülenen fotoğrafların kaldırılmasını isteyen bir talep aldığında, söz konusu fotoğrafların görüntülenmesinin internet kullanıcılarının bilgi edinme özgürlüğü hakkının kullanılması için gerekli olup olmadığını tespit etmelidir. Bu kapsamda, arama sonuçlarında görüntülenen küçük resim biçimindeki fotoğrafların, alındığı internet sitesinde yayınlanma bağlamından bağımsız şekilde ele alınması gerekmektedir.⁷⁴³

Arama sonuçlarında görüntülenen küçük resim biçimindeki fotoğraflar metinli veya metinsiz olabilir. Her iki durumda da, arama motoru operatörü, bu fotoğrafların görüntülenmesinin bilgi edinme özgürlüğü hakkının kullanılması için gerekli olup

⁷⁴⁰ TU and RE v Google LLC, Case C-460/20 (ECJ 08 Aralık 2022) para. 64, 65; Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, ECJ 13 Mayıs 2014, para. 66.

⁷⁴¹ TU and RE v Google LLC, ECJ 08 Aralık 2022, para. 64, 65.

⁷⁴² TU and RE v Google LLC, para. 104.

⁷⁴³ TU and RE v Google LLC, para. 104.

olmadığını ve kamu yararına ilişkin bir tartışmaya katkıda bulunup bulunmadığını tespit etmek için, birbiriyle çatışan hak ve menfaatleri ayrı ayrı tartmalıdır.⁷⁴⁴ Böylece, herhangi bir içeriğe referans veren bağlantının kaldırılması talebinin ifade özgürlüğünün üstün gelmesi gerekçesiyle reddedilmesi, otomatik olarak küçük resim şeklindeki fotoğrafların kaldırılması talebinin reddini de gerektirmemektedir. İkincisi hakkındaki karar, resimlerin kamuoyunu bilgilendirici niteliğine göre değişebilecektir. Buna karşın, içeriğe referans veren bağlantının kaldırılması talebinin kabul edilmesi halinde, bu makalede yer alan fotoğrafların küçük resimler şeklinde gösterilmesinin kaldırılması gerekmektedir. Aksi takdirde, internet kullanıcıları, küçük resimlerde yer alan ve küçük resimlerin alındığı makalenin yayınlandığı internet sayfasına yönlendiren bağlantı sayesinde makalenin tamamına erişmeye devam edeceğinden, içeriğe referans veren bağlantının kaldırılmasının pratik etkisi kalmayacaktır.⁷⁴⁵

ABAD, unutulma hakkına ilişkin içtihadında, bu hakkın coğrafi kapsamını da açıklığa kavuşturmuştur. Fransız Danıştay'ı tarafından ABAD'ın önüne getirilen bir davada⁷⁴⁶ Mahkeme unutulma hakkının coğrafi sınırlarının belirlenmesi sorununa odaklanmıştır. Davanın çıkış noktası, Google'ın unutulma hakkı kapsamında, Avrupa'daki kullanıcıların liste dışı bırakılan URL'leri görmelerini engelleyen bir coğrafi engelleme özelliği uygulamaya koyması, yani URL'leri dünyanın kalanı için arama sonuçlarında görünür bırakması üzerine Fransız Veri Koruma Otoritesi (CNIL) tarafından 100.000 Euro para cezasına mahkûm edilmesidir. ABAD, davayı hem 2018 yılında yürürlükten kaldırılan AB Veri Koruma Direktifi hem de GDPR ışığında analiz etmiştir.

Bu davada ABAD tarafından ele alınan temel sorun, veri koruma mevzuatının unutulma hakkı kapsamında bir URL'nin liste dışı bırakılmasına karar verildiğinde bunun dünya çapında veya AB içinde ya da yalnızca ulusal düzeyde uygulanmasını gerektirecek şekilde yorumlanıp yorumlanmayacağıdır. Buna göre, dünya çapında uygulama URL'nin arama motorunun tüm sürümlerinden kaldırılmasını, AB ile sınırlı uygulama tüm Üye Devletlere karşılık gelen sürümlerinden kaldırılmasını ve ulusal uygulama ise yalnızca

⁷⁴⁴ TU and RE v Google LLC, para. 98-101.

⁷⁴⁵ TU and RE v Google LLC, para. 106, 107.

⁷⁴⁶ Google LLC, successor in law to Google Inc v Commission nationale de l'informatique et des libertés (CNIL), Case C-507/17 (ECJ 24 Eylül 2019).

talep eden kişinin ikamet ettiği üye devlete karşılık gelen versiyondan kaldırılmasını gerektirecektir.⁷⁴⁷

24 Eylül 2019 tarihinde ABAD, Direktif ve GDPR metinleri ile AB yasama organının arama motoru operatörlerine AB sınırlarını aşan bir yükümlülük getirmeyi amaçlamadığını belirterek arama motoru operatörlerinin, AB hukuku kapsamında arama motorunun dünya çapındaki tüm versiyonlarındaki bağlantıları kaldırmasının gerekmediğine⁷⁴⁸ karar vermiştir.⁷⁴⁹ Bununla birlikte kararda arama motorlarının, bir URL'nin arama sonuçlarından kaldırılmasına karar verdiklerinde bunu, hangi Üye Devletten geldiği fark etmeksizin, AB'deki tüm sürümlerden kaldırmaları gerektiğinin altı çizilmiştir.⁷⁵⁰

Kararda bilgiye erişimdeki kamu çıkarının üçüncü devletler arasında önemli ölçüde farklılık gösterdiğinden temel hakların dengelenmesi farklı ülkelerde farklı sonuçlara yol açabileceği belirtilerek küresel uygulamanın doğasında var olan zorluklara da dikkat çekilmiştir. Dolayısıyla, ABAD'ın unutulma hakkını coğrafi olarak sınırladığı bu karar, AB üyesi olmayan ülkelerin hukuk sistemlerine saygının dışa vurumu niteliğindedir.⁷⁵¹ Bununla birlikte, küresel uygulamanın yasaklanmadığının ve gerekli hallerde üye devletlerin yetkili kurumlarının arama motorlarından, İlgili URL'nin arama motorunun tüm sürümlerinden kaldırmaları yönünde talepte bulunabileceğinin de altını çizmek gerekmektedir. Ancak bunu için, veri sahibinin mahremiyet hakkı ve kendisiyle ilgili kişisel verilerin korunması hakkı ile bilgi edinme özgürlüğü hakları arasında bir denge kurulması gerekmektedir.⁷⁵²

⁷⁴⁷ Google LLC, successor in law to Google Inc v Commission nationale de l'informatique et des libertés (CNIL), para. 43.

⁷⁴⁸ Mahkeme, AB hukukunun küresel uygulamayı gerektirmediğini açıklarken, bunu yasaklamadığının da altını çizmiştir. Böylece, Üye devletlere istisnai hallerde de olsa küresel uygulama konusunda açık kapı bırakılmıştır. Google LLC, successor in law to Google Inc v Commission nationale de l'informatique et des libertés (CNIL), para. 72.

⁷⁴⁹ Google LLC, successor in law to Google Inc v Commission nationale de l'informatique et des libertés (CNIL), para. 62.

⁷⁵⁰ Google LLC, successor in law to Google Inc v Commission nationale de l'informatique et des libertés (CNIL), para. 73.

⁷⁵¹ Mary Samonte, "Google v. CNIL: The Territorial Scope of the Right to Be Forgotten Under EU Law", **European Papers - A Journal on Law and Integration**, C. 2019 4, S. 3, 2020, s. 844, doi:10.15166/2499-8249/332.

⁷⁵² Google LLC, successor in law to Google Inc v Commission nationale de l'informatique et des libertés (CNIL), para. 72, 73.

Unutulma hakkı bakımından gündeme gelen bir başka belirsizlik de söz konusu başvurular bakımından ispat yükünün hangi tarafta olduğuna ilişkindir. Unutulma hakkı başvurularının usulünü de etkileyen bu husus ABAD tarafından yakın zamanda ele alınmıştır.⁷⁵³

Bu kapsamda, unutulma hakkı talebinde bulunan kişiden bilgilerin yanlış olduğunu ispat etmek amacıyla, içeriği barındıran sitenin yayıncısı aleyhine verilmiş bir adli kararı ibraz etmesinin istenip istenemeyeceği; arama motoru sağlayıcısının bu yükümlülüğü yerine getirmesi için başvurucunun ilgili URL'lerin haksız olduğunu ileri sürmesinin yeterli olup olmayacağı; arama motoru sağlayıcısının, bilgilerin doğru olup olmadığını belirlemek amacıyla gerekli adımları atmasının gerekip gerekmeyeceği sorularına cevap aranmıştır.⁷⁵⁴ ABAD, başvurucudan adli bir karar talep edilmesinin başvurucuya; gerekli araştırmaları yapma şeklinde aktif bir rol oynama yükümlülüğünün ise arama motoru sağlayıcısına makul olmayan bir yük getireceğini belirtmiştir. Arama motoruna böyle bir yük yüklenmesi ayrıca, doğru olup olmadığını tespit etmek amacıyla gerçekleri araştırma yükünü üstlenmek zorunda kalmamak için bağlantıların sistematik olarak kaldırılması riski de taşımaktadır. Bu da ifade ve bilgi edinme özgürlüğünün kullanılması üzerinde caydırıcı bir etki yaratabilecektir.⁷⁵⁵ Dolayısıyla, ilgili bağlantının haksızlığını kanıtlama yükümlülüğü, unutulma hakkı talebinde bulunan kişiye aittir. Bu bağlamda, referansın kaldırılmasını talep eden kişiden *"yalnızca, belirli bir davanın koşullarının ışığında, kendisinden bu açık yanlışlığı tespit etmek için bulmaya çalışmasının makul olarak istenebileceği kanıtları sunması"* talep edilebilir:

“İlk olarak, atıfta bulunulan içeriğin yanlış olması nedeniyle referansın kaldırılmasını talep eden kişinin yükümlülüklerine ilişkin olarak, söz konusu içerikte bulunan bilgilerin veya en azından bu bilgilerin bir bütün olarak içerikle ilgili olarak önemsiz olmayan bir kısmının açıkça yanlışlığını ortaya koymak bu kişinin görevidir. Ancak, söz konusu kişiye, kaynak gösterme hakkının pratikteki etkisini zayıflatabilecek aşırı bir yük yüklemekten kaçınmak için, söz konusu kişi yalnızca, somut davanın koşulları ışığında, söz konusu açık yanlışlığı

⁷⁵³ TU and RE v Google LLC, Case C-460/20 (ECJ 08 Aralık 2022).

⁷⁵⁴ Garrigues-Ángela López Cárcel, “Right to Be Forgotten: Developments with Regard to de-Referencing in the Light of Inaccurate Information”, **Lexology**, 26.01.2023, <https://www.lexology.com/library/detail.aspx?g=d63e8758-1ffc-4273-a767-5ca772642d3b>, (23.12.2024).

⁷⁵⁵ TU and RE v Google LLC, ECJ 08 Aralık 2022 para. 70, 71.

tespit etmek için kendisinden makul olarak bulması istenebilecek kanıtları sunmalıdır. Bu bağlamda, söz konusu kişiden, prensip olarak, dava öncesi aşamadan itibaren, arama motorunun operatörüne yaptığı referansın kaldırılması talebini desteklemek üzere, söz konusu web sitesinin yayıncısı aleyhine verilmiş bir yargı kararını, ara yargılamada verilmiş bir karar şeklinde bile olsa, sunması istenemez. Söz konusu kişiye böyle bir yükümlülük yüklemek, kendisine makul olmayan bir yük yüklemek anlamına gelecektir.”⁷⁵⁶

Buna göre, başvurucunun, bilginin açıkça yanlış olduğunu kanıtlayabilecek ve referans verilen içerikte bulunan bilgilerin veya en azından bu bilgilerin bir bütün olarak içerikle ilgili olarak önemsiz olmayan bir kısmının açıkça yanlışlığını ortaya koyabilecek ilgili ve yeterli kanıt sunması halinde arama motoru sağlayıcısı unutulma hakkı talebini kabul etmekle yükümlüdür. Aynı durum, veri sahibinin web sitesinin yayıncısına karşı, atıfta bulunulan içerikte bulunan ve içeriğin bütünüyle ilgili olarak önemsiz olmayan bilgilerin en azından ilk bakışta yanlış olduğu bulgusuna dayanan bir yargı kararı sunması halinde de geçerlidir.⁷⁵⁷

Sonuç olarak, unutulma hakkı kapsamında internet şirketleri, veri sahibinin korunan hakları ile internet kullanıcılarının meşru menfaatleri arasında denge kurmak ve ilkinin üstün geldiği hallerde unutulma hakkı taleplerini kabul ederek kişisel verilerin yer aldığı bağlantıları arama sonuçlarından kaldırmakla yükümlüdür. Başvurucunun bağlantıda yer alan bilginin açıkça yanlış olduğunu kanıtlanması halinde; bu tür bilgilere erişme ve bunları yayma hakları korunmayacağı, başka bir ifadeyle veri sahibinin hakları karşısında internet kullanıcılarının korunan bir menfaati söz konusu olmayacağı için unutulma hakkı talebinin kabul edilmesi gerekmektedir. İnternet şirketleri, bu taleplerle ilgili olarak herhangi bir araştırma ya da delil toplama yükümlülüğü altında değildir; gerekli bilgi ve belgeler başvuru tarafından sunulmalıdır. Son olarak, unutulma hakkının uygulanması bakımından şirketler, kural olarak üye devletlerle sınırlı olarak bağlantıları arama sonuçlarından çıkarmakla yükümlüdür. Yine de belli durumlarda, istisnai olarak, hakkın küresel olarak uygulanması da gündeme gelebilecektir.

⁷⁵⁶ TU and RE v Google LLC, para. 68.

⁷⁵⁷ TU and RE v Google LLC, para. 72.

ÜÇÜNCÜ BÖLÜM

TÜRK HUKUKUNDA İNTERNET ŞİRKETLERİNE İLİŞKİN MEVCUT HUKUKİ ÇERÇEVE VE ÖNERİLER

Türkiye’de otuz bir yıl önce başlayan internet kullanımından bu yana, internetin kullanım amaçları git gide çeşitlenmiş, kullanıcı sayısı ise hızla artmıştır. Özellikle, 2010’lu yıllarda sosyal medya kullanımının artmasıyla, internet günlük hayatın vazgeçilmez bir parçası haline gelmiştir.

2024 yılı itibariyle, Türkiye’de nüfusun yüzde 86,5’i internet kullanmakta ve günün 7 saat 6 dakikasını internette geçirmektedir. Ayrıca, aktif sosyal medya kullanıcı sayısı nüfusun yüzde 67,4’üne; sosyal medyada geçirilen süre ise 2 saat 36 dakikaya ulaşmıştır.⁷⁵⁸ Dünya geneline bakıldığında bu oranlar ortalamanın üzerinde kalmaktadır.⁷⁵⁹ Türkiye’de kullanıcılar tarafından en çok tercih internet sitelerine bakıldığında, 57.5 milyon kullanıcı sayısı ile Youtube ilk sırada gelmektedir. Youtube’u 57.1 milyon ile Instagram, 37.73 milyon ile Tiktok, 34.35 milyon ile Facebook ve 20.67 kullanıcı sayısı ile X takip etmektedir.⁷⁶⁰

İnternet kullanımının gittikçe yaygınlaşması ve ülkemizde neredeyse herkesin interneti an azından bir amaçla kullanır hale gelmesi internetin hukuken ele alınış biçimini de etkilemiştir. Günümüzde internet, haberleşme özgürlüğü, düşünce ve ifadeyi yayma özgürlüğü, iktisadi girişim hürriyeti, eğitim ve öğrenim hakkı başta olmak üzere Anayasa’da tanımlı birçok hak ve hürriyetin kullanılması noktasında araçsallaştırılmıştır. Bu küresel ortam, aynı zamanda, nefret söylemi ya da çocuk pornografisinin yayılması, şiddete kışkırtma, telif hakkı ihlalleri, dolandırıcılık, kimlik hırsızlığı, kara para aklama gibi topluma yönelik güvenlik risklerini artıran hukuka aykırı davranışlar için “elverişli” bir ortam sağlamıştır. Bunun sonucunda internet, tamamen kontrol edilebilir olmasa da

⁷⁵⁸ We Are Social and Meltwater, Digital 2024: Turkey, Nisan 2024. <https://datareportal.com/reports/digital-2024-turkey>

⁷⁵⁹ Dünya genelinde toplam internet kullanıcı sayısı 5.44 milyardır. Buna göre dünya nüfusunun yüzde 67.1’i internet kullanmaktadır. Sosyal medya kullanıcılarının sayısı ise 50.7 milyar olup bu sayının nüfusa oranı yüzde 62.6’dır. We Are Social and Meltwater, Digital 2024 April Global Statshot Report, Nisan 2024. <https://datareportal.com/reports/digital-2024-april-global-statshot>, (23.12.2024).

⁷⁶⁰ We Are Social and Meltwater, Digital 2024: Turkey, Nisan 2024. <https://datareportal.com/reports/digital-2024-turkey>, (23.12.2024).

kötüye kullanımın önlenmesi amacıyla, farklı ülkelerde farklı sistemler kullanılarak hukuki düzenlemelere tabi tutulmuştur.⁷⁶¹ Bu kapsamda, toplumun tümünün ve özellikle de çocuklar ile gençlerin ve ailelerin bu alandaki risk ve tehlikelere karşı korunması amacıyla internetin güvenli kullanımının sağlanmasına yönelik tedbirler alınmış ve farklı biçimlerde de olsa giderek artan bir oranda internetle ilgili müdahaleler içeren uygulamalara gidilmiştir.

Türk hukukunda da dünyadaki gelişmelere paralel olarak, internetin sağladığı imkanların suistimal edilmesi suretiyle işlenen suçlarla mücadele edilebilmesi, uyuşturucu ve uyarıcı madde kullanımını özendirici, intihara yöneltici, cinsel istismar ve kumar oynamaya teşvik edici vb. yayınlara karşı gerekli önleyici tedbirlerin alınması amacıyla özel bir hukuki çalışma başlatılmış ve 2007 yılında kabul edilen İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun (*İnternet Kanunu*) ile internet yönetimine ilişkin temel kurallar belirlenmiştir. İnternet Kanunu, Avrupa Birliği normlarıyla uyum sağlamak amacıyla Avrupa Parlamentosu ve Konseyi'nin E- Ticaret Direktifi ve karşılaştırmalı hukuk bilgileri göz önünde bulundurularak hazırlanmış⁷⁶² ve bugüne dek çok sayıda değişikliğe, iptale, ilğaya konu olmuştur.⁷⁶³

⁷⁶¹ Gönenç Gürkaynak, İlay Yılmaz, Pınar Kara, “Türk İnternet Hukuku Uygulamasının ve Mevzuatının Evriminin İlk Dönemini Tamamlaması İçin Öneriler ve Gözlemler”, https://www.gurkaynak.av.tr/docs/Turk_Internet_Hukuku_Uygulamasinin_ve_Mevzuatinin_Evriminin_Ilk_Donemini_Tamamlamasi_Icin_Oneriler_ve_Gozlemler.pdf, (23.12.2024).

⁷⁶² Genel Gerekeçe, 5651 İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, Esas Komisyon Raporu Sıra Sayısı 1397, <https://cdn.tbmm.gov.tr/KKBSPublicFile/D22/Y5/T1/DosyaKomisyonRaporunuVerdi/0c374bbe-43db-42d8-bde3-a58adfbbc25c.htm>, (24.10.2024).

⁷⁶³ Birinci Değişiklik, 5809 Sayılı Elektronik Haberleşme Kanun, R.G., T. 10.11.2008, S. 27050; İkinci Değişiklik, 661 Sayılı Avrupa Birliği Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname ile Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun Hükmünde Kararname, R.G. T. 02.11.2011, 28103/1; Üçüncü Değişiklik, 6495 Sayılı Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun, R.G. T. 02.08.2013 S. 28726; Dördüncü Değişiklik, 6518 Sayılı Aile ve Sosyal Politikalar Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname ile Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun, R.G. T. 19.02.2014, S. 28918; Beşinci Değişiklik, 6527 Sayılı Bazı Kanunlarda Değişiklik Yapılması Hakkında Kanun R.G. T. 01.03.2014, S. 28928, Altıncı Değişiklik, 6552 Sayılı İş Kanunu ile Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılması ile Bazı Alacakların Yeniden Yapılandırılmasına Dair Kanun, R.G. T. 11.09.2014, S. 29116/1; Yedinci Değişiklik, Anayasa Mahkemesinin 2/10/2014 Tarihli ve E: 2014/149, K: 2014/151 Sayılı Kararı; Sekizinci Değişiklik, Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılması Hakkında Kanun, R.G. T. 15.04.2015, S. 29327, Dokuzuncu Değişiklik, Anayasa Mahkemesinin 8/12/2015 Tarihli ve E: 2014/87, K: 2015/112 Sayılı Kararı; Onuncu Değişiklik, 671 Olağanüstü Hal Kapsamında Bazı Kurum ve Kuruluşlara İlişkin Düzenleme Yapılması Hakkında Kanun Hükmünde Kararname, R.G. T. 17.08.2016, S. 29804; On Birinci Değişiklik, 6757 Olağanüstü Hal Kapsamında Bazı Kurum ve Kuruluşlara İlişkin Düzenleme Yapılması

İnternetin ulusal sınırları aşan, çok boyutlu, çok aktörlü, dinamik ve dağınık yapısı internetin yol açtığı sorunlarla mücadelede yeni yöntemlerin benimsenmesini zorunlu kılmaktadır. Bu sorunlar ancak teknolojik altyapıyı hazırlamak, servis sağlayıcılar, sosyal medya şirketleri ve öteki kişiler tarafından kullanılacak standartları tespit etmek, ulusal veya uluslararası mekanizmalar kurulmasına veya mevcut mekanizmaların işletilmesine ve geliştirilmesine katkıda bulunmak gibi teknolojinin, uluslararası ilişkilerin ve hukukun gereklerine uygun başka önlemler almak suretiyle çözüme kavuşturulabilir.⁷⁶⁴

Sosyal medya platformlarında üretilen içeriği kontrol altında tutma, kullanıcıların etkileşim yöntemlerini ve biçimini belirleme imkânı önemli oranda sosyal medya şirketlerinin elinde olduğundan bu şirketlerin insan haklarının bir yükümlüsü olarak kabul edilmeleri ve bu yükümlülüklerin netleştirilmesi de şüphesiz çözümün önemli parçasıdır.

Bu kapsamda, 2020 yılında⁷⁶⁵ İnternet Kanunu'nda yapılan kapsamlı değişikliklerle, *sosyal ağ sağlayıcılar* özel bir sorumluluk ve yükümlülük rejimine tabi tutulmuştur.⁷⁶⁶ Sosyal ağ sağlayıcılara yönelik özel düzenlemelerle, teknolojik gelişmeler ışığında sınırları ve kullanım alanı hızla genişleyen internet ortamında etkinliği giderek artan, gerçek veya tüzel kişiliği bulunan alanların hukuki bir çerçeveye alınması ve bu bağlamda ihdas edilen yükümlülüklerin muhatabının belirlenmesi amaçlanmıştır.⁷⁶⁷

Hakkında Kanun Hükmünde Kararnamenin Değiştirilerek Kabul Edilmesine Dair Kanun, R.G. T. 24.11.2016, S. 29898; On İkinci Değişiklik, 700 Anayasada Yapılan Değişikliklere Uyum Sağlanması Amacıyla Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılması Hakkında Kanun Hükmünde Kararname, R.G. T. 07.07.2018, S. 30471/2; On Üçüncü Değişiklik, Anayasa Mahkemesinin 15/11/2017 Tarihli ve E: 2015/76, K: 2017/153 Sayılı Kararı; On Dördüncü Değişiklik, 7188 Ceza Muhakemesi Kanunu ve Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun, R.G. T. 24.10.2019, S. 30928; On Beşinci Değişiklik, 7226 Sayılı Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun, R.G. T. 26.03.2020, S. 31080/1; On Altıncı Değişiklik, 7253 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda Değişiklik Yapılmasına Dair Kanun, R.G. T. 31.07.2020, S. 31202; On Yedinci Değişiklik, 7418 Basın Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun, R.G. T. 18.10.2022, S. 31987; On Sekizinci Değişiklik, Anayasa Mahkemesinin 11/10/2023 Tarihli ve E: 2020/76, K: 2023/172 Sayılı Kararı.

⁷⁶⁴ Recep Tayyip Erdoğan Başvurusu, 2014/5376 (AYM 28 Ocak 2020), para. 42.

⁷⁶⁵ 7253 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda Değişiklik Yapılmasına Dair Kanun, (2020), <http://www.lexpera.com.tr/resmi-gazete/metin/internet-ortaminda-yapilan-yayinlarin-duzenlenmesi-ve-bu-yayinlar-yoluyla-islenen-suclarla-mucadele-8>, (12.10.2024).

⁷⁶⁶ 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun (İnternet Kanunu), (2007), m. 2(1), <http://www.lexpera.com.tr/mevzuat/kanunlar/internet-ortaminda-yapilan-yayinlarin-duzenlenmesi-ve-bu-yayinlar-yoluyla-islenen-suclarla-mucadele/1>, (12.10.2024)

⁷⁶⁷ E.2020/76, K.2023/172 (AYM 11 Ekim 2023), para. 10.

I. İnternet Şirketlerinin Sorumluluklarına İlişkin Temel Çerçeve

İnternet aktörlerin düzenlenmesinde, hizmet sağlayıcıların belirli koşullar altında hukuka aykırı içerikten sorumluluktan muaf tutulması genel olarak kabul gelen bir yaklaşımdır.⁷⁶⁸ AB E-Ticaret Direktifi ve karşılaştırmalı hukuk göz önünde bulundurularak hazırlanan⁷⁶⁹ 5651 sayılı İnternet Kanunu'nda da bu yaklaşım benimsenmiş ve sunulan hizmetin niteliğine göre farklı muafiyet koşullarına yer verilmiştir.

İnternet Kanunu'nda internet aktörleri, Avrupa Birliği düzenlemelerinden farklı bir şekilde ele alınmıştır. E-Ticaret Direktifi ve Dijital Hizmetler Yasası'nda, mevcut düzenlemeler özellikle “basit iletim”, “ön belleğe alma” ve “barındırma” hizmetleri olarak bilinen hizmetlerden oluşan aracı hizmetlere yöneliktir. İnternet Kanunu'nda ise bu aktörler, “içerik sağlayıcılar”, “yer sağlayıcılar”⁷⁷⁰, “erişim sağlayıcılar” ve “sosyal ağ sağlayıcılar” olarak düzenlenmiştir. İçerik sağlayıcılar, internetin teknik imkânlarını kullanıcılara sağlayanlar olmayıp, sadece kullanıcıların erişimine sunulan içerikleri sağlayanları ifade etmektedir. E-Ticaret Direktifi'nde yer almayan içerik sağlayıcılar, “*internet ortamı üzerinden kullanıcılara sunulan her türlü bilgi veya veriyi üreten, değiştiren ve sağlayan gerçek veya tüzel kişiler*” şeklinde tanımlanarak Kanun'da düzenlenmiştir. Kanunda, erişim sağlayıcılar olarak ifade edilen araçlar ise E-Ticaret Direktifi'nde yer alan “basit iletim” sağlayıcılardandır.⁷⁷¹

Yer sağlayıcılar, hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişileri ifade etmektedir. Kendileri bir içerik üretmeyen yer sağlayıcılar, bu yönüyle içerik sağlayıcılardan ayrılmaktadır. Yer sağlayıcıları erişim sağlayıcılardan ayıran temel nokta ise, yer sağlayıcıların devamlılık içerisinde veri/bilgi depolama

⁷⁶⁸ Mehmet Bedii Kaya, “The regulation of Internet intermediaries under Turkish law: Is there a delicate balance between rights and obligations?”, **Computer Law & Security Review**, C. 32, S. 5, 2016, s. 768.

⁷⁶⁹ Genel Gerekeçe, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun.

⁷⁷⁰ E-Ticaret Direktifi'nde “hosting providers” olarak ifade edilen internet araçları, Türk hukukunda yer sağlayıcılar ya da barındırma sağlayıcılar olarak farklı şekillerde ifade edilmektedir. 5651 Sayılı Kanun'da “yer sağlayıcılar” ifadesi tercih edilmiştir.

⁷⁷¹ Jan Bernd Nordemann, “The Functioning of the Internal Market for Digital Services: Responsibilities and Duties of Care of Providers of Digital Services”, European Sources Online, s. 10, <https://www.europeansources.info/record/the-functioning-of-the-internal-market-for-digital-services-responsibilities-and-duties-of-care-of-providers-of-digital-services/>, (24.10.2024); Julia Hörnle, **Internet Jurisdiction Law and Practice**, Oxford, Oxford University Press, 2021, s. 37.

hizmeti sunarken, erişim sağlayıcıların anlık olarak ve içeriğini kontrol etme olanakları olmaksızın verilerin aktarımını sağlayarak kullanıcılarına internete erişim imkânı sağlamalarıdır.⁷⁷²

İnternet Kanunu'na göre içerik sağlayıcılar, internet ortamında kullanıma sundukları her türlü içerikten sorumludur. Bununla birlikte içerik sağlayıcılar, bağlantı sağladıkları içerikten sorumluluktan muaf tutulmuştur. Bu muafiyetin tek istisnası ise, içerik sağlayıcının bağlantıyı sunuş biçiminden bu içeriği benimsediği ve kullanıcının söz konusu içeriğe ulaşmasını amaçladığının açıkça belli olmasıdır. Bu durumda içerik sağlayıcı, hukuka aykırı içerikten sorumlu olacaktır.⁷⁷³

Kanunda yer sağlayıcıların sorumluluktan muafiyeti ise, E-Ticaret Direktifi ve Dijital Hizmetler Yasası'nda temel bir prensip olarak kabul edilen genel izleme yükümlülüğü yasağına uygun olarak düzenlenmiştir. Buna göre yer sağlayıcılar, sağladığı içeriği kontrol etmek veya hukuka aykırı bir faaliyetin söz konusu olup olmadığını araştırmakla yükümlü değildir. Yer sağlayıcılar, ayrıca, Kanunun 8. ve 9. maddeleri uyarınca hukuka aykırı içerikle ilgili bir bildirim almaları hali dışında hukuka aykırı içerikten sorumlu da değildir.⁷⁷⁴ Türk hukukunda, yer sağlayıcıların sorumluluktan muafiyetine ilişkin tartışmalar özellikle kişilik haklarına aykırılık teşkil eden⁷⁷⁵ ya da fikri mülkiyet hakkını ihlal eden içeriklerle⁷⁷⁶ ilgili olarak gelişmiş ve yer sağlayıcının bir şekilde haberdar edilmiş olması şartıyla hukuka aykırı içerikten sorumlu olacağı kabul edilmiştir.⁷⁷⁷

Erişim sağlayıcılar da yer sağlayıcılar gibi kendisi aracılığıyla erişilen bilgilerin içeriklerinin hukuka aykırı olup olmadıklarını ve sorumluluğu gerektirip gerektirmediğini kontrol etmekle yükümlü olmayıp yalnızca Kanun hükümlerine uygun olarak haberdar

⁷⁷² Feral-Schuhl, C. (2018) *Cyberdroit, le Droit à l'Épreuve de l'Internet* (Paris: Dalloz)'den aktaran Zeynep Yasaman, "Avrupa Birliği ve Türk Hukuku Bakımından İnternet Yer Sağlayıcılarının Marka İhlalleri Kapsamında Sorumlulukları", **Marmara Üniversitesi Avrupa Topluluğu Enstitüsü Avrupa Araştırmaları Dergisi**, C. 27, S. 2, 2019, s. 267.

⁷⁷³ "İnternet Kanunu", m. 4(2).

⁷⁷⁴ "İnternet Kanunu", m. 4(2). m. 5(2).

⁷⁷⁵ E. 2015/10004, K. 2016/1023 (Yargıtay 4. HD. 27 Ocak 2016); 2013/15828, K. 2014/9951 (Yargıtay 4. HD. 16 Haziran 2014).

⁷⁷⁶ E. 2018/307, K. 2020/149 (İstanbul 2. Fikrî ve Sınai Haklar Hukuk Mahkemesi 26 Şubat 2020); E. 2018/566, K. 2020/388 (İstanbul 2. Fikrî ve Sınai Haklar Hukuk Mahkemesi 12 Kasım 2020).

⁷⁷⁷ E. 2019/5303, K. 2020/629 (Yargıtay 11. HD. 21 Ocak 2020).

edilmeleri halinde erişim sağladıkları hukuka aykırı içeriğe erişimi engellemekle yükümlüdür.⁷⁷⁸

İnternet Kanunu'nun yer sağlayıcıların sorumluluktan muafiyetine ilişkin bu hükümleri, E-Ticaret Direktifi ve Dijital Hizmetler Yasası'nda öngörülen muafiyet rejiminden sorumluluğu başlatan hareket türü bakımından ayrılmaktadır. İnternet Kanunu'na göre, yer sağlayıcılar “haberdar edilmeleri” halinde hukuka aykırı içeriği yayından çıkarma yükümlülüğü altındayken; AB mevzuatına göre yer sağlayıcının sorumluluğu “haberdar olduğunda” başlamaktadır.⁷⁷⁹ Buna göre, İnternet Kanunu yer sağlayıcıları kendi inisiyatifleri ile farkına vardıkları hukuka aykırılığa ilişkin sorumluluktan da muaf tutarak yalnızca bildirim dayanan bir sorumluluk rejimi öngörmektedir.

Anlaşılabacağı üzere Kanun'da, aracı hizmet sağlayıcıların sorumluluktan muafiyeti sunulan hizmetin niteliğine göre düzenlenmiştir. Dolayısıyla, bir internet şirketinin hukuka aykırı içerikten sorumluluğunun belirlenmesinde ilgili içerik bakımından hangi sıfatla hareket ettiği önem teşkil etmektedir. Örneğin, bir internet sitesinin yönetim ve denetiminden sorumlu gerçek kişinin internet sitesinde yayınlanan haberlere yapılan yorumlardan cezai sorumluluğuna ilişkin bir davada Yargıtay, sanığın haberler bakımından içerik sağlayıcı olmasına karşın haberlere yapılan yorumlar yönünden yer sağlayıcı olduğu tespit edilmiş ve İnternet Kanunu uyarınca sanığın yer sağladığı içeriği kontrol etmek veya hukuka aykırı bir faaliyetin söz konusu olup olmadığını araştırmakla yükümlü olmadığı belirtilmiştir.⁷⁸⁰

5651 sayılı İnternet Kanunu, internet aracı hizmet sağlayıcıları, üçüncü taraf içeriklerine ilişkin sorumluluktan muaf tutmakla birlikte hizmet sağlayıcılar için geniş bir yükümlülükler yelpazesi öngörmektedir. Kanun'da temel olarak dört alan düzenlenmektedir: i) içerik sağlayıcılar, yer sağlayıcılar, erişim sağlayıcılar gibi internet aktörlerinin hukuki, cezai ve idari yükümlülükleri ve sorumlulukları (md. 4, 5, 6); ii) belirli suçlar için erişim engelleme prosedürü ve özellikle gecikmesinde sakınca bulunan hallerde bu tür suçlarla mücadeleyle ilişkin diğer ayrıntılar (md. 8, 8/A); iii) İnternet içeriği

⁷⁷⁸ “İnternet Kanunu”, m. 4(2).

⁷⁷⁹ “ECD”, m. 14(1); “DSA”, m. 6(1).

⁷⁸⁰ E. 2020/19282, K. 2020/21719 (Yargıtay 4. CD. 23 Aralık 2020).

nedeniyle özel hayatın gizliliğinin ihlal edildiği durumlarda bildirim ve yayından kaldırma prosedürleri, içeriğin kaldırılması ve bu içeriğe erişimin engellenmesi (9/A); iv) sosyal ağ sağlayıcıların ek yükümlülükleri (ek m. 4).

Bu bölümde, hizmet sağlayıcıların sorumlulukları ve yükümlülükleri Kanun'un sistematigi dikkate alınarak, içerik, yer ve erişim sağlayıcılar için öngörülen ortak yükümlülükler ve sosyal ağ sağlayıcılar için öngörülen ek yükümlülükler şeklinde iki başlıkta ele alınacaktır.

A. İçerik, Yer ve Erişim Sağlayıcıların Yükümlülükleri

İnternet Kanunu'nda içerik, yer ve erişim sağlayıcılara sundukları hizmetlerin niteliğine göre farklılık gösteren yükümlülükler öngörülmüştür. Buna göre, belirtilen tüm hizmet sağlayıcılar bilgilendirme ve içeriğin yayından çıkarılması ve erişimin engellenmesine ilişkin yükümlülüklerle tabidir.⁷⁸¹ Yer sağlayıcılar ve erişim sağlayıcılar ayrıca, trafik bilgilerini belirli bir süre için saklamakla da yükümlüdür. Buna göre, yer sağlayıcıların, yer sağladığı hizmetlere ilişkin trafik bilgilerini bir yıldan az ve iki yıldan fazla olmamak üzere yönetmelikte belirlenecek süre kadar saklaması ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlaması; erişim sağlayıcıların ise faaliyetine son vereceği tarihten en az üç ay önce durumu Kuruma, içerik sağlayıcılarına ve müşterilerine bildirmesi ve trafik bilgilerine ilişkin kayıtları yönetmelikte belirtilen esas ve usullere uygun olarak Kuruma teslim etmesi gerekmektedir.⁷⁸²

1. Bilgilendirme Yükümlülüğü

İnternet Kanunu'nun 3. maddesinde yer alan düzenlemeye göre, internet şirketlerinin ilk yükümlülükleri bilgilendirme yükümlülüğüdür. Buna göre, içerik, yer ve erişim sağlayıcıları, İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik'te belirtilen esas ve usûller çerçevesinde tanıtıcı bilgilerini kendilerine ait internet ortamında kullanıcıların ulaşabileceği şekilde ve güncel olarak bulundurmakla yükümlüdür.⁷⁸³

⁷⁸¹ "İnternet Kanunu", m. 3(1), 4(1,2), 5(2), 6(1).

⁷⁸² "İnternet Kanunu", m. 5(3), 6(1).

⁷⁸³ "İnternet Kanunu", m. 3(1).

İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik'e göre, ticari veya ekonomik amaçlı içerik sağlayıcı, yer sağlayıcı ve erişim sağlayıcıların bilgilendirmekle yükümlü oldukları tanıtıcı bilgiler a) gerçek kişi ise adı ve soyadı, tüzel kişi ise; unvanı ve sorumlu kişiler, vergi kimlik numarası veya ticaret sicil numarası, b) yerleşim yeri, tüzel kişi ise merkezinin bulunduğu yer, c) elektronik iletişim adresi ve telefon numarası, ç) sunduğu hizmet, bir merciin iznine veya denetimine tabi bir faaliyet çerçevesinde yapılıyor ise, yetkili denetim merciine ilişkin bilgilerden oluşmaktadır.⁷⁸⁴ Ticari veya ekonomik amaçlı içerik sağlayıcılar yer ve erişim sağlayıcılardan farklı olarak, yer sağlayıcıya ilişkin tanıtıcı bilgileri de doğru, eksiksiz ve güncel olarak ana sayfasında bulundurmakla yükümlüdür.⁷⁸⁵

Yönetmelik'te, Kanun'dan farklı olarak yalnızca ticari veya ekonomik amaçlı içerik sağlayıcıları, yer sağlayıcıları ve erişim sağlayıcılarından bahsedilerek bilgilendirme yükümlülüğünün muhatapları sınırlandırılmıştır. Bu sınırlandırma, internet şirketleri bakımından olmasa da internet forumlarında tartışmalara katılanlar, blog sahipleri, internet aracılığı ile yayın yapan gazetelerde yer alan haberlere yorum yazanlar, sosyal medya kullanıcıları gibi ticari veya ekonomik amacı olmayan içerik sağlayıcıların yükümlülükleri bakımından Kanun'dan farklı sonuç doğurmaktadır. Kanun'da benimsenen yaklaşım tercih edildiğinde, belirtilen kişiler de bilgilendirme yükümlülüğü ile karşı karşıya kalacaktır. Bu durum, internet kullanıcılarının ad-soyad, adres, telefon numarası gibi kişisel veri teşkil eden bilgilerini diğer tüm kullanıcıların ulaşabileceği şekilde paylaşımlarını gerektirecektir. İnternet ortamında düşüncelerini ifade etmek ve kamusal tartışmalara katılmak isteyen kullanıcıların kişisel verilerini paylaşımlarını zorunlu kılan böyle bir yükümlülük ifade özgürlüğü bakımından caydırıcı bir etki de doğurabilecek niteliktedir. Bu nedenle, Kanun'da öngörülen geniş çerçevenin ifade özgürlüğü ve kişisel verilerin korunması haklarına uygun şekilde değiştirilmesi isabetli olacaktır.⁷⁸⁶

⁷⁸⁴ İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik, (R.G. T. 30.11.2007, S. 26716.), m. 5(1).

⁷⁸⁵ İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik, m. 5(2).

⁷⁸⁶ E. Eylem Aksoy Retornaz, "5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkındaki Kanun Kapsamında İçerik Sağlayıcının Yükümlülükleri ve Ceza Sorumluluğu", **Ceza Hukuku Dergisi**, C. 16, S. 45, 2021, s. 4.

2. Trafik Bilgilerini Saklama Yükümlülüğü

İnternet Kanunu'na göre, yer sağlayıcılar ve erişim sağlayıcılar *“tarafllara ilişkin IP adresi, port bilgisi, verilen hizmetin başlama ve bitiş zamanı, yararlanılan hizmetin türü, aktarılan veri miktarı ve varsa abone kimlik bilgilerini”* ifade eden trafik bilgisini belirli süreliğine saklamakla yükümlüdür.

Bu yükümlülük kapsamında yer sağlayıcılar, yer sağladıkları hizmetlere ilişkin trafik bilgilerini bir yıldan az ve iki yıldan fazla olmamak üzere⁷⁸⁷; erişim sağlayıcılar ise sağladıkları hizmetlere ilişkin yönetmelikte belirtilen trafik bilgilerini altı aydan az ve iki yıldan fazla olmayacak şekilde⁷⁸⁸ yönetmelikte belirlenecek süre kadar saklamak ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamakla yükümlüdür. 2014 yılında 6527 sayılı Kanunla yapılan değişiklikle hizmet sağlayıcılar trafik bilgilerini Telekomünikasyon İletişim Başkanlığı ile paylaşmakla da yükümlü kılınmıştır; ancak yer ve erişim sağlayıcılar tarafından saklanan trafik bilgisinin Telekomünikasyon İletişim Başkanlığı (TİB) tarafından herhangi bir gerekçe veya neden göstermeksizin temin edilmesine olanak sağlayan düzenleme Anayasa Mahkemesi tarafından iptal edilmiştir. AYM, TİB tarafından herhangi bir kurala ve sınırlamaya tabi olmaksızın istenildiği zaman ve şekilde elde edilebilir olmasını temel hak ve özgürlüklerin korunması bakımından sorunlu bulmuştur.

Kişisel verilerin korunması, iletişimin gizliliği, düşünce ve ifadeyi yayma özgürlüğü, haberleşme özgürlüğü gibi hak ve özgürlüklerle doğrudan ilgili olan⁷⁸⁹ trafik bilgilerini saklama yükümlülüğü de Anayasa Mahkemesi tarafından incelenmiş ve Anayasa'ya uygun bulunmuştur. Anayasa Mahkemesi, söz konusu verilerin ulaşılabilir olmasının kişilerin tercihleri, politik eğilimleri, sağlık bilgileri, ticari sırları, düşünceleri ve davranışları hakkında fikir verebileceğinden kişilerin özel hayatlarına müdahale edilme riskini de beraberinde getirdiğini kabul etmekle birlikte⁷⁹⁰; internet üzerinden işlenen suçlarla mücadele edilmesi açısından önemli ve gerekli olan bilgilerin kaybolmasının önlenmesi ve faillerin ortaya çıkarılmasını sağlama amacına yönelik bu

⁷⁸⁷ “İnternet Kanunu”, m. 5(3).

⁷⁸⁸ “İnternet Kanunu”, m. 6(1)/b.

⁷⁸⁹ E.2014/149, K.2014/151 (AYM 02 Ekim 2014).

⁷⁹⁰ E.2014/149, K.2014/151 (AYM 02 Ekim 2014); E.2014/87, K.2015/112 (AYM 08 Aralık 2015), para. 178.

düzenleme ile bilgilerin saklanacağı süreye ilişkin alt ve üst sınırların belirlenmiş olduğunu ve erişim ve yer sağlayıcılara bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlama yükümlülüğü de yüklendiğini belirterek iptal talebini reddetmiştir.⁷⁹¹

3. İçeriğinin Yayından Çıkarılması ve/veya Erişimin Engellenmesine İlişkin Yükümlülükler

İnternet Kanunu'nda, hukuka aykırı içeriğin yayından çıkarılması ve/veya bu içeriğe erişimin engellenmesine prosedürlerine ilişkin olarak kapsamlı düzenlemelere yer verilmiştir. Buna göre, internet ortamında temel hak ve hürriyetlerin korunması ve güvenli bir ortamın sağlanabilmesi için içerik sağlayıcılar, yer sağlayıcılar, erişim sağlayıcılar; Bilgi Teknolojileri ve İletişim Kurumu ile Kurumun Başkanı ve Erişim Sağlayıcıları Birliği hukuka aykırı içeriğin yayından çıkarılması ve/veya içeriğin erişime engellenmesini sağlamakla yükümlüdür.

İnternet şirketleri, hukuka aykırı içeriklere ilişkin olarak, yargı organları ve idari makamlar tarafından alınan kararlara katlanmak⁷⁹² ve uyar-kaldır usulü çerçevesinde,

⁷⁹¹ AYM, E.2014/87, K.2015/112, 08.12.2015, § 181. Venedik Komisyonu, yer ve erişim sağlayıcılara trafik bilgilerini saklama yükümlülüğü yükleyen bu düzenlemelerin mahremiyet hakkı ve kişisel verilerin korunması hakkı bakımından yeterli güvence sağlamadığını değerlendirmektedir: “Hükümlerin meşru amacı suçla mücadele olmasına rağmen, bu amaç ışığında herhangi bir ayırım yapılmaksızın tüm internet kullanıcılarına uygulanmaktadır; yani haklarında ciddi suçların işlenmesine karıştıklarına dair şüpheler bulunan kişiler ve verilerinin saklanması ciddi suçların soruşturulmasına katkıda bulunabileceği diğer kişilerle sınırlı değildir. Ayrıca, bu maddeler kapsamındaki veri saklama tedbiri, hükümlerde belirtilen bir alt ve bir üst sınır arasındaki tüm dönemi kapsar ve ciddi suçların işlendiğine dair şüphelerin bulunduğu alt ve üst sınırlar arasındaki belirli bir süreyle sınırlı değildir. Saklama süresinin kesinlikle gerekli olan süreyle sınırlı olmasını sağlamak için bu süreyi belirleyecek bazı objektif kriterler olmalıdır. Ayrıca, hükümler tedbiri maddi kapsamı bakımından sınırlandırmamaktadır: tedbir, organize suçlar, terörizm veya pedofili gibi ciddi suçlar listesiyle sınırlı değildir ve yukarıda detaylandırıldığı üzere, verilerin kullanımına ilişkin suçların ciddiyeti için bir eşik değer öngörmemektedir.” AYM 08 Aralık 2015 para. 181; Venedik Komisyonu, yer ve erişim sağlayıcılara trafik bilgilerini saklama yükümlülüğü yükleyen bu düzenlemelerin mahremiyet hakkı ve kişisel verilerin korunması hakkı bakımından yeterli güvence sağlamadığını değerlendirmektedir: “Hükümlerin meşru amacı suçla mücadele olmasına rağmen, bu amaç ışığında herhangi bir ayırım yapılmaksızın tüm internet kullanıcılarına uygulanmaktadır, yani haklarında ciddi suçların işlenmesine karıştıklarına dair şüpheler bulunan kişiler ve verilerinin saklanması ciddi suçların soruşturulmasına katkıda bulunabileceği diğer kişilerle sınırlı değildir. Ayrıca, bu maddeler kapsamındaki veri saklama tedbiri, hükümlerde belirtilen bir alt ve bir üst sınır arasındaki tüm dönemi kapsar ve ciddi suçların işlendiğine dair şüphelerin bulunduğu alt ve üst sınırlar arasındaki belirli bir süreyle sınırlı değildir. Saklama süresinin kesinlikle gerekli olan süreyle sınırlı olmasını sağlamak için bu süreyi belirleyecek bazı objektif kriterler olmalıdır. Ayrıca, hükümler tedbiri maddi kapsamı bakımından sınırlandırmamaktadır: tedbir, organize suçlar, terörizm veya pedofili gibi ciddi suçlar listesiyle sınırlı değildir ve yukarıda detaylandırıldığı üzere, verilerin kullanımına ilişkin suçların ciddiyeti için bir eşik değer öngörmemektedir.” “Venice Commission on Law No. 5651 on Regulation of Publications on the Internet and Combating Crimes Committed by Means of Such Publication (“The Internet Law”), CDL-AD(2016)011, 2016.”, 2016.

⁷⁹² “İnternet Kanunu”, m. 8(5), 8/A(1), 9(8), 9/A(3), Ek 4(9).

hakları ihlal edilenler tarafından yapılan içeriğin çıkarılmasına ilişkin başvuruları sonuçlandırmakla⁷⁹³ yükümlüdür. Kanun'da hukuka aykırı içerikle mücadeleye ilişkin olarak içeriğin yayından çıkarılması ve erişimin engellenmesi usullerine yer verilmiş⁷⁹⁴ ve bu kararlara ilişkin olarak üç farklı prosedür öngörülmüştür: i) içeriğin çıkarılması ve erişimin engellenmesi kararları ile yerine getirilmesi (m. 8), ii. gecikmesinde sakınca bulunan hâllerde içeriğin çıkarılması ve/veya erişimin engellenmesi (m. 8/A) iii) Özel hayatın gizliliği nedeniyle içeriğe erişimin engellenmesi. Uygulamada sıklıkla başvuru alan usullerden biri olan kişilik haklarını ihlal eden internet yayınlarından yayından çıkarılması ve erişimin engellenmesi prosedürü (m. 9) ise Anayasa Mahkemesi tarafından iptal edilmiştir.⁷⁹⁵ Anayasa Mahkemesi, iptal kararının yürürlüğe gireceği tarihi ertelemesine rağmen, bu süre zarfında yeni bir düzenleme yapılmamıştır. Bu kapsamda, 8, 8A ve 9A maddelerinde düzenlenen usuller ele alındıktan sonra 9. maddede öngörülen usul ve bu usule ilişkin iptal sebepleri, iptal edilmiş olmasına rağmen, ilerleyen süreçte yeni bir düzenleme yapılması ihtimali göz önünde bulundurularak incelenecektir.

İnternet Kanunu'nun 8. maddesi, internet hizmet sağlayıcılara Kanun'da öngörülen suçların⁷⁹⁶ oluştuğuna dair yeterli şüphe üzerine yargı organları ya da idari makamlarca tedbiren içeriği kaldırması ve/veya erişimi engellenmesi kararı verilmesi

⁷⁹³ "İnternet Kanunu", m. 9(1), Ek 4(3).

⁷⁹⁴ Venedik Komisyonu, Kanun'da içerik yönetimine ilişkin olarak içeriğin çıkarılması ve erişimin engellenmesine alternatif "açıklama", "cevap", "düzeltme", "özür", "içeriğin yenilenmesi", "erişimin yenilenmesi" vb. gibi daha az müdahaleci tedbirlere yer verilmemesini eleştirmekte ve Kanunda yer alan tedbirler bakımından orantılılık değerlendirmesine imkân verecek değişikliklerin yapılmasını tavsiye etmektedir. "Venice Commission on Law No. 5651 on Regulation of Publications on the Internet and Combating Crimes Committed by Means of Such Publication ("The Internet Law"), CDL-AD (2016)011, 2016.", s. 10.

⁷⁹⁵ E. 2020/76, K. 2023/172 (AYM 11 Ekim 2023).

⁷⁹⁶ "İnternet Kanunu", m. 8(1):

"a) 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanunu'nda yer alan;

1) İntihara yönlendirme (madde 84),

2) Çocukların cinsel istismarı (madde 103, birinci fıkra),

3) Uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma (madde 190),

4) Sağlık için tehlikeli madde temini (madde 194),

5) Müstehcenlik (madde 226),

6) Fuhuş (madde 227),

7) Kumar oynanması için yer ve imkân sağlama (madde 228) suçları.

b) 25/7/1951 tarihli ve 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanunda yer alan suçlar.

c) (Ek:25/3/2020-7226/32 md.) 29/4/1959 tarihli ve 7258 sayılı Futbol ve Diğer Spor Müsabakalarında Bahis ve Şans Oyunları Düzenlenmesi Hakkında Kanunda yer alan suçlar.

ç) (Ek:13/10/2022-7418/32 md.) 1/11/1983 tarihli ve 2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanununun 27 nci maddesinin birinci ve ikinci fıkrasında yer alan suçlar."

halinde, içerik yer ve erişim sağlayıcıları, kararın bildirilmesinden itibaren derhal ve en geç dört saat içinde bu kararı yerine getirmeleri yükümlülüğü yüklemektedir.⁷⁹⁷

Bu madde uyarınca, internet şirketlerinin yükümlülükleri, yargı organları tarafından alınan “koruma tedbiri” kararlarından; ya da Bilgi Teknolojileri ve İletişim Kurumu Başkanı tarafından alınan "idari tedbir" kararlarından kaynaklanmaktadır.⁷⁹⁸

Bu kararlar iki şekilde uygulanmaktadır. Başkan tarafından resen karar alınması halinde bu karar BTK tarafından içerik, yer ya da erişim sağlayıcılara bildirilmektedir. Kararın hâkim/mahkeme yahut Cumhuriyet savcısı tarafından verilmesi halinde ise kararın bir örneği gereği yapılmak üzere Kurum’a gönderilmekte; bu karar yine Kurum tarafından içerik, yer ya da erişim sağlayıcılara bildirilmektedir.⁷⁹⁹

Bu tür tedbir kararlarının uygulanması başlı başına, Anayasa ve AIHS’e aykırılık teşkil etmemekle birlikte söz konusu düzenlemeler muhtemel kötüye kullanma durumlarına karşı sunulan hukuki kontrol güvencesi konusunda etkili olmalı ve yasağın sınırlandırılması hususunda bilhassa katı olan yasal bir çerçevede getirilmelidir.⁸⁰⁰

8. maddenin dördüncü fıkrası kapsamında BTK Başkanı’nın resen içeriğin çıkarılması ve/veya erişimin engellenmesine karar verme yetkisi sık sık tartışma konusu olmuştur.⁸⁰¹ Nitekim, bu madde çeşitli değişikliklere ve iptal kararlarına da konu olmuştur. İnternet ortamında paylaşılan içeriklerin çok hızlı yayılabildiği ve bu içeriklere çocuklar gibi korumasız bireyler de dâhil olmak üzere toplumun her kesimi tarafından kolayca erişilebildiği göz önünde bulundurulduğunda, Başkana suç oluşturan içeriklerle

⁷⁹⁷ “İnternet Kanunu”, m. 8(5).

⁷⁹⁸ İnternet Kanununda, 2020 yılında, 7253 sayılı Kanun ile yapılan değişikliklerden önce, Başkan tarafından iki farklı durumda resen erişimin engellenmesi kararı verilmesi mümkündü: “...İçeriği birinci fıkra belirtilen suçları oluşturan yayınların içerik veya yer sağlayıcısının yurt dışında bulunması halinde veya içerik veya yer sağlayıcısı yurt içinde bulunsan bile, içeriği birinci fıkranın (a) bendinin (2), (5) ve (6) ve (7) numaralı alt bentlerinde ve (c) bendinde yazılı suçları oluşturan yayınlara ilişkin olarak erişimin engellenmesi kararı re’sen Başkan tarafından verilir. Bu karar, erişim sağlayıcısına bildirilerek gereğinin yerine getirilmesi istenir.” Söz konusu değişiklikten önce, bu madde somut norm denetimi kapsamında Danıştay tarafından Anayasa Mahkemesi’nin önüne getirilmiştir. Anayasa Mahkemesi, inceleme aşamasında değiştirilmiş olan söz konusu kuralın bakılmakta olan dava yönünden uygulanacak kural olma niteliğini sürdürdüğünü belirterek, 8. maddesinin (1) numaralı fıkrasının (a) bendinin (5) numaralı alt bendi ile sınırlı olarak esas incelemeye geçmiştir.

⁷⁹⁹ “İnternet Kanunu”, m. 8(3), 8(4).

⁸⁰⁰ Cengiz and Others v. Turkey, 48226/10 and 14027/11 (ECtHR 01 Aralık 2015), para. 62.

⁸⁰¹ 27.03.2024 tarihli Youtube ve 02.08.2024 tarihli Instagram yasakları bu madde kapsamında yapılmış ve kamuoyunda önemli tartışmalara yol açmıştır.

ilgili hızlı bir şekilde karar alabilme yetkisinin verilmesi kamu yararı amacına hizmet etmektedir.⁸⁰² Bununla birlikte, bu yetkinin keyfi bir şekilde kullanılmasına karşı yeterli güvencelerin sağlanmaması başta ifade özgürlüğü olmak üzere temel hak ve özgürlüklerin ihlal edilmesine yol açabilecektir. Başkanın resen karar alabilme yetkisinin ele alındığı Anayasa Mahkemesi kararlarında da düzenlemenin bu iki boyutu birlikte ele alınmaktadır.

Anayasa Mahkemesi 2017 tarihli kararında, Kanun'un 8(4) maddesinin ilk haline ilişkin anayasallık denetimi yapmıştır. Dava konusu düzenlemeye göre, Başkanlık içeriği Kanun'un birinci fıkrasında belirtilen suçları oluşturan yayınların içerik veya yer sağlayıcısının yurt dışında bulunması halinde veya içerik veya yer sağlayıcısı yurt içinde bulunsu bile, içeriği birinci fıkranın (a) bendinin (2) ve (5) ve (6) numaralı alt bentlerinde yazılı suçları oluşturan yayınlara ilişkin olarak resen erişimin engellenmesine karar verme yetkisine sahipti. Anayasa Mahkemesi, inceleme aşamasında değiştirilmiş olan söz konusu düzenlemenin bakılmakta olan dava yönünden uygulanacak kural olma niteliğini sürdürdüğünü belirterek, 8. maddesinin (1) numaralı fıkrasının (a) bendinin (5) numaralı alt bendi ile sınırlı olarak esas incelemeye geçmiştir.⁸⁰³ Anayasa Mahkemesi, yalnızca suç işlemeye veya suç işlenmesini kolaylaştırmaya yönelik internet yayınları yapan siteler ile asıl amacı bu olmamakla beraber içeriği suç oluşturan bazı yayınlara da yer verilen sosyal medya platformları arasında ayırım yaparak Anayasa'nın 22. maddesinde güvence altına alınan hakim onayı güvencesinin haberleşme veya iletişim amacı taşıyan sosyal medya platformlarını da kapsadığını belirtmiştir. Mahkeme'ye göre:

⁸⁰² E.2015/76, K.2017/153 (AYM 15 Kasım 2017).

⁸⁰³ Anayasa Mahkemesi değişikliklerin kapsamını ve incelemenin sınırlarını şu şekilde ortaya koymuştur: "4. 15.8.2016 tarihli ve 671 sayılı Olağanüstü Hal Kapsamında Bazı Kurum ve Kuruluşlara İlişkin Düzenleme Yapılması Hakkında Kanun Hükmünde Kararname ile 5651 sayılı Kanun'da değişiklikler yapılmıştır. Kararname'nin 22. maddesi ile Kanun'a eklenen ek 3. maddenin birinci fıkrası uyarınca Telekomünikasyon İletişim Başkanlığı (TİB) kapatılmıştır. Kararname'nin 21. maddesinin (d) numaralı fıkrasıyla, itiraz konusu kuralı da içeren 8. maddenin (4) numaralı fıkrasında yer alan "Başkanlık" ibaresi "Başkan" şeklinde değiştirilmiştir. Kanun'un Kararname'nin 20. maddesiyle değiştirilen 2. maddesinin birinci fıkrasının (c) bendine göre ise Başkan, Bilgi ve Teknolojileri ve İletişim Kurumu Başkanı'nı ifade eder. Dolayısıyla Kararname ile yapılan değişiklikle, Kanun'un 8. maddesinin itiraz konusu kuralı içeren (4) numaralı fıkrasında sayılan hâllerde erişimin engellenmesi kararının resen Bilgi ve Teknolojileri ve İletişim Kurumu Başkanı tarafından verileceği kurala bağlanmıştır. İtiraz konusu kural esas inceleme aşamasında değiştirilmiş olmakla beraber itiraz başvurusunda bulunan mahkemenin bakmakta olduğu dava yönünden uygulanacak kural olma niteliğini sürdürdüğünden Anayasa'ya aykırılık iddiasının incelenmesi gerekir." E.2015/76, K.2017/153 (AYM 15 Kasım 2017), para. 4.

“Esas amacı haberleşme ve bilgi paylaşımı olan bu sitelerde yer alan içeriği suç oluşturabilecek yayınlar nedeniyle hâkim onayı olmaksızın sitenin tümüne yönelik olarak resen erişimin engellenmesi kararı verilmesi Anayasa’nın 22. maddesinde, haberleşmenin kanunla yetkili kılınmış mercii tarafından engellenmesi hâlinde engelleme kararının yirmi dört saat içinde görevli hâkimin onayına sunulacağı şeklinde açıkça ifade edilen güvenceyle bağdaşmamaktadır.”⁸⁰⁴

Anayasa Mahkemesi söz konusu düzenlemeyi ifade özgürlüğü bakımından da ele almıştır. Mahkeme, internet ve sosyal medyanın günümüzde düşünceyi açıklamanın en etkili ve yaygın yöntemlerinden biri hâline geldiğini vurgulamakla birlikte, ifade özgürlüğünün sınırsız olmadığını, Anayasa’da öngörülen güvencelere uygun olarak sınırlandırılabilirliğinin altını çizmiştir. Kararda, dava konusu düzenlemeye ilişkin olarak şu değerlendirmelere yer verilmiştir:

“Kamu gücüne temel hak ve özgürlüklere yönelik sınırlama yetkisi tanıyan yasal düzenlemelerin bu yetkinin kullanılmasına ilişkin kapsam ve usulleri yeterli bir açıklıkta tanımlaması da gerekmektedir. Kanun’un erişimin engellenmesine imkân tanıyan 8/A ve 9. maddelerinde; engelleme kararının öncelikle ilgili yayın, kısım, bölüm ile ilgili olarak (URL, vb. şeklinde) verilmesi ancak teknik olarak ilgili içeriğe erişimin engellenmesinin yapılamadığı veya yalnızca ilgili içeriğe erişimin engellenmesiyle Kanun’da belirtilen amaca ulaşamayacağı durumlarda internet sitesinin tümüne yönelik olarak erişimin engellenmesi kararı verileceği düzenlenmiştir.

İtiraz konusu kuralda ise TİB tarafından müstehcenlik suçu oluşturan yayınlara resen erişimin engellenmesi kararı verileceği belirtilmekle yetinilmiş, Kanun’un yukarıda anılan hükümlerinde öngörüldüğü gibi erişimin kademeli olarak engellenip engellenmeyeceğine ilişkin herhangi bir düzenlemeye yer verilmemiştir. Böylece itiraz konusu kuralla idareye kapsam ve sınırları belirsiz şekilde erişimin engellenmesi yetkisi tanınmıştır. Erişimin engellenmesi kararı verilmesinin dayanağı olan itiraz konusu kural anlaşılır, açık ve net olma

⁸⁰⁴ E.2015/76, K.2017/153 (AYM 15 Kasım 2017), para. 27.

zorunluluğunu karşılamadığından Anayasa'nın 13. maddesinde öngörülen temel hak ve özgürlüklerin kanunla sınırlanması güvencesiyle bağdaşmamaktadır.”⁸⁰⁵

Anayasa Mahkemesinin söz konusu iptal kararı, her ne kadar Kanun'un 8. maddesinin (1) numaralı fıkrasının (a) bendinin (5) numaralı alt bendi ile sınırlı olsa da, söz konusu düzenleme ile Başkanlığa verilen ve inceleme konusu olmayan diğer yetkiler de belirlilik ilkesine aykırılık teşkil etmektedir.

Kanun'un 8(4) maddesi, esaslı iki değişikliğe konu olmuştur. İlk olarak, 31.07.2020 tarih ve 7253 sayılı Kanunla⁸⁰⁶ yapılan değişiklikle, Başkan, içeriği maddede belirtilen suçları oluşturan yayınlara ilişkin olarak erişimin engellenmesi kararı yanında içeriğin çıkarılması kararı vermekle de yetkilendirilmiştir. 18.10.2022 tarih ve 7418 sayılı Kanun⁸⁰⁷ ile de Başkanın resen karar verme yetkisine yönelik bir sınır teşkil eden, yer, içerik ya da yer sağlayıcının yurt dışında ya da yurt içinde bulunması ayrımı kaldırılmıştır. Böylece Başkanın resen karar verme yetkisi 8/1. maddede belirtilen tüm suçları kapsayacak şekilde genişletilmiştir.

Başkan'ın resen içeriğin çıkarılmasına karar verebilmesine ilişkin ilk değişiklik hakkında Anayasa Mahkemesi'ne başvurulmuş ve Mahkeme, söz konusu düzenlemeyi masumiyet karinesi kapsamında incelemiştir. Dava konusu düzenlemeye göre, içeriğin çıkarılması kararının verilebilmesi için söz konusu içeriğe ilişkin yayını yapan kişi hakkında adli sürecin başlaması ve bu kişinin ceza mahkemesince mahkûm edilmiş olması gerekmemekte; 8. maddenin (1) numaralı fıkrasında sayılan suçların işlendiğinin Başkan tarafından *tespit edilmiş olması* gerekli ve yeterli olmaktadır. Mahkeme, Başkan'a ceza yargılamasından kopuk şekilde ve nihai bir tedbir olarak böyle bir yetki verilmesinin masumiyet karinesi ile bağdaşmadığına hükmederek iptal kararı vermiştir⁸⁰⁸:

“Suç şüphesi altında bulunan kişiye ilişkin olarak çeşitli adli ve idari tedbirlerin alınmasına anayasal bir engel bulunmamaktadır. Ancak öngörülen tedbirin ceza yargılaması süreciyle bağlantılı olarak yürütülen geçici bir tedbir niteliğinde

⁸⁰⁵ E.2015/76, K.2017/153 (AYM 15 Kasım 2017), para. 32-33.

⁸⁰⁶ 7253 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda Değişiklik Yapılmasına Dair Kanun.

⁸⁰⁷ 7418 sayılı Basın Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun, (2022), m. 32.

⁸⁰⁸ E.2020/76, K.2023/172. Kararın Resmî Gazete'de yayımlanmasından başlayarak 9 ay sonra, 10.10.2024 tarihinde yürürlüğe girmiştir.

olması gerekir. Ceza yargılaması sürecinden tamamen kopuk olarak uygulanan ve nihai nitelik taşıyan tedbirler, kişinin ceza mahkemesi kararından önce suçlu muamelesi görmesi sonucunu doğurduğundan masumiyet karinesini zedeler.

Dava konusu kurallarda öngörülen tedbirin ceza yargılaması sürecinden kopuk ve Başkan tarafından yapılacak bir suç tespitine bağlı olarak uygulanan nihai bir tedbir niteliğinde olduğu anlaşılmaktadır. Başkan tarafından uygulanan idari tedbir, tedbirin uygulamasının gerekçesini oluşturan suçla ilgili olarak başlatılan ceza soruşturması sürecinde gözden geçirilememekte, yargılama mahkûmiyet dışında bir hükümle neticelense bile içeriğin çıkarılması kararı ayakta kalmaya devam etmektedir. Bu durumda, masumiyet karinesinin birinci boyutunu oluşturan ve bir kimsenin suçlu olduğu kesinleşmiş bir mahkeme kararıyla tespit edilene kadar ona suçlu gibi muamele edilemeyeceğine ilişkin güvence anlamsız hâle gelmektedir.

Sonuç olarak ceza kanunlarında suç olarak düzenlenen eylemlerin işlendiğinin henüz kesinleşmiş bir mahkeme kararıyla tespit edilmeden idari bir makamın yapacağı suç tespitine bağlı olarak nihai bir tedbir mahiyetinde olan içeriğin çıkarılması kararı verilmesinin ve bu kararın icra edilmemesi durumunda idari para cezası uygulanmasının masumiyet karinesini ihlal ettiği değerlendirilmiştir.”⁸⁰⁹

İptal kararında, BTK Başkanı’nın, Kanun’un 8. maddesinin birinci fıkrasında listelenen suçları oluşturan yayınlara ilişkin olarak içeriğin çıkarılması kararı verme yetkisi ve bu kararı yerine getirmeyen içerik ve yer sağlayıcılara para cezası verme yetkisi iptal edilmiştir.

Mevcut düzenlemeye göre, BTK Başkanı bu suçları oluşturan yayınlara ilişkin olarak artık yalnızca erişim engellenmesi kararı verebilecektir. Söz konusu düzenlemeye göre, esasen suçla ilgili olarak verilecek erişimin engellenmesi kararı da ceza yargılaması süreciyle bağlantılı şekilde ilerlememekte ve yargılamanın sonucuna göre etkisi değişmemektedir. Öte yandan, Mahkemenin 2017 tarihli iptal kararında vurguladığı

⁸⁰⁹ E.2020/76, K.2023/172, para. 88-86.

üzere, idareye kapsamı ve sınırları belirsiz şekilde erişimin engellenmesi kararı verilmesi haberleşme özgürlüğü ve temel hak ve özgürlüklerin sınırlandırılmasına ilişkin güvencelerle bağdaşmamaktadır. Dolayısıyla, Başkan'ın erişimin engellenmesine karar verme yetkisi de aynı sebeplerle Anayasa aykırılık teşkil ettiğinden, Anayasa Mahkemesinin konuya ilişkin tüm kararları dikkate alınarak yeniden düzenlenmesi gerekmektedir.

8. maddede öngörülen usule göre, hizmet sağlayıcıların içeriğin çıkarılması ve/veya erişimin engellenmesi kararlarını derhal ve en geç dört saat içinde yerine getirmesi gerekmektedir. Aksi takdirde, koruma tedbiri olarak verilen kararın yerine getirilmemesi halinde adli para cezasına; idari tedbir olarak verilen kararının yerine getirilmemesi halinde ise idari para cezasına hükmedilecektir.⁸¹⁰

Kanun'un 8. maddesinin on yedinci fıkra hükmüne göre, erişimin engellenmesinde kural olarak URL tabanlı erişim engelleme yöntemi kullanılacaktır. Ancak teknik olarak bu yöntemin uygulanmasının mümkün olmadığı hallerde⁸¹¹ internet sitesinin tamamına erişimin engellenmesi söz konusu olabilecektir. Söz konusu düzenleme, erişimin engellenmesi kararları bakımından ölçülülük değerlendirilmesi yapılmasına imkân sağlamaktadır. Bu madde, erişimin engellenmesi kararlarının kademeli olarak alınmasını ve teknik bir imkânsızlık söz konusu olmadıkça internet sitesinin tamamının erişime engellenmemesini gerektirmektedir. Bununla birlikte, teknik

⁸¹⁰ 8(11). maddede, kararın gereğinin yerine getirilmemesi halinde idari para cezası uygulanacağına dair "...ilgili içerik, yer ve erişim sağlayıcısına,..." ibaresi iptal edilmiş ve 10.10.2024 tarihinde yürürlüğe girmiştir, E.2020/76, K.2023/172, para. 88-86.

⁸¹¹ Recep Tayyip Erdoğan Başvurusu'nda AYM, TİB'den başvuru konusu erişimin engellenmesi kararının yerine getirilmemesinin gerekçesini bildirmesini istemiştir. TİB tarafından yazılan yazıda, erişimin engellenmesi kararlarının yerine getirilmesine ilişkin teknik engeller şu şekilde açıklanmıştır: "Günümüz İnternet dünyasında mevcut teknoloji ile tüm siteye erişim engellenmeden sadece URL bazında engelleme 'http' tipi sitelerde ve bağlantılarda mümkün olmakta, SSL destekli kriptolu 'HTTPS' tipi sitelerde ve bağlantılarda URL bazında engelleme teknik olarak mümkün olamamaktadır. Zira, erişim sağlayıcılarca bu amaçla kullanılan filtreleme cihazlarının teknik özellikleri 'HTTPS' linklerini filtre etmeye imkân vermemektedir. Nitekim, Türkiye'deki büyük erişim sağlayıcılarının (Türk Telekom, Avea, Turkcell, Vodafone, Türksat, TTNET, Turknet, İşnet) bu konuda TİB'e yapmış oldukları bildirim ve cevabi yazılarda bu durum açık ve net şekilde ifade edilmektedir. Dolayısıyla, özellikle 'HTTPS' protokolü ile kriptolu yayın yapan twitter ve facebook benzeri sosyal medya içeriklerine teknik olarak URL bazında erişim engelleme yapılamamaktadır. Bu nedenle, mahkeme kararlarına konu bu tür yasadışı içeriklerin yayından kaldırılması ancak ilgili web sitesi tarafından söz konusu içeriğin yayından çıkartılması ile gerçekleşebilmektedir. Bu yüzden TİB bu gibi durumlarda ilgili İnternet sitesine içerik çıkarmaya ilişkin bildirim e-postası atmak dışında herhangi bir işlem tesis edememektedir. Keza, ilgili sitenin yasadışı içeriği çıkartmamakta direnmesi durumunda, birtakım sakıncalar bulunmakla birlikte, mahkeme kararlarının uygulanması bakımından bahsi geçen sitenin tümüne erişimin engellenmesinden başka çıkar yol kalmamaktadır." Recep Tayyip Erdoğan Başvurusu, para. 17.

bir imkansızlığın olması halinde yargı organları ya da idari makamların, web sitesinin tamamına erişimin engellenmesinin hedeflenen amaç ile orantılı olup olmayacağını ilişkin bir değerlendirme yapmalarını gerektirmemektedir. Bu tür bir tedbir, Avrupa İnsan Hakları Mahkemesi'nin içtihadı uyarınca gerekli olan⁸¹² bir orantılılık testi uygulamasını⁸¹³ gerektirmediğinden, çok miktarda bilgiyi erişilemez hale getirebilecektir. Bu durum uygulamada, internet kullanıcılarının haklarının önemli ölçüde kısıtlanmasına ve ölçülülük kriterine aykırı uygulamalara yol açabilmektedir.⁸¹⁴

27.3.2015 tarihli ve 6639 sayılı Kanun'un 29. maddesi ile eklenen 8/A maddesi ise, gecikmesinde sakınca bulunan hallere ilişkin olarak internet şirketlerine içeriğin çıkarılması ve/veya erişimin engellenmesi kararlarına katlanma yükümlülüğü yüklemektedir. Söz konusu düzenlemede kanunda belirtilen hallerin varlığı halinde⁸¹⁵, kural olarak hâkim kararıyla; içeriklerin ivedilikle yayından çıkarılması ve/veya engellenmesinin gerekli olduğu hallerde ise ilgili idari kurumların talebi üzerine istisnai olarak BTK Başkanı tarafından alınması içeriğin çıkarılması ve/veya erişimin engellenmesi kararı alınması; kararın erişim sağlayıcılar ile içerik ve yer sağlayıcılara Başkan tarafından derhâl bildirilmesi; erişim, içerik ve yer sağlayıcılar tarafından bildirimden itibaren en geç dört saat içinde derhâl uygulanması ve 24 saat içinde sulh ceza hâkiminin onayına sunulması öngörülmüştür. Hâkimin de kararını kırk sekiz saat

⁸¹² AİHM, Ahmet Yıldırım / Türkiye kararında bu gerekliliği şu şekilde ifade etmiştir: “Ancak, başvuruyu değerlendiren hakimlerin, özellikle Google Sites'a erişimi topyekûn engelleme ihtiyacını değerlendirerek çatışan ilgili çıkarları tartmaya çalıştıklarına dair hiçbir gösterge yoktur. Mahkeme'nin görüşüne göre, bu eksiklik, yerel mahkemelere Mahkeme'nin Sözleşme'nin 10. maddesi uyarınca belirlediği kriterlere uygun olarak Google Sites'ın topyekûn erişime engellenmesinin gerekliliğine ilişkin bir inceleme yükümlülüğü öngörmeyen 5651 sayılı Kanun'un 8. maddesinin lafzının bir sonucudur. Bununla birlikte, bu tür bir yükümlülük doğrudan Sözleşme'den ve Sözleşme kurumlarının içtihatlarından kaynaklanmaktadır. Mahkemeler, kararlarını verirken, ihlalde bulunan web sitesine erişimi engellemenin tek yolunun Google Sites'a erişimin topyekûn engellemesi olduğunu tespit etmiştir. Bununla birlikte, Mahkeme'nin görüşüne göre, diğer unsurların yanı sıra, bu tür bir tedbirin çok miktarda bilgiyi erişilemez hale getirerek, İnternet kullanıcılarının haklarını önemli ölçüde kısıtladığını ve önemli bir yan etkiye sahip olduğunu dikkate almaları gerekirdi.” Ahmet Yıldırım v. Turkey, 3111/10 (ECtHR 18 Aralık 2012), para. 66.

⁸¹³ “Venice Commission on Law No. 5651 on Regulation of Publications on the Internet and Combating Crimes Committed by Means of Such Publication (“The Internet Law”), CDL-AD (2016)011, 2016.”, s. 27.

⁸¹⁴ Baran Tursun Uluslararası, Dünya Ölçeğinde Silahsızlanma, Yaşam Hakkı, Özgürlük, Demokrasi, Barış ve Dayanışma Vakfı (Baransav) ve Keskin Kalem Yayıncılık ve Ticaret A.Ş. Başvurusu, 2015/18581 (AYM 26 Eylül 2019), para. 55; Cahit Yiğit Başvurusu, 2016/2736 (AYM 27 Kasım 2019) para. 39; Ali Ergin Demirhan Başvurusu, 2015/16368 (AYM 11 Mart 2020), para. 39. Danıştay da teknik imkansızlık gerekçesiyle bir sitenin tamamına yönelik erişimin engellenmesi kararının verilmesinin hukuka aykırı olduğunu yönünde karar vermektedir. E.2015/1192, K. 2020/1077 (Danıştay 13. D. 02 Haziran 2020).

⁸¹⁵ Bu haller, “yaşam hakkı ile kişilerin can ve mal güvenliğinin korunması, milli güvenlik ve kamu düzeninin korunması, suç işlenmesinin önlenmesi veya genel sağlığın korunması sebeplerinden bir veya birkaçıdır.”, “İnternet Kanunu”, m. 8/A(1).

içinde açıklaması gerekmektedir; aksi takdirde karar kendiliğinden kalkmaktadır.⁸¹⁶ Kanun'un 8/A maddesine göre, ilgili internet şirketleri ayrıca, maddede belirtilen suçların faillerine ulaşmak için gerekli olan bilgileri hâkim kararı üzerine adli mercilere vermekle de yükümlüdür.⁸¹⁷

Gecikilmesi halinde telafisi imkânsız zararların ortaya çıkabileceği hallerde istisnai olarak Başkan tarafından karar alınması halinde, bu idari tedbir kararının yirmi dört saat içerisinde hâkim onayına sunulması gerekliliği, bahsi geçen kararların hukuki denetime tabi olmasını sağlamaktadır. Bununla birlikte, bu madde kapsamında alınan kararların çelişmeli bir yargılamada bir mahkeme tarafından gözden geçirilme olasılığı bulunmamaktadır. Başka bir ifadeyle, bu hukuki denetimde karşı tarafın görüşleri alınamamakta; hâkim kararını dosya üzerinden, delil toplamaksızın, sınırlı bir inceleme ile vermektedir.⁸¹⁸ Öte yandan, tedbir kararının akabinde, failler hakkında soruşturma açıldığı takdirde soruşturma veya kovuşturmanın sonucuna göre yargı mercileri tarafından erişimin engellenmesi tedbirinin akıbeti hakkında bir karar verilebilmesi mümkünken; soruşturma açılmadığı takdirde erişimin engellenmesine ilişkin söz konusu tedbir, internet kullanıcılarını engellenen içeriğe belirsiz bir süreyle erişmekten alıkoyacaktır.⁸¹⁹ Örneğin, Wikipedia'nın yaklaşık üç yıl süre ile erişime kapatılmasını konu alan bireysel başvuru kararında AYM, makale içeriklerinde yer alan ve çoğu tartışmalı ifadelerin sahipleri bilindiği halde bu kişiler hakkında da bir ceza soruşturması yoluna başvurulmasının tercih edilmemiş olduğuna dikkat çekmiştir.⁸²⁰ Dolayısıyla, Wikipedia'nın kapatılmasını haklı gösteren vahim nitelikte bir içerik bulunmamasına rağmen⁸²¹ çok sayıda internet kullanıcısı tarafından aktif şekilde kullanılan platforma uzun bir süre erişilememiştir.

Anayasa Mahkemesi, söz konusu düzenlemenin bu yönlerini ve bunun ifade özgürlüğü üzerindeki etkilerini dikkate alarak, 8/A maddesinin; ancak ivedilikle müdahale etmeyi gerektirecek hâllerde işletilmesi gereken istisnai bir yol olduğunu değerlendirmiştir. Bu istisnai yolun tespitine ilişkin olarak da Mahkeme, *bir görüşte*

⁸¹⁶ "İnternet Kanunu", m. 8/A(2).

⁸¹⁷ "İnternet Kanunu", m. 8(A)/4.

⁸¹⁸ Birgün İletişim ve Yayıncılık Ticaret A.Ş. Başvurusu, 2015/18936 (AYM [GK] 12 Temmuz 2019), para. 69.

⁸¹⁹ Birgün İletişim ve Yayıncılık Ticaret A.Ş. Başvurusu, para. 70.

⁸²⁰ Wikimedia Foundation Inc. ve Diğerleri Başvurusu, 2017/22355 (AYM [GK] 26 Aralık 2019) para. 94.

⁸²¹ Wikimedia Foundation Inc. ve Diğerleri Başvurusu, para. 94.

haklılık veya ilk bakışta (prima facie) haklılık kriteri geliştirmiş; erişimin engellenmesi tedbirinin haklılığını bu kriterlerin gerçekleşmesine bağlamıştır.⁸²² Buna göre, “*şiddeti öven, kişileri terör örgütünün yöntemlerini benimsemeye, şiddet kullanmaya, nefrete, intikam almaya veya silahlı direnişe tahrik ve teşvik eden yayınlar gibi internet ortamında demokratik toplum düzenini tehlikeye atan yayınların daha ileri bir inceleme yapılmaya gerek olmaksızın ilk bakışta anlaşılabilirdiği hâllerde 5651 sayılı Kanun’un 8/A maddesinde öngörülmüş olan ve Başkan tarafından verilen kararı içeren istisnai usul işletilebilir.*”⁸²³ Mahkeme, bu sayede internet ortamında yapılan yayınlara karşı kamusal menfaatlerin hızlı bir şekilde korunması ihtiyacıyla ifade hürriyeti arasında adil bir denge sağlanabileceğini belirtmiştir. Anayasa Mahkemesi’nin Kanun’un 8/A maddesinin uygulanmasına ilişkin ortaya koyduğu bu güvenceler uygulamada bir karşılık bulamamıştır.

Nitekim, Anayasa Mahkemesi, *Artı Media Gmbh*⁸²⁴ kararında, Kanun’un 8/A maddesindeki usulün yargılama hukukunun usule ilişkin güvencelerini barındırmadığını, sıkı ve etkili bir koruma mekanizmasına sahip olmadığını, demokratik toplum düzeninin gereklerine uygun ve orantılı karar verilmesini sağlayacak güvenceleri içermediğini tespit ederek ifade ve basın özgürlüklerini ihlal ettiğini tespit etmiş ve ihlalin doğrudan kanundan kaynaklandığı sonucuna varmıştır.⁸²⁵

Kanunda öngörülen üçüncü usul ise, 9/A maddesinde öngörülen özel hayatın gizliliği nedeniyle içeriğe erişimin engellenmesi usulüdür. Bu maddede, ilgili internet yayını dolayısıyla özel hayatının gizliliğinin ihlal edilmesi halinde; i. özel hayatının gizliliğinin ihlal edildiğini iddia eden kişilerin başvurusu üzerine ya da ii. gecikmesinde sakınca bulunan hallerde doğrudan Başkanın emri üzerine BTK tarafından tedbiren⁸²⁶ erişimin engellenmesine karar verilmesi öngörülmüştür. Her iki durumda da karar Kurum tarafından verilmekte, ardından hâkimin onayına sunulmaktadır.

⁸²² Birgün İletişim ve Yayıncılık Ticaret A.Ş. Başvurusu, para. 71.

⁸²³ Birgün İletişim ve Yayıncılık Ticaret A.Ş. Başvurusu, para. 72; Wikimedia Foundation Inc. ve Diğerleri Başvurusu, para. 75.

⁸²⁴ Artı Media Gmbh Başvurusu, 2019/40078 (AYM [GK] 14 Eylül 2023).

⁸²⁵ Artı Media Gmbh Başvurusu, para. 44-47; Ahmet Alphan Sabancı ve Diğerleri Başvurusu, 2015/13667 (AYM 21 Kasım 2023).

⁸²⁶ “İnternet Kanunu”, m. 9/A(1).

Eriřim saęlayıcılar, Başkan tarafından kiřilerin talebi üzerine verilen eriřimin engellenmesi kararının Eriřim Saęlayıcıları Birlięi'ne bildirilmesinden itibaren derhal, en ge drt saat iinde kararın gereęini yerine getirmekle ykmldr. Bu durumda, eriřimin engellenmesini talep eden kiřiler, talepte bulunduęu andan itibaren yirmi drt saat iinde hâkim onayına sunmakla ykmldr. Hâkimin kararını kırk sekiz saat iinde aıklamaması halinde, eriřimin engellenmesi kararı kendilięinden kalkmaktadır.⁸²⁷

zel hayatın gizlilięinin ihlaline baęlı olarak gecikmesinde sakınca bulunan hallerde doęrudan Başkan tarafından verilen kararın ise, yine Başkan tarafından yirmi drt saat iinde hâkim onayına sunulması ve hâkimin de kararını kırk sekiz saat iinde aıklaması gerekmektedir.⁸²⁸ 9/A maddesinin on birinci fıkrasında, beřinci fıkrada belirtilenin aksine, hakim kararının kırk sekiz saat iinde aıklanmaması halinde eriřimin engellenmesi kararının akıbetinin ne olacaęına iliřkin bir dzenlemeye yer verilmemiřse de, Anayasa Mahkemesi; belirtilen srede hakim onayına sunulmaması ya da hakim'in belirtilen srede kararını aıklamaması halinde eriřimin engellenmesi kararının kendilięinden kalkacaęına iliřkin kuralın bu usul bakımından da geerli olduęunu kabul etmiřtir.⁸²⁹

9/A maddesinin drdnc fıkrasında, eriřimin engellenmesi kararının her iki durumda da zel hayatın gizlilięini ihlal eden yayın, kısım, blm, resim, video ile ilgili olarak uygulanacaęı belirtilmektedir.⁸³⁰

Kanun'da ngrlen dięer usuller gibi, 9/A maddesinde ngrlen usul de Anayasa Mahkemesi tarafından incelenmiřtir. Anayasa Mahkemesi 2015 tarihinde verdięi kararında, 9/A maddesi ile haberleřme ve ifade zgrlęne getirilen sınırlamaların bařkalarının hak ve zgrlklerinin korunması meřru amacına dayandıęını, idareye verilen yetkinin kapsam ve usulleri ile bu yetkiyi nasıl kullanacaęı ve eriřimin engellenmesini ne řekilde uygulayacaęı ayrıntılı bir řekilde gsterildięi, "*zel hayatın gizlilięinin ihlali*" ve "*gecikmesinde sakınca bulunan haller*" ibarelerinin ierik ve kapsamının kanun koyucu tarafından nceden tek tek belirlenmesinin mmkn

⁸²⁷ "İnternet Kanunu", m. 9/A (5).

⁸²⁸ "İnternet Kanunu", m. 9/A (9).

⁸²⁹ E.2014/92, K.2016/6 (AYM 28 Ocak 2016), para. 69.

⁸³⁰ "İnternet Kanunu", m. 9/A(4); AYM, E.2014/87, K.2015/112 2015, para. 245.

olmadığını belirterek düzenlemenin Anayasa'ya aykırı olmadığına karar vermiş ve iptal talebini reddetmiştir.⁸³¹

Anayasa Mahkemesinin Kanun'da öngörülen diğer usullere ilişkin yıllar içinde dönüşen içtihadı göz önünde bulundurulduğunda, 9/A maddesinde öngörülen usulün de Anayasa'da öngörülen güvencelere uygun olmadığını söylemek mümkündür. Nitekim Venedik Komisyonu'nun, 5651 sayılı Kanunla ilgili görüşünde, 9/A maddesinin bir ceza veya hukuk usulü çerçevesinde alınan geçici veya ihtiyati bir tedbirle ilgili olmamasına rağmen yargılama hukukuna ilişkin güvenceleri sağlamadığını; duruşma yapılmasını orantılılık değerlendirmesi ve kararın müteakip bir yargılamada yeniden değerlendirilmesini gerektirmediğini belirtilerek değiştirilmesi tavsiye edilmiştir.⁸³²

Kanunun 9/A maddesi, idari bir kurum olan BTK tarafından erişimin engellenmesi kararı alınmasını ve kararın sonradan hâkim denetimine sunulmasını öngörmektedir. Söz konusu düzenlemede hangi gerekçelerin idari bir organ tarafından derhal engellemeyi haklı kılabilceği belirtilmemiştir. Sekizinci fıkrada öngörülenin aksine, birinci fıkrada öngörülen usul gecikmesinde sakınca bulunan hallerle de sınırlandırılmamıştır. Oysa Anayasa'nın 22. maddesine göre, haberleşme hürriyetine idari mercii kararıyla müdahale ancak gecikmesinde sakınca bulunan hallerde mümkündür.⁸³³ Başkanın kararı yargı denetimine tabi olsa ve karar yargı denetimi sonucunda kaldırılrsa bile Başkan tarafından uygulanan tedbir ifade özgürlüğü hakkına ciddi bir müdahale ile sonuçlanmış olacaktır.⁸³⁴ Öte yandan, beşinci fıkrada hâkimin kararını, "*özel hayatın gizliliğinin ihlal edilip edilmediğini değerlendirerek*" vereceğinden bahsedilmekteyse de en geç kırk sekiz saat içinde açıklanması gereken bu karar kapsamında ne şekilde bir inceleme yapılacağı hususu da belirsizdir. Kanun'un 9A maddesi, bu sebeplerle hem ifade özgürlüğünün hem de özel hayatın gizliliğinin korunması bakımından yeterli güvence sağlamamaktadır.

⁸³¹ AYM, E.2014/87, K.2015/112, para. 237-243.

⁸³² "Venice Commission on Law No. 5651 on Regulation of Publications on the Internet and Combating Crimes Committed by Means of Such Publication ("The Internet Law"), CDL-AD (2016)011, 2016.", para. 61, 62.

⁸³³ Anayasa, m. 22(2).

⁸³⁴ "Venice Commission on Law No. 5651 on Regulation of Publications on the Internet and Combating Crimes Committed by Means of Such Publication ("The Internet Law"), CDL-AD (2016)011, 2016." para. 71.

Anayasa Mahkemesi tarafından iptal edilen 9. madde ise bir tedbir kararı niteliğinde olmayıp kişilik haklarının ihlal edilmesi halinde erişimin engellenmesine ilişkin esaslı kararların alındığı tam teşekküllü ve bağımsız bir usul teşkil etmekteydi. Bu maddede, internet yayını nedeniyle kişilik haklarının ihlal edildiğini iddia eden kişiler için; i. içerik sağlayıcısına, buna ulaşılamaması halinde yer sağlayıcısına başvuru ve ii) doğrudan sulh ceza hakimine başvuru şeklinde iki yol öngörülmüştü. Buna göre, içerik ve/veya yer sağlayıcıların, kişilik haklarının ihlal edildiğini iddia eden kişilerin taleplerini yirmi dört saat içinde cevaplandırmaları gerekmekteydi. Dolayısıyla bu madde servis sağlayıcılara, adli ve idari merciler tarafından alınan kararlara katlanma yükümlülüğü yanında kişiler tarafından uyarı yöntemi ile yapılan başvuruları cevaplandırma yükümlülüğü de yüklemekteydi.

9. maddede öngörülen içeriğin çıkarılması ve/veya erişimin engellenmesi usulü, taleplerin sulh ceza hâkimliğince 24 saat içinde ve duruşma yapılmaksızın dosya üzerinden karara bağlanmasını gerektirmekteydi. Dolayısıyla, bu madde herhangi bir hukuk veya ceza usulünün tesis edilmesini gerektirmemiştir. Öte yandan, bu madde kapsamında alınan kararların üst derece mahkemesi tarafından denetlenebilmesi de söz konusu değildi. Bu durum, 9. madde kapsamında alınan kararlarda hem ifade özgürlüğü hem de özel hayatın gizliliğine ilişkin hak ihlallerine yol açmıştır.

9. madde metninde bu yönde bir ifadeye yer verilmese de bu maddede öngörülen usul Anayasa Mahkemesi içtihadında yıllarca, *özel hayatın ve kişilik haklarının hızlı ve etkili bir şekilde korunması ihtiyacı nedeniyle öngördüğü özel ve hızlı sonuç alınabilecek bir koruma tedbiri kararı* olarak nitelendirilmiştir. Buna göre, 9. madde kapsamında içeriğin çıkarılması ve/veya erişimin engellenmesi kararının ancak, kişinin çıplak resimlerinin veya video görüntülerinin yayımlanması gibi kişilik haklarının ihlal edildiğinin daha ileri bir inceleme yapılmaya gerek olmaksızın ilk bakışta anlaşılabildiği hâllerde verilebileceğini kabul etmiştir.⁸³⁵ Nitekim Mahkeme çeşitli bireysel başvuru kararlarında, böyle bir durum söz konusu olmamasına rağmen Kanun'un 9. maddesinin uygulanmasının Anayasa'ya aykırılık teşkil ettiğine karar vermiştir.⁸³⁶

⁸³⁵ Ali Kızık Başvurusu, para. 62, 63.

⁸³⁶ Miyase İlknur ve Diğerleri Başvurusu, 2015/15242 (AYM 18 Temmuz 2018); Ips İletişim Vakfı Başvurusu, 2015/14758 (AYM 30 Ekim 2018); Ips İletişim Vakfı (2), 2015/15873 (AYM 07 Mart 2019).

Keskin Kalem Yayıncılık ve Ticaret A.Ş. ve Diğerleri kararında ise Mahkeme, sorunun kanundan kaynaklandığına karar vererek pilot karar usulünün⁸³⁷ uygulanmasına karar vermiştir.⁸³⁸ Bu kararda Anayasa Mahkemesi, Kanun'un 9. maddesine ilişkin olarak şu değerlendirmelerde bulunmuştur:

*"...dava ve itiraz konusu kuralların kişilik haklarına yapılan saldırılara karşı internet içeriğinin sınırlandırılmasına yönelik kademeli bir müdahale yöntemi sunmadığı ve kurallar kapsamında yapılan sınırlamanın internet ortamında yer alan belirli bir içeriğe erişimi engellemek suretiyle o içeriğin belirli bir ülke sınırları içinden ulaşılmasına, kararın verildiği tarihten itibaren süresiz olarak engel olduğu anlaşılmaktadır. Bu yönüyle kurallar ifade ve basın özgürlüklerine ağır bir müdahale teşkil etmektedir. Kurallar ile düzenlenen usul, internet ortamında bulunan zararlı içeriklerle diğer başka usullerle mücadele edilebildiği sürece başvurulmaması gereken bir yöntemdir. Bu çerçevede kurallar, kamusal makamların takdir yetkisini daraltarak keyfi davranışların önüne geçebilmek için yargılama hukukunun usule ilişkin güvencelerinin yanında demokratik toplum düzeninin gereklerine uygun ve orantılı karar verilmesini sağlayacak güvenceleri de barındırmamaktadır."*⁸³⁹

Mahkeme 9. maddenin ifade özgürlüğü bakımından yargılama usulüne ilişkin güvenceler yanında demokratik toplum düzeninin gereklerine uygun ve orantılı karar verilmesini sağlayacak güvenceleri içermediğine ilişkin tespitlerinin kişilik hakları bakımından da geçerli olduğunu belirtmiştir. Dolayısıyla, söz konusu düzenleme, ifade özgürlüğüne yönelik keyfi müdahalelere karşı yeterli güvence içermediği gibi kişilik hakları bakımından da etkili bir başvuru yolu teşkil etmemiştir.⁸⁴⁰

⁸³⁷ Pilot karar usulü, İhlalin yapısal bir sorundan kaynaklandığının tespiti ile bu sorunun başka başvurulara, bir diğer ifadeyle yeni ihlallere sebebiyet verdiğinin anlaşılması veya bu durumun yeni başvurulara sebebiyet verebileceğinin öngörülmesi hâlinde uygulanan bir usuldür. Pilot karar usulünün uygulanmasıyla benzer nitelikteki başvurular idari mercilerce bu ilkeler çerçevesinde çözümlenir; çözümlenmediği takdirde Mahkeme tarafından topluca görülerek karara bağlanır. Anayasa Mahkemesi İçtüzüğü, R.G. 12.07.2012/28351, m. 75.

⁸³⁸ *Keskin Kalem Yayıncılık ve Ticaret A.Ş. ve Diğerleri* Başvurusu, 2018/14884 (AYM [GK] 27 Ekim 2021).

⁸³⁹ *Keskin Kalem Yayıncılık ve Ticaret A.Ş. ve Diğerleri* Başvurusu, para. 129-132.

⁸⁴⁰ İ.D. ve Diğerleri Başvurusu, 2016/14513 (AYM 28 Aralık 2022); Atalay Candelen ve Diğerleri Başvurusu, 2016/596 (AYM 25 Ocak 2024).

Keskin Kalem Yayıncılık ve Ticaret A.Ş. ve Diğerleri kararıyla, 5651 sayılı Kanun'un sistematik olarak ihlale yol açtığı değerlendirilmesine rağmen, tespit edilen yapısal sorunun çözümü için gerek yasama organı gerek ilgili kamu otoritelerince bir değişiklik gerçekleştirilmediği gibi sulh ceza hâkimliklerince söz konusu madde kapsamında içeriğin çıkarılması ve erişimin engellenmesi kararı verilmeye devam etmiştir. Anayasa Mahkemesi de bu doğrultuda, benzer nitelikteki başvurular hakkında toplu şekilde karar vermiştir.⁸⁴¹

Kanunun 9. maddesine ilişkin bu süreç, AYM'nin 11/10/2023 tarih ve E.2020/76, K.2023/172 sayılı kararıyla son bulmuştur. Söz konusu maddede yer alan çeşitli düzenlemelerin Anayasa'ya aykırı olduğu iddiasıyla açılan davada AYM, 9. maddenin tamamını, iptal kararı sonrası uygulanma imkânı kalmadığı gerekçesiyle iptal etmiştir.⁸⁴² İptal kararıyla, arama motorlarına kişilik haklarını ihlal eden içeriklere ilişkin olarak başvuranın adının kişilik haklarını ihlal eden içeriklerle ilişkilendirilmemesini sağlama yükümlülüğü yükleyen, bu bakımdan unutulma hakkına yasal dayanak teşkil eden onuncu fıkra hükmü de yürürlükten kalkmıştır.⁸⁴³

Anlaşılabacağı üzere, 5651 sayılı Kanun uyarınca hizmet sağlayıcılara internet içeriğinin çıkarılması ve/veya erişimin engellenmesine ilişkin yükümlülük yükleyen maddeler Anayasa'da öngörülen güvencelerle bağdaşmamaktadır. Kanun'da öngörülen usullere ilişkin temel sorunlardan biri, idari mercilerin suç tespiti yapma ve bu kapsamda hâkim kararı güvencesine aykırı şekilde resen karar alma yetkisi verilmiş olmasıdır. Sorunun diğer boyutu ise, Kanun'un genel gerekçesinde tedbir olarak nitelendirilen usullerin ilgili ve yeterli gerekçe gösterilmeksizin ve yargılama hukukunun usulüne ilişkin güvencelerinden yoksun şekilde süresiz etki gösterecek şekilde uygulanmasıdır. Tüm tarafların sürece dahil edilmemesi ve bu eksikliklerin yargılamanın ilerleyen aşamalarında telafi edilmesini sağlayacak mekanizmaların eksikliği ve demokratik

⁸⁴¹ Abdullah Kaya ve Diğerleri Başvurusu, 2016/1430, (22 Kasım 2023), para. 17.

⁸⁴² AYM, E.2020/76, K.2023/172, 11.10.2023. Kararın Resmî Gazete'de yayımlanmasından başlayarak 9 ay sonra, 10.10.2024 tarihinde yürürlüğe girmiştir.

⁸⁴³ Anayasa Mahkemesi tarafından iptal edilen 9. maddenin onuncu fıkrasında, unutulma hakkı şu şekilde düzenlenmişti: “İnternet ortamında yapılan yayın içeriği nedeniyle kişilik hakları ihlal edilenlerin talep etmesi durumunda hâkim tarafından, başvuranın adının bu madde kapsamındaki karara konu internet adresleri ile ilişkilendirilmemesine karar verilebilir. Kararda, Birlik tarafından hangi arama motorlarına bildirim yapılacağı gösterilir.”

toplum düzeninin gereklerine uygun ve orantılı karar verilmesini sağlayacak güvencelerin olmaması Anayasa'ya aykırı kararlara yol açmaktadır.

Nitekim Venedik Komisyonu da İnternet Kanunu ile ilgili görüşünde, Kanun'da öngörülen usullere ilişkin kapsamlı değerlendirmelerde bulunmuştur. Komisyon, Kanun'un 8. maddesi kapsamında bir ceza yargılamasına bağlı olarak ortaya çıkan ve kaderi ceza yargılamasına bağlı olan erişimin engellenmesi usulünün “*tedbir*” niteliği taşıdığını belirtmiştir.⁸⁴⁴ Nitekim, 8. maddenin yedinci ve sekizinci fıkralarına göre, söz konusu yargılama sonucunda kovuşturmayaya yer olmadığına hükmedilmesi ya da beraat kararı verilmesi halinde içeriğin çıkarılması ve/veya erişimin engellenmesi kararı hükümsüz kalmaktadır.⁸⁴⁵ Venedik Komisyonu, 8. madde uyarınca Başkan'ın yargı denetimi olmaksızın erişimin engellenmesine karar verebilme yetkisinin yeniden gözden geçirilmesi gerektiğini belirtmektedir.

Öte yandan, Komisyon, Kanunu'nun 8A, 9 ve 9A maddelerinde öngörülen erişimin engellenmesi usullerinin ise, 8. maddede öngörülen usulden farklı olarak bağımsız ve özel bir erişim engelleme mekanizması teşkil ettiğini; bu usuller çerçevesinde, esas yargılamadaki bir sonuç beklenmeksizin, çelişmeli bir yargılamada bir mahkeme tarafından gözden geçirilme olasılığı olmadan, duruşma yapılmaksızın ve üst mahkemeye itiraz imkânı olmaksızın alınacak kararların, ifade özgürlüğüne ilişkin usul güvencelerini sağlamakta yetersiz kalacağını değerlendirmiştir.⁸⁴⁶

B. Sosyal Ağ Sağlayıcıların Ek Yükümlülükleri

İnternet teknolojilerindeki gelişmelerle birlikte sosyal ağların kullanımının yaygınlaşması bu hizmetleri sağlayan internet şirketlerinin sayısının artmasına ve internetin yönetiminde daha etkili olmalarına yol açmıştır. Bu değişiklik, bir yandan sosyal hayatı zenginleştiren, bilgi edinme süreçlerini kolaylaştıran, yeni iş fırsatları doğuran; diğer yandan bireylerin başta kişilik hakları olmak üzere temel haklarına ağır saldırıların gerçekleştirildiği ve yanlış bilgilerin yayılması, siber zorbalık, sanal

⁸⁴⁴ Venice Commission, On Law No. 5651 on Regulation of Publications on the Internet and Combating Crimes Committed by Means of Such Publication (“The Internet Law”), CDL-AD (2016)011, 2016, para. 34.

⁸⁴⁵ “İnternet Kanunu”, m. 8(7,8).

⁸⁴⁶ Venice Commission On Law No. 5651 on Regulation of Publications on the Internet and Combating Crimes Committed by Means of Such Publication (“The Internet Law”), para. 60.

dolandırıcılık, pornografi, çocuk istismarı, fuhuş, kumar, şiddetin, nefretin ve ırkçılığın yayılması, terörizmin desteklenmesi ve yaygınlaştırılması gibi topluma ve devlete yönelik gerçek güvenlik risklerinin ve zararlarının oluşmasına neden olan internetin hukuken ele alınış biçimini de doğrudan etkilemiştir. Buna göre, sunulan hizmetin insan haklarına etkisi daha büyük ve olası zararının daha fazla olduğu durumlarda, bu hizmetin yerine getirilmesine ilişkin sorumluluk ve yükümlülükler de o kadar büyük olmalıdır.

Sosyal medya platformlarında üretilen içeriği kontrol altında tutma, kullanıcıların etkileşim yöntemlerini ve biçimini belirleme imkânı önemli oranda sosyal medya şirketlerinin elindedir. Bu platformlar kullanıcılar arasında yaygın şekilde kullanıldığından sosyal medya şirketlerinin hak ve yükümlülüklerini gösteren, onların davranışlarını düzenleyen, kesin ve öngörülebilir bir mevzuat sisteminin oluşturulması kaçınılmazdır.⁸⁴⁷

Bu kapsamda, 7253 sayılı Kanun⁸⁴⁸ ile sosyal ağ sağlayıcılar, 5651 sayılı İnternet Kanunu kapsamında özel olarak ele alınmış ve temel hak ve özgürlükler üzerindeki güç ve etkileri dikkate alınarak kapsamlı yükümlülöklere tabi kılınmıştır.

İnternet Kanunu'nun 2. maddesinde sosyal ağ sağlayıcılar, “*sosyal etkileşim amacıyla kullanıcıların internet ortamında metin, görüntü, ses, konum gibi içerikleri oluşturmalarına, görüntülemelerine veya paylaşımlarına imkân sağlayan gerçek veya tüzel kişiler*” olarak tanımlanmıştır. Bu tanıma göre, sosyal ağ sağlayıcılar kavramı ile sosyal etkileşim amacı bulunan, kullanıcıların içerik oluşturabildikleri, görüntüleyebildikleri veya paylaşabildikleri yer sağlayıcı niteliği bulunan ortamların ifade edildiği anlaşılmaktadır.⁸⁴⁹ Dolayısıyla, sosyal ağ sağlayıcılar, yer sağlayıcıların bir alt kategorisi olarak ifade edilebilir. Yer sağlayıcılar ile sosyal ağ sağlayıcılar arasındaki temel fark, depolanan bilgilerin kullanıcı etkileşimi ve sosyal bağlar ön planda tutularak kamuya yayılmasında yatmaktadır. Yer sağlayıcılar yalnızca bilgi depolarken, sosyal ağlar ayrıca bilgileri kamuya açık hale getirmektedir.⁸⁵⁰

⁸⁴⁷ Recep Tayyip Erdoğan Başvurusu, para. 44-47.

⁸⁴⁸ 7253 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda Değişiklik Yapılmasına Dair Kanun.

⁸⁴⁹ AYM, E.2020/76, K.2023/172, para. 6.

⁸⁵⁰ Buiten, “The Digital Services Act”, 2021, s. 23.

Belirtmek gerekir ki, aynı zamanda bir yer sağlayıcı olan sosyal ağ sağlayıcılar da İnternet Kanunu’nun 5. maddesinin birinci fıkrası uyarınca, üçüncü tarafların hukuka aykırı içeriklerinden sorumluluktan muaftır. Sosyal ağ sağlayıcılar, kural olarak yer sağladığı içeriği kontrol etmek veya hukuka aykırı bir faaliyetin söz konusu olup olmadığını araştırmakla yükümlü değildir. Bununla birlikte, Ek 4. madde ile sosyal ağ sağlayıcılarına, içerik veya yer sağlayıcı olmalarından kaynaklanan mevcut sorumluluklarına ek olarak yeni yükümlülükler yüklenmiştir. Bu düzenlemeyle, sosyal ağ sağlayıcılarının hem genel olarak içerik ve yer sağlayıcı olmaktan kaynaklanan yükümlülükleri hem de bu maddede özel olarak belirtilen yükümlülükleri yerine getirmeleri amaçlanmıştır.⁸⁵¹ Başka bir deyişle, sosyal ağ sağlayıcılara yönelik daha kapsamlı bir yükümlülük alanı oluşturulmuştur. Bu yükümlülükler, temsilci belirleme ve bildirme, şeffaflık, içerik moderasyonu, bilgi paylaşma, kullanıcı haklarına saygı, veri saklama, çocuk koruma ve kriz planı oluşturma yükümlülükleridir. Yükümlülüklerin kapsamı ise sosyal ağ sağlayıcının Türkiye’deki kullanım yoğunluğuna göre değişiklik göstermektedir.

1. Temsilci Belirleme ve Bildirme Yükümlülüğü

Temsilci belirleme ve bildirme yükümlülüğü ile kişiler tarafından yapılacak başvuruların cevaplandırılması ve yetkili makamlarca gönderilecek tebligat, bildirim veya taleplerin alınarak gereğinin yapılmasını sağlamak üzere sosyal ağ sağlayıcılar ile muhataplık ilişkisinin kurulması amaçlanmıştır.⁸⁵² Ek 4. maddenin birinci fıkrasına göre, Türkiye’den günlük erişimi bir milyondan fazla olan yurt dışı kaynaklı sosyal ağ sağlayıcıların, Türkiye’de temsilci belirlemeleri ve bildirmeleri gerekmektedir. Türkiye’den günlük erişimi belirtilen sayının altında olan sosyal ağ sağlayıcılar bu madde kapsamında temsilci belirleme ve bildirme yükümlülüğü altında değildir. Öte yandan, sosyal ağ sağlayıcıya Türkiye’den günlük erişim on milyondan fazla ise, sosyal ağ sağlayıcının sorumluluğu saklı kalmak kaydıyla, temsilci de teknik, idari, hukuki ve mali yönlerden tam yetkili ve sorumludur.⁸⁵³

⁸⁵¹ “İnternet Kanunu”, m. Ek 4(17).

⁸⁵² Genel Gerekçe, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun.

⁸⁵³ “İnternet Kanunu”, m. Ek 4(1).

Maddenin ikinci fıkrasında sosyal ağ sağlayıcıların temsilci belirleme ve bildirme yükümlülüğünün yerine getirilmemesi haline ilişkin olarak kademeli bir yaptırım sistemi öngörülmüştür. Buna göre, bildirimden sonra sosyal ağ sağlayıcıya sırasıyla idari para cezası, reklam verme yasağı, internet trafiği bant genişliğinin yüzde elli oranında daraltılması ve internet trafiği bant genişliğinin yüzde doksan oranına kadar daraltılması şeklinde yaptırımlar uygulanabilmektedir. Söz konusu yükümlülüğün yaptırım kararının ardından yerine getirilmesine ilişkin olarak idari para cezalarında indirim; diğerlerinde ise cezanın kaldırılması öngörülmektedir.⁸⁵⁴

Trafik bant genişliğinin yüzde doksan oranına kadar kısıtlanabilmesi yaptırımı, sosyal ağın neredeyse erişilemez hale gelmesine neden olabilecektir. Bu bakımdan sosyal ağ sağlayıcıların teşebbüs özgürlüğüne ve kullanıcıların da iletişim hakkı, ifade özgürlüğü, özel hayata saygı, haberleşme özgürlüğü ile basın özgürlüğü kapsamında çeşitli eleştirilere konu olmuştur.⁸⁵⁵ Anayasanın 13. maddesi uyarınca, temel hak ve özgürlüklere yönelik müdahaleler meşru amaca dayanmalı ve ölçülü olmalıdır. Bununla birlikte, müdahalenin ölçülülüğünden söz edebilmek için müdahale aracının amacı gerçekleştirmeye elverişli olması, aynı amacın daha hafif bir tedbir ile gerçekleştirilmesinin mümkün olmaması ve uygulanan tedbir ile bireyin hakkına yapılan müdahale ile kamusal yarar arasında makul bir dengenin gözetilmesi gerekmektedir.

Ek 4. maddede düzenlenen temsilci belirleme ve bilgilendirme yükümlülüğü ile Kanunun etkili şekilde uygulanabilmesi için sosyal ağ sağlayıcılar ile muhataplık ilişkisi kurulması amaçlanmaktadır. Söz konusu yaptırımlarla da sosyal ağ sağlayıcılar, adım adım temsilci belirlemeye zorlanmaktadır. Dolayısıyla müdahalenin, kamu düzeninin korunması ve kullanıcı haklarının korunması meşru amacına dayandığı söylenebilir. Öte yandan söz konusu düzenleme ile hem kademeli bir yaptırım sistemi öngörülmüş hem de hâkime bant daraltma yaptırımı bakımından, oran belirleme konusunda takdir yetkisi tanınmıştır. Dolayısıyla yaptırım kararlarında, sosyal medya araçlarının düşüncüyü

⁸⁵⁴ “İnternet Kanunu”, m. Ek 4(2).

⁸⁵⁵ Murat Volkan Dülger, “Sosyal Ağ Sağlayıcıların İnternet Haber Sitelerinin ve Şebekeler Üstü Hizmet Sağlayıcıların Hukuki Rejimi ve Eleştirisi”, 2023, s. 41, <https://papers.ssrn.com/abstract=4425002>, (18.11.2024). Söz konusu düzenlemenin Anayasa’ya aykırılığı iddiasıyla açılan davada da trafik bant genişliğinin yüzde doksan oranında daraltılması yaptırımının orantısız olacağı ileri sürülmüştür. Dava Dilekçesi, E. 2020/76 K. 2023/172 <https://normkararlarbilgibankasi.anayasa.gov.tr/Dosyalar/Kararlar/DilekcePDF/2023-172-nrmd.pdf>

açıklama ve bilgi edinme hakları bakımından önemi⁸⁵⁶ göz önünde bulundurularak hassas bir denge kurulmalıdır.⁸⁵⁷

2. İçerik Moderasyonuna İlişkin Yükümlülükler

Ek 4. madde ile sosyal ağ sağlayıcılar, idari ve adli merciler tarafından verilen kararların yerine getirilmesine ilişkin yükümlülükler yanında içerik moderasyonuna ilişkin ek yeni yükümlülüklerle tabi kılınmıştır. Bu doğrultuda, sosyal ağ sağlayıcılara bir yandan etkili bir uyarı yöntemi kurma diğer yandan öğrendiği hukuka aykırı içeriği ihbar etme yükümlülüğü yüklenmiştir.

Ek 4. maddenin üçüncü fıkrasına göre, Türkiye’den günlük erişimi bir milyondan fazla olan sosyal ağ sağlayıcılar, Kanunun 9A maddesi kapsamında özel hayatın gizliliğinin ihlal edildiğini iddia eden kişiler tarafından yapılan başvuruları, başvurudan itibaren en geç kırk sekiz saat içinde cevaplandırmakla yükümlüdür. Maddede doğrudan ifade edilmese de bu düzenleme ile Kanun’un 2. maddesinde tanımlanan uyarı yöntemi kastedilmektedir. Anayasa Mahkemesi kararıyla iptal edilmeden önce, Kanun’un 9. maddesi de yer sağlayıcıların kişilik hakları ihlal edilenler tarafından yapılan başvuruları belirli süre içinde cevaplandırmalarını gerektirmekteydi. Ancak bu düzenleme, uygulamada etkili bir sistem sağlamamaktaydı. Sosyal ağ sağlayıcılara yönelik düzenleme ile bu yükümlülük idari para cezası ile yaptırıma bağlanmış⁸⁵⁸ ve olumsuz cevapların gerekçeli olarak verilmesi de zorunlu hale getirilmiştir.⁸⁵⁹ Sosyal ağ

⁸⁵⁶ Youtube Llc Corporation Service Company ve Diğerleri Başvurusu, 2014/4705 (AYM [GK] 29 Mayıs 2014), para. 52.

⁸⁵⁷ Temsilci belirleme ve bildirme yükümlülüğünün getirilmesinin ardından, Dailymotion, Youtube, Tiktok, Facebook ve Instagram gibi sosyal medya şirketleri temsilci atama süreçlerini başlatmıştır. Son olarak X de, bant daraltma kararının alındığına ilişkin bildirim kendisine ulaşmasından sonra söz konusu yükümlülüğünü yerine getirmiştir. <https://www.trthaber.com/haber/gundem/sosyal-medya-platformu-x-turkiyede-temsilcilik-acti-859255.html> Bunun ardından X’e uygulanan reklam yasağı kararı da kaldırılmıştır. BTK Kararı, K. 29529, T. 22.05.2024, RG. S. 32555, T. 24.05.2024. Dolayısıyla bugüne kadarki süreçte, temsilci belirleme ve bildirme yükümlülüğünü yerine getirmeyen şirketlere para cezaları ve reklam yasakları uygulanmıştır. Şirketler bu aşamadan sonra söz konusu yükümlülüğü yerine getirdiklerinden, bu yükümlülük kapsamında bant daraltma cezası uygulama alanı bulmamıştır. Türkiye Üçüncü Sektör Vakfı, Sivil Toplum için Elverişli Ortam İzleme Matrisi, Ülke Raporu: Türkiye 2020-2021, s. 72.

⁸⁵⁸ “İnternet Kanunu”, m. Ek 4(8).

⁸⁵⁹ “İnternet Kanunu”, m. Ek 4(3).

sağlayıcılar ayrıca, başlık etiketleri ve öne çıkarılan içeriklerin de uyarı yöntemi ile kaldırılabilmesi için de etkili bir mekanizma kurmakla yükümlü kılınmıştır.⁸⁶⁰

Öte yandan, ek 4. maddenin onuncu fıkrası ile BTK Başkan'ı tarafından Kanun kapsamında verilen içeriğin çıkarılması ve/veya erişimin engellenmesi kararlarının gereğini yerine getirmeyen sosyal ağ sağlayıcılara daha ağır yaptırımlar öngörülmüştür. Buna göre, 8 ve 8A maddeleri kapsamındaki idari tedbirler saklı kalmak kaydıyla sosyal ağ sağlayıcıya sırasıyla reklam verme yasağı, trafik bant genişliğinin yüzde elli oranında daraltılması ve trafik bant genişliğinin yüzde doksan oranına kadar daraltılması yaptırımları uygulanabilecektir. Reklam verme yasağı doğrudan Başkan tarafından, bant genişliğinin daraltılması ise Başkanın başvurusu üzerine hâkim tarafından verilebilecektir.⁸⁶¹

Anayasa Mahkemesi'nin Başkan'ın internet içeriğin çıkarılması ve/veya erişimin engellenmesi kararı verme yetkisine ilişkin içtihadı göz önünde bulundurduğunda, Başkan tarafından verilen kararların yerine getirilmemesi halinde uygulanabilecek yaptırımlar tartışmalı bir hal almaktadır. Öncelikle, Başkan'ın resen internet içeriğinin çıkarılması ve/veya erişimin engellenmesine karar verme yetkisi özellikle hakim kararı güvencesini karşılamaktadır.⁸⁶² Öte yandan, Başkan'ın suç tespiti yaparak içeriğin çıkarılmasına karar verme ve bu kararın icra edilmemesi halinde idari para cezası verme yetkileri masumiyet karinesine aykırı olduğu gerekçesiyle AYM tarafından iptal edilmiştir.⁸⁶³ Dolayısıyla, Başkan'ın Kanun'un 8. maddesi kapsamındaki yetkileri Anayasal güvencelerle bağdaşmamaktadır. AYM, Başkan'ın Kanun'un 8/A maddesi kapsamındaki yetkisinin ise ancak gecikmesinde sakınca bulunan hâller ve müdahalenin haklılığının ilk bakışta anlaşılabilirdiği durumlarda kullanılabileceğini kabul etmiştir.⁸⁶⁴ İçişleri Bakanlığı Emniyet Genel Müdürlüğünün talebi üzerine Başkan tarafından alınan ve hakim tarafından da onaylanan 46 URL adresine erişimin engellenmesi kararına karşı yapılan *Artı Media Gmbh* başvurusunda ise AYM, 8/A maddesinin mevcut hâliyle

⁸⁶⁰ “İnternet Kanunu”, m. Ek 4(15).

⁸⁶¹ “İnternet Kanunu”, m. Ek 4(10).

⁸⁶² AYM, E.2015/76, K.2017/153, para. 26; Youtube Llc Corporation Service Company ve diğerleri [GK], para. 62. Youtube Llc Corporation Service Company ve diğerleri kararının 62. paragrafında hâkim kararı güvencesinden bahsedilmiş ancak ihlal kararı bu sebebe dayandırılmamıştır. AYM üyeleri Serruh Kaleli ve Engin Yıldırım tarafından yazılan farklı gerekçede bu husus net bir şekilde ifade etmiştir.

⁸⁶³ AYM, E.2020/76, K.2023/172.

⁸⁶⁴ Wikimedia Foundation Inc. ve Diğerleri Başvurusu, para. 76; Birgün İletişim ve Yayıncılık Ticaret A.Ş. Başvurusu, para. 71, 72; Ali Ergin Demirhan Başvurusu, para. 31.

kamusal makamların takdir yetkisini daraltarak keyfî davranışların önüne geçebilecek, çatışan haklar arasında adil bir denge kurulmasını garanti edebilecek temel güvencelere sahip olmadığını belirterek kanunilik ölçütünü taşımadığına hükmetmiştir.⁸⁶⁵ Başkanın içeriğin çıkarılması ve/veya erişimin engellenmesine yetkilerinin Anayasal güvencelerle bağdaşmadığına yönelik bu tespitler; söz konusu yetkiler kapsamında alınan kararların yerine getirilmemesi halinde trafik bant genişliğinin yüzde doksan oranına kadar daraltılmasına varabilecek ilave yaptırımlar öngören onuncu fıkra hükmünü de tartışmalı hale getirmiştir.

Ek 4. madde ile sosyal ağ sağlayıcıların hukuka aykırı içerikli ilgili sorumlulukları da açıklığa kavuşturulmuştur. Buna göre hukuka aykırılığı hâkim veya mahkeme kararı ile tespit edilen içeriğin sosyal ağ sağlayıcıya bildirilmesi durumunda, bildirimle rağmen yirmi dört saat içinde içeriği çıkarmayan veya erişimi engellemeyen sosyal ağ sağlayıcı, doğan zararların tazmin edilmesinden sorumludur.⁸⁶⁶ Bu hukuki sorumluluğun işletilmesi için içerik sağlayıcının sorumluluğuna gidilmesi veya içerik sağlayıcıya dava açılması şartı aranmamaktadır. Sosyal ağ sağlayıcının diğer sorumluluk hali ise, başlık etiketleri veya öne çıkarılan içerikler aracılığıyla ortam sağladığı başkasına ait yayın yoluyla işlenen suçtan sorumluluğuna ilişkindir. Ek 4. maddenin on beşinci fıkrasının ikinci cümlesine göre, suç teşkil eden içeriği bildirimle rağmen derhal ve en geç dört saat içinde kaldırmayan sosyal ağ sağlayıcı söz konusu içerikten doğrudan sorumludur.⁸⁶⁷ Burada, söz konusu suç tespitinin kim tarafından yapılacağına konusunda açık bir ifadeye yer verilmemiştir; ancak on dördüncü fıkra hükmü göz önünde bulundurulduğunda, bu tespitinin mahkeme kararıyla yapılacağı anlaşılmaktadır. Nitekim, Sosyal Ağ Sağlayıcı Hakkında Usul ve Esaslar'da da bu iki sorumluluk hali birlikte ele alınmaktadır.⁸⁶⁸

3. Şeffaflık Yükümlülüğü

Ek 4. madde ile kullanıcıların platformlarda daha güvenli ve adil bir deneyim yaşamalarını sağlamak amacıyla sosyal ağ sağlayıcılara şeffaflık ve hesap verebilirliğe

⁸⁶⁵ Artı Media Gmbh Başvurusu, para. 49.

⁸⁶⁶ “İnternet Kanunu”, m. Ek 4(14).

⁸⁶⁷ “İnternet Kanunu”, m. Ek 4(15).

⁸⁶⁸ Bilgi Teknolojileri ve İletişim Kurulu Kararı, Sosyal Ağ Sağlayıcı Hakkında Usul ve Esaslar, 2023/Dk-İd/119, 28.03.2023, m. 36.

ilişkin kapsamlı yükümlölükler yüklenmiştir.⁸⁶⁹ Orantılılık ilkesi gereğince bu yükümlölükler yalnızca Türkiye’den günlük erişimi bir milyonun üzerinde olan sosyal ağ sağlayıcıları için geçerlidir. Sosyal ağ sağlayıcıların şeffaflık yükümlölükleri şu hususları kapsamaktadır:

- i. Adli ve idari merciler ile kişiler tarafından bildirilen içeriklerin uygulanmasına ilişkin istatistiksel ve kategorik bilgiler,
- ii. Kullanıcı eşitliği ve tarafsızlığını sağlamak için alınan tedbirler,
- iii. Suç teşkil eden içerik ve başlık etiketlerinin yayınlanmamasına ilişkin tedbirler,
- iv. İçerik öneri sistemlerinde kullanılan parametreler,
- v. Kullanıcılara, önerilen içeriklere ilişkin tercihlerini güncelleme ve kişisel verilerinin kullanılmasını sınırlandırma seçeneği sunulması kapsamında alınan tedbirler,
- vi. Reklam politikalarına ilişkin bilgiler.

Buna göre, belirtilen nitelikteki sosyal ağ sağlayıcılar Temmuz ve Aralık aylarında olacak şekilde altı aylık sürelerle şeffaflık raporları hazırlamak ve bunları BTK’ya sunmak; kullanıcılara eşit ve tarafsız davranmak; bu Kanun kapsamındaki suçlara ilişkin içerikler ile başlık etiketlerinin yayınlanmamasına ilişkin kendi sistem, mekanizma ve algoritmalarında gerekli tedbirleri almak; öneri sistemlerinin işleyişine ilişkin bilgilere internet sitesinde yer vermek; kullanıcılara önerdikleri içeriklere ilişkin tercihlerini güncelleme ve kişisel verilerinin kullanılmasını sınırlandırma seçeneği sunmak ve sundukları reklamlara ilişkin bilgilerden oluşan bir reklam kütüphanesi oluşturarak bunu internet sitesinde yayınlamak zorundadır.

⁸⁶⁹ Madde Gerekeçleri, 7418 sayılı Basın Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun, Esas Komisyon Raporu Sıra Sayısı 340, m. 34.

Şeffaflık raporlarında, bu yükümlülükler kapsamında alınan tedbirler ile adli ve idari mercilerin kararları ile kullanıcıların taleplerine ilişkin istatistiksel ve kategorik bilgilerin tamamına yer verilmesi gerekmektedir.⁸⁷⁰ Sosyal Ağ Sağlayıcı Hakkında Usul ve Esaslar uyarınca, bu bilgiler şu şekildedir: “a) İçeriğin çıkarılması ve/veya erişimin engellenmesi kararlarının uygulanmasına ve kişilerden gelen başvuruların alınması ve değerlendirilmesine yönelik teknik altyapıya ve kararları uygulayacak personel niteliklerine ve idari kapasiteye dair bilgiler, b) Kararların uygulanma süresi ve şekli ile coğrafi kapsamına dair detaylı süreç bilgileri, c) Kişilerden gelen başvuruların sayısı, türü, olumlu veya olumsuz değerlendirilmesi, cevaplandırılması, olumsuz cevaplandırılanların gerekçeleri, sonuçlandırılma süreleri gibi sürece ilişkin kategorik ve istatistiksel bilgiler, ç) Adli veya idari makamlarca gönderilen kararlara ilişkin olarak kararı veren ve kararı gönderen merci, kararın gönderilme şekli, kararın türü, karara dayanak mevzuat hükmü, kararların gereğinin yerine getirilme süreleri gibi kategorik ve istatistiksel bilgiler, d) Özdenetim kapsamında gerçekleştirilen faaliyetlere ilişkin kategorik ve istatistiksel bilgiler, e) Kullanıcılara eşit ve tarafsız davranılması hususuna yönelik alınan tedbirlere dair bilgiler, f) Kullanıcılara önerilen içeriklere ilişkin tercihlerin güncellenmesine ve kullanıcıların kişisel verilerinin kullanılmasını sınırlandırma seçeneği sunulmasına yönelik alınan gerekli tedbirlere dair bilgiler, g) Başlık etiketleri, öne çıkarılan veya erişimi azaltılan içeriklere ilişkin algoritmalar ve şeffaflık politikalarına ilişkin bilgiler, ğ) Reklam politikalarına ilişkin bilgiler, h) Reklam kütüphanesi oluşturulmasına ve internet sitesinde yayınlanmasına ilişkin hususlar, ı) Kanun kapsamındaki suçlara ilişkin içerikler ile başlık etiketlerinin yayınlanmamasına ilişkin kendi sistem, mekanizma ve algoritmasında alınan gerekli tedbirlere dair bilgiler.”⁸⁷¹

Sosyal ağ sağlayıcılar ek 4. maddenin dördüncü fıkrası uyarınca özel hayatın gizliliğinin ihlali durumunda kişiler tarafından yapılan başvuruların sonuçlarına ilişkin hazırlanan raporu kişisel verilerden arındırarak kendi internet sitesinde kamuoyuyla paylaşmakla da yükümlü kılınmıştır.⁸⁷² Şeffaflık raporları, kullanıcıların ve düzenleyici kurumların, platformların nasıl çalıştığına dair daha iyi fikir sahibi olabilmeleri ve olası sorunlara karşı daha etkin önlemler alınabilmesi bakımından önem teşkil etmektedir.

⁸⁷⁰ “İnternet Kanunu”, m. Ek 4(4).

⁸⁷¹ Bilgi Teknolojileri ve İletişim Kurulu Kararı, Sosyal Ağ Sağlayıcı Hakkında Usul ve Esaslar, m. 10.

⁸⁷² “İnternet Kanunu”, m. Ek 4(4).

Örneğin X tarafından bugüne kadar toplam 7 şeffaflık raporu açıklanmıştır. Ocak-Haziran 2024 dönemini kapsayan son rapora göre, belirtilen dönemde “taciz” konusunda toplam 371,258 bildirim alınmış ve bu bildirimler platform tarafından yüzde 71.26 oranında karşılanmıştır.⁸⁷³ Önceki dönemlere kıyasla belirtilen dönemde taciz konulu taleplerin de bu taleplerin karşılanma oranının da arttığı görünmektedir.⁸⁷⁴ Bu ayrıntılı veri, hem kullanıcılar hem de kamu otoriterleri bakımından yol gösterici niteliktedir.

4. Veri Lokalizasyonu Yükümlülüğü

Sosyal ağ sağlayıcılar veri lokalizasyonu yükümlülüğü uyarınca Türkiye’deki kullanıcı verilerinin Türkiye’de saklanmasını sağlayacak tedbirleri almakla yükümlü kılınmıştır.⁸⁷⁵ Bu yükümlülük kullanıcı verilerinin yurtdışına aktarılmasıyla oluşabilecek risklerin minimize edilmesi ve veri güvenliğinin sağlanması bakımından önemlidir. Bununla birlikte, söz konusu yükümlülüğün kapsamı belirsizdir. Bu yükümlülük, (i) ilgili verilerin Türkiye’de bulunan fiziksel bir sunucuda barındırılmasını ya da (ii) ilgili verilerin Türkiye’de bulunan bir merkezde yer alan bir bulut bilişim sisteminde barındırılmasını gerektirebilir. Oysa Kanun’da bu tür verilerin nasıl ve ne zaman Türkiye’de barındırılmış sayılacağına ilişkin herhangi bir kriter belirlenmemiştir. Öte yandan düzenlemede Türkiye’de barındırılması gereken veri kategorileri de sınırlandırılmamıştır. Bu nedenle, Türkiye’de yerleşik kullanıcılar için kimlik, iletişim, hesap veya ödeme verileri dahil ancak bunlarla sınırlı olmamak üzere bir kullanıcıya ait olan ve/veya bir kullanıcıyı tanımlayan her türlü veri bu kapsamda değerlendirilebilecektir.⁸⁷⁶

⁸⁷³ Türkiye Şeffaflık Raporu Temmuz 2024, <https://transparency.x.com/tr/reports/countries/tr>, (23.12.2024).

⁸⁷⁴ Örneğin Ocak 2024 raporuna göre belirtilen dönemde taciz başlıklı 56.569 bildirimden %26.32’si; Temmuz 2023 raporuna göre ise 17.612 bildirimden %24.97’si karşılanmıştır. Türkiye Şeffaflık Raporu Ocak 2024; Türkiye Şeffaflık Raporu Temmuz 2023, <https://transparency.x.com/tr/reports/countries/tr>, (23.12.2024).

⁸⁷⁵ “İnternet Kanunu”, m. Ek 4(4).

⁸⁷⁶ Gonenc Gurkaynak, Ceren Yıldız, Burak Yesilaltay, “Recently Proposed Amendments to Turkish Internet Law: Obligations Imposed on Social Network Providers”, ss. 7, 8, https://www.gurkaynak.av.tr/Content/dosya/1178/d1982-mondaq_recently-proposed-amendments-to-turkish-internet-law-obligations-imposed-on-social-network-providers.pdf, (10.10.2024).

5. Bilgi Sağlama Yükümlülüğü

Ek 4. maddeyle sosyal ağ sağlayıcılara, bilgi sağlama yükümlülüğü bakımından da ek yükümlülükler yüklenmiştir. Bu kapsamda; i) belirli suçlara ilişkin olarak faillerin tespit edilmesi için gerekli bilgileri adli mercilere sağlama yükümlülüğü⁸⁷⁷, ii) hukuka aykırı içeriğe ilişkin bir farkındalık elde ettiğinde bu içeriği ve içerik sahibine ilişkin bilgileri kolluk birimlerine sağlama yükümlülüğü⁸⁷⁸ ve iii) İnternet Kanunu'na uyum sağlanması amacıyla Kurum tarafından talep edilen bilgi ve belgeleri sağlama yükümlülüğü⁸⁷⁹ şeklinde üç farklı yükümlülüğten bahsetmek mümkündür.

Sosyal ağ sağlayıcılar Ek 4. maddenin beşinci fıkrasında belirtilen hallerde, yargılama faaliyetlerinin akamete uğramasının önüne geçilmesi amacıyla,⁸⁸⁰ adli mercilerle gerekli bilgileri paylaşmakla yükümlü kılınmıştır. Buna göre beşinci maddede listelenen suçlarla ilgili olarak; soruşturma aşamasında Cumhuriyet savcısı, kovuşturma aşamasında mahkeme tarafından talep edilmesi halinde failere ulaşmak için gerekli bilgileri adli mercilere verecektir.⁸⁸¹ Bu yükümlülüğün yerine getirilmesi halinde, sosyal ağ sağlayıcının trafik bant genişliğinin yüzde doksan oranında daraltılması yaptırımı uygulanabilecektir. Belirtmek gerekir ki, söz konusu düzenlemede kademeli bir yaptırım sistemi yerine doğrudan sosyal ağ sağlayıcının neredeyse erişilemez kılınması sonucunu doğuracak bir yaptırım öngörülmüştür.⁸⁸²

Bu yükümlülük, suçla mücadele ve kamu güvenliği gibi önemli amaçlara hizmet etmektedir. Ancak, bu iş birliği sürecinde kullanıcıların kişisel verilerinin paylaşılması, kaçınılmaz olarak ifade özgürlüğünün bir parçası olarak kabul edilen anonimlik hakkı⁸⁸³

⁸⁷⁷ 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, m. Ek 4(5).

⁸⁷⁸ Ibid., m. Ek 4(16).

⁸⁷⁹ Ibid., m. Ek 4(18).

⁸⁸⁰ Madde Gereçekçeleri, 7418 sayılı Basın Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun, Esas Komisyon Raporu Sıra Sayısı 340, m. 34.

⁸⁸¹ “İnternet Kanunu”, m. Ek 4(5) hükmüne göre bu suçlar şunlardır: “Türk Ceza Kanunu’nda yer alan;

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)”.⁸⁸²

⁸⁸² Ibid., m. Ek 4(5).

⁸⁸³ “Promotion and Protection of the Right to Freedom of Opinion and Expression”, 16.05.2011 para. 84; “Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and

ile çelişki yaratabilecek bir durumdur. Gerçekten de bireylerin özellikle tartışmalı konularda fikirlerini beyan etme istekliliği bunu anonim olarak yapma olasılığıyla doğrudan bağlantılıdır. Dolayısıyla anonimlik hakkına ilişkin müdahalelerde, karşı kaya gelen menfaatler arasında adil bir denge kurulması önem teşkil etmektedir.

Ek 4. maddede yer alan, çocukların cinsel istismarı ve terör suçlarına ilişkin olarak faille ulaşmak için gerekli bilgilerin elde edilmesi Devletin pozitif yükümlülüğünün bir gereğidir.⁸⁸⁴ Bununla birlikte özellikle siyasi söylemler söz konusu olduğunda, anonimliğin görüşlerin, fikirlerin ve bilgilerin serbest akışını teşvik etmedeki rolünün göz ardı edilmemesi gerekmektedir.⁸⁸⁵ Bu kapsamda, ek 4. maddede yer alan suçlardan “*Halkı yanıltıcı bilgiyi alenen yayma (TCK, madde 217/A)*” suçu kapsamında, faillerin tespit edilmesine ilişkin bilgilerin paylaşılması yükümlülüğü ifade özgürlüğü bakımından caydırıcı etki yaratabilecek bir niteliktedir. Nitekim Venedik Komisyonu da söz konusu 217/A maddesinin “*yeterince açık olmadığı*”nı ve bu tür bir düzenlemenin caydırıcı etki doğurabileceğini ifade etmiştir.⁸⁸⁶ Bu suça ilişkin düzenleme, her ne kadar Anayasa Mahkemesi tarafından iptal edilmese de⁸⁸⁷, altı üye tarafından ayrı ayrı yazılan karşı oy yazılarında, kanun maddesinin belirsiz olduğu ve ifade özgürlüğünün kullanımına ilişkin olarak ciddi bir caydırıcı etkinin gündeme gelebileceği değerlendirilerek söz konusu düzenlemenin Anayasaya aykırılık teşkil ettiği ifade edilmiştir.⁸⁸⁸ Dolayısıyla, sosyal ağ sağlayıcılara, son derece tartışmalı olan bu suç kapsamında, kişilerin bilgilerini adli makamlarla paylaşma yükümlülüğünün yükleyen ve bu yükümlülüğün yerine getirilmemesi halinde hem sosyal ağ sağlayıcının hem de tüm kullanıcıların haklarını

Expression (A/HRC/29/32)”; “Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective (A/HRC/38/47)”, United Nations, 18.06.2018, <https://www.ohchr.org/en/documents/thematic-reports/ahrc3847-report-special-rapporteur-violence-against-women-its-causes-and>, para. 60. and UN HRC, Kaye D., Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 22 May 2015, UN Doc. A/HRC/29/32. Anonimlik hakkı, kadınların kamusal tartışmalara katılabilmelerine, cinsiyet stereotipleri ve sosyal tabuların kısıtladığı konularda görüş bildirebilmelerine de uygun bir zemin hazırladığından kadınların ifade özgürlüğünün ve mahremiyet haklarını garanti altına almaktadır. UN HRC, Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective, 18 June 2018, A/HRC/38/47, para. 60.

⁸⁸⁴ K.U. v. Finland, para. 48, 49.

⁸⁸⁵ Standard Verlagsgesellschaft MbH v. Austria (no. 3), para. 93-95.

⁸⁸⁶ Venedik Komisyonu ve Avrupa Konseyi, İnsan Hakları ve Hukukun Üstünlüğü Genel Müdürlüğü (DGI) Acil Ortak Görüşü, ‘Ceza Kanunu Değişiklik Tasarısı “Yanlış veya Yanıltıcı Bilgi” İle İlgili Hüküm Hakkında’, S. CDL-PI (2022)032, 2022, para. 87, 92.

⁸⁸⁷ E.2022/129, K.2023/189 (AYM 08 Kasım 2023).

⁸⁸⁸ Zühtü Arslan, Hasan Tahsin Gökcan, Engin Yıldırım, M. Emin Kuz, Yusuf Şevki Hakyemez ve Kenan Yaşar tarafından yazılan karşı oy yazıları, AYM, E.2022/129, K.2023/189.

etkileyecek şekilde trafik bant genişliğinin yüzde doksan oranında daraltılmasını öngören düzenlemeyi ifade özgürlüğü ve demokratik toplum düzeninin gerekleri ile bağdaştırmak mümkün görünmemektedir.

Ek 4. maddenin on altıncı fıkrası ise, kişilerin can ve mal güvenliğini tehlikeye sokan bir içeriğin öğrenilmesi ve gecikmesinde sakınca bulunması halinde içeriğin ve içerik sahibinin kolluk birimlerine bildirilmesi yükümlülüğünü düzenlemektedir. İnternet yoluyla işlenen suç oranlarındaki artış ve bu suçların kolluk kuvvetlerince tespitine ilişkin çeşitli zorluklar karşısında, sosyal ağ sağlayıcılara harekete geçme yükümlülüğü yüklenmesi sonradan telafi edilemeyecek zararların önlenmesi bakımından önem teşkil etmektedir. Nitekim, çeşitli ulusal yasalarda ve Avrupa Birliği Dijital Hizmetler Yasası'nda da sosyal ağ sağlayıcılara yönelik benzer düzenlemelere yer verilmiştir. Bununla birlikte, söz konusu düzenlemeler, kamu yararı ile ifade özgürlüğü ve özel hayatın gizliliği gibi temel haklar bakımından eleştirilere konu olmaktadır.⁸⁸⁹

Ek 4. maddenin on altıncı fıkrasına göre, sosyal ağ sağlayıcıları tetiklemesi beklenen içerikler kişilerin can ve mal güvenliğini tehlikeye sokan içeriklerdir. Mukayeseli hukukta, sosyal ağ sağlayıcıların bildirim yükümlülüğü daha çok insan ticareti, terörizm, çocuk istismarı gibi suçlarla bağlantılı olarak ele alınırken; söz konusu düzenlemede herhangi bir suç tipinden bahsedilmemektedir. Söz konusu yükümlülük her ne kadar gecikmesinde sakınca bulunan hallerle sınırlandırılmış olsa da yükümlülüğün kapsamı belirsizliğini korumaktadır. Sosyal ağ sağlayıcılar, söz konusu içerikleri, kendi inisiyatifleri ile yaptıkları incelemeler ya da kullanıcı bildirimleri sonucunda öğrenebilirler. Kanunun 5. maddesi uyarınca, sosyal ağ sağlayıcılar içeriği kontrol etmekle yükümlü olmadıklarından, sosyal ağ sağlayıcılar özellikle kullanıcı bildirimleri yoluyla ilgili içeriği öğrenecektir. Bu bildirimlere ilişkin herhangi bir çerçevenin çizilmemesi, diğer hususlarla birlikte, idari para cezalarına maruz kalmak istemeyen sosyal ağ sağlayıcıları yeterince gerekçelendirilmemiş bildirimlerde dahi inceleme yapmaksızın harekete geçmelerine yol açarak ifade özgürlüğü bakımından caydırıcı etki doğurabilir.⁸⁹⁰ Çok sayıda nitelsiz bildirim, aynı zamanda, kolluk kuvvetlerine orantısız bir yük yükleyerek düzenlemenin etkisini azaltabilir. Dolayısıyla, sosyal ağ sağlayıcıların bu

⁸⁸⁹ A. (Anna) Pivaty, P. T. J. (Pieter) Wolters, "The obligation to notify suspicions of criminal offences in the Digital Services Act under scrutiny", **Boom Strafbblad**, C. 3, S. 5, 2022, s. 190.

⁸⁹⁰ Pivaty, Wolters, "The obligation to notify suspicions of criminal offences in the Digital Services Act under scrutiny", s. 193.

yükümlüğünün sınırlandırılması hem ifade özgürlüğünün korunması hem de ciddi suçlarla etkili şekilde mücadele edilebilmesi açısından önem arz etmektedir.⁸⁹¹

Son olarak, ek 4. maddenin on sekizinci fıkrası ise sosyal ağ sağlayıcının İnternet Kanunu'na uyum sağlanması amacıyla talep edilen bilgi ve belgeleri en geç üç ay içerisinde Kurum'a verme yükümlülüğüne ilişkindir. Belirtmek gerekir ki 2014 yılında 6518 sayılı Kanun⁸⁹² ile yapılan değişikliklerle içerik, yer ve erişim sağlayıcılara benzer bir yükümlülük getirilmişti. Buna göre içerik, yer ve erişim sağlayıcıların Telekomünikasyon İletişim Başkanlığı'nın talep ettiği bilgileri talep edilen şekilde Başkanlığa teslim etmeleri ve Başkanlıkça bildirilen tedbirleri almaları gerekmektedir. Bu yükümlülüklerin kişilerle ilgili bilgileri de kapsayabileceğini değerlendiren Anayasa Mahkemesi söz konusu düzenlemelerde talep edilen bilgilerin kapsamına, mahiyetine, ne kadar süre ile saklanacağına ilişkin herhangi bir belirlilik bulunmamasını sorunlu bulmuştur.⁸⁹³ Buna karşın, ek 4. maddenin on sekizinci fıkrasında, Kurum tarafından talep edilebilecek bilgilerin sosyal ağ sağlayıcının İnternet Kanunu'na uyumuna ilişkin bilgiler olacağı açıkça ifade edilmiş ve bu bilgiler örneklendirilmiştir. Buna göre, Kurum, sosyal ağ sağlayıcının Kanuna uyumuna ilişkin olmak kaydıyla, kurumsal yapı, bilişim sistemleri, algoritmalar, veri işleme mekanizmaları ve ticari tutumlar dahil her türlü konuya ilişkin olabilecektir.⁸⁹⁴

6. Çocuk Koruma Yükümlülüğü

Ek 4. maddenin yedinci fıkrasına göre tüm sosyal ağ sağlayıcılar, çocukların sosyal ağlarda daha etkin korunması bakımından çocuklara özgü ayrıştırılmış hizmet sunma konusunda gerekli tedbirleri almakla yükümlüdür.⁸⁹⁵ Ek 4. maddenin yedinci fıkrasında, bu yükümlülüğün kapsamına ilişkin başkaca bir hususa yer verilmemiştir. Sosyal Ağ Sağlayıcı Hakkında Usul ve Esaslar'da ise bu yükümlülükle ilgili olarak, çocuk

⁸⁹¹ Martin Husovec, **Principles of the Digital Services Act**, Oxford University Press, 2024, s. 229.

⁸⁹² 6518 sayılı Aile ve Sosyal Politikalar Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname ile Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun, (2014).

⁸⁹³ AYM, E.2014/87, K.2015/112, para. 169. BTK'nin ve İletişim Başkanlığı'nın görevi kapsamında ilgili yerlerden bilgi belge talep edebilme yetkisine ilişkin farklı düzenlemeler de mevcuttur. Bu yetkilerin, kişisel verilerin korunması hakkı kapsamında tartışıldığı diğer AYM kararları için bkz. E.2017/16, K.2019/64, (AYM, 24 Temmuz 2019); E.2018/134, K.2021/13, (AYM 03 Mart 2021).

⁸⁹⁴ "İnternet Kanunu", m. Ek 4(18).

⁸⁹⁵ "İnternet Kanunu", m. Ek 4(7).

olduğu anlaşılabilen kullanıcılara sunulan içerik, reklam ve hizmetlerde; 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, hususlarının dikkate alınması gerektiği belirtilerek sosyal ağ sağlayıcılara yol gösterilmiştir.⁸⁹⁶

Sosyal ağ sağlayıcıların çocukların korunmasına ilişkin yükümlülüklerinin daha net ve belirli hale getirilmesi hem öngörülebilirliğin sağlanması hem de çocuk koruma mekanizmalarının daha etkili hale getirilebilmesi bakımından üzerinde durulması gereken bir konudur. Bu noktada, internet ortamında çocukların korunması bakımından kapsamlı bir çerçeve sunan AB Dijital Hizmetler Yasası yol gösterici mahiyettedir.

DSA’da bir çevrimiçi platform, hüküm ve koşulları küçüklerin hizmeti kullanmasına izin verdiğinde; hizmeti küçüklere yönelik olduğunda veya ağırlıklı olarak küçükler tarafından kullanıldığında; sağlayıcı, hizmetinin alıcılarından bazılarının küçük olduğunun başka bir şekilde farkında olduğunda, örneğin hizmetinin alıcılarının yaşlarını ortaya koyan kişisel verilerini başka amaçlarla zaten işlediğinde, çocuklar için erişilebilir olarak kabul edilmekte ve çocukların korunmasına ilişkin yükümlülüklerle tabi olmaktadır.⁸⁹⁷ Çocuk koruma yükümlülüğü kapsamında, platformlar, çevrimiçi arayüzlerini küçükler için en yüksek düzeyde gizlilik, emniyet ve güvenlik sağlayacak şekilde tasarlamalı; küçüklerin korunmasına yönelik standartlar benimsemeli; yaş doğrulama ve ebeveyn kontrol araçları, reşit olmayanların istismarı bildirmelerine veya uygun şekilde destek almalarına yardımcı olmayı amaçlayan araçlar dahil olmak üzere doğrudan çocuk haklarını korumaya yönelik hedefli tedbirler⁸⁹⁸ almalıdır. Bu kapsamda, Avrupa Komisyonu’nun *Çocuklar ve Gençler için Dijital On Yıl: Çocuklar İçin Daha İyi Bir İnternet İçin Yeni Avrupa Stratejisi (BIK+)* bildirisi gibi en iyi uygulamaların dikkate alınmalıdır. DSA’ya göre, hizmet alıcısının reşit olmadığını makul bir kesinlikle bilindiği hallerde, platformun hizmet alıcısının kişisel verilerini kullanarak profillemeye dayalı reklamlar sunması yasaktır. Bununla birlikte, bu yasak, hizmet alıcısının reşit olup

⁸⁹⁶ Bilgi Teknolojileri ve İletişim Kurulu Kararı, Sosyal Ağ Sağlayıcı Hakkında Usul ve Esaslar, m. 14.

⁸⁹⁷ “DSA”, resital 71.

⁸⁹⁸ “DSA”, m. 35(1)/j

olmadığının tespit edilmesi için ek kişisel veri işlenmesine yol açacak şekilde anlaşılmamalıdır.⁸⁹⁹

7. Kriz Planı Oluşturma Yükümlülüğü

İnternet Kanunu'nun ek 4. maddesinin on dokuzuncu fıkrası sosyal ağ sağlayıcıların kamu güvenliğini ve kamu sağlığını etkileyen olağanüstü durumlara ilişkin kriz planı oluşturmalarını ve bunu Kurum'a bildirmelerini gerektirmektedir.⁹⁰⁰ Bu tür krizler, terör eylemleri, deprem ve kasırga gibi doğal afetler ve ayrıca pandemiler ve kamu sağlığına yönelik diğer ciddi tehditlerden kaynaklanabilir. Kanunda bu yükümlülüğün yerine getirilmesine ilişkin başkaca bir düzenlemeye yer verilmemiştir. Bununla birlikte DSA, böylesi acil durumlarda alınabilecek tedbirlere ve tedbirlerin ölçülülüğüne ilişkin bir çerçeve sunmaktadır. Kriz planlarında örneğin, içerik denetleme süreçlerinin uyarlanması ve içerik denetlemeye ayrılmış kaynakların artırılması, hüküm ve koşulların, ilgili algoritmik sistemlerin ve reklam sistemlerinin uyarlanması, farkındalık yaratma önlemlerinin alınması, güvenilir bilgileri tanıtmak ve çevrimiçi arayüzlerinin tasarımını uyarlamak yer alabilir. Bu tür önlemler yalnızca kamu güvenliğinin ve kamu sağlığının kesinlikle gerektirdiği hallerle sınırlı olarak uygulanmalı ve ölçülülük ilkesi uyarınca bu mekanizma kapsamında alınan önlemlerde tüm tarafların hakları ve meşru çıkarları gerektiği gibi dikkate alınmalıdır.⁹⁰¹

II. Belirli Konulara Özgülenmiş Düzenlemeler

5651 sayılı İnternet Kanunu, içerik, yer ve erişim sağlayıcılar ile sosyal ağ sağlayıcıların yükümlülüklerine ilişkin temel bir çerçeve sunmaktadır. Bu yükümlülükler sektör ya da içerik ayırt edilmeksizin belirtilen tüm hizmet sağlayıcılara yöneliktir. Bununla birlikte, kişisel verilerin korunmasına ilişkin Kişisel Verilerin Korunması Kanunu ve e-ticaret platformlarını düzenleyen Elektronik Ticaretin Düzenlenmesi Hakkında Kanun'da da çeşitli yükümlülükler ele alınmaktadır.

⁸⁹⁹ “DSA”, resital 71.

⁹⁰⁰ “İnternet Kanunu”, m. Ek 4(19).

⁹⁰¹ “DSA”, resital 91.

A. Kişisel Verilerin Korunması Kanunu

Bilişim teknolojilerindeki hızlı gelişmeler, çok büyük miktarda veri toplanmasını, farklı kaynaklardan gelen verilerin birleştirilmesini ve bu verilerin detaylı analiz edilmesini kolaylaştırmıştır. Bu durum kişisel verilerin kötüye kullanılması riskini de beraberinde getirmiştir. İnternet şirketleri açısından bakıldığında, bu şirketler kullanıcılarından topladığı kişisel verileri kullanarak gelir elde ettiklerinden kişisel verilerin korunmasına ilişkin yükümlülüklerinin belirlenmesi önem arz etmektedir.

Türkiye’de ilk defa 1989 yılında kişisel verilerin korunmasına ilişkin özel bir kanun çıkarmak amacıyla komisyon kurulmuş ancak çalışmalarını tamamlayamadan dağılmıştır. 2000 yılında yeniden bir komisyon oluşturulmuş ve üç yıl süren çalışmalar sonucunda bir kanun tasarısı hazırlamıştır. Ne var ki, bu tasarı da kanunlaşmamıştır. 2008 ve 2014 yıllarında, Adalet Bakanlığı öncülüğünde yeni bir tasarı hazırlanıp Türkiye Büyük Millet Meclisi’ne (TBMM) sunulmuşsa da yasama dönemi sona erdiği için söz konusu kanun teklifleri kadük hale gelmiştir. 26 Aralık 2014 tarihinde “Kişisel Verilerin Korunması Kanunu Tasarısı” TBMM Başkanlığına sunulmuştur. Tasarı, 24 Mart 2016 tarihinde kanunlaşmış ve 6698 sayılı Kişisel Verilerin Korunması Kanunu 7 Nisan 2016 tarih ve 29677 sayılı Resmî Gazete’de yayımlanarak yürürlüğe girmiştir.⁹⁰²

6698 sayılı Kişisel Verilerin Korunması Kanunu’nda⁹⁰³ kişisel verilerin işlenmesinde yer alan iki farklı aktöre atıfta bulunmaktadır: veri işleyenler ve veri sorumluları. Bu ayrım, farklı aktörlerin farklılaşan yükümlülüklerinin belirlenmesinde önemli bir rol oynamaktadır. Veri sorumluları, kişisel verilerin kullanımına ilişkin kararları alan taraftır. Verileri "tek başına veya başkalarıyla birlikte" muhafaza eder ve ne şekilde kullanılacağına karar verirler.⁹⁰⁴ Bu nedenle, daha kapsamlı ve sıkı kurallara uymak zorundadırlar. Veri işleyenler ise kişisel verileri muhafaza etmekle birlikte verilerin kullanımı konusunda veri sorumlusunun talimatlarını takip ederler. Dolayısıyla, veri sorumlularına kıyasla daha sınırlı yükümlülüklerle tabidirler.

⁹⁰² KVKK, Kişisel Verilerin Korunması Kanunu ve Uygulaması, s. 16. <https://kvkk.gov.tr/yayinlar/K%C4%B0%C5%9E%C4%B0SEL%20VER%C4%B0LER%C4%B0N%20KORUNMASI%20KANUNU%20VE%20UYGULAMASI.pdf>, (10.10.2024).

⁹⁰³ 6698 sayılı Kişisel Verilerin Korunması Kanunu, (2016), <https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=6698&MevzuatTur=1&MevzuatTertip=5>.

⁹⁰⁴ “General Data Protection Regulation”, m. 4(7).

Barındırma hizmeti sağlayıcıları, sosyal medya platformları ve arama motorları gibi hizmetler, kullanıcı verilerini aktif olarak işleyerek kendi hizmetlerini geliştirdiklerinden, bu veriler üzerinde kontrol sahibi olmaktadır. Bu nedenle, bu tür hizmet sağlayıcılar, veri koruma düzenlemeleri kapsamında veri sorumlusu olarak kabul edilirler. Ancak, kullanıcıların ürettiği içeriklerin işlenmesi söz konusu olduğunda, bu hizmet sağlayıcılarının veri sorumlusu mu yoksa veri işleyen mi olduğu, işleme amaçları ve araçları üzerindeki kontrol düzeylerine göre belirlenmektedir.⁹⁰⁵

Bu kapsamda, belirtilen hizmetleri sağlayan internet şirketleri de 6698 sayılı Kanun'da veri sorumlusu için öngörülen yükümlülüklerle tabidir. Buna göre, veri sorumlusu sıfatı taşıyan internet şirketleri Kanun'un 5. ve 6. maddeleri uyarınca kişisel verileri, ancak ilgili kişinin açık rızasıyla ya da bu maddelerde belirtilen istisnai haller⁹⁰⁶ kapsamında işleyebilecektir. Bununla birlikte hizmet sağlayıcılar veri işlemenin hukuka ve dürüstlük kurallarına uygun olmasını, doğru ve güncel olmasını, belirli, açık ve meşru

⁹⁰⁵ Timmermans, "The Role of Internet Intermediaries in the Protection of Freedom of Expression and Personal Data", s. 32-33.

⁹⁰⁶ Buna göre, aşağıdaki şartlardan birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür:

"a) Kanunlarda açıkça öngörülmesi.

b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.

c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.

ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.

d) İlgili kişinin kendisi tarafından alenileştirilmiş olması.

e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.

f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması". Kişisel Verilerin Korunması Kanunu, m. 5(2).

Özel nitelikli kişisel verilerin işlenmesi ise ancak şu hallerde mümkündür:

"a) İlgili kişinin açık rızasının olması,

b) Kanunlarda açıkça öngörülmesi,

c) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin, kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması,

ç) İlgili kişinin alenileştirdiği kişisel verilere ilişkin ve alenileştirme iradesine uygun olması,

d) Bir hakkın tesisi, kullanılması veya korunması için zorunlu olması,

e) Sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlarca, kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi ile sağlık hizmetlerinin planlanması, yönetimi ve finansmanı amacıyla gerekli olması,

f) İstihdam, iş sağlığı ve güvenliği, sosyal güvenlik, sosyal hizmetler ve sosyal yardım alanlarındaki hukuki yükümlülüklerin yerine getirilmesi için zorunlu olması,

g) Siyasi, felsefi, dini veya sendikal amaçlarla kurulan vakıf, dernek ve diğer kâr amacı gütmeyen kuruluş ya da oluşumların, tâbi oldukları mevzuata ve amaçlarına uygun olmak, faaliyet alanlarıyla sınırlı olmak ve üçüncü kişilere açıklanmamak kaydıyla; mevcut veya eski üyelerine ve mensuplarına veyahut bu kuruluş ve oluşumlarla düzenli olarak temasta olan kişilere yönelik olması." 6698 sayılı Kişisel Verilerin Korunması Kanunu, m. 6(3).

amaçlara dayanmasını, bu amaçlarla ilgili olarak sınırlı ve ölçülü olmasını ve ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesini sağlamaktan sorumludur.⁹⁰⁷ İşlenme şartlarının tamamının ortadan kalkması halinde ise kişisel verilerin veri sorumlusu tarafından resen veya ilgili kişinin talebi üzerine silinmesi, yok edilmesi veya anonim hâle getirilmesi gerekmektedir.⁹⁰⁸

Bu kapsamda sosyal medya platformları, bloglar, internet haber siteleri gibi ifade özgürlüğünün kullanılmasına aracılık eden çevrimiçi hizmet sağlayıcıların, veri işleme faaliyetlerinde kişisel verilerin korunması hakkı ile ifade özgürlüğü arasında makul denge kurmaları gerekmektedir. Bu noktada, platformun içerik sağlayıcı olarak mı yoksa yer sağlayıcı olarak mı hareket ettiğinin belirlenmesi önemlidir. Örneğin, bir kişinin fotoğrafının, açık rızası alınmadan bir haber içeriğinde kullanılmasıyla ilgili olarak sosyal medya platformunun sorumluluğunun ele alındığı bir başvuruda Kurum, sitedeki içeriklerin üyeler tarafından oluşturulabileceği gibi veri sorumlusunun editörleri tarafından da oluşturulmasının mümkün olduğunu; platformun ilk durumda içerik sağlayıcı, kullanıcı/üyelerin oluşturup yayımladığı ve sitenin herhangi bir müdahalesi veya denetimi olmayan içerikler bakımından ise yer sağlayıcı niteliği taşıdığını belirtmiştir. Başvuruya konu içeriğin veri sorumlusunun bünyesinde içerik üreten bir editör tarafından oluşturulduğunu tespit eden Kurum platformun 6698 sayılı Kanun kapsamında veri sorumlusu sıfatını haiz olduğuna ve Kanun kapsamındaki yükümlülüklerle tabi olacağına karar vermiştir.⁹⁰⁹

İfade özgürlüğü bakımından önem teşkil eden hususlardan biri de Kanun’u 28. maddesinde Kanun’un 28’inci maddesinde düzenlenen istisna hükümleridir. Birinci fıkra uyarınca; *“kişisel verilerin milli savunmayı, milli güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği, özel hayatın gizliliği veya kişilik haklarını ihlal etmemek ya da suç teşkil etmemek kaydıyla sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi”* halinde Kanun uygulama alanı bulmayacaktır. Buna göre, kişisel veri işleminin, ifade özgürlüğü kapsamında tam istisnai hal olarak değerlendirilebilmesi için suç teşkil etmemek kaydıyla özel hayatın gizliliğini de ihlal etmemesi; kişilik haklarına saldırı mahiyetinde olmayan haberin

⁹⁰⁷ 6698 Sayılı Kişisel Verilerin Korunması Kanunu, m. 4.

⁹⁰⁸ 6698 Sayılı Kişisel Verilerin Korunması Kanunu, m. 7.

⁹⁰⁹ K. 2021/989 (KVKK 30 Eylül 2021).

hukuka uygun olduğunun kabul edilebilmesi için de kamu ilgi ve yararı taşıması, gerçek ve güncel olması, öz ile biçim arasındaki dengenin gözetilmiş olması gerekmektedir. Diğer taraftan, ifade özgürlüğü ile kişilik hakları arasında denge kurulurken de basında yer alan yazı veya ifadelerin kamuoyunu ilgilendiren genel yarara ilişkin bir tartışmaya sağladığı katkı, hedef alınan kişinin tanınmışlık düzeyi ve yazının amacı, ilgili kişinin medyaya karşı önceden yaptığı davranışları, bilginin elde edilme yöntemi ve doğruluğu, yayının içeriği, biçimi, sonuçları ve yapılan haber dolayısıyla uygulanan yaptırımın ağırlığı kriterleri esas alınmalıdır.⁹¹⁰

Çevrimiçi hizmet sağlayıcıların ifade özgürlüğü ve kişisel verilerin korunması hakkı arasında denge kurmalarını gerektiren bir başka yükümlük de unutulma hakkına ilişkin yükümlülüklerdir.⁹¹¹ Unutulma hakkı, Türk hukuk mevzuatında kavramsal olarak yer almasa da⁹¹² yargı kararlarıyla kabul edilmiştir. Unutulma hakkı, henüz 6698 sayılı Kanun yürürlüğe girmeden önce Anayasa Mahkemesi tarafından ele alınmış ve internet haber arşivlerindeki kişisel verilere erişimin engellenerek kişilerin yaptıklarının unutulmasının sağlanması yönündeki talebi unutulma hakkı olarak nitelendirmiştir.⁹¹³ Bu kararda Anayasa Mahkemesi, unutulma hakkı ile ilgili içeriğin tamamen ortadan kaldırılmasının amaçlanmadığı belirtmiş ve bu hak kapsamında arşivde arama yapmaya imkân tanıyan haber ile kişi arasında ilişki kuran kişisel verilerin silinmesi, haberin anonim hâle getirilmesi, haber içeriğinin bir kısmına erişimin engellenmesi gibi birçok yöntem benimsenebileceğini kabul etmiştir.⁹¹⁴

Kişisel Verileri Koruma Kurumu da unutulma hakkını geniş bir perspektiften ele almakta ve mevzuatımızda unutulma hakkını sağlamaya yönelik çok çeşitli araçlar olduğunu ifade etmektedir. 5651 sayılı Kanunun özel hayatın gizliliği nedeniyle içeriğe

⁹¹⁰ K. 2023/767 (KVKK, 11 Mayıs 2023).

⁹¹¹ Ayşenur Ocak, “Hakları Dengelemek: Unutulma Hakkı İfade Özgürlüğüne Karşı”, **Türkiye Adalet Akademisi Dergisi**, S. 33, 2018, ss. 507-36.

⁹¹² Anayasa Mahkemesi tarafından iptal edilmeden önce 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun’un 9. maddesinin onuncu fıkrası, unutulma hakkının yasal dayanağı olarak kabul edilmekteydi. Bu maddede unutulma hakkı şu şekilde düzenlenmişti: “İnternet ortamında yapılan yayın içeriği nedeniyle kişilik hakları ihlal edilenlerin talep etmesi durumunda hâkim tarafından, başvuranın adının bu madde kapsamındaki karara konu internet adresleri ile ilişkilendirilmemesine karar verilebilir. Kararda, Birlik tarafından hangi arama motorlarına bildirim yapılacağı gösterilir.” Mahkeme, 9. maddenin tamamını iptal ettiğinden bu dayanak da ortadan kalkmıştır. AYM, E.2020/76, K.2023/172.

⁹¹³ N.B.B. Başvurusu, 2013/5653 (AYM 03 Mart 2016), para. 42.

⁹¹⁴ N.B.B. Başvurusu, para. 52.

erişimin engellenmesi yönündeki düzenlemesi ya da Kişisel Verilerin Korunması Kanunu'nun kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesine ilişkin 7. maddesi bu kapsamda kabul edilebilecektir. Hangi yöntemin uygulanacağı ise somut olaya göre belirlenecektir.⁹¹⁵

Arama motorlarının verilerin yayınlanmasında belirleyici role sahip olmaları, onları unutulma hakkının sağlanması bakımından da önemli hale getirmektedir. Nitekim Kurum da bu önemi dolayısıyla ilgili kişilerin ad ve soyadları ile arama motorları üzerinden yapacakları aramalar neticesinde çıkan sonuçların indekslenmeyecek şekilde teknik düzenlemeye tabi tutulması konusunda usul ve esaslar kabul etmiştir. Buna göre, unutulma hakkına ilişkin taleplerde öncelikle arama motorlarına başvuruda bulunulması gerekmektedir. Arama motorlarının bu talepleri değerlendirirken kişinin temel hak ve özgürlükleri ile kamunun söz konusu bilgiyi edinmesinden sağlayacağı menfaatler arasında bir denge testi yapmaları gerekmektedir. Veri sorumlusu arama motorlarının söz konusu talepleri reddetmeleri veya başvuru sahibine cevap vermemeleri halinde ise Kurula şikâyetle bulunulabilecektir.⁹¹⁶ Bu kapsamda Kurum'a yapılan bir başvuruda, kamu üniversitesinde görev yapmakta olan başvurucu, aile yakınının işe alınması ile ilgili usulsüzlük iddiaları üzerine üniversite tarafından soruşturma açılması hakkındaki haberlerin kaldırılması talebiyle arama motoruna yaptığı başvurunun reddedilmesinden yakınmıştır. Kurum, somut başvuru çeşitli açılardan değerlendirmiş; *“ilgili kişinin kamu üniversitesinde görev yapmakta olduğu, başvuru konusu hususlarda ilgili kişinin aile yakınının işe alınması ile ilgili usulsüzlük iddiaları sonucunda üniversite tarafından soruşturma açıldığı bilgisinin doğru olduğu, söz konusu bağlantılarda yer alan haberin ilgili kişinin çalışma yaşamına ilişkin olduğu ve ilgili kişinin hâlihazırda aynı işi yaptığı, bilgilerin özel nitelikli kişisel veri niteliği taşımadığı, yapılan haberlerin 2020 tarihli olduğu, dolayısıyla güncel olduğu, bilginin kişi açısından risk doğurmadığı ve içeriklerin gazetecilik faaliyeti kapsamında değerlendirilebileceği, öte yandan, bilginin kişi hakkında ön yargıya sebep olabileceği ancak bunun kanıtlanabilir nitelikte olmadığı, ilgili kişiye ilişkin bilgilerin yayınlanmasında yasal zorunluluk bulunmadığı, bilginin kişinin kendisi tarafından yayımlanmadığı, bilginin ceza gerektiren bir suçla ilgili*

⁹¹⁵ K. 2020/481 (KVKK, 23 Haziran 2020).

⁹¹⁶ K. 2020/481 (KVKK, 23 Haziran 2020).

*olmadığı hususlarını...” göz önünde bulundurarak veri sorumlusu arama motorunun kararını yerinde olduğunu kabul etmiştir.*⁹¹⁷

Kanun’un 10. ve 12. maddelerinde veri sorumlusunun yükümlülükleri ele alınmaktadır. Bu yükümlülüklerden ilki aydınlatma yükümlülüğü, diğeri ise veri güvenliğine ilişkin yükümlülüklerdir. Veri sorumlusu ayrıca, ilgili kişinin kişisel verilerin işlenmesi, aktarılması, silinmesi gibi taleplerini karşılamakla da yükümlüdür.⁹¹⁸

Buna göre, veri sorumlusu, aydınlatma yükümlülüğü kapsamında kişisel verilerin elde edilmesi sırasında veri sorumlusu veya yetkilendirdiği kişi, ilgili kişilere; a) veri sorumlusunun ve varsa temsilcisinin kimliği, b) kişisel verilerin hangi amaçla işleneceği, c) işlenen kişisel verilerin kimlere ve hangi amaçla aktarılabileceği, ç) Kişisel veri toplamanın yöntemi ve hukuki sebebi ve d) 11 inci maddede sayılan diğer hakları konusunda bilgi vermekle yükümlüdür. Bu yükümlülük sayesinde, bir yandan kişisel verilerin işlenmesi aktarılması ve toplanması bakımından şeffaflık sağlanırken diğer yandan da ilgili kişiler haklarından faydalanırken kimlere ne gibi taleplerle başvurabileceğini öğrenmiş olacaktır.⁹¹⁹

Veri sorumlusu veri güvenliğine ilişkin olarak ise kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini engellemek ve kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır. Bu madde uyarınca alınması gereken teknik ve idari tedbirlere ilişkin başlıca yöntemler Kişisel Verileri Koruma Kurulu tarafından Kişisel Veri Güvenliği Rehberi’nde kapsamlı bir şekilde ele alınmıştır.⁹²⁰ Bu tedbirlere ilişkin olarak uygun güvenlik düzeyinin belirlenmesinde, teknolojinin durumu, uygulamaların maliyeti, korunacak verilerin niteliği ile var olan riskin dikkate alınması gerekmektedir.⁹²¹ Ayrıca veri ihlali durumunda veri

⁹¹⁷ K. 2020/927 (KVKK, 8 Aralık 2020).

⁹¹⁸ 6698 Sayılı Kişisel Verilerin Korunması Kanunu, m. 11.

⁹¹⁹ Sezen Kama Işık, **Avrupa Veri Koruma Hukukuna Anayasal Bir Bakış**, (Doktora Tezi), Marmara Üniversitesi, Sosyal Bilimler Enstitüsü, Kamu Hukuku Anabilim Dalı Kamu Hukuku Bilim Dalı, 2019, s. 266.

⁹²⁰ KVKK, Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler) https://www.kvkk.gov.tr/yayinlar/veri_guvenligi_rehberi.pdf

⁹²¹ Kama Işık, *Avrupa Veri Koruma Hukukuna Anayasal Bir Bakış*, s. 267.

sorumlusu, kişisel veri ihlalinin muhtemel sonuçlarını dikkate alarak gecikmeksizin veri koruma kuruluna ve ilgili kişilere bildirimde bulunmak zorundadır.⁹²²

Çevrimiçi hizmet sağlayıcılar bakımından üzerinde durulması gereken yükümlülüklerden biri de kişisel verilerin yurtdışına aktarımına ilişkindir. Kişisel verilerin yurtdışına aktarılması koşullarının düzenlendiği 9. madde, 2024 yılında yapılan değişikliklerle⁹²³ farklı bir kimliğe bürünmüştür. Bu değişikliklerin arka planında, yurt dışına veri aktarımının sadece ilgili kişilerin açık rızalarına bağlı olmasını öngören yaklaşımın ticari hayatta sıklıkla kullanılan ve sunucuları yurt dışında bulunan ve çoğu bulut tabanlı yazılım ve uygulamaların önünün açılabilmesidir.⁹²⁴

Buna göre, kişisel verilerin yurt dışına aktarılması için genel kural, veri sahibinin açık rızasının alınmasıdır. İlgili kişinin açık rızası aranmaksızın kişisel verilerin yurt dışına aktarılabilmesi için Kanunun 5. maddesinin ikinci fıkrası ile 6. maddesinin üçüncü fıkrasında belirtilen şartlardan birinin bulunması ve Kurul tarafından kişisel verilerin aktarılacağı ülke bakımından yeterli korumanın bulunduğu karar verilmiş olması (yeterlilik kararı) gerekmektedir. Hakkında yeterli korumayı sağladığı yönünde karar bulunmayan ülkeler bakımından ise, ilgili kişinin açık rızası aranmaksızın kişisel verilerin aktarılması, veri işleme şartlarından birinin bulunması şartıyla sadece Türkiye’deki ve ilgili ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kurulun izin vermesi durumunda mümkün olabilmektedir.⁹²⁵

B. Elektronik Ticaretin Düzenlenmesi Hakkında Kanun

Elektronik Ticaretin Düzenlenmesi Hakkında Kanunda⁹²⁶ hizmet sağlayıcılar, aracı hizmet sağlayıcılar ve aracı hizmet sağlayıcıların elektronik ticarete ilişkin sorumluluklarına ilişkin düzenlemeler yer almaktadır.

⁹²² Kişisel Verilerin Korunması Kanunu, m. 12(5).

⁹²³ 7499 sayılı Ceza Muhakemesi Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun, (2024).

⁹²⁴ “Madde Gerekçeleri, 7499 sayılı Ceza Muhakemesi Kanunu İle Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun, Yasama Dönemi, Esas Komisyon Raporu Sıra Sayısı 109”, <https://cdn.tbmm.gov.tr/KKBSPublicFile/D28/Y2/T2/DosyaKomisyonRaporunuVerdi/cfb35b8a-65cc-44e7-b1bc-4764e98175b9.pdf>, m. 34.

⁹²⁵ Kişisel Verilerin Korunması Kanunu, m. 9.

⁹²⁶ 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun, (2014).

Kanunda, hizmet sağlayıcıların bilgi verme ve sipariş alma gibi süreçlere ilişkin yükümlülükleri yanında aracı hizmet sağlayıcıların hukuka aykırı içerikten sorumluluğu da düzenlenmektedir. Buna göre aracı hizmet sağlayıcı, içerik kontrolü yapmakla yükümlü değildir. Dolayısıyla, kural olarak hizmet sağlayıcı tarafından sunulan içerik ve içeriğe konu mal veya hizmetle ilgili hukuka aykırı hususlardan sorumlu değildir.⁹²⁷ Bununla birlikte, elektronik ticaret aracı hizmet sağlayıcı, sunulan içeriğin hukuka aykırı olduğundan herhangi bir şekilde haberdar olması hâlinde, bu içeriği gecikmeksizin yayımdan kaldırarak hukuka aykırı hususu ilgili kamu kurum ve kuruluşlarına bildirmekle yükümlüdür.⁹²⁸ Buna göre, elektronik ticaret aracı hizmet sağlayıcılar, 5651 sayılı İnternet Kanunu'ndan öngörülenden farklı olarak, yalnızca “haberdar edildiklerinde” değil aynı zamanda “haberdar olduklarında” da hukuka aykırı içerikten sorumlu tutulmuştur.

Esasen, elektronik ticaret aracı hizmet sağlayıcıların hukuka aykırı içerikle ilgili sorumluluktan muafiyetine ilişkin bu yaklaşım, 6563 sayılı Elektronik Ticaret Kanun'u yürürlüğe girmeden önce, Yargıtay Hukuk Genel Kurulu tarafından kabul edilmiştir. Yargıtay Hukuk Genel Kurulu, marka hakkını ihlal eden içeriğe internet sitesinde yer verilmesinin marka hakkına tecavüz teşkil ettiğini belirtmekle birlikte, bu tecavüz eyleminden yer sağlayıcının da sorumlu tutulabilmesinin koşulunun yer sağlayıcının tecavüzden haberdar edilmesi olduğunu kabul etmiştir. Bu kapsamda, kendisine karşı dava açılmış olmasıyla içeriğin hukuka aykırılığından haberdar olan platformun dava tarihinden itibaren söz konusu içerikten sorumlu olduğuna karar vermiştir.⁹²⁹

9. maddenin üçüncü fıkrası ise, fikri ve sınai mülkiyet hakkı bakımından bir uyar-kaldır mekanizması öngörmektedir. Bünyesinde milyonlarca ürün barındıran pazar yerlerinde, fikri ve sınai mülkiyet hakkı ihlalleriyle karşılaşma ihtimalinin oldukça yüksek olduğundan, bu mekanizma hem tüketicilerin hem de hak sahiplerinin haklarının korunabilmesi bakımından önem teşkil etmektedir. Buna göre, elektronik ticaret aracı hizmet sağlayıcı, fikri ve sınai mülkiyet hakkı ihlaline dair bilgi ve belgeye dayanan bir şikâyet aldığı anda, şikâyete konu ürünü yayımdan kaldırmak ve durumu taraflara bildirmekle yükümlüdür. Hizmet sağlayıcının, şikâyetin aksini gösteren bilgi ve belgeye

⁹²⁷ 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun, m. 9(1).

⁹²⁸ 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun, m. 9(2).

⁹²⁹ Gittigidiyor Kararı, E. 2013/11-1138, K. 2014/16 (Yargıtay Hukuk Genel Kurulu 15 Ocak 2014).

dayanarak buna itiraz etmesi halinde ise şikâyeteye konu ürünün yeniden yayımlaması gerekmektedir.⁹³⁰

Günlük işlem hacimleri dikkate alındığında, elektronik ticaret aracı hizmet sağlayıcıların hukuka aykırı içerikten sorumluluğundan bahsedebilmek için kendilerine yapılacak bildirimin usuli bir bildirimden ziyade yaklaşık ispata yeterli delillerle gerekçelendirilmiş bir bildirim olması gerekmektedir.⁹³¹ Yargı yoluna başvurulmuş olması halinde, kararın sonucunun beklenmesi hakkaniyete aykırı sonuçlar doğurabilecektir. Örneğin, bir elektronik ticaret platformunun hukuka aykırı içerikten sorumluluğunun ele alındığı davada, derece mahkemesi; platformun hukuka aykırılıktan haberdar olduğu tarih bakımından *“tedbir kararının tebliğinin baz alınması gerektiği, zira sunulan raporun itiraz süreci ve mahkemenin sunulan raporla doğrudan bağlı olmadığı kararının tebliğinin baz alınması gerektiği, zira sunulan raporun itiraz süreci ve mahkemenin sunulan raporla doğrudan bağlı olmadığı dikkate alındığında rapor içeriğine dayalı içerik kaldırılmasının davalıdan beklenemeyeceği”*ni kabul etmiştir.⁹³² Kanaatimizce, bu yaklaşım, 6563 sayılı Kanun’un 9. maddesi ve 5651 sayılı Kanun’un 5. maddesi ile bağdaşmamaktadır. Nitekim Yargıtay Hukuk Genel Kurulu da hukuka aykırı içeriğe ilişkin dava açılmış olmasını, haberdar olma koşulunun sağlanmasında yeterli kabul etmiştir. Söz konusu davada ise, dava açılmış olması yanında, davacının iddialarını destekleyen bir bilirkişi raporu olduğu da göz önünde bulundurulduğunda, platformun hukuka aykırı içerikten haberdar olmasına rağmen harekete geçmediği kabul edilmelidir.

III. Yeni Bir İnternet Kanunu İçin Öneriler

Türk hukukunda, internetin yol açtığı sorunlarla mücadele girişimleri, henüz internetin yeni yeni kullanılmaya başladığı yıllara kadar uzanmaktadır. İlk defa 1989 yılında kişisel verilerin korunmasına ilişkin düzenleme yapmak üzere bir komisyon oluşturulduğunu ve bu çabaların çok geçmeden yinelenildiğini hatırlamak önemlidir. İnternetin kullanım alanlarının çeşitlendiği; bloglar ve platformlar sayesinde

⁹³⁰ 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun, m. 9(3).

⁹³¹ E. 2019/618 K.2019/8167 (Yargıtay 11. HD. 16 Aralık 2019); E.2021/32, K.2021/18 (İstanbul 4. Fikrî ve Sınai Haklar Hukuk Mahkemesi 23 Kasım 2021); E.2022/996 K.2024/1262 (Ankara BAM 20. HD. 05 Temmuz 2024); Y.11 HD. T., 2019/618 E., 2019/8167 K., T. 16.12.2019; İstanbul 4. Fikrî ve Sınai Haklar Hukuk Mahkemesi, 2021/32 E., 2021/18 K., T. 23.11.2021; Ankara BAM 20. Hukuk Dairesi, 2022/996 E., 2024/1262 K., 05.07.2024.

⁹³² İstanbul 2. Fikrî ve Sınai Haklar Hukuk Mahkemesi, 12 Kasım 2020.

kullanıcıların kendi içeriklerini oluşturmaya başladığı; internetin sadece bilgiye erişmek için kullanılan bir araç olmaktan çıkıp, iletişim, eğlence, ticaret ve sosyalleşmenin önemli bir aracı haline geldiği 2000’li yıllarda çevrimiçi hizmet sağlayıcıları düzenleyen bir Kanun çıkarılması da bir farkındalığın yansımasıdır.

Ne var ki, interneti düzenlemek, internetin potansiyel etkilerine yönelik farkındalıktan çok daha fazlasını gerektirmektedir. Bartlett’in “*internetin gelecekte nasıl işleyeceğini hesaba katmadan, bugününe bakarak kötü yasalar çıkarmak kolay olacaktır*”⁹³³ serzenişi de bu zorluğun ifade edilmiş biçimlerinden biridir. İnternetin düzenlenmesi teknolojinin dinamik yapısı ve küresel doğası nedeniyle oldukça karmaşık bir süreçtir. Bir yandan, bilgiye erişim ve ifade özgürlüğü gibi temel hakların korunması gerekliliği, diğer yandan bireylerin mahremiyeti ve kamu düzeninin sağlanması gibi öncelikler, düzenleyici çerçevelerin sınırlarını zorlamaktadır. Bunun yanında, internet ve daha geniş anlamda dijital dünyanın alt yapısının özel şirketlerin elinde olması da söz konusu düzenleme çabalarını karmaşık bir hale getirmektedir.

Türk hukukunda, internetin düzenlenmesi tam da bu karmaşıklığı yansıtan bir serüvende ilerlemiştir. 2000 yılında yürürlüğe giren Avrupa Birliği E-Ticaret Direktifi göz önünde bulundurularak hazırlanan, yürürlüğe girdiği 2007 yılından bu yana 14 kez değişikliğe, 4 kez de Anayasa Mahkemesi’nin iptal kararına konu olan 5651 sayılı Kanun (İnternet Kanunu), bu yönüyle oldukça “dinamik”tir. Belirtmek gerekir ki, bu dinamizm, İnternet Kanununu çağın gereklerine cevap veren bir niteliğe kavuşturmamış; bilakis Anayasa Mahkemesi’nin ortaya koyduğu ilke ve tespitlerle bağdaşmayan, internet ortamında özellikle önemli hale gelen ifade özgürlüğü ve kişilik haklarını yeterince koruyamayan bir uygulamaya yol açmıştır. Geline nokta, İnternet Kanun’u; hukuka aykırı içeriğin çıkarılması ve erişimin engellenmesine ilişkin usullerin temel hak ve özgürlükler bakımından yeterli güvence taşımadığı, kişilik haklarına aykırı içeriğin çıkarılması ve/veya erişimin engellenmesini düzenleyen 9. maddenin tamamen iptal edildiği ve oluşan boşluğu dolduracak bir düzenlemenin de yapılmadığı bir hal almıştır.

⁹³³ Yazar, bu görüşünü İngiltere’de internetin düzenlenmesine ilişkin görüşmeler sırasında belirtmiştir. <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/communications-committee/the-internet-to-regulate-or-not-to-regulate/oral/83478.html>, (13.10.2024).

Çevrimiçi platformların bir kamusal alana dönüştüğü, internet şirketlerinin ifade özgürlüğünün kullanılmasında kilit aktörler haline geldiği, yapay zekâ, blockchain, metaverse gibi yeni teknolojilerin ortaya çıkmasıyla daha da karmaşıklaşan dijital ortamda; bu gelişmelere cevap verebilen bir internet düzenlenmesi daha da önemli hale gelmiştir. Nitekim, bu gelişmeler Avrupa Birliği’nde dijital hizmetlerin daha güvenli, adil ve şeffaf bir şekilde sunulmasını sağlayacak yenilenmiş ve vizyoner bir çerçeve oluşturulmasına yönelik bir girişimi başlatmıştır.⁹³⁴ Bu girişimler 19 Ekim 2022 tarihinde Dijital Hizmetler Yasası (DSA)’nın kabul edilmesiyle sonuçlanmıştır.

Bu bölümde, Türk hukukunda çevrimiçi ortamı düzenlemeye yönelik artan ihtiyaca katkı sunabilmek için bazı önerilere yer verilecektir. Bu öneriler, her şeyden önce Türk hukukunun yaklaşık yirmi yıla dayanan tecrübesine dayanmaktadır. Bununla birlikte DSA’nın temel hakların etkin bir şekilde korunduğu güvenli, öngörülebilir ve güvenilir bir çevrimiçi ortam sağlamayı amaçlayan kapsamı ve AIHM’in internet teknolojilerindeki gelişmelerle birlikte gelişen içtihadı da önemli bir vizyon sağlamaktadır.

A. İçerik Moderasyonuna İlişkin Öneriler

5651 sayılı Kanun’da, Anayasa Mahkemesi’nin iptal kararıyla birlikte, içerik moderasyonuna ilişkin üç prosedür bulunmaktadır. Bu üç prosedür uyarınca içeriğe şu iki şekilde müdahale edilebilmektedir: i) ilgili yayına ya da sitenin tamamına erişimi engellenme ve ii) içeriği yayından çıkarma. İnternet şirketleri adli ve idari makamlar tarafından karar verilmesi halinde, bu kararların gereklerini yerine getirmeleri gerekmektedir.

Buna göre, çocuk istismarı, uyuşturucu ticareti, müstehcenlik, fuhuş, Atatürk’e hakaret gibi belirli suçların işlenmesi halinde adli merciler ya da resen Başkan kararıyla (m. 8); ulusal güvenlik, kamu düzeni, halk sağlığı ve suçun önlenmesi gibi sebeplerle gecikmesinde sakınca olan hallerde hakim ya da Cumhurbaşkanlığı veya bazı bakanlıkların talebi üzerine Başkan tarafından (m. 8/A) ve özel hayatın gizliliğinin ihlal edilmesi durumunda kişilerin talebi üzerine ya da özel hayatın gizliliğine bağlı olarak gecikmesinde sakınca olan hallerde doğrudan Başkan tarafından (m. 9/A) erişimin

⁹³⁴ “Impact Assessment 1”, para. 5.

engellenmesi kararı verilebilmektedir. İlk durumda Başkan tarafından verilen kararlar yargı denetimine tabi değilken; diğerlerinde Başkanın kararının yirmi dört saat içerisinde hâkim onayına sunulması gerekmektedir. Kanunda öngörülen kademeli sisteme göre, bu kararlar kural olarak ihlalin gerçekleştiği yayın, kısım, bölüm ile ilgili olarak (URL, vb. şeklinde) verilir; ancak, teknik yetersizlikler söz konusu internet sitesinin tümüne erişim engellenebilir. Özel hayatın gizliliğini ihlal eden hallerde, yalnızca URL şeklinde erişimin engellenmesi kararı verilmesi mümkündür.

Kanuna göre, içeriğin yayından çıkarılmasına ise, 8. maddede belirtilen suçların işlenmesi halinde yalnızca adli merciler tarafından; 8/A maddesinde belirtilen sebeplerle gecikmesinde sakınca olan hallerde ise yine hâkim ya da Cumhurbaşkanlığı veya bazı bakanlıkların talebi üzerine ve sonrasında hâkim onayına sunulacak şekilde Başkan tarafından karar verilebilmektedir.

Bu sistemde, bir idari makam olan BTK Başkan'ı tarafından suç işlendiği tespiti yapılarak, hâkim kararı güvencesine aykırı şekilde bir internet sitesinin tamamına, belirsiz bir süreliğine erişim engellenebilmektedir. Kanun, ulusal güvenlik, kamu düzeni, suç işlenmesinin önlenmesi gibi sebeplerle gecikmesinde sakınca olan hallerde, kararın yeniden gözden geçirilmesine ilişkin bir usul öngörmediğinden; engellenen internet sitelerinin yıllarca erişilemez olması da mümkündür. Öte yandan, içerik moderasyonu kapsamında alınabilecek kararlar erişimin engellenmesi ve içeriğin yayından çıkarılmasından ibaret olup; orantılılık ilkesi çerçevesinde daha az kısıtlayıcı tedbirlerin (örneğin, içerik sağlayıcı tarafından açıklama veya düzeltme yapılması ya da yer sağlayıcının içeriğin görünürlüğünü azaltması) uygulanması imkânı bulunmamaktadır.

İçerik moderasyonuna ilişkin süreçlerde, doğrudan Kanun'dan kaynaklanan bu sorunlar yanında uygulamada da önemli sorunlar vardır. Sulh ceza hakimliklerinin ilgili ve yeterli gerekçe ihtiva etmeyen, somut olaya özgü değerlendirme içermeyen, içerikle sınırlama sebebi arasında ilişkiyi ortaya koymayan, muğlak ifadelerden oluşan ve ilk bakışta ihlal kriterine karşılamayan kararlar yerleşik bir hal almıştır.⁹³⁵ Bu durum,

⁹³⁵ Artı Media Gmbh Başvurusu, para. 46.

Kanun'un keyfi kararların önüne geçebilecek, çatışan haklar arasında adil bir denge kurulmasını garanti edebilecek temel güvencelere sahip olmamasının bir sonucudur.

İnternet ortamında suç teşkil eden, kamu düzenini tehdit eden, kişilik haklarını ihlal eden yayınlarla mücadeleyi amaçlayan ve bu amaçla internet şirketlerine içerik moderasyonuna ilişkin yükümlülükler yüklenmesi devletin pozitif yükümlülüğünün bir gereğidir. Ancak, internet, modern demokrasilerde tartışmaların ve politik faaliyetlerin merkezinde yer aldığından, bu kapsamda alınacak kararlar ile kullanılan metotların demokrasi ve insan haklarına duyulan saygıyla bağlantılı olduğu unutulmamalıdır. Anayasa Mahkemesi tarafından da dikkat çekildiği gibi çağdaş demokrasiler, yasa dışı içerikle mücadeleyi, internet ortamında söz sahibi olan tüm aktörler ile iş birliği içerisinde hareket ederek yürütmekte ve devletin daha az müdahil olduğu yöntemleri benimsemektedirler.⁹³⁶

Avrupa Konseyi İnsan Hakları Komiserliği'nin 2014'te yayımladığı İnternet ve Dijital Dünyada Hukukun Üstünlüğü başlıklı rapor da bu konuya ışık tutmaktadır. Özellikle engelleme sistemlerinin genellikle şeffaf olmaması, hangi sitelerin neden engellendiği konusunda kamuoyuna yeterli bilgi verilmemesi ve kararların temyiz edilebilir olmaması önemli eleştiriler arasındadır. Ayrıca, engelleme kararlarının çoğu zaman yanlış pozitifler (yani yasadışı içerik barındırmayan sitelerin de engellenmesi) doğurabileceği belirtilmektedir.

Avrupa İnsan Hakları Mahkemesi'ne göre de devletler veya özel sektör aktörleri tarafından getirilen her türlü erişim kısıtlaması ulaşılabilir ve öngörülebilir olmalı, meşru bir amaca hizmet etmeli ve orantılılık ilkesi uyarınca hedefe ulaşmak için en az müdahaleyi içermelidir. Ayrıca, bu tür kararların yargı denetimine açık olması ve şeffaf bir şekilde kamuoyuna açıklanması zorunludur.⁹³⁷ AİHM içtihadında, tek bir yasadışı içeriğin varlığı nedeniyle yüzlerce yasal içeriğin engellenmesi, ölçüsüz bir müdahale olarak kabul edilmektedir.⁹³⁸ Bu tür kararlar, web sitesinin içerebileceği yasal ve yasadışı bilgiler arasındaki ayrımı göz ardı etmekte ve yasadışı olduğu tespit edilmemiş büyük miktarda içeriği erişilemez hale getirmektedir. Web sitesinin tamamına erişimin

⁹³⁶ Keskin Kalem Yayıncılık ve Ticaret A.Ş. ve Diğerleri Başvurusu, para. 136.

⁹³⁷ Vladimir Kharitonov v. Russia, 10795/14 (ECtHR 23 Haziran 2020) para. 45; OOO Flavus and Others v. Russia, 12468/15, 23489/15 (ECtHR 23 Haziran 2020), para. 30-36.

⁹³⁸ Vladimir Kharitonov v. Russia, para. 38.

engellenmesi, engelleme kararının kapsamını başlangıçta hedeflenen yasadışı içeriğin çok ötesine genişletmek gibi pratik bir etkiye sahiptir.⁹³⁹

Türk hukukunda, erişimin engellenmesine yönelik prosedürlerin öngörülebilirlik, orantılılık, şeffaflık ve keyfi kararların önüne geçebilecek mekanizmaların sağlanması gerekmektedir.

Bu kapsamda, *ilk olarak* içerik moderasyonuna ilişkin kararlar arasında bir ayrım yapılmalıdır. Bu kararların bir yargılamayla bağlantılı olarak tedbiren uygulanması ile yargılama sürecinden bağımsız olarak uygulanması farklı gerekliliklere tabidir. Venedik Komisyonu'na göre, kanunun ihlal edildiğine dair makul bir şüphe ve telafisi mümkün olmayan bir zarar tehlikesi olduğunda tedbir olarak içeriğin çıkarılması ve erişimin engellenmesi mümkündür. Bu durumda yargılama hâkimi, müteakip ceza veya hukuk yargılamalarında tedbirin sürdürülmesinin gerekliliğini gözden geçirebilmeli ve makul şüpheyi destekleyen unsurların bulunmadığı veya tehlikenin önlendiği kanaatine varması halinde bu tedbiri derhal kaldırabilmelidir.

Bir yargılama sürecinden bağımsız olarak içerik moderasyonunu gerektiren usullerde ise; internet sağlayıcısına kendini savunması, hâkime de iyi gerekçelendirilmiş bir karar verebilmesi için yeterli zaman ve imkân ve özellikle de ifade özgürlüğü bakımından orantılılık değerlendirmesi yapması için duruşma yapma yetkisi verilmesi gerektiği söylenebilir. Duruşma, hâkime davanın tüm somut koşullarını doğru bir şekilde inceleme ve ifade özgürlüğü ile başkalarının hakları arasında adil bir denge kurmak için tarafların görüşlerini değerlendirme fırsatı verecektir.⁹⁴⁰

İkinci olarak, içerik moderasyonuna ilişkin usuller hâkim kararı güvencesine⁹⁴¹ uygun şekilde düzenlenmelidir. Buna göre, idari bir kararla alınacak kararlar istisnai

⁹³⁹ OOO Flavus and Others v. Russia, para. 37.

⁹⁴⁰ Venice Commission On Law No. 5651 on Regulation of Publications on the Internet and Combating Crimes Committed by Means of Such Publication ("The Internet Law"), para. 61-62.

⁹⁴¹ "Millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; haberleşme engellenemez ve gizliliğine dokunulamaz. Yetkili merciin kararı yirmidört saat içinde görevli hâkimin onayına sunulur. Hâkim, kararını kırksekiz saat içinde açıklar; aksi halde, karar kendiliğinden kalkar." Ay. m. 22(2).

olmalı ve yargı denetimine tabi olmalıdır. Keyfi kararların önüne geçilebilmesi için, idari makamlara resen karar alabilme yetkisi verilmemelidir.

Üçüncü olarak, etkili bir uyarı mekanizmasının kurulması gerekmektedir. 5651 sayılı Kanunun mevcut şekline göre, yalnızca Türkiye’den günlük erişimi bir milyondan fazla olan sosyal ağ sağlayıcılar, kişilerin hukuka aykırı içeriği bildirmelerini sağlayacak bir uyarı sistemi kurmakla yükümlüdür.⁹⁴² Her ne kadar Kanun’un 5. maddesine göre, *“yer sağlayıcı, yer sağladığı hukuka aykırı içeriği bu Kanunun 8 inci ve 9 uncu maddelerine göre haberdar edilmesi hâlinde yayından çıkarmakla yükümlü”* olsa da bu madde bir uyarı sistemi sağlamamaktadır. Madde metninde yer almasına rağmen 9. madde yürürlükten kalktığından, yer sağlayıcı ancak 8. maddeye göre haberdar edilebilecektir ki bu da kişilerin değil idari mercilerin bildirimine ilişkindir. Öte yandan bu maddeye aykırılık halinde, çevrimiçi hizmet sağlayıcıya yönelik bir yaptırım öngörülmemekte, hizmet sağlayıcı yalnızca sorumluluktan muafiyet rejiminin dışına itilmektedir. Bu yaklaşım, hukuka aykırı içeriklerle etkili mücadele açısından yetersiz kalmaktadır.

Dolayısıyla, bu mekanizmanın tüm yer sağlayıcılar için, boyutları ne olursa olsun, hukuka aykırı içeriklere ilişkin bildirimde bulunulabilecek erişilebilir ve kullanıcı dostu bir uyarı sistemi kurma zorunluluğu ile güçlendirilmesi gerekmektedir. Bu uyarılar, pek çok durumda çevrimiçi hizmet sağlayıcıya yarışan haklar arasında denge kurmak gibi oldukça zor bir görev yükleyecektir. Dolayısıyla ifade ve bilgi özgürlüğüyle uyumlu, bilinçli ve özenli kararlar alınabilmesi için, uyarı sistemleri kesin ve yeterli bir şekilde gerekçelendirilmiş bildirimlerin sunulmasına olanak tanımalıdır. Uyarı sisteminin etkili olabilmesi için, hizmet sağlayıcıların bu kapsamda aldıkları kararlara karşı idari ya da adli mercilere itirazda bulunulabilmelidir. Bu kapsamda, uyarı üzerine alınan kararlarda hizmet sağlayıcılar, kararın nedenleri ve karar karşı başvuru olanakları konusunda bilgilendirilmelidir.⁹⁴³

Uyarı sistemi bakımından önem teşkil eden bir başka husus da hizmet sağlayıcının eyleme geçmesini gerektirecek eşiğin belirlenmesidir. AB Dijital Hizmetler Yasası (DSA) uyarınca, bu yükümlülük bildirim konu içerik veya faaliyetin hukuka

⁹⁴² “İnternet Kanunu”, m. Ek 4(3,8).

⁹⁴³ “DSA”, resital 53, 54.

aykırılığının "detaylı bir hukuki inceleme" gerektirmeksizin anlaşılabilir olması koşuluna bağlıdır. Buna göre, hizmet sağlayıcılardan karmaşık bir hukuki analiz yapması beklenmemekte, bariz bir ihlal tespit edilebilecek durumlarda eyleme geçmeleri istenmektedir.⁹⁴⁴ Bu yaklaşım, Anayasa Mahkemesi'nin internet içeriğinin kısıtlanmasına ilişkin geliştirdiği "ilk bakışta ihlal" doktrini⁹⁴⁵ ile de uyum içerisindedir. Bu bakımdan, uyarı sistemlerinin de yayınının kişilik haklarını apaçık bir şekilde ihlal ettiğinin daha ilk bakışta anlaşıldığı durumlarda işletilecek şekilde düzenlenmesi yerinde olacaktır. Böylece, asıl işi hukukçuluk olmayan internet şirketlerine aşırı yükümlülük getirmeden yarışan haklar arasında adil bir denge kurulması sağlanabilecektir.

Dördüncü olarak, yer sağlayıcıların sorumluluktan muafiyet rejimi yeniden ele alınmalıdır. Daha önce de belirtildiği gibi, AB hukukundan farklı olarak Türk hukukunda, yer sağlayıcılar hukuka aykırı içerikten yalnızca 8. madde kapsamında bir bildirim aldıklarında sorumlu hale gelmektedir. Hukuka aykırı içerikle mücadele, etkili bir uyarı-eylem sistemi yanında yer sağlayıcıların daha fazla sorumluluk üstlenmelerini gerektirmektedir. Bu kapsamda, bir genel izleme yükümlülüğüne yol açmamak kaydıyla; yer sağlayıcıların sorumluluk rejimi, hukuka aykırı içerikten kendi inisiyatifleri sonucunda haberdar oldukları hallerde de harekete geçmelerini sağlayacak şekilde düzenlenmelidir.⁹⁴⁶

Bu hususta, AİHM içtihadı da hassas bir çerçeve sunmaktadır. AİHM, açıkça nefret söylemi ve şiddete teşvik içeren yorumlar söz konusu olduğunda internet portallarına daha geniş sorumluluklar yüklenebileceğini kabul etmektedir.⁹⁴⁷ Öyle ki Mahkeme, bu tür içerikler söz konusu olduğunda, teknik imkanlara sahip olmayan bir bireyin dahi kendi sosyal medya hesabında yapılan yorumlardan sorumlu olabileceğini kabul etmiştir.⁹⁴⁸ Buna karşın, nefret söylemi ve şiddete teşvik içermemekle birlikte saldırgan, kaba vb. nitelikteki üçüncü taraf içerikleri bakımından ise AİHM, prensip olarak çevrimiçi hizmet sağlayıcıları uyar-kaldır mekanizmasını etkili bir şekilde

⁹⁴⁴ "DSA", m. 16(3).

⁹⁴⁵ Ali Kızık Başvurusu, para. 62.

⁹⁴⁶ "DSA", resital, 22-26.

⁹⁴⁷ Pihl v. Sweden para. 37; Zöchling v. Austria, para. 13.

⁹⁴⁸ Sanchez v. France, para. 179-180.

işletildiği sürece hukuka aykırı içerikten sorumlu tutmamakta ve aksinin araçlar üzerinde caydırıcı etkiye yol açabileceğini kabul etmektedir.⁹⁴⁹

Beşinci olarak, orantılılık ilkesi gereğince, hem idari ve adli merciler tarafından alınacak kararlar hem de çevrimiçi hizmet sağlayıcılar için alınacak kararlarda alternatif sistemlerin uygulanabilmesini mümkün hale getirmek gerekmektedir. Hukuka aykırı içerikle ilgili olarak, içeriğin alt sıralara düşürülmesi (*demotion*), değersizleştirilmesi⁹⁵⁰ (*demonetisation*), erişiminin engellenmesi veya kaldırılması gibi içeriğin mevcudiyetini, görünürlüğünü ve erişilebilirliğini etkileyen veya bir alıcının hesabının kalıcı olarak kapatılması veya askıya alınması gibi hizmet alıcılarının bu bilgileri sağlama kabiliyetini etkileyen farklı kararlar alınabileceği göz önünde bulundurulmalıdır.⁹⁵¹ Yine bu kapsamda kişilik hakkını ihlal eden içerikler bakımından, hakları ihlal edilenlerin ad ve soyadlarının içerikle ilişkilendirilmemesini ifade eden unutulma hakkına yasal dayanak kazandırılması önem teşkil etmektedir.

Son olarak, içerik moderasyon süreçlerinde şeffaflığı sağlayacak mekanizmalar kurulmalıdır. Herkes, internet şirketlerinin hem kendi inisiyatifleri ile hem de adli ve idari mercilerin kararları üzerine uyguladıkları kararlara ve kararların gerekçelerine erişebilmelidir. Özellikle alınan kararlardan ikincil olarak etkilenen diğer kişilerin yargı yollarına başvurabilmesini sağlayacak şekilde bilgi edinebilmelerinin sağlanması gerekmektedir. Şeffaflığın güvence altına alınması, bilgiye erişim hakkının korunması yanında, hak arama hürriyetinin etkin bir şekilde kullanılabilmesinin de teminatıdır. Aksi durum, kamuoyunun karar süreçlerini denetleme yetisini elinden almakta, potansiyel olarak bireylerin temel haklarını zayıflatmakta ve demokratik hesap verebilirliği zedelemektedir.⁹⁵²

⁹⁴⁹ Høiness v. Norway, para. 73-75.

⁹⁵⁰ İnternet kullanıcılarının, YouTube veya Instagram (daha az olarak Facebook) gibi platformlarda para kazanabilecekleri iş modellerinden biri de platformun sunduğu programlar aracılığıyla para kazancı elde etmesidir. Bu programlar, reklam verenlerin içerik boyunca veya içeriğin üzerine çeşitli biçimlerde (örneğin, bannerlar, multimedya klipleri) reklam görüntülemelerine izin verir. İçerik yönetimi kapsamında platformlar (genellikle sosyal medya platformları), tek taraflı olarak, içerik oluşturucu/etkili kişinin gelir akışına erişimini engelleyebilir. Bu tedbir, kullanıcının yalnızca belirli videolar için potansiyel geliri kaldırdığından, çok katı bir tedbir olarak değerlendirilmemektedir. Zingales, “Demonetization – Glossary of Platform Law and Policy Terms”.

⁹⁵¹ “DSA”, m. 3(1)/t.

⁹⁵² Vladimir Kharitonov v. Russia, para. 44.

B. Şeffaflık Yükümlülüğüne İlişkin Öneriler

5651 Sayılı İnternet Kanunu, sosyal ağ sağlayıcıların şeffaflık yükümlülükleri açısından geniş bir çerçeve çizmektedir.

Buna göre, sosyal ağ sağlayıcıların altı aylık dönemlerle Türkçe şeffaflık raporları hazırlamaları ve bu raporlarda şu hususlara yer vermeleri gerekmektedir: i. kendilerine bildirilen içeriğin çıkarılması ve/veya erişimin engellenmesi kararlarının uygulanmasına ve özel hayatın gizliliğini ihlal eden içerikler bakımından uyarı yöntemi ile yapılan başvurulara ilişkin istatistiksel ve kategorik bilgileri, ii. kullanıcı eşitliği ve tarafsızlığı kapsamında alınan tedbirler, iii. suç teşkil eden içeriklerin ve başlık etiketlerinin yayınlanmamasını sağlamak için gerekli sistem ve mekanizmaları, iv. öneri sistemlerinde kullanılan parametreler, v. kullanıcılara önerilen içeriklere ilişkin tercihleri güncelleme ve kişisel verilerinin kullanılmasını sınırlandırma seçeneği sunma konusunda alınan tedbirler. Ek 4. maddede, istatistiksel ve kategorik bilgileri içeren Türkçe hazırlanmış raporların altı aylık dönemlerle Kuruma bildirilmesi öngörülmektedir. Adli ve idari merciler tarafından yapılacak bildirimlerden farklı olarak, uyarı yöntemi ile kişiler tarafından yapılan başvurulara ilişkin raporun, kişisel verilerden arındırılmak suretiyle sosyal ağ sağlayıcının kendi internet sitesinde de yayınlanması da gerekmektedir.⁹⁵³

Şeffaflık yükümlülükleri kapsamında, sosyal ağ sağlayıcılarının platformlarındaki içerik denetim süreçlerinin izlenmesi, kullanıcılara yönelik ayrımcı uygulamalar yapmalarının önlenmesi, kullanıcıların platform üzerindeki deneyimlerine dair daha fazla kontrol sahibi olmalarının sağlanması, reklam süreçlerinin açık hale getirilmesi ve kullanıcıların platform üzerindeki ticari uygulamalara dair bilgi edinmesine olanak tanınması önemlidir.

Bununla birlikte, internet ortamında hukukun üstünlüğünün sağlanabilmesi daha fazla şeffaflık gerektirmektedir. Bu teknoloji şirketlerinin interneti düzenleme biçimlerine duyulan güvenin artırılmasının da ön koşuludur.⁹⁵⁴ Şeffaf bir internet yönetimi, bir yandan şirketlerin hareket biçimlerini ve karar alma süreçlerinin; diğer yandan da internet yönetişiminin bileşenlerinden olan idari ve adli merciler ile internet kullanıcılarının bu

⁹⁵³ “İnternet Kanunu”, m. Ek 4(4).

⁹⁵⁴ Suzor, *Lawless*, s. 139.

sürece etkilerinin aydınlatılmasını gerektirir. Türk hukukunda çevrimiçi içi hizmet sağlayıcıların şeffaflık yükümlülüklerinin bu hususlar ışığında yeniden ele alınması gereklidir. Bu yükümlülükler öngörülebilir ve orantılı olmalıdır.

Bu kapsamda öncelikli olarak ele alınması gereken hususlardan biri, şeffaflık yükümlülüklerinin muhatabının belirlenmesidir. Mevcut düzenlemeye göre, şeffaflık yükümlülükleri, Türkiye’den günlük erişimi bir milyondan fazla olan yurt içi veya yurt dışı kaynaklı sosyal ağ sağlayıcılara yöneliktir. Dolayısıyla, bu erişim düzeyinin altında kalan sosyal ağ sağlayıcılar ve sosyal ağ sağlayıcılardan⁹⁵⁵ olmayan arama motorları (*belirtilen erişim düzeyinden bağımsız olarak*) şeffaflık yükümlülüklerin muhatabı değildir. Avrupa Birliği Dijital Hizmetler Yasası’na göre, aracı hizmet sağlayıcılar, çevrimiçi platformlar ve arama motorları boyutlarına göre değişen kapsamda şeffaflık yükümlülüklerine tabidir.⁹⁵⁶ Buna göre, örneğin, mikro ve küçük ölçekli aracı hizmet sağlayıcılar hizmetin sunulmasına ilişkin güncel bilgileri hizmet koşullarında açıkça belirtmekle yükümlüken şeffaflık raporlama yükümlülüğüne tabi değildir.

Türk hukukunda da şeffaflık yükümlülüklerine ilişkin kademeli bir sistem kurulması ve kavramsal tercihin bir sonucu olarak dışlanan arama motorlarının bu yükümlülüklerin kapsamına alınması daha güvenli bir dijital ortamın tesisine katkı sağlayacaktır. Bu bağlamda, özellikle Türkiye’de yoğun erişime sahip çevrimiçi platformlar ve arama motorlarının şeffaflık raporlama yükümlülükleri çerçevesinde; içerik kaldırma süreçleri, algoritmaların işleyişi, bu algoritmaların doğruluk oranları ve hata payları, adli ve idari makamların talepleri, kullanıcı başvuruları, reklam politikaları, çocukların çevrimiçi ortamda karşılaşılabilecekleri riskler kapsamında alınan önlemler gibi konularda kamuoyunu ve ilgili kurumları bilgilendirmesi zorunlu hale getirilmelidir.

Öte yandan, İnternet Kanunu’nda çevrimiçi hizmet sağlayıcıların, hizmetlerinin kullanılmasına ilişkin kurallarını içeren hizmet koşullarının şeffaflığına ilişkin bir yükümlülük yer almamaktadır. Özel kişiler arasında bir sözleşme görünümü veren; ancak çevrimiçi hayatın kurallarını belirleyerek gündelik hayatın yönetiminde önemli bir rol

⁹⁵⁵ İnternet Kanunu’nun 2. maddesine göre, sosyal ağ sağlayıcı kavramı, sosyal etkileşim amacıyla kullanıcıların internet ortamında metin, görüntü, ses, konum gibi içerikleri oluşturmalarına, görüntülemelerine veya paylaşımlarına imkân sağlayan gerçek veya tüzel kişileri ifade etmektedir.

⁹⁵⁶ “DSA”, resital 48.

oynadıklarından anayasal düzenlemelere benzetilen⁹⁵⁷ bu metinlerin, sunulan hizmetin türü ya da hizmet sağlayıcının büyüklüğü gibi ayrımlar göz önünde bulundurularak şeffaflık yükümlülüğü kapsamında ele alınması önemlidir.⁹⁵⁸

Nitekim Dijital Hizmetler Yasası'nda da sözleşme özgürlüğü ilkesine saygı gösterilmesi gerekliliği kabul edilmekle birlikte şeffaflık, hizmet alıcılarının korunması ve keyfi sonuçların önlenmesi amacıyla, bu sağlayıcıların hüküm ve koşullarının içeriği, uygulanması ve yürütülmesine ilişkin bazı kuralların belirlenmesi gerektiğine dikkat çekilmiştir.⁹⁵⁹

Bu doğrultuda, hizmet koşullarına ilişkin artırılmış şeffaflık yükümlülükleri ile internet kullanıcılarının izin verilen ya da yasaklanan içeriklerin neler olduğu; hizmet koşullarına aykırı halinde ne tür kararlar alınabileceği; alınan kararlara karşı hangi itiraz yollarına başvurulabileceği; kullanıcı verilerinin ne şekilde toplandığı ya da kullanıldığı gibi hususlarda yeterli bilgiye sahip olmaları sağlanmalıdır. Ayrıca, hizmet kullanımını sonlandırılmasına ilişkin erişilebilir bilgiler sunulması ve önemli değişiklikler yapıldığında, kullanıcıları etkin yöntemlerle bilgilendirmeleri güvence altına alınmalıdır. Böylelikle, kullanıcıların hizmet sağlayıcıları ile etkileşimlerinde daha adil ve öngörülebilir sonuçlar elde edilmesi sağlanacaktır. İnternet ortamında bazı içerikler, içerik sahibinin hesabının askıya alınmasını ya da kapatılmasını dahi gerektirebileceğinden; hizmet koşulları açık, erişilebilir ve kullanıcılar tarafından kolayca anlaşılabilir olmalıdır. Örneğin, çocuklar tarafından da erişilmesi mümkün olan hizmetlere ilişkin hizmet şartlarının, çocukların anlayabileceği açıklıkta olması gerekir.

Ayrıca, şeffaflık raporlarında adli ve idari merciler tarafından bildirilen içeriğin çıkarılması ve/veya erişimin engellenmesi kararlarının uygulanmasına ilişkin istatistiksel ve kategorik bilgilerin de kamuoyuyla paylaşılması sağlanmalıdır. Ek 4. maddenin dördüncü

⁹⁵⁷ Suzor, *Lawless*, s. 13; Edoardo Celeste, “Terms of service and bills of rights: new mechanisms of constitutionalisation in the social media environment?”, **International Review of Law, Computers & Technology**, C. 33, S. 2, 2019, ss. 122-38.

⁹⁵⁸ İngiltere'de sosyal medya platformları ve diğer online hizmet sağlayıcılarının yükümlülüklerinin ele alındığı Online Safety Act, buna ilişkin kapsamlı yükümlülükler içermektedir. Chapter 3 Terms of Services: Transparency, Accountability, Freedom of Expression, <https://www.legislation.gov.uk/ukpga/2023/50>, (15.10.2024). OSA'daki yükümlülüklerin kapsamı için bkz. Beatriz Kira, Laura Schertel Mendes, “A Primer on the UK Online Safety Act”, **Verfassungsblog**, 2023, <https://verfassungsblog.de/a-primer-on-the-uk-online-safety-act/>, (23.12.2024).

⁹⁵⁹ “DSA”, resital 45.

fıkrası, kişiler tarafından yapılan başvurulara ilişkin raporlardan farklı olarak, adli ve idari mercilerin kararlarının uygulanmasına ilişkin istatistiklerin sosyal ağ sağlayıcının internet sitesinde paylaşılmasını gerektirmemektedir.⁹⁶⁰ Oysa, sosyal ağ sağlayıcıların adli ve idari mercilerden aldıkları bildirimlerin ve bildirimler üzerine ne şekilde hareket ettiklerinin bilinmesi hesap verebilirliğin bir gereğidir. Her ne kadar bazı platformlar adli ve idari mercilerin taleplerine ilişkin bilgilere raporlarında gönüllü olarak yer verse de⁹⁶¹ kamuoyunun yeterli şekilde bilgilendirilebilmesi ve şeffaflığın sağlanabilmesi için bu husus platformların inisiyatifine bırakılmamalıdır.

C. Risk Yönetimine İlişkin Öneriler

İnternet Kanunu'nda, 2022 yılında yapılan değişikliklerle⁹⁶² sosyal ağ sağlayıcılara risk yönetimi bağlamında değerlendirilebilecek bir kısım yükümlülükler yüklenerek internet ortamında sunulan hizmetlerin güvenliğini sağlamaya yönelik önemli bir adım atılmıştır.

Kanun, belirli bir kullanıcı sayısına erişen sosyal ağ sağlayıcıların; Kanun kapsamındaki suçlara ilişkin içerikler ile başlık etiketlerinin yayınlanmamasına ilişkin tedbirler almalarını, kullanıcılarına önerdikleri içeriklerde kullandıkları algoritmik parametreleri açıklamalarını, reklam kütüphanesi oluşturmalarını, çocuk kullanıcıların güvenliğini sağlamalarını ve kriz planı hazırlamalarını gerektirmektedir.⁹⁶³ Bu yükümlülükler, temel hak ve hürriyetlerin gerçekleştirilmesine yönelik yeni fırsatlar sunan dijital ortamın potansiyel riskleriyle mücadelenin kritik bir bileşeni olarak, kapsamlı bir risk yönetim stratejisinin önemli bir parçasını teşkil etmektedir.

Birleşmiş Milletler İş Dünyası ve İnsan Haklarına Dair Rehber İlkeler'de, risk yönetimi, şirketlerin insan haklarına saygı gösterme sorumluluğunun bir gereği olarak kabul edilmiştir. Rehber İlkeler göre, risk yönetimine ilişkin yükümlülükler, şirketin

⁹⁶⁰ “İnternet Kanunu”, m. Ek 4(4).

⁹⁶¹ Örneğin Google, bugüne kadar yayınladığı tüm raporlarında bireysel talepler yanında idari taleplere ilişkin de bilgilere yer vermiştir. <https://transparencyreport.google.com/report-downloads?hl=tr>, (16.10.2024). Meta ise, Instagram ve Facebook platformlarına ilişkin geçmiş dönemlerdeki raporlarından farklı olarak, 2024 yılında yayınladığı iki raporunda da kişiler tarafından yapılan başvurular yanında adli ve idari makamlarda alınan taleplere ilişkin bilgilere de yer vermiştir. <https://transparency.meta.com/reports/regulatory-transparency-reports/>, (16.10.2024).

⁹⁶² 7418 sayılı Basın Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun, m. 34..

⁹⁶³ “İnternet Kanunu”, m. Ek 4(4).

büyüklüğü ve insan hakları üzerindeki etkisine göre değişebilecektir. Buna göre, mevcut riskler telafi edici, potansiyel riskler ise önleyici ve azaltıcı çözüm yöntemini gerektirmektedir.⁹⁶⁴ Ciddi insan hakları etkilerinin olması halinde de şirketlerden buna ilişkin raporlama yapmaları beklenmektedir.

Avrupa Birliği Dijital Hizmetler Yasası (DSA) da risk yönetimi yükümlülüklerine büyük bir önem atfetmektedir. Aracı hizmet sağlayıcılar, platformlarındaki kullanıcı güvenliğini sağlamak, temel hakları korumak ve kötüye kullanımın önüne geçmek amacıyla kapsamlı tedbirler almak zorundadır. Bu yükümlülükler, özellikle çok büyük çevrimiçi platformlar ve arama motorları için daha da katmanlıdır. Buna göre, çok büyük çevrimiçi platformlar ve arama motorlarının cinsel istismar, nefret söylemi gibi hukuka aykırı içeriğin yayılması, temel haklar, demokratik süreçler ve halk sağlığı, çocuklar, toplumsal cinsiyete dayalı şiddet gibi diğer toplumsal kaygılarla ilgili olarak sistemik riskleri derinlemesine değerlendirilmeleri ve teknik kapasiteleri, kullanıcı kitleleri ve temel haklar üzerindeki etkileri ölçüsünde makul ve etkili risk azaltıcı tedbirler almaları gerekmektedir.⁹⁶⁵

Risk yönetimine ilişkin bu yükümlülüklerin arka planında, platformların yapılandırılma ve yönetilme biçiminin şirketlerin kararlarına bağlı olduğu gerçeği yatmaktadır. Bu durum, şirketlere kullanıcı deneyimini şekillendirme konusunda büyük bir güç verdiğinden bu güç kullanıcıların zarar görmemesi için sorumluluğu da beraberinde getirmektedir. Dolayısıyla, şirketlerin, aldıkları kararların doğrudan sonuçları olacağını göz önünde bulundurarak, kullanıcıların güvenliğini ön planda tutmalarını sağlayacak tedbirlerin alınması önemlidir.

Söz konusu tedbirler, platform arayüzlerinin ve hüküm koşullarının riskleri en aza indirecek şekilde uyarlanmasını, bildirim ve harekete geçme mekanizmalarının iyileştirilmesini, algoritmik sistemlerin geliştirilmesini, güvenilir bilgi kaynaklarının görünürlüğünün artırılmasını, şüpheli içeriğin etiketlenmesini ve uygun davranış kurallarının uygulanmasını kapsayabilir.⁹⁶⁶

⁹⁶⁴ “BM Guiding Principles”, ilke 17.

⁹⁶⁵ “DSA”, para. 79-83.

⁹⁶⁶ “DSA”, m. 35.

İnternet Kanunu'nda 2022 yılında yapılan değişikliklerin amacı da internet ortamında insanların onur, şeref ve saygınlığının, kişisel haklarının, özel hayatlarının dokunulmazlığının ve kişisel verilerinin korunması için ihtiyaç duyulan önleyici ve koruyucu mekanizmaları geliştirilmesidir.⁹⁶⁷ Bu amacın gerçekleştirilmesi, risk yükümlülüklerinin daha kapsamlı ve öngörülebilir bir biçimde ele alınmasıyla mümkün olabilir.

Bu bağlamda, çevrimiçi hizmet sağlayıcılarının risk yönetimi ile ilgili yükümlülükleri, hizmetlerin ölçeği, insan hakları üzerindeki potansiyel etkileri ve risk kapasiteleri dikkate alınarak yeniden değerlendirilmelidir. Risk yönetimine ilişkin yükümlülüklerin belirlenmesinde, sunulan hizmetlerin çocuklar tarafından erişilebilirliği önemli bir kriter olmalıdır. Özellikle, temel hak ve özgürlüklere yönelik ciddi riskler taşıyan çevrimiçi hizmet sağlayıcılarının, hizmetlerini sunarken sistemik riskleri analiz etmeleri ve bu riskleri azaltmaya yönelik önlemler almaları sağlanmalıdır.

Risk yönetimine ilişkin yükümlülüklerde, çevrimiçi ortamın kadınlar ve diğer hassas gruplar üzerindeki potansiyel etkileri özel olarak değerlendirilmelidir. Örneğin, cinsiyet temelli nefret söylemi, tehdit ya da taciz içeriklerin olumsuz etkilerini ortadan kaldırmaya yönelik tedbirler alınabilir.

Çocukların çevrimiçi güvenliğinin sağlanması da risk yönetimi yükümlülüğünün önemli bir boyutunu oluşturmaktadır. Bu nedenle, İnternet Kanunu'nda öngörülen mevcut çerçevenin, daha belirgin ve kapsamlı tedbirlerle genişletilmesi önemlidir. Bunun için öncelikle, çocuklar için zararlı içeriğin kapsamına ilişkin net bir çerçeve oluşturulmalıdır. Bu tedbirler, platformların hizmetlerinin çocukların hakları üzerindeki olası etkilerini değerlendirirken, çocukların platformların tasarımını ve işleyişini ne kadar kolay anladıklarını ve zararlı içeriklere maruz kalma risklerini göz önünde bulundurmalarını sağlamaya yönelik olmalıdır. Çocukların zayıflıklarından ve deneyimsizliklerinden faydalanan arayüz tasarımları veya bağımlılık yaratıcı özelliklerin bu riskleri artırabileceği gözden kaçırılmamalıdır.⁹⁶⁸

⁹⁶⁷ Madde Gerekeçleri, 7418 sayılı Basın Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun, Esas Komisyon Raporu Sıra Sayısı 340.

⁹⁶⁸ “DSA”, resital 81.

SONUÇ

Dijitalleşme, ifade özgürlüğü ve bilgi edinme hakkı gibi temel hak ve özgürlüklerin kullanımında yeni bir dönemi başlatmıştır. İnternet, erişilebilirliği ve çok sayıda veriyi saklama ve yayma konusundaki yeterliliği dolayısıyla, güncel bilgiye erişmenin ve daha genel anlamda bilginin yayılmasının en önemli aracı haline gelmiştir. Bu bakımdan, yeni demokrasilerde yeni mecralar yoluyla kullanılan ifade özgürlüğü “demokrasinin oksijeni” olarak kabul edilmektedir. Öte yandan, zaman, dijital gelişmelerin yanlış bilgilerin yayılması, siber zorbalık, sanal dolandırıcılık, pornografi, çocuk istismarı, fuhuş, kumar, şiddetin, nefretin ve ırkçılığın yayılması, terörizmin desteklenmesi ve yaygınlaştırılması gibi yıkıcı etkileri de gün yüzüne çıkarmıştır. Dijital gelişmelerin bu iki boyutu, çevrimiçi ortamın yönetimine ilişkin tartışmalara yol açmıştır. Her gün milyarlarca insan tarafından kendilerini ifade etmek, tartışmak, eleştirmek, araştırmak, görüş ve içerik oluşturmak için kullanılan internet bu yönüyle bir kamusal alana dönüşmüştür. Böylece, bu yeni kamusal alanı yöneten internet şirketleri demokratik süreçleri şekillendirmede benzeri görülmemiş bir fırsat elde etmiştir. İnternet şirketlerinin bu etkinliği, kişisel özerkliğe saygı ve iktidar gücünün keyfi kullanımının dışlanması düşüncelerine dayanan hukukun üstünlüğü ilkesini önemli ölçüde aşındırmıştır. Bu durum, çevrimiçi ortamda temel hak ve özgürlüklerin korunması ve hukukun üstünlüğü ilkesinin tesisine yönelik ulusal ve uluslararası girişimleri beraberinde getirmiştir.

Esasen, şirketler ve insan hakları ilişkisi, küreselleşmenin ekonomik güçler üzerindeki etkisi ve toplumların bu etkinin olumsuz sonuçlarını yönetmedeki yetersizliği dolayısıyla yaklaşık yirmi yıldır insan hakları hukukunun önemli tartışma alanlarından biri olmuştur. Bu yönde atılmış en önemli adımlardan biri, Birleşmiş Milletler İnsan Hakları Konseyi’nin İş Dünyası ve İnsan Haklarına Dair Rehber İlkeler’i (UNGPs) onaylamasıdır. İş dünyası ile insan hakları ilişkisinin kurulması ve şirketlerin insan hakları yükümlülüklerine ilişkin küresel standartların ortaya koyulması bakımından bir dönüm noktası olarak kabul edilen Rehber İlkeler, şirketlerin sorumluluklarının sektörel olarak da ele alınması bakımından bir basamak tahtası işlevi görmüştür. BM Rehber İlkeler, üç temel prensipten oluşmaktadır:

- Devletlerin uygun politikalar, düzenlemeler ve yargısal süreçler aracılığıyla, şirketler de dahil üçüncü tarafların insan hakları ihlallerine karşı koruma yükümlülüğü.
- Şirketlerin başkalarının haklarını ihlal etmemek için gereken özeni göstermesi ve kendi faaliyetlerinden kaynaklanan olumsuz etkileri ele almasını ifade eden insan haklarına saygı gösterme sorumluluğu.
- Mağdurların yargı yoluyla ya da yargı dışı mekanizmalarla etkili çözüm yollarına erişiminin sağlanması.

Rehber İlkeler uyarınca şirketlerin insan haklarına saygı gösterme sorumluluğunu yerine getirmek için insan haklarını bilmeleri ve bu haklara saygı gösterdiklerini göstermeleri gerekmektedir. Bu da a) insan haklarına saygı gösterme sorumluluklarını yerine getirme taahhüdünü içeren bir politika benimsenmesi; b) insan hakları üzerindeki etkilerini belirlemek, önlemek, azaltmak ve ele almak için durum değerlendirme süreci işletilmesi ve c) neden oldukları veya katkıda bulundukları olumsuz insan hakları etkilerini gidermek için süreçler oluşturulması da dahil olmak üzere şirketlerin büyüklüklerine ve koşullarına uygun politikalar ve süreçler ile mümkündür. Rehber İlkeler’de tüm şirketleri kapsayacak şekilde ortaya koyulan bu çerçeveye göre internet şirketleri, en azından insan haklarına saygı göstermekle ve şirketler için öngörülen somut adımları atmakla sorumludur. Bu sorumluluk öncelikle, internet şirketlerinin insan hakları ihlallerine ilişkin olarak bir politika taahhüdünde bulunmalarını ve faaliyetlerinin insan hakları üzerindeki etkilerini değerlendirmelerini gerektirmektedir.

Birleşmiş Milletler sisteminde, çevrimiçi ortamın yarattığı riskleri ele alan ve bu ortamı yöneten internet şirketlerinin insan hakları sorumluluklarını ortaya koyan çeşitli kararlar da kabul edilmiştir. Rehber İlkelerin internet sektörüne uyarlanması olarak görülebilecek bu kararlarda içerik düzenlemesi, gözetim ve dijital güvenlik, şeffaflık sorunları ele alınmış ve çözüm önerilerine yer verilmiştir. İfade özgürlüğü ile ilgili olarak, şirketlerin faaliyetlerinin her aşamasında insan hakları standartlarını uygulamalarını tavsiye edilmektedir. Bunun için de şirketler en azından, internetin kullanımına ilişkin kuralları belirlemeli ve bu kuralların uygulanmasında şeffaflığı mümkün olan en üst düzeyde sağlamalıdır. Çevrimiçi ortamda dönüştürücü bir etkiye yol açan yapay zeka teknolojileri de özellikle son dönemlerde BM’nin ele aldığı temel meselelerden biri haline gelmiştir. Bu kapsamda, insanlar gibi kültürel bağlamı değerlendirme, ironi tespit etme

veya “aşırılık yanlısı” içerik ya da nefret söylemi gibi konuları doğru bir şekilde tanımlamak için gerekli olan eleştirel analizi yapma yeteneğine sahip olmayan algoritmaların içerik düzenleme süreçlerini daha da zorlaştırabileceğine dikkat çekilmiş ve bu teknolojilerin geliştirilmesinde şeffaflık temelinde insan haklarına ilişkin durum değerlendirme süreçlerinin işletilmesi gerektiği belirtilmiştir. BM, nefret söylemi ve dezenformasyonla mücadele kapsamında da şirketlerin sorumluluğunu kabul etmektedir. Bu sorumluluk kullanıcı haklarına duyarlı bir yaklaşım benimsenmesini, mevcut endişelere proaktif bir şekilde yanıt verilmesini ve internet kullanıcılarının güçlendirilmesini gerektirmektedir.

Ekonomik İş Birliği ve Kalkınma Örgütü (OECD) bünyesinde de dijital gelişmeler göz önünde bulundurularak şirketlerin insan hakları yükümlülükleri ele alınmıştır. OECD, Çok Uluslu Şirketler için Sorumlu İş Davranışı Rehberi ve Dijital Hizmet Sağlayıcılar için Rehber İlkeler gibi araçlarla, şirketlere insan hakları, çalışma standartları, çevre ve yolsuzlukla mücadele konularında kapsamlı bir çerçeve sunmaktadır.

Çalışmada, uluslararası örgütler tarafından sunulan bu genel çerçeve ortaya koyulduktan sonra, Avrupa hukukundaki gelişmeler kapsamlı bir şekilde ele alınmıştır. Bu doğrultuda Avrupa Konseyi ve Avrupa Birliği’nde çevrimiçi ortamda temel hak ve hürriyetlerin güvence altına alınması ve hukukun üstünlüğünün sağlanmasına yönelik düzenlemeler ve konunun farklı boyutlarını ortaya çıkaran yargı kararları analiz edilmiştir.

Avrupa Konseyi’nde internet ortamında insan haklarının korunmasına yönelik çalışmalar, henüz internet kullanımının yaygınlaşmadığı dönemlere uzanmaktadır. İnternet hukukunun erken döneminde kabul edilen tavsiye kararlar ve bildirilerde, özel sektörün internet yönetimindeki etkisi kabul edilerek özel sektör aktörleri, hükümetler ve sivil toplumla işbirliği içinde, bilgi ve iletişim teknolojilerinin kötüye kullanımı veya yasadışı amaçlarla kullanımından kaynaklanan insan haklarına yönelik tehdit, risk ve kısıtlamaları önleme ve bunlara karşı koymak için önlemler almaya, bu teknolojiler aracılığıyla insan haklarının geliştirilmesi için davranış kuralları ile diğer öz düzenleme biçimlerini oluşturmaya ve bunların kapsamını daha da genişletmeye davet edilmiştir. Devletlere de özel şirketleri şeffaflığı özendirmeleri ve diğerlerinin yanı sıra bilgi alma

ve verme hakkı ile ilgili olarak içerik ve hizmetlere erişimin engellenmesi ve bunların filtrelmesi konusunda teknoloji ve hizmetlerin bireysel kullanıcılarına bilgi, rehberlik ve yardım sağlamak için ortak standartlar ve stratejiler geliştirmeye teşvik etmeleri tavsiye edilmiştir. 2018 yılında kabul edilen İnternet Aracılarının Rol ve Sorumluluklarına İlişkin Tavsiye Kararı'nda ise, internet araçlarının internetin yönetimindeki belirleyici rolleri ele alınmış; araçların sorumlulukları şeffaflık, içerik denetimi, kişisel verilerin kullanımı, etkili bir çözüme erişim şeklinde dört başlıkta ele alınmıştır.

Avrupa İnsan Hakları Mahkemesi (AİHM) içtihadında, internet ortamında temel hak ve özgürlüklerin korunmasına dair önemli gelişmeler yaşanmıştır. Belirtmek gerekir ki, şirketlerin Sözleşme kapsamında insan haklarına saygı gösterme sorumlulukları, devletin temel hakların garantörü olmaktan kaynaklanan yükümlülüklerini ifade eden “pozitif yükümlülükler” kavramıyla sıkı bir ilişki içerisinde. AİHM, pozitif yükümlülükler doktrinini, *Editorial Board of Pravoye Delo ve Shtetel/Ukrayna* kararıyla internet alanına genişletmiştir. İlerleyen yıllarda, özellikle ifade özgürlüğü ile özel hayata saygı hakkı ile bağlantılı olarak internet şirketlerinin sorumlulukları farklı boyutlarıyla incelenmiştir. AİHM, çevrimdışı hakların çevrimiçi ortamda da etkili şekilde korunması gereğini vurgularken, internetin özgül dinamiklerini göz önünde bulundurarak dijital politikanın uyarlanması gerektiğine işaret etmiştir. Mahkeme, internet araçlarının belirli şartlar altında üçüncü taraf içeriklerinden sorumlu olmamaları gerektiğini kabul etmekle birlikte, bu şirketlerin insan hakları ihlalleri riskini önleme açısından özen yükümlülüğüne sahip olduğunun da altını çizmiştir.

AİHM, açıkça nefret söylemi ve şiddete teşvik içeren yorumlar söz konusu olduğunda internet portallarına daha geniş sorumluluklar yüklenebileceğini kabul etmektedir. Öyle ki Mahkeme, bu tür içerikler söz konusu olduğunda, teknik imkanlara sahip olmayan bir bireyin dahi kendi sosyal medya hesabında yapılan yorumlardan sorumlu olabileceğini kabul etmiştir. Buna karşın, nefret söylemi ve şiddete teşvik içermemekle birlikte saldırgan, kaba vb. nitelikteki üçüncü taraf içerikleri bakımından ise AİHM, prensip olarak çevrimiçi hizmet sağlayıcıları uyar-kaldır mekanizmasını etkili bir şekilde işletildiği sürece hukuka aykırı içerikten sorumlu tutmamakta ve aksinin araçlar üzerinde caydırıcı etkiye yol açabileceğini kabul etmektedir.

Avrupa Birlięi, yakın dönemde kabul edilen düzenlemelerle birlikte internet şirketlerinin insan hakları yükümlölükleri bakımından oldukça kapsamlı bir çerçeve sunmaktadır. 2000 yılında kabul edilen E-Ticaret Direktifi'nden 2022 yılında kabul edilen Dijital Hizmetler Yasası'na (DSA) geçiş sürecinde internet şirketlerinin yükümlölüklerini yeniden şekillendirilmiştir. DSA, şirketlere sorumluluktan muafiyet, menşei ülke ilkesi ve genel izleme yükümlölüğü yasağı gibi prensipleri korurken, dijital çağın gerekliliklerine uygun yeni yükümlölükleri de getirmiştir. Özen yükümlölükleri olarak ifade edilen bu yükümlölükler DSA'da; aracı hizmet sağlayıcılar, barındırma sağlayıcıları, çevrimiçi platformlar ve çok büyük çevrimiçi platformlar (VLOPs) ile çok büyük arama motorları (VLOSEs) arasında ayırım yapan kademeli bir yapıda ele alınmıştır. Bu kapsamda internet şirketlerine yönelik hem içerik denetimi hem de risk yönetimine ilişkin çok çeşitli yükümlölükler öngörülmüştür.

DSA, içerik denetimi konusunda bir yandan çevrimiçi hizmet sağlayıcıların hukuka aykırı içerikle mücadelede daha aktif olmalarını; diğer yandan da bu mücadelenin hukukun üstünlüğü ilkesine uygun şekilde ve temel haklara saygı çerçevesinde sürdürülmesini amaçlamaktadır. Bu doğrultuda şirketler, etkili bildirim ve eylem sistemi kurarak kullanıcıların hukuka aykırı içerik hakkında kolaylıkla harekete geçip sonuç alabilmelerini sağlamak, manipölatif arayüz tasarımlarından kaçınmak, reklam hedeflemesinde hassas verilerin kullanılmamasını temin etmek, çocuklar için erişilebilir hizmetlerde yüksek düzeyde gizlilik ve güvenlik önlemleri almak ve bu kapsamda alınan tedbirleri raporlamakla yükümlü kılınmıştır.

DSA, aktif kullanıcı sayısının belirli bir seviyenin üzerinde olması dolayısıyla çevrimiçi güvenliğin sağlanması, kamuoyunun şekillendirilmesi ya da çevrimiçi ticaretin sürdürülmesi bakımından geniş bir etki alanına sahip çok büyük çevrimiçi platformlar ve çok büyük arama motorları için ayrıca risk yönetimine ilişkin de yükümlölükler de öngörmüştür. Buna göre bu kategoride yer alan internet şirketleri, çocuk istismarı materyalleri, terörist içerikler, nefret söylemi ve bireyleri hedef alan hukuka aykırı reklamlar, fikri mülkiyet haklarını ihlal eden içerikler vb. gibi hukuka aykırı içeriklerin yayılmasından ya da tehlikeli mallar, güvenli olmayan oyuncaklar, hukuka aykırı ilaçlar, taklitler, dolandırıcılıklar gibi tüketicilerin korumasını ihlal eden uygulamalardan kaynaklanabilecek risklerin yönetmek ve risk azaltıcı tedbirler almakla yükümlüdür. Bu tedbirler etkili, orantılı ve makul olmalıdır.

Avrupa Birlięi hukuku bakımından, mevcut düzenleyici çerçevenin yorumlanmasında Avrupa Birlięi Adalet Divanı (ABAD) kararlarının önemli bir rolü vardır. ABAD, özellikle sorumluluktan muafiyet rejiminin kapsamının belirlenmesi ve internet ortamında yarışan haklar arasında denge durulmasına yönelik önemli kararlar vermiştir. Öte yandan, ECD ve DSA’da kabul edilen genel izleme yükümlülüęü yasağı da kararlarda üzerinde durulan hususlardan biridir. ABAD, hizmet sağlayıcıların, (1) önleyici bir tedbir olarak; (2) masrafları yalnızca kendisine ait olmak üzere; (3) kullanıcılar arasında ayırım gözetmeksizin ve 4) sınırsız bir süre için; (5) sunucularında depolanan bilgileri filtreleyecek bir filtreleme sistemi kurmaya zorlanmasının genel izleme yükümlülüęü anlamına geleceęine ve AB hukuku ile uyumsuz olduęunu kabul etmiştir. Bununla birlikte, Mahkeme, genel izleme ile özel izleme kavramlarını birbirinden ayırarak böyle bir yasağın '*belirli bir durumda*' izleme yükümlölükleriyle ilgili olmadıęını ortaya koymuştur. ABAD, ilk defa 2014 yılında kabul ettięi unutulma hakkının farklı boyutlarına yönelik kararlara da internet şirketlerinin bu hak kapsamındaki yükümlölüklerini belirlemiştir. Buna göre unutulma hakkı, içerięe referans veren bağlantının kaldırılması yanında, makaleyi gösteren küçük resimler şeklinde görüntölenen fotoęrafların kaldırılmasını da gerektirebilmektedir. Mahkeme ayrıca AB üyesi olmayan ölkelerin hukuk sistemlerine saygının bir sonucu olarak, unutulma hakkının dünya çapında bir uygulama gerektirmedięine hükmetmiştir. Unutulma hakkı bakımından gündeme gelen bir başka belirsizlik de söz konusu başvurular bakımından ispat yükünün hangi tarafta olduęuna ilişkindir. ABAD’a göre, internet şirketleri, bu taleplerle ilgili olarak herhangi bir araştırma ya da delil toplama yükümlölüęü altında deęildir; makul düzeyde gerekli bilgi ve belgeler başvuru tarafından sunulmalıdır.

Çalıřmada, Türk hukukundaki mevcut durum da kapsamlı bir şekilde ele alınmış; erişimin engellenmesi ve içeriğın çıkarılmasına dair prosedürlerde anayasal güvencelerin yetersizlięi ve şeffaflık ile risk yönetimine ilişkin yükümlölüklerdeki eksiklikler tespit edilmiştir.

Türk hukukunda internet şirketlerinin yükümlölüklerine ilişkin temel düzenleme bugüne de çok sayıda deęişikliğe, iptale ve ilğaya konu olan 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun (İnternet Kanunu)’dur. 2020 yılında yapılan deęişiklikle sosyal aę sağlayıcıların özel bir sorumluluk ve yükümlölük rejimine tabi

tutulması önemli bir adım olmakla birlikte, bu düzenlemeler internetin potansiyel riskleri ile baş edebilme konusunda yeterli olmadığı gibi internet ortamında yarışan hak ve menfaatler arasında adil bir denge kurulabilmesine elverişli değildir.

İnternet Kanunu'nda içerik yer ve erişim sağlayıcılar bilgilendirme, trafik bilgilerini saklama ve internet içeriğinin kaldırılması ve/veya erişimin engellenmesine ilişkin yükümlülükler tabidir. Sosyal ağ sağlayıcılar ise bunlara ek olarak temsilci belirleme ve bildirme, şeffaflık, içerik moderasyonu, bilgi paylaşma, kullanıcı haklarına saygı, veri saklama, çocuk koruma ve kriz planı oluşturma yükümlülüklerine tabidir. Bu yükümlülükler analiz edildiğinde, mevcut çerçevenin içerik moderasyonu, şeffaflık ve risk yönetimi bakımından yeterli olmadığı anlaşılmaktadır. İçerik moderasyonuna ilişkin süreçlerde, yargılama hukukunun usule ilişkin güvencelerinin eksikliği ile keyfi kararların önüne geçebilecek, çatışan haklar arasında adil bir denge kurulmasını garanti edebilecek temel güvencelerin yokluğu öne çıkan sorunlardır. Bunun yanında, Kanun'da öngörülen şeffaflık yükümlülükleri de içerik moderasyon süreçlerinin her açıdan izlenmesini sağlayacak düzeyde değildir. Kanun'da risk yönetimine ilişkin yükümlülükler yüzeysel olarak ele alınmıştır. Bu da nefret söylemi, çocuk istismarı, demokratik süreçler, halk sağlığı, çocuklar, toplumsal cinsiyete dayalı şiddet gibi diğer toplumsal kaygılarla ilgili olarak risklerin değerlendirilmesi ve ortadan kaldırılması ya da azaltılması konusunda yetersizliğe yol açmaktadır. Bu bakımdan, Türk hukukunda uluslararası standartlara uyum sağlama çabaları olumlu bir gelişme olarak değerlendirilse de şeffaflık, hesap verebilirlik ve risk yönetimi alanlarında reformlara ihtiyaç olduğu açıktır.

Bu çalışmada, Türk hukukunda çevrimiçi ortamı düzenlemeye yönelik artan ihtiyaca katkı sunabilmek için çeşitli önerilere yer verilmiştir. Bu öneriler şu şekilde sıralanabilir:

1. İçerik moderasyonuna ilişkin kararlar arasında bir ayırım yapılmalıdır. Bu kararların bir yargılamayla bağlantılı olarak tedbiren uygulanması ile yargılama sürecinden bağımsız olarak uygulanması farklı gerekliliklere tabi olmalıdır.

2. İerik moderasyonuna ilişkin usuller hâkim kararı güvencesine uygun şekilde düzenlenmelidir. İdari bir kararla alınacak kararlar istisnai olmalı ve yargı denetimine tabi olmalıdır.
3. İnternet şirketlerinin etkili, erişilebilir ve kullanıcı dostu uyarı-eylem mekanizması kurmaları ve bu mekanizmaları işletmeleri sağlanmalıdır.
4. Orantılılık ilkesi gereğince, hem idari ve adli merciler tarafından alınacak kararlar hem de çevrimiçi hizmet sağlayıcılar için alınacak kararlarda alternatif sistemlerin uygulanabilmesi mümkün hale getirilmelidir.
5. İerik moderasyon süreçlerinde şeffaflığı sağlayacak mekanizmalar kurulmalıdır. Herkes, internet şirketlerinin hem kendi inisiyatifleri ile hem de adli ve idari mercilerin kararları üzerine uyguladıkları kararlara ve kararların gerekelerine erişebilmelidir.
6. Şeffaflık yükümlülüğüne ilişkin kademeli bir sistem kurulmalı ve şirketler büyüklüklerine göre deėişen şeffaflık yükümlölüklerine tabi tutulmalıdır. Kavramsal tercihin bir sonucu olarak dışlanan arama motorları da bu yükümlölüklerin kapsamına alınmalıdır.
7. Şeffaflık raporlarında adli ve idari merciler tarafından bildirilen içeriğın ıkarılması ve/veya erişimin engellenmesi kararlarının uygulanmasına ilişkin istatistiksel ve kategorik bilgilerin de kamuoyuyla paylaşılması sağlanmalıdır.
8. İnternet şirketlerinin risk yönetimi ile ilgili yükümlölükleri, hizmetlerin öleėi, insan hakları üzerindeki potansiyel etkileri ve risk kapasiteleri dikkate alınarak yeniden deėerlendirilmelidir. Özellikle, temel hak ve özgürlöklere yönelik ciddi riskler taşıyan çevrimiçi hizmet sağlayıcılarının, hizmetlerini sunarken sistemik riskleri analiz etmeleri ve bu riskleri azaltmaya yönelik önlemler almaları sağlanmalıdır.

9. Risk yönetimine ilişkin yükümlölüklerde, çevrimiçi ortamın kadınlar, çocuklar ve diğér hassas gruplar üzerindeki potansiyel etkileri özel olarak değérlendirilmelidir.

Sonuç olarak, internetin hızla gelişen doğası ve yeni risklerin ortaya çıkması göz önüne alındığında, interneti düzenleme süreci, sürekli güncellenmesi gereken dinamik bir alan olarak ele alınmalıdır. Bu doğrultuda, kullanıcı haklarını koruma ve internet şirketlerinin insan hakları yükümlölüklerini yerine getirmelerini sağlama amacıyla, yeni teknolojik gelişmelere uygun düzenleyici çerçeveler oluşturulmalı ve bu çerçeveler toplumsal ihtiyaçlar doğrultusunda sürekli yenilenmelidir.



KAYNAKÇA

Kitaplar ve Makaleler

AKANDJI-KOMBE Jean-François, “Positive Obligations under the European Convention on Human Rights”, **Human Rights Handbooks**, No. 7, 2007.

AKRIVOPOULOU Christina M., “The Right to Public Privacy under Surveillance: CCTV Technology and the Myth of ‘Public Security’”, Human Rights and Risks in the Digital Era: Globalization and the Effects of Information Technologies, **IGI Global Scientific Publishing**, 2012, ss. 25-32.

AKSOY RETORNAZ E. Eylem, “5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkındaki Kanun Kapsamında İçerik Sağlayıcının Yükümlülükleri ve Ceza Sorumluluğu”, **Ceza Hukuku Dergisi**, C. 16, S. 45, 2021, ss. 9-32.

ALAFAA Princess U., “Data Privacy and Data Protection: The Right of User’s and the Responsibility of Companies in the Digital World.”, 07.01.2022.

ANGELOPOULOS Christina, “Beyond the Safe Harbours: Harmonising Substantive Intermediary Liability for Copyright Infringement in Europe”, **Intellectual Property Quarterly**, S. 3, 2013, ss. 253-274.

ANGELOPOULOS Christina, Stijn SMET, “Notice-and-Fair-Balance: How to Reach a Compromise between Fundamental Rights in European Intermediary Liability”, **Journal of Media Law**, C. 8, S. 266, 2016, ss. 1-36.

ASH Timothy Garton, **Free Speech: Ten Principles for a Connected World**, Yale University Press, 2016.

AXWORTHY Lloyd, “The Mouse Is Mightier than the Sword”, **Human Rights and the Internet**, ed. Steven Hick, Edward F. Halpin, Eric Hoskins, London: Palgrave Macmillan UK, 2000, ss. 16-20.

BAISTROCCHI Pablo, “Liability of Intermediary Service Providers in the EU Directive on Electronic Commerce”, **Santa Clara High Technology Law Journal**, C. 19, S. 1.

BALKIN Jack M., “Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society”, **New York University Law Review**, S. 79, 2004, ss. 1-55.

———, “Free Speech Is a Triangle”, **Columbia Law Review**, C. 118, 2018, s. 2011.

BARENDT Eric, “Freedom of Expression”, **The Oxford Handbook of Comparative Constitutional Law**, ed. Michel Rosenfeld, András Sajó, Oxford University Press, 2012.

BENEDEK Wolfgang, Matthias C. KETTEMANN, **Freedom of Expression and the Internet: Updated and Revised 2nd Edition**, Council of Europe, 2020.

———, **İfade özgürlüğü ve internet**, Ankara: Adalet Bakanlığı, 2016.

BLITT Robert C., “Beyond Ruggie’s Guiding Principles on Business and Human Rights: Charting an Embrasive Approach to Corporate Human Rights Compliance”, **Texas International Law Journal**, C. 48, S. 1, 2012.

BOYAR, Oya, “Devletin Pozitif Yükümlülükleri ve Dolaylı Yatay Etki”, **İnsan Hakları Avrupa Sözleşmesi ve Anayasa** (ed. Sibel İnçeoğlu), 3. bs, 2013.

BOYAR Oya, Sezen Kama IŞIK, “Dördüncü Kuşak Haklar ve Bilişim Teknolojilerinin Doğuşunda Mahremiyet Kavramına Karşılaştırmalı Bir Bakış”, **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, C. 25, S. 2, 2019, ss. 602-23.

BOYLE Kevin, Sangeeta SHAH, “Thought, Expression, Association and Assembly”, **International Human Rights Law** (ed. Daniel Moeckli, Sangeeta Shah, David Harris, Sandesh Sivakumaran), OUP Oxford, 2014.

BOZARTH Jane, **Social Media for Trainers: Techniques for enhancing and extending learning**, John Wiley & Sons, 2010.

BUITEN Miriam, “The Digital Services Act: From Intermediary Liability to Platform Regulation”, 2021, **JIPITEC**, C. 12, S. 5, 2021, ss. 361-380.

BURI Ilaria, Joris VAN HOBOKEN, “‘The Digital Services Act (DSA) Proposal: A Critical Overview’: Discussion Paper”, 2021, <https://dare.uva.nl/search?identifier=d51d31c3-cfef-4034-b04a-c353f4ac07ea>.

CÁRCEL Garrigues-Ángela López, “Right to Be Forgotten: Developments with Regard to de-Referencing in the Light of Inaccurate Information”, **Lexology**, 26.01.2023.

CELESTE Edoardo, “Terms of service and bills of rights: new mechanisms of constitutionalisation in the social media environment?”, **International Review of Law, Computers & Technology**, C. 33, S. 2, 2019, ss. 122-38.

CLAPHAM Andrew, **Human Rights in the Private Sphere**, Oxford, New York: Oxford University Press, 1996.

COCHE Eugénie, “Countering Terrorism Propaganda Online Through TERREG and DSA: A Battlefield or a Breath of Hope for Our Fundamental Human Rights?”, **The Legal Challenges of the Fourth Industrial Revolution**, ed. Dário Moura Vicente, Sofia De Vasconcelos Casimiro, Chen Chen, Law, Governance and Technology Series, Cham: Springer International Publishing, 2023, C. 57, ss. 313-33.

CUSTERS Bart, “New Digital Rights: Imagining Additional Fundamental Rights for the Digital Era”, **Computer Law & Security Review**, C. 44, 2022, ss. 1-13.

DE GREGORIO Giovanni, **Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society**, Cambridge, Cambridge University Press, 2022.

———, “From Constitutional Freedoms to the Power of the Platforms: Protecting Fundamental Rights Online in the Algorithmic Society”, **SSRN Scholarly Paper**, Rochester, NY: Social Science Research Network, 2018, <https://papers.ssrn.com/abstract=3365106>.

DE STREEL Alexandre, Martin HUSOVEC, “The E-Commerce Directive as the Cornerstone of the Internal Market”, European Union, 2020, [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648797/IPOL_STU\(2020\)648797_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648797/IPOL_STU(2020)648797_EN.pdf).

DOUEK Evelyn, “Content Moderation as Systems Thinking”, **Harvard Law Review**, C. 136, S. 2, 2022.

DROGE Cordula, ‘Positive Verpflichtungen der Staaten in der Europäischen Menschenrechtskonvention’, **Beiträge zum ausländischen öffentlichen Recht und Völkerrecht**, C. 159, 2003, s. 379-392.

DÜLGER Murat Volkan, “Sosyal Ağ Sağlayıcıların İnternet Haber Sitelerinin ve Şebekeler Üstü Hizmet Sağlayıcıların Hukuki Rejimi ve Eleştirisi”, 2023, <https://papers.ssrn.com/abstract=4425002>, (18.11.2024).

FERNÁNDEZ-DÍEZ En Ignacio Garrote, “Comparative analysis on national approaches to the liability of Internet intermediaries for infringement of copyright and related rights”, WIPO, 2014, <https://www.wipo.int/publications/en/details.jsp?id=4145&plang=E>, (8.10.2024).

FROSIO Giancarlo, Christophe GEIGER, “Taking Fundamental Rights Seriously in the Digital Services Act’s Platform Liability Regime”, **European Law Journal**, C. 29, S. 1-2, 2023, ss. 31-77.

FRYDMAN Benoît, Ludovic HENNEBEL, Gregory LEWKOWICZ, “Co-regulation and the rule of law”, **Governance, Regulation and Powers on the Internet**, ed. Cécile Méadel, Eric Brousseau, Meryem Marzouki, Cambridge: Cambridge University Press, 2012, ss. 133-50.

GALLI Federico, Andrea LOREGGIA, Giovanni SARTOR, “The Regulation of Content Moderation”, **The Legal Challenges of the Fourth Industrial Revolution**, ed. Dário Moura Vicente, Sofia De Vasconcelos Casimiro, Chen Chen, Law, Governance and Technology Series, Cham: Springer International Publishing, 2023, C. 57, ss. 63-87.

GREENBERG Marc H., “A Return to Lilliput: The LICRA v. Yahoo! Case and the Regulation of Online Content in the World Market”, **Berkeley Technology Law Journal**, C. 18, 2003, ss. 1191-1258.

G’SSELL Florence, “The Digital Services Act (DSA): A General Assessment”, Content Regulation in the European Union–The Digital Services Act, **Trier Studies on Digital Law 1**, 2023.

GURKAYNAK Gonenc, Ceren YILDIZ, Burak YESILALTAY, “Recently Proposed Amendments to Turkish Internet Law: Obligations Imposed on Social Network Providers”, https://www.gurkaynak.av.tr/Content/dosya/1178/d1982-mondaq_-recently-proposed-amendments-to-turkish-internet-law-obligations-imposed-on-social-network-providers.pdf, (10.10.2024).

GÜRKAYNAK Gönenç, İlay YILMAZ, Pınar KARA, “Türk İnternet Hukuku Uygulamasının ve Mevzuatının Evriminin İlk Dönemini Tamamlaması İçin Öneriler ve Gözlemler”,https://www.gurkaynak.av.tr/docs/Turk_Internet_Hukuku_Uygulamasinin_ve_Mevzuatinin_Evriminin_Ilk_Donemini_Tamamlamasi_Icin_Oneriler_ve_Gozlemler.pdf, (23.12.2024).

HABERMAS Jürgen, Frank, “The Public Sphere: An Encyclopedia Article (1964) (çev. Sara Lennox, Frank Lennox)”, **New German Critique**, S. 3, 1974, ss. 49-55.

HICKOK Elonnai, “Intermediary Liability and State Surveillance, Global Information Society Watch”, <https://giswatch.org/en/communications-surveillance/intermediary-liability-and-state-surveillance>, (22.10.2024).

HOWARD Philip N. vd., “Opening closed regimes: what was the role of social media during the Arab Spring?”, Working Paper, 2011, https://deepblue.lib.umich.edu/bitstream/handle/2027.42/117568/2011_Howard-Duffy-Freelon-Hussain-Mari-Mazaid_PITPI.pdf?sequence=1%26isAllowed=y, (24.12.2024).

HORNLE Julia, **Internet Jurisdiction Law and Practice**, Oxford, New York: Oxford University Press, 2021.

HUSOVEC Martin, “Mandatory Filtering Does Not Always Violate Freedom of Expression: Important Lessons from Poland v Council and European Parliament (C-401/19)”, **Common Market Law Review**, C. 60, S. 1, 2023, ss. 173-98.

———, **Principles of the Digital Services Act**, Oxford University Press, 2024.

———, “Rising above Liability: The Digital Services Act as a Blueprint for the Second Generation of Global Internet Rules”, **Berkeley Technology Law Journal**, C. 38, 2023, ss. 883-920.

JØRGENSEN Rikke Frank, **Framing the Net**, Edward Elgar Publishing, 2013.

———, “Human Rights and Private Actors in the Online Domain”, **New Technologies for Human Rights Law and Practice**, ed. Jay D. Aronson, Molly K. Land, Cambridge: Cambridge University Press, 2018, ss. 243-69.

———, “ICT and Human Rights”, The Danish Institute for Human Rights Denmark’s National Human Rights Institution, 2017.

JOUGLEUX Philippe, **Facebook and the (EU) Law: How the Social Network Reshaped the Legal Framework**, Springer International Publishing, 2022.

JULIA BARCELO Rosa, “Liability for on-line intermediaries: A European Perspective”, **European Intellectual Property Review**, C. 20, S. 12, 1998, S. 12, ss. 454-63.

KAMA IŞIK Sezen, *Avrupa Veri Koruma Hukukuna Anayasal Bir Bakış*, (Doktora Tezi), Marmara Üniversitesi, Sosyal Bilimler Enstitüsü, Kamu Hukuku Anabilim Dalı Kamu Hukuku Bilim Dalı, 2019.

KAYA Mehmet Bedii, “The regulation of Internet intermediaries under Turkish law: Is there a delicate balance between rights and obligations?”, **Computer Law & Security Review**, C. 32, S. 5, 2016, ss. 759-74.

KELLER Daphne, “The Right Tools: Europe’s Intermediary Liability Laws and the EU 2016 General Data Protection Regulation” **European Private Law eJournal**, 2017.

KIRA Beatriz, Laura SCHERTEL MENDES, “A Primer on the UK Online Safety Act”, *Verfassungsblog*, 2023, <https://verfassungsblog.de/a-primer-on-the-uk-online-safety-act/>, (23.12.2024).

KORPISAARI Päivi, “From Delfi To Sanchez – When Can An Online Communication Platform Be Responsible For Third-Party Comments? An Analysis Of The Practice Of The ECtHR And Some Reflections On The Digital Services Act”, **Journal of Media Law**, C. 14, S. 2, 2022, ss. 352-77.

LAIDLAW Emily, “A Framework for Identifying Internet Information Gatekeepers”, *International Review of Law, Computers & Technology*, C. 24, S. 3, 2010, ss. 263-276.

LANNON John, *Human Rights and Information Communication Technologies: Trends and Consequences of Use: Trends and Consequences of Use*, **IGI Global**, 2012.

MACKINNON Rebecca vd., “Fostering Freedom Online: The Role of Internet Intermediaries”, UNESCO, 2014.

MADIEGA Tambiama, **Reform of the EU Liability Regime for Online Intermediaries: Background on the Forthcoming Digital Services Act: In Depth Analysis**, LU: Publications Office, 2020.

MANHEIM Karl, Lyric KAPLAN, “Artificial Intelligence: Risks to Privacy and Democracy”, **Yale Journal of Law and Technology**, C. 21, S. 106, 2019.

MARONI Marta, “A Court’s Gotta Do, What a Court’s Gotta Do. An Analysis of the European Court of Human Rights and the Liability of Internet Intermediaries Through Systems Theory”, **EUI Working Papers**, 2019.

MCGILL Matthew D., “Unleashing the Limited Public Forum: A Modest Revision to a Dysfunctional Doctrine”, **Stanford Law Review**, C. 52, S. 4, 2000, ss. 929-57.

MCGONAGLE Tarlach, “The Council of Europe and Internet Intermediaries: A Case Study of Tentative Posturing”, **Human Rights In The Age Of Platforms**, The MIT Press, 2019.

METHVEN O'BRIEN Claire, "Business and Human Rights in Europe 2011-2021: A Decade in Review", **European Yearbook of Human Rights**, European Yearbook on Human Rights, 2021, ss. 407-448.

MIFSUD BONNICI, J. P., C. N. J. DE VEY MESTDAGH, "Right Vision, Wrong Expectations: The European Union and Self-Regulation of Harmful Internet Content", **Information and Communication Technology Law**, C. 14(2), ss. 133-49.

MILES Tom, "UN investigators cite Facebook Role in Myanmar Crisis, Reuters, 13 March 2018", 2018, <https://www.reuters.com/article/us-myanmar-rohingya-facebook/un-investigators-cite-facebook-role-in-myanmar-crisis-idUSKCN1GO2PN/> (20.12.2024).

MILLER Katharine, "Privacy in an AI Era: How Do We Protect Our Personal Information?", 18.03.2024, <https://hai.stanford.edu/news/privacy-ai-era-how-do-we-protect-our-personal-information>, (24.12.2024).

MONTAGNANI Maria Lillà, Alina TRAPOVA, "New Obligations for Internet Intermediaries in the Digital Single Market-Safe Harbors in Turmoil?", **Journal of Internet Law**, C. 22, S. 7, 2019.

MOON Richard, **The Constitutional Protection of Freedom of Expression**, University of Toronto Press, 2000.

NATH Aakanksha, Arpita SAHA, "U.N. Global Compact: The Lifeline of Corporate Social Responsibility", **SSRN Electronic Journal**, 2008, ss. 27, 28, <https://papers.ssrn.com/abstract=1329289>, (1.8.2022).

NEWTON Alex, "Any Volunteers? Challenges And Opportunities For Corporations Implementing The Responsibility to Respect Human Rights.", **Australian Journal of Corporate Law**, C. 28, S. 1, 2013, ss. 72-81.

———, **The Business of Human Rights: Best Practice and the UN Guiding Principles**, Routledge, 2019.

NORDEMANN Jan Bernd, “The Functioning of the Internal Market for Digital Services: Responsibilities and Duties of Care of Providers of Digital Services”, **European Sources Online**, <https://www.europeansources.info/record/the-functioning-of-the-internal-market-for-digital-services-responsibilities-and-duties-of-care-of-providers-of-digital-services/>, (24.10.2024)

NUNZIATO Dawn, “From Town Square to Twittersphere: The Public Forum Doctrine Goes Digital”, **GW Law Faculty Publications & Other Works**, 2018.

O'BRIEN Claire Methven, Sumithra DHANARAJAN, “The Corporate Responsibility to Respect Human Rights: A Status Review”, **National University of Singapore**, C. Working Paper 2015/005, 2015, https://law.nus.edu.sg/wp-content/uploads/2020/04/005_2015_Sumi-Dhanarajan.pdf, (10.11.2023)

OCAK Ayşenur, “Hakları Dengelemek: Unutulma Hakkı İfade Özgürlüğüne Karşı”, **Türkiye Adalet Akademisi Dergisi**, S. 33, 2018, ss. 507-36.

ORUC Toygar Hasan, “The Prohibition of General Monitoring Obligation for Video-Sharing Platforms under Article 15 of the E-Commerce Directive in Light of Recent Developments: Is It Still Necessary to Maintain It?”, **Journal of Intellectual Property, Information Technology and Electronic Commerce Law**, C. 13, 2022, ss. 176-99.

ÖZENÇ Berke, “Toplantı ve Gösteri Yürüyüşü Özgürlüğü ve Mekân Yasakları”, **İstanbul Üniversitesi Hukuk Fakültesi Dergisi**, C. 73, S. 2, 2016, ss. 87-133.

PETKOVA Bilyana, “Privacy as Europe’s First Amendment”, **European Law Journal**, C. 25, S. 2, 2019, ss. 140-54.

PIVATY Anna, Pieter WOLTERS, “The obligation to notify suspicions of criminal offences in the Digital Services Act under scrutiny”, **Boom Strafbblad**, C. 3, S. 5, ss. 187-95.

POLLICINO Oreste, “Digital Private Powers Exercising Public Functions: The Constitutional Paradox in the Digital Age and its Possible Solutions”, 2021, https://www.academia.edu/47231825/Digital_Private_Powers_Exercising_Public_Funct

ions_The_Constitutional_Paradox_in_the_Digital_Age_and_its_Possible_Solutions, (19.07.2024).

———, “Judicial Protection of Fundamental Rights in the Transition from the World of Atoms to the Word of Bits: The Case of Freedom of Speech”, **European Law Journal**, 2019.

PSYCHOGIOPOULOU Evangelia, “The CJEU as a fundamental rights adjudicator in social media cases”, **Social Media, Fundamental Rights and Courts**, Routledge, 2023.

QUINTAIS João Pedro, “Between Filters and Fundamental Rights”, *Verfassungsblog*, 2022, <https://verfassungsblog.de/filters-poland/>, (12.10.2024).

QUINTAIS João Pedro, Christina ANGELOPOULOS, “YouTube and Cyando, Joined Cases C-682/18 and C-683/18 (22 June 2021): Case Comment (HvJ EU 22 Juni 2021, YouTube En Cyando)”, 2022.

ROGERS Michelle Paulson and Jacob, “Victory in France: Court Rules in Favor of the Wikimedia Foundation”, *Diff*, 20.06.2016, <https://diff.wikimedia.org/2016/06/20/france-legal-victory/>, (10.05.2023).

ROSATI Eleonora, “The Role, Responsibility and Liability of Online Intermediaries under EU IP Law”, **Handbook of Fashion Law**, Chapter 7, Routledge, 2024.

ROSENFELD Michel, András SAJÓ, **The Oxford Handbook of Comparative Constitutional Law**, OUP Oxford, 2012.

RUGGIE John Gerard, Tamaryn NELSON, “Human Rights and the OECD Guidelines for Multinational Enterprises: Normative Innovations and Implementations Challenges”, **Brown Journal of World Affairs**, C. 22, 2015, s. 99.

SAGAR Sander, Thomas HOFFMAN, “Intermediary Liability in the EU Digital Common Market-From the E-Commerce Directive to the Digital Services Act”, **IDP. Internet, Law and Politics E-Journal**. No. 34, 2021.

SALİHPAŞAOĞLU Yaşar, “Özel Hayatın Kapsamı: Avrupa İnsan Hakları Mahkemesi İçtihatları Işığında Bir Değerlendirme”, **Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi**, C. 17, S. 3, 2013, ss. 227-66.

SARTOR Giovanni, “Human rights and information technologies”, **The Oxford Handbook of Law, Regulation and Technology** (ed. R Brownsword, E Scotford, K Yeung), Oxford University Press, Oxford, 2017, s. 424.

SAVIN Andrej, **EU Internet Law**, Elgar European Law series, 2020.

———, “The EU Digital Services Act: Towards a More Responsible Internet”, Copenhagen Business School, **CBS Law Research Paper**, No. 21-04, 2021.

SCHEMBERA Stefan, Alice HENGVOSS, “Institutional Drivers of Responsible Innovation: The Impact of the UN Global Compact in the Digital Age”, <https://papers.ssrn.com/abstract=3485060>, (11.11.2019).

SEGURA María José, Contemporary Threats to Human Rights in the Online Public Sphere, (Doktora Tezi), University of Southern Denmark, 2017.

SENFTLEBEN Martin, Christina ANGELOPOULOS, “The Odyssey of the Prohibition on General Monitoring Obligations on the Way to the Digital Services Act: Between Article 15 of the E-Commerce Directive and Article 17 of the Directive on Copyright in the Digital Single Market”, 2020.

SOLOVE Daniel J., “The Limitations of Privacy Rights”, **Notre Dame Law Review**, C. 98, S. 3, 2022, ss. 975-1036.

SPANO Robert, “The Rule of Law as the Lodestar of the European Convention on Human Rights: The Strasbourg Court and the Independence of the Judiciary”, **European Law Journal**, C. 27, S. 1-3, 2021, ss. 211-27.

STALLA-BOURDILLON Sophie, “Internet Intermediaries as Responsible Actors? Why It Is Time to Rethink the E-Commerce Directive as Well”, **The Responsibilities of**

Online Service Providers, ed. Mariarosaria Taddeo, Luciano Floridi, Law, Governance and Technology Series, Springer International Publishing, 2017, C. 31, ss. 275-93.

SUZOR Nicolas, “Digital Constitutionalism: Using the Rule of Law to Evaluate the Legitimacy of Governance by Platforms”, **Social Media + Society**, C. 4, S. 3, 2018.

———, **Lawless: The Secret Rules That Govern our Digital Lives**, Cambridge, Cambridge University Press, 2019.

TIMMERMANS Louise, The Role of Internet Intermediaries in the Protection of Freedom of Expression and Personal Data: Human Rights in a Digital Age, (Master Tezi), University of Montpellier, 2017.

TOURKOKHORITI Ioanna, “The Digital Services Act and the EU as the Global Regulator of the Internet”, SSRN Scholarly Paper, Rochester, NY: Social Science Research Network, 10.07.2023, <https://papers.ssrn.com/abstract=4505169>.

———, “The Digital Services Act and the EU as the Global Regulator of the Internet”, *Chicago Journal of International Law*, C. 24, 2023, ss. 129-47.

TYMOFEYEVA Alla, “Indirect Obligations of Business Entities under the European Convention of Human Rights”, **Zech Yearbook of Public and Private International Law**, C. 8, 2018, ss. 291-305.

UYGUN Oktay, Devlet Teorisi, İstanbul: On İki Levha, 2017.

VAJIC Nina, Panayotis VOYATZIS, “The Internet And Freedom Of Expression: A ‘Brave New World’ and The European Court Of Human Rights’ Evolving Case Law”, *Freedom Of Expression, Essays in Honour of Nicolas Bratza*, 2012, 319-420.

WALDRON Jeremy, “The Concept and the Rule of Law”, **Georgia Law Review**, C. 43, S.1, ss. 1–61.

WILMAN Folkert, “The Digital Services Act (DSA)-An Overview”, **SSRN Scholarly Paper**, Rochester, NY, Social Science Research Network, 2022.

YASAMAN Zeynep, “Avrupa Birliđi ve Türk Hukuku Bakımından İnternet Yer Sağlayıcılarının Marka İhlalleri Kapsamında Sorumlulukları”, **Marmara Üniversitesi Avrupa Topluluđu Enstitüsü Avrupa Araştırmaları Dergisi**, C. 27, S. 2, 2019, ss. 263-91.

YÜCEL DERİCİLER Özge, “Şirketlerin İnsan Haklarına İlişkin Yükümlölüklerinin Niteliđi ve Temellendirilmesi Sorunu: Saygı Gösterme Sorumluluđu Ne Yükler?”, **Antalya Bilim Üniversitesi Hukuk Faköltesi Dergisi**, Cilt: 6, Sayı: 11, 2018.

———, **Uluslararası Esnek Hukuktan Bağlayıcı Hukuka: Şirketler ve İnsan Hakları**, On İki Levha, 2023.

ZINGALES Nicolo, “Demonetization – Glossary of Platform Law and Policy Terms”, 17.12.2021, <https://platformglossary.info/demonetization/>.

Belgeler, Kararlar ve Düzenlemeler

“Commission Decision of 26 July 2000 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the Safe Harbour Privacy Principles and Related Frequently Asked Questions Issued by the US Department of Commerce”, European Commission, <https://www.europeansources.info/record/2000-520-ec-commission-decision-of-26-july-2000-pursuant-to-directive-95-46-ec-of-the-european-parliament-and-of-the-council-on-the-adequacy-of-the-protection-provided-by-the-safe-harbour-privacy-pri/>, (12.10.2024).

Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (notified under document C(2016) 4176) (Text with EEA relevance) (2016), http://data.europa.eu/eli/dec_impl/2016/1250/oj/eng, (12.10.2024).

“Commission Recommendation of 6 May 2003 Concerning the Definition of Micro, Small and Medium-Sized Enterprises (Text with EEA Relevance) (Notified under Document Number C(2003) 1422)”, European Commission, 06.05.2003, <http://data.europa.eu/eli/reco/2003/361/oj/eng>, (5.10.2024).

“Committee on Women’s Rights annexed to Report on the Commission proposal for a Council Decision adopting a Multiannual Community Action Plan on promoting safe use of the Internet (Report of the Committee on Civil Liberties and Internal Affairs Rapporteur Mr Gerhard Schmid (A4-0234/98)”, 09.06.1998.

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions A Digital Single Market Strategy for Europe, C. COM(2015) 192 § (2015), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192>.

“Convention 108 +, Convention for the protection of individuals with regard to the processing of personal data”, Council of Europe, 18.05.2018,

<https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1>, (20.09.2024).

“Council Recommendation of 24 September 1998 on the Development of the Competitiveness of the European Audiovisual and Information Services Industry by Promoting National Frameworks Aimed at Achieving a Comparable and Effective Level of Protection of Minors and Human Dignity (98/560/EC)”, OJ L, Council of the European Union, 24.09.1998, <http://data.europa.eu/eli/reco/1998/560/oj/eng>.

“Çokuluslu İşletmeler ve Sosyal Politikaya İlişkin İlkeler Üçlü Bildirgesi (MNE Bildirgesi)”, 03.03.2017, <https://www.ilo.org/tr/publications/cokuluslu-isletmeler-ve-sosyal-politikaya-iliskin-ilkeler-uclu-bildirgesi>.

Decision No 276/1999/EC of the European Parliament and of the Council of 25 January 1999 adopting a multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks, C. OJ L 33 § (1999), [http://data.europa.eu/eli/dec/1999/276\(1\)/oj/eng](http://data.europa.eu/eli/dec/1999/276(1)/oj/eng).

“Declaration by the Committee of Ministers on Internet governance principles Decl(21/09/2011_2)”, Council of Europe, 21.09.2011, [https://search.coe.int/cm/#{%22CoEIdentifier%22:\[%2209000016805cc2f6%22\],%22sort%22:\[%22CoEValidationDate%20Descending%22\]}](https://search.coe.int/cm/#{%22CoEIdentifier%22:[%2209000016805cc2f6%22],%22sort%22:[%22CoEValidationDate%20Descending%22]}).

“Declaration of the Committee of Ministers on human rights and the rule of law in the Information Society (CM(2005)56)”, Council of Europe, 13.05.2005, https://www.coe.int/t/dgap/goodgovernance/activities/public_participation_internet_governance/Declaration-Information-Society/011_DeclarationFinal%20text_en.asp.

“Declaration of the Committee of Ministers on the UN Guiding Principles on business and human rights”, Council of Europe, 16.04.2014, [https://search.coe.int/cm/#{%22CoEIdentifier%22:\[%2209000016805c6ee3%22\],%22sort%22:\[%22CoEValidationDate%20Descending%22\]}](https://search.coe.int/cm/#{%22CoEIdentifier%22:[%2209000016805c6ee3%22],%22sort%22:[%22CoEValidationDate%20Descending%22]}).

“Declaration on freedom of communication on the Internet”, Council of Europe, 28.05.2003, <https://rm.coe.int/16805dfbd5>.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, C. OJ L 281 § (1995), <http://data.europa.eu/eli/dir/1995/46/oj/eng>.

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'), C. OJ L 178 § (2000), <https://eur-lex.europa.eu/eli/dir/2000/31/oj/eng>.

“Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the Coordination of Certain Provisions Laid down by Law, Regulation or Administrative Action in Member States Concerning the Provision of Audiovisual Media Services”, OJ L 95, 15.4.2010, <https://eur-lex.europa.eu/eli/dir/2010/13/oj>, (5.12.2024).

Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, <https://eur-lex.europa.eu/eli/dir/2011/93/oj>, (23.10.2024).

Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, <https://eur-lex.europa.eu/eli/dir/2017/541/oj>, (23.10.2024).

Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities (2018), <http://data.europa.eu/eli/dir/2018/1808/oj/eng>, (16.11.2024).

Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (2019), <https://eur-lex.europa.eu/eli/dir/2019/790/oj>, (23.12.2024).

“Disinformation and Freedom of Opinion And Expression. Report of the Special Rapporteur on The Promotion and Protection of The Right to Freedom of Opinion and Expression, Irene Khan (A/HRC/47/25)”, United Nations, 2021, <https://documents.un.org/doc/undoc/gen/g21/085/64/pdf/g2108564.pdf>, (20.10.2024).

“General Comment No. 16 on State obligations regarding the impact of the business sector on children’s rights (CRC/C/GC/16)”, United Nations, 2013, <https://www2.ohchr.org/english/bodies/crc/docs/crc.c.gc.16.pdf>, (1.10.2024).

“Guiding Principles on Business and Human Rights: Implementing the United Nations ‘Protect, Respect and Remedy’ Framework (HR/PUB/11/04)”, United Nations, 2011, https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf, (2.11.2024).

“Guiding Principles on Business and Human Rights: Implementing the United Nations ‘Protect, Respect and Remedy’ Framework. Report of the Special Representative of the Secretary-General on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises (A/HRC/17/31)”, United Nations, 21.03.2011, <https://digitallibrary.un.org/record/705860>, (10.10.2023).

“ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights”, European Commission, (2013), <https://op.europa.eu/en/publication-detail/-/publication/ab151420-d60a-40a7-b264-adce304e138b>, (1.10.2023).

“Illegal and harmful content on the internet. Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions. (COM (96) 487)”, European Commission, 1996, <https://aei.pitt.edu/5895/>.

“Impact Assessment Accompanying the Document Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC’ (SWD (2020) 348) Part 1/2”, 15.12.2020.

“Impact Assessment Report Annexes Accompanying the Document Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC’ (SWD(2020) 348) Part 2/2”, 15.12.2020.

“Opinion on Law No. 5651 on Regulation of Publications on the Internet and Combating Crimes Committed by Means of Such Publication (‘The Internet Law’)", Venice Commission,[https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD\(2016\)011-e](https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2016)011-e).

“Promotion and Protection of the Right to Freedom of Opinion and Expression (A/70/361)", United Nations, 08.09.2015, <https://digitallibrary.un.org/record/805706>.

“Promotion and protection of the right to freedom of opinion and expression (A/71/373)", UN, 09.09.2016, <https://documents.un.org/doc/undoc/gen/n16/278/27/pdf/n1627827.pdf>, (1.5.2021).

“Promotion and protection of the right to freedom of opinion and expression (A/73/348)", UN, 2018, <https://documents.un.org/doc/undoc/gen/n18/270/42/pdf/n1827042.pdf>, (21.10.2024).

“Promotion and protection of the right to freedom of opinion and expression (A/74/486)", UN, 2019, <https://documents.un.org/doc/undoc/gen/n19/308/13/pdf/n1930813.pdf>, (21.10.2024).

“Protect, Respect and Remedy: A Framework for Business and Human Rights. Report of the Special Representative of the Secretary-General on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises, John Ruggie (A/HRC/8/5)", United Nations, 07.04.2008, <https://digitallibrary.un.org/record/625292>, (10.7.2023).

“Protection of Minors and Human Dignity in Audiovisual and Information Services- Consultations on the Green Paper. Commission Staff Working Paper. (SEC (97) 1203)”, European Commission, 1997, <https://aei.pitt.edu/1164/>.

“Recommendation CM/Rec(2007)11 of the Committee of Ministers to member states on promoting freedom of expression and information in the new information and communications environment”, 26.09.2007, [https://search.coe.int/cm/#{%22CoEIdentifier%22:\[%2209000016805d4d0e%22\],%22sort%22:\[%22CoEValidationDate%20Descending%22\]}](https://search.coe.int/cm/#{%22CoEIdentifier%22:[%2209000016805d4d0e%22],%22sort%22:[%22CoEValidationDate%20Descending%22]}), (4.3.2022).

“Recommendation CM/Rec(2007)16 of the Committee of Ministers to member states on measures to promote the public service value of the Internet”, 07.11.2007, [https://search.coe.int/cm/#{%22CoEIdentifier%22:\[%2209000016805d4a39%22\],%22sort%22:\[%22CoEValidationDate%20Descending%22\]}](https://search.coe.int/cm/#{%22CoEIdentifier%22:[%2209000016805d4a39%22],%22sort%22:[%22CoEValidationDate%20Descending%22]}), (5.5.2022).

“Recommendation CM/Rec(2008)6 of the Committee of Ministers to Member States on Measures to Promote the Respect for Freedom of Expression and Information with Regard to Internet Filters, Adopted on 26 March 2008”, (23.10.2024), https://www.coe.int/en/web/freedom-expression/committee-of-ministers-adopted-texts/-/asset_publisher/C10Tb8ZfKDoJ/content/declaration-by-the-committee-of-ministers-on-internet-governance-principles-adopted-on-21-september-2011, (5.5.2022).

“Recommendation CM/Rec(2012)3 of the Committee of Ministers to Member States on the Protection of Human Rights with Regard to Search Engines”, 04.04.2012, https://www.coe.int/en/web/freedom-expression/committee-of-ministers-adopted-texts/-/asset_publisher/aDXmrol0vvsU/content/recommendation-cm-rec-2012-3-of-the-committee-of-ministers-to-member-states-on-the-protection-of-human-rights-with-regard-to-search-engines-adopted-by, (12.10.2023).

“Recommendation CM/Rec(2012)4 of the Committee of Ministers to Member States on the Protection of Human Rights with Regard to Social Networking Services”, 04.04.2012, https://www.coe.int/en/web/freedom-expression/committee-of-ministers-adopted-texts/-/asset_publisher/aDXmrol0vvsU/content/recommendation-cm-rec-2012-4-of-the

committee-of-ministers-to-member-states-on-the-protection-of-human-rights-with-regard-to-social-networking-service, (12.10.2023).

“Recommendation CM/Rec(2014)6 of the Committee of Ministers to Member States on a Guide to Human Rights for Internet Users”, 16.04.2014, https://www.coe.int/en/web/freedom-expression/committee-of-ministers-adopted-texts/-/asset_publisher/aDXmrol0vvsU/content/recommendation-cm-rec-2014-6-of-the-committee-of-ministers-to-member-states-on-a-guide-to-human-rights-for-internet-users-adopted-by-the-committee-of-, (1.10.2023).

“Recommendation CM/Rec(2016)3 of the Committee of Ministers to Member States”, Council of Europe, <https://edoc.coe.int/en/fundamental-freedoms/7302-human-rights-and-business-recommendation-cmrec20163-of-the-committee-of-ministers-to-member-states.html>, (23.10.2024).

“Recommendation CM/Rec(2018)2 of the Committee of Ministers to Member States on the Roles and Responsibilities of Internet Intermediaries”, Council of Europe, 07.03.2018, https://www.coe.int/en/web/freedom-expression/committee-of-ministers-adopted-texts/-/asset_publisher/aDXmrol0vvsU/content/recommendation-cm-rec-2018-2-of-the-committee-of-ministers-to-member-states-on-the-roles-and-responsibilities-of-internet-intermediaries, (10.10.2024).

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), <https://eur-lex.europa.eu/eli/reg/2016/679/oj>, (24.10.2024).

Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online, <https://eur-lex.europa.eu/eli/reg/2021/784/oj>, (23.10.2024).

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 (2022), <https://eur-lex.europa.eu/eli/reg/2022/2065/oj>, (2.5.2023).

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), <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>, (01.11.2024).

“Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (A/HRC/17/27)”, United Nations, 16.05.2011, <https://digitallibrary.un.org/record/710170>.

“Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (A/HRC/29/32)”, United Nations, <https://primarysources.brillonline.com/browse/human-rights-documents-online/promotion-and-protection-of-all-human-rights-civil-political-economic-social-and-cultural-rights-including-the-right-to-development;hrdhrd99702016149>, (22.10.2024).

“Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (A/HRC/32/38)”, United Nations, 2016, <https://digitallibrary.un.org/record/842541>, (1.05.2021).

“Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (A/HRC/38/35)”, United Nations, 2018, <https://documents.un.org/doc/undoc/gen/g18/096/72/pdf/g1809672.pdf>, (21.10.2024).

“Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective (A/HRC/38/47)”, United Nations, 18.06.2018, <https://www.ohchr.org/en/documents/thematic-reports/ahrc3847-report-special-rapporteur-violence-against-women-its-causes-and>.

“The right to privacy in the digital age Report of the Office of the United Nations High Commissioner for Human Rights (A/HRC/27/37)”, United Nations, 2014, <https://documents.un.org/doc/undoc/gen/g14/088/54/pdf/g1408854.pdf>, (3.10.2023).

“The right to privacy in the digital age (A/RES/68/167)”, United Nations General Assembly, 2014, <https://documents.un.org/doc/undoc/gen/n13/449/47/pdf/n1344947.pdf>, (20.09.2024).

“The right to privacy in the digital age Report of the United Nations High Commissioner for Human Rights (A/HRC/39/29)”, United Nations, 2018, <https://documents.un.org/doc/undoc/gen/g18/239/58/pdf/g1823958.pdf>, (4.10.2023).

“The right to privacy in the digital age. Report of the United Nations High Commissioner for Human Rights (A/HRC/48/31)”, United Nations, 2021, <https://documents.un.org/doc/undoc/gen/g21/249/21/pdf/g2124921.pdf>, (5.8.2024).

“The Rule of Law on The Internet and in The Wider Digital World: Issue Paper”, Council of Europe Publ, 2014, <https://rm.coe.int/16806da51c>, (10.08.2024).

Venedik Komisyonu ve Avrupa Konseyi, İnsan Hakları ve Hukukun Üstünlüğü Genel Müdürlüğü (DGI) Acil Ortak Görüşü, ‘Ceza Kanunu Değişiklik Tasarısı “Yanlış veya Yanıltıcı Bilgi” İle İlgili Hüküm Hakkında’, S. CDL-PI (2022)032, 2022, <https://d.barobirlik.org.tr/2022/venedikkomisyonu.pdf>, (19.10.2024).

Türk Yargı Kararları

Abdullah Kaya ve Diğerleri Başvurusu, 2016/1430, (22 Kasım 2023).

Ahmet Alphan Sabancı ve Diğerleri Başvurusu, 2015/13667 (AYM 21 Kasım 2023).

Ali Ergin Demirhan Başvurusu, 2015/16368 (AYM 11 Mart 2020).

Ali Kıdık Başvurusu, 2014/5552 (AYM 26 Ekim 2017).

Atalay Candelen ve Diğerleri Başvurusu, 2016/596 (AYM 25 Ocak 2024).

Birgün İletişim ve Yayıncılık Ticaret A.Ş., 2015/18936 (AYM [GK] 12 Temmuz 2019).

Cahit Yiğit Başvurusu, 2016/2736 (AYM 27 Kasım 2019).

Ips İletişim Vakfı (2), 2015/15873 (AYM 07 Mart 2019).

Ips İletişim Vakfı Başvurusu, 2015/14758 (AYM 30 Ekim 2018).

İ.D. ve Diğerleri Başvurusu, 2016/14513 (AYM 28 Aralık 2022).

Keskin Kalem Yayıncılık ve Ticaret A.Ş. ve Diğerleri Başvurusu, 2018/14884 (AYM [GK] 27 Ekim 2021).

Miyase İlknur ve Diğerleri Başvurusu, 2015/15242 (AYM 18 Temmuz 2018).

N.B.B. Başvurusu, 2013/5653 (AYM 03 Mart 2016).

Recep Tayyip Erdoğan Başvurusu, 2014/5376 (AYM 28 Ocak 2020).

Wikimedia Foundation Inc. ve Diğerleri, 2017/22355 (AYM [GK] 26 Aralık 2019).

2013/15828, K. 2014/9951 (Yargıtay 4. HD. 16 Haziran 2014).

E.2014/149, K.2014/151 (AYM 02 Ekim 2014).

E.2014/87, K.2015/112 (AYM 08 Aralık 2015).

E. 2015/10004, K. 2016/1023 (Yargıtay 4. HD. 27 Ocak 2016).

E.2014/92, K.2016/6 (AYM 28 Ocak 2016).

E.2015/76, K.2017/153 (AYM 15 Kasım 2017).

E. 2019/618 K.2019/8167 (Yargıtay 11. HD. 16 Aralık 2019).

E. 2019/5303, K. 2020/629 (Yargıtay 11. HD. 21 Ocak 2020).

E. 2018/307, K. 2020/149 (İstanbul 2. Fikrî ve Sınai Haklar Hukuk Mahkemesi 26 Şubat 2020).

E.2015/1192, K. 2020/1077 (Danıştay 13. D. 02 Haziran 2020).

E. 2018/566, K. 2020/388 (İstanbul 2. Fikrî Ve Sınai Haklar Hukuk Mahkemesi 12 Kasım 2020).

E. 2020/19282, K. 2020/21719 (Yargıtay 4. CD. 23 Aralık 2020).

E.2021/32, K.2021/18 (İstanbul 4. Fikrî ve Sınai Haklar Hukuk Mahkemesi 23 Kasım 2021).

E. 2020/1865 K. 2022/1740 (İstanbul BAM 16. HD. 20 Ekim 2022).

E.2020/76, K.2023/172 (AYM 11 Ocak 2023).

E.2022/129, K.2023/189 (AYM 08 Kasım 2023).

Avrupa İnsan Hakları Mahkemesi Kararları

Ahmet Yildirim v. Turkey, 3111/10 (ECtHR 18 Aralık 2012).

Akdeniz and Others v. Turkey, 20877/10 (ECtHR 11 Mart 2014).

Appleby and Others v. the United Kingdom, 61080/14 (ECtHR 06 Mayıs 2003).

August v. the United Kingdom (dec.), 32848/06 (ECtHR 21 Ocak 2003).

Axel Springer Ag v. Germany, 39954/08 (ECtHR [GC] 07 Şubat 2012).

B.B. c. France, 5335/06 (ECtHR 26 Ocak 2006).

Biancardi v. Italy, 77419/16 (ECtHR 25 Kasım 2021).

Big Brother Watch and Others v. the United Kingdom, 58170/13, 62322/14, 24960/15 (ECtHR [GC] 25 Mayıs 2021).

Breyer v. Germany, 50001/12 (ECtHR 30 Ocak 2020).

Cengiz and Others v. Turkey, 48226/10 and 14027/11 (ECtHR 01 Aralık 2015).

Delfi as v. Estonia, 64569/09 (ECtHR [GC] 16 Haziran 2015).

Dink/Türkiye, 2668/07, 6102/08, 30079/08, 7072/09, 7124/09 (ECtHR 14 Eylül 2010).

Editorial Board of Pravoye Delo and Shtekel v. Ukraine, 33014/05 (ECtHR 05 Mayıs 2011).

Editorial Board of Pravoye Delo and Shtekel v. Ukraine, 33014/05 (ECtHR 05 Mayıs 2011).

Editorial Board of Pravoye Delo and Shtekel v. Ukraine, 33014/05 (ECtHR 05 Mayıs 2011).

Fadeyeva v. Russia, 4856/03, 69889/01, 23697/02, 69315/01, 72701/01 (ECtHR 09 Haziran 2005).

Fuchsmann v. Germany, 71233/13 (ECtHR 19 Ekim 2017).

Gaši and Others v. Serbia, 24738/19 (ECtHR 06 Eylül 2022).

Gaskin v. The United Kingdom, 10454/83 (ECtHR 07 Temmuz 1989).

Gaughran v. the United Kingdom, 45245/15 (ECtHR 13 Şubat 2020).

Gaughran v. the United Kingdom, 45245/15 (ECtHR 13 Şubat 2020).

Handyside v. the United Kingdom, 57499/17, 74536/17, 80215/17, 9323/18, 16128/18, 25920/18 (ECtHR 07 Aralık 1976).

Høiness v. Norway (ECtHR 19 Mart 2019).

Hurbain v. Belgium, 57292/16 (ECtHR [GC] 04 Temmuz 2023).

Jersild v. Denmark, 57891/17 (ECtHR [GC] 23 Eylül 1994).

Khelili c. Suisse, 16188/07 (ECtHR 18 Ekim 2011).

K.U. v. Finland, 2872/02 (ECtHR 02 Aralık 2008).

Leander v. Sweden, 9248/81 (ECtHR 26 Mart 1987).

L.h. v. Latvia, 52019/07 (ECtHR 29 Nisan 2014).

López Ostra v. Spain, 39666/16, 27733/21, 57905/21 (ECtHR 09 Aralık 1994).

Magyar Jeti Zrt v. Hungary, 11257/16 (ECtHR 04 Aralık 2018).

Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary, 22947/13 (ECtHR 02 Şubat 2016).

Marckx v. Belgium, 62980/10, 57534/16, 60594/16, 61095/16, 65741/16, 1023/17, 1996/17 (ECtHR 13 Haziran 1979).

Mediengruppe Österreich GmbH v. Austria, 37713/18 (ECtHR 26 Nisan 2022).

M.L. and W.W. v. Germany, 60798/10, 65599/10 (ECtHR 28 Haziran 2018).

Mosley v. the United Kingdom, 48009/08 (ECtHR 10 Mayıs 2011).

Neij and Sunde Kolmisoppi v. Sweden, 40397/12 (ECtHR 19 Şubat 2013).

OOO Flavus and Others v. Russia, 12468/15, 23489/15 (ECtHR 23 Haziran 2020).

Ooo Zhivaya Fotografiya v. Russia (communicated), 48932/19 (ECtHR 15 Haziran 2020).

Ozgur Gundem v. Turkey, 23144/93 (ECtHR 16 Mart 2000).

Österreichischer Rundfunk v. Austria, 35841/02 (ECtHR 07 Aralık 2006).

Palomo Sánchez and Others v. Spain, 28955/06, 28957/06, 28959/06, and 28964/06 (23.10.2024).

Panteleyenko v. Ukraine, 11901/02 (ECtHR 29 Haziran 2006).

Peck v. the United Kingdom, 60898/00 (ECtHR 28 Ocak 2003).

Pihl v. Sweden, 74742/14 (ECtHR 07 Şubat 2017).

Private Networks Lp v. Russia (communicated), 4945/20 (ECtHR 01 Eylül 2020).

Roman Zakharov v. Russia, 47143/06 (ECtHR [GC] 04 Aralık 2015).

S. and Marper v. the United Kingdom, 30562/04, 30566/04 (ECtHR [GC] 04 Aralık 2008).

Sanchez v. France, 45581/15 (ECtHR [GC] 15 Mayıs 2023).

Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland, 931/13 (ECtHR [GC] 27 Haziran 2017).

Shimovolos v. Russia, 30194/09 (ECtHR 21 Haziran 2011).

Skalka v. Poland, 3019/04 (ECtHR 27 Mayıs 2003).

Sõro v. Estonia, 22588/08 (ECtHR 03 Eylül 2015).

Standard Verlagsgesellschaft MbH v. Austria (no. 3), 39378/15 (ECtHR 07 Aralık 2021).

Stoll v. Switzerland, 69698/01 (ECtHR [GC] 10 Aralık 2007).

Sürek v. Turkey (no. 1), 26682/95 (ECtHR [GC] 08 Temmuz 1999).

Tamiz v. the United Kingdom (dec.), 3877/14 (ECtHR 19 Eylül 2017).

Taylor-Sabori v. the United Kingdom (dec.), 11782/85 (ECtHR 29 Mayıs 2001).

Telegram Messenger Llp and Telegram Messenger Inc. v. Russia (communicated), 13232/18 (ECtHR 29 Ekim 2020).

Times Newspapers Ltd v. the United Kingdom, 3002/03, 23676/03 (ECtHR 10 Mart 2009).

Uzun v. Germany, 35623/05 (ECtHR 02 Eylül 2010).

Valenzuela Contreras v. Spain, 34724/14, 58208/14, 21969/15, 23735/16, 23740/16, 65993/16, 14118/17 (ECtHR 30 Temmuz 1998).

Verein Gegen Tierfabriken Schweiz (vgt) v. Switzerland (no. 2), 32772/02 (ECtHR [GC] 30 Haziran 2009).

Vgt Verein Gegen Tierfabriken v. Switzerland, 24699/94 (ECtHR 28 Haziran 2001).

Vladimir Kharitonov v. Russia, 10795/14 (ECtHR 23 Haziran 2020).

Von Hannover v. Germany (no. 2), 40660/08, 60641/08 (ECtHR [GC] 07 Şubat 2012).

Węgrzynowski and Smolczewski v. Poland, 33846/07 (ECtHR 16 Temmuz 2013).

X and Y v. the Netherlands, 8978/80 (ECtHR 26 Mart 1985).

Zöchling v. Austria, 4222/18 (ECtHR 05 Eylül 2023).

Avrupa Birliği Adalet Divanı Kararları

Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV, Case C-360/10 (ECJ 16 Şubat 2012).

Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, Case C-311/18 (ECJ 16 Temmuz 2020).

Eva Glawischnig-Piesczek v Facebook Ireland Limited, Case C-18/18 (ECJ 03 Ekim 2019).

Frank Peterson v Google LLC and Others and Elsevier Incv Cyando AG, Joined Cases C-682/18 and C-683/18 (ECJ 22 Haziran 2021).

GC and Others v Commission nationale de l'informatique et des libertés (CNIL), Case C-136/17 (ECJ 24 Eylül 2019).

Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, Case C-131/12 (ECJ 13 Mayıs 2014).

Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, Case C-131/12 (ECJ 13 Mayıs 2014).

L'Oréal SA and Others v eBay International AG and Others, Case C-324/09 (ECJ 12 Temmuz 2011).

Maximillian Schrems v Data Protection Commissioner, Case C-362/14 (ECJ 06 Ekim 2015).

McFadden v. Sony Music, C-484/14 (ECJ 15 Eylül 2016).

Opinion of Advocate General Saugmandsgaard Øe delivered on 15 July 2021. Republic of Poland v European Parliament and Council of the European Union., Case C-401/19 (ECJ 2019).

Opinion of Advocate General Saugmandsgaard Øe delivered on 16 July 2020. Frank Peterson v Google LLC and Others and Elsevier Inc.v Cyando AG. (ECJ 2018).

Republic of Poland v European Parliament and Council of the European Union, Case C-5/16 (ECJ 21 Haziran 2018).

Republic of Poland v European Parliament and Council of the European Union, Case C-401/19 (ECJ 26 Nisan 2022).

Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), Case C-70/10 (ECJ 24 Kasım 2011).

TU and RE v Google LLC, Case C-460/20 (ECJ 08 Aralık 2022).

UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH and Wega Filmproduktionsgesellschaft mbH, Case C-314/12 (ECJ 27 Mart 2014).