Dr. Mehmet Bedii KAYA

İNTERNET HUKUKU

2. Baskı

onikilevha

İÇİNDEKİLER

İKİNCİ BASKIYA ÖNSÖZ VII

ÖNSÖZ IX

İÇİNDEKİLER XIII

KISALTMALAR XXV

§1. GİRİŞ VE KONUNUN TAKDİMİ 1

BİRİNCİ KISIM
TEMEL KAVRAMLAR

§2. İNTERNET 6

I. İnternetin gelişim süreci 6

II. Çalışma prensipleri 11

III. Temel kavramlar 13

A. Ağ (Network) 13

B. IP adresi (Internet Protocol) 15

C. DNS (Domain Name System) 18

D. URL (Uniform Resource Locator) 20

E. MAC adresi 21

F. Bulut bilişim (Cloud Computing) 22

G. Web 2.0 24

H. İçerik dağıtım ağı (CDN - Content Delivery Network) 25

I. Ağ tarafsızlığı (Network Neutrality) 25
IV. İnternetin kullanım alanları 31

İKİNCİ KISIM
İNTERNETİN ULUSLARARASI YÖNETİŞİMİ

§3. İNTERNETİN ULUSLARARASI YÖNETİŞİMİ 36
I. Internet Corporation for Assigned Names and Numbers (ICANN) 36
II. Internet Assigned Numbers Authority (IANA) 39
III. Internet Engineering Task Force (IETF) 40
IV. Internet Research Task Force (IRTF) 42
V. Internet Architecture Board (IAB) 43
VI. Internet Governance Forum (IGF) 44
VII. International Organization for Standardization (ISO) 48
VIII. Internet Society (ISOC) 48
IX. World Wide Web Consortium (W3C) 49
X. Internet Network Operators' Groups 50
XI. İnternet yönetişiminin geleceği 50
XII. İnternette yerelleşme mi, fragmantasyon mu? 56

ÜÇÜNCÜ KISIM
ERİŞİMİ ENGELLEME VE FİLTRELEME

§4. İNTERNETE ERİŞİMİN ENGELLENMESİ VE İNTERNETİN FİLTRELENMESİ 60
I. Engellemenin coğrafi kapsamına göre 62
A. Ülkesel engelleme 62
B. Bölgesel engelleme 63
II. Engellemenin ağ kapsamına göre 63
A. İnternet omurgası temelli engelleme 63

B. İSS temelli engelleme 64
C. Kurumsal engelleme 65
D. Platform temelli engelleme 66
E. Bireysel engelleme 68
F. Cihaz temelli engelleme 69
III. Engelleme sürecine göre 69
A. Doğrudan engelleme 69
B. Uyar-kaldır yöntemiyle engelleme 70
IV. Engelleme süresine göre 71
A. Geçici engelleme 71
B. Kalıcı engelleme 72
V. Engelleme sistemine göre 73
A. Otomatik engelleme 73
B. Bireysel engelleme 74
VI. Engellemenin kaynağına göre 75
A. Kullanıcı nezdinde engelleme 75
B. Hizmet sağlayıcı nezdinde engelleme 75
VII. Engellemenin hedef içeriğinin türüne göre 75
A. Statik engelleme 75
B. Dinamik engelleme 75
VIII. Engelleme kararının alınış zamanına göre 76
A. İhlal sonrası engelleme 76
B. İhlal öncesi engelleme 76
IX. Engellemenin genel niteliğine göre 77
A. Kamusal engelleme 77
B. Özel engelleme 78
X. Kullanılan tekniğe göre 78
A. IP engellemesi 79
B. DNS engellemesi 80
C. URL engellemesi 82
D. Port engellemesi 83
E. Proxy engellemesi 84
F. İçerik engellemesi 84

G. Siber saldırı yöntemiyle engelleme 86
H. Alan adına el koyma veya alan adını terkin yöntemi 88
I. Bulut bilişim engellemesi 89
J. Fiziksel sunucu müdahalesi 89
K. Ağ hataları 90
L. Bağlantı yavaşlatma 90
M. Sosyal teknikler 91
XI. Değerlendirme 93

§5. İÇERİK FİLTRELEME VE ENGELLEME YÖNTEMLERİNİ AŞMA YOLLARI 94
I. Yöntem ve teknikler 94
A. IP değişikliği 94
B. DNS değişikliği 95
C. Alan adı değişikliği 97
D. URL değişikliği 97
E. VPN ve diğer trafik aktarma yöntemleri 98
F. Uzak masaüstü bağlantısı 98
G. Online çeviri sistemleri 99
H. Önbellek kullanımı 99
I. Kopya içerik kullanımı 100
J. İçerik aldatması 100
II. Değerlendirme 101

DÖRDÜNCÜ KISIM
AVRUPA KONSEYİ VE İNTERNET

§6. AVRUPA KONSEYİ 108
I. İnternette Özel Hayatın Korunmasına İlişkin Tavsiye Kararı (1999) ..108
II. Arşiv Erişimine Yönelik Bir Avrupa Politikası Hakkında Tavsiye Kararı (2000) 111
III. Siber İçeriğin Öz Düzenlemesine İlişkin Tavsiye Kararı (2001) 115
IV. İnternette İletişim Özgürlüğüne İlişkin Deklarasyon (2003) 119

V. Bilgi Toplumunda İnsan Hakları ve Hukukun Üstünlüğü Deklarasyonu (2005) 127
VI. Yeni Bilgi ve İletişim Ortamında Çocukların Güçlendirilmesi Tavsiye Kararı (2006) 131
VII. Yeni Bilgi ve İletişim Ortamında İfade ve Bilgi Özgürlüğünün Geliştirilmesine İlişkin Tavsiye Kararı (2007) 132
VIII. İnternetin Kamu Hizmeti Boyutunun Geliştirilmesine Yönelik Önlemlere İlişkin Tavsiye Kararı (2007) 132
IX. İnternet Filtreleri Bağlamında İfade ve Bilgi Özgürlüğüne Saygının Teşvik Edilmesine Yönelik Tedbirleri İçeren Tavsiye Kararı (2008) 133
X. İnternet Ortamında Çocukların İtibar, Güvenlik ve Mahremiyetlerinin Korunmasına İlişkin Deklarasyon (2008) ..136
XI. Çocukları Zararlı İçeriğe ve Davranışlara Karşı Koruma ve Çocukların Yeni Bilgi ve İletişim Ortamına Aktif Katılımlarını Yaygınlaştırmaya İlişkin Tavsiye Kararı (2009) ...138
XII. Ağ Tarafsızlığı Deklarasyonu (2010) 141
XIII. İnternet Protokol Adres Kaynaklarının Kamu Yararına Uygun Yönetimine İlişkin Deklarasyon (2010) 143
XIV. Alan Adları ve İsim Dizeleri Bağlamında İfade ve Bilgi Özgürlüğü ile Toplantı ve Örgütlenme Özgürlüğünün Korunmasına İlişkin Deklarasyon (2011) 145
XV. İnternet Yönetişimi İlkeleri Deklarasyonu (2011) 146
XVI. Yeni Bir Medya Nosyonuna İlişkin Tavsiye Kararı (2011) 150
XVII. İnternetin Evrenselliğini, Bütünlüğünü ve Açıklığını Koruma ve Geliştirmeye İlişkin Tavsiye Kararı (2011) 151
XVIII. Özel Olarak İşletilen İnternet Platformları ve Online Hizmet Sağlayıcıları Bağlamında İfade Özgürlüğü ile Toplantı ve Örgütlenme Özgürlüğünün Korunması Deklarasyonu (2011) ...155
XIX. Arama Motorları Bağlamında İnsan Haklarının Korunmasına İlişkin Tavsiye Kararı (2012) 157
XX. Sosyal Ağ Hizmetleri Bağlamında İnsan Haklarının Korunmasına İlişkin Tavsiye Kararı (2012) 167
XXI. İnternet Kullanıcıları İçin İnsan Hakları Rehberi (2014) 169
XXII. Bilginin İnternet Ortamında Sınır Ötesine Serbestçe Akışına İlişkin Tavsiye Kararı (2015) 178

XXIII. Ağ Tarafsızlığı Bağlamında İfade Özgürlüğü Hakkı ile Özel Hayat Hakkının Korunması ve Geliştirilmesine İlişkin Tavsiye Kararı (2016) 182
XXIV. İnternet Özgürlüğüne İlişkin Tavsiye Kararı (2016) 186
XXV. İnternet Aracı Platformlarının Rolleri ve Sorumluluklarına İlişkin Tavsiye Kararı (2018) 197

BEŞİNCİ KISIM
AVRUPA İNSAN HAKLARI MAHKEMESİ VE İNTERNET

§7. AVRUPA İNSAN HAKLARI MAHKEMESİNİN İNTERNET HUKUKUNA İLİŞKİN KARARLARI 206

§8. AHMET YILDIRIM V. TÜRKİYE 209
I. Davanın gelişimi 209
II. Hukuki arka plan 211
III. AİHM'nin tespit ve değerlendirmeleri 216
IV. Yargıç Paulo Pinto de Albuquerque'nin mutabık görüşü 219
V. Değerlendirme 221

§9. AKDENİZ V. TÜRKİYE 224
I. Kararın detaylı incelemesi 224
II. Değerlendirme 228

§10. CENGİZ VE DİĞERLERİ V. TÜRKİYE 230
I. Davanın gelişimi 230
II. Hukuki arka plan 232
III. Tarafların iddiaları 233
IV. AİHM'nin tespit ve değerlendirmeleri 235
A. Kabul edilebilirliğe yönelik tespit ve değerlendirmeler 235
B. Müdahalenin haklılığına ilişkin tespit ve değerlendirmeler 238
V. Yargıç Paul Lemmens'in mutabık görüşü 239
VI. Değerlendirme 240

§11. DELFİ AS V. ESTONYA 243
I. Davanın gelişimi 244
A. Harju İlk Derece Mahkemesinde tazminat davasına ilişkin ilk inceleme 246
B. Harju İlk Derece Mahkemesinde tazminat davasına ilişkin ikinci inceleme 247
C. Tallinn İstinaf Mahkemesinin kararı 248
D. Estonya Yüksek Mahkemesinin kararı 248
E. Hükmün Delfi AS şirketi tarafından yerine getirilmesi ve şirketin iş modelindeki değişiklikler 250
II. Hukuki arka plan 251
III. AİHM Birinci Dairenin kararı 252
IV. Delfi AS şirketinin iddiaları 252
V. Estonya Hükûmetinin savunması 253
VI. Müdahil üçüncü tarafların görüşleri 253
VII. AİHM'nin tespit ve değerlendirmeleri 255
A. Kanunilik 256
B. Meşru amaç 257
C. Demokratik bir toplumda gereklilik 257
VIII. Yargıçlar Raimondi, Karakaş, De Gaetano ve Kjølbro'nun müşterek mutabık görüşü 262
IX. Yargıç Boštjan Zupančič'in mutabık görüşü 264
X. Yargıçlar Sajó ve Tsotsoria'nın müşterek muhalif görüşü 265
XI. Değerlendirme 270

§12. KALDA V. ESTONYA 274
I. Davanın gelişimi 274
II. Hukuki arka plan 276
III. Tarafların iddiaları 277
IV. AİHM'nin tespit ve değerlendirmeleri 279
V. Yargıç Jon Fridrik Kjølbro'nun muhalif görüşü 280
VI. Değerlendirme 283

§13. MTE VE INDEX.HU ZRT V. MACARİSTAN 285

I. Davanın gelişimi 285
II. Hukuki arka plan 289
III. Tarafların iddiaları 289
IV. Macaristan Hükûmetinin savunması 291
V. AİHM'nin tespit ve değerlendirmeleri 291
A. Kanunla öngörülme açısından inceleme 291
B. Demokratik toplum düzeninin gerekliliklerine uygunluk 293
C. Genel tespitler ve uygulanabilir kriter 293
1. İhtilafa konu yorumların içerik ve bağlamı 296
2. Yorumların asıl yazarlarının sorumluluğu 296
3. Başvurucular tarafından alınan tedbirler ve mağdur tarafın tutumu 297
4. Yorumların mağdur taraf üzerindeki sonuçları 298
5. Başvurucular üzerindeki neticeler 298
D. Sonuç 299
VI. Yargıç Egidijus Kūris'in mutabık görüşü 300
VII. Değerlendirme 301

§14. JANKOVSKİS V. LİTVANYA 304
I. Davanın gelişimi 304
II. Hukuki arka plan 307
III. Tarafların iddiaları 307
IV. Litvanya Hükûmetinin savunması 308
V. AİHM'nin tespit ve değerlendirmeleri 309
A. Kanunla öngörülme açısından inceleme 310
B. Müdahalenin meşru amaç için gerçekleştirilip gerçekleştirilmediği 310
C. Demokratik toplum düzeninin gerekliliklerine uygunluk 310
VI. Değerlendirme 312

§15. ROLF ANDERS DANİEL PİHL V. İSVEÇ 314
I. Davanın gelişimi 314
II. Hukuki arka plan 315

III. AİHM'nin tespit ve değerlendirmeleri 316
IV. Değerlendirme 319

§16. TAMİZ V. BİRLEŞİK KRALLIK 321
I. Davanın gelişimi 321
II. Yerel yargılama süreci 324
III. Hukuki arka plan 327
IV. Tarafların iddiaları 328
A. Birleşik Krallık Hükûmetinin görüşleri 328
B. Başvurucunun iddiaları 329
C. Müdahil üçüncü tarafların görüşleri 330
1. Google Inc. 330
2. Media Legal Defence Initiative (MLDI) 331
3. Article 19 332
V. AİHM'nin tespit ve değerlendirmeleri 332
VI. Değerlendirme 335

§17. M.L. VE W.W. V. ALMANYA 337
I. Davanın gelişimi 337
A. Birinci talep ve yargılama 338
B. İkinci talep ve yargılama 343
C. Üçüncü talep ve yargılama 345
D. Diğer talepler 346
II. Hukuki arka plan 346
III. Tarafların iddiaları 346
IV. Alman Hükûmetinin savunması 348
V. AİHM'nin tespit ve değerlendirmeleri 349
A. Genel olarak 349
B. Kriterlerin somut uyuşmazlığa uygulanması 352
C. Kamu yararını ilgilendiren bir tartışmaya katkı 352
D. İlgili kişinin bilinirliğinin derecesi ve raporun konusu 354
E. İlgili kişinin medyaya yönelik önceki davranışları 355
F. Yayının içeriği, şekli ve sonuçları 355

G. Fotoğrafların hangi koşullarda alındığı 356
H. Sonuç....356
VI. Değerlendirme 357

§18. MAGYAR JETİ ZRT V. MACARİSTAN....361
I. Davanın gelişimi....361
II. Hukuki arka plan....365
III. Tarafların iddiaları 365
IV. Macar Hükûmetinin savunması 367
V. Müdahil tarafların görüşleri 369
VI. AİHM'nin tespit ve değerlendirmeleri 372
A. Bir müdahale olup olmadığı....372
B. Kanunilik....372
C. Meşru amaç....373
D. Demokratik toplum düzeninin gerekliliği....374
E. Yargıç Paulo Pinto de Albuquerque'nin mutabık görüşü.... 380
VII. Değerlendirme 384

§19. HØINESS V. NORVEÇ 386
I. Davanın gelişimi.... 386
II. Hukuki arka plan....391
III. Başvurucunun iddiaları....391
IV. Norveç Hükûmetinin savunması 392
V. AİHM'nin tespit ve değerlendirmeleri....393
VI. Değerlendirme 395

§20. KABLİS V. RUSYA 396
I. Davanın gelişimi....396
II. Hukuki arka plan....399
III. Tarafların iddiaları 401
IV. AİHM'nin tespit ve değerlendirmeleri.... 403
V. Değerlendirme 408

§21. BULGAKOV V. RUSYA 410

I. Davanın gelişimi 410
II. Hukuki arka plan 411
III. Tarafların iddiaları 413
IV. Rus Hükûmetinin savunması 413
V. Başvurucunun iddiaları 414
VI. Müdahil tarafların görüşleri 415
VII. AİHM'nin tespit ve değerlendirmeleri 416
VIII. Yargıçlar Lemmens, Dedov ve Poláčková'nın mutabık görüşü 422
IX. Değerlendirme 423

§22. ENGELS V. RUSYA 426
I. Davanın gelişimi 426
II. Hukuki arka plan 427
III. Tarafların iddiaları 430
IV. Rus Hükûmetinin savunması 430
V. Başvurucunun iddiaları 431
VI. Müdahil tarafların görüşleri 432
VII. AİHM'nin tespit ve değerlendirmeleri 433
VIII. Değerlendirme 440

§23. OOO FLAVUS VE DİĞERLERİ V. RUSYA 443
I. Davanın gelişimi 443
II. Hukuki arka plan 445
III. Tarafların iddiaları 448
IV. Rus Hükûmetinin savunması 448
V. Başvuruculaın iddiaları 449
VI. Müdahil tarafların görüşleri 450
VII. AİHM'nin tespit ve değerlendirmeleri 451
VIII. Değerlendirme 460

§24. VLADİMİR KHARİTONOV V. RUSYA 461
I. Davanın gelişimi 461
II. Hukuki arka plan 463
III. Tarafların iddiaları 466

IV. Başvurucunun iddiaları 466
V. Rus Hükûmetinin savunması 468
VI. Müdahil tarafların görüşleri 470
VII. AİHM'nin tespit ve değerlendirmeleri 472
VIII. Yargıçlar Lemmens, Dedov ve Poláčková'nın mutabık görüşü 480
IX. Değerlendirme 484

ALTINCI KISIM
DEĞERLENDİRMELER

§25. AİHM KARARLARI IŞIĞINDA İNTERNET ORTAMININ DÜZENLENMESİ 488
I. Avrupa Konseyi ve internet 488
II. AİHM ve internet 498
III. İdeal bir internet yasası nasıl olmalıdır? 506

§26. SONUÇ 514

KAYNAKÇA 519

KAVRAM DİZİNİ 537

KISALTMALAR

AB	:	Avrupa Birliği
ABAD	:	Avrupa Birliği Adalet Divanı
ABD	:	Amerika Birleşik Devletleri
AİHS	:	Avrupa İnsan Hakları Sözleşmesi
BTK	:	Bilgi Teknolojileri ve İletişim Kurumu
DARPA	:	US Defence Information Systems Agency
DNS	:	Domain Name System
DPI	:	Deep Packet Inspection
DRM	:	Digital Rights Managament
HTTP	:	Hyper Text Transfer Protocol
HTTPS	:	Secure Hyper Text Transfer Protocol
IAB	:	Internet Architecture Board
IANA	:	Internet Assigned Numbers Authority
ICANN	:	Internet Corporation for Assigned Names and Numbers
IGF	:	Internet Governance Forum
IoT	:	Internet of Things
IP	:	Internet Protocol
IRTF	:	Internet Research Task Force
ISO	:	International Organization for Standardization
ISOC	:	Internet Society

İSS	:	İnternet Servis Sağlayıcısı
IXP	:	Internet Exchange Point
LIR	:	Local Internet Registry
MAC	:	Media Access Control
NASA	:	The National Aeronautics and Space Administration
NIST	:	National Institute of Standards and Technology
NTIA	:	National Telecommunications and Information Administration
para.	:	paragraf
POP	:	Point of Presence
RFC	:	Request for Comments
RG	:	Resmî Gazete
RIR	:	Regional Internet Registry
RTÜK	:	Radyo ve Televizyon Üst Kurulu
s.e.t.	:	Son Erişim Tarihi
SMTP	:	Simple Mail Transfer Protocol
SSL	:	Secure Sockets Layer
TBMM	:	Türkiye Büyük Millet Meclisi
TCP	:	Transmission Control Protocol
TİB	:	Telekomünikasyon İletişim Başkanlığı
URL	:	Uniform Resource Locator
VOIP	:	Voice Over Internet Protocol
W3C	:	World Wide Web Consortium

§1. GİRİŞ VE KONUNUN TAKDİMİ

İnternet, küresel bir bilgiye erişim ve iletişim ağıdır. İnternet, en yalın tanımıyla, aynı dili konuşan bilişim sistemlerinin küresel ağıdır.[1] Konuşulan dilin teknik adı protokoldür. TCP/IP isimli protokol vasıtasıyla ağ üzerinde iletişim kurulmakta ve bilgi, ağda dolaşıma girmektedir.

İnternet; güvenlik değil güven ilkesi üzerine inşa edilmiş, sürekli iletişim ve birlikte çalışabilirlik (*inter-operability*) yaklaşımı ile geliştirilmiştir. İnternetin gelişimi bilim ve ulusal güvenliğin evliliği olarak betimlenmektedir.[2] Benzer şekilde, internetin gelişim hikâyesi merkezin ölümü, ağın politik ve ticari yükselişi olarak da ifade edilmektedir.[3]

İnternet ağı her geçen gün büyümekte; sosyal, ekonomik, kültürel, siyasi veya ticari amaçlarla kullanılmaktadır. Mobil cihazlar sayesinde artık neredeyse her yerde ağa erişmek mümkündür. Veri barındırma maliyetinin nispeten düşmesi ve yeni nesil sosyal ağ platformları sayesinde sınıflandırılması neredeyse mümkün olmayan çeşitlilik ve boyuttaki içerik internet ortamında barındırılabilir hâle gelmiştir. Bu içerikler, önceden belirlenmemiş güzergâhlarla ağda dolaşıma girmekte ve ülkelerin sınırlarını saniyeler içinde aşmaktadır. Bunların neticesinde internetin kontrolü ve internet ortamındaki içerikten sorumluluğun nasıl olacağı güncel bir sorun hâline gelmiştir.

İnternetin düzenlenmesi hem ulusal hem de uluslararası hukukun en güncel meselesidir. Algılama ve belirsizlik döneminde gerçekleştirilen katı regülasyon dalgaları, bir dönem yerini daha serbest bir deregülasyon yaklaşımına bırakmıştır. Ağların büyümesi ve hayatın her alanının

---

1 **Lambert, Paul** (2018) *Gringras: The Laws of the Internet*, Haywards Heath, Bloomsbury Professional, s. 1.

2 **Sherry, John/Brown, Colleen** (2004) "*History of the Internet*": Bidgoli, Hossein (Editör) *The Internet Encyclopedia - Volume 2*, Hoboken New Jersey, John Wiley & Sons, s. 114.

3 **Ryan, Johnny** (2010) *A history of the Internet and the digital future*, London, Reaktion Books, s. 7.

en temel bileşeni hâline gelmesiyle tüm dünyada yeni bir *re-regülasyon* dönemine girildiğinin işaretleri doğudan batıya, güneyden kuzeye tüm dünyada gözlemlenmektedir.

Re-regülasyon dalgasının en temel kırılma noktaları; terörizmle, radikalleşme ve aşırıcılıkla mücadele, seçim güvenliğinin sağlanması, dezenformasyon, nefret söylemi, şiddete teşvik ve çocuk pornografisiyle mücadele, dolandırıcılığın önlenmesi, fikrî mülkiyet haklarının korunması, kamu sağlığının ve genel olarak da kamu düzeninin korunması gibi alanlardır. Özellikle sosyal medya şirketleri gibi platformların ciddi bir ekonomik değere ulaşması, toplumsal tartışmaları yönlendirmeye başlaması ve hatta klasik medyanın önüne geçmesi devletlerin bu alanı düzenlemeye yönelik iştahını artırmıştır.

İnternetin kullanım alanlarının yaygınlaşması ve kullanım oranlarının artmasıyla birlikte devletlerin internete müdahaleleri de artmıştır. Başlangıçta suçla mücadele amacıyla internete müdahale eden devletler, zamanla kendi ideolojilerine göre internet içeriğini düzenlemeye ve istenmeyen içeriği filtrelemeye yahut bunlara erişimi engellemeye başlamıştır.

Her devlet, istenmeyen içeriğe erişimi engellemek için farklı yöntem ve teknikler kullanmaktadır. Bazı devletler tek bir yöntem kullanırken bazıları birden çok yöntemi aynı anda kullanmakta ve hatta bazı otoriter devletler hukuk dışı yöntemlere başvurabilmektedir. Özellikle devletlerin demokrasi ve insan hakları konularındaki yaklaşımları engelleme sürecinin saydamlığını, hesap verilebilirliği, etkin koruma mekanizmalarının işlerliğini doğrudan etkilemektedir.

İnternetin kontrolü, bir yanıyla da uluslararası hukukla bağlantılı bir konudur. Bir devletin uyguladığı engelleme ve filtreleme yöntemleri sebebiyle, sınır aşan veri akışına halel gelebilmektedir. Yine, bir devletin sınırları içerisinde yer alan ve yurt dışına yayın yapan bir platforma uygulanan kısıtlama, başka devletlerdeki bireylerin ifade özgürlükleri ile diğer bazı temel hak ve özgürlüklerini zedeleyebilmektedir. Özellikle trafik yönetimi amacıyla altyapıda uygulanan kuralların şeffaflığı bu sebeple önem taşımaktadır. Mesele, sınır aşan nehirlerin uluslararası hukuktaki durumuna benzetilebilir.

İnternetin teknik kontrolü, bünyesinde muhtelif yapısal sorunlar barındıran bir meseledir. Şifreleme teknolojilerinin yaygınlaşması, yerelleşme, ağların fragmantasyonu, içeriğin kontrolü için çok büyük ölçekte verinin işlenmesi gerekliliği ağ izleme teknolojilerinin yetersiz kalmasına sebep olmaktadır. Aşırı engelleme veya hiç engellememenin, diğer bir deyişle hatalı pozitif (*false positive*) ve hatalı negatif (*false negative*) durumların ortaya çıkması kaçınılmaz olmaktadır.

İnternet hukukunun bir diğer temel sorunu, içeriğin sınıflandırılmasıdır. İnternet ortamında her türlü içerik kendisine yer bulabilmektedir. Genel olarak hukuka aykırı içerik ve zararlı içerik şeklinde ikili bir ayrım yapılsa da bu ayrım, hukuk düzenlerinin farklılığı ve bu alandaki bağlayıcı uluslararası düzenlemelerin sınırlı sayıda olması sebebiyle yetersiz kalmaktadır.

Benzer bir sorun, internet ortamındaki içeriklerden sorumlulukta da gözlemlenmektedir. Bir hukuk düzeninin ifade özgürlüğü sınırları içinde gördüğü bir içeriğin başka bir hukuk düzeninde hukuka aykırı içerik kategorisinde değerlendirilmesi pekâlâ mümkündür. Müstehcenliğin tanımından terörizmin tanımına kadar geniş bir yelpazede rastlanan bu tür tanım farklılıklarıyla platformların hukuki tanımlamasında da karşılaşılmaktadır. Bazen platformdaki içerikler doğrudan platformla özdeşleştirilip içerik sahibi ile platform sahibi aynı sorumluluk rejimine tabi tutulmakta, bazen de içerik sahibi ve platform sahibi özel kurallar vasıtasıyla müstakil sorumluluk rejimlerine tabi kılınmaktadır.

Platformlar için genel kabul gören güvenli liman yaklaşımı da özellikle nefret söylemi ile mücadele, şiddete teşvik çağrılarının önlenmesi ve dezenformasyonla mücadele gibi sebeplerle farklı şekilde uygulanmaya başlamıştır. Yer sağlayıcı konumundaki platformların, barındırdıkları üçüncü kişilere ait içeriklerden veya haber sitelerinin, kullanıcı yorumlarından sorumsuzluğunun istisnaları her geçen gün artmaktadır. Özellikle, insan hakları alanındaki içtihatlarda da ana kuraldan sapma çarpıcı şekilde gözlemlenmektedir. Keza, küresel pandemiler gibi olağanüstü dönemlerde tüm kurallar ters yüz edilebilmekte veya askıya alınabilmektedir.

İnternet hukuku, dinamik bir alandır; yeni gelişen teknolojiler ve ortaya çıkan sorunlarla yeni biçimler almaktadır. Bu alan özellikle yargı içtihat-

larıyla şekillenmektedir. Algılama ve belirsizlik döneminin geride kaldığı, artık daha somut ve spesifik sorunlara ilişkin detaylı kuralların var olduğu bir noktaya gelinmiştir. Bazen bağlayıcı hukuk kuralları bazen yumuşak hukuk kuralları bu alanın düzenlenmesinde belirleyici olabilmektedir.

Bu çalışmanın amacı, internet hukuku alanına ilişkin güncel sorunları insan hakları hukuku ekseninde incelemektir. Çalışma, özellikle internete, internet ortamındaki içeriğe erişimin engellenmesi, içeriğin kaldırılması, internet ortamında kişilik haklarının korunması, internet platformlarının hukuki sorumluluğu, unutulma hakkı, üçüncü kişilere ait internet içeriğinden sorumluluk, üçüncü kişilere ait internet bağlantılarından sorumluluk meselelerini etraflıca ele almaktadır. İnternetin teknik işleyişine ve uluslararası yönetişimine kapsamlı şekilde yer veren bu çalışmada Avrupa Konseyinin internete ilişkin tüm deklarasyonları ve tavsiye kararları ile AİHM'nin internetle ilgili tüm kararları incelenmekte, ideal bir internet düzenlemesinin nasıl olması gerektiği sorusunun yanıtı bulunmaya çalışılmaktadır.

Çalışma şu şekilde yapılandırılmıştır: **İlk bölüm** olan bu bölümde çalışmanın kapsamı ve çerçevesi hakkında bilgi verilmiştir. **İkinci bölümde** internet, internetin gelişim süreci, çalışma prensipleri ve temel kullanım alanları incelenmiştir. **Üçüncü bölümde** internetin uluslararası yönetişimi ve bu yönetişimin teknik, politik ve hukuki olarak sorumlu kuruluşları ele alınmıştır. **Dördüncü bölümde** internete erişimin engellenmesi ve internetin filtrelenmesi konusuna yer verilirken müteakip **beşinci bölümde** bu engelleme yöntem ve tekniklerini aşma yolları değerlendirilmiştir. Çalışmanın **altıncı bölümü** Avrupa Konseyine ayrılmıştır. Bu bölümde Avrupa Konseyinin internete ilişkin yayımladığı bütün deklarasyonlar ve aldığı tavsiye kararları etraflıca incelenmiştir. **Yedi ila yirmi dördüncü bölümler**, AİHM'nin internetle ilgili temel kararlarına ayrılmıştır. Bu bölümlerde AİHM'nin kararları detaylı şekilde incelenmiş ve her bölümün sonunda müstakil bir karar değerlendirmesine yer verilmiştir. Çalışmanın **yirmi beşinci bölümü** "AİHM kararları ışığında ideal bir internet düzenlemesi hangi nitelikleri haiz olmalıdır?" sorusunun yanıtını bulmaya çalışmaktadır. **Yirmi altıncı bölüm** ise tüm çalışmaya ilişkin genel değerlendirmelere ayrılmıştır.

BİRİNCİ KISIM

TEMEL KAVRAMLAR

§2. İNTERNET

I. İnternetin gelişim süreci

İnternet, teknik ve tam tanımıyla, IP ve TCP protokollerini ve ağlar arası bağlantıyı mümkün kılan DNS ve paket *route* etme protokolleri gibi protokolleri kullanan, kamu ve özel sektöre ait telekomünikasyon ağlarının ara bağlantı yaptığı küresel bir bilgiye erişim ve iletişim ağıdır.[4] İnternet üzerinden iletişim telefon hatları üzerinden iletişime benzese de interneti telefondan farklı kılan temel unsur, önceden belirlenmiş sınırının olmaması ve dinamikliğidir.[5]

İnternet ne bir anlaşma ne de bir plan dâhilinde geliştirilmiştir.[6] İnternetin gelişim hikâyesi merkezin ölümü, ağın politik ve ticari yükselişi olarak ifade edilebilir.[7] İnternet, temelleri Amerika Birleşik Devletleri (ABD) ile Sovyetler Birliği'nin nükleer çalışmalar ve uzay çalışmaları alanındaki rekabetinin gölgesinde atılmış bir teknolojidir. İnternetin doğuşu, ABD'nin askerî amaçlı veri iletişimi için kurduğu Advanced Research Projects Agency (ARPA) çalışmalarına dayanmaktadır.[8]

ARPA, Sovyetler Birliği'nin 4 Ekim 1957 tarihinde ilk uydusu Sputnik'i uzaya göndermesiyle beraber ABD ve Sovyetler Birliği arasında kızışan uzay yarışının bir sonucu olarak 1958 yılında kurulmuş araştırma

---

4 **Mueller, Milton/Mathiason, John/Klein, Hans** (2007) *"The Internet and Global Governance: Principles and Norms for a New Regime"* Global Governance, C:13, Sayı: 2, 237-254, s. 237.

5 **Mathiason, John** (2009) *Internet governance: the new frontier of global institutions*, London, Routledge, s. 6.

6 **Ryan**, s. 7.

7 **Ryan**, s. 7.

8 İnternetin tarihçesi için bkz. **Internet Society** (1997), *"Brief History of the Internet"*, <https://www.internetsociety.org/wp-content/uploads/2017/09/ISOC-History-of-the-Internet_1997.pdf>

birimidir.[9] ARPA'nın kurulmasından kısa bir süre sonra, uzay ve roket çalışmaları Ulusal Havacılık ve Uzay Bilimleri Dairesinin (NASA - National Aeronautics and Space Administration) görev alanına bırakılmıştır. ARPA, uzay ve roket teknolojileri dışında kalan yüksek teknoloji alanındaki çalışmalara yoğunlaşmıştır.

1960'lı yılların başında askerî alanda önemli bir ihtiyaç gün yüzüne çıkmıştır: nükleer saldırılara dayanıklı bir iletişim mecrası.[10] Bu doğrultuda ARPA'nın ilk çalışmalarından birisi uzak mesafelerde yer alan bilgisayarların birbirine bağlanması alanında olmuştur. 1960'lı yılların başlarında ABD'de askerî birliklerin, kamu kurumlarının, üniversitelerin bilgisayarları arasında veri iletişimi için farklı teknolojiler kullanılmaktaydı. 1958 yılında Bell Laboratories tarafından "*modülatör-demodülator*" (modem) cihazları geliştirilerek dijital bilgisayar verisinin analog telefon hatları üzerinden gönderilmesi ve tekrar bilgisayar verisi formatına dönüştürülmesi sağlanmıştır.[11]

Analog hatların temel sorunu, sınırlı sayıda bağlantıya olanak verebilmesi ve merkezden uzaklaştıkça sinyal kalitesinin düşmesiydi. Ayrıca her bir bilgisayar başka bir bilgisayarla kendine özgü ağ protokolü üzerinden ve farklı formatta veri iletişimi yaptığı için bilgisayarlar arası iletişim pratik değildi. Bu sebeple, bilgisayarlar arasında bir ağ kurabilmek için tüm bilgisayarların sistem ayarlarının değiştirilmesi ve yazılım ile donanımlarının uyumlulaştırılması gerekmekteydi. Ağ kurmanın pratik olmaması ve ekonomik bakımdan külfetli olması sebebiyle ağlar büyüyememekteydi. Bu da verinin bilgisayarlar arasında iletimini ve dolayısıyla bilgi paylaşımını zorlaştırmaktaydı.

Yazılım ve donanım uyumsuzluğu sorunu dışında o dönemki ağların bir diğer sorunu, her bir ağın çalışmak için bir ana bilgisayara ihtiyaç duymasıydı. Ana bilgisayar saldırı veya teknik bir sorun sebebiyle kapandığı takdirde tüm ağ çökmekteydi. Veriler de belirli güzergâhlar üzerinden iletildiği için bir bağlantı hattının kesilmesi durumunda o güzergâh ile

---

[9] **Sherry/Brown**, s. 115.

[10] **Ryan**, s. 11.

[11] History of the Internet and Web <http://www.anderbergfamily.net/ant/history/>

iletişim tamamen kesilmekteydi. Tüm bu sebeplerle ABD Savunma Bakanlığı, nükleer saldırı dâhil herhangi bir saldırı sırasında veya sonrasında askerî kuvvetler, devlet kurumları ve araştırma merkezleri arasında kesintisiz iletişim sağlanması amacıyla 1969 yılında ARPA birimi bünyesinde ARPANET projesi üzerinde çalışmaya başlamıştır.[12]

Proje kapsamında öncelik, bilgisayarlar arasında veri iletişimi için ortak bir ağ protokolü standardının oluşturulmasına verilmiştir. Dünyanın farklı noktalarında farklı donanım ve farklı işletim sistemlerine sahip olan bilgisayarlar arasında veri iletişimi sağlanabilmesi için Vinton Cerf ve Robert Kahn tarafından Transmission Control Protocol (TCP) ve Internet Protocol (IP) protokolleri geliştirilmiştir.[13]

IP protokolü bilginin veri şeklinde dijital forma dönüştürülmesini, TCP protokolü ise verilerin nihai iletim adresine ulaştırılmasını sağlamaktadır. TCP/IP protokolünün geliştirilmesiyle bilgisayarlar arasında verinin herhangi bir merkeze ihtiyaç duymaksızın paketler hâlinde ve aktif herhangi bir ağ üzerinden iletimi olanaklı hâle gelmiştir. Ayrıca protokolün bir standart olarak kabul edilmesiyle donanım ve yazılım uyumsuzluğu sorunu giderilmiş, bilgisayarlar arasında kesintisiz veri iletişimi sağlanmıştır.

ARPANET, askerî amaçlar dışında üniversiteleri ve diğer kamu kurumlarını kapsayacak şekilde yayılmış ve geniş bir ağ oluşturmuştur. Bu gelişmelere bağlı olarak özel işletmeler de zamanla bu geniş ağın içine dâhil edilmiştir. Askerî amaçlı kullanılan ağ 1983 yılında MILNET adı altında ARPANET'ten ayrılmıştır. ARPANET, kamusal kullanıma açılmış ve National Science Foundation (NSF) tarafından yönetilmeye başlamıştır. Bu dönemde ağın en önemli özelliği ticari kullanıma kapalı olmasıydı.[14]

---

[12] ARPANET hakkında kapsamlı bilgi için bkz. **Lukasik, Stephen** (2011) "*Why the Arpanet Was Built*", IEEE Annals of the History of Computing, Cilt:33, Sayı:3, s. 4-21.

[13] **Cerf, Vinton G/Kahn, Robert E** (1974) "*A Protocol for Packet Network Intercommunication*" IEE Transactions on Communications, Cilt: 22, s. 637-648.

[14] **National Science Foundation**, "*NSFNET Acceptable Use Policy*", <http://old.cni.org/docs/infopols/NSF.html>

Diğer taraftan, Centre Europeén Recherces Nucléares (CERN) çalışanı Tim Berners-Lee tarafından 1992 yılında World Wide Web (www) standardı ve temel dosya transfer protokolü Hypertext Transfer Protocol (http) geliştirilmiştir. Bu standardizasyon sayesinde internet üzerinden yazı, resim, ses, video gibi farklı nitelikteki verilere veri bütünlüğü bozulmadan erişmek mümkün olmuştur.

İnternetin gelişiminde önemli aşamalardan birisi altyapının özelleştirilmesi aşamasıdır. 1994 yılında internet altyapı piyasası liberalleştirilmiş, altyapının özel sektör tarafından kurulması ve işletilmesinin önü açılmıştır. Bu girişimin lehinde ve aleyhinde çeşitli görüşler öne sürülmüştür. Lehte görüşler, devletin bu konuda geri plana çekilmesinin, kamu kaynaklarının harcanmasını azaltıcı bir etkide bulunacağı noktasında toplanmıştır. Diğer taraftan, özel sektörün bu konuda temel aktör olmasının ayrımcılığa yol açarak bazı kullanıcıları izole edebileceği ve ayrıca özel sektörün ayda milyarlarca paketin iletildiği ağı yönetmekte yetersiz kalacağı şeklinde endişeler dile getirilmiştir.[15]

ARPANET, zaman içerisinde farklı kurum, kuruluş ve kişilerin katkılarıyla günümüz internetine dönüşmüştür. İnternetin gelişimi bilim ve ulusal güvenliğin evliliği olarak betimlenmektedir.[16] Esasında 1960'lı yıllarda bilgisayar ve iletişim alanları birbirinden bağımsız disiplinler olarak varlıklarını sürdürmekteydi. Bunların tek bir sistem altında kullanılmaya başlaması, bu bağlamda bir devrim olmuştur. İnternet, kompleks mühendislik sorunlarının açık ve iş birlikçi şekilde çözülmeye çalışıldığı bir ortamda doğmuştur.[17]

ARPANET projesi kapsamında uzak konumlardaki bilgisayarlar arasında ağ bağlantısı sağlamaya yönelik çalışmaların yapıldığı dönemlerde dünyanın farklı noktalarında farklı kapsam ve nitelikte çalışmalar da vardı.[18] ARPANET projesinin temel farkları; hızlı yaygınlaşması, sadece

---

[15] **Lawis, Peter H.**, "*U.S. Begins Privatizing Internet's Operations*" <http://www.nytimes.com/1994/10/24/business/us-begins-privatizing-internet-s-operations.html>

[16] **Sherry/Brown**, s. 114.

[17] **Sherry/Brown**, s. 122.

[18] **Sherry/Brown**, s. 119; Örneğin nükleer saldırıya dayanıklı bir iletişim hattı arayışlarında ilk sistematik çözüm 1962 yılında bir RAND araştırmacısı olan Paul

askerî kurumların değil üniversiteler başta olmak üzere geniş bir topluluğun katılımına kısa sürede müsaade etmesi ve açık olmasıydı.

Şüphesiz, internetin ilk mimarları interneti şu an olduğu gibi kamuya açık bir ağ olarak tasarlamamışlardır. Tam aksine, internet askerî bir proje olarak geliştirilmiştir ve belirli noktalarda hâlâ onu geliştiren ABD'nin güvenlik stratejisinin bir parçası olmaya devam etmektedir.[19] İnternet ağına her geçen gün yeni bilgisayarlar eklenerek internet bugünkü hâlini almıştır. İnternet ve TCP/IP protokolü sayesinde bilgi, bilgisayarlar aracılığıyla belirli bir merkeze ihtiyaç duymaksızın ve kesintisiz olarak dünyanın her noktasına iletilmektedir. Artık sadece telefon şirketleri değil, dijital televizyon altyapısı sağlayıcıları ile elektrik firmaları dahi bu anlamda altyapı sağlayıcısı ve ağ operatörleri hâline gelmiştir.

Türkiye'de ilk internet bağlantısı 1993 yılında Ortadoğu Teknik Üniversitesinden (ODTÜ) gerçekleştirilmiştir. 12 Nisan 1993'te ODTÜ Bilgi İşlem Daire Başkanlığından, 64 kbps kapasiteli hat ile ABD'de bulunan National Science Foundation Network ağına ilk bağlantı gerçekleştirilmiştir.[20]

Baran tarafından ortaya konulmuştur. Özellikle, nöroloji alanındaki çalışmalardan haberdar olan Baran, merkezî dağıtım noktası olmayan ve hataya toleranslı bir ağ yapısı üzerinde çalışmalar yapmıştır. Beynin bir kısmının hasar görmesi durumunda, geriye kalan kısmının çalışmaya devam etmesi; belli bir kelimeyi hatırlamayan yaşlı insanların o kelimeye en yakın eş anlamlı kelimeyi kullanmasından ilham alarak verinin herhangi bir merkeze ihtiyaç duymadan ağ üzerindeki bir noktadan diğer bir noktaya aktarımının mümkün olacağı bir model geliştirmeye çalışmıştır. Modelin temelini, verinin paketlere bölünmesi ve herhangi bir merkeze uğramadan, ağ üzerinde yayılmış şekilde bulunan veri yönlendiricileri ile verilerin hedefe ulaşması oluşturmaktaydı. Bu şekilde, merkeze hiyerarşik olarak bağlılık ortadan kaldırılmış olmaktaydı. **Baran, Paul** (1964) "*On Distributed Communications: I. Introduction To Distributed Communications Networks*", <http://www.rand.org/content/dam/rand/pubs/research_memoranda/2006/RM3420.pdf>; **Ryan**, s. 14.

[19] **Arx, Kim G.** (2003) "*ICANN - Now and Then: ICANN's Reform and Its Problems*", Duke Law & Technology Review, Cilt: 2, s. 1-22, s. 3.

[20] İnternet Tarihi <http://www.internetarsivi.metu.edu.tr/tarihce.php>

II. Çalışma prensipleri

İnternet, dünyanın herhangi bir noktasında herhangi bir işletim sistemini veya bilgisayar donanımını kullanan herhangi bir kişinin dâhil olabileceği açık ağ mimarisi prensibine göre tasarlanmıştır. Açık mimari, yayımlanmış standartlara sahip tasarım demektir. İnternet için bu standart, TCP/IP protokolüdür. Bu protokolün çalışma esasları uluslararası bir standart olarak kabul edilmiştir. Bu sayede internet küresel bir ağ hâlini almıştır. İnternetin çalışması TCP/IP'den ibaret değildir. Başkaca protokoller farklı görevler yerine getirse de ana protokol TCP/IP protokolüdür.

TCP/IP protokolü sayesinde kişi veya kurumların, mevcut ağ yapılarında köklü değişiklik yapmak zorunda kalmadan ve ek donanıma ihtiyaç duymadan internete bağlanmaları mümkün olmaktadır. İnternete bağlanan kimsenin hangi işletim sistemini veya donanımı kullanarak internete bağlandığı, veri iletimi sırasında oluşturulacak paketin niteliğini etkilememektedir.

İnternetteki uygulamalar ağ üzerinde değil, web sitelerinin barındırıldığı sunucu olarak adlandırılan bilgisayarlarda çalışmakta ve TCP/IP protokolü, çalışan programlar arasında ayrım yapmamaktadır.[21] Bu durum geniş manada ağ tarafsızlığı olarak ifade edilmektedir. [22] Zira internet protokolü her türlü yazılıma ve donanıma karşı tarafsızdır.[23]

TCP/IP teknolojisine göre, iletilecek veri önce paketlere ayrılır ve her bir parça, içerik katmanı ve etiket katmanı olmak üzere temelde iki katmanda paketlenerek ağ içerisinde iletilir.[24] İçerik katmanında verinin bir parçası, etiket katmanında ise verinin nihai iletim adresi yer almaktadır. İnternet kullanıcısı tarafından oluşturulan veri paketleri, İnternet Servis Sağlayıcısı (İSS) olarak adlandırılan aracılar tarafından internet

[21] **Bayamlıoğlu, İbrahim Emre** (2008) *Fikir ve Sanat Eserleri Hukukunda Teknolojik Koruma*, İstanbul, On İki Levha Yayıncılık, s. 342.

[22] **Bayamlıoğlu**, s. 340.

[23] İnternette özellikle suçla mücadele etmek ve müzik gibi fikir ve sanat eserlerinin paylaşılmasını önlemek için ağ temelli düzenlemeler yapılmasına yönelik eleştiriler için bkz. **Bayamlıoğlu**, s. 338.

[24] **Hall, Eric A.** (2000) *Internet core protocols: the definitive guide*, Cambridge, O'Reilly, s. 6.

ağına aktarılmaktadır. Diğer bir deyişle, İSS'ler verilerin kullanıcılardan ana internet ağına taşınmasında sadece aracılık etmektedir. İSS'ler tarafından aktarılan paketler; fiberoptik veya normal kablolar, kısa mesafeli kablosuz bağlantılar yahut uydu hatları gibi değişik noktalardan, internet ağına bağlı bulunan ve *router* olarak adlandırılan ağ donanımları tarafından nihai iletim adreslerine taşınır.

İnternet öncesinde de ağlar arasında veri iletişimini mümkün kılan yöntemler vardı. İnterneti bu yöntemlerden farklı kılan temel husus, verinin ağdaki hareketidir. İnternet dışındaki diğer ağlarda veriyi bir noktadan diğer noktaya göndermek için sadece alıcıyı belirtmek yetmemekte, ayrıca verinin izleyeceği güzergâhların da belirlenmesi gerekmekteydi. İnternet ağında ise sadece alıcının belirtilmesi yeterli olup *router* olarak adlandırılan ağ donanımları paketin nihai adresine ulaştırılmasını sağlamaktadır. Bu da interneti pratik ve yaygın kılan en temel özelliktir.

İnternete bağlı her bilgisayarın Internet Protocol (IP) adı verilen eşsiz bir numerik adresi vardır. Bir sunucu üzerinde sadece bir web sitesi barınabileceği gibi sunucunun teknik kapasitesine göre binlerce web sitesi de barınabilir. *Router*lar web sitelerini IP adreslerine göre tanımlar ve paketleri, üzerlerindeki etiket katmanına göre nihai iletim adreslerine iletir. Diğer bir deyişle, *router*lar paketin içeriğiyle ilgilenmeksizin sadece etiket katmanına göre paketleri işler.

Paketler r*outer*lar tarafından nihai iletim adreslerine en kısa mesafeden ulaştırılmaya çalışılır. Eğer paket iletilirken ağda herhangi bir saldırı nedeniyle veya başkaca bir sebeple kesinti oluşursa paket, *router* tarafından başka bir ağ güzergâhına aktarılır ve bu şekilde nihai hedefine ulaştırılır. Nihai iletim adreslerine varan paketler otomatik olarak birleştirilerek orijinal hâllerine dönüştürülür.

İnternet üzerindeki bilgi alışverişi veri paketlerinin farklı güzergâhlar üzerinden taşınması suretiyle gerçekleştirildiği için dünyadaki bir bilgisayarın diğer bir bilgisayardan daha fazla önemi olmadığı gibi tüm veri iletiminin gerçekleştirilmesinden sadece bir bilgisayar sorumlu değildir.[25] Bu şekilde, internet ağına bağlı herhangi bir kullanıcı herhangi bir

[25] **Hofstetter, Fred Thomas** (2006) *Internet literacy*, Boston, McGraw-Hill/Irwin, s. 20.

ülkedeki başka bir kullanıcıya veriyi göndermekte, veri saniyeler içinde farklı devletleri ve dolayısıyla farklı hukuk rejimlerini herhangi bir merkeze uğramadan aşmaktadır.

İnternet; kablolar, uydular, radyo frekansları ve hatta elektrik iletim hatları üzerinden dünyanın farklı noktalarında bulunan cihazları birbirine bağlamaktadır. Özellikle SpaceX Starlink gibi ticari girişimlerin uydularının yaygınlaşmasıyla internete erişebilirlik konusunda ciddi bir mesafe katedilmiş olacaktır. Öte yandan uydu interneti; elektronik haberleşme alanında yetkilendirme rejimlerine, yeni internet altyapı tekellerinin ortaya çıkmasına, bilişim suçu işlenmesi durumunda dijital delillerin elde edilmesine, internet erişiminin kısıtlanmasına ilişkin yeni tartışmaları da beraberinde getirecektir.

Kısaca, internet yakınlık-uzaklık kavramlarını anlamsızlaştıran bir ortamdır.[26] Dünyanın neresinde barındırılırsa barındırılsın tüm web siteleri, kullanıcılara aynı uzaklıktadır. İnterneti klasik iletişim ve bilgiye erişim araçlarından ayıran temel nokta, yakınlık- uzaklık kavramlarını kökten değiştirmiş olmasıdır. Bir web sitesinin dünyanın hangi noktasında barındırıldığı, erişen kullanıcı bakımından bir fark yaratmamaktadır. İki web sitesinin birbirine uzaklığının sadece kavramsal bir değeri olup fiziki mesafeyle bir ilişkisi bulunmamaktadır. Sanal gerçeklik olarak ifade edilen bu durum interneti kendine özgü bir ortam hâline getirmektedir.

III. Temel kavramlar

A. Ağ (Network)

Ağ; cihazların bilgi paylaşması ve iş birliği yapmasına olanak tanıyan özel donanım veya yazılım kullanan, birbirine fiziksel veya mantıki olarak bağlanmış bilgisayarların veya diğer ağ cihazlarının toplamı olarak tanımlanabilir.[27] İnternete bağlanmak aslında bir ağın parçası olmak de-

[26] **Bayamlıoğlu**, s. 34.

[27] **Kozierok, Charles M.** (2005) *The TCP/IP guide : a comprehensive, illustrated Internet protocols reference*, San Francisco, No Starch Press, s. 6.

mektir. Benzer şekilde, bir cihazı elektrik prizine takmak elektrik ağına dâhil olmak anlamına gelir.

Ağın, internete erişmek, internet erişimini paylaşmak, veri güvenliği ve yönetimini sağlamak, performans artırmak ve dengelemek, oyun oynamak ve benzeri eğlence amaçlı kullanımları çok yaygın olsa da ağlar, bağlantı amaçlı ağlar ve paylaşım amaçlı ağlar olarak iki temel kategoride sınıflandırılabilir.[28] Ağın değeri, ne kadar çok bağlantı yapabildiği veya ne kadar çok kişiyi bağlayabildiğiyle ölçülür.[29]

İnternet, farklı alt ağların bir araya gelmesinden oluşmaktadır. Bir veri, bir noktadan başka bir noktaya taşınırken farklı hukuki ilişkilerin konusu olabilmektedir. Örneğin, iki İSS trafiğin doğrudan internet omurgası yerine transit olarak birbirlerinin ağlarından geçmesini kararlaştırabilir. İki ağ arasında bu şekilde karşılıklı trafik alışverişi yapılarak, diğer bir deyişle *peering* ilişkisiyle veri özel bir hukuki statü içerisinde aktarılmaktadır. İnternet trafiği taşıyan iki veya daha fazla işletmeci arasında internet trafiği değişiminin yapılmasına imkân vermek üzere belirlenen ortak bir noktada tesis edilen ve İnternet Değişim Noktaları (IXP - Internet Exchange Point)[30] olarak adlandırılan altyapılar, daha büyük ölçekte internet trafiğinin değişimi için kavşak görevi üstlenmektedir.

Benzer şekilde, ağa farklı noktalardan bağlanmak yerine tek bir varlık noktası (POP - Point of Presence) üzerinden bağlantı yaparak verinin ağda daha güvenli bir rota izlemesi de pekâlâ imkân dâhilindedir. Örnekleri artırmak mümkündür. Bu çalışmanın kapsamı bakımından önemli olan, A noktasından B noktasına veri alışverişini hukuki olarak sınıflandırırken ulusal ve uluslararası farklı hukuki ilişkilerin ve kamu, özel kişiler, uluslararası kuruluşlar gibi farklı paydaşların varlığını göz ardı etmemektir.

Öte yandan, internetin yaygınlaşmasıyla birlikte modern toplum "bilgi toplumu" olarak adlandırılmaya başlamıştır. Ne var ki bu kavram,

---

[28] **Kozierok**, s. 7.

[29] **Ryan**, s. 84.

[30] İnternet Değişim Noktalarının güncel durumunu gösteren harita için bkz. Internet Exchange Map <https://www.internetexchangemap.com>

modern toplumun, önceki dönemleriyle farkını yeterince ifade edememektedir. Nihayetinde, avcı-toplayıcı hayattan tarım ekonomisine, oradan da üretim ekonomisine geçişte zaten temel belirleyici unsur bilgi olmuştur. Bilgi ve iletişim teknolojilerinin hayatın her alanında kullanılması sebebiyle bu dönemde modern toplumun değerlerini en iyi "ağ toplumu" kavramının yansıttığı düşünülmektedir.[31]

Sosyal medya sitelerinin çok hızlı şekilde yaygınlaşması ve dünya genelinde benimsenmesi ağ toplumu kavramının yerindeliğini göstermektedir. 5G ağların daha hızlı ve sürekli bağlantı sağlaması ve eşyaların internetinin (IOT - Internet of Things) de yaygınlaşmasıyla ağ toplumunda farklı bir dönüşüm yaşanacaktır.[32] 2022 itibarıyla her bir evde en az 50 farklı bağlantı noktası olacağı tahmin edilmektedir.[33]

Modern birey, farklı amaçlarla çeşitli ağlara bağlanır. İş için başka, aşk için başka bir sosyal ağda etkileşim içerisine girer. Ağlar üzerinde modern dilencilik dahi yapılmaktadır. Görülen rüyayı internet ortamında paylaşma imkânı tanıyıp benzer rüyaları gören kişileri buluşturan ağlar bile vardır. Ağ, bir yandan da yerel kültür ile diğer kültürler arasında etkileşimi artırmış ve *netizen* olarak adlandırılan yeni bir internet vatandaşı anlayışını da ortaya çıkarmıştır. Öyle ki farklı coğrafyalarda yaşayan kişiler ortak bir ülkü altında toplanmakta, internet ortamında örgütlenmekte, bir konuya beraber tepki göstermekte ve kamuoyu oluşturmaktadır.

B. IP adresi (Internet Protocol)

İnternete bağlı her aygıtın Internet Protocol (IP) denilen eşsiz bir numerik adresi vardır. IP adreslerinin sabit bir noktaları ve tek merkezleri bulunmamaktadır, bunlar tamamen kavramsal niteliktedir.[34] Telefon numaraları veya posta kodlarının aksine IP adresleri coğrafi konumlar-

---

[31] **Bayamlıoğlu**, s. 21.

[32] **ICANN**, "*5G Technology*", <https://www.icann.org/en/system/files/files/octo-004-23jan20-en.pdf>

[33] **TechSpot**, "*Wi-Fi 6 Explained: The Next Generation of Wi-Fi*" <https://www.techspot.com/article/1769-wi-fi-6-explained/>

[34] **Mathiason**, s. 10.

dan bağımsızdır.[35] Diğer bir deyişle, IP adresinin kendisi ağdaki mevcut konumu hakkında bilgi vermemektedir. Ağa bağlı bir cihazdan bir başka cihazı yani bir IP adresinden bir başka IP adresini bulma işlevi *router* cihazları tarafından gerçekleştirilmektedir. *Router* cihazları paketlerin ağda iletiminden sorumludur ve internette paketler bir *router* cihazından diğerine atlayarak nihai varış noktasına ulaşmaktadır.[36]

IP adresi; ağa bağlı cihazların birbirini tanımak, birbiriyle iletişim kurmak ve birbirine veri yollamak için kullandıkları bir adresleme sistemidir. IPv4 formatındaki bir IP adresi 216.58.212.46 örneğindeki gibidir. Bu IP numaraları içerisinde 192.168.x.x ve 10.x.x.x ile başlayanlar özel ağlar için ayrılmıştır.

IP adresleri, dinamik ve statik olarak iki bölüme ayrılır. Genel olarak dinamik IP adresi kullanılır. Dinamik IP adresleri, zamana ve oturuma göre değişir çünkü hizmet sağlayıcı o an için boş olan IP adresini kullanıcıya atar. Statik IP adresi ise belirli bir ağa bağlı cihazların ağ üzerinden birbirlerine veri yollamak için kullandıkları, zamana ve oturuma göre değişmeyen, sistem yöneticisi tarafından belirlenip tanımlanan ve değiştirilebilen IP adresi olarak ifade edilebilir.

IP adreslerinin kısıtlı olmasının önüne geçmek için çeşitli ara yöntemler kullanılmaktadır. Bu yöntemlerin en yaygın olanlarından birisi, NAT IP (Network Address Translation IP) kullanımıdır. NAT, bir ağda bulunan bilgisayarın, kendi ağı dışında bir ağa veya internete çıkarken farklı bir IP adresi kullanabilmesi için geliştirilmiş bir internet protokolü olup bilgisayarın sahip olduğu IP adresini istenilen başka bir adrese dönüştürür.[37] Bu şekilde iç ağda özel IP'ler kullanılırken, NAT yapabilen uygun *router*lar vasıtasıyla IP adresleri genel adreslere çevrilerek dış bağlantılar sağlanmaktadır. Özellikle mobil internet bağlantılarının yaygın-

---

[35] **Mueller, Milton** (2002) *Ruling the root Internet governance and the taming of cyberspace*, Cambridge, MIT Press, s.33.

[36] **Mueller**, s. 33.

[37] **Dodd, Annabel Z.** (2012) *The Essential Guide to Telecommunications*, Upper Saddle River, Prentice Hall, s. 268; **İTÜ**, *"NAT (Network Address Translation - Ağ Adresi Çeviricisi)"* <http://bidb.itu.edu.tr/seyirdefteri/blog/2013/09/07/nat-(network-address-translation---a%C4%9F-adresi-%C3%A7eviricisi)>

laşmasıyla beraber her bir mobil kullanıcıya dinamik de olsa bir IP adresi atamak zorlaşmıştır. Mobil ağlarda NAT IP bu sebeple yaygındır.

NAT IP dışındaki bir diğer önemli uygulama ise PORT bazlı paylaşımdır. Her bir internet servisinin kendine özgü, port olarak adlandırılan bir alt bağlantı numarası vardır.[38] Port numarası, bağlantının bir işletim sistemindeki sonlandırılma noktasıdır. Örneğin, internet trafiği temel olarak 80 numaralı port üzerinden yayın yaparken e-posta servisleri Simple Mail Transfer Protocol (SMTP) protokolü üzerinden 25 numaralı portu kullanmaktadır. Bir bağlantının içerisinde farklı port noktaları üzerinden farklı noktalara ve uygulamalara bağlantı yapılabilir. Bu esasla, aynı IP adresi ve farklı port noktaları üzerinden farklı kullanıcıların internet ağına bağlanması mümkündür. Mobil ağlarda bu yöntem yaygındır.

IP adreslerinin sayısal anlamda yetersizliği ve teknik anlamda bazı konulardaki kısıtlılıkları esasında internetin daha ilk dönemlerinde belirgin hâle gelmiştir. Ancak, ağın dinamik ve dağıtık (*distrubuted*) yapısı IP protokolünde radikal bir reformu mümkün kılmamıştır. 1990'lı yılların başında yeni nesil IP protokolünün nasıl olması gerektiği tartışılmaya başlamış ve Internet Engineering Task Force (IETF)[39] tarafından çeşitli öneriler ortaya atılmıştır.[40] Sonradan IPv6 olarak adlandırılacak bu protokol, IPv4 sistemiyle eş güdümlü çalışacak şekilde kurgulanmış; bu şekilde kademeli, yumuşak ve minimum riskli bir geçiş tasarlanmıştır.[41] Bu sebepledir ki IPv6 protokolü internet için devrimsel değil, evrimsel bir gelişme olarak nitelendirilmektedir.[42]

128 bit adres uzunluğuna sahip IPv6, yaklaşık 10 üzeri 39 biricik sayısal değere olanak vermektedir. Oysaki IPv4 sistemi, en fazla 4 milyarı

---

[38] İnternet servislerinin kullandıkları port numaraları için bkz. **IANA**, "*Port Numbers*", <http://www.iana.org/assignments/port-numbers>

[39] IETF hakkında daha fazla bilgi için bkz. **§3(III)**[Internet Engineering Task Force (IETF)].

[40] Örneğin bkz. **Bradner S/Mankin A**, "*The Recommendation for the IP Next Generation Protocol*", <https://tools.ietf.org/html/rfc1752>

[41] **IETF**, "*IPv6 is an Internet Standard*", <https://www.ietf.org/blog/ipv6-internet-standard/>

[42] **Bradner S/Mankin A**, "The Recommendation for the IP Next Generation Protocol".

biraz aşan sayıda (tam olarak 4.294.967.296) adres temin edebilmektedir. IPv6 daha basitleştirilmiş bir başlık yapısı içermekte ve route etme açısından kolaylıklar sağlamaktadır. Ayrıca, güvenlik bakımından da IPv6 daha kolay uygulanabilir bir güvenlik yapısı sunmaktadır. IPv6 ile birlikte, internete bağlı her bir cihaza doğrudan IP adresi atanması mümkün olacaktır. Bu IP adresi ile cihazların ağda takibi ve konumlandırılması kolaylaşacaktır. IPv6, özellikle akıllı eşyaların yönetimi ve ağa bağlanabilirliği (eşyaların interneti) açısından önemli kolaylıklar sağlayacaktır.[43] Örnek bir IPv6 adresi, 3ffe:1900:4445:3:200:f8ff:fe21:67cf şeklindedir.

IP adresi, kişiyi değil ağdaki cihazı gösterir. Özellikle dinamik IP adreslerinin kullanıldığı durumlarda, cihaz başında işlem yapan kişiyi tespit için ayrı bir adli bilişim süreci işletmek gerekecektir. IPv6 dönüşümü hızla sürmektedir. Tüm bu dönüşüm süreci tamamlandığında kişilerle doğrudan eşleştirilmiş IP adreslemesi mümkün olacaktır.

C. DNS (Domain Name System)

İnternet sitelerine erişim için kullanılacak IP adreslerinin hatırlanması zor olduğu için Alan Adı Sistemi (DNS - Domain Name System) geliştirilerek IP adreslerinin yerine geçen harf dizilerinin kullanılması sağlanmıştır. Bu sistem sayesinde örneğin web tarayıcısına "google.com" yazmak suretiyle 72.14.235.104 IP numaralı sunucuda barındırılan Google arama motorunun içeriğine erişmek mümkün olmaktadır.

Alan adı, internet üzerinde bulunan bilgisayar veya internet sitelerinin adresini belirlemek için kullanılan internet protokol numarasını tanımlayan addır. DNS, okunması ve akılda tutulması kolay olan ve genelde aranan adres sahipleri ile ilişkilendirilebilen simgesel isimlerle yapılan adreslemede, karşılığı olan internet protokolü numarasını bulmakta ve kullanıcıya vermektedir.

---

[43] Türkiye'de de kamu kurumlarının IPv6'ya geçişleri için 2010 yılında yayımlanan Başbakanlık genelgesiyle çalışmalar başlatılmıştır. Bkz. "2010/25 sayılı Başbakanlık Genelgesi - Kamu Kurum ve Kuruluşları için IPv6'ya Geçiş Planı", RG 8.12.2010/27779.

DNS, hiyerarşik şekilde yapılanmıştır.[44] Alan adı için en üst düzey yönetim A kök sunucusu tarafından gerçekleştirilmekte ve diğer 12 kök sunucu A kök sunucusu değerlerini referans almaktadır.[45] Kök sunucuların altında jenerik (*generic*), ülke kodlu (*country code*) ve altyapıya (*infrastructure*) göre ayrılmış üst düzey alan adları (*top level domains*) vardır. Alan adları "ilk gelen alır" prensibine göre bireylere veya kurumlara tahsis edilmektedir. Ülke kodlu uzantılar için ise bazı sınırlamaların uygulanması mümkündür. Örnek bir alan adı "mbkaya.com" şeklindedir.

Bir alan adının farklı bölümlere ayrılması ve alt alan adlarının farklı fiziki konumlarda barındırılması teknik olarak mümkündür. Alan adlarının bu tür alt kısımlarına "*subdomain*" denilmektedir. Örnek bir alt alan adı "hukuk.mbkaya.com" şeklindedir. Ayrıca, alan adı ile "www" eş değer kavramlar değildir. Esasında "www" sık kullanılan bir alt alan adıdır. Bir internet sitesine "www" ön ekini kullanmadan da erişmek ve siteyi kullanmak mümkündür.

Ülke kodlu üst düzey alan adları tescil edildikleri ülkede barındırılmak zorunda değildir. Türkiye'nin üst düzey alan adı olan "tr" uzantılı bir web sitesi, ABD'deki bir sunucuda hizmet kalitesinde herhangi bir sorun yaşanmadan barındırılabilir.

Web sitelerinin kullandığı servislerin birbirinden bağımsız şekilde farklı ülkelerdeki farklı sunucularda barındırılması mümkündür. Örneğin, "tr" uzantılı bir web sitesinin 80 portundan erişilen ana içeriği ABD'deki bir sunucuda barındırılırken başka porttan erişilen e-posta servisleri Almanya'daki bir sunucuda barındırılabilir. Benzer şekilde, alan adının içerikleri Türkiye'de barındırılırken alt alan adı (*subdomain*) başka bir ülkede barındırılabilir.

---

[44] DNS konusunda kapsamlı bilgi için bkz. **Arx**; **Mueller**.

[45] Kök sunucular hakkında daha fazla bilgi için bkz. **ICANN**, "*Brief Overview of the Root Server System*", <https://www.icann.org/en/system/files/files/octo-010-06may20-en.pdf>; Kök sunuculara ilişkin güncel bir harita için bkz. **Root Server Technical Operations Association**, <https://www.root-servers.org>

D. URL (Uniform Resource Locator)

Uniform Resource Locator (URL), internette resim, yazı veya müzik gibi bir kaynağa karşılık gelen, standart bir formata uygun karakter dizgisidir. URL, internet üzerindeki bir kaynağın koordinatıdır. Pratik bir anlatımla URL, internette gezinirken herhangi bir kaynağa tıklandığında tarayıcının adres çubuğunda görünen adrestir.

Örnek bir URL adresi "https://www.mbkaya.com/hukuk/internetmevzuat.pdf" şeklindedir. Bu URL adresi şöyle çözümlenebilir:

https **:** Protokol (HTTPS Protokolü)

www **:** Alt alan adı (subdomain)

mbkaya **:** Alan adı (domain)

com **:** Üst düzey alan adı (Top Level Domain - TLD)

/hukuk/internetmevzuat.pdf : Dosya yolu

Mobil bağlantıların yaygınlaşmasıyla beraber mobil cihazlarla uyumlu, daha az trafik gerektiren internet sayfalarının sayısı artmıştır. Bu tür sayfalar farklı URL adreslerinde barındırılmaktadır. Örneğin içerik "mbkaya.com" adresinde barındırılırken aynı içeriğe "http://mobil.mbkaya.com" adresinden de mobil cihazlara uyumlu şekilde erişilmektedir. Yukarıda açıklandığı üzere "www" bir alt alan adıdır. Dolayısıyla, bir içeriğin "www"li hâli ile "www"siz yalın hâli farklı URL'ler olarak nitelendirilecektir.

URL adresleri için önemli bir diğer husus ise veri transfer protokolüdür. Hiper Metin Transfer Protokolü (HTTP - Hyper Text Transfer Protocol), internette yer alan verilere ulaşmak amacıyla kullanılan standart bir iletişim protokolüdür. Güvenli Hiper Metin Transfer Protokolü (HTTPS - Secure Hyper Text Transfer Protocol) ise Secure Sockets Layer (SSL) güvenlik sertifikası eklenmek suretiyle güvenli iletişim ve veri aktarma olanağı sağlayan bir protokoldür.[46] SSL, prensip olarak, ilave bir

[46] **Dodd**, s. 233; **Boncella, Robert J** (2004) "*Secure Sockets Layer (SSL)*": Bidgoli, Hossein (Editör), *The Internet Encyclopedia - Volume 3*, Hoboken New Jersey, John Wiley & Sons;

yazılım kurulmasını gerektirmeyen, internet tarayıcılarıyla doğrudan kullanılabilen bir güvenlik çözümüdür. SSL, sunucu ve kullanıcı arasındaki trafiği kriptolojik şekilde şifreleyerek verilerin bütünlüğünü ve gizliliğini sağlamaktadır.

İnternetin en sihirli enstrümanı bağlantılardır. Bağlantılar aracılığıyla, internet ortamındaki farklı noktalarda yer alan içerikleri bulmak mümkün hâle gelmiştir. İçeriği oluşturan kişiden önceden izin almaya gerek olmaksızın bağlantılar vasıtasıyla internette gezinmek pratik bir hâl almıştır. [47] Öyle ki, bağlantılar ifade özgürlüğünün internet ortamında kullanılmasının en temel bileşeni durumundadır.[48]

E. MAC adresi

MAC adresi (Media Access Control), "*ağ donanımının tanımlanmasını sağlayan, ağ üzerinde bir aygıta imalat sırasında verilen 48 bitten oluşan, on altılık tabanda ifade edilen ortak erişim yönetimi*" olarak tanımlanmaktadır.[49] Diğer bir ifadeyle, MAC (Media Access Control), ağa ve internete kablolu veya kablosuz bağlantı kuran her aygıtın kendine özel ve aygıtı tanıtan adresidir. MAC adresi, ağ adaptörü üretildiğinde üzerine kodlanan, özgün bir seri kodudur. Fiziksel adres olarak da adlandırılmaktadır.

MAC adresi, iki nokta veya kısa çizgiyle ayrılmış altı grup hâlindeki iki haneli harf ve/veya rakamlardan oluşur. MAC adresinin ilk kısmı, donanımı üreten üretici firmaya özgü Organizationally Unique Identifier (OUI) olarak da belirtilen koddur. Adresin geriye kalan kısmı ise o cihazın özgün kodudur. Örnek bir MAC adresi "C8-60-00-BA-95-65" şeklindedir.

IETF, "*The TLS Protocol*" <https://www.ietf.org/rfc/rfc2246.txt>

47 **Berners-Lee, Tim** (1997) "*Links and Law: Myths*" <https://www.w3.org/DesignIssues/LinkMyths.html>

48 Bu konuda önemli bir değerlendirme için bkz. **Berners-Lee, Tim**, "*Long Live the Web: A Call for Continued Open Standards and Neutrality*", <https://www.scientificamerican.com/article/long-live-the-web/>

49 **Jandarma Genel Komutanlığı Kriminal Dairesi Başkanlığı** (2016) *Kriminal Terimleri Sözlüğü*, Ankara, TDK Yayınları, s. 81.

MAC adresi farklı amaçlarla kullanılabilir. Örneğin, MAC adresi esas alınarak ağdaki teknik sorunların tespiti pratik hâle gelmektedir. MAC adresinin sabit olması, ağ içerisinde gönderici ve alıcıların tanımlanmasına hizmet eder. Aynı doğrultuda, *router*ların sadece belirli MAC adreslerinden trafiği kabul etmesi sağlanarak ağa izinsiz bağlantıların kısıtlanması mümkündür. Bazı yazılım lisanslarının MAC adresine göre onaylanması; bazı interaktif hizmetlerin MAC adresine göre verilmesi imkân dâhilindedir. MAC adresi sabit bir kod olmasına rağmen birtakım teknik müdahalelerle işletim sistemi ayarlarının değiştirilmesi ve bu şekilde söz konusu kısıtlamaların aşılması mümkün olabilmektedir.

F. Bulut bilişim (Cloud Computing)

Bulut bilişim; işlemci gücü ve depolama alanı gibi bilişim kaynaklarının ihtiyaç duyulan anda, ihtiyaç duyulduğu kadar kullanılması esasına dayanan, uygulamalar ile altyapının birbirinden bağımsız olduğu ve izin verilen her yerden veriye kontrollü erişimin mümkün olduğu, gerektiğinde kapasitenin hızlı bir şekilde artırılıp azaltılabildiği, kaynakların kullanımının kolaylıkla kontrol altında tutulabildiği ve raporlanabildiği bir bilişim türüdür.[50] Bulut bilişim dinamik olarak ölçeklenebilen ve genellikle sanallaştırılan kaynakların internet üzerinden hizmet olarak sunulduğu yeni bir bilişim yöntemidir.[51] Esasında bulut bilişim yeni bir teknolojiden ziyade, bilgi ve iletişim teknolojilerinin yeni bir bilişim hizmet modeliyle sunulmasıdır.

ABD Ulusal Standartlar ve Teknoloji Enstitüsü (NIST - National Institute of Standards and Technology), bulut bilişimi, yapılandırılabilir bilişim kaynaklarından oluşan ortak bir havuza, uygun koşullarda ve isteğe bağlı olarak her zaman, her yerden erişime imkân veren bir model olarak tanımlamaktadır. Söz konusu kaynaklar (bilgisayar ağları, sunucular, veri tabanları, uygulamalar, hizmetler vb.) asgari düzeyde yönetimsel çaba ve hizmet alıcı-hizmet sağlayıcı etkileşimi gerektirecek kolaylıkta te-

---

[50] **TSE** (2013) "*Bulut Bilişim Güvenlik ve Kullanım Standardı (Taslak)*", <https://www.tse.org.tr/upload/tr/dosya/duyuruyonetimi/1082/12122014170015-2.pdf>

[51] **Furht, Borko** (2010) "*Cloud Computing Fundamentals*": Borivoje, Furht/Escalante, Armando (Editör) *Handbook of cloud computing*, New York, Springer, s. 3.

darik edilebilmekte ve elden çıkarılabilmektedir.[52] Bulut bilişim; 1910'lu yıllarda ortaya çıkmış olan, Amerikan şirketlerinin kendi özel jeneratörleri yerine ortak güç noktasına bağlantı yapmasına olanak sağlayan ve bu şekilde maliyetleri düşüren Samuel Insull'un "*güç havuzu*" modeline benzemektedir.[53]

Bulut bilişimin temel unsurları; isteğe bağlı ve kendi kendine hizmet, geniş ağ erişimi, ortak kaynak havuzu, çabukluk ve esneklik ile ölçülebilir hizmettir. Bulut bilişim konumlandırma modellerine göre ise özel bulut, topluluk bulutu, kamuya açık bulut, hibrit bulut gibi çeşitleri bulunmaktadır.

Bulut bilişimde birbirinden farklı üç temel hizmet sunum modeli vardır:[54]

Hizmet olarak yazılım [SaaS - Software as a Service): Hizmet olarak yazılım modelinde, servis sağlayıcı tarafından sunucu üzerinde bulundurulan yazılım uygulamasının kullanıma sunulması söz konusudur. Bu şekilde lisans, yazılım ve benzeri maliyetler açısından avantajlar sağlanmaktadır.

Hizmet olarak platform (PaaS - Platform as a Service): Hizmet olarak platform modelinde, servis sağlayıcı tarafından kullanıcısına kendi uygulamalarını geliştirebileceği ve çalıştırabileceği bir platform ile tamamlayıcı servisler ve gerekli teknolojik altyapı bütüncül şekilde sunulmaktadır.

Hizmet olarak altyapı (IaaS - Infrastructure as a Service): Hizmet olarak altyapı modelinde, kullanıcının, ihtiyacı olan temel bilişim kaynaklarını (işlemci, depolama, ağ kaynağı vb.) kendisinin yapılandırabilmesi ve bunların üzerine, ihtiyaç duyduğu işletim sistemini ve uygulamaları kurabilmesi sağlanmaktadır.

---

[52] **NIST** (2011) "*The NIST Definition of Cloud Computing*", <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>, s. 2.

[53] **Ryan**, s. 181.

[54] **Furht**, s. 5.

Bilgi teknolojileri alanındaki donanım ve yazılım yatırım maliyetlerini düşürmesi ve gelişmiş performans sağlaması bulut bilişimin avantajları arasındadır. Bununla birlikte konuya ilişkin teknik standartlar ve yasal düzenlemelerin yetersizliği; hizmet kalitesi ve güvenilirliğine, hizmet sunan tarafa ait veri merkezlerinde saklanan, hizmet alıcı tarafa ait kişisel verilerin veya ticari sırların gizliliğine ve toplu hâlde saklanan verilerin güvenliğine yönelik ihlallere daha kolay hedef olunabilmesi gibi birtakım güçlükleri de beraberinde getirmektedir.[55] Bulut bilişimin özellikle güvenlik boyutuna yönelik olarak ISO (International Organization for Standardization) tarafından yürütülen standart çalışmaları, bu dezavantajları ortadan kaldırmak adına önemli gelişmelerdir.[56] 2022 itibarıyla yeni uygulamaların %90'ının bulut temelli olacağı tahmin edilmektedir.[57]

G. Web 2.0

İnternetin kullanım alanlarının çeşitlenmesiyle birlikte web siteleri, etkileşimli uygulamalarını artırmıştır. Kullanıcı etkileşimini artırarak internetin etkinliğini en üst düzeye çıkarmak için çeşitli teknolojiler geliştirilmiştir. Web 2.0 yüksek etkileşimli yeni nesil internet teknolojilerinin genel adıdır.[58] Kavram temel olarak web sitelerinin sundukları ve kullanıcı katılımına imkân tanıyan teknolojileri ifade etmektedir. Web 2.0 teknolojileri kullanıldığında kullanıcılar yorum yazarak, resim göndererek veya bizzat içerik oluşturarak içeriğin bir parçası hâline gelmektedir. Diğer bir deyişle,

---

[55] 11. Ulaştırma, Denizcilik ve Haberleşme Şurasında Haberleşme Komisyonu tarafından hazırlanan Bulut Bilişim Raporu için bkz. **Haberleşme Komisyonu**, *"Bulut Bilişim"*, <https://www.btk.gov.tr/File/?path=ROOT/1/Documents/Sayfalar/Arastirma_Raporlari/Bulut_Bilisim.pdf>; Amerikan hukukunda bulut bilişimin düzenlenmesine ilişkin güncel tartışmalar için bkz. **Bilgiç, Seçil** (2018) "Something Old, Something New, And Something Moot: the Privacy Crisis under the Cloud Act" Harvard Journal of Law & Technology, Cilt: 32, Sayı: 1, s. 321-355.

[56] Bkz. ISO/IEC 27017:2015 - Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services.

[57] **IDC**, "Worldwide Cloud 2019 Predictions" <https://www.idc.com/research/viewtoc.jsp?containerId=US43001718>

[58] **O'Reilly, Tim**, *"Web 2.0 Nedir"*, <http://www.turk-internet.com/portal/yazigoster.php?yaziid=14394>

Web 2.0 teknolojileri verinin akış yönünü değiştirmekte ve her bir kullanıcı edilgen olmaktan çıkarak birer içerik sağlayıcıya dönüşmektedir.[59]

H. İçerik dağıtım ağı (CDN - Content Delivery Network)

İnternet sitelerinin farklı coğrafyalara hizmet sunmaya başlaması ve sunulan hizmetlerin kesintisiz çalışmasına yönelik ihtiyacın artması sebebiyle, internet içeriğinin farklı yerlerde konumlandırılmış sunuculara dağıtılması yaygın olarak kullanılan bir yöntemdir.[60] İçerik dağıtım ağı olarak da adlandırılan bu yöntemle, kullanıcıların kendilerine en yakın sunucuya erişerek en hızlı hizmeti alması mümkün olmaktadır. Sitelerin içeriği bu sunucular arasında anlık olarak senkronize edilmekte ve herhangi bir sunucuda kesinti yaşanması durumunda kullanıcı en yakın aktif sunucuya yönlendirilerek hizmetlerin kesintisiz çalışması sağlanmaktadır.

I. Ağ tarafsızlığı (Network Neutrality)

Ağ tarafsızlığı ilkesi, "*içerik sağlayıcılara erişim hizmeti sunan şebeke işletmecilerine öncül olarak ayrım gözetmeme yükümlülüğü getirilmesi*" olarak tanımlanabilir.[61] Ağ tarafsızlığı temel olarak ayrım gözetmeme ilkesine dayanmaktadır ve şebeke işletmecilerinin belirli içerikleri engelleme,

---

[59] Nispeten popülerliğini yitirse de Web 2.0 teknolojisinin temel taşları Extensible Markup Language (XML) ve Rich Site Summary (RSS) gibi etiket programlama dilleridir. Bu diller internet siteleri arasında otomatik içerik değişimi yapılmasını mümkün kılmaktadır. Örneğin, bir içerik sağlayıcısı kendi internet sitesini güncellediğinde güncellemiş olduğu içerik anında o sitenin XML veya RSS servisine abone olmuş tüm bağlantılarında görünmektedir. Bu şekilde, içerik otomatik olarak birçok internet sitesinde anında yayımlanabilmektedir.

[60] "Content distribution networks" olarak adlandırılan bu yöntemin avantajları, dezavantajları ve kapsamlı bir inceleme için bkz. **Fei, Zongming** (2001), "*A Novel Approach to Managing Consistency in Content Distribution Networks*", <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.19.4192&rep=rep1&type=pdf>

[61] **BTK**, "*Şebeke Tarafsızlığı*", <https://www.btk.gov.tr/uploads/pages/slug/sebeke-tarafsizligi.pdf>, s. 5; Bu ilke hakkında kapsamlı ve mukayeseli bir inceleme için bkz. **Keser Berber, Leyla/Sert, Elif/Atabey, Ayça** (2020) *Net Neutrality, Turkey, and Beyond - A Road Map for Net Neutrality Regulation in Turkey*, İstanbul, On İki Levha Yayıncılık.

önceliklendirme ve yavaşlatma gibi internetin açık, tarafsız ve erişilebilir doğasına aykırı kabul edilebilecek her türlü uygulamalarını yasaklamaktadır. Bu sebeple, ağ tarafsızlığı ilkesine ilişkin tartışmaların temel vurgusu internetin adil bir ortamda, eşit şartlarda, herkesin ulaşabileceği şekilde, açık ve tarafsız olmasına dayanır.[62] Ağ tarafsızlığı ilkesi şu şekilde özetlenebilir: Her bit[63] eşit doğar ve ağda eşit şekilde seyahat eder.

Ağ tarafsızlığı, internet yönetişiminin en çok tartışılan konularından biri olmaya devam etmektedir. Bunun nedeni, ağ tarafsızlığı ilkesine ilişkin tartışmaların tüketici hukuku, insan hakları hukuku ve rekabet hukuku başta olmak üzere farklı alanlarla ilgili olmasıdır. Ağ tarafsızlığı ilkesi gerek son kullanıcıların haklarının korunması gerek adil bir ortamda dijital ekosisteme dayanan ekonomik gelişim ve yenilikçiliğin teşvik edilmesi için oldukça önemlidir.

Ağ tarafsızlığı ilkesini anlamak için ağ tarafsızlığının temelini oluşturan ilkeleri anlamak gerekir. Bu ilkeler; teknoloji tarafsızlığı (*technology neutrality*), şeffaflık (*transparency*), ayrımcılık gözetmeme (*non-discrimination*), bloklamama (*non-blocking*), bant genişliğini daraltmama (*non-throttling*) ve önceliklendirmeme (*non-prioritization*) kurallarını kapsar. Bu temel ilkeler, ağ tarafsızlığına ilişkin hukuki düzenlemelerin oluşturulması noktasında oldukça önemlidir.

Teknoloji Tarafsızlığı: Teknolojiden bağımsız olarak aynı ilkelerin farklı teknolojilere ve cihazlara ayrımcılık gözetmeden uygulanması ilkesidir.[64] Teknoloji tarafsızlığı ilkesi, kullanılan teknoloji fark etmeksizin ağ tarafsızlığına ilişkin tüm ilkelerin eşit şekilde uygulanmasını gerektirir.

Şeffaflık: Şeffaflık ilkesi, trafik yönetim teknikleri ve uygulamalarının kullanıcılara şeffaf bir şekilde sunulmasını gerektirir. Ayrıca, bu ilke rekabete aykırı olan ayrımcılık uygulamalarını azaltacak ön koşullardan biri olarak

---

[62] **BTK**, "*Şebeke Tarafsızlığı*", s. 7.

[63] Bir bit, bilgisayarın işlediği en küçük veri parçasıdır. Bir harf 8 bitlik bir veriye tekabül etmektedir.

[64] Bkz. **Maxwell, Winston/Bourreau, Marc** (2014) "*Technology Neutrality in Internet, Telecoms and Data Protection Regulation*", <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2529680>

görülür.[65] Bu ilke kapsamında, internet servis sağlayıcıların, trafik yönetimine ilişkin uygulamalarını kullanıcıların anlayabileceği açıklıkta anlatması gerekmektedir. Şeffaflık ilkesi ve ağ tarafsızlığı ilkesi arasında sıkı bir ilişki vardır. Bu ilişki tüketicilerin korunması açısından oldukça önemlidir. Bunun sebebi, kullanıcıların ihtiyaçlarına ve beklentilerine en uygun internet servis sağlayıcısını seçme haklarına saygı duyulması ve kullanıcılarda yaratılan beklentinin karşılanmasının tüketicinin korunması noktasında önem arz etmesidir.[66] Özetle, şeffaflık ilkesi tüketici haklarına saygı duyulmasına ve şeffaf bir rekabet ortamı yaratılmasına katkı sağlar.

Ayrımcılık Gözetmeme: Ayrımcılık gözetmeme ilkesi ağ tarafsızlığı ilkesinin temel dayanağını oluşturur.[67] Bu ilke kapsamında, servis sağlayıcılardan yasal içerik, uygulama ve hizmetler için ayrım gözetmeyen bir muamelede bulunmaları beklenmektedir.

Bloklamama: Bloklama, şebeke işletmecilerinin, internet içerik sağlayıcılarına ait veriyi şebekeleri üzerinde taşımayı reddetmeleri durumudur ve ağ tarafsızlığı ilkesi kapsamında kabul görmemektedir.

Bant genişliğini daraltma: İnternet trafiğini yönetmek ve tıkanıklığı en aza indirmek için kullanılan bir teknik olan bant genişliği daraltma, belirli trafik türlerini düşürür ve bu nedenle içeriğin kalitesini olumsuz etkiler.

Önceliklendirmeme: Önceliklendirme, internet erişimi sağlayıcılarının, şebekelerinde tıkanıklık olması durumunda dahi bazı abonelerine sorunsuz veri iletimi garantisi vermesi anlamına gelmektedir.[68] Önceliklendirmeme ilkesi rekabet açısından değerlendirildiğinde şebeke işletmecilerinin, önceliklendirilmiş hizmeti sadece bazı abonelere değil tüm abonelere sunmaları gerekliliğini ifade eder. Bu ilke, ayrımcılık gözetmeme ilkesi ile yakından ilişkidir. Önceliklendirmeme ilkesi ayrımcılık gözetmeme ve adil bir rekabet ortamının sağlanması açısından çok önemlidir.

---

[65] **BTK**, "*Şebeke Tarafsızlığı*", s. 16.

[66] Bu konuda kapsamlı bir değerlendirme için bkz. **Gök, Mehmet Salih** (2012) *5651 sayılı Kanun ve Bilgi Güvenliği İlişkisi*, İstanbul, On İki Levha Yayıncılık, s.17-20.

[67] **Keser Berber, Leyla/Sert, Elif/Atabey, Ayça**, s. 20.

[68] **BTK**, "*Şebeke Tarafsızlığı*", s. 18.

Yukarıda belirtilen ilkelerin tümü, ağ tarafsızlığına ilişkin düzenlemelerin temel amacına ulaşmasında eşit derecede öneme sahiptir. Ancak bazı durumlarda, bu ilkeler farklı coğrafyalarda farklı şekillerde yorumlanabilir. Bu ilkeler ve istisnaları özellikle Avrupa Birliği'nin 25 Kasım 2015 tarihli ağ tarafsızlığına ilişkin düzenlemeleri kapsamında detaylı olarak belirlenmiştir.[69]

Ağ tarafsızlığı kapsamında tartışılan çok önemli diğer bir konu da son kullanıcılara ücretsiz/sponsorlu hizmet sunumu (*zero rating*) ile ilgilidir. Bu konuda farklı görüşler bulunsa da ağ tarafsızlığı ilkesinin ayrımcılığı kesin bir şekilde reddeden doğası ve temel dayanağı olan ayrımcılık gözetmeme ilkesi, *zero rating* de dâhil olmak üzere her türlü ayrımcılığın kesin bir şekilde yasaklanmasını destekler niteliktedir. Genel olarak, *zero rating* uygulaması, duruma göre farklılık gösteren ve hangi hizmetlerin ücretsiz olarak, hangi kapasiteyle, kime sunulup sunulmayacağının sorgulanmasını gerektiren, hem olumlu hem de olumsuz sonuçlar verme potansiyeline sahip bir uygulamadır.[70] *Zero rating* uygulamalarına izin verildiği belirli durumlarda ağ tarafsızlığı kapsamında diğer temel ilkelere uyum beklenmektedir.

Ağ tarafsızlığı ve *zero rating* programları arasında hassas bir ilişki vardır. Bu ilişkinin hassasiyeti; bu programların ağ tarafsızlığı üzerindeki etkisinin, *zero rating* tekliflerinin yaratacağı fırsat ve risklerin bu tekliflere yönelik farklı düzenleyici yaklaşımlar ile birlikte etraflıca değerlendirilmesini gerektirir.[71] *Zero rating* programlarının yanlış uygulanmasıyla önemli

---

[69] **European Commission**, "*Open Internet*" <https://ec.europa.eu/digital-single-market/en/open-internet-net-neutrality>; Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union, OJ L 310, 26.11.2015.

[70] Kapsamlı bir değerlendirme için bkz. **Belli, Luca** (2016) "*Net Neutrality Reloaded: Zero Rating, Specialised Service, Ad Blocking and Traffic Management Annual report of the UN IGF Dynamic Coalition on Net Neutrality*", <http://www.ict-21.ch/com-ict/IMG/pdf/Net-Neutrality.pdf>

[71] Bkz. **CERRE (Centre on Regulation in Europe)** (2018), "*A Fresh Look at Zero-Rating*" <https://cerre.eu/sites/cerre/files/CERRE_ZeroRating_FinalReport_0.pdf>

ölçüde zayıflatılabilecek ağ tarafsızlığı ilkelerinin başında ayrımcılık gözetmeme ilkesi gelir. Yanlış uygulamalar, ağ tarafsızlığı konusunun temel dayanağı olan ayrımcılık gözetmeme ilkesinin yanı sıra, ağ tarafsızlığının özü olan diğer temel ilkeler için de tehdit oluşturabilir. Öte yandan, *zero rating* programları kullanıcıya yukarıda belirtilen şeffaflık gibi diğer temel ilkelere uyumlu şekilde sunulduğunda *zero rating* uygulamasının ifade özgürlüğü ve medya çoğulculuğu gibi konularda olumlu etkisi olduğu savunulmaktadır.[72]

Farklı düzenleyici kurumlar, *zero rating* programlarına ilişkin farklı yaklaşımlara sahiptir. Ancak AB ve ABD'deki genel yaklaşım, *zero rating* programlarının durum bazında (*case by case)* değerlendirilmesi ve uygulanması yönündedir.[73] Avrupa Birliği'nin ağ tarafsızlığına ilişkin yasal düzenlemeleri ve kabul görmüş standart politika ve prosedürleri vardır.[74] Bunlar arasında en önemlisi 25 Kasım 2015 tarihli ve 2015/2120 sayılı Açık İnternet'e ilişkin düzenlemedir. Bu düzenleme her ne kadar ağ tarafsızlığı ilkeleri için ayrıntılı bir çerçeve oluşturmuşsa da uygulamada eksikliği hissedilen yasal boşluklar bıraktığı için eleştirilmiştir. Eleştirilere örnek olarak yasal düzenlemede *zero rating* programlarına ilişkin net bir çerçeve belirlenmemiş olması ve değerlendirmenin ulusal düzenleyici makamlara bırakılmış olması verilebilir.[75]

Öte yandan, politikaları şekillendirme veya internet altyapısı için temel kuralları belirleme konusundaki rollerine bağlı olarak uluslararası kuruluşların ağ tarafsızlığına yönelik çeşitli yaklaşımları vardır. Ağ tarafsızlığına ilişkin yasal düzenlemeler için ilkeler belirlemiş olan Ağ Tarafsızlığı Uzmanları Çalıştayı'nı (NN Experts Roundtable) başlatan Inter-

---

[72] **Keser Berber, Leyla/Sert, Elif/Atabey, Ayça**, s. 32.

[73] Karşılaştırmalı bir değerlendirme için bkz. **Keser Berber, Leyla/Sert, Elif/Atabey, Ayça**, s.6.

[74] Bkz. **BEREC** (2016) "*About BEREC's Net Neutrality Guidelines*", <https://berec.europa.eu/files/document_register_store/2016/8/NN%20Factsheet.pdf>; **BEREC** (2016) "*Guidelines on the Implementation by National Regulators of European Net Neutrality Rules*", <https://berec.europa.eu/eng/document_register/subject_matter/berec/download/0/6160-berec-guidelines-on-the-implementation-b_0.pdf>

[75] **Keser Berber, Leyla/Sert, Elif/Atabey, Ayça**, s. 32.

net Society'nin ağ tarafsızlığına ilişkin tartışmalarda aktif bir rolü vardır.[76] Bunun yanı sıra, ICANN gibi bazı kuruluşlar, internet altyapısının teknik tarafında kalan görevleri nedeniyle ağ tarafsızlığına ilişkin tartışmalarda aktif bir role sahip değildir.[77]

Son kullanıcılar başta olmak üzere, internet ekosisteminin diğer aktörlerinin bakış açısından ağ tarafsızlığı ilkesinin etraflıca değerlendirilmesi gerekmektedir. Zira ağ tarafsızlığına ilişkin tartışmalar; adil bir rekabet ortamının sağlanması, dijital ekonominin gelişmesi, inovasyonun teşviki gibi konular ile insan hakları hukuku, rekabet hukuku ve tüketici hukuku gibi alanlarda farklı paydaşlar üzerinde güçlü bir etkiye sahiptir. Ağ tarafsızlığı ilkesi gerek son kullanıcıların temel insan haklarının korunması gerek adil bir ortamda dijital ekosisteme dayanan ekonomik gelişim ve inovasyonun teşvik edilmesi için oldukça önemlidir. Bu sebeple, ağ tarafsızlığının sağlanamaması durumunda farklı paydaşlar üzerinde oluşabilecek etkilere ilişkin tartışmaları değerlendirmek önemlidir. Ağ tarafsızlığı ilkesine ilişkin tartışmalar çok yönlüdür. Bu, aynı zamanda adil rekabet, belirli içeriğin tercihli muamelesi, pazar gücünün değerlendirilmesi, mevcut düzenlemelerin eksiklikleri, hak temelli risk değerlendirmeleri ve daha pek çok kavrama ilişkin dinamikleri iyi anlamayı gerektirir.

Genel olarak, ağ tarafsızlığının korunması aynı zamanda son kullanıcıların haklarının, en başta ifade özgürlüğü olmak üzere temel insan haklarının ve açık internet erişiminin korunması anlamına gelmektedir.[78] Ağ tarafsızlığı ve açık internetin korunması, son kullanıcıların bilgiye erişme ve internet üzerinden paylaşım yapma, dolayısıyla ifade özgürlüğü haklarından yararlanmalarına olanak tanır. Bunlara ek olarak, ağ tarafsızlığı ilkesine saygı göstermek demek aynı zamanda işletmelerin tü-

---

[76] **Internet Society**, "Net Neutrality Experts' Roundtable Series", <https://www.internetsociety.org/tag/netneutrality/>

[77] Bkz. **Keser Berber, Leyla/Sert, Elif/Atabey, Ayça**, s. 64.

[78] Bkz. **Access Now** (2017) "*Net Neutrality Matters For Human Rights Across The Globe*" <https://www.accessnow.org/net-neutrality-matters-human-rights-across-globe/>; **Belli, Luca** (2016) "*End-to-End, Net Neutrality and Human Rights*": Belli, Luca; De Filippi, Primavera (Editörler) *Net Neutrality Compendium*, Cham, Springer.

keticilere ulaşmasını sağlamak ve böylece erişim, rekabet ve inovasyona destek olmak demektir. Özetle, ağ tarafsızlığının hem iş dünyasını, genel ekonomiyi, rekabet ve inovasyonu etkileyen boyutu hem de kullanıcıların haklarının korunması açısından son derece önemli bir rolü vardır. Ağ tarafsızlığına ilişkin yasal düzenlemeleri değerlendirirken ilkenin bu özellikleri göz önünde tutulmalıdır.

IV. İnternetin kullanım alanları

İnternetin kullanıldığı alanlar ve internete bağlı insan sayısı günden güne hızla artmaktadır. 2020 yılı itibarıyla beş milyarı aşkın kişinin interneti kullandığı tahmin edilmektedir. Özellikle, mobil aygıtlar üzerinden hızlı internet bağlantısına imkân veren 3G gibi teknolojilerin yaygınlaşmasıyla internet kullanıcısı sayısının daha da hızlı artması beklenmektedir. Benzer şekilde, eşyaların interneti (*internet of things*) denilen akıllı cihazların yaygınlaşması, ağa bağlı cihaz sayısının artışına ivme kazandırmaktadır.

İnternetin sosyal, ekonomik veya kültürel amaçlarla kullanım alanlarının artmış olması, internete olası bir müdahale durumunda bundan etkilenecek temel hak ve hürriyetlerin sayısını da aynı oranda artırmaktadır. Diğer bir deyişle, sadece iletişim hakkı ve bilgiye erişim hakkı değil, aynı zamanda özel hayatın gizliliği, din ve vicdan hürriyeti, düşünceyi açıklama ve yayma hakkı, bilim ve sanat hakkı, mülkiyet hakkı, maddi ve manevi varlığı geliştirme hakkı gibi birçok hak da bundan etkilenmektedir. İnternetin hayatın hangi alanlarında kullanıldığının tespit edilmesi, engelleme kararlarından etkilenen hakların belirlenmesini kolaylaştıracaktır.

İnternetin öne çıkan en temel özelliklerinden birisi, küresel bir kitle iletişim aracı olmasıdır. Televizyon veya radyo gibi klasik kitle iletişim araçları da geniş kitlelere ulaşmakla birlikte belirli bir coğrafyaya hitap ettikleri için sınırlılık taşırlar.[79] Oysa internet, coğrafi sınırlara veya belirli bir merkeze bağlı olmadan ortak bir standart dil üzerinden çalışma esasına göre tasarlanmıştır. Bu özelliği sayesinde internet herkese hitap

[79] **Falcıoğlu, Mete Özgür** (2004) *Karşılaştırmalı Hukuk ve (Amerikan Hukuku ve Viyana Antlaşması) Türk Hukukunda Elektronik Satım Sözleşmesi ve Kurulması*, Ankara, Yetkin, s. 49.

etmektedir. Ayrıca, internet diğer kitle iletişim araçlarından farklı olarak muhatap kitleyle etkileşimi mümkün kılmaktadır. Diğer bir deyişle internet, kullanıcılarını klasik kitle iletişim araçlarının aksine edilgen olmaktan çıkarıp etken bir hâle getirmektedir.[80]

İnternet bağlantı ücretlerinin ucuzlaması ve devletlerin interneti yaygınlaştırmak için yaptıkları özendirme ve destekleme faaliyetlerinin sonucunda internet kullanmak bir lüks olmaktan çıkmış ve artık temel bir yetenek hâlini almıştır. Bu sebeple, interneti kimler kullanıyor sorusuna tüketici bir yanıt vermek zorlaşmaktadır. Aynı şekilde, internetin etkileşimli özelliği, internetin kullanım alanları için tüketici bir listeleme yapmayı imkânsız kılmaktadır.

İnternet, ticaretin de önemli bir enstrümanıdır. Özellikle, internet üzerinden elektronik ticaretin yaygınlaşması internetin ticari amaçlı kullanımını ön plana çıkarmıştır. eBay üzerinden satılan ilk ürün, 1995 yılında satılmış kırık bir lazer sunum aletidir.[81] Sadece 2016 yılında eBay, 100 milyar dolara yakın bir ticaret hacmi gerçekleştirmiştir.

Öte yandan internet suçta araç olarak kullanılabileceği gibi internet üzerinden suç işlenmesi de mümkündür. Özellikle, terör örgütleri interneti propaganda, militanların eğitimi, haberleşme, bilgi toplama amacıyla yoğun bir şekilde kullanmaktadır. Başkasının ağına saldırı yapma ve verilerine müdahale etme gibi internete özgü suçların da işlenmesi mümkündür. Bazen bu tür suçlar büyük maddi zararlara sebep olabilmektedir. Örneğin, Filipinler'den yayılan "I love you" isimli bir virüsün dünya genelinde milyarca dolar zarara sebep olduğu tahmin edilmektedir.[82]

İnternet, devletler tarafından da çeşitli amaçlarla kullanılmaktadır. Devletler, vatandaşlarına hem hizmet sunmak hem de onları kontrol

---

[80] **Falcıoğlu**, s. 49.

[81] **Ryan**, s. 120.

[82] **Goldsmith, Jack L/Wu, Tim** (2006) *Who controls the Internet? Illusions of a borderless world*, New York, Oxford University Press; Bilişim sistemlerinin kötüye kullanılması ve bu şekilde haksız yarar ele edilmesine ilişkin kapsamlı bir çalışma için bkz. **Açıkgöz, Emre İkbal** (2020) *Bilişim Sistemi Aracılığıyla Haksız Yarar Sağlama Suçu (TCK m. 244/4)*, Ankara, Adalet Yayınevi.

etmek amacıyla interneti kullanabilmektedir. Öte yandan internet insan hakları alanında da örgütlenmek, ihlalleri takip etmek ve ortak eyleme geçmek için haberleşme gibi amaçlarla etkin şekilde kullanılmaktadır.

Yukarıda belirtildiği üzere, internetin hangi amaçlarla kullanıldığı sorusuna tam bir yanıt vermek mümkün değildir. Esasında internet hangi amaçla kullanılıyorsa kişi interneti o amaca göre yargılayacaktır.

İnterneti sadece müzik dinlemek için kullanan bir kişi bakımından internet, radyoyla veya bir MP3 çalar ile ikame edilebilecek bir şeydir. İnterneti yalnızca iletişim amacıyla kullanan bir kişi için ise internet sadece bir telefondur.

İnterneti çok amaçlı ve etkin şekilde kullanan bir hâkim veya savcıdan, sınırlama için en ölçülü kararı vermesi beklenebilir. İnterneti çok amaçlı ve etkin şekilde kullanan bir avukat, müvekkilinin internete yönelik taleplerine en makul çözümü bulmaya çalışabilir. İnterneti çok amaçlı ve etkin şekilde kullanan bir siyasetçi, internetin yaygınlaşması ve daha etkin kullanılmasını politik bir hedef yapabilir. İnterneti çok amaçlı ve etkin şekilde kullanan bir kamu görevlisi, internete yönelik müdahalede meşru menfaatin ne olacağını makul şekilde yorumlayabilir. Bu örnekler artırılabilir ve de genelleme yapmak her zaman mümkün olmayabilir. Ancak, internetin hayatın her alanına nüfuz etmesi ve eşyaların interneti başta olmak üzere kullanım amaçlarının çeşitlenmesi karşısında klasik yöntemlerle internete müdahale edilmesi zamanın ruhuna aykırı olacaktır.

İKİNCİ KISIM

İNTERNETİN ULUSLARARASI YÖNETİŞİMİ

§3. İNTERNETİN ULUSLARARASI YÖNETİŞİMİ

İnternet ağının tamamını kontrol eden tek bir otorite yoktur. İnternetin yönetimi ve işlerliği, çeşitli ulusal ve uluslararası kurumlar tarafından iş birliği içerisinde sağlanmaktadır. İnternet ağının tamamını yöneten tek bir otoritenin olmaması, internetin hukuksuz bir ortam olduğu anlamına gelmemektedir. İnternet ağının kontrolüne ilişkin ulusal ve uluslararası düzeyde birçok düzenleme bulunmaktadır. İnternette ayrıca *netiquette* olarak adlandırılan ve internet kullanıcılarının oluşturduğu bazı etik kurallar, sosyal normlar da bulunmaktadır.[83]

İnternetin teknik, hukuki ve politik açıdan yönetimi ve yönetişimi farklı kurum ve kuruluşlar tarafından gerçekleştirilmektedir. Bu kurum ve kuruluşların en önemlileri şunlardır:

I. Internet Corporation for Assigned Names and Numbers (ICANN)

İnternet Tahsisli Sayılar ve İsimler Kurumu (ICANN - Internet Corporation for Assigned Names and Numbers) 1998'de kurulan, kâr amacı gütmeyen bir kuruluştur. ICANN, faaliyetlerine ABD Ticaret Bakanlığı ile yapmış olduğu mutabakat çerçevesinde başlamıştır ve ilk ortaya çıktığı günden bu yana farklı kurum ve kuruluşlar tarafından yönetilen DNS sistemini küresel ölçekte yönetmektedir.[84]

---

[83] Bu tür kurallara uymak gönüllülük esasına bağlıdır. Robots.txt ve inAd.txt dosyalarının kullanılması buna güncel örnek olarak gösterilebilir. Yaygın *netiquette* ilkeleri için bkz. **IETF**, "*Netiquette Guidelines*", <http://www.ietf.org/rfc/rfc1855.txt>; Ayrıca bkz. **Kayany, Joseph M** (2004) "*Internet Etiquette (Netiquette)*": Bidgoli, Hossein (Editör) *The Internet encyclopedia - Volume 2*, Hoboken New Jersey, John Wiley & Sons.

[84] **NTIA (National Telecommunications and Information Administration)** "*Memorandum of Understanding Between the U.S. Department of Commerce and the Internet Corporation for Assigned Names and Numbers*", <http://www.ntia.doc.gov/ntiahome/domainname/icann-memorandum.htm>

ABD Ticaret Bakanlığı, Beyaz Kitap olarak da bilinen 5 Haziran 1998 tarihli politika açıklamasında, internetin uluslararası ticari kullanımının yaygınlaşması ve internetle ilgili kararlara uluslararası katılım taleplerinin artması gibi sebeplerle katılımcı yeni bir yapının oluşturulması gerektiğini belirtmiştir.[85] Bakanlık, DNS sisteminin rekabeti ve uluslararası katılımı artıracak şekilde özelleştirilmesine yönelik çalışmalarının bir neticesi olarak istikrar, rekabet, aşağıdan yukarıya özel sektör koordinasyonu ve temsil ilkeleri çerçevesinde 1998 yılında ICANN'i yetkilendirmiştir.[86]

Ana sözleşmesinde ICANN'in tüm internet topluluğunun faydasına faaliyet göstereceği belirtilmiştir:[87] ICANN, bu bağlamda zaman içerisinde geliştirdiği çoklu paydaş katılım modeli yöntemini kullanarak farklı paydaşların karar alma süreçlerine mümkün olduğunca katılmasını sağlamaya çalışmaktadır.

ICANN'in en önemli yetkisi, kök sunucular olarak da bilinen temel DNS sunucularının yönetimidir. İnternet trafiğini düzenleyen toplam 13 kök sunucu bulunmaktadır ve her bir sunucu ICANN tarafından akredite edilmiş farklı kurumlarca yönetilmektedir.[88] Türkiye özelinde İstanbul'da üç, Ankara'da ise iki yerel sunucu bulunmaktadır.[89] Bu sunuculardan en önemlisi ABD'de bulunan A sunucusudur. Ana ve yerel kök sunucular arasında herhangi bir ihtilaf doğması durumunda A sunucusunda bulunan kayıtlar geçerli kabul edilir.

ICANN, alan adları sisteminin teknik yönetimi, protokol parametrelerinin belirlenmesi ve kök sunucu sisteminin yönetimi işlevlerini de

---

[85] **NTIA**, "*Statement of Policy, Management of Internet Names and Addresses 63 Fed. Reg. 31741(1998)*", <https://www.ntia.doc.gov/federal-register-notice/1998/statement-policy-management-internet-names-and-addresses>

[86] ICANN'ın ortaya çıkışı ve işleyişi hakkında kapsamlı bilgi için bkz. **Soysal, Tamer** (2014) *İnternet Alan Adları Hukuku (Domain Name Law)*, Ankara, Adalet, s. 202-232.

[87] **ICANN**, "*Articles of Incorporation of Internet Corporation for Assigned Names And Numbers*" <https://www.icann.org/resources/pages/articles-2012-02-25-en>

[88] **Root Server Technical Operations Association** <http://www.root-servers.org>

[89] İstanbul: D, E, L; Ankara: I ve L yerel kök sunucuları. D, Marlyland Üniversitesi; E, NASA Ames Research Center; I, Netnod ve L yerel kök sunucusu ICANN tarafından yönetilmektedir.

koordine etmekle görevlendirilmiştir. Bu yetkileri sebebiyle internetin tamamını ICANN'in yönettiği şeklinde bir yanılgı vardır. ICANN'in internet ekosistemi üzerindeki etkisi yadsınamaz olsa da interneti ICANN tek başına yönetmemektedir. İlerleyen bölümlerde açıklanacağı üzere, farklı kurum ve kuruluşlar politik, teknik, hukuki ve sosyal roller üstlenerek internetin uluslararası, bölgesel ve yerel yönetimine katılmaktadır.

ICANN, bir kamu kurumu mudur? Hukuki olarak nasıl nitelendirilmelidir? ICANN, her ne kadar internetle ilgili çok kritik bir kamu hizmetini yerine getiriyorsa da kendini kâr amacı gütmeyen bir özel kuruluş olarak nitelendirmektedir. Faaliyetlerini ABD Ticaret Bakanlığıyla yaptığı yetkilendirme sözleşmesine göre sürdürdüğünü belirtmektedir. Bu konu Amerikan yargısında *McNeil v. VeriSign, Inc.* davasında tartışılmış ve ICANN'in bir kamu kurumu olmadığına hükmedilmiştir.[90] Hâliyle devletin, ifade özgürlüğü başta olmak üzere temel hak ve özgürlüklerin korunmasına ilişkin yükümlülüklerinden dolayı doğrudan sorumlu olmadığı belirtilmiştir.

ICANN'in bir kamu kurumu olmaması, temel hak ve hürriyetlerin korunmasıyla ilgisi bulunmadığı manasına gelmemektedir. ICANN'in faaliyetlerinin mahremiyet ve kişisel verilerin korunması hakkı, örgütlenme hakkı, ekonomik, sosyal ve kültürel haklar, ifade özgürlüğü, internette siber güvenlik hakkı, katılım, kapsama, eşitlik ve ayrımcılık yapmama, hak arama başta olmak üzere insan hakları bağlamında muhtelif etkileri vardır.[91] Örneğin, tüm kelime ve isimlerin alan adlarında kullanılabilmesi hakkı, ifade özgürlüğü; alan adı sisteminin güvenliğinin sağlanması amacıyla kullanılan DNSSEC, internette siber güvenlik hakkı; WHOIS politikası, mahremiyet ve kişisel verilerin korunması hakkı; IP adreslerinin koordinasyonu ve dağıtımı ekonomik, sosyal ve kültürel haklar; uyuşmazlık çözüm mekanizmaları ise hak arama özgürlüğüyle ilişkilidir.

---

[90] Dava için bkz. **Nunziato, Dawn C** (2009) *Virtual freedom: Net Neutrality and Free Speech in the Internet age*, Stanford, Stanford Law Books, s. 108-109.

[91] **ICANN**, "*Scoping the relation between ICANN and Human Rights*" <https://community.icann.org/download/attachments/53772653/ICANN%20and%20Human%20Rights%20Jan2018.pdf>

II. Internet Assigned Numbers Authority (IANA)

İnternet Tahsisli Sayılar Otoritesi (IANA - Internet Assigned Numbers Authority), ICANN ile koordinasyon içerisinde IP adreslerinin yönetimini gerçekleştirmek ve ICANN gibi bağımsız olarak faaliyet göstermek üzere ABD tarafından yetkilendirilmiş bir kuruluştur.[92] IANA, internetin temel fonksiyonlarının yerine getirilmesinden sorumludur.

IANA, 1972 yılında Birleşik Devletler Savunma Bilgi Sistemleri Ajansı (DARPA - US Defence Information Systems Agency) tarafından oluşturulmuştur. Belirli tarihlerde yenilenen sözleşmeler kapsamındaki yetkilendirmeyle faaliyetlerini sürdürmektedir.[93] Temel faaliyet alanları DNS kök sunucusu ile .int ve .arpa alan adlarını yönetmek; IP adreslerinin (IPv4 ve IPv6) küresel havuzu ile AS numaralarını (Autonomous System Numbers - Otonom Sistem Numaraları)[94] kontrol etmek ve bunları Bölgesel İnternet Tescil Kuruluşlarına (Regional Internet Registries) dağıtmak; IP numaralama sistemlerini standart belirleyen kuruluşlarla uyumlu şekilde yönetmektir.

IANA, IP adreslerinin küresel koordinasyonunu sağlamakta ve bu adresleri Bölgesel İnternet Tescil Kuruluşlarına ihtiyaçlara ve küresel politikalara uygun şekilde atamaktadır. IANA, her bir tescil kuruluşuna atanan tüm IP ve AS numara bloklarının kaydını tutmaktadır. Her bir tescil kuruluşu bölgesel ihtiyaçlarına göre taleplerini IANA'ya iletmekte ve tahsis bu şekilde gerçekleşmektedir. Tahsis edilen bu IP adresleri Bölgesel İnternet Tescil Kuruluşları tarafından ya İSS'lere ya da varsa Ulusal İnternet Tescil Kuruluşlarına atanmaktadır.

Bölgesel İnternet Tescil Kuruluşları belirli bir bölgenin IP adres aralıkları ve AS numaralarını yöneten ve tescil eden, birbirleriyle eş güdüm içerisinde faaliyet gösteren, kâr gütmeyen kuruluşlardır.

---

92 **IANA**, "*About the Internet Assigned Numbers Authority*" <http://www.iana.org/about/>

93 **Soysal**, s. 232.

94 AS numarası tek ve açıkça tanımlanmış bir *routing* politikası olan bir veya birden daha fazla ağ yöneticisi tarafından işletilen IP ağ gruplarıdır. Daha fazla bilgi için bkz. **IETF**, "*Guidelines for creation, selection, and registration of an Autonomous System (AS)*" <https://tools.ietf.org/html/rfc1930>

Mevcut Bölgesel İnternet Tescil Kuruluşları ve yönettikleri bölgeler şöyledir:

AFRINIC **:** Afrika, Hint Okyanusu'nda belirli bölgeler

APNIC **:** Asya'da belirli bölgeler, Okyanusya'da belirli bölgeler

ARIN **:** Kanada, birçok Karayip ve Kuzey Atlantik adası, ABD

LACNIC **:** Latin Amerika, Karayipler'de belirli bölgeler

RIPE NCC **:** Avrupa, Orta Doğu, Orta Asya

ICANN ve IANA tarafından belirlenen ve uygulanan esaslara göre IP adresleri, bloklar hâlinde Bölgesel İnternet Tescil Kuruluşları (RIR - Regional Internet Registry) tarafından Yerel İnternet Tescil Kuruluşlarına (LIR - Local Internet Registry) tahsis edilmekte ve bu kuruluşlarca aralarındaki özel anlaşmalarla internet hizmet sağlayıcılara verilmektedir.

III. Internet Engineering Task Force (IETF)

Internet Engineering Task Force (IETF), internetin temel teknik standartlarının oluşması sürecine aktif katkı sağlayan önemli bir oluşumdur.[95] IETF, bir şirket olmadığı gibi şirkete benzer ticari yapısı da yoktur; tamamen kendine özgü kurallarla ve prensiplerle faaliyet göstermektedir. Faaliyetlerine katılımda gönüllülük esası geçerlidir. IETF'nin temel felsefesini, David Clark'ın şu sözü özetlemektedir: "*Biz kralları, başkanları ve oylamayı reddediyoruz. Biz genel konsensüse ve çalışan koda inanıyoruz.*"[96]

IETF interneti yönetmemekte, bu konuda emredici kurallar ihdas etmemektedir. Yapmış olduğu çalışmalar genellikle bir standart hâline dönüşse de IETF, bir standardizasyon kuruluşu da değildir. IETF, gönüllü olarak standartlar geliştirmekte ve bu standartlar çoğu zaman kabul

[95] **Hoffman, Paul**, "*The Tao of IETF: A Novice's Guide to the Internet Engineering Task Force*", <https://www.ietf.org/tao.html>

[96] Orijinal hali: "We reject: kings, presidents and voting. We believe in: rough consensus and running code." bkz. **Resnick, Pete** "*On Consensus and Humming in the IETF*", <https://tools.ietf.org/html/rfc7282>

görmektedir. Ancak, IETF ne interneti kontrol etmekte ne de bu bağlamda bir kolluk faaliyeti icra emektedir. Esasında, bu aşağıdan yukarıya katılımcı modeli sayesinde IETF'nin yaygın kabul görmesi nedeniyle IETF ile Uluslararası Standartlar Teşkilatı (ISO - International Organization for Standardization) arasında ciddi politik çatışmalar da yaşanmıştır.[97]

İlk IETF toplantısı Ocak 1986'da San Diego'da gerçekleşmiştir. Avrupa'daki ilk toplantısını ise Temmuz 1993'te Hollanda'nın Amsterdam şehrinde yapmıştır. Hâlihazırda IETF toplantıları Amerika ve Avrupa'nın dışında Asya'da da gerçekleştirilmektedir. IETF şu an 115 çalışma grubuyla internetin teknik alanındaki çalışmaları yönlendirmektedir.[98]

Bu çalışma gruplarında herkesin bir konuyu "Request for Comments (RFC)" olarak adlandırılan süreci başlatarak gündeme getirmesi ve tartışmaya açması mümkündür. Bu süreçte ne nitelikli çoğunluk ne de oy birliği ile karar verilmektedir. "Kaba konsensüs" (*rough consensus*) olarak ifade edilen kritik kabul eşiği veya genel temayül, her konuda farklı şekilde ortaya çıkabilmektedir. Kaba konsensüs, basit olarak, en güçlü itirazların yersiz veya yanlış olduğu konusunda katılımcıların çoğunun tatmin edilmesine kadar tartışılması şeklinde tanımlanabilir. IETF'nin yönetişim modeli, bu bağlamda doğrudan ve katılımcı demokrasinin pek çok örneğini bünyesinde barındırmaktadır.

Bir konunun RFC olarak tartışmaya açılması veya kabul edilmesi onu kendiliğinden standart hâline getirmemektedir.[99] Her bir RFC sürecinde, IANA ile uyumluluk, güvenlik ve fikrî mülkiyet haklarına uyum gibi kriterler de ayrıca gözetilmektedir.[100] Özellikle mevcut patentlerle uyum konusu önem taşımaktadır.[101] IETF'nin amacı, geliştirmiş olduğu

---

[97] **DeNardis, Laura** (2009) *Protocol politics: the globalization of Internet governance*, Cambridge, MIT Press, s. 69.

[98] **IETF**, "*Working Group Guidelines and Procedures*" <https://tools.ietf.org/html/rfc2418>

[99] **Huitema, C/Postel, J/S. Crocker,** "*Not All RFCs are Standards*" <https://tools.ietf.org/html/rfc1796>

[100] Fikri mülkiyet konusu için bkz. **Bradner, S**, "Intellectual Property Rights in IETF Technology" <https://tools.ietf.org/html/rfc3979>

[101] **Hoffman, Paul,** "*The Tao of IETF: A Novice's Guide to the Internet Engineering Task*

standartların mümkün olan en geniş şekilde kullanılmasıdır. IETF "*mümkün olan yerde patentsiz iyi teknolojiyi kullan*" ilkesini benimsemektedir.

IETF kapsamındaki bir RFC'ye normatif dayanak verilmesi ve bunun örnek uygulama kabul edilmesi suretiyle de bazı uygulamalar geliştirilebilmektedir. Örneğin, Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'in 7. maddesi, İnternet Mühendisliği Görev Grubu Yorum Talebi olarak adlandırdığı 3647 numaralı RFC'ye bağlayıcılık kazandırmış ve elektronik imza hizmet sağlayıcılarının, sertifika ilkeleri ile sertifika uygulama esaslarını bu RFC'ye uygun olarak hazırlamasını zorunlu kılmıştır.[102] Benzer şekilde, Kayıtlı Elektronik Posta Rehberi ve Kayıtlı Elektronik Posta Hesabı Adreslerine İlişkin Tebliğ'in 17. maddesi uyarınca, kayıtlı elektronik posta hesabı adreslerinin IETF RFC 2821'e ve IETF RFC 2822'ye uygun oluşturulması esastır.[103]

IV. Internet Research Task Force (IRTF)

Internet Research Task Force (IRTF), IETF ile eş güdümlü çalışan bir oluşumdur. IETF, kısa vadeli mühendislik ve standardizasyon süreçleriyle ilgilenirken, IRTF daha ziyade internet protokolleri, internet uygulamaları mimarisi ve internet teknolojisi alanlarında uzun vadeli araştırma konularıyla ilgilenmektedir.[104] IRTF bünyesindeki araştırma grupları şunlardır:

- CFRG - Crypto Forum Research Group
- GAIA - Global Access to the Internet for All Research Group
- HRPC - Human Rights Protocol Consideration Research Group
- ICCRG - Internet Congestion Control Research Group
- ICNRG - Information-Centric Networking Research Group

Force".

[102] Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ RG 06.01.2005/25692.

[103] Kayıtlı Elektronik Posta Rehberi ve Kayıtlı Elektronik Posta Hesabı Adreslerine İlişkin Tebliğ RG 16.05.2012/28294.

[104] **Internet Research Task Force** <https://irtf.org>

- MAPRG - Measurement and Analysis for Protocol Research Group
- NFVRG - Network Function Virtualization Research Group
- NMRG - Network Management Research Group
- NWCRG - Network Coding Research Group
- T2TRG - Thing-to-Thing Research Group

IRTF; kriptoloji, herkes için internete küresel erişim, insan hakları protokolünün gözetilmesi, internet yoğunluk kontrolü, bilgi temelli ağlar, protokoller için ölçüm ve analiz, ağ fonksiyonu görselleştirme, ağ yönetimi, ağ kodlama ve eşyaların interneti gibi geniş bir konu yelpazesinde araştırma faaliyetlerini sürdürmektedir.[105]

V. Internet Architecture Board (IAB)

Internet Architecture Board (IAB), internetin temel mimarisini gözeten bir oluşumdur.[106] IAB, 1983 yılında, internetin genel olarak ABD'nin bir araştırma projesi olduğu dönemlerde kurulan Internet Activities Board'un halefidir. IETF gibi IAB çalışmaları da gönüllülük esasına dayanır.

Genel olarak, IAB bütüncül teknik öneriler getirmeyi hedeflemez, bunun yerine internetin ve protokollerinin düzgün işleyebilmesi için gerekli olan genel teknik ilkeleri tanımlamaya çalışır.[107] IAB'nin, politik

[105] Daha önceki çalışma grupları: Authentication Authorisation Accounting Architecture, Anti-Spam, Building Differentiated Services, Delay-Tolerant Networking, End Middle End, End-to-End, Group Security, Host Identity, Internet Digital Rights Management, Information Infrastructure Architecture, Internet Measurement, Interplanetary Internet, Internet Resource Discovery, IP Mobility Optimizations, Network Complexity, Namespace, Peer-to-Peer, Public Key Next-Generation, Privacy and Security, Reliable Multicast, Routing, Scalable Adaptive Multicast, Software-Defined Networking, Searchable Internet Resource Name, Services Management, Transport Modeling, Virtual Networks. Eski ve yeni tüm çalışma grupları için bkz. **IRTF**, "*Current Research Groups*" <https://irtf.org/groups>

[106] **Carpenter, B,** "Charter of the Internet Architecture Board (IAB)" <https://tools.ietf.org/html/rfc2850>

[107] **Internet Architecture Board**, "*Description*" <https://www.iab.org/about/

konulardaki sınırlı rolü dışında teknik veya ticari konularda resmî hiçbir görevi yoktur. IAB, içinden doğduğu IETF ile eş güdümlü çalışarak IETF bünyesindeki çalışma gruplarının tutarlılığı ve bütünlüğünü gözetir.[108] Aynı doğrultuda, IRTF'nin çalışmaları da IAB'nin denetim ve gözetimi altında yürütülür.

IAB ayrıca IETF'nin standartlarla ilgili kararlarına karşı itiraz makamıdır. Standartlar sürecinin düzgün işletilmediğine dayanılarak IAB'ye hem usuli hem de teknik gerekçelerle itirazda bulunulabilir. IAB'nin RFC sürecinin editoryal yönetimi ve yayını ile bazı internet tahsis numaralarından da sorumluluğu söz konusuyken bu yetkilerini sırasıyla RFC Editor ve IANA'ya devretmiştir. Hâlihazırda bu konularda sadece denetim yetkisiyle hareket etmektedir.

VI. Internet Governance Forum (IGF)

Birleşmiş Milletler Genel Sekreterliğinin himayesinde ve Uluslararası Telekomünikasyon Birliğinin (ITU) öncülüğünde 10-12 Aralık 2003 tarihlerinde Cenevre'de düzenlenen Dünya Bilgi Toplumu Zirvesi'nde, internet yönetişimi sorunu önemli bir tartışma konusu olmuştur. Ancak bu konuda terminolojik düzeyde bile fikir birliğinin olmaması sebebiyle somut bir ilerleme kaydedilememiştir. Zirvede temel olarak, internet yönetişiminde Birleşmiş Milletlerin aktif bir rol alması gerektiğine yönelik görüşler öne çıkmıştır.

Zirve sonucunda kabul edilen Eylem Planı'nda, Birleşmiş Milletler Genel Sekreterliğinden internet yönetişimi için bir çalışma grubu kurması talep edilmiş; bu grubun, gelişmiş ve gelişmekte olan ülkelerin hükûmet, özel sektör ve sivil toplum temsilcileri ile hükûmetler arası ve uluslararası organizasyonların tam ve aktif katılımını mümkün kılacak açık ve kapsayıcı bir süreçle oluşturulması istenmiştir. Bu çalışma grubundan, 2005 yılına kadar internet yönetişimi alanında araştırmalar yapması ve eylemler için tekliflerde bulunması beklenmiştir. En önemlisi, bu

description/>

[108] **Galvin, J**, "*IAB and IESG Selection, Confirmation, and Recall Process: Operation of the Nominating and Recall Committees*" <https://www.ietf.org/rfc/rfc2727.txt>

çalışma grubundan internet yönetişimine ilişkin bir tanım geliştirmesi istenmiştir.Working Group on Internet Governance (WGIG) isimli bu çalışma grubunun hazırladığı raporda internet yönetişimi şu şekilde tanımlanmıştır:

"İnternet yönetişimi; devletler, özel sektör ve sivil toplum tarafından, kendi rolleri, ortak ilkeleri, normları, kuralları, karar alma usulleri ile internetin oluşumunu ve kullanımını şekillendiren programların geliştirilmesi ve uygulanmasıdır." [109]

Yönetişim kavramı, OECD tarafından "*bir ülkenin ekonomik ve sosyal kaynaklarının yönetiminde sahip olunan güç ve yetkilerin kullanımı*" olarak tanımlanmıştır.[110] Söz konusu kavram konusunda üzerinde uzlaşılmış standart bir tanım bulunmadığı için yönetişimin ne olduğu ve kapsamı her düzlemde ve konuda farklı şekilde somutlaşmaktadır.

WGIG'ye göre internet yönetişiminde dikkate alınması gereken politik alanlar şunlardır:[111]

- Kök alan dosyaları ve sisteminin yönetimi
- Ara bağlantı maliyetleri
- İstenmeyen e-posta
- Küresel politika oluşumuna etkin katılım
- Kapasite geliştirme
- Alan adlarının tahsisi
- IP adresleme
- Fikrî mülkiyet hakları
- İfade hürriyeti
- Veri koruma ve mahremiyet hakları
- Tüketici hakları
- Çok dillilik

---

[109] **WGIG** (2005) "*Report of the working group on Internet governance*", <http://www.wgig.org/docs/WGIGREPORT.pdf>, s. 4.

[110] **OECD**, "*Governance*" <https://stats.oecd.org/glossary/detail.asp?ID=7236>

[111] **WGIG**, s. 5-8.

WGIG, ayrıca, detaylarına girmeksizin yakınsama ve gelecek nesil ağlar ile elektronik ticaret konularına da dikkat çekmiştir. WGIG, internetin uluslararası teknik ve politik yönetişimi için radikal sayılacak dört öneride bulunmuştur. Özellikle hiçbir devletin internetin uluslararası yönetişiminde üstün bir rolü olmaması gerektiğini; yönetişim faaliyetini sürdürecek teşkilatın çok taraflı, şeffaf, demokratik ve devletler ile özel sektörü, sivil toplumu ve uluslararası organizasyonları kapsayıcı ve katılımcı olması gerektiğini belirtmiştir.[112] WGIG, bu bağlamda, Küresel İnternet Konseyi (Global Internet Council), Dünya İnternet Tahsisli Sayılar ve İsimler Kurumu (WICANN - World Internet Corporation for Assigned Names and Numbers) ve Küresel İnternet Yönetişimi Forumu (GIGF - The Global Internet Governance Forum) gibi kurumsal yapıların da tesis edilmesini önermiştir.

Birleşmiş Milletler nezdinde bu tür tartışmaların yapılmasını gereksiz bulan ve her şeyin yolunda olduğunu düşünenlerin yanı sıra her şeyin yolunda olmadığını, tek ve aşikâr çözümün internet üzerinde daha büyük bir devletler arası kontrol olduğunu düşünenler de bulunmaktadır.[113] Bu doğrultuda, WGIG tarafından yapılan çalışma en azından usuli katkı olarak, çoklu paydaşlı iş birliğinin faydalarını göstermiş, Dünya Bilgi Toplumu Zirvesi müzakerelerini kolaylaştırmış, internet yönetişimi tartışmalarına kamusal katılımı sağlamıştır. Esaslı katkı olarak, internet yönetişiminin niteliği ve kapsamını açıklığa kavuşturmuş, hem yatay hem de dikey seviyede bütüncül değerlendirmeler yapmış, temel kaynakların denetimi için internetin temel kaynaklarının yönetişimine ilişkin küresel tartışmalara yoğunlaşmaya olanak tanıyan dört model sunmuş ve internetle ilgili kamusal politikaların koordinasyonu ve tartışılmasından sorumlu, devletlerin, özel sektörün ve sivil toplumun eşit koşullarla katıldığı İnternet Yönetişimi Forumu (IGF - Internet Governance Forum) isimli bir forumun oluşturulmasını önermiştir.[114]

---

[112] **WGIG**, s. 12.

[113] **Drake, William J** (2005) *Reforming Internet governance: perspectives from the Working Group on Internet Governance (WGIG)*, New York, United Nations Information and Communication Technologies Task Force, s. 249.

[114] **Drake**, s. 249-265; **WGIG**, s. 16.

Dünya Bilgi Toplumu Zirvesi'nin II. Aşaması ise 16-18 Kasım 2005 tarihleri arasında Tunus'ta yapılmıştır.[115] Zirveye 175 ülke resmî katılım sağlamıştır. Zirvede, Avrupa Birliği radikal bir teklifte bulunmuş ve alan adı yönetiminin ICANN ve ABD Ticaret Bakanlığından alınıp Birleşmiş Milletler nezdinde faaliyet gösterecek bir ihtisas kurumuna aktarılmasını önermiştir.[116] Bu teklif ABD'nin direnciyle karşılaşmış ancak artan uluslararası baskıyı dindirmek ve konunun uzun vadeli tartışılmasını sağlamak amacıyla İnternet Yönetişimi Forumunun bir diyalog kanalı olarak kullanılması kararlaştırılmıştır.[117]

IGF, internete yönelik politikaların tartışıldığı, çoklu paydaş katılım modeline dayalı bir platformdur. IGF'nin amacı, en iyi uygulamaların ve tecrübelerin paylaşılmasına fırsat oluşturmak, güncel sorunları tespit etmek ve bunları hem ilgili makamların hem de kamunun dikkatine sunarak internet yönetişimi için kapasite geliştirilmesine katkı sunmaktır.[118]

IGF, internet yönetişiminin en etkin şekilde işletildiği, teknik ve politik alanlardan çok geniş bir yelpazeden paydaşların katıldığı bir forumdur. IGF sürecinin, küresel politik sorunların konuşulması, politik süreçlerin yönetimi, politik konuların hem bilimsel hem de teknik boyutlarıyla uğraşılması ve artan katılımcılık ile kapsayıcılık gibi alanlarda oluşturduğu tecrübe ve bu bağlamdaki katkıları internet ekosisteminin gelişiminde önemlidir.[119]

---

[115] Dünya Bilgi Toplumu Zirvesi <http://www.bilgitoplumu.gov.tr/uluslararasi-calismalar/dunya-bilgi-toplumu-zirvesi/ikinci-asama-tunus/>

[116] **Goldsmith/Wu**, s. 171.

[117] **International Telecommunication Union** (2005), *"Report of the Tunis phase of the World Summit on the Information Society, Tunis, Kram Palexpo, 16-18 November 2005 WSIS-05/TUNIS/DOC/9(Rev.1)-E"*, <http://www.itu.int/net/wsis/docs2/tunis/off/9rev1.pdf>, s. 17.

[118] **IGF**, *"About IGF FAQs"* <http://www.intgovforum.org/multilingual/content/about-igf-faqs>; IGF, 2014 yılında Türkiye'nin ev sahipliğinde İstanbul'da gerçekleşmiştir. Diğer IGF toplantıları şu şehirlerde yapılmıştır: Guadalajara (2016), João Pessoa (2015), İstanbul (2014), Bali (2013), Bakü (2012), Nairobi (2011), Vilnius (2010), Şarm El-Şeyh (2009), Hyderabad (2008), Rio de Janeiro (2007), Atina (2006).

[119] **Kurbalija, Jovan** (2010) *An introduction to Internet Governance*, Msida, Malta, Diplo Foundation, s. 180.

VII. International Organization for Standardization (ISO)

Uluslararası Standartlar Teşkilatı (ISO - International Organization for Standardization), Uluslararası Elektroteknik Komisyonunun çalışma sahasına giren elektrik ve elektronik mühendisliği konuları dışında bütün teknik ve teknik dışı dallardaki standartların belirlenmesi çalışmalarını yürütmek gayesiyle 1946'da Cenevre'de kurulan uluslararası teşkilattır.[120] ISO üyesi devlet sayısı 162'dir.

ISO'nun internet ekosistemi açısından önemi, yayımlamış olduğu ISO 3166 standardıdır.[121] Söz konusu standart, ülkelerin iki harfli (*alpha-2*), üç harfli (*alpha-3*) ve üç haneli numerik kodlarını (*numeric-3*) düzenlemektedir.[122] Standart, ülke adları ve uzantılardaki değişiklikleri yansıtmak amacıyla düzenli olarak güncellenmektedir.

ISO 3166 standardı, üst düzey alan adlarının ülke kodlarının tanımı için ilk defa 1984 tarihli RFC 920'de zikredilmiş ve 1986'dan bu yana da kullanılmaktadır.[123] Standardın yönetimi ve güncellemesi ICANN'in de aralarında olduğu 14 kuruluşun temsilcisinden oluşan ISO 3166 Maintenance Agency (ISO3166/MA) yönetim temsilciliği tarafından sürdürülmektedir.[124]

VIII. Internet Society (ISOC)

1980'li yılların başından itibaren internetin, ana araştırma amaçlarını aşarak genel bir kullanıcı kitlesine ulaşması ve ağda ticari aktivi-

---

[120] **ISO**, "*About ISO*" <http://www.iso.org/iso/home/about.htm>

[121] **ISO**, "*ISO 3166-1:2013 Codes for the representation of names of countries and their subdivisions*" <http://www.iso.org/iso/home/standards/country_codes.htm>

[122] **ISO**, "*ISO Country codes*" <https://www.iso.org/obp/ui/>

[123] **Postel J/Reynolds J**, "*Domain Requirements*", <https://tools.ietf.org/rfc/rfc920.txt>; Ayrıca bkz. **IETF**, "*Domain Administrators Guide*", <https://tools.ietf.org/html/rfc1032>; **IETF**, "*Domain Name System Structure and Delegation*", <https://www.rfc-editor.org/rfc/rfc1591.txt>

[124] **ICANN**, "*ICANN and the International Organization for Standardization (ISO)*", <https://www.icann.org/resources/pages/icann-iso-3166-2012-05-09-en>

telerin artmasıyla beraber, internetin dağınık sosyal topluluğunu bir araya getirmek amacıyla 1991 yılında, kâr amacı gütmeyen bir oluşum olan Internet Society (ISOC) kurulmuştur.[125] ISOC, hem IETF hem de Internet Architecture Board'u kapsayan kurumsal bir şemsiye olarak tesis edilmiştir.[126] ISOC, bilgisayar ağlarının gönüllü iş birliğini küresel bir araştırma-geliştirme bilgi ve iletişim altyapısına dönüştürmek felsefi amacıyla kurulmuştur.[127] ISOC, bir bakıma internet yönetişiminin sivil toplum kanadını temsil etmektedir.

IX. World Wide Web Consortium (W3C)

World Wide Web Consortium (W3C), web standartlarını geliştiren bir uluslararası topluluktur. Topluluğun geçmişi Tim Berners-Lee'nin 1989 yılında CERN'de "World Wide Web"i geliştirdiği döneme dayanır.[128] Tim Berners-Lee "World Wide Web" konseptini geliştirmiş ve bu amaçla kullanılan ilk sunucu ile kullanıcı programını yazmıştır. Ayrıca, belgelerin birbiriyle bağlantı kurmasına olanak tanıyan belge biçimlendirme dili olan HyperText Markup Language (HTML) dilinin ilk versiyonunu yazmış; URL, http ve HTML için temel çerçeveyi geliştirmiştir.[129] W3C tarafından geliştirilmiş HTML dilinin 5. versiyonu (HTML5), 2017 itibarıyla bu dilin en yaygın şekilde benimsenmiş ve güncel versiyonudur.

Tim Berners-Lee, Ekim 1994'te Massachusetts Institute of Technology, Laboratory for Computer Science bünyesinde W3C topluluğunu kurmuştur. W3C, teknik standartları ve yönergeleri mümkün olan en geniş konsensüsle oluşturmaya çalışmaktadır. W3C topluluğunda ilginç tartışmalar da yaşanmıştır. Örneğin, 2019 yılında Google, mahremiyet ihlallerine yönelik genel bir engelleme getiren bir tasarıya karşı çıkarken

---

[125] **ISOC**, "*Brief History of the Internet*" <http://www.internetsociety.org/sites/default/files/Brief_History_of_the_Internet.pdf>, s. 12.

[126] **Ryan**, s. 100.

[127] **ISOC**, "*Internet Society Founding - An Oral History of the Internet Society's Founding*", <https://www.internetsociety.org/internet-society-founding>

[128] **Berners-Lee, Tim**, "*Information Management: A Proposal*", <https://www.w3.org/History/1989/proposal.html>

[129] **W3C**, "*Facts About W3c*", <https://www.w3.org/Consortium/facts>

yirmi dört farklı kuruluş bu yönde bir standardın geliştirilmesi için olumlu oy kullanmıştır.[130] Mahremiyet korumasının bir internet standardı hâline gelmesi durumunda bilhassa çevrim içi davranışsal reklamcılık ve çerezler alanında önemli kırılmaların olması kaçınılmazdır.

X. Internet Network Operators' Groups

İnternet Ağ İşletmecileri Grupları (NOGs - Internet Network Operators' Groups), internet ağ işletmecilerinin, karşılıklı menfaatlerini tartışmak için oluşturdukları, resmî olmayan, ülke bazlı veya bölgesel gruplardır.[131] Bu grupların üyeleri genellikle İnternet Servis Sağlayıcıları, İnternet Değişim Noktaları (IXP), Bölgesel Alan Adı Tescil Kuruluşları, güvenlik toplulukları, IPv6, alan adı ve kök sonucu işletmecileri ve diğer ağ işletmecileri gibi kuruluşlardır. Bu grup içerisindeki tartışmalar internetin sağlam, güvenli ve stabil şekilde çalışmasının devamı için önemlidir. Bu tür tartışmalar ayrıca ağ uzmanlarının ve araştırma toplulukları ile teknik toplulukların birbirleriyle haber ve güncellemeleri paylaşmaları, en iyi uygulamaları birbirlerine aktarmaları, yeni teknolojileri veya protokolleri tartışmaları, öğretmeleri ve birbirlerinden öğrenmeleri için fırsatlar sunmaktadır. [132]

XI. İnternet yönetişiminin geleceği

Hangi ülkeye kaç tane IP adresi tahsis edileceği, hangi IP adresi aralıklarının kullanılabileceği, hangi alan adlarının hangi şartlarda kayıt edilebileceği, hangi üst düzey alan adlarının oluşturulacağı ve bunları kimin kontrol edeceği sorunu, bazıları tarafından telefon numaralarının veya trafik plakalarının tahsisi gibi basit bir teknik sorun olarak görül-

---

[130] **Vynck, Gerrit**, "*Google Blocks Privacy Push at the Group That Sets Web Standards*" <https://www.bloomberg.com/news/articles/2019-09-24/google-blocks-privacy-push-at-the-group-that-sets-web-standards>

[131] Internet Network Operations' Groups <http://www.senki.org/network-operations-groups-meeting/>

[132] Internet Network Operations' Groups <http://www.senki.org/network-operations-groups-meeting/>

mektedir.[133] Ancak, internetin kullanım alanlarının artması, milyarlarca dolarlık elektronik ticarete ev sahipliği yapması, alan adlarının değerlenmesi ve çeşitli fikrî mülkiyet sorunlarına yol açması, internet üzerinden veri iletişiminin ulusal güvenliğin bir parçası olarak görülmesi gibi sebeplerle alan adları ve IP adreslerinin yönetimi büyük bir menfaat çatışması doğurmaktadır.[134]

İnternet alan adları ve IP numaralandırma politikalarının kontrolü sorunu sadece devletler ve özel sektör arasındaki bir ihtilaf değildir. Sorun okyanuslar, hava ve uzay gibi evrensel kaynaklar üzerindeki çekişmelerden nitelik olarak farklı, devletler arası menfaat sorunudur. İnternet, dünyayı saran atmosfer gibi tüm insanlığın ortak değeri olarak nitelendirilmektedir.[135] Ayrıca, devletlerin internet üzerindeki hâkimiyetlerine ilişkin tartışmalar, uzay ile ilgili egemenlik tartışmalarına benzetilmektedir.[136] Uzay ve gök cisimlerinin hukuki statüsü konusunda egemenlik ilkesinden hareket edilmemektedir.[137] Benzer şekilde, internetin düzenlenmesi sorunu uluslararası suların düzenlenmesi sorununa da benzetilmektedir.[138] Devletlerin iktisadi ve bilimsel gelişme derecesi ne olursa olsun, bu tür kaynaklardan yararlanmanın tüm devletlere açık olması kabul edilmektedir. Diğer bir deyişle, egemenlik hakkından ziyade yararlanma hakkı ön plana çıkmaktadır. İnternetin kendine özgü yapısı ve artan sosyal, siyasal ve ekonomik önemi sebebiyle her devlet farklı iç dinamiklerden dolayı internet üzerindeki etkisini artırmak istemektedir.

İnternetin yönetimi veya yönetişimiyle ilgili kurum ve kuruluşların bugünkü görev ve yetkilerine kavuşmaları kolay ve hızlı olmamıştır. İnternetin nasıl yönetileceği sorunu, bir dönem "*alan adı savaşları (domain*

---

[133] **Goldsmith/Wu**, s. 31.

[134] **Zittrain, Jonathan** (1999) "*ICANN: Between the Public and the Private Comments before Congress*", Berkeley Technology Law Journal, Cilt: 14, Sayı: 3, s. 1071-1094, s. 1074 vd.

[135] **Ryan**, s. 196.

[136] **Goldsmith/Wu**, s. 171; Benzer bir analoji çevre hukuku için de yapılmaktadır. Bkz. **Kulesza, Joanna** (2012) *International Internet law*, Milton Park, Routledge, s. 144.

[137] **Toluner, Sevin** (1996) *Milletlerarası Hukuk Dersleri: Devletin Yetkisi*, İstanbul, Beta, s. 49; ayrıca bkz. **Pazarcı, Hüseyin** (2015) *Uluslararası Hukuk*, Ankara, Turhan Kitabevi, s. 307.

[138] **Ryan**, s 197.

name wars)" olarak adlandırılan bir süreçten geçmiştir.[139] Meselenin kökeninde meşruiyet sorunu yattığı kadar, bu ölçüde büyük, dağıtık ve kendine özgü teknik yapısı olan, çok farklı egemenlik alanlarını, kurumları ve kişileri ilgilendiren bir alanın regülasyonuyla ilk kez karşılaşılması da bir diğer etkendir.[140]

ABD, özellikle ICANN'in kurulduğu ve alan adları konusunda yetkilendirildiği dönemde farklı bir yöntem tercih etmiş ve geleneksel bir uluslararası organizasyon yerine sınırları gri alanlarla çizilmiş ve yetkisini paydaşlarından alan bir yapı oluşturmuştur. İnternetin yapısı o kadar dağıtıktır ki, onu kuran yapılar o kadar çeşitli ve informeldir ki ABD'nin bile tek başına onu yönetme ve çekip çevirme meşruiyeti olmadığı düşünülmektedir.[141]

ICANN ve IANA'nın mevcut yetkilerine rağmen, internetin işlerliği için tüm devletlerin aktif katılımı zorunludur. İnternet trafiğinin aktığı hatlar ve web sitelerini barındıran sunucular dünyanın her tarafına yayılmıştır. İnternet trafiği saniyeler içerisinde farklı ülkeleri katederek akmaktadır. Bu karmaşık yapı sebebiyle bir noktadaki kesinti dünyanın çok uzak bir noktasındaki internet trafiğini olumsuz etkileyebilmektedir. Ayrıca, genel veya bölgesel internet noktalarının kontrolü, bakımı ve hatların sayısının artırılması için de devletler arası iş birliği gerekmektedir.

İnternetin işlerliğinde her devletin menfaati vardır. Mevcut çoklu paydaş katılım modellerine rağmen ICANN ve IANA'nın şu anki yapılanma şekilleri internetle ilgili politikaların ve uygulamaların taraflı olmasına yol açmaktadır.[142] ABD, özellikle ICANN'i uluslararası katılıma açma konusunda çeşitli denemelerde bulunsa da sahip olduğu yetkileri devretme konusunda hiçbir zaman istekli davranmamakta; ekonomik

---

[139] **Mueller**, s. 2.

[140] **Mueller**, s. 5.

[141] **Mueller**, s. 5.

[142] **Fuller, Kathleen E** (2001) "*ICANN: The Debate Over Governing the Internet*", Duke Law & Technology Review, Cilt: Rev 1, s. 1-9.; **Muldoon, James P** (2012) "*New types of organizations and global governance in the twenty-first century - The case of ICANN*": Oestreich, Joel E (Editör) *International Organizations as Self-directed Actors : A Framework for Analysis*, Abingdon, Routledge, s. 243-244.

ve ulusal güvenlik menfaatleri gereğince mevcut konumunu korumak istemektedir.

ICANN'in Los Angeles'ın yanında Singapur ve İstanbul'da yönetim merkezleri açması bu konudaki uluslararası baskıyı dindirmeye yönelik taktiksel manevralar olarak değerlendirilebilir. Zira ABD'nin adil davranmadığı ve kaynakları tek taraflı olarak kendi menfaatine kullandığına ilişkin eleştiriler sürmektedir. Bu amaçla, sürecin şeffaflığını sağlamaya yönelik muhtelif girişimler vardır.[143]

Başta Avrupa Birliği olmak üzere uluslararası toplum, internet üzerindeki ABD etkisinin kırılması için çeşitli girişimlerde bulunmuştur. İnternetin yoğun ticari işlemler ve kritik iletişim alanlarında kullanılması, devletlerin gizlilik politikalarının farkı olması, ulusal güvenlik tehditleri ve internet altyapı yatırımları bu girişimleri tetikleyen sebepler arasında yer alır. Ayrıca ICANN'in, kök sunucularının güvenliğini sağlayamaması ve devletlerin bu yöndeki taleplerini geri çevirmesi de bu yöndeki girişimleri hızlandırmıştır.

Yukarıda da açıklandığı üzere, 2005 yılında Tunus'ta gerçekleştirilen Dünya Bilgi Toplumu Zirvesi'nin II. Aşaması'nda Avrupa Birliği radikal bir teklifte bulunmuş ve alan adı yönetiminin ICANN ve ABD Ticaret Bakanlığından alınarak Birleşmiş Milletler nezdinde faaliyet gösterecek bir ihtisas kurumuna aktarılmasını önermiştir. ABD bu konuda taviz vermemiş, esaslı bir direnç göstermiştir.

İnternet, ABD'nin askerî iletişim stratejisinin bir parçası olarak ortaya çıkmıştır. ABD, interneti aynı amaç için kullanmaya devam etmekte ve elektronik ticaret ABD ekonomisinin önemli dinamiklerinden birisini oluşturmaktadır. İnternetle ilgili politikaların, görünürde bağımsız ancak gerçekte ABD'nin etkisinde bulunan ICANN tarafından belirlenmesi ve icra edilmesi sayesinde ABD'nin siyasal sorumluluktan kaçtığı iddia edilmektedir.[144]

---

[143] Bkz. **§6(XIII)**[İnternet Protokol Adres Kaynaklarının Kamu Yararına Uygun Yönetimine İlişkin Deklarasyon].

[144] **Fuller**, s. 2.

İnternet yönetişimi alanındaki bir diğer önemli gelişme ise 2014 yılında başlatılan IANA Geçiş Süreci'dir.[145] ABD, elindeki yetkileri kademeli olarak ICANN'e devretmek suretiyle geri planda kalmaya çalışmaktadır. IANA Geçiş Süreci, kök sunucularının yönetiminin ABD Ticaret Bakanlığı bünyesinde kurulan Ulusal Telekomünikasyon ve Enformasyon Yönetimi (NTIA) tarafından tamamen ICANN'e bırakılmasını kapsayan bir süreçtir. Aynı doğrultuda ICANN'in şeffaflık ve hesap verebilirliği artırılmaya, uluslararası toplumun internet yönetişimi sürecine daha fazla katılımı sağlanmaya çalışılmaktadır.

Bu süreç, ABD Ticaret Bakanlığının, DNS sisteminin, rekabeti ve uluslararası katılımı artıracak şekilde özelleştirilmesine yönelik 1997 yılında başlattığı çalışmalarının en önemli ayağıdır. Bu geçişin ABD tarafından kontrollü şekilde gerçekleştirilmesinin, uzun süredir artarak devam eden uluslararası baskının bir kırılmaya yol açmadan azaltılmasını sağladığı düşünülmektedir.[146]

Öte yandan, internet yönetiminin Birleşmiş Milletlere bırakılmasına da çeşitli eleştiriler getirilmektedir. Eleştiriler, bu adımın bürokrasiyi artıracağı ve bunun da internet gibi dinamik yönetim gerektiren bir alanın işlerliğini tehlikeye düşüreceği endişesine dayanmaktadır.[147] Ayrıca, internet yönetiminin Birleşmiş Milletlere ek mali külfet getireceği ve kurumun bu külfeti tüm devletlere eşit olarak yansıtmakta zorlanacağı iddia edilmektedir. Bunların yanı sıra, Birleşmiş Milletlerin mevcut yapılanmasının, karar alma süreçlerinde Güvenlik Konseyinin beş daimî üyesi lehine dengesizlik yaratması ve aynı dengesizliğin internet politikalarına da yansıyacağı korkusu, olası bir Birleşmiş Milletler yönetiminin önünde engel oluşturmaktadır.

---

[145] **APNIC**, "*Explained: IANA Transition*", <https://www.apnic.net/wp-content/uploads/2017/01/IANA-Factsheet.pdf>; Ayrıca bkz. **ICANN**, "*ICANN Board Transmits IANA Stewardship Transition Proposal and Enhancing ICANN Accountability Recommendations to NTIA*", < https://www.icann.org/stewardship>

[146] **Post, David G/Kehl, Danielle** (2015), "*Controlling Internet Infrastructure The "IANA Transition" and Why It Matters for the Future of the Internet Part I*", <https://static.newamerica.org/attachments/2964-controlling-internet-infrastructure/IANA_Paper_No_1_Final.32d31198a3da4e0d859f989306f6d480.pdf>

[147] **Arx**, s. 14.

İnternet yönetişimi konusunda, dar ve geniş açı olmak üzere iki yorum vardır.[148] Dar yoruma göre, internet yönetişimi konuları sadece DNS (Domain Name System - Alan Adı Sistemi), IP numaraları ve kök sunucular gibi internet altyapısına ve ICANN'in bu alandaki ana aktör olma durumuna odaklıdır. Temel alanlar ise teknik standardizasyon, kaynak dağıtımı ve atama, kamu politikası süreci, politikayı belirleme, politikayı icra etme ve uyuşmazlık çözümü süreçleridir. Geniş yoruma göre ise internet yönetişimi altyapı konuları ile sınırlı olmamalı; hukuksal, ekonomik, sosyokültürel hususlar ve gelişmeye ilişkin konularla da ilgilenmelidir.

Mathiason, internetin yönetime değil ancak yönetişime konu olabileceğini internetin sınırsız ve çok farklı paydaşı ilgilendiren niteliğini göz önüne alarak ve bu bağlamda uluslararası rejimlerle analoji kurarak açıklamaktadır.[149] Yönetişimin, Latince "bir gemiyi sevk ve idare etmek" şeklindeki etimolojik kökenine de dikkat çeken Mathiason, internetin de tıpkı bir geminin sevk ve idare edilmesi gibi yönetişime konu olması gerektiğini ileri sürmektedir. Esasında dünyadaki ilk uluslararası organizasyonların iletişimle ilgili olması tesadüf değildir.[150] Bu öncü kuruluşlar, Dünya Posta Birliği ve Uluslararası Telekomünikasyon Birliğidir (eski adıyla Uluslararası Telgraf Birliği). Öte yandan bu köklü geçmiş, iletişim alanındaki uluslararası iş birliğinin gerekliliğini de göstermektedir.

WGIG'nin tanımına rağmen, internetin ve yönetişimin ifade ettiği anlam konusunda hâlâ fikir birliği olmadığı ileri sürülmektedir.[151] Herkes, interneti kullanım amacına göre tanımlamaktadır. İnterneti müzik dinlemek için kullanan birisi için internet ve yönetişimi sorunu radyoların regülasyonundan farksızdır. Benzer şekilde, interneti sadece haberleşmek için kullanan kimse için internet ve yönetişimi sorunu telefonun regülasyonundan farksızdır.

---

[148] **Mathiason**, s. 17.

[149] **Mathiason**, s. 17.

[150] **Mathiason**, s. 12.

[151] **Mathiason**, s. 6.

Esasında internetin yeni tür bir sosyal sözleşme gerektirdiği tartışılmaktadır.[152] Yukarıda da açıklandığı üzere meselenin kökeninde meşruiyet sorunu yattığı kadar, bu ölçüde büyük, dağıtık ve kendine özgü teknik yapısı olan, çok farklı egemenlik alanlarını, kurumları ve kişileri ilgilendiren bir alanın regülasyonuyla ilk kez karşılaşılması da önemli bir etkendir. Sorun okyanuslar, çevre, hava ve uzay gibi evrensel kaynaklar üzerindeki çekişmelerden nitelik olarak farklıdır. Sadece devletleri ilgilendirmeyen, bireyleri, özel şirketleri, sivil toplumu, resmî veya informel birçok kuruluşu, donanım ve yazılım üreticilerini, basını, medya şirketlerini, kısaca herkesi ilgilendiren bir sorundur. Bu konuda ortak paydada buluşulması uzun sürecektir. Dolayısıyla internet yönetişiminin de uzun yıllar tartışılacağı açıktır. Uzun vadede, bu alanın bir uluslararası sözleşmeyle, uluslararası hukukun şemsiyesi altında bütünüyle düzenlenmesi beklenmektedir.[153]

XII. İnternette yerelleşme mi, fragmantasyon mu?

İnternette yerelleşme artmaktadır. Bu alandaki en önemli girişim, ICANN tarafından 16 Kasım 2010 tarihi itibarıyla alan adlarında yerel dillerin kullanılmaya başlamasıdır.[154] Bu doğrultuda alan adları sisteminin 22 farklı dili desteklemesi hedeflenmektedir. Söz konusu girişimden bağımsız şekilde, devletlerin, internette kendi dillerinde içerik oluşturmaya, görünürlüklerini artırmaya ve bunu ulusal politikanın bir parçası hâline getirmeye yönelik çeşitli girişimleri ve teşvikleri vardır.

Yerelleşme sadece dille sınırlı değildir. Verinin ülke içerisinde barındırılmasına, internet trafiğinin ülke içerisinde tutulmasına, Internet Exchange Point (IXP) olarak adlandırılan internet trafik kavşaklarının ülke sınırları içerisinde konumlandırılmasına yönelik talepler artmaktadır. Farklı yelpazede hizmetler sunan bulut sistemlerinin gelişimi de internette otonom alanlar oluşturmaktadır.

---

[152] **Mueller**, s. 5.

[153] **Kulesza**, s. 152.

[154] **ICANN**, "*Internationalized Domain Names*", <https://www.icann.org/resources/pages/idn-2012-02-25-en>

Verinin ve trafiğin yerelde tutulması (veri lokalizasyonu) kişisel verilerin korunması gerekliliğini aşan, ulusal güvenlik bağlamında ele alınan bir hususdur. Tüm internet kullanıcılarının ve internet faaliyetlerinin sıkı gözetim ve denetime tabi tutulması, internet trafiğinin kapsamlı şekilde incelenmesi, şifreli iletişimin kısıtlanması ve internet faaliyetlerine özgü yaptırımların geliştirilmesi gibi devlet pratiklerinin dünya genelinde yaygınlaşması söz konusudur. Yerelleşme ile başlayan bu trendin, internette fragmantasyona yol açması ve internetin küresel ağ niteliğinin bundan esaslı şekilde etkilenmesi beklenmektedir. Fragmantasyon; filtreleme ve engelleme yöntemlerinin artması ve kapsamının genişlemesi, mahremiyet düzenlemelerinin katılaşması, güvenlik duvarları, yerel diller, yerel sosyal medya mecraları, ağ tarafsızlığının terki sonucu öncelikli içeriklerin artması gibi farklı şekillerde ortaya çıkabilir.[155]

Yerelleşme ve fragmantasyonun bu hızda artmasıyla beraber her bir devlete ait müstakil ve dış ağ ile sınırlı etkileşimi olan özel internet adacıklarının oluşması kaçınılmaz hale gelmektedir. Bunun neticesinde ise internetin küresel bir ağ olmaktan çıkması ve oluşan bu yeni adacıklar arasında seyahat etmenin de özel kurallara tabi tutulması söz konusu olacaktır.[156]

Aslında kendi içerik ve yayın kuralları, ihtilaf çözüm mekanizmalarıyla internet adacıkları oluşmaktadır. Fiziki serbest dolaşımdaki sınırlara benzer şekilde internet ortamında sanal sınırlar kurularak belirli kullanıcıların daha kaliteli ve nitelikli içeriğe erişmesi ve altyapıyı kullanması söz

---

[155] **Hill, Jonah Force** (2012), "*Internet Fragmentation - Highlighting the Major Technical, Governance and Diplomatic Challenges for U.S. Policy Makers*", <http://www.belfercenter.org/sites/default/files/legacy/files/internet_fragmentation_jonah_hill.pdf>, s. 10-11.

[156] Örneğin, Rusya bu konuda öne çıkmakta, kendi ağını kurmak için çalışmalar yapmaktadır. Yakın zamanda gerçekleşen bir testte, internet ağına olan bağlantı geçici olarak kapatılmıştır. Bkz. **Cimpanu, Catalin**, "*Russia to disconnect from the internet as part of a planned test*", <https://www.zdnet.com/article/russia-to-disconnect-from-the-internet-as-part-of-a-planned-test/>; Benzer şekilde Almanya ve Hollanda'nın ortak askerî internet ağı kurma girişimi vardır. Tactical Edge Networking #TEN olarak adlandırılan projeye uzun vadede diğer NATO ülkelerinin de katılması beklenmektedir. Bkz. **Cimpanu, Catalin**, "*Germany and the Netherlands to build the first ever joint military internet*", <https://www.zdnet.com/article/germany-and-the-netherlands-to-build-the-first-ever-joint-military-internet/>

konusu olmaktadır. Nasıl ki gerçek dünyada seyahat kısıtlamaları varsa internet ortamında oluşan adacıklar arasında seyahat etmek de farklı gerekçelerle özel kurallara tabi tutulmaktadır.[157]

Tüm bunlar yaşanırken, internete ilişkin başka bir alanda da merkezîleşme artmaktadır. Cloudfare gibi içerik dağıtım ağları ve özel DNS hizmetlerinin tekelleşmesi neticesinde, bu tür hizmetlerin sürdürülebilirliği hayati önem kazanmaktadır. Cloudfare sitesindeki bir kesinti farklı ülkelerdeki milyonlarca web sitesini etkileyebilmektedir. Benzer bir merkezîleşme VPN gibi *proxy* hizmetlerini sunan hizmet sağlayıcılarda da gözlemlenmektedir. VPN hizmetlerinin bir elin parmağını geçmeyecek sayıda şirketin elinde toplanmış olması dikkat çekicidir.

İnternetin küresel ağ niteliğini koruyabilmesi için internet yönetişiminde yerel ihtiyaçları karşılayacak, sorunlara hızlı ve etkin çözümler getirecek mekanizmaların geliştirilmesi, internet ağıyla ilgili dışlayıcı politikalardan uzak durulması zaruridir. Ortak aklın bu konuda bir çözüm geliştirememesi durumunda internetin, henüz teknolojik olgunluğa bile ulaşamadan ve kendisinden küresel olarak tam istifade edilemeden ortadan kalkacağı düşünülmektedir.[158]

---

[157] **Smith, Graham** (2017) "*Cyberborders and the Right to Travel in Cyberspace*": Kohl, Uta (Editör) *The Net and the Nation State - Multidisciplinary Perspectives on Internet Governance*, Cambridge, Cambridge University Press.

[158] **Ryan**, s. 197.

ÜÇÜNCÜ KISIM

ERİŞİMİ ENGELLEME VE FİLTRELEME

§4. İNTERNETE ERİŞİMİN ENGELLENMESİ VE İNTERNETİN FİLTRELENMESİ

Devletler farklı sebep ve yöntemlerle internet içeriğine müdahale etmektedir. Devletler belirli işlemlerin internet üzerinden gerçekleştirilmesini tamamıyla yasaklayabildikleri gibi, vatandaşlarının tüm internet aktivitelerini takip etme yoluna da gidebilmektedir. Hukuka aykırı veya zararlı bir içeriği tespit ettiklerinde ise o içerikten vatandaşlarını korumak amacıyla erişimi engelleme adı verilen müdahale yöntemine başvurmaktadırlar.

İnternet içeriğine erişimin engellenmesi için kullanılan yöntemler çeşitlidir. Engellemenin kapsamı, kullanılan teknik, engelleme süresi, engelleme öncesi ve sonrası takip edilen süreçler devletten devlete değişmektedir. Kullanılan yöntemler her şeyden önce devletlerin teknolojik gelişmişlikleriyle doğrudan bağlantılıdır. Erişimi engelleme tekniklerini uygulamak külfetli altyapı yatırımları gerektirdiği için ekonomik gelişmişlik düzeyi de diğer bir faktör olarak ortaya çıkmaktadır. Ayrıca kullanılacak yöntem, erişimi engellemenin hangi düzeyde gerçekleştirilmek istendiğine yani engellemenin dozajına göre de değişmektedir.

Bazı devletler tek bir yöntem kullanırken bazıları birden çok yöntemi bir arada kullanmakta ve hatta bazı otoriter devletler hukuk dışı yöntemlere bile başvurabilmektedir. Özellikle, devletlerin demokrasi ve insan hakları konularındaki yaklaşımları engelleme sürecinin saydamlığını, hesap verilebilirliği, etkin koruma mekanizmalarının işlerliğini doğrudan etkilemektedir. Bu arada, tedbirin olağan veya olağanüstü dönemde uygulanıyor olmasını ayrı ayrı değerlendirmek gerektiği de akılda tutulmalıdır.

İçeriğin engellenmesi ile içeriğin yayından kaldırılması farklı kavramlardır. İçeriğin engellenmesi yönteminde kullanıcının bir içeriğe fiilî erişimi kısıtlanmaktadır. İçeriğin yayından kaldırılması ise içerik veya yer

sağlayıcılar tarafından içeriğin sunuculardan veya barındırılan içeriklerden çıkarılmasını ifade etmektedir.

İçeriğe erişimin engellenmesi içerik yayından kaldırılıncaya kadar başvurulan öncelikli bir tedbirdir. İçeriğin yayından kaldırılması her zaman mümkün olmayabilir. Zira bunun için mahkeme kararı veya idari bir karar gerekebilir. Benzer şekilde, içeriğin yurt dışında barındırıldığı durumlarda içeriğe uygulanacak hukukun tespiti ve tespit edilen hukuk gereğince ilgili sürecin işletilmesi gerekir. Bunun için uluslararası adli yardımlaşma hükümlerinin de takip edilmesi lazım gelir. İşte bu noktada, içeriğe erişimin engellenmesi yöntemi içerik yayından kaldırılıncaya kadar geçici koruma sağlamaktadır. Bazı durumlarda ise içeriğin yayından kaldırılması ile ilgili süreç hiç işletilmeden erişimin engellenmesi yöntemine başvurulabilmektedir.

İnternet içeriğinin filtrelenmesi veya erişimin engellenmesi, bir yanıyla da uluslararası hukuk ile bağlantılıdır. Bir devletin uyguladığı engelleme ve filtreleme yöntemleri sebebiyle, sınır aşan veri akışına halel gelebilir. Yine, bir devletin sınırları içerisinde yer alan ve yurt dışına yayın yapan bir platforma uygulanan kısıtlama, başka devletlerdeki bireylerin ifade özgürlükleri ile diğer bazı temel hak ve özgürlüklerini zedeleyebilir. Özellikle trafik yönetimi amacıyla altyapıya ilişkin kuralların keyfî şekilde uygulanması neticesinde, sınır aşan trafiğin etkilenmesi teknik olarak mümkündür. Bu bölümde, internet içeriğine erişimi engellemek için kullanılabilecek yöntem ve teknikler sınıflandırılmaya çalışılmıştır. Bu sınıflandırma tahdidî değildir ve burada sayılanlar dışında kalan farklı ve özgün yöntem ve tekniklerle internet içeriğine müdahale edilmesi mümkündür.

Bu bölümde, herhangi bir ülkeyle bağlı kalınmaksızın genel yöntem ve teknikler derlenmiştir. Sınıflandırmanın asıl amacı, internet içeriğine müdahalenin farklı gerekçelere dayanabildiğini, aynı anda birden fazla tekniğin iç içe geçerek uygulanabildiğini göstermek ve bu doğrultuda tüm teknik ihtimalleri nazara almayan bir hukuki değerlendirmenin eksik olacağına dikkat çekmektir.

Önemle belirtmek gerekir ki bu bölümde genel bir sınıflandırma yapılmaktadır. Kullanılan yöntem veya tekniğin herhangi bir ülkenin hukukuna uygunluğuna ilişkin bir değerlendirme özellikle yapılmamıştır. İlgili hukuk düzeninin incelendiği kısımlarda çapraz atıflar yapılmak suretiyle bu tür değerlendirmelere yer verilecektir.

I. Engellemenin coğrafi kapsamına göre

A. Ülkesel engelleme

İnternet içeriğinin engellenmesi veya filtrelenmesi ülke genelinde gerçekleştirilebileceği gibi bölgesel olarak da gerçekleştirilebilir. Ülkesel müdahale yönteminde, internetin hem yurt içi bağlantı noktalarının hem de yurt dışı çıkış noktalarının kontrol altına alınması gerekmektedir. Bu uygulamanın sonuç vermesi, çıkış noktalarının kontrolündeki etkinliğe bağlıdır.

İnternete erişim sağlama hizmetinin devlet tekelinde olduğu ve tüm internet altyapısını çoğu zaman tek bir telekomünikasyon şirketinin yönettiği ülkeler ile özel sektörün faaliyet göstermesine ve birden fazla piyasa oyuncusuna izin verilen ülkeler için müstakil değerlendirmeler yapmak gerekir. Buna bağlı olarak, belirli bir içeriğe erişim engellenebilir, internet ağına tüm bağlantı ülke genelinde kısıtlanabilir veya belirli bir içeriğe yahut tüm internet ağına erişim yavaşlatılabilir.

Ülkesel engelleme, internet ağına erişim için kullanılan tüm mecralarda gerçekleştirilebileceği gibi salt mobil ağlarda veya belirli bir mecrada dar şekilde uygulanabilir. Özellikle, somut olayda engellemenin temel amacı, engelleme kararından hangi mecranın etkileneceği konusunda belirleyici olacaktır. Örneğin, toplumsal olaylar sebebiyle sadece mobil internet bağlantısının (3G, 5G vb.) engellenmesi gibi. Aynı doğrultuda, engelleme, uygulama temelli de gerçekleştirilebilir. Örneğin, belirli mobil uygulamaların engellenmesi gibi.

Öte yandan teorik olarak tartışılan güncel bir konu, bir ülkenin, internet ağına erişiminin tamamen engellenip engellenemeyeceğidir.

Alınacak bir yaptırım kararı neticesinde bir ülkenin internet erişiminin tamamen kısıtlanması, bu şekilde bir toplumun internet ağından izolasyonu mümkün müdür? Bu soru, özellikle siber savaşın kızışmasıyla daha sık gündeme gelecektir.

B. Bölgesel engelleme

İnternet içeriğine erişim, bazı durumlarda ülkesel değil bölgesel olarak da engellenebilir. Özellikle, kamu düzenini bozucu nitelikteki toplantı, gösteri, sosyal olay, ayaklanma, saldırı ve terör olayları sırasında veya bunların hemen akabinde internet içeriğine bölgesel olarak müdahale edilebilir. Bu tür bir müdahale, somut olayın özelliklerine göre tedbirlerin ölçülülüğünü sağlayabilir. Bu bağlamda, belirli bir içeriğe erişim engellenebileceği gibi, dar veya geniş bir bölgede, ilin tamamında veya bir ilçede internet ağına tüm bağlantı kısıtlanabilir yahut belirli bir içeriğe veya tüm internet ağına erişim yavaşlatılabilir.

Bölgesel engelleme, internet ağına erişim için kullanılan tüm mecralarda gerçekleştirilebileceği gibi salt mobil ağlarda veya belirli bir mecrada dar şekilde uygulanabilir. Özellikle, somut olayda engellemenin temel amacı, engelleme kararından hangi mecranın etkileneceği konusunda belirleyici olacaktır. Örneğin, sosyal olaylar sebebiyle sadece mobil internet bağlantısının (3G, 4.5G vb.) engellenmesi gibi. Aynı doğrultuda, engelleme, uygulama temelli de gerçekleştirilebilir. Örneğin, belirli mobil uygulamaların engellenmesi gibi.

II. Engellemenin ağ kapsamına göre

A. İnternet omurgası temelli engelleme

İnternet içeriğine erişim İSS'ler nezdinde ayrı ayrı engellenebileceği gibi ana internet omurgası üzerinden ülke genelinde ve tek aşamada da engellenebilir. Devletlerin bu konudaki tercihleri; coğrafi büyüklüklerine, ülke genelinde faaliyet gösteren İSS'lerin sayısına, telekomünikasyon sektörünün özel sektöre açık olup olmamasına göre değişmektedir.

İnternet içeriğine erişimi engellemek için kullanılan bir yöntem, içeriğin doğrudan ana internet omurgası üzerinden engellenmesidir.[159] Bu yöntemde, erişim engellemesi doğrudan ülke genelindeki ana internet ağına işlenmekte ve böylece İSS'lerden bağımsız bir şekilde ülke genelinde içeriğe erişim engellenmektedir. Bu yöntem sayesinde, ülke genelinde aynı anda ve seviyede internet içeriklerine erişim engellenmektedir.

B. İSS temelli engelleme

İnternet içeriğine erişimin İSS'ler aracılığıyla engellenmesi de mümkündür.[160] Mahkeme kararları veya idari kararlar doğrudan İSS'ye veya varsa onu temsil eden birliğe gönderilmekte, içeriğe erişimin ilgili İSS'nin kontrolündeki tüm ağ üzerinde engellenmesi sağlanmaktadır.

Erişim engellemesinin etkili olabilmesi için, engelleme kararının tüm İSS'ler tarafından aynı anda ve aynı teknik kullanılarak uygulanması gerekmektedir. Dolayısıyla bu yöntem, ülke genelinde az sayıda İSS'nin faaliyette bulunduğu, tüm sektörün devlet tekelinde olduğu veya erişim sağlayıcıların yeknesak uygulama geliştirmek için bir birlik şeklinde örgütlendiği ülkelerde etkin bir şekilde kullanılabilmektedir.

Engellemenin her bir İSS nezdinde ayrı ayrı uygulanması bürokratik bir süreç gerektirdiği için engelleme kararlarının İSS'ler tarafından geç veya hiç uygulanmaması riski ortaya çıkmaktadır.[161] Bu da farklı İSS'lerden hizmet alan internet kullanıcıları arasında eşitsizlik doğurabilmektedir. Örneğin, bir İSS'ye bağlı kullanıcılar erişim engellemesi sebebiyle birçok web sitesine ulaşamazken, kararları icra etmekte geciken İSS'ye bağlı kullanıcılar engelleme kararı alınmış web sitelerini ziyaret edebilmektedir.

Benzer şekilde, İSS'ler tarafından erişim engellemesi için farklı teknikler kullanılması engellemenin etkinliğinin ülke genelinde farklı-

---

[159] **Faris, Robert/Villeneuve, Nart** (2008) "*Measuring Global Internet Filtering*": Deibert, Ronald/Palfrey, John/Rohozinski, Rafal/Zittrain, Jonathan (Editörler) *Access denied: the practice and policy of global Internet filtering*, Cambridge, MIT Press, s.12.

[160] **Faris/Villeneuve**, s. 12.

[161] **Faris/Villeneuve**, s. 14.

laşmasına sebep olacaktır. Erişim engelleme teknolojileri ne kadar hızlı gelişiyorsa engellemeleri aşacak teknolojiler de aynı hızda gelişmektedir. Bu sebeple, İSS'lerin, erişimi etkin bir şekilde engelleyecek ve kolay aşılamayacak teknolojiler kullanması gerekmektedir. Ülke genelinde her İSS'nin farklı gelişmişlikte teknolojiler kullanması, tıpkı kararların geç uygulanmasında olduğu gibi kullanıcılar arasında eşitsizlik doğuracaktır.

İSS temelli engelleme çoğu zaman o ülkenin vatandaşı yurt dışına çıktığı zaman da onu takip edebilir. Örneğin, mobil operatörlerin ağında uygulanan engelleme, roaming durumunda kişi yurt dışında olduğunda da uygulanmaya devam edebilmektedir.

C. Kurumsal engelleme

Kurumsal engelleme yöntemi, belirli internet içeriğine sadece belirli ağlarda erişimin engellenmesidir. Örneğin, internetin toplu kullanıma sunulduğu internet kafeler gibi alanlarda, akademik ağda, okulda, hava limanında, trende,[162] hapishanede, kütüphanede veya kamusal olarak kullanılan ağda, varsayılan (*default*) olarak belirli içeriklere erişim engellenebilmektedir. Kurumsal engelleme kapsamında belirli MAC adreslerini kullanan cihazlar engellenebileceği gibi farklı politikalar da uygulanabilir.

Kurumsal engellemenin altında farklı motivasyonlar yatabilir.[163] Örneğin, ağ güvenliğini tehdit eden unsurları önlemek veya bunlara yanıt vermek için belirli tür içerik engellenebilir. *Malware* (zararlı yazılım) içeren uygulamaların, *spam*lerin (yığın mesaj) veya *phising* (e-dolandırıcılık) içeren mesajların engellenmesi söz konusu olabilir.

Kurumsal engelleme ayrıca ağı yönetmek amacıyla da gerçekleştirilmektedir. Örneğin, bant genişliğini kontrol etmek maksadıyla belirli

---

[162] Sosyal medyada yer alan bir örneği paylaşmak gerekirse; kişi, İsviçre'de bindiği trende Netflix üzerinden film izlemeye başlar; tren İsviçre'den Almanya'ya geçer ve film, Almanya'da telif hakları sebebiyle sunulmadığı için durur; kişi filmin sonunu öğrenemez. Bkz. <https://twitter.com/larsr_h/status/1140662967584923648>

[163] **InternetSociety**,"*InternetSocietyPerspectivesonInternetContentBlocking:AnOverview*",<https://www.internetsociety.org/sites/default/files/ContentBlockingOverview_20170326_FINAL_0.pdf>, s 7.

içerikler kısıtlanabilir. İşverenler, istihdam ettikleri kişilerin daha verimli çalışmasını sağlamak amacıyla sosyal medya sitelerine erişimi engelleyebilir veya video içeriği barındıran sitelere erişimi yavaşlatabilir.

D. Platform temelli engelleme

Platform temelli engelleme yönteminde, belirli siteler veya uygulamalar (özellikle arama motorları ve bulut uygulamaları) bazı içeriklere yönelik engelleme yapmaktadır.[164] Bu sayede, tüm platform engellenmeksizin içerikler filtrelenmiş şekilde son kullanıcının erişimine açılmaktadır. IP dağıtım tabloları sayesinde bir internet kullanıcısının, bir internet sitesine hangi ülkeden veya şehirden bağlandığını tespit etmek mümkündür. Statik IP kullanılan durumlarda doğruluk payı daha da artmaktadır. Bu şekilde ziyaretçilere yerelleştirilmiş hizmetler sunulabildiği gibi yerel düzenlemelere de daha kolay uyum sağlanabilmektedir.

Bu yöntemle bazı uygulamaların belirli ülkelerden indirilmesi kısıtlanabileceği gibi fikrî mülkiyet sınırlamaları sebebiyle kimi içerikler yalnızca belirli ülkelerde erişilebilir kılınabilir. Bazı durumlarda ise bir mahkeme kararının veya idari kararın gereğinin yerine getirilmesi amacıyla bu yöntem uygulanabilir. Örneğin, bir ülkede suç kabul edilen içeriğe yönelik alınan kararın ülkede yerleşik olmayan hizmet sağlayıcı tarafından icra edilmesi gerekebilir. Bu durumda içerik, yurt içinde bulunan içerik veya yer sağlayıcılar için sunuculardan, barındırılan içerikten çıkarılabilir. Yurt dışındakiler içinse içerik veya yer sağlayıcının kendi sistemlerinde aldığı tedbirle içeriğe yurt içinden erişim engellenebilir.

Benzer şekilde, VPN kullananların platforma erişimi engellenebileceği gibi online davranışsal reklamcılık uygulamalarıyla sadece belirli profile sahip kullanıcıların platforma erişimine izin verilebilir. Yine, bazı platformların, reklamların gösterimini sınırlayan *adblocker* benzeri uygulamaları kısıtlaması bu engelleme yöntemine örnek verilebilir.

---

[164] **Internet Society**, "*Internet Society Perspectives on Internet Content Blocking: An Overview*", s. 17.

Platformların kendi barındırdıkları içerikleri denetlemesi ve politikalarına aykırı -örneğin, müstehcen veya nefret söylemi içeren- içerikleri kaldırması; içeriklerin dinamikliği, çeşitliliği ve yapısal olmaması sebebiyle teknik olarak zor bir süreçtir. "*Upload filter*" ve "*download filter*" denilen yöntemler de bu kategoride değerlendirilebilir. Bu alanda yapay zekâ teknolojileri kullanılıyor olsa da her zaman ideal sonuçlara ulaşmak mümkün olamamaktadır.[165]

Platform temelli engellemelerde arama motorları etkin bir şekilde kullanılmaktadır.[166] Arama motorları bu tür bir filtrelemeyi ilgili ülkenin hukukuna uymak için gerçekleştirebileceği gibi, zararlı içerikleri önlemek veya yaş kısıtlı içeriklerin gösterimini kısıtlamak gibi amaçlarla kendi inisiyatifiyle de gerçekleştirebilir.[167]

Böyle bir filtreleme, Google arama motorunun Almanya ve Fransa'da erişilen versiyonunda uygulanmaktadır.[168] Özellikle unutulma hakkı kapsamında platform temelli engelleme daha fazla ön plana çıkmakta ve bu bağlamda girift hukuki sorunlar doğurmaktadır. Öte yandan arama motorları alanında farklı hizmet sağlayıcıların varlığı, bu alandaki kullanıcı tercihlerinin hızla değişmesi, arama motoru filtrelemelerinin teknik olarak kolay aşılabilmesi sebebiyle bu yöntemin etkinliği de sorgulanmaktadır.[169]

---

[165] Bu konuda örnek bir uygulama için bkz. **Simonite, Tom**, "*AI Has Started Cleaning Up Facebook, but Can It Finish?*" <https://www.wired.com/story/ai-has-started-cleaning-facebook-can-it-finish/>

[166] **Internet Society**, "*Internet Society Perspectives on Internet Content Blocking: An Overview*", s. 18.

[167] Örneğin, Google arama motorunun Safe Search uygulaması zararlı veya müstehcen içeriklerin kısıtlanması için kullanılmaktadır. **Google**, "*Filter explicit results using SafeSearch*", <https://support.google.com/websearch/answer/510?source=gsearch&hl=en> Yandex arama motoru da müstehcen içeriklerin arama sonuçlarından filtrelenmesi için benzer bir uygulamaya sahiptir. **Yandex**, "*Filter adult content*" <https://yandex.com/support/search/additional-features/adult-filter.html>

[168] **Zittrain, Jonathan/Edelman, Benjamin**, "*Localized Google search result exclusions*", <https://cyber.harvard.edu/filtering/google/>

[169] **Internet Society**, "*Internet Society Perspectives on Internet Content Blocking: An Overview*", s. 21.

E. Bireysel engelleme

Bireysel engelleme yöntemi, belirli bir kişinin tüm internet bağlantısına erişiminin engellenmesidir. Bu yöntem özellikle internet ortamında fikrî mülkiyet ihlallerini önlemek amacıyla tartışılmış bir yöntemdir. "Üç İhlal Kuralı" olarak çevrilebilecek "Three Strikes Law" kuralına göre, internet ortamında fikrî mülkiyet ihlali yapan kişiye değişik zamanlarda iki uyarı yapılacak ve söz konusu davranışı terk etmemesi durumunda kişi ceza, yavaşlatılmış internet veya internet bağlantısının tamamen kesilmesi şeklindeki bir yaptırıma maruz kalacaktır.[170] Üç İhlal Kuralı; Tayvan, Güney Kore, Fransa, Birleşik Krallık ve Yeni Zelanda'da yasal düzeyde, İrlanda'da ise özel tedbir yöntemiyle uygulanmaktadır.[171] Keza benzer bir düzenleme tasarısı 2020 yılında ABD'de hazırlanmıştır.[172]

Önemli bir tartışma da bir kişinin belirli kişilerle iletişime geçmesinin yasaklanmasına yönelik mahkeme kararlarının internet ortamında uygulanabilirliğidir. Örneğin, aile içi şiddetin önlenmesi kapsamında hâkim tarafından verilecek önleyici tedbir kararlarıyla, korunan kişinin iletişim araçları ile veya sair surette rahatsız edilmemesi gibi özel tedbirlerin alınması mümkündür. Bu tür bir tedbir kararıyla bir kişinin belirli bir kişiyle internet ortamında iletişim kurması engellenebilir mi? Hem bilgiye erişim hem de iletişim amaçlı kullanılabilen internetin telefon ve benzeri araçlardan farklı bir çalışma yöntemi olduğu tartışmasızdır. Böyle bir kararın internet ortamında etkin şekilde uygulanması teknik olarak zordur. Ayrıca, kişilerin internete bağlanabildiği cihaz ve ortamların çe-

---

[170] Üç İhlal Kuralının hukuki, sosyal ve ekonomik boyutlarının değerlendirilmesi için bkz. **Haber, Eldar** (2011) *"The French Revolution 2.0: Copyright and the Three Strikes Policy"*, Harvard Journal of Sports and Entertainment Law, Sayı: 2, s. 297-339; Üç İhlal Kuralı ABD'nin Kaliforniya eyaletinde farklı şekilde uygulanmaktadır. CAL. PENAL CODE § 667 (2011) düzenlemesine göre üç suçtan dolayı hüküm giyen kişi suçun niteliğine bakılmaksızın 25 yıl hapis cezasıyla cezalandırılır. Bu konuda kapsamlı bir inceleme için bkz. **Kieso, Douglas W.** (2005) *Unjust Sentencing and the California Three Strikes law*, New York, LFB Scholarly Pub.

[171] **Haber**, s. 299.

[172] **Trendacosta, Katherine**, *"This Disastrous Copyright Proposal Goes Straight to Our Naughty List"*, <https://www.eff.org/deeplinks/2020/12/disastrous-copyright-proposal-goes-straight-our-naughty-list>

şitlenmesi kişiye özel engellemelerin nasıl uygulanacağını da tartışmalı hâle getirecektir.

F. Cihaz temelli engelleme

Ağda cihaz temelli engellemelerin de uygulanması mümkündür. İkinci bölümde incelendiği üzere yerel ağda MAC adresi sabit olduğu için ağ içerisinde gönderici ve alıcıların tanımlanması mümkündür. Ayrıca *router*ların sadece belirli bir MAC adresinden trafiği kabul etmesi sağlanarak ağa izinsiz bağlantıların kısıtlanması mümkündür. Aynı doğrultuda belirli bir içerik politikası kapsamında da cihaz temelli engellemenin uygulanması mümkündür.

Öte yandan modemlerin veya *router*ların, erişim engellemenin etkinliğini artırmak amacıyla programlanması mümkündür. Özellikle erişim sağlama hizmetinin devlet tekelinde olduğu, kullanıcıların belirli model ve tipte modem ve *router* kullandığı alanlarda cihaz temelli kısıtlamalar uygulanabilir. Böylece internete bağlanılan ilk noktadan filtreleme veya erişim kısıtlamasının uygulanması söz konusu olabilir.

III. Engelleme sürecine göre

A. Doğrudan engelleme

Doğrudan engelleme durumunda, internet içeriği, muhataba herhangi bir ihtar yapılmadan engellenmektedir. Bu yönteme, özellikle içeriğin suç teşkil ettiği veya yayında kalmasının zararı artırdığı durumlarda başvurulmaktadır. Ayrıca hem içerik hem de erişim sağlayıcının yurt dışında bulunması durumunda bu yöntem özellikle tercih edilmektedir. Diğer bir deyişle, ülkede web sitesiyle ilgili herhangi bir muhatabın bulunmadığı durumlarda bu engelleme yöntemine müracaat edilmektedir.

B. Uyar-kaldır yöntemiyle engelleme

Uyar-kaldır yönteminde, adli veya idari birimler, hukuka aykırı veya zararlı içeriğin kaldırılması için içerik sağlayıcıya ya da somut olayın özelliklerine göre servis sağlayıcıya ihtarda bulunmaktadır. İçerik sağlayıcı veya yer sağlayıcı tarafından içeriğin belirli bir süre içerisinde kaldırılmaması durumunda erişim engelleme kararı gündeme gelmektedir. İçerik veya yer sağlayıcılar, bu süre zarfında kararın hukuka uygunluğunu sorgulama fırsatı bulabildikleri için kendilerini savunabilmekte ve olası bir erişim engelleme kararının olumsuz etkileri bu şekilde bertaraf edilebilmektedir.[173] Bu yöntem ancak içerik ve erişim sağlayıcıdan en az birinin yurt içinde olması veya ülkede bir temsilcisi bulundurması durumunda etkili olarak kullanılabilmektedir.

Uyar-kaldır yöntemi, uluslararası internet hukukunun en temel ilkesi hâline gelmiştir. Uyar-kaldır, ihtilafların arabuluculuk yöntemiyle çözümlenmesine benzetilebilir. Uyuşmazlıkları pratik şekilde çözmeye imkân tanıdığı için usul ekonomisine de hizmet etmektedir.

Uyar-kaldır bildirimleri münferiden gönderilebileceği gibi otomatik olarak toplu şekilde de gönderilebilir. Otomatik bildirim yöntemi özellikle telif haklarının korunması amacıyla sıklıkla kullanılmaktadır. İnterneti bir içeriğin dijital ayak izini takip ederek tarayan uygulamalar, standart ihlal bildirim metinlerini alan adı, IP veya sitede tespit edilen başka bir e-posta adresine otomatik olarak göndermektedir. Bu esnada, arama motorlarından söz konusu içeriğe verilen bağlantıların kaldırılması için ilgili şikâyet mekanizması da harekete geçirilmektedir.

Otomatik uyar-kaldır yönteminin avantajı bir hakkı -bu bazen kişilik hakkı bazen telif hakkıdır- etkin şekilde koruması; dezavantajı ise ilgisiz içeriği engelleme riski taşımasıdır. Telif örneğinden hareket etmek gerekirse, hukuken izin verilen sınırlar içerisinde bir konuyu eleştirmek amacıyla bir videonun bir kısmının kullanılması durumunda dahi otomatik uyar-kaldır yöntemi neticesinde hukuka uygun içerik kaldırılabilir

[173] **Akdeniz, Yaman/Altıparmak, Kerem** (2008) *İnternet: Girilmesi Tehlikeli ve Yasaktır - Türkiye'de İnternet İçerik Düzenlemesi ve Sansüre İlişkin Eleştirel Bir Değerlendirme*, Ankara: İmaj.

yani "sansüre uğrayabilir". Öyle ki bir telif hakkı sahibi kendi içeriğini bile yanlışlıkla kaldırtabilir.[174]

Tüm bu sorunlar ışığında, hakkını korumak isteyen tarafa düşen en önemli sorumluluk, henüz uygulamanın tasarım aşamasında, kötüye kullanımı önlemek için gerekli koruma tedbirlerini hayata geçirmesi ve hak arama yollarının etkinliğini sağlamasıdır. Özellikle bu konuda salt otomatik botlarla değil, doğrudan insan müdahalesiyle şikâyetlerin sunulması imkânı tanınmalıdır.

IV. Engelleme süresine göre

A. Geçici engelleme

Bir internet içeriğine erişimin, tedbir amaçlı olarak geçici süreyle engellenmesi mümkündür. Bu yola, hukuki bir ihtilaf durumunda ihtiyati tedbir, bir suç şüphesinin varlığı hâlinde ise koruma tedbiri olarak başvurulabilmektedir. İhtiyati tedbirin amacı, bir dava açmadan önce veya dava sırasında geri dönülmez hak kayıplarının oluşmasını önlemek veya mevcut durumun devamını engellemektir.[175] Koruma tedbirleri, suç şüphesinin ortaya çıkmasıyla yargılama yapılarak kesin hükme varıncaya kadar yargılamanın sağlıklı işlemesini temin edecek tedbirlerdir.[176] Koruma tedbirlerine başvurularak, haklı görünüşe öncelik verilerek, ortada henüz kesin bir hüküm olmadan temel hak ve hürriyetlere müdahale edilmektedir.[177]

Geçici engellemenin bir diğer türü ise belirli bir dönemde belirli bir konuya veya içeriğe yönelik engelleme uygulanmasıdır. Örneğin, seçim

---

[174] **Der Sar, Ernesto Van**, "*Hollywood Studios Flag Their IMDb Listings as "Pirate" Links*", <https://torrentfreak.com/hollywood-studios-flag-their-imdb-listings-as-pirate-links-180818/>

[175] **Kuru, Baki/Arslan, Ramazan/Yılmaz, Ejder** (2005) *Medeni Usul Hukuku*, Ankara, Seçkin Yayıncılık, s. 694.

[176] **Kunter, Nurullah/Yenisey, Feridun/Nuhoğlu, Ayşe** (2006) *Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku*, İstanbul, Beta Yayınları, s. 753.

[177] **Kunter/Yenisey/Nuhoğlu**, s. 753.

dönemlerinde veya olağanüstü hâl durumunda belirli içeriklere veya platformlara müdahale edilmesi. Korona virüsü salgını sırasında ağ trafiğini rahatlatmak için Netflix benzeri platformların kısıtlanması da buna örnek olarak gösterilebilir. Benzer şekilde, dezenformasyonla mücadele bağlamında bot ve trol hesapların tespiti için geçici engelleme bir araç olarak kullanılabilir.[178]

B. Kalıcı engelleme

Mahkemeler veya idari makamlar tarafından bir internet içeriğine erişimin kalıcı olarak engellenmesi kararı verilebilir. Öte yandan, bazı durumlarda, geçici bir tedbir olarak başvurulan koruma tedbirleri kalıcı engellemeye sebebiyet verebilmektedir.[179] İhtiyati tedbir kararı alındıktan sonra zamanında dava açılmazsa karar kendiliğinden hükümsüz hâle geleceği için karar gereğince erişimi engellenmiş içeriğe erişimin tekrar açılması gerekir. Aynı şekilde, ceza yargılamasının ortadan kalkmasıyla koruma tedbiri olarak uygulanan erişim engellemenin de kaldırılması lazımdır. Ancak, bürokratik sebeplerle internet içerikleri üzerindeki bu tür engellemeler çoğu zaman kaldırılmamaktadır.

Başka bir ülkede erişim engeli konulan web siteleri, erişim engelini kaldırmak için o ülkedeki itiraz mekanizmalarını işletmenin ekonomik külfeti sebebiyle engellemeleri kaldıramamaktadır. Özellikle internet içeriklerinin farklı ülkeler tarafından engellendiği durumlarda bu külfet daha da artmaktadır. Bunun sonucunda bu tür web sitelerine erişim belirsiz süreyle engellenmiş olmaktadır. Web siteleri yanlışlıkla engellenen site sahipleri de yaptırıma uğrama korkusuyla itiraz mekanizmalarını harekete geçirmekten çekinebilmektedir. Bu da internet içeriklerinin kalıcı olarak engellenmesine sebep olmaktadır.

---

[178] Bkz. **Roy, Eleanor Ainge**, "*Papua New Guinea bans Facebook for a month to root out 'fake users'*" <https://www.theguardian.com/world/2018/may/29/papua-new-guinea-facebook-ban-study-fake-users>

[179] **Akdeniz/Altıparmak**, s. 69.

V. Engelleme sistemine göre

A. Otomatik engelleme

Otomatik engelleme yönteminde, hukuka aykırı veya zararlı olarak nitelendirilen içerik, ağdaki özel bir filtreleme uygulaması aracılığıyla engellenmektedir.[180] Söz konusu filtreleme yazılımı belirli anahtar kelimeleri veya belirli internet sitelerine erişimi engelleyebilir. Otomatik engellemeye esas veri tabanlarının oluşturulmasında engellemenin ağ kapsamına göre farklı yöntemler kullanılabilmektedir. Referans veri tabanı doğrudan İSS veya kamu otoritesince oluşturulabileceği gibi kaynak ve zaman tasarrufu yapmak için başka hizmet sağlayıcılardan, örneğin içerik işaretleme hizmet sağlayıcısından da temin edilebilir.

Veri tabanının yönetimi ve güncellenmesi bu yöntemdeki en temel sorundur. Ayrıca, bu yöntemin kullanılmasının çeşitli sakıncaları bulunmaktadır. Erişimin, ana internet omurgası veya İSS temelli engellenmediği durumlarda, web sitelerine sadece kamu kurumları veya internet kafelerden erişilemediği için içerik sahipleri bu tür engellemelerden haberdar dahi olamamaktadır.[181] Öte yandan, bilhassa listelerin özel şirketler tarafından hazırlanıp kullanıldığı durumlarda veri tabanının denetimi mümkün olmadığı için engellemeler keyfîliğe yol açmaktadır. Nihayetinde, engellenecek içerikler için bu tür durumlarda son kararı kamu otoritesi yerine özel şirketler vermiş olmaktadır.

Sadece kamu otoriteleri değil, bireysel kullanıcılar da özellikle ağ güvenliğini sağlamak, zararlı içerikleri önlemek ve benzeri amaçlarla filtreleme yazılımları kullanabilmektedir. Kullanıcılar bu yazılımlarda daha çok bulut temelli çözümleri tercih etmekte, bu şekilde içeriğin incelenmesi kullanıcının bilgisayarı veya mobil cihazı yerine ağda gerçekleştirilmekte,

---

[180] **Zittrain, Jonathan/Palfrey, John** "*Internet Filtering: The Politics and Mechanisms of Control*": Deibert, Ronald/Palfrey, John/Rohozinski, Rafal/Zittrain, Jonathan (Editörler) *Access denied: the practice and policy of global Internet filtering*, Cambridge, MIT Press, s. 36-38.

[181] **Akdeniz/Altıparmak**, s. 49.

içerik kontrolü pratik şekilde yapılmaktadır.[182] Ağ trafiği üçüncü şahıslara ait ağa aktarıldığı için bu tür uygulamaların kişisel verilerin korunması ve mahremiyeti ile güvenlik açısından önemli sonuçları vardır.

Otomatik engelleme, kullanıcı bildirimlerine veya geri beslemesine dayalı olarak da gerçekleştirilebilir. Kullanıcılar, belirli bir içeriği doğrudan şikâyet ederek veya hukuka aykırı ya da zararlı olarak işaretleyerek otomatik engelleme sisteminin bu içeriğe yönelik bir tedbir uygulamasını sağlayabilirler. Bazı platformlarda *super-flagging* olarak da adlandırılan özel yetkilerle, platformdaki belirli içeriklerin özel iş ortakları ve hatta kolluk kuvvetlerince gözden geçirilmesini sağlamaya dönük bir uygulama hâlihazırda mevcuttur.

Bu yöntemin en büyük avantajı, kullanıcıların platform içerik politikasının icrasında doğrudan söz sahibi olması, katılımcılığın sağlanmasıdır. Ancak bu, istismara ve çoğunluğun kendi içerik tercihlerini dayatmasına da yol açabilir. Söz konusu durum bir nevi akran sansürü olarak da nitelendirilebilir. Burada platforma düşen en önemli sorumluluk, platformu tasarım aşamasında kötüye kullanımı önlemek için gerekli tedbirleri uygulaması ve hak arama yollarının etkinliğini sağlamasıdır. Özellikle bu konuda salt otomatik botlarla değil, doğrudan insan müdahalesiyle şikâyetlerin sunulması imkânı tanınmalıdır.

B. Bireysel engelleme

Bireysel engelleme yönteminde her bir internet içeriği için müstakil engelleme kararı alınmaktadır. Alınan kararlar, icra edilmek üzere mahkemeler veya kamu yetkililerince engellemenin ağ kapsamına göre ülke genelinde faaliyet gösteren her bir İSS'ye gönderilmekte veya doğrudan internet omurgasında uygulanmaktadır.

---

[182] **Internet Society**, "*Internet Society Perspectives on Internet Content Blocking: An Overview*", s. 11.

VI. Engellemenin kaynağına göre

A. Kullanıcı nezdinde engelleme

İnternet içeriğine internet kullanıcısının bağlandığı ağ noktasında erişim engellenebilir. Yaygın kullanılan engelleme yöntemi de budur. Kullanıcının kendisi de bir filtreleme yazılımı ve hatta *adblocker* gibi reklam engelleme uygulaması kullanarak belirli içeriğe erişimi engelleyebilir.

B. Hizmet sağlayıcı nezdinde engelleme

İnternet içeriğini engellemenin diğer bir yöntemi, hizmet sağlayıcı nezdinde uygulanan engellemedir. Bu engelleme türünde hizmet sağlayıcı (teknik yetkisine göre yer veya içerik sağlayıcısı) hizmetlerine veya sunulan belirli içeriğe bazı kullanıcıların erişimi kısıtlanmaktadır. Yukarıda açıklanan platform temelli engelleme aynı zamanda hizmet sağlayıcı nezdinde engellemenin de örneğidir.[183]

VII. Engellemenin hedef içeriğinin türüne göre

A. Statik engelleme

Bazı internet içerikleri belirli bir URL'de statik olarak yer alırken bazı içerikler canlı olarak sunulmakta, bunlara aynı URL adresiyle tekrar erişilememektedir. Bu doğrultuda, statik içeriğin engellenmesiyle dinamik içeriğin engellenmesi farklı yöntem ve teknikler gerektirmektedir. Statik içeriğin engellenmesi bir özellik arz etmemekte, belirli bir URL adresindeki içerik engellenmektedir.

B. Dinamik engelleme

Bazı internet içerikleri internet ortamında statik olarak yer almamakta, belirli URL adreslerinde sadece belirli bir anda görüntülenmektedir. Canlı video gösterimleri, dinamik içeriklerin en bilinen örnekleridir. Bu

[183] Bkz. **§4(II)(Ç)**[Platform temelli engelleme].

tür sistemlerde farklı içerikler için farklı zaman aralıklarında yayın yapılabilmekte, farklı URL adreslerinin yanı sıra farklı IP adresleri de yayın için kullanılabilmektedir.

Dinamik içeriklerin hukuka aykırı veya zararlı unsurlar barındırması durumunda, bunlara müdahale edebilmek için hızlı ve teknik değişikliklere hemen cevap verecek nitelikte yöntemlere ihtiyaç vardır. Ayrıca, bu tür içerikler yargılamaya konu olduğunda esaslı bir delillendirme sorunu ortaya çıkmaktadır. Zira dinamik içerik, talep konusu yapıldığı esnada sabit bir URL adresinde yer almamakta, içeriğin sonradan tespiti mümkün olmamaktadır. Bu tür içerikler için önleyici tedbirlerin alınması veya idari makamlara özel yetkiler tanınması tartışılmaktadır.[184]

VIII. Engelleme kararının alınış zamanına göre

A. İhlal sonrası engelleme

En klasik ve yaygın engelleme yöntemi, engelleme kararının ihlalden sonra alındığı yöntemdir. Bu yöntemde, internet ortamında mevcut bulunan bir içeriği hedef alan özel bir engelleme kararı alınır. Diğer bir deyişle, somut bir içeriğe yönelik somut bir karar alınmaktadır.

B. İhlal öncesi engelleme

Bazı istisnai durumlarda, internet ortamında yer alan içeriğe hızlı şekilde müdahale etme gereği doğar. Bunun için mahkemelere ve belirli durumlarda idari makamlara hızlı karar alınması ve kararın gereğinin icra edilmesi adına yetki verilebilmektedir.

Kimi durumlarda, hukuka aykırı içerik henüz internet ortamında yer almadığından ihlal doğmamıştır ancak doğması muhtemeldir. İhlal durumunda telafisi mümkün olmayan zararlar ortaya çıkacaktır. İşte ihlal öncesi engelleme yönteminde, istisnai bazı durumlarda belirli tür içeriğe

[184] Bu konuda güncel bir örnek için bkz. **Maxwell, Andy**, "MPAA Granted 'Dynamic' Pirate Site Blocking Order in Singapore" <https://torrentfreak.com/mpaa-granted-dynamic-pirate-site-blocking-order-in-singapore-181006/>

yönelik peşin bir engelleme kararı verilmekte; ihlal oluştuğu zaman bu karar icra edilmektedir. Örneğin, yakında vizyona girmesi beklenen ve fikrî mülkiyet ihlaline konu olması kuvvetle muhtemel bir sinema filmi için "John Doe" (isimsiz) bir engelleme kararı alınarak internet ortamında yayımlandığı anda bu korsan içeriğe erişimin İSS'ler tarafından engellenmesi tartışılmaktadır.[185]

IX. Engellemenin genel niteliğine göre

A. Kamusal engelleme

Kamusal engelleme kamusal bir politika veya düzenleme gereği gerçekleştirilen engellemedir. Bir içeriğin, ceza kanunlarına, vergi düzenlemelerine veya belirli bir içerik kuralına uymaması sebebiyle engellenmesi buna örnektir. Bu konuda standart bir uygulama olmasa bile "*451 Unavailable For Legal Reasons*" hata kodu, içeriğin hukuki sebeplerle engellendiği hakkında fikir verebilmektedir.[186]

Öte yandan, hizmet sağlayıcılar bazen hukuki yükümlülükten kaçınmak adına içeriği belirli bölgelerin erişimine kısıtlayabilir. AB Genel Veri Koruma Tüzüğü'ne takılmamak için içeriğin kısıtlanması bunun güncel örneğidir.[187] Korona virüsü sebebiyle internet altyapısını rahatlatmak için Netflix gibi yüksek trafikli video platformlarının engellenmesi de kamusal engellemeye örnek gösterilebilir.

Bir diğer kamusal engelleme sebebi, diplomatik amaçlı engellemedir. Bir devletin başka bir devlete ait veya o devletle bağlantılı bir siteyi yahut hizmet sağlayıcıyı engellemesine misilleme olarak diğer devletin de benzer nitelikte bir engellemede bulunması bu duruma örnektir. Bu,

---

[185] Bkz. **Gupta, Juhi** (2013) "*John Doe Copyright Injunctions in India*" Journal of Intellectual Property Rights, Sayı: 18, s. 351-359.

[186] Fahrenheit 451 kitabından ihlam alan bu engelleme sebebi için bkz. **Mozilla**, "*451 Unavailable For Legal Reasons*" <https://developer.mozilla.org/en-US/docs/Web/HTTP/Status/451>

[187] Örnek engelleme için bkz. **BBC**, "*GDPR: US news sites unavailable to EU users under new rules*", <https://www.bbc.com/news/world-europe-44248448>

uluslararası hukukta bir devletin başka bir devletin tasarruflarına misli ile karşılık vermesi uygulamasının dijital diplomaside sıklıkla karşılaşılan modern bir görünümüdür.

B. Özel engelleme

Özel engelleme yönteminde, hizmet sağlayıcı, yer sağlayıcı veya içerik sağlayıcının kendi içerik veya yayın politikası gereği içerik engellenir. Örneğin, bir sosyal medya sitesinin, bazı içerikleri hukuka aykırı olmasa da filtrelemesi veya bunlara erişimi kısıtlaması gibi. Bir mobil operatörün ticari amaçla belirli reklam içeriğini trafiğinde engellemesi de buna örnek gösterilebilir.

X. Kullanılan tekniğe göre

Erişim engellemede kullanılacak teknik, devletlerin teknolojik gelişmişliğine ve ihtiyaç duyulan engellemenin yoğunluğuna göre değişmektedir. Bazı devletler temel IP engellemesi gibi yöntemlerle yetinirken bazıları farklı katmanlardan oluşan kombine teknikler kullanmaktadır. Engelleme tekniklerinin etkili olması için engellemenin ülke genelindeki internet trafiğinin tüm çıkış noktalarında uygulanması gerekir.

Erişim engellemede yüzde yüz başarılı bir teknik bulunmamaktadır.[188] Bu amaçla kullanılabilecek her bir tekniğin kendine özgü güçlü ve zayıf tarafları vardır. Bu sebeple devletler, kullandıkları teknolojinin mükemmel olmasından ziyade etkili olmasına önem vermektedir.[189]

Her bir engelleme tekniği, ilgisiz web sitelerini engelleme (aşırı engelleme) veya hedeflenen web sitelerini engelleyememe (etkisiz engelleme) riski taşımaktadır.[190] Söz konusu durum, hastalık teşhisinde

---

[188] **Zittrain/Palfrey**, s. 34.

[189] **Goldsmith/Wu**, s. 103.

[190] **Murdoch, Steven J/Anderson, Ross** (2008) "*Tools and Technology of Internet Filtering*": Deibert, Ronald/Palfrey, John/Rohozinski, Rafal/Zittrain, Jonathan (Editörler) *Access denied: the practice and policy of global Internet filtering*, Cambridge, MIT Press.

kullanılan yöntemlere benzetilerek hatalı pozitif (*false positive*) ve hatalı negatif (*false negative*) olarak da ifade edilebilir.

İnternet içeriğinin hızla değişmesi ve içeriğin değişik web sitelerine yayılması, engellemeyi çoğu zaman imkânsız kılmaktadır. Bu sebeple, kullanılacak tekniğin etkinliği engellenmek istenen web sitesinin özelliklerine göre değişmektedir. Aşağıda, yaygın olarak kullanılan erişim engelleme teknikleri yer almaktadır.

A. IP engellemesi

İkinci bölümde incelendiği üzere, internet ortamında ağ noktaları IP adresi üzerinden konumlandırılır. En temel erişim engelleme yöntemi, içeriğin barındığı sunucuların IP adreslerini engellemektir. Engellemenin kapsamına göre, ya her bir İSS nezdinde ya da ana internet omurgasında ilgili içeriğin bulunduğu ağın veya sunucunun IP adresinin engellenmesi yoluna gidilebilmektedir.

IP engellemesi en pratik engelleme yöntemidir ve bu tekniği uygulamak için kapsamlı donanım ve yazılım yatırımına gerek yoktur. Bununla birlikte, IP engellemesi tekniği başlıca iki nedenden dolayı etkin bir erişim engelleme tekniği olmaktan uzaktır. Daha önce açıklandığı üzere, bir sunucunun birden fazla internet içeriğini veya web sitesini barındırması mümkündür. "Reverse IP Address Lookup" sorgulamasıyla, bir IP adresinde barınan komşu web sitelerinin tespit edilmesi mümkündür.[191] Bu sebeple, hukuka aykırı veya zararlı içerikli bir web sitesine erişimin engellenmesi durumunda aynı sunucuda barınan zararsız diğer tüm siteler de otomatik olarak engellenmektedir. Bu durumda, ceza hukukunun temel ilkeleri olan ceza sorumluluğunun şahsiliği ve koruma tedbirlerinin ölçülülüğü ilkeleri ihlal edilmektedir. Zira engellenmek istenen web sitesiyle aynı IP adresini paylaşan tüm web siteleri söz konusu tedbire maruz kalmaktadır.

[191] Örnek bir sorgu için Reverse IP Lookup <https://hackertarget.com/reverse-ip-lookup/>

Erişim engeli uygulanan web sitesinin barındırıldığı sunucu değiştirildiğinde web sitesinin IP adresi de değişeceğinden engelleme otomatik olarak ortadan kalkar. Bazı durumlarda sunucu değiştirmeye bile gerek olmadan IP değişikliğine gitmek teknolojik olarak mümkündür. Tüm bu sebeplerden dolayı, IP engelleme yöntemi, engellenecek web sitesinin özellikleri göz önüne alınarak diğer yöntemlerle birlikte kullanıldığı takdirde etkili olacaktır.

Öte yandan, IP engellemesi bir web sitesinin tüm servislerini erişime kapatmaktadır. İnternet kullanıcıları siteyi ziyaret edemediği gibi web sitesinin e-posta servisleri de kullanılamaz hâle gelir. IP engellemesinin, servis temelli olarak yapılması teknolojik olarak mümkündür.[192] Her bir internet servisinin kendine özgü, "port" olarak adlandırılan bir alt bağlantı numarası vardır.[193] Örneğin internet trafiği temel olarak 80 numaralı port üzerinden yayın yaparken e-posta servisleri SMTP protokolü üzerinden 25 numaralı portu kullanır. Sadece 80 numaralı port üzerinde yapılacak bir sınırlama ile web trafiği engellenirken, web sitesinin diğer temel servislerinin kullanılmaya devam etmesi sağlanabilir. Bu şekilde, erişim engellemenin özellikle iletişim özgürlüğü üzerindeki ağır sonuçlarının kısmen hafifletilmesi mümkün olabilir.

B. DNS engellemesi

İkinci bölümde incelendiği üzere, internet sitelerine erişim için kullanılan IP adreslerinin hatırlanması zor olduğundan DNS alan adı sistemi geliştirilmiş ve IP adreslerinin yerine geçen, alan adı olarak adlandırılan harf dizilerinin kullanılması sağlanmıştır.DNS engelleme tekniğinde alan adı tüm alt içeriği ile birlikte erişime kapatılmaktadır.[194] Kullanıcı web sitesine girmeye çalıştığında, alan adlarının IP çözümlemesini yapan DNS sunucusu, engellenmesi istenen web sitesinin çözümleme talebini yanıtsız bırakır. Bu şekilde siteye erişim engellenmiş olur. Her bir İSS nezdinde uygulanacak DNS engellemesi yöntemi sayesinde, internet

[192] **Murdoch/Anderson**, s. 59.

[193] İnternet servislerinin kullandıkları port numaraları için bkz. **IANA**, "*Port Numbers*", <http://www.iana.org/assignments/port-numbers>

[194] **Murdoch/Anderson**, s. 60.

trafiğine ulaşmadan önce kullanıcı erişim sorgusunun engellenmesi ve böylece ağ trafiğinin hafifletilmesi de mümkün olmaktadır. Ayrıca, sisteme müdahale edilerek alan adının tamamen alakasız bir IP adresine de gönderilmesi mümkündür.

DNS engelleme tekniği altyapıda kapsamlı bir dönüşüm yapılmadan, minimum maliyetle, pratik şekilde uygulanabilmektedir. Fakat bu yöntemin en büyük dezavantajı, IP engellemesinde olduğu gibi, alan adını tüm alt içeriği ile birlikte erişime kapatmasıdır.[195] Dünya çapında yayın yapan ve milyonlarca internet kullanıcısına ücretsiz blog, e-posta veya benzeri hizmetler veren web sitelerinin engellenmesi ağır sonuçlar doğurabilmektedir. Özellikle Cloudflare gibi, milyonlarca web sitesine içerik dağıtım hizmeti ve özel DNS hizmeti sunan bir altyapının isim sunucularını engellemek, internet ortamına ölçüsüz bir müdahale doğuracaktır.

Birden fazla web sitesini barındıran sunucu üzerinde uygulanan DNS engellemesi -tıpkı IP engellemesinde olduğu gibi- ceza hukukunun temel ilkeleri olan ceza sorumluluğunun şahsiliği ve koruma tedbirlerinin ölçülülüğü ilkelerini ihlal eder. Keza, bu şekilde ifade özgürlüğü ile bilgiye erişim ve bilgiyi yayma haklarına da ölçüsüz bir müdahale söz konusu olabilecektir. DNS engelleme tekniğinin aşırı bir engellemeye dönüşebileceği diğer bir örnek ise URL kısaltıcılara yönelik engellemedir. Sadece bir alan adına yönelik engellemeyle milyonlarca müstakil sayfanın engellenmesi söz konusu olabilecektir.

İkinci bölümde açıklandığı üzere ülke kodlu üst düzey alan adları, tescil edildikleri ülkede barındırılmak zorunda değildir. Bu sebeple, bir web sitesinin ülke kodlu üst düzey alan adının engellenmesiyle o ülkede barındırılan web sitelerinin engellenmesi birbirinden farklı durumlardır.

---

[195] DNS engellemesinin etkileri için özellikle bkz. **Internet Society** (2012) "*Internet Society Perspectives on Domain Name System (DNS) Filtering*", <https://www.internetsociety.org/sites/default/files/Perspectives%20on%20Domain%20Name%20System%20Filtering-en.pdf>

C. URL engellemesi

URL internette resim, yazı veya müzik gibi bir kaynağa karşılık gelen, standart bir formata uygun bir karakter dizgisidir. URL internet üzerindeki bir kaynağın koordinatıdır. Pratik bir anlatımla URL, internette gezinirken herhangi bir kaynağa tıklandığında tarayıcının adres çubuğunda görünen adrestir.

URL engellemesi koordinatları bilinen, hukuka aykırı veya zararlı bir içeriğin engellenmesi amacıyla kullanılan bir tekniktir.[196] Bu yöntemin en önemli avantajı, hukuka aykırı veya zararlı içerik için tüm web sitesinin içeriğinin engellenmesine gerek kalmamasıdır. DNS ve IP engelleme yöntemlerinin aksine, bu engelleme yönteminin kullanılması için belirli bir donanım ve yazılım yatırımına ihtiyaç vardır.

URL engelleme *proxy* aracılığıyla, güvenlik duvarlarında veya *router*lar aracılığıyla uygulanabilir.[197] Bir kullanıcının hukuka aykırı veya zararlı olarak etiketlenmiş bir URL adresine erişip erişmediğini kontrol edebilmek için İSS'nin o kullanıcının tüm internet trafiğini incelemesi gerekmektedir. Bu teknik "derin paket analizi" (DPI - Deep Packet Inspection) olarak da adlandırılmaktadır ve önceden belirlenmiş bir ağ politikası gereğince işletmecilerin, sabit veya mobil ağları üzerinden iletilen tüm paketlerin içeriklerini incelemesi esasına dayanmaktadır.[198] DPI ayrıca kurumsal engelleme yöntemi olarak, belirli verilerin kurumsal ağ dışına çıkmasını önleme (DLP - Data Loss Prevention) uygulamalarıyla birlikte veya müstakil şekilde ya da kurumsal ağda belirli içeriklerin takibi için de kullanılabilir.

DPI teknolojisinin de bazı eksiklikleri ve zayıf yanları vardır. Her şeyden evvel DPI teknolojisi, şifrelenmiş internet içeriğini ("https://" ile başlayan URL'ler gibi) filtreleyemez. Yine, tüm paketlerin okunması için sisteme müdahale edilmesi de güvenlik açısından esaslı riskler taşımak-

---

[196] **Murdoch/Anderson**, s. 64.

[197] **Internet Society**, "*Internet Society Perspectives on Internet Content Blocking: An Overview*", s. 15.

[198] **Dodd**, s. 10-14.

tadır.[199] Bu nedenle, İSS'lerin normal trafik ile hukuka aykırı veya zararlı içerik olarak işaretlenmiş trafiği ayrıştırması "https" protokolünde mümkün değildir. Ayrıca, DPI teknolojisinin internet trafiğini yavaşlatma riski bulunmaktadır. Hıza etki etmemesi için külfetli bir donanım ve yazılım yatırımına ihtiyaç vardır.

DPI teknolojisinin uygulandığı ağlardaki diğer bir risk ise bilgi güvenliği riskidir. Nihayetinde bu tekniğin uygulanması için, internete erişilen her bir noktada hem sabit hem mobil ağlarda tüm trafiğin incelenmesi gerekmektedir.[200] Dolayısıyla bu teknik, kişisel verilerin korunması ve bilgi güvenliği açısından çeşitli riskleri beraberinde getirmektedir.

Öte yandan, URL engelleme tekniğinin bazı durumlarda DNS veya IP engelleme benzeri sonuçlar doğurarak ölçüsüz engellemeye yol açması mümkündür. Örneğin, bir internet sitesinin tüm sayfaları URL engelleme tekniğiyle engellenirse böyle bir sonuç doğacaktır. Benzer şekilde, bir internet sitesinin ana açılış sayfası (index.html, index.php, index.asp gibi) da nihayetinde bir URL olduğu için bu indeks sayfası engellenirse DNS engellemeye benzer bir sonuç doğacaktır. Keza, bir e-ticaret sitesinin veya pazar yeri platformu içindeki bir mağazanın URL'si engellenirse yine bu tür sonuçlar doğar. Dolayısıyla, URL engellemenin her zaman hakkaniyetli sonuçlar doğuracağını söylemek mümkün değildir. Anılan örneklerde olduğu gibi bu sistem istismar edilerek ölçüsüz engellemeler yapılması söz konusu olabilir.

D. Port engellemesi

İkinci bölümde incelendiği üzere her bir internet servisinin kendine özgü, port olarak adlandırılan bir alt bağlantı numarası vardır. Port numarası, bağlantının bir işletim sistemindeki sonlandırılma noktasıdır. Port

---

[199] DNS önbellek zehirlenmesi bu tür riskleri barındıran yöntemlerden birisidir. Bu konuda bkz. **Son, Sooel/Shmatikov, Vitaly** (2010) "*The Hitchhiker's Guide to DNS Cache Poisoning*": Jajodia, Sushil/Zhou, Jianying (Editörler) *Security and Privacy in Communication Networks*, Berlin, Springer, s. 466-483.

[200] İnternete bağlantı için belirli tür donanım ve yazılımın kullanılmasının zorunlu tutulması durumunda engellemenin kullanıcı nezdinde gerçekleşmesi ihtimali yok sayılmamaktadır.

engelleme tekniğinde, belirli hizmetlerin kullandığı port numaralarına yönelik ve sadece bu portlarla sınırlı bir kısıtlama yapılmaktadır. Örneğin, VoIP (Voice over Internet Protocol) hizmetlerine yönelik bir müdahale için sadece bu hizmetlerin kullandığı portların engellenmesi gibi.

E. Proxy engellemesi

Proxy, internet içeriğine erişim için kullanılan bir ara sunucudur.[201] *Proxy* sunucusuna daha çok internetteki bir içeriğe doğrudan bağlanmak istenilmediği durumlarda başvurulmaktadır. *Proxy* kullanmanın çeşitli avantajları bulunmaktadır. *Proxy* sunucusu erişilmek istenen veriyi önbelleğine aldığı için kullanıcılar web sitelerine daha hızlı şekilde erişir ve gereksiz ağ trafiğinin önüne geçilir.

Proxy sunucusu içerik ve kullanıcı arasında filtreleme görevi üstlendiği için kullanıcının istenmeyen içerikle veya virüs gibi zararlı programlarla karşılaşma riskini ortadan kaldırır. Ayrıca, *proxy* sunucuları içerik ve kullanıcı arasında yer aldığından asıl kullanıcının kimliğinin gizlenmesine olanak verir. Sağladığı bu avantajlar sebebiyle *proxy* sunucuları, üniversiteler ve kütüphaneler gibi internetin ücretsiz ve ortak kullanıma açık olduğu alanlarda yaygın şekilde kullanılmaktadır. Devletler *proxy* sunucularını internet bağlantı noktalarına konumlandırarak web içeriğini filtreleyebilmekte ve bireylerin hangi web sitesine veya hangi tür içeriğe erişebileceğini belirlemektedir.[202] *Proxy* sunucuları bu şekilde erişim engellemesi amacıyla kullanılmaktadır.

F. İçerik engellemesi

IP ve DNS engellemesi teknikleri kullanılarak TCP/IP protokolü altında belirli bir noktaya gönderilen veya belirli bir noktadan alınan veri parçacıklarının engellenmesi sağlanmakta, veri içeriğine müdahale edilmemektedir. İçeriğe müdahale edebilmek için ağdaki veri akışına müdahale etmek gerekir. Bu şekilde hem URL hem alan adı hem de içeriğe müdahale etmek mümkün olmaktadır.

---

[201] **Dodd**, s. 439.

[202] **Murdoch/Anderson**, s. 61.

Ağın belirli kuralları tanıyarak otomatik engelleme yapması, fikir ve sanat eserlerinin dijital ortamda korunması için kullanılan Dijital Hak Yönetimi (DRM - Digital Rights Managament)[203] sistemleriyle aynı prensiplerle çalışmaktadır. DRM sistemleri hem eserler üzerindeki hakların dijital ortamda tanımlanmasını hem de bu hakka dayanarak eserin kullanım ve erişimini denetlemeyi sağlamaktadır.[204] DRM sistemleri nihayetinde birer ağ yazılımı olduğu için ağın kendisinin belirtilen sınırlamaları otomatik olarak tanıması ve ancak izin verilen türde verilerin akışına izin vermesi sağlanmaktadır. Diğer bir deyişle, bu sistem hukuk kurallarının somut olaya uygulanmasında olduğu gibi sadece davranışı tespit etmekle yetinmemekte, ağdaki ihlalleri yaptırıma bağlamakta ve ayrıca bireyleri sürekli gözetleyerek otosansür uygulamalarını sağlamaktadır.[205]

Daha önce açıklandığı üzere, *router*lar, içerik katmanına müdahale etmeksizin veri paketlerinin üzerinde yer alan etiket katmanını esas alarak veri iletimini gerçekleştirmektedir. Veriler parça parça iletildiğinden, engellenecek içeriğin tespit edilebilmesi için paketlerin bir noktada birleştirilerek denetlenmesi gerekmektedir. Engellenmeyen içerik, tekrar parçalara ayrılarak nihai iletim adresine gönderilmelidir. *Router*ların, DRM sistemleriyle aynı prensiplere göre programlanarak ağ üzerinde belirli kelimeleri içeren veri parçalarını denetlemeleri sağlanabilmektedir. Bu sayede, bir noktadan başka bir noktaya iletilen veri parçalarının içerik katmanında kelime, URL veya alan adı temelli inceleme yapılması mümkün olmaktadır. Bunun için DPI teknolojisinin kullanılması gerekir.

Router programlama sisteminin farklı devletler tarafından kullanılması durumunda bir veri, geçtiği her noktada hukuka uygunluk denetimine tabi tutulmuş olmaktadır. Diğer bir deyişle, ağ tarafsızlığı ortadan kalkarak devletlerin kendi kurallarını internet ağına yaymaları ve eş zamanlı icra etmeleri gibi bir durum ortaya çıkmaktadır.[206]

---

[203] DRM, dijital formattaki içeriğin bilişim sistemleri tarafından tanımlanmasını ilgilendiren süreç ve teknolojilerin genel adıdır. Bkz. **Bayamlıoğlu**, s. 302 vd.

[204] **Bayamlıoğlu**, s. 303.

[205] **Bayamlıoğlu**, s. 304.

[206] Ağ tarafsızlığı için bkz. **§2(III)(Ğ)**[Ağ tarafsızlığı].

DPI teknolojisi çok farklı içerik türleriyle çalışabilir. Sadece metin temelli kullanılabildiği gibi ileri düzey sistemlerde resim veya farklı içerik türlerini de tanıyabilir, filtreleyebilir veya engelleyebilir. Özellikle metin temelli kısıtlamaları aşmak için aynı metnin resim formatında kullanıldığı durumlarda resimlerin sistemde analiz edilmesiyle hedef resim filtrelenebilir veya engellenebilir.

Öte yandan içerik engellemesi çoğu zaman aşırı engellemeye sebep olmaktadır. Örneğin, İngiliz Essex ve Sussex Üniversitelerinin web siteleri erişim engelleme sistemine "zararsız site" olarak tanıtılmadıkları sürece alan adlarında bulunan "sex" kelimesi sebebiyle cinsel içerikli web sitesi muamelesi görecektir.[207] Benzer şekilde, cinsel hastalıklar konusunda bilgi veren bir sağlık sitesi de bu tür bir engellemeye takılabilecektir.

Diğer taraftan, web sitelerinin içeriğinin (https şeklinde) şifreli olarak sunulduğu durumlarda, içerik engelleme sistemleri engelleme yapamamaktadır. Şifreli internet trafiği normal internet trafiğinden görece yavaş olmasına rağmen, internet bağlantı hızlarındaki artışlar bu yavaşlığı esaslı bir faktör olmaktan çıkarmıştır. Ayrıca, bu alandaki teknoloji ucuzladığından yaygınlaşması daha da hızlanmıştır.

G. Siber saldırı yöntemiyle engelleme

Siber saldırı yöntemleri kullanılarak internet ortamında yer alan içeriğe erişimin engellenmesi, yavaşlatılması veya aksatılması mümkündür. Bazen devletler, egemenlik alanları dışında kalan yabancı ağlarda barındırılan içeriklere erişimi tamamen engelleme ihtiyacı duyabilir. Bu durum daha çok ülke genelinde erişim engellemenin beklenen faydayı vermediği veya siyasi muhaliflerin yahut terör örgütlerinin propagandalarını tamamen engelleme ihtiyacı duyulduğunda gündeme gelmektedir. Örneğin, devlet siyasi muhaliflerin internet içeriklerine erişimi ülke genelinde engellemiş ve içerikleri ülke genelinde etkisiz kılmış olabilir.

---

[207] Benzer şekilde İngiltere Başbakanının özel danışmanı Dominic Cummings de sosyadı Twitter'ın pornografiyi engelleme filtresine takılmıştır. **Hern, Alex**, "*Anti-porn filters stop Dominic Cummings trending on Twitter*", <https://www.theguardian.com/politics/2020/may/27/anti-porn-filters-stop-dominic-cummings-trending-on-twitter>

Ancak, içerikler dünya genelinde erişilir olmaya devam ettiği için devlet, engelleme amacına ulaşamamıştır.

Bu gibi durumlarda, bazı otoriter devletler, kullanımı hukuka aykırı olan Distributed Denial of Service (DDOS) isimli ağ saldırı yöntemine başvurabilmektedir. DDOS atakları 1988 yılından beri farklı şekillerde var olmuş bir ağ saldırı yöntemidir.[208] Benzer şekilde Service Overloading, Message Flooding, Clogging, Spoofing, ARP Spoofing, IP Spoofing, DNS Spoofing, DNS Hijacking, DNS Poisoning, DNS Throttling gibi teknikler de bu amaçla kullanılabilir.

DDOS, bilişim sistemlerini işlemez hâle getirmek için kullanılan bir ağ saldırı yöntemidir.[209] DDOS atakları, hem ağ sistemini çökertmek hem de sistemi gereksiz sorgularla meşgul edip normal işleyişini yavaşlatmak için kullanılmaktadır. DDOS saldırılarında virüs veya başkaca bir yöntem kullanılarak birçok bilgisayarın belirli bir hedefe gereksiz komut göndermesi sağlanır. Aynı anda birden çok bilgisayarın hedefe saldırması, asıl saldırı yapanın kimliğinin gizlenmesine yardımcı olur. Aynı anda binlerce bilgisayardan milyonlarca sorgu alan ağ veya sunucu bu sorgulara yanıt vermekle meşgul olur. Saldırı sonucunda ya ağ tamamen çöker ya da bağlantı hızı yavaşladığı için ağa erişim zorlaşır. Böylece, siteye tüm dünya üzerinden erişim engellenmiş olur.

DDOS atakları ağ trafiğini tehdit eden en büyük siber saldırı yöntemidir. DDOS saldırılarının failleri dünyanın herhangi bir yerinden dünyadaki herhangi bir ağa saldırabilirler. DDOS atakları intikam, düşmanlık, kaybolan statünün tanınması veya elde edilmesi, siyasal aktivizm, bilgisayar kaynakları üzerinde kontrol elde etmek, ün ve şöhret kazanmak, bilgi savaşları, ekonomik veya askerî casusluk gibi amaçlarla yapılabilir. Sadece saldırmış olmak için saldırmak (elektronik vandalizm) da bu tür atakların gerekçesi olabilir.[210] Bazen devletler, binlerce bilgisayar arasından DDOS

---

[208] **Ryan**, s. 194.

[209] **McQuade, Samuel C** (2009) *Encyclopedia of cybercrime*, Westport, Greenwood Press, s. 63-64.

[210] **Schultz, E Eugene** (2004) "*Denial of Service Attacks*": Bidgoli, Hossein (Editör) *The Internet encyclopedia - Volume 1*, Hoboken New Jersey, John Wiley & Sons, s. 425.

saldırılarının asıl faillerinin tespitinin zor oluşundan yararlanarak bunu hukuka aykırı bir engelleme tekniği olarak kullanabilmektedir.

H. Alan adına el koyma veya alan adını terkin yöntemi

Alan adını terkin yönteminde, bir içeriğin internette bulunmasını sağlayan alan adı ilgili sicilden kaldırılmaktadır.[211] Bu tekniğe *domain de-registration* de denilmektedir.

Alan adlarının tescil ve terkin işlemleri yerleşik ve detaylı kurallara göre sürdürülmektedir. Bu sebeple, söz konusu engelleme tekniği çok dar kapsamda (örneğin, ülke kodlu üst düzey alan adlarında) uygulama alanı bulabilecek bir tekniktir. Ülke kodlu olmayan alan adlarının terkini, hukuka uygunluğa hangi hukuka göre karar verileceği gibi sorunları da beraberinde getirmektedir.[212] Öte yandan, ABD'nin, bu yöntemi uyuşturucu satışından taklit mal satışına kadar birçok alanda etkin kullandığını belirtmek gerekir.[213] Benzer bir mücadele, korona virüsü salgını sürecinde FBI tarafından gerçekleştirilmiştir.[214]

---

[211] **Murdoch/Anderson**, s. 64.

[212] Mart 2011'de ABD makamlarınca İspanyol bir şirkete ait olan "rojadirecta.org" adına el koyulmuş; ancak, İspanyol mahkemesi içeriğin ve internet sitesinin hukuka uygun faaliyet gösterdiğine karar vermiştir. Alan adı daha sonra sahibine iade edilmiştir. Bkz. **Samuels, Julie**, "Rojadirecta: The Government Reverses Course and Returns Domains Without Explanation. Again" <https://www.eff.org/deeplinks/2012/08/rojadirecta-government-reverses-course-and-returns-domains-without-explanation>

[213] İlgili yasal dayanak için bkz. 18 USC 1956(h), 981, 982 ve 2323; Örnek uygulama için bkz. **FBI**, "*Federal Courts Order Seizure of 150 Website Domains Involved in Selling Counterfeit Goods as Part of DOJ, ICE-HSI, and FBI Cyber Monday Crackdown*" <https://archives.fbi.gov/archives/washingtondc/press-releases/2011/federal-courts-order-seizure-of-150-website-domains-involved-in-selling-counterfeit-goods-as-part-of-doj-ice-hsi-and-fbi-cyber-monday-crackdown>; Benzer şekilde bkz. **Maxwell, Andy**, "*US Embassy Threatens to Close Domain Registry Over 'Pirate Bay' Domain*" <https://torrentfreak.com/us-embassy-threatens-to-close-domain-registry-over-pirate-bay-domain-170620/>

[214] **Stone, Jeff**, "*FBI enlists internet domain registries in fight against coronavirus scams*" <https://www.cyberscoop.com/fbi-coronavirus-scams-internet-domains/>

I. Bulut bilişim engellemesi

İkinci bölümde açıklandığı üzere, bulut bilişim dinamik olarak ölçeklenebilen ve genellikle sanallaştırılan kaynakların internet üzerinden hizmet olarak sunulduğu yeni bir bilişim yöntemidir.[215] Bulut bilişimde üç temel farklı hizmet sunum modeli vardır: hizmet olarak yazılım, hizmet olarak platform, hizmet olarak altyapı. Bulut bilişim altyapısı, barındırma hizmeti sunma veya yazılımı farklı kişilere aynı altyapı üzerinden kullandırma gibi çeşitli amaçlarla kullanılabilir.

Bulut bilişim gün geçtikçe yaygınlaşmakta ve çeşitlenmektedir. Altyapının, platformun veya yazılımın hizmet olarak sunulması yahut karma çözümler geliştirilmesi mümkündür. Özellikle *hizmet olarak yazılım* çözümlerinin yaygınlaşmasıyla, çok güçlü bir işlemci veya geniş bir belleğe gerek kalmaksızın, internet bağlantısı olan basit işlemcilerle çok komplike işlemlerin yapılması mümkün hâle gelmiştir.

Bulut bilişim altyapısının karma amaçlar için kullanıldığı durumlarda, sistemin kullandığı altyapıya DNS veya IP temelli engelleme gerçekleştirilirse engelleme tedbiri tüm bulut sisteminin işleyişini aksatacaktır. Böyle bir durumda sadece bilgiye erişim veya iletişim hakları değil, o bulut hangi amaçlarla kullanıyorsa o kadar farklı nitelikte hakka müdahale edilmiş olacaktır.

J. Fiziksel sunucu müdahalesi

İnternete bağlanmak, en basit tanımıyla, ağa bağlı bir cihazın içindeki bir dosyaya erişmektir. İnternet ağına bağlı her cihaz, ağdaki diğer cihazlara erişim için kullanılabileceği gibi diğer cihazlara yayın yapmak amacıyla da kullanılabilir. Çok temel yazılımlarla bir dizüstü bilgisayarın veya cep telefonunun sunucu olarak yapılandırılması ve internet yayını yapması mümkündür.

Nihayetinde internete bağlı her bir sunucunun fiziksel olarak bir yerlerde barındırılması gerekir. Bu da ilgili sunucuya (ki bu bir dizüstü

[215] Bkz. **§2(III)(E)**[Bulut bilişim]

bilgisayar da olabilir, veri merkezinde barındırılan gelişmiş bir sunucu da) fiziki müdahalede bulunarak internet içeriğinin engellenmesini mümkün hâle getirir. Bulunduğu ülkenin hukuk kurallarına aykırı içerik taşıyan sunucunun internet bağlantısı fiziksel olarak kesilerek sunucudaki içeriğe erişim tamamen engellenebilir.[216]

K. Ağ hataları

Erişim engellemelerinde sık rastlanan diğer bir durum ise internet içeriğine erişilmeye çalışıldığında bağlantı hatası oluştuğunu gösteren mesajlarla karşılaşmaktır.[217] Bu tür mesajlarla karşılaşan ziyaretçiler ile içerik ve hizmet sağlayıcılar siteye teknik bir sorundan dolayı erişilemediği yanılgısına düşmekte, bir engelleme tedbiri uygulandığının farkına dahi varamamaktadır.

Özellikle telekomünikasyon sektörünün devlet tekelinde olduğu ve dolayısıyla tüm internet ağının sadece devlet tarafından yönetildiği ülkelerde bu yöntem etkin bir erişim engelleme yöntemi olarak kullanılabilir. Nihayetinde, devlet tekeli yüzünden içerik veya yer sağlayıcıların elinde hatanın çözümlenmesini sağlayacak ve ağda ayrıntılı inceleme yapacak yetkiler olmadığından devlet müdahalesi ispatlanamamaktadır.

L. Bağlantı yavaşlatma

İçeriğe müdahalenin bir diğer yöntemi, bağlantı yavaşlatmadır. Yavaşlatma, engellemenin coğrafi kapsamına göre ülkesel veya bölgesel bazda uygulanabileceği gibi, engellemenin ağ kapsamına göre internet omurgası temelli, İSS temelli veya kurumsal temelli uygulanabilir. Aynı doğrultuda, DPI teknolojisinin yardımıyla da belirli bir internet içeriğine erişimin yavaşlatılması mümkündür. Örneğin, sosyal medya sitelerine erişim belirli bir coğrafyada ve/veya belirli bir zaman aralığında yavaşlatılabilir. Yine, toplumsal olaylar sebebiyle sadece mobil internet bağlantısının yavaşlatılması da söz konusu olabilmektedir.

---

[216] **Murdoch/Anderson**, s. 64.

[217] **Murdoch/Anderson**, s. 69.

M. Sosyal teknikler

Devletler, bazı sebeplerden dolayı doğrudan engelleme kararı almak yerine başka yöntemler kullanarak içeriğe erişimi fiilen zorlaştırmakta veya kullanıcıların otosansür uygulamasını sağlamaktadır. Bu yöntemler, etkililiğinin bireysel davranışlara dayanması sebebiyle sosyal teknikler olarak adlandırılmaktadır.[218] Kullanıcılar üzerinde öyle bir baskı ortamı oluşturulmuştur ki caydırıcı etki dolaylı olarak internet içeriklerine yansımaktadır.

İnternetin etkin bir şekilde kullanılabilmesi için internete bağlantı öncesi ve bağlantı sonrası sınırlamaların devletler tarafından asgari düzeyde tutulması gerekmektedir. Devletlerin internete kimlerin bağlanabileceğini belirlemesi, bağlantıda gerçek kimlik bilgilerinin girilmesini zorunlu kılması, tüm internet trafiğini kaydetmesi veya internete bağlananların her adımını izlemesi mümkündür. Tüm bunlar bireyler üzerinde erişim engellemenin doğurduğuna benzer olumsuz sonuçlar oluşturmaktadır. Ziyaret edilen her web sitesinin devlet tarafından kontrol edildiği düşüncesi bireyler üzerinde psikolojik baskı yaratır. Öte yandan, internette web sitesi oluşturmak için katı bürokratik aşamaların geçilmesini istemek veya sadece ülke üst düzey alan adı uzantılı sitelerin kullanılmasını zorunlu kılmak da erişim engellemeye benzer sonuçlar doğurabilir.

Devletler erişim, yer ve toplu kullanım sağlayıcıları çeşitli yöntemlerle ve seviyelerde takip ve kontrol etmektedir. Örneğin, faaliyetler için ön izin alma şartı veya faaliyete başladıktan sonra bildirim yapma zorunluluğu gibi. Erişim, yer ve toplu kullanım sağlayıcıların hukuki ve cezai sorumlulukları da farklı sorumluluk rejimlerine tabi kılınmıştır. Söz konusu aktörlerin sorumluluğunun artırılması, hizmet sağlayıcıların müşterileri kabul ederken daha seçici davranmasına sebep olmaktadır.

Otoriter rejimlerde, hizmet sağlayıcılar kendilerini hukuki sorumluluk altına sokmamak için kamu otoritelerince sakıncalı kabul edilen içerikleri barındırmaktan çekinmektedir. Hatta sakıncalı içerikleri bu

[218] **Murdoch/Anderson**, s. 65.

konuda bir bildirim veya ihtara gerek olmaksızın sistemlerinden bizzat kendileri kaldırabilmektedir.

İnternet ortamında gelir elde etmeyi yasaklamak (*demonitezation*) veya internet ortamındaki faaliyeti aşırı şekilde vergilendirmek de bir sosyal teknik olarak değerlendirilebilir. Artan külfet kişiyi dolaylı olarak bir otosansüre itmektedir.

Benzer bir şekilde, bazı internet siteleri, kullanıcıların internete hangi ülkeden bağlandığını ya IP dağıtım tabloları sayesinde kendileri tespit etmekte veya kullanıcıya siteye girişinde sorarak öğrenmektedir. İnternet sitesinde, tespit edilen ülkeye özel sakıncalı bir içerik varsa kullanıcının bu içeriğe erişmesi doğrudan site tarafından tamamıyla engellenmekte veya kullanıcıya içeriğin sakıncalı olduğu ihtar edilmektedir.

Peki, bir devletin, telekomünikasyon altyapısını bilinçli olarak geliştirmemesi, yatırımlara izin vermemesi, özel sektörü kısıtlaması, fiber altyapıları yaygınlaştırmaması veya telekomünikasyon sektöründe rekabeti geliştirici tedbirler almaması sosyal teknik olarak kabul edilebilir mi? Bu soruya cevap verebilmek için ilgili devletin internete erişim politikaları bütüncül olarak incelenmelidir. Öyle ki kullanıcılara, içerik sağlayıcılara ve internet platformlarına karşı, ifade özgürlüğünü zedeleme niyetiyle kamunun katılımını önleme amaçlı stratejik davalar (SLAPP - *strategic lawsuits against public participation*) veya kötü niyetli ve bezdirme amaçlı davalar açılabilir. İşte bunları önlemeye dönük özel bir düzenleme yapılmaması bile sosyal teknik olarak nitelendirilebilir.

Sosyal tekniklerin etkililiği bireylerin bu konuda gösterdiği katılım ve dirence göre değişmektedir. Devletlerin engelleme politikaları bireyler üzerinde psikolojik etki yaratmaktadır. Sorumluluk korkusu dolaylı şekilde tamamlayıcı sansüre veya platform sansürüne dönüşmektedir.[219] Son tahlilde devletler doğrudan engelleme yapmadıkları için, ortaya çıkan durumdan sorumlu olmadıklarını ileri sürmektedir. Neticede, kullanılan

[219] Bu konuda ifade özgürlüğü bağlamında kapsamlı bir değerlendirme için bkz. **§11(X)** [Yargıçlar Sajo ve Tsotsoria'nın Müşterik Muhalif Görüşü].

bu sosyal teknikler başta ifade hürriyeti, özel hayatın gizliliği, iletişim özgürlüğü olmak üzere çeşitli temel hak ve hürriyeti ihlal etmektedir.

XI. Değerlendirme

Girişte belirtildiği üzere internet içeriğine erişimin engellenmesi için kullanılan sadece bir yöntem yoktur. Engellemenin kapsamı, kullanılan teknik, engelleme süresi, engelleme öncesi ve sonrası takip edilen süreç devletten devlete değişmektedir. Özellikle belirtmek gerekir ki teknik gelişmeler, toplumsal olaylar, olağanüstü hâller bu yöntem ve tekniklerin çok kısa bir sürede farklı yönlere evrilmesine neden olmaktadır. Bu sebeple, her bir engelleme yöntemi veya tekniğinin hukuka uygunluğu, ilgili hukuk düzlemine göre değerlendirilmelidir. Bu konuda genelleme yapmak doğru değildir.

Bir ülkede uygulanan engelleme yöntem ve tekniklerinin, içerik sağlayıcılar ve sosyal medya platformları ile o ülke arasındaki iş birliğiyle yakından ilgili olduğunun altını çizmek gerekir. Şöyle ki yukarıda izah edilen platform temelli engelleme yöntemi uygulanıyorsa diğer engelleme yöntem ve tekniklerini kullanmaya zaten gerek yoktur. İş birliği arttıkça içeriklerin bizzat platform tarafından kaldırılma oranı artmakta, bu da erişimi engelleme tedbirlerine duyulan ihtiyacı azaltmaktadır. Yani erişimi engelleme tedbirlerinin sayısıyla platform temelli engelleme arasında ters orantı vardır.

Görüleceği üzere erişimin engellenmesi kararlarının sayısı tek başına bir gösterge değildir. İçeriğin platformlar nezdinde kaldırılmasına ilişkin istatistiklerin de şeffaf olarak yayımlanması önem arz eder. Bir ülkenin internete ilişkin özgürlükçü bir yaklaşıma sahip olup olmadığına ilişkin sağlıklı bir muhakeme ancak bu iki veri birlikte hesaba katılarak yapılabilir.

§5. İÇERİK FİLTRELEME VE ENGELLEME YÖNTEMLERİNİ AŞMA YOLLARI

Dördüncü bölümde incelendiği üzere internet içerikleri, değişik yöntem ve teknikler kullanılarak filtrelenmekte veya engellenebilmektedir. İçerik filtreleme ve engelleme yöntemleri engellemenin coğrafi kapsamına göre, ülkesel ve bölgesel engelleme; ağ kapsamına göre, internet omurgası, İSS temelli ve kurumsal engelleme; sürecine göre, doğrudan engelleme ve uyar-kaldır yöntemiyle engelleme; süresine göre, geçici ve kalıcı engelleme; sistemine göre, otomatik ve bireysel engelleme; kullanılan tekniğe göre ise IP engellemesi, DNS engellemesi, URL engellemesi, *proxy* engellemesi, içerik engellemesi, siber saldırı yöntemleri ile engelleme, alan adına el koyma veya alan adını terkin yöntemi, fiziksel sunucu müdahalesi, ağ hataları, bağlantı yavaşlatma ve sosyal tekniklerdir.

İnternet içeriğine yönelik filtrelemeler ve engellemeler farklı yöntem ve tekniklerle aşılabilmektedir. Filtreleme ve erişimi engelleme yöntemleri kombine şekilde kullanılabildiği gibi bunları aşma yöntemleri de kombine şekilde kullanılabilmektedir.

Bu bölümde, internet içeriğini filtreleme ve erişim engelleme tedbirlerini aşmak için başvurulabilecek yöntem ve teknikler sınıflandırılmaya çalışılmıştır. Bu sınıflandırma tahdidî değildir. Burada sayılanların dışında kalan farklı ve özgün yöntem ve tekniklerle internet içeriğine yönelik müdahaleler aşılabilir. Aşağıda, herhangi bir ülkeyle bağlı olmaksızın genel yöntem ve teknikler derlenmiştir.

I. Yöntem ve teknikler

A. IP değişikliği

İnternet içeriğinin barındırıldığı sunucunun IP adresinin engellendiği durumlarda, sunucu yöneticisi tarafından IP adresinin değiştirilmesi

engellemeyi etkisiz kılacaktır. Örneğin, IP havuzunda yer alan ve engellemeye konu edilmemiş bir başka IP adresi pratik şekilde kullanılabilir. Sunucuyu barındıran şirketi değiştirmeksizin sadece IP değişikliği yapmanın maliyeti düşük olmakla birlikte, sunucu ayarlarının yeni IP adresine göre yapılandırılması bazı teknik sorunlar oluşturabilmektedir.

IP havuzunda başka IP olmadığı veya tüm IP blokunun engellendiği bazı durumlarda tek alternatif, yer sağlayıcıyı değiştirmektir. Ancak, bunun için yeni yer sağlayıcıyla yeni bir hizmet sözleşmesi yapılması gerekeceğinden engellemenin aşılması mali açıdan külfetli olacaktır.

Sosyal teknikler kısmında açıklandığı üzere yer sağlama hizmeti sunan şirketlerin faaliyeti birçok devlet tarafından izin sistemine tabi tutulmakta ve şirketlerin faaliyetleri kontrol edilmektedir. Yer sağlayıcı şirketler, hem sunmuş oldukları hizmetlerin işlerliğinin etkilenmemesi hem de hukuki veya cezai sorumluluk altına girmemek için erişimi engellenmiş veya şüpheli içerikleri barındırmaktan çekinebilmektedir.

Yukarıda izah edilen yöntem, engellemenin içerik sağlayıcısı tarafından aşılması yöntemidir. Bireysel internet kullanıcılarının da VPN gibi -aşağıdaki bölümlerde açıklanacak- teknikleri kullanmak suretiyle IP engellemesini işlevsiz kılmaları mümkündür.

B. DNS değişikliği

DNS engelleme tekniğinde alan adı tüm alt içeriği ile birlikte erişime kapatılmaktadır. Alan adlarının IP çözümlemesini yapan DNS sunucusu, kullanıcı engellenmek istenen web sitesine girmeye çalıştığında bu sitenin çözümleme talebini yanıtsız bırakır. Bu şekilde siteye erişim engellenmiş olur.

Kullanıcının internet içeriğine erişebilmesi için içeriğin yer aldığı alan adının, internet hizmet sağlayıcısı tarafından çözümlenmesi gerekmektedir. DNS engellemesi bu çözümlemenin sonuçsuz kalmasını sağlamaktadır. Bu engellemeyi aşmak için kullanıcı nezdinde DNS ayar-

ları değiştirilerek kullanıcının ulaşmaya çalıştığı alan adının başka DNS sunucuları tarafından çözümlenmesi sağlanmaktadır.[220]

Bu tür hizmetler veren birçok işletme bulunmaktadır. Örneğin, Google Public DNS, openDNS, DynDNS, Comodo Secure DNS, Yandex. DNS. Bazı internet tarayıcılarında bu özellik "*built-in*" bir özellik olarak bulunmakta ve DNS değişikliği pratik şekilde gerçekleşebilmektedir. Opera ve Comodo Dragon tarayıcılarının çözümleri *built-in* çözümlere örnek olarak gösterilebilir. Benzer şekilde, bazı akıllı telefonların işletim sistemlerinde de özel bir DNS ayarı olabilmektedir.

Öte yandan, DNS sunucularının da hem DNS hem de IP engelleme tekniğiyle engellenmesi mümkündür. Özellikle erişime engellemenin etkinliğini artırmak amacıyla bu tür DNS çözümlemeleri de engellenmektedir. Bu doğrultuda, belirli çözümlemeler engellenebileceği gibi, erişimi engelleme kararı verilen yayınlara alternatif yollardan erişmeyi engelleyecek tedbirleri alma konusunda İSS'lere genel bir yükümlülük de getirilebilir. İSS, kendi ağındaki trafiği analiz etmek suretiyle gereken tedbirleri alacaktır.

DNS alanındaki en önemli gelişme DNS-over-HTTPS tekniğinin yaygınlaşmasıdır.[221] Bu yöntemde DNS çözümlemeleri tamamen şifreli bir kanalla gerçekleşmektedir. Bu özelliğin tarayıcılarda *varsayılan* olarak aktif hâle getirilmesi durumunda, erişim engellemelerini etkisiz kılma konusunda farklı bir aşamaya geçilecektir. Bu yöntem, tarayıcıları bilgiye erişimde yeni bir konuma getirmekte, DNSSEC'nin yaygınlaşmaması sebebiyle ortaya çıkan mahremiyet sorunlarına çözüm sunmaktadır. Diğer yandan, DNS çözümlemelerinin tamamen ülke dışındaki sunucularda gerçekleşmesi sebebiyle dijital mahremiyet tartışmaları da ayrı bir seviyeye taşınacaktır.[222]

---

[220] **Murdoch/Anderson**, s. 67.

[221] **IETF**, "*DNS Queries over HTTPS (DoH) - Request for Comments: 8484*", <https://tools.ietf.org/html/rfc8484>

[222] **Simon, Maarten/Müller, Moritz**, "*Does the arrival of DoH mean browsers should be regulated?*" <https://www.sidn.nl/en/news-and-blogs/does-the-arrival-of-doh-mean-browsers-should-be-regulated>

C. Alan adı değişikliği

DNS engellemesinin içerik sağlayıcılar tarafından bertaraf edilmesinin bir diğer yöntemi ise alternatif ve bağlantılı alan adları tescil etmek ve kullanmaktır.[223] Ancak, engellemeden sonra hedef kitlenin yeni alan adından bir şekilde haberdar edilmesi gerekir. Ayrıca, her bir alan adı tescilinin ve altyapıyı yeni sisteme taşımanın maliyeti vardır.

D. URL değişikliği

URL engellemesi, koordinatları bilinen hukuka aykırı veya zararlı bir içeriğin engellenmesi amacıyla kullanılan bir tekniktir. Bu yöntemin en önemli avantajı, hukuka aykırı veya zararlı bir içerik için web sitesinin tüm içeriğinin engellenmesine gerek olmamasıdır. Bu avantajına rağmen, en kolay aşılabilecek yöntemdir. İnternet ortamındaki bir içeriğe erişmek, bir bilgisayarın içeriğindeki dosyaya erişmek demektir. URL adresi, dosya yolu değiştirilerek URL engellemesinin kolayca aşılması mümkündür.

URL masking tekniğiyle URL'yi gizlemek ve içeriğe birden çok URL adresinden ulaşmak mümkündür. Bu şekilde, bir URL engellense bile içeriğe diğer URL adresleri üzerinden erişilebilir. Ayrıca, URL adresinin uzun olduğu durumlarda kısaltmak amacıyla muhtelif URL oluşturma araçları kullanılmaktadır. Örneğin, Google URL Shortener, TinyURL, Bitly ve Ow.ly gibi araçlar.

Bazı uygulamalar, bağlantı sağladıkları içeriklerin URL adreslerini otomatik olarak kısaltmaktadır. Örneğin, Twitter "t.co" alan adını ve bu alan adı altında oluşturduğu URL'leri kullanmaktadır. Twitter'ın bu hizmeti kullanma amacı URL adreslerini kısaltmak, bağlantı tıklama istatistiklerini tutmak ve kullanıcılarının zararlı içeriklere erişmesini önlemektir.[224] Twitter, "t.co" adresini "https" protokolünde sunmaktadır. HTTPS trafiğinin ayrıştırılması teknik olarak mümkün olmadığı için

[223] **Citizen Lab (University of Toronto)** (2007) *"Everyone's guide to by-passing Internet censorship for citizens worldwide"* <http://citizenlab.org/guides/everyones-guide-english.pdf>, s. 28.

[224] **Twitter**, *"About Twitter's link service (http://t.co)"* <https://support.twitter.com/articles/109623>

URL engellemesi uygulanamayacaktır. Alternatif olarak "t.co" alan adına DNS temelli uygulanacak bir erişim engellemesi, dolaylı olarak tüm Twitter bağlantılarını erişilmez kılacaktır.

E. VPN ve diğer trafik aktarma yöntemleri

VPN, uzak bir noktada bulunan bir ağa güvenle bağlanmak için kullanılan bir yöntemdir.[225] Bu yöntem kullanılarak ses, görüntü veya veri içeren herhangi bir ağ trafiği güvenli şekilde iletilebilir. VPN kullanmanın en önemli avantajı, transfer edildiği zaman veriyi şifrelemesi ve güvende tutmasıdır. Bu teknik kullanılarak tüm trafik, internet ağına başka bir sunucu aracılığıyla taşınmaktadır. VPN, özellikle çalışanların iş ağına güvenle bağlanmasını sağlayan pratik bir araçtır.

VPN ile trafik aktarımı yapıldığı için bu yöntemin, erişim engellemelerini aşmak amacıyla kullanılması mümkündür. TOR tarayıcısı ve *The Invisible Internet Project* (I2P) gibi araçlar da bir çeşit trafik aktarma yöntemi olduğundan engellemeleri aşmak için kullanılmaktadır. Bazı tarayıcılarda bu tür trafik aktarım araçları ve VPN hizmeti, gömülü hâlde gelmektedir.

VPN sunucuları hem engellemeleri aşmak için hem de çeşitli suçlarda araç olarak kullanılabildiğinden devletlerin sıkı takibine tabidirler. Herhangi bir kayıt tutmadıkları iddiasında olan bazı VPN hizmet sağlayıcılarının da aslında bir şekilde kayıt tuttukları, yakın zamanda bir güvenlik sızıntısı vesilesiyle gün ışığına çıkmış bir gerçekliktir.[226]

F. Uzak masaüstü bağlantısı

Mevcut işletim sistemleri, internet kullanılarak bilgisayarların uzak mesafeden kontrol edilmesini mümkün kılmaktadır. Bu yöntem, fiziksel erişimin olmadığı veya zor olduğu bilgisayarların tek bir noktadan

[225] **Ferguson, Paul/Huston, Geoff**, "*What is a VPN?*" <https://www.potaroo.net/papers/1998-3-vpn/vpn.pdf>

[226] **Nichols, Shaun**, "*Seven 'no log' VPN providers accused of leaking – yup, you guessed it – 1.2TB of user logs onto the internet*" <https://www.theregister.com/2020/07/17/ufo_vpn_database/>

kontrolüne olanak vermektedir. Uzak masaüstü kullanıcısı bağlandığı bilgisayarın tüm servislerinden sanki o bilgisayarın karşısındaymış gibi yararlanabildiği için bu teknik, erişim engeli uygulanan web sitelerine ulaşmak için de kullanılabilmektedir. Proxy ve VPN kullanımında olduğu gibi siteye erişen asıl bilgisayar uzaktan bağlanılan bilgisayar olduğu için internet kullanıcısının kimliği de gezinme sırasında gizlenmektedir. Bu teknikle bir ağda uygulanan engellemeler başka bir ağa bağlanmak suretiyle aşılmaktadır.

G. Online çeviri sistemleri

İnternette ücretsiz olarak sunulan birçok çeviri sitesi yer almaktadır. Google Translate, Babelfish gibi popüler çeviri siteleri bir web sitesini eş zamanlı olarak istenilen dile çevirebilmektedir. Çeviri, içeriğin çeviri sitesinin önbelleğine alınması suretiyle gerçekleştirilmekte ve içerik, kullanıcıya önbellekten sunulmaktadır. Çeviri siteleri kullanılarak, erişime engellenmiş bir web sitesinin içeriğine ulaşmak mümkün olmaktadır.[227] Başka bir deyişle, online çeviri siteleri bir tür proxy işlevi görmektedir.

H. Önbellek kullanımı

Arama motorları ve çeşitli siteler, internet içeriğini, farklı amaçlarla işlemek üzere kendi sunucularında saklamaktadır.[228] Benzer şekilde, bazı internet siteleri internet içeriklerinin değişik zamanlarda alınmış kopyalarını tutmaktadır. Örneğin, "www.archive.org" sitesi 279 milyar internet sayfasının kopyasını arşivinde saklamaktadır. Aynı amaçla "www.cachedview.com" birçok önbellek sitesine tek bir noktadan erişim sağlamaktadır.

Bir internet içeriğine erişim engellendiğinde arama motoru veya ilgili sitenin önbelleğinde bulunan içerik bundan etkilenmez. Şayet web sitesi önbelleğe alınmışsa ek bir yazılım veya başkaca bir yöntem gerek-

---

[227] **Citizen Lab (University of Toronto)**, s. 28.

[228] Önbellek konusunda popüler diğer bir web sitesi ise www.archive.org'dur. Bu web sitesi 85 milyar web sitesini önbelleğinde tutmaktadır. Bkz. Internet Archive: Wayback Machine <http://www.archive.org/web/web.php>

meksizin erişim engelleme kararına rağmen sitenin içeriğine ulaşmak mümkündür.[229]

I. Kopya içerik kullanımı

Web 2.0 teknolojilerinin yaygınlaşmasıyla internet sitelerinin etkileşimi arttığından bir içerik çok kısa süre içerisinde birçok internet sitesinde yayımlanabilmektedir. Bir internet sitesine erişim engellendiğinde, içerik farklı kanallardan başka sitelere yayılarak erişim engelleme tedbirinin amacına ulaşması önlenebilmektedir. Kopya internet sitelerinin sayısının milyonları bulması ve internet sitelerinin otomatik olarak içeriklerini güncelleştirebilmeleri sebebiyle bu tür sitelerle mücadele büyük çaba gerektirmektedir.

Dağıtık yapıda içerik kullanılması, esasında sadece engellemeleri aşmak için değil, internet sitelerinin performansını artırmak; aynı anda coğrafi olarak farklı noktalardan yayın yapmak suretiyle trafik yükünü dağıtmak amacıyla da kullanılmaktadır. İkinci bölümde açıklandığı üzere, içerik dağıtım ağları vasıtasıyla bir web sitesi farklı sunucular, IP adresleri ve altyapılarda aynı anda yayın yapabilmektedir. Kopya içerikler bizzat içerik sağlayıcı tarafından oluşturulabileceği gibi internette içeriklerin kopyalarını otomatik olarak tutan ve farklı amaçlarla faaliyet gösteren arşiv siteleri de yaygındır.

Bir içerik engellense bile farklı konumlarda bulunan önbelleklerden içeriğe erişilmeye devam edilebilmektedir. Milyonlarca kopya içerik, verinin kaynağını ve bir suç işlendiğinde failin tespitini imkânsızlaştırmaktadır. Bu tür bir girişimle karşı karşıya kalan devletler, engellemenin seviyesini artırarak ve farklı teknikleri kombine şekilde kullanarak söz konusu içerikle mücadele etmektedir.

J. İçerik aldatması

İçerik engellemesi tekniği kullanılarak gerçekleştirilen erişim engellemesini aşmak için çeşitli yöntemler kullanılmaktadır. Bu yöntemlerin

[229] **Citizen Lab (University of Toronto)**, s. 28.

başında içerik gizleme yöntemi gelmektedir. Bu yöntemde web sitesinin ana temasını oluşturan anahtar kelimeler yerine ilgisiz kelimeler kullanılmakta ve bu şekilde web siteleri engellemeden kurtulmaktadır. Demokrasi kelimesi yerine "lahana", çok partili sistem için "havuç" kelimesi kullanılması gibi.[230] Bu yöntem, devlet sansüründen kurtulmak için film ve kitapların isimlerini değiştirmek şeklinde kullanılagelen klasik yöntemin internet ortamına yansımış hâlidir. İçerik engellemelerini bertaraf etmek için etkin olarak kullanılabilirse de hedef kitlenin bu yeni anahtar kelimelerden habersiz olması düşüncelerin hedef kitleye ulaştırılamaması riskini doğurmaktadır.[231]

İçerik aldatması, içeriğin URL adresi veya doğrudan web sitesinin alan adı için de kullanılabilmektedir. Alan adlarında "ilk gelen alır" ilkesi uygulandığından pornografik içerikli bir web sitesi için www.insanhaklarivehurriyetleri.com gibi bir alan adının kullanılmasının önünde hiçbir engel yoktur. Web sitesinde kullanılan resimlerin tanıtma bilgisi olan *meta tag* kodlarında ilgisiz kelimeler kullanılarak resimlerin de filtreleme sistemleri tarafından algılanması engellenmektedir.

Bir diğer aldatma yöntemi ise bilinçli yazım hatasıdır. Bu yöntemde, gizlenmeye çalışılan kelimelerin arasına rastgele karakterler eklenir ve bunlar 1 puntoya kadar küçültülerek gizlenir. Örneğin, "demokrasi" kelimesinin "de-m.okras,i" şeklinde yazılması. Şunu da belirtmek gerekir ki filtreleme sistemleri de gün geçtikçe akıllanmaktadır. Makine öğrenmesi yöntemleriyle bu tür bilinçli yazım hataları büyük ölçüde tespit edilebilmektedir.

II. Değerlendirme

Erişim engelleme ve filtreleme teknolojilerinin gelişimine paralel olarak bu tür engelleme ve filtrelemeleri aşma yöntemleri de aynı hızda gelişmektedir. Bazı engelleme ve filtrelemeler çok kolay aşılabilirken bazılarını aşmak uzun soluklu bir çaba gerektirmektedir. Bu alanda sıkı bir

[230] **Goldsmith/Wu**, s. 103.

[231] **Goldsmith/Wu**, s. 103.

mücadele ve rekabet söz konusudur. Bazı durumlarda kurumsal iletişim, bankacılık veya elektronik ticaret için kullanılan VPN uygulamaları da engellemelerin etkinliğini artırmak için engelleme kapsamına alınabilmektedir. Her yöntem ve tekniğin güçlü ve zayıf yönleri, avantajları ve dezavantajları vardır. Bir içeriğe yönelik engellemenin kolay aşılabilir olması devletin bilinçli tercihi olabileceği gibi teknolojik yetersizliğinin bir sonucu da olabilir.

İnternet ortamında yer alan bir içeriğe neden erişilemediği sorusunun yanıtını vermek her zaman kolay değildir. İçeriğe erişmek için, aşılması gereken çok farklı katmanlar olabilir. İçeriğe erişimi engellemek için birden çok yöntem ve teknik beraber kullanılarak katmanlar artırılabilir veya somut içeriğe yönelik ilave katman eklenebilir. Farklı yöntemler birlikte kullanılmak suretiyle özgün çözümler geliştirilebilir. Bu sebeple, bir içeriğe erişilememesinin çok farklı gerekçeleri olabileceği akılda tutulmalıdır.

İçeriğe kişisel bilgisayarda kullanılan filtreleme yazılımı sebebiyle erişilemeyebileceği gibi yerel ağdaki filtreleme uygulaması tarafından koyulan kısıtlama sebebiyle de erişilemeyebilir. İçeriğe internet servis sağlayıcısının uyguladığı kısıtlamalar sebebiyle de erişilemeyebilir, platform tarafından uygulanan bir kısıtlama sebebiyle de. Diğer bir deyişle, kişisel katman, kurumsal katman, internet servis sağlayıcısı katmanı, ülkesel katman, bölgesel katman, platform katmanı gibi çok farklı katmanlardaki bir müdahale içeriği erişilmez kılabilir. Keza, meşru bir amaç için yapılan engelleme, amacından saparak sansür aracına dönüştürülebilir.

Çok basit yöntemlerle çok kompleks sistemlerin aşılması mümkündür.[232] Örneğin, yasaklı site veri tabanını referans alan bir sistemde Google Translate gibi bir online çeviri sitesiyle engellemenin aşılması gibi. İnternet tarayıcılarında gömülü şekilde bulunan ve giderek yaygınlaşan

[232] Örneğin PING ile dosya transferi bu kapsamda değerlendirilebilir. Bu konuda kapsamı bir inceleme için bkz. **Muharremoğlu, Gökhan**, *"PING ile Port'suz Dosya Transferi Yaparak Firewall Aşmak"*, <https://www.bilgiguvenligi.gov.tr/kurumsal-guvenlik/ping-ile-portsuz-dosya-transferi-yaparak-firewall-asmak.html>

built-in VPN veya DNS değiştirme seçenekleri de basit ama etkili yöntemler arasında sayılabilir.

Öte yandan engellemeleri aşma teknikleri gizli bilgiler değildir. Her erişim engelleme kararından sonra, engellemenin nasıl aşılabileceği hem internette hem de yazılı ve görsel basında ayrıntılarıyla yer alabilmektedir.[233] Hatta engellenen sayfalarda bu doğrultuda yönlendirmeler bile yer alabilmektedir. Bu sebeple, erişim engelleme ve filtreleme kararları çok kısa bir sürede etkilerini yitirebilmektedir.

Bazı teknikler kimi zaman o kadar etkisiz olabilmektedir ki erişim engelleme kararına rağmen bir internet sitesi, ülke genelinde en çok ziyaret edilen siteler arasında yer alabilmektedir. Bu alandaki teknolojilerin yaygınlaşması devletlerin aldıkları erişim engelleme kararlarını anlamsız kılabilmektedir. Denilebilir ki bu tür kararlar erişimi engellemekten ziyade erişimin zorlaştırılmasına hizmet etmektedir.[234]

Diğer taraftan, internet ortamında şifreli içeriklerin sayısı hızlıca artmaktadır. Önceleri ağ trafiğini yavaşlatmamak adına güçlü şifreleme algoritmaları kullanılmamaktaydı. Ancak, internet bağlantı hızlarının hem sabit hem mobil ağlarda artmasıyla beraber HTTP ve HTTPS sitelerine erişimde esaslı bir fark kalmamıştır. Ayrıca, internet sitelerinde HTTPS protokolünün kurulma maliyeti de göreceli olarak azalmıştır.[235] HTTPS protokolünü kullanan sitelerin sayısının artması derin paket analizi sistemlerini ve dolayısıyla URL engelleme tekniğini etkisiz kılmaktadır.

---

[233] **Akdeniz/Altıparmak**, s. 60.

[234] **Akdeniz/Altıparmak**, s. 78.

[235] Bu konuda kapsamlı bir analiz için bkz. **Zittrain, Jonathan/Faris, Robert/Noman, Helmi/Clark, Justin/Tilton, Casey/Morrison-Westphal, Ryan** (2017) "*The Shifting Landscape of Global Internet Censorship*" Berkman Klein Center Research Publication No. 2017-4, Harvard Public Law Working Paper No. 17-38, <https://ssrn.com/abstract=2993485>; **The Institute for Information Security & Privacy at Georgia Tech** (2016) "*Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others*", <http://www.iisp.gatech.edu/sites/default/files/images/online_privacy_and_isps.pdf>

Yapılan bir araştırmaya göre hacim olarak ABD'deki internet trafiğinin %49'u şifrelidir.[236] Şifreli iletişimin kırılması için bazı yöntemlerin (örneğin *man-in-the-middle SSL interception*) kullanılması mümkün olsa da bu tür yöntemler tüm ağ güvenliğini riske etmekte ve güncel tarayıcılar sayesinde kullanıcılar tarafından fark edilebilmektedir.[237] Yine de uygulamada bu tür yöntemlere rastlanmaktadır.[238]

Alternatif erişim yöntemleri hem engellenip hem de bunların kullanılması suç hâline getirilebilir veya kullanıcı başka bir yöntemle cezalandırılabilir. Örneğin, izinsiz VPN kullanan bir cihaz şebekede tamamen engellenerek telefonun, elektronik haberleşme altyapısında kullanımının yasaklanması söz konusu olabilir. Alternatif erişim yöntemlerini kullanmanın müstakil suç olarak tanımlanması kolay olmayabilir. Ancak, uygulanacak politikanın etkinliğini sağlamak adına bu konuda bir suç politikasının oluşturulması pekâlâ mümkündür.

Erişimi engelleme yöntemlerinin çeşitli riskleri barındırdığı da gözden kaçırılmamalıdır. Bu risklerin başında bilgi güvenliği riski gelmektedir.[239] Engellemeleri aşmak için yurt dışı merkezli çözümlerin kullanılması ülkedeki kişisel verilerin yurt dışına aktarılması riskini taşır. Bu tür uygulamalar, virüs ve benzeri zararlı yazılımları da barındırabilmektedir. Dolayısıyla, erişim engelleme ve filtreleme kararlarının etki analizi yapılmalı, ulaşılmak istenen amaç ile kullanılacak yöntemin oluşturacağı bilgi güvenliği riskleri hassas şekilde tartılmalıdır.

Erişim engelleme için birden çok tekniğin birlikte kullanılması engellemelerin aşılmasını zorlaştırmaktadır. Buna cevap olarak engelleme aşma yöntemleri de kombine şekilde kullanılabilmektedir. Örneğin, bir web sitesinin aynı anda farklı alan adları kullanarak DNS engellemesinden, farklı ülkelerde yer alan birbirinden bağımsız barındırma hizmet-

---

[236] **The Institute for Information Security & Privacy at Georgia Tech**, s. 3.

[237] **Internet Society**, "*Internet Society Perspectives on Internet Content Blocking: An Overview*", s. 15.

[238] Fransa Hazine Müsteşarlığı'nın bu yöntemi kullandığı iddia edilmektedir. Bkz. **Leyden, John**, "*French gov used fake Google certificate to read its workers' traffic*" <https://www.theregister.co.uk/2013/12/10/french_gov_dodgy_ssl_cert_reprimand/>

[239] Bu konuda kapsamlı bir inceleme için bkz. **Gök**, s. 65 vd.

lerini kullanarak IP engellemesinden, *URL masking* yöntemiyle URL engellemesinden ve şifrelenmiş içerik kullanarak içerik engellemesinden kurtulması teknolojik olarak mümkündür.

İnternet ortamında devletler ve bireyler arasında erişim engelleme konusunda bir mücadele sürmektedir. Erişim engellemenin kolay veya zor aşılıyor olması, engellemenin ölçüsüzlüğünü veya hukuka aykırılığını hiçbir koşulda ortadan kaldırmamaktadır. Ayrıca, internet bilgisi orta düzeyin altında olan ve en basit engelleme aşma tekniklerini dahi kullanamayacak bireyler her zaman var olacaktır. Bu sebeple, yukarıda da ifade ettiğimiz gibi, bu tür yöntemler erişimi engellemekten ziyade erişimin zorlaştırılmasına hizmet etmektedir.[240] Bazı durumlarda ise bir içerikten duyulan kamusal hoşnutsuzluğun somut yansıması olarak, uygulamada etkinliği tartışmalı bu tür yöntemler her şeye rağmen kullanılabilir.

[240] **Akdeniz/Altıparmak**, s. 78; Benzer şekilde bkz. **Dülger, Murat Volkan** (2007) "*İnternet Erişiminin Engellenmesinin Hukuksal Açıdan Değerlendirilmesi ve 5651 Sayılı Yasayla Getirilen Düzenleme*" İstanbul Barosu Dergisi, Cilt: 81, Sayı: 4, s. 1477-1545, s. 1480.

DÖRDÜNCÜ KISIM

AVRUPA KONSEYİ VE İNTERNET

§6. AVRUPA KONSEYİ

Avrupa Konseyi, internetin yaygınlaşması, sosyal ve ekonomik hayata etkisinin artmaya başlamasıyla birlikte özellikle insan hakları açısından çeşitli tavsiye kararları almış, deklarasyonlar ve rehberler yayımlamıştır. Çoğu yumuşak hukuk kuralı niteliğinde olan, temelde bağlayıcılığı bulunmayan, tavsiye niteliğindeki bu metinlerin önemi nedir? Bu belgeler temelde bağlayıcı olmasa da uzun vadede insan hakları hukukunun gelişimi, mevzuatın biçimlendirilmesi ve AİHM içtihatlarının şekillenmesinde önemli rollere sahiptir.

Bilhassa AİHM kararlarında bu belgelerden alıntılar ve bu belgelere açık atıflar yapıldığı dikkate alındığında dolaylı bağlayıcı etki daha net gözlemlenebilmektedir. Diğer bir deyişle yumuşak hukuk kuralları sert hukuk kurallarının özünü, ruhunu, temel gelişim dinamiğini oluşturmaktadır. Teknik ve dinamik alanların yumuşak hukuk kuralları ile düzenlenmesi en makul yaklaşımdır.

Bu bölümde, Avrupa Konseyinin temel internet yönetişim belgelerine yer verilecektir. Çalışmanın amacı ve kapsamına uygun olarak, sadece internet hukukuyla doğrudan bağlantılı olanlar derinlemesine ele alınacak, dolaylı bağlantılı olanlar ise genel hatlarıyla incelenecektir.

I. İnternette Özel Hayatın Korunmasına İlişkin Tavsiye Kararı (1999)

Avrupa Konseyi Bakanlar Komitesinin 23 Şubat 1999 tarihinde kabul ettiği İnternette Özel Hayatın Korunmasına İlişkin Tavsiye Kararı - Bireylerin Bilgi Otobanlarında Kişisel Verilerin Toplanması ve İşlenmesi Bakımından Korunması İçin Prensipler[241] başlıklı kararı, bilgi toplumu-

[241] **Avrupa Konseyi**, "*Recommendation No. R (99) 5 of the Committee of Ministers to member states for the protection of privacy on the Internet - Guidelines for the protection of individuals with regard to the collection and processing of personal data on information highways*", <https://

nun hukuki çerçevesinin gelişmesine mühim katkılar sunmuş öncü bir metindir.[242]

Tavsiye Kararı, internet kullanıcıları ve internet hizmet sağlayıcıları için ayrı ayrı teknik ve hukuki tavsiyelerde bulunmaktadır. Tavsiyeler her türlü bilgi otobanını kapsayacak şekilde hazırlanmıştır. Bu doğrultuda, internet hizmet sağlayıcısı kavramı Tavsiye Kararı'nda geniş manada kullanılmıştır. Tavsiyelerin, niteliklerine uygun düştüğü ölçüde erişim sağlayıcılar, içerik sağlayıcılar, ağ sağlayıcılar, tarayıcı yazılım tasarlayıcılar (*navigation software designers*) ve forum operatörleri gibi farklı aktörler için de geçerli olduğu belirtilmiştir.

Tavsiye Kararı, internetin güvenli bir alan olmadığı hatırlatmasıyla başlamakta, kullanıcılara şifreleme teknolojilerini kullanmalarını ve sistemlere şifre koymalarını salık vermektedir. Bu hatırlatmadan sonra, internet ortamındaki her işlemin bir iz bıraktığı ve bunun da kişilerin profillerinin çıkarılmasına imkân tanıdığının altı çizilmiştir. Buna karşı çözüm önerisi olarak anonim erişim gösterilmiştir.

Peki bu durumda, anonimliğin suçla mücadelede ortaya çıkardığı sorunlar nasıl bertaraf edilecektir? Karar'da, mümkün olduğunca takma adların kullanılması ve kişisel veri paylaşılacak platformlarda seçici davranılması önerilmektedir. Ayrıca, hukuki sorumluluk doğmaması için, zararlı iletilerden kaçınılması tavsiye edilmektedir.

Tavsiye Kararı, Avrupa Konseyinin 108 sayılı Sözleşmesi'yle hukuki temeli atılmış kişisel verilerin korunmasına ilişkin farkındalığı artırmaya çalışmıştır. Mahremiyete saygı gösterilmesinin ve bu bağlamda kişisel verilerin korunmasının temel bir insan hakkı olduğu açıkça vurgulanmıştır. Tavsiye Kararı, internet hizmet sağlayıcılarının, kişisel verilerin amacına uygun kullanılmasından sorumlu olduğunu belirtmiştir. Karar, kullanıcıların hizmet sağlayıcıya, hangi tür kişisel verileri hangi yöntemle

search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016804f4429>

[242] **Avrupa Konseyi,** "*Contribution by the Council of Europe to the 2nd Preparatory Committee for the World Summit on the Information Society (Geneva, 17-28 February 2003)*" <https://www.itu.int/dms_pub/itu-s/md/03/wsispc2/c/S03-WSISPC2-C-0032!!PDF-E.pdf>, s. 6.

ve amaçla topladığını, işlediğini ve sakladığını sormasını hatta bu soruları zaman zaman yenilemesini önermiştir. Ayrıca, kullanıcılara internet hizmet sağlayıcıların kişisel verileri aktardığı üçüncü kişileri de sorgulamaları tavsiye edilmektedir. Tatmin edici bir yanıt alınamadığı takdirde yetkili makamlara başvurularak kanuni hak arama yollarının işletilmesi gerektiği vurgulanmıştır. Keza, yurt dışı veri aktarımına ilişkin farkındalık da artırılmaya çalışılmıştır.

Tavsiye Kararı, kullanıcılara yönelik tavsiyelerin yanında internet hizmet sağlayıcılarına da çeşitli önerilerde bulunmaktadır. İlk öneri, internet hizmet sağlayıcılarının uygun bilişim teknolojilerini kullanarak verilerin bütünlüğü ve gizliliğine ilişkin gerekli tedbirleri almasına yöneliktir. Aynı doğrultuda, kullanıcılara karşı şeffaf olmaları ve onları internetteki mahremiyet riskleri hakkında bilgilendirmeleri gerektiği hatırlatılmaktadır. Tavsiye Kararı'nda, bilgi güvenliğine ilişkin ihlallerde kullanıcılara bildirim yapma gerekliliğinin izleri de görülmektedir.

Tavsiye Kararı, internet hizmet sağlayıcılarına, hizmetlerinin anonim şekilde kullanılabilmesi için gerekli teknik imkânları sunmalarını önermektedir. Karar, AB Genel Veri Koruma Tüzüğü sayesinde bilinirliği tüm dünyada artan mahremiyet temelli tasarım ilkesini de özünde barındıran öncü bir metindir. Öyle ki internet hizmet sağlayıcılarının, sistemlerini kişisel veriyi kullanmayı gerektirmeyecek veya gerektirdiği durumlarda asgari düzeyde kullanacak şekilde tasarlamaları tavsiye edilmiştir. Aynı doğrultuda, kişisel verilerin açık, belirli ve meşru amaçlarla işlenmesi ve işleme amacına erişmek için gerekli süreyle sınırlı olarak saklanması gerektiğinin altı çizilmiştir.

Tavsiye Kararı, internet hizmet sağlayıcılara yönelik şeffaflık önerilerini de somutlaştırmıştır. İnternet sitelerinde mahremiyet politikalarına yönelik bir bağlantı yer alması ve bu bağlantıdaki içeriğin güncel tutulması gerektiği belirtilmiştir. İnternet ortamında kişisel verileri yayınlayacak hizmet sağlayıcıların iki kez düşünmesi gerektiği zira bu durumun hem kişilerin mahremiyetini ihlal edebileceği hem de kanun tarafından yasaklanmış olabileceği hatırlatılmıştır. Son olarak, kişisel verilerin yurt dışına aktarılmasında, transfere hukuken izin verilip verilmediği konusunda

yetkili makamların onayının alınması gerektiği belirtilmiştir. Keza, kişisel verinin aktarıldığı yurt dışındaki alıcıdan, verinin korunması için gerekli güvenlik önlemlerini alması talep edilmeli denilmiştir.

Yukarıda belirtildiği üzere, İnternette Özel Hayatın Korunmasına İlişkin Tavsiye Kararı, kişisel verilere ilişkin 108 sayılı Sözleşme'ye ilişkin farkındalığı artırmak amacıyla kaleme alınmıştır. Avrupa Konseyinin temel metodolojisi, öz düzenleme (*self-regulation*) yöntemidir. Mücadele, kullanıcılar ve hizmet sağlayıcılar nezdinde gerçekleştirilmektedir. Bilgi otobanlarındaki en temel sorunlar anonimlik, veri güvenliği ve mahremiyet olarak tespit edilmiştir. Bu konular hem ulusal hem de uluslararası düzeyde bilişim ve teknoloji hukukunun en güncel tartışma alanları olmaya devam etmektedir.

Tavsiye Kararı'nı ele alan Avrupa Birliği Madde 29 Çalışma Grubu, bu alanda bir yol göstericiliğe ihtiyaç duyulduğu için metnin önemli olduğuna vurgu yapmıştır. Bununla birlikte, metin, kısa olmasının yanı sıra veri süjelerinin internet ortamında verilerinin toplanması ve hareketlerinin takip edilmesine ilişkin bazı teknik hususlarda temel bilgileri olduğu varsayımından hareket etmesi sebebiyle eleştirmiştir.[243]

II. Arşiv Erişimine Yönelik Bir Avrupa Politikası Hakkında Tavsiye Kararı (2000)

Arşiv Erişimine Yönelik Bir Avrupa Politikası Hakkında Tavsiye Kararı, Avrupa Konseyi Bakanlar Komitesinin 13 Temmuz 2000 tarihli 717. Toplantısı'nda kabul edilmiştir.[244] Tavsiye Kararı, Avrupa Konseyinin üyeleri arasında daha yakın bir birlik oluşturma amacını hatırlatarak bunun ancak kültürel alanda ortak eylemle mümkün olacağı girişiyle baş-

---

[243] **Article 29 - Data Protection Working Party**, "Third Annual Report on the Situation Regarding the Protection of Individuals with Regard to the Processing of Personal Data and Privacy in the Community and in Third Countries - Covering the Year 1998, Adopted on 22nd December, 1999" <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2000/wp35_en.pdf>, s. 49.

[244] **Avrupa Konseyi**, "*Recommendation No. R (2000) 13 of the Committee of Ministers to member states on a European policy on access to archives*", <https://rm.coe.int/16804cea4f>

lamaktadır. Karar, Avrupa Konseyinin uluslararası alandaki en önemli iki enstrümanı olan Avrupa İnsan Hakları Sözleşmesi (AİHS) ve 108 sayılı Sözleşme'ye atıf yapmış, insan hakları ve kişisel verilerin korunmasına ilişkin temel rejime dikkat çekmiştir.

Esasında Avrupa Konseyinin arşivlere erişim konusuyla belirli ölçüde bağlantılı, 1981[245] ve 1991[246] yıllarında alınmış başka tavsiye kararları da bulunmaktadır. 2000 tarihli yeni Tavsiye Kararı, önceki kararları da gözeterek arşivlere erişime ilişkin sorunları güncel gelişmeler ışığında adreslemeye çalışmıştır.

Tavsiye Kararı'na göre arşivler, kültürün temel ve yeri doldurulamaz unsurudur, insan hafızasının devamlılığını temin eder. Tarihe yönelik artan ilgiye ve farklı toplumların bu konuda hayata geçirdiği yapısal değişikliklere dikkat çeken Karar, her bir ferdinin objektif bir şekilde tarihinin unsurlarını bilme imkânı olmadığı sürece bir ülkenin tam manasıyla demokratik olarak nitelendirilemeyeceğini belirtmiştir. Bu önemine rağmen, ulusal ve uluslararası seviyede anayasal ve yasal düzenlemelerdeki şeffaflık, gizlilik, mahremiyetin korunması, tarihî bilgiye erişim ile ilgili çatışan düzenlemeler sebebiyle karmaşık sorunlar ortaya çıkmakta, her bir ülkede arşivlere erişim farklı şekilde algılanmaktadır.

Tarihçilerin ve sivil toplumun tarihsel süreci daha iyi anlamlandırmasına ilişkin temennisini belirten Tavsiye Kararı, yakın Avrupa tarihinin anlaşılmasının ihtilafları önlemeye hizmet edeceğini belirtmiştir. Bu genel girişten sonra Avrupa Konseyi, üye devletlere, arşivlere erişime ilişkin bu Tavsiye Kararı'nda belirtilen ilkeleri gözeten ve mevcut düzenlemeleri de bu ilkelerle uyumlu hâle getiren bir yasal düzenleme yapma çağrısında bulunmuştur.

---

[245] **Avrupa Konseyi**, "*Recommendation No. R (81) 19 of the Committee of Ministers to Member States on the access to information held by public authorities*", <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804f7a6e>

[246] **Avrupa Konseyi**, "*Recommendation (91)10 of the Committee of Ministers to member states on the communication to third parties of personal data held by public bodies*", <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804c1486>

Tavsiye Kararı'nda arşiv, "*tarih, biçim veya aracı ne olursa olsun herhangi bir birey veya kurumsal yapı tarafından iş sürecinde oluşturulan veya alınan ve kalıcı muhafaza için arşiv kurumlarına iletilen belgelerin toplamı*" olarak tanımlanmıştır. Aksi belirtilmediği sürece, mevcut Tavsiye'nin sadece "kamusal arşivler" ve resmî makamlarca oluşturulanlar için geçerli olduğu belirtilmiştir.[247]

Avrupa Konseyi, arşivlere erişime ilişkin kanuni bir düzenleme yapılmasını ve böyle bir kanun hazırlanırken de kişisel verilerin korunmasına ilişkin düzenlemelerle uyumun gözetilmesini tavsiye etmektedir.[248] Tavsiye Kararı, kamusal arşivlere erişimi bir hak olarak nitelendirmekte ve demokratik değerlere saygı duyan her sistemde, bu hakkın uyurkluk, statü veya fonksiyondan bağımsız olarak tanınması gerektiğini belirtmektedir.[249] Öyle ki arşivlere erişim, kamu arşiv hizmetlerinin bir parçasıdır ve ücretsiz olmalıdır.[250] Yapılacak düzenlemede, herhangi bir kısıtlama olmaksızın kamusal arşivlerin açılması veya genel kapatılma süreleri belirlenmelidir.[251]

Arşivlere erişim hakkına bir kısıtlama getirilebilir mi? Tavsiye Kararı'na göre demokratik bir toplumda, ulusal güvenlik, dış politika ve kamu düzeni gibi korunmaya değer önemli bir kamusal menfaat varsa veya kişilerin, özel hayatlarına ilişkin bilgilerin yayımlanmasına karşı korunması söz konusuysa böyle bir kısıtlama getirilebilir yeter ki bu tür kısıtlamaların açık bir kanuni dayanağı olsun.[252] Arşivlere erişimin teknik detaylarına ve özel erişim taleplerine de değinen Tavsiye Kararı, niteli-

---

[247] **Avrupa Konseyi**, *Arşiv Erişimine Yönelik Bir Avrupa Politikası Hakkında Tavsiye Kararı*, para. 1.

[248] **Avrupa Konseyi**, *Arşiv Erişimine Yönelik Bir Avrupa Politikası Hakkında Tavsiye Kararı*, para. 3.

[249] **Avrupa Konseyi**, *Arşiv Erişimine Yönelik Bir Avrupa Politikası Hakkında Tavsiye Kararı*, para. 5.

[250] **Avrupa Konseyi**, *Arşiv Erişimine Yönelik Bir Avrupa Politikası Hakkında Tavsiye Kararı*, para. 6.

[251] **Avrupa Konseyi**, *Arşiv Erişimine Yönelik Bir Avrupa Politikası Hakkında Tavsiye Kararı*, para. 7.

[252] **Avrupa Konseyi**, *Arşiv Erişimine Yönelik Bir Avrupa Politikası Hakkında Tavsiye Kararı*, para. 7.1.-7.2.

ğine uygun düştüğü ölçüde benzer düzenlemelerin özel arşivler için de getirilmesini önermektedir.[253]

Tavsiye Kararı'nın önerileri etik, usuli ve teknik ilkeler olarak üç ana kategoride sınıflandırılabilir.[254] Arşive erişimin bir hak olarak kabul edilmesi, bu hakkın herkese aynı şekilde uygulanması, kısıtlamaların sadece kamusal menfaatleri ve özel bireyleri korumak için gerekliyse uygulanması, tüm kısıtlamaların süreyle sınırlandırılması, kısıtlı erişimli belgelere erişim koşullarının herkes için aynı olması kararın etik kısmıdır.

Karar'da ifade edilen ve usuli ilkelerle ilişkili olan gereklilikler ise şunlardır: arşivlere ilişkin tüm hukuki düzenlemelerin birbiriyle uyumlu olması, kamusal arşivlere erişimin bir ülkede aynı kurallara tabi tutulması, tüm kısıtlamaların kanuni bir dayanağının olması, kullanıcıların kısıtlı erişimli belgelere erişimi talep etme haklarının olması ve bu tür taleplerin reddi durumunda itiraz imkânının tanınması, genel veya özel erişim talebinin reddine ilişkin sürecin yazılı olarak sunulması.

Son olarak, kamu kayıtlarına erişim için ücret alınmaması, arşiv kurumlarının kullanıcılarına erişimi kısıtlamaması, kullanıcıya kısmi erişim sağlandığı takdirde bilgilendirmede bulunulması gereklilikleri ile özel arşivlere de imkân olduğu ölçüde kamusal arşivlerinkine benzer kuralların uygulanması Karar'ın teknik kısmını oluşturur.

Arşivlere erişim konusu bilgi edinme hakkıyla da bağlantılı bir konudur. Avrupa Konseyi, 2009 yılında arşivleri de içeren resmî belgelere erişim alanında, 205 numaralı Sözleşme olarak bilinen Resmî Belgelere Erişime İlişkin Sözleşme'yi imzaya açmıştır.[255] Henüz çok yüksek bir kabul edilme oranına kavuşmamış olsa da bu Sözleşme, konunun bilgi edinme

---

[253] **Avrupa Konseyi**, *Arşiv Erişimine Yönelik Bir Avrupa Politikası Hakkında Tavsiye Kararı*, para. 9-12.

[254] **Kecskeméti, Charles/Székely, Iván** (2005) *Access to Archives: A Handbook of Guidelines for Implementation of Recommendation No R (2000)13 on a European Policy on Access to Archives*, Belgium, Council of Europe Publishing, s. 12-16.

[255] **Avrupa Konseyi**, "*Convention on Access to Official Documents CETS No.205*" <https://rm.coe.int/1680084826>; Sözleşme'nin gayri resmî tercümesi için bkz. **Aykaç, Alper Can** (2009) "*Resmî Belgelere Erişime İlişkin Avrupa Konseyi Sözleşmesi*" TBB Dergisi, Sayı: 83, s. 402-411.

hakkının uluslararası boyutunu göstermesi açısından önemlidir.[256] Keza, unutulma hakkının kullanılması bağlamında arşivlerin internet ortamında genel erişime açık tutulması sorunu önemli bir tartışma konusudur. Tavsiye Kararı'nda da belirtildiği üzere, kişilerin özel hayatlarına ilişkin bilgiler içermesi durumunda arşivlere erişimin kısıtlanması mümkündür. Tabii ki böyle bir kısıtlama kanuni dayanağa sahip olmalı ve toplumun genel olarak bilgi edinme hakkına ölçüsüz müdahale niteliği taşımaması için objektif kriterlere tabi tutulmalıdır.

III. Siber İçeriğin Öz Düzenlemesine İlişkin Tavsiye Kararı (2001)

Siber İçeriğin Öz Düzenlemesine İlişkin Tavsiye Kararı, Avrupa Konseyi Bakanlar Komitesinin 5 Eylül 2001 tarihli 762. Toplantısı'nda kabul edilmiştir.[257] Tavsiye Kararı'nın asıl amacı, hukuka aykırı ve zararlı içerikle mücadelede temel bir usul geliştirmektir.

Tavsiye Kararı, AİHS'nin 10. maddesinde güvence altına alınan ifade özgürlüğü ve bilgiye erişim hakkının bireylerin sosyal, ekonomik, kültürel ve siyasal gelişimi için gerekliliğini tekrar etmiştir. Giriş kısmında, yeni bilişim ve teknoloji hizmetlerinin geliştirilmesinin sınır tanımaksızın herkesin bilgi ve fikirleri ifade etmek, almak ve vermek hakkının gelişimine, her bir bireyin ve toplumun demokratik kültürüne hizmet etmesi gerektiği vurgulanmıştır. Keza, yeni bilişim ve teknoloji hizmetleri insanların şerefine, başta küçükler olmak üzere başkalarının insan hak ve özgürlüklerine halel getirmemelidir.

---

[256] 1 Aralık 2020 itibarıyla Türkiye, 205 sayılı Sözleşme'ye henüz taraf değildir.

[257] **Avrupa Konseyi**, "*Recommendation Rec (2001) 8 of the Committee of Ministers to member states on self-regulation concerning cyber content (self-regulation and user protection against illegal or harmful content on new communications and information services)*", <https://www.osce.org/files/f/documents/0/7/31584.pdf>

Tavsiye Kararı; şiddet, vahşet veya pornografi içeren videoların dağıtımı,[258] ırkçı içerikli video oyunları,[259] elektronik medyada şiddetin temsili[260] ve nefret söylemine[261] ilişkin önceki Avrupa Konseyi kararları ile Birleşmiş Milletlerin kabul ettiği Her Türlü Irk Ayrımcılığının Ortadan Kaldırılmasına İlişkin Uluslararası Sözleşme'ye atıf yapmıştır.

Tavsiye Kararı, "zararlı içerik" tanımını yapmıştır. Ulusal ceza mevzuatlarındaki hukuka aykırı içerik ile özellikle küçükler ve onların fiziksel, zihinsel ve ahlaki gelişimleri için neyin potansiyel anlamda zararlı olarak nitelendirileceği hususları zararlı içerik kavramı altında ele alınmıştır.

Tavsiye Kararı, öz düzenleyici yapıların (*self-regulatory organisations*) ulusal koşullar ve teamüller ile uyum içerisinde belirli normları ortak düzenleme yöntemiyle düzenleyebileceğini de kabul etmektedir. Bu doğrultuda, hukuka aykırı içeriği kaldırmak ve kullanıcıları zararlı içeriklere karşı korumak için yeni bilgi ve iletişim endüstrilerinin öz düzenleyici girişimlerine ve kullanıcılara içeriği seçme ve filtreleme imkânı sağlayan teknik standartlar ile aygıtlara işaret edilmiştir. Tavsiye Kararı, tüm bu çerçevede öz düzenlemeyi desteklemeyi, yaygınlaştırmayı ve kullanıcıları hukuka aykırı veya zararlı içeriklere karşı korumayı amaçlamaktadır.

Tavsiye Kararı'nın ilk bölümü öz düzenleyici yapılara ayrılmış, öz düzenlemeye ilişkin prensip ve mekanizmalar belirtilmiş, kullanıcıların yeni bilgi ve iletişim hizmetlerinde hukuka aykırı veya zararlı içeriğe karşı

---

[258] **Avrupa Konseyi**, "*Recommendation No. R (89) 7 concerning principles on the distribution of videograms having a violent, brutal or pornographic content*", <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804e8fe8>

[259] **Avrupa Konseyi**, "*Recommendation No. R (92) 19 on video games with a racist content*", <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804d74f7>

[260] **Avrupa Konseyi**, "*Recommendation No. R (97) 19 on the portrayal of violence in the electronic media*", <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680509212>

[261] **Avrupa Konseyi**, "*Recommendation No. R (97) 20 on "hate speech"*", <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680505d5b>

korunması için muhtelif öneriler getirilmiştir.[262] Avrupa Konseyi, üye devletlerin, internet hizmet sağlayıcılar, içerik sağlayıcılar ve kullanıcılar gibi aktörleri temsil eden yapılar oluşturmasını teşvik etmektedir. Bu yapıların kendi yetki alanlarında düzenleyici mekanizmalar kurmaları, özellikle de davranış kuralları geliştirmeleri ve bu kurallara uyumu takip etmeleri önerilmektedir. Keza, medya alanındaki öz düzenleyici kuruluşların, bu standartlarını mümkün olduğunca yeni bilgi ve iletişim hizmetlerine de uygulaması tavsiye edilmektedir.

Avrupa Konseyi, konunun yönetişim ve paydaş katılımı boyutuna ilişkin tavsiyelerde de bulunmuştur. Bu bağlamda, üye devletlere, oluşturulacak öz düzenleyici yapıları danışmanlık, toplantı, uzman görüşleri gibi yöntemlerle yasama sürecine katılmaya ve normların uygulanmasını izlemeye teşvik etmeleri önerilmektedir. Bu tür yapılar arasında Avrupa genelinde ve uluslararası düzeyde iş birliğinin artırılması da tavsiye edilmektedir.

Tavsiye Kararı'nda öz düzenleyici yapılar dışında ele alınan bir diğer konu ise içerik tanımlayıcılarıdır.[263] Karar'da üye devletlere, içeriği tarafsız şekilde etiketleyerek bir içerik üzerinde kullanıcıların kendi değerlendirmelerini yapmalarına imkân tanıyacak "*içerik tanımlayıcı*" aktörünü mümkün olan en geniş coğrafi ölçüde ve öz düzenleyici yapılarla birlikte tanımlaması tavsiye edilmektedir. İçerik tanımlayıcıdan beklenen, şiddet ve pornografi içeren, aynı şekilde tütün veya alkol kullanımını teşvik eden veya kumar hizmetlerine dair içeriği ve küçüklerle yetişkinler arasında denetimsiz ve anonim iletişim imkânı sağlayan içerikleri belirlemesidir.

İçerik tanımlayıcının yapmış olduğu sınıflandırmanın icrası nasıl gerçekleşecektir? Amaç içeriği kaynağında engellemek olduğu için içerik sağlayıcıların, içerik tanımlayıcıları tarafından belirlenen kriterleri sistemlerinde uygulayarak içeriğin kaynağında tanınması ve kaynağından bağımsız şekilde bu tür içeriğin filtrelenmesi hedeflenmektedir.

---

[262] **Avrupa Konseyi**, *Siber İçeriğin Öz Düzenlemesine İlişkin Tavsiye Kararı*, Chapter I.

[263] **Avrupa Konseyi**, *Siber İçeriğin Öz Düzenlemesine İlişkin Tavsiye Kararı*, Chapter II.

Tavsiye Kararı, hukuka aykırı veya zararlı içerikle mücadelede içerik tanımlayıcılara daha fazla rol vererek içerik seçme araçlarının geliştirilmesini önermektedir.[264] Karar, üye devletlerin geniş bir yelpazede arama araçlarının ve filtreleme profillerinin geliştirilmesini teşvik etmelerini önermektedir. Bu tür araçlar sayesinde kullanıcıların içerik sağlayıcıların belirlediği kriterlere göre içeriği seçmeleri mümkün olacaktır.

İçeriğe ilişkin yaklaşım, kullanıcıların gönüllülük esasının üzerine inşa edilmektedir. Bu doğrultuda, üye devletler, içerik ve hizmet sağlayıcıların küçüklere zararlı içerikler için yaş doğrulama sistemleri, kişisel tanımlama kodları, şifreler, şifreleme ve deşifre sistemleri veya elektronik bir kodla kart üzerinden erişim gibi koşullu erişim araçlarını geliştirmesini teşvik etmelidir.

Tavsiye Kararı'nda ele alınan bir diğer mekanizma ise içerik şikâyet sistemleridir.[265] Tavsiye Kararı, üye devletlere internet servis sağlayıcıları, içerik sağlayıcıları, kullanıcı birlikleri veya diğer kuruluşları şikâyet hattı benzeri şikâyet mekanizmaları kurmaya teşvik etmesini önermektedir. Bu tür içerik şikâyet sistemleri, hukuka aykırı olduğu varsayılan içeriğe uygun işlemin yapılabilmesi için, kamu otoriteleri tarafından sağlanan şikâyet hatlarıyla desteklenmelidir.

Tavsiye Kararı'nda, bu tür şikâyet sistemlerinin sahip olması gereken asgari ortak nitelikler de belirlenmiştir. Ayrıca, şikâyet mekanizmalarının birbirleriyle ve kamu otoriteleriyle iş birliğinin artırılması ve özellikle hukuka aykırı olduğu varsayılan içerikle ilgili sınır aşan iş birliği için lüzumlu hukuki ve idari tedbirlerin alınması gerektiği vurgulanmıştır.

İçerikle ilgili ihtilafların çözümü için Tavsiye Kararı arabuluculuk usulünü önermektedir.[266] Avrupa Konseyi, üye devletlere, yerel düzeyde ve gönüllülük esasına göre işleyecek, mahkeme dışı uzlaşmayı sağlayacak adil, bağımsız, erişilebilir ve etkin yapılar veya usuller ile ihtilafların çözümü için arabuluculuk mekanizmaları oluşturmalarını tavsiye etmektedir.

---

[264] **Avrupa Konseyi**, *Siber İçeriğin Öz Düzenlemesine İlişkin Tavsiye Kararı*, Chapter III.

[265] **Avrupa Konseyi**, *Siber İçeriğin Öz Düzenlemesine İlişkin Tavsiye Kararı*, Chapter IV.

[266] **Avrupa Konseyi**, *Siber İçeriğin Öz Düzenlemesine İlişkin Tavsiye Kararı*, Chapter V.

İçerik şikâyet sistemlerine ilişkin yapılar gibi arabuluculuk yapılarının da Avrupa genelinde iş birliği içerisinde olması, sınır tanımaksızın herkesin erişimine açık bulunması, mahkeme dışında alınan uzlaşma kararlarının kamu ve temel usul kuralları bağlamında karşılıklı tanınması ve icrasının temin edilmesi ayrıca sağlanmalıdır.

Tavsiye Kararı'nın son kısmı ise kullanıcı bilgilendirmesi ve farkındalığın artırılmasına ilişkindir.[267] Buna göre, üye devletlerden, kamusal içerik, eğitim içeriği ve çocuklar için uygun içerik gibi içeriği tanımayı kolaylaştıracak kalite etiketleri geliştirilmesini teşvik etmeleri beklenmektedir. Aynı şekilde, üye devletlerin öz düzenleyici mekanizmalar, içerik tanımlayıcılar, filtreleme araçları, erişim kontrol araçları, içerik şikâyet mekanizmaları, mahkeme dışı uzlaşma ve tahkim süreçleriyle ilgili kamusal farkındalığı artırmaları beklenmektedir.

Siber İçeriğin Öz Düzenlemesine İlişkin Tavsiye Kararı, internet ortamında hukuka aykırı-zararlı içerik ayrımı yaptığı ve bu içeriklerin düzenlenmesine ilişkin temel araçları tanımladığı için öncü bir politik enstrümandır. Avrupa Konseyinin öz düzenleme yaklaşımı, Avrupa Birliği'nin çocuklara yönelik online güvenlik ve özellikle çocukların online mahremiyetinin korunması politikalarının da temel taşını oluşturmuştur.[268]

IV. İnternette İletişim Özgürlüğüne İlişkin Deklarasyon (2003)

İnternette İletişim Özgürlüğüne İlişkin Deklarasyon, Avrupa Konseyi Bakanlar Komitesinin 28 Mayıs 2003 tarihli 840. Toplantısı'nda kabul edilmiştir.[269] Deklarasyon, AİHS'nin 10. maddesiyle güvence altı-

---

[267] **Avrupa Konseyi**, *Siber İçeriğin Öz Düzenlemesine İlişkin Tavsiye Kararı*, Chapter VI.

[268] **Van der Hof, Simone/Van den Berg, Bibi/Schermer, Bart** (2014) *Minding Minors Wandering the Web: Regulating Online Child Safety*, The Hague, T.M.C. Asser Press, s. 131.

[269] **Avrupa Konseyi**, "*Committee of Ministeres Declaration on freedom of communication on the Internet*", <https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805dfbd5>

na alınan ifade özgürlüğü ve bilgiye erişim hakkı ile ifade özgürlüğü ve bilginin internet ortamında özgürce dolaşımı üzerine kaleme alınmıştır.

Deklarasyon, AİHS'nin 10. maddesinin ikinci fıkrası bağlamında ifade özgürlüğü ile diğer meşru haklar ve menfaatler arasında bir denge kurulması gerekliliğini vurgulayarak ve Siber İçeriğin Öz Düzenlemesine İlişkin Tavsiye Kararı ile Avrupa Konseyinin kitle iletişim araçlarına[270] ilişkin politik belgelerine atıf yaparak başlamaktadır.

Deklarasyon'a göre, internet üzerinden iletişime kamusal erişimi politik sebepler veya başka motivasyonlarla kısıtlama girişimleri demokratik ilkelere aykırılık teşkil etmektedir. Bu endişenin giderilmesinin temel yöntemi, herhangi bir sınır tanımaksızın internet ortamındaki iletişimin ön denetiminin bir istisnai durum olarak kalması ve bireylerin internete erişimine ilişkin engellerin kaldırılmasıdır.[271]

Deklarasyon, internet aracılığıyla hizmet sunumunun, kullanıcıların muhtelif yerel ve yabancı kaynaklardan çoğulcu içeriğe erişimini temin edeceğini ifade etmiştir. Bu sebeple hizmet sağlayıcıların salt nakledici olduğu veya üçüncü tarafların sunduğu içeriklere iyi niyetle erişim sağladıkları yahut bu tür içerikleri barındırdıkları durumlarda sorumluluklarının sınırlandırılması gerektiği belirtilmiştir. Ayrıca bu konuları düzenleyen önemli bir Avrupa Birliği düzenlemesi olan AB E-Ticaret Direktifi'ne atıf yapılmıştır. Başlangıç kısmında belirtilen çeşitli haklar arasında denge sağlanması gerekliliğini tekrar hatırlatan Deklarasyon, internet ortamında iletişimin insan onuru, insan hakları ve başta küçükler olmak üzere başkalarının temel haklarına halel getirmemesi gerektiğini vurgulamıştır.

Deklarasyon'un denge gözetilmesi gerektiğini belirttiği bir diğer konu ise internet ortamında anonim olma hakkı ve suçla mücadele soru-

---

[270] **Avrupa Konseyi**, "*Resolution No. 1 of the 5th European Ministerial Conference on Mass Media Policy (Thessaloniki, 11-12 December 1997)*", <https://rm.coe.int/16804f49ed>

[271] Bu konuda bkz. **Avrupa Konseyi**, "*Recommendation No. R (99) 14 Of the Committee of Ministers to Member States on universal community service concerning new communication and information services*", <https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680502333>

nudur. Deklarasyon, internet ortamında yer alan hukuka aykırı içeriklerle mücadelede hizmet sağlayıcıların kolluk kuvvetleriyle iş birliğinin önemine değinmiştir. Ardından Deklarasyon'da internet özgürlüğüne ilişkin şu yedi ilke ortaya konulmuştur:

İlke 1: İnternet için içerik kuralları

İlke 2: Öz düzenleme veya ortak düzenleme

İlke 3: Devletin ön kontrolünün bulunmaması

İlke 4: Bireylerin bilgi toplumuna katılımının önündeki engellerin kaldırılması

İlke 5: İnternet aracılığıyla hizmet sunma özgürlüğü

İlke 6: Hizmet sağlayıcıların internet içeriğinden dolayı kısıtlı sorumluluğu

İlke 7: Anonimlik

Deklarasyonun ilk ilkesi, internet için içerik kurallarıdır. Deklarasyon uyarınca üye devletler internet ortamındaki içeriklere, başka enstrümanlarla içerik sunumuna uygulanandan daha katı bir kısıtlama getirmemelidir. Bu şekilde, online ve offline içerik ayrımı ortadan kaldırılmaya çalışılmıştır.

Tıpkı Siber İçeriğin Öz Düzenlemesine İlişkin Tavsiye Kararı gibi İnternette İletişim Özgürlüğüne İlişkin Deklarasyon da öz düzenlemeye yer vermektedir. Deklarasyon'un üçüncü ilkesi öz düzenleme ve ortak düzenlemeye ilişkindir. Üye devletlerin, bu bağlamda, internet ortamında yayımlanan içeriğe ilişkin olarak öz düzenleme ve ortak düzenleme yöntemlerini teşvik etmeleri beklenmektedir.

Deklarasyon'un üçüncü temel ilkesi, devletin ön kontrolünün bulunmaması gerekliliğine ilişkindir. Buna göre, kamu otoriteleri her türlü sınırdan bağımsız olarak genel engelleme veya filtreleme tedbiri uygulayarak kamunun bilgiye erişimini veya internet ortamında başka tür iletişimi engellememelidir. Deklarasyon bu genel kurala küçüklerin korunmasına

ilişkin bir istisna getirmektedir. Söz konusu istisnaya göre, küçüklerin korunması için özellikle internet erişimi olan okul veya kütüphane gibi yerlerde filtreleme uygulamalarının kullanılması mümkündür. Keza, AİHS'nin 10. maddesinin ikinci fıkrasındaki korumalara riayet edilmesi kaydıyla, açıkça tanımlanabilir bir internet içeriğinin kaldırılması veya alternatif olarak bu içeriğe erişimin kısıtlanması, ulusal makamların içeriğin hukuka aykırılığına ilişkin geçici veya nihai bir karar almış olmasına bağlıdır.

Deklarasyon'un açıklayıcı notunda, üçüncü ilkeye ilişkin aşağıdaki yoruma yer verilmiştir:

"Devletin ön kontrolünün bulunmaması

Bu ilke, toplumun internet ortamındaki aramalarında devletin ön kontrolünün bulunmamasının öneminin altını çizmektedir. Birtakım devletler gerçekten de vatandaşlarının bazı yabancı veya yerel internet sitelerinin içeriklerine erişimlerini siyasi gerekçelerle engelleme eğilimi içindedir. Bu uygulama ve devletin ön kontrolüne ilişkin her türlü benzer uygulama sert bir şekilde kınanmalıdır.

Her ne kadar devletler istenmeyen içeriğe erişimi engelleyici geniş çaplı önlemleri hiçbir koşulda almamalılar ise de küçüklerin korunması için gerekli istisnalara izin verilmelidir. Küçüklerin internete örneğin okul veya kütüphanelerde erişimleri sırasında, kamu kurumları zarar verici içeriklere erişimin engellenmesi için bilgisayarlara filtre kurulmasını talep edebilir.

Devletin ön kontrolünün bulunmaması, bir içeriğin, yalnızca ceza hukuku değil, idare hukuku ve medeni hukuk gibi diğer hukuk dalları açısından da yasal olmadığına ilişkin yetkili ulusal makamlar tarafından alınan geçici veya nihai bir karar sonucunda silinmesi veya buna erişimin engellenmesi için gerekli önlemlerin alınması imkânını şüphesiz ki ortadan kaldırmaz. Yasa dışı bir içeriğe toplumun erişiminin engellenmesi, bu şekilde alınabilecek önleyici tedbirlerden sayılabilir. Ön kontrole sebep olabilecek bu tarz önlemler, İnsan Hakları ve Temel Özgürlüklerin Korunmasına İlişkin Sözleşme'nin 10.2 maddesinin hükümlerine uygun olmalı ve açıkça tespit edilebilen bir internet içeriğine yönelmelidir."

Deklarasyon'un dördüncü ilkesi, bireylerin bilgi toplumuna katılımının önündeki engellerin kaldırılmasına dairdir. Bu doğrultuda, üye devletler, internet iletişimi ve bilgi hizmetlerine herkesin adil şekilde ve makul bir ücretle erişimini özendirmeli ve teşvik etmelidir. Deklarasyon, evrensel hizmet yaklaşımını öne çıkarmaktadır. Deklarasyon ayrıca kamunun aktif katılımının, örneğin web siteleri oluşturmak ve işletmek gibi, herhangi bir lisanslama veya benzer etkiye sahip bir şarta tabi tutulmaması gerektiğini belirtmektedir.

İnternete erişim hakkıyla bağlantılı bir diğer hak ise internet ortamında hizmet sunma özgürlüğüdür. Deklarasyonun beşinci ilkesi bu hakka ilişkindir. Söz konusu ilkeye göre, internet aracılığıyla hizmet sunma hakkı salt kullanılan iletim mecrası sebebiyle özel bir yetkilendirme düzenine tabi tutulmamalıdır.

Deklarasyon, üye devletlere bu konuda aktif bir yükümlülük getirerek onları internet aracılığıyla sunulan hizmetlerde farklı kullanıcı ve sosyal grupların ihtiyaçlarını karşılayacak, çoğulculuğu sağlayacak tedbirleri almaya davet etmektedir. Hizmet sağlayıcıların ulusal ve uluslararası telekomünikasyon ağlarına erişimde ayrımcılığa uğramamasını temin edinen düzenleyici kurallarla hizmet sunmaları sağlanmalıdır.

Deklarasyon, internet aracılığıyla hizmet sunma özgürlüğünü tamamlayıcı bir hakkı da tanımlamaktadır: hizmet sağlayıcıların internet içeriğinden dolayı kısıtlı sorumluluğu. Deklarasyon'un altıncı maddesi, üye devletlerin, hizmet sağlayıcılara internet ortamında erişim sağladıkları, ilettikleri veya barındırdıkları içeriği izlemeye veya hukuka aykırı bir faaliyete ilişkin unsurları veya olayları aktif olarak araştırmaya ilişkin genel bir yükümlülük getirmemesini önermektedir. Üye devletler, hizmet sağlayıcıların fonksiyonlarının -ulusal hukukta tanımlandığı üzere- bilgiyi iletme veya internete erişim sağlamayla sınırlı olduğu durumlarda internet ortamındaki içerikten sorumlu tutulmamasını temin etmelidir.

Deklarasyon, hizmet sağlayıcıların fonksiyonlarının kısıtlı olmadığı durumlar için farklı bir hukuki sorumluluk rejimi öngörmektedir. Deklarasyon'un altıncı maddesine göre, hizmet sağlayıcılar fonksiyonları daha geniş olduğunda ve üçüncü kişilere ait içerikleri barındırdıklarında

üye devletler tarafından şu durumlarda sorumlu tutulabilir: İç hukukta tanımlandığı üzere bu tür içeriklerin hukuka aykırılıklarından haberdar olunduğu takdirde veya söz konusu aktivitenin yahut bilginin hukuka aykırılığını ifşa eden olaylar veya durumlar bağlamında tazminata ilişkin bir talep gerçekleştiğinde içerik derhal kaldırılmaz veya bilgi ya da hizmetlere erişimi kısıtlamazsa. Üye devletler, bu doğrultuda, hizmet sağlayıcıların iç hukuktaki yükümlülüklerini tanımlarken içeriği ilk noktada yayına sokan kişinin ifade özgürlüğünün ve aynı zamanda kullanıcıların bu bilgiye tekabül eden haklarının korunmasına özen göstermelidir. Deklarasyon, bu tür bir sorumluluk durumunun hizmet sağlayıcılar aleyhine, uygun olduğu ölçüde, bir hukuk kuralının ihlalini durdurma veya önlemeye ilişkin bir tedbir kararı alınmasını engellemediğini belirtmektedir.

Deklarasyon'da yer alan son ilke ise internet ortamında anonim olmaya ilişkindir. Deklarasyon'un yedinci ilkesi uyarınca, online takibe karşı korumayı temin etmek ve ifade özgürlüğünü geliştirmek amacıyla, üye devletler, kullanıcıların internet ortamında kimliklerinin ifşa edilmemesine ilişkin taleplerine saygı göstermelidir. Bu yükümlülük, üye devletlerin iç hukuka, AİHS'ye ve yargı ile kolluğa ilişkin diğer uluslararası sözleşmelere göre cezai fiillerin sorumlularının tespit ve takibi için önlemler alması ve iş birliği içinde bulunmasına engel değildir.

İlke 1: İnternet için içerik kuralları

Üye devletler, internet içeriğine, diğer içerik dağıtım araçlarına getirilen düzenlemelerin ötesinde bir sınırlama getirmemelidirler.

İlke 2: Öz düzenleme veya ortak düzenleme

Üye devletler, internete sunulan içeriğin öz düzenlenmesi veya ortak düzenlenmesini teşvik etmelidir.

İlke 3: Devletin ön kontrolünün bulunmaması

Kamu otoriteleri, engelleme veya filtreleme gibi genel önlemler vasıtasıyla, sınır tanımayan bir şekilde toplumun bilgiye veya internet ortamındaki diğer iletişim olanaklarına erişiminin önüne geçmemelidir.

Bu durum küçüklerin bulunabileceği okul veya kütüphane gibi yerlerde onların korunması amacıyla filtreleme yapılmasını engellemeyecektir.

Yetkili ulusal makamlar bunun hukuki olmadığı hususunda geçici veya nihai bir karar verdikleri takdirde, İnsan Hakları ve Temel Özgürlüklerin Korunmasına İlişkin Sözleşme'nin 10.2 maddesinde yer alan güvencelere saygı gösterilmesi kaydıyla, açıkça tespit edilebilen bir internet içeriğinin silinmesi için veya alternatif olarak, buna erişimin engellenmesi için gerekli önlemler alınabilir.

İlke 4: Bireylerin bilgi toplumuna katımının önündeki engellerin kaldırılması

Üye Devletler, herkesin İnternet haberleşmesine ve bilgi hizmetlerine ayrımcılığa tabi tutulmadan bir şekilde ve makul bir ücretle katılmasını teşvik etmeli ve desteklemelidir. Ayrıca, bireysel web siteleri oluşturarak ve işleterek kamuya aktif katılım, herhangi bir lisans veya benzeri etkide bir gerekliliğe tabi tutulmamalıdır.

İlke 5: İnternet aracılığıyla hizmet sunma özgürlüğü

İnternet aracılığıyla hizmet sunumu salt iletim için kullanılan mecra sebebiyle özel bir yetkilendirme düzenine tabi tutulmamalıdır.

Üye Devletler, internet aracılığıyla farklı kullanıcıların ve sosyal grupların ihtiyaçlarını karşılayan çoğulcu hizmetlerin sunulmasını teşvik edecek tedbirler almalıdır. Hizmet sağlayıcıların ulusal ve uluslararası telekomünikasyon ağlarına ayrım gözetmeksizin erişimini temin eden düzenleyici bir çerçevede faaliyette bulunmaları temim edilmelidir.

İlke 6: Hizmet sağlayıcıların internet içeriğinden dolayı kısıtlı sorumluluğu

Üye Devletler, hizmet sağlayıcılara internet ortamında erişime sundukları, ilettikleri veya barındırdıkları içeriği izlemelerine yönelik veya hukuka aykırı faaliyetlere ilişkin vakıaları veya durumları aktif olarak araştırmaya yönelik bir yükümlülük yüklememelidir.

Üye Devletler, hizmet sağlayıcıların ulusal hukuk tarafından tanımlandığı şekliyle bilgiyi iletmek veya internete erişim sağlamak gibi içeriğe yönelik fonksiyonlarının sınırlı olduğu durumlarda, içerikten dolayı sorumlu tutulmamalarını temin etmelidir.

Hizmet sağlayıcıların fonksiyonlarının daha geniş olduğu durumlarda ve başka taraflardan kaynaklanan içerikleri barındırdıkları durumlarda, Üye Devletler hizmet sağlayıcıları, eğer iç hukukta tanımlandığı şekliyle bilgi veya hizmetlerin hukuka aykırılığı niteliğine veya zarar için bir tazmin talebine veya faaliyetin veya bilginin hukuka aykırılığını gösteren olaylar ve koşullar hakkında haberdar edildikleri an söz konusu bilgi veya hizmetleri derhâl kaldırmaz veya erişimi kısıtlamazlarsa içerik veya hizmetten beraber sorumlu tutabilirler.

Bir önceki paragrafta yer alan hizmet sağlayıcıların ulusal hukuktaki sorumluluklarını tanımlarken, bilgiyi evvela erişilebilir kılan kişilerin ifade özgürlüğüne ve kullanıcıların bilgiye tekabül eden haklarına gerekli olan itina gösterilmelidir.

Tüm durumlarda, yukarıdaki sorumluluk kısıtlaması hizmet sağlayıcıların mümkün oldukça bir kanunun ihlalini durdurma veya önlemeleri için aleyhlerine tedbir alınabilmesine halel getirmemelidir.

İlke 7: Anonimlik

Online gözetlemeye karşı koruma sağlamak ve bilgi ve fikirlerin özgürce ifade edilmesini geliştirmek amacıyla, Üye Devletler internet kullanıcılarının kimliklerini ifşa etmemeye yönelik arzularına saygı göstermelidir. Bu durum, Üye Devletlerin iç hukuk, İnsan Hakları ve Temel Özgürlüklerin Korunmasına İlişkin Sözleşme ve yargı ile kolluk alanındaki diğer uluslararası sözleşmeler uyarınca suç niteliğindeki eylemlerin sorumlularını tespit edebilmek için tedbirler almaları ve iş birliği içerisinde olmalarına halel getirmez.

V. Bilgi Toplumunda İnsan Hakları ve Hukukun Üstünlüğü Deklarasyonu (2005)

Bilgi Toplumunda İnsan Hakları ve Hukukun Üstünlüğü Deklarasyonu, Avrupa Konseyi Bakanlar Komitesi tarafından 13 Mayıs 2005 tarihinde kabul edilmiştir.[272] Bu Deklarasyon, Dünya Bilgi Toplumu Zirvesi'nin Tunus Aşaması'na Avrupa Konseyinin görüşü olarak sunulmuştur.

Deklarasyon'un ilk vurgusu, bilgi ve iletişim teknolojilerinin toplumu dönüştürücü etkisi üzerine olmuştur. Üye devletler, bilgi ve iletişim teknolojilerinin, mevcut insan hakları enstrümanlarının aslen geliştiği sosyal, teknolojik ve hukuki ortamı değiştirme potansiyeli taşıdığının farkındadır. Aynı şekilde, üye devletler, bu tür teknolojilerin demokratik süreçlerin ayrılmaz parçası olduğunu, insan haklarının kullanılmasında geniş imkânlar sunabildiğini, AİHS'de güvence altına alınan tüm hakların bilgi çağında da tamamen geçerli olduğunu ve yeni teknolojik gelişmelerden bağımsız olarak korunması gerektiğini vurgulamıştır. Keza, bilgi ve iletişim teknolojilerinin, insan hakları ihlallerinin etkisini de büyük ölçüde artıracağı belirtilmiştir.

Deklarasyon, üye devletlere, bilgi toplumunun geliştirilmesi ve AİHM'nin güncel içtihatlarına uyum sağlanması için mevcut kurallarını ve politikalarını gözden geçirme çağrısı yapmaktadır. Bu çağrıda özel olarak terörle mücadele bağlamında insan hakları standartlarının gözetilmesi gerektiği hatırlatılmaktadır. Ayrıca, tüm süreçlere sivil toplum, özel sektör ve ilgili diğer paydaşların kapsayıcı şekilde katılımının sağlanması için üye devletlere davette bulunulmuştur.

Deklarasyon'un "Bilgi toplumunda insan hakları" ana başlığı altında yer alan bölümler şunlardır:

1. İfade özgürlüğü, bilgi ve iletişim hakkı
2. Özel hayatın gizliliği ve haberleşmenin mahremiyetine saygı hakkı

---

[272] **Avrupa Konseyi**, "*Declaration of the Committee of Ministers on human rights and the rule of law in the Information Society CM(2005)56*", <https://www.coe.int/t/dgap/goodgovernance/Activities/Public_participation_internet_governance/Declaration-Information-Society/011_DeclarationFinal%20text_en.asp>

3. Eğitim hakkı ve yeni bilgi teknolojilerine erişimin teşvik edilmesinin önemi ve bunların ayrımcılık olmaksızın kullanımı
4. Köleliğin ve zorla çalıştırmanın yasaklanması ve insan kaçakçılığının yasaklanması
5. Adil yargılanma hakkı ve kanunsuz ceza olmaz ilkesi
6. Mülkiyetin korunması
7. Serbest seçim hakkı
8. Toplanma özgürlüğü

Deklarasyon'un ilk kısmı bilgi toplumunda insan haklarına ilişkindir. Bu kısma, ifade özgürlüğü, bilgi ve iletişim hakkıyla giriş yapılmakta, bir içeriğe salt dijital formatta olması sebebiyle ayrım yapılmaması gerektiği belirtilmektedir. Bilgi ve iletişim teknolojileri aracılığıyla işlendiği durumlarda da ırkçılık, ırka dayalı ayrımcılık ve çocuk pornografisi gibi hukuka aykırı içeriklerle mücadeleye devam edilmelidir.

Avrupa Konseyi; Siber İçeriğin Öz Düzenlemesine İlişkin Tavsiye Kararı ve İnternette İletişim Özgürlüğüne İlişkin Deklarasyon'da olduğu gibi Bilgi Toplumunda İnsan Hakları ve Hukukun Üstünlüğü Deklarasyonu'nda da öz düzenleme ile ortak düzenleme yöntemlerinin önemini tekrarlamıştır. Deklarasyon'da, hem devlet sansüründen hem de bilgi ve iletişim teknolojileri endüstrisi, internet servis sağlayıcıları, yazılım geliştiricileri, içerik sağlayıcıları ve Uluslararası Ticaret Odası gibi paydaşların yani özel sektörün sansüründen kaçınılması gerektiği belirtilmiştir. Ayrıca, bireylerin içeriklere erişiminin yaygınlaştırılması gerektiği de hatırlatılmıştır.

Deklarasyon'un ilk kısmında ele alınan bir diğer konu ise kişisel verilerin korunmasıdır. Deklarasyon'a göre, bilgi ve iletişim teknolojileri aracılığıyla kişisel verilerin büyük ölçekte işlenmesine olanak tanınması, özel hayat ile haberleşmenin mahremiyetine ciddi etkilerde bulunmuştur. Bu alandaki etkileri sınırlamak için Deklarasyon, çözüm olarak mahremiyet artırıcı teknolojilerin (PETs - Privacy Enhancing Technologies) yaygınlaştırılmasını önermektedir. Her türlü bilgi ve iletişim teknolojisi özel hayatın gizliliğine ve haberleşmenin mahremiyetine saygı göstermelidir.

Deklarasyon'un ilk kısmının üçüncü alt başlığı eğitime ayrılmıştır. Deklarasyon, elektronik öğrenme yöntemlerinin, eğitim marifetiyle ve dünya genelinde insanların bilgi düzeyini artırarak demokratik vatandaşlığa katkı sağladığını belirtmiştir. Ayrıca, "*bilgisayar okuryazarlığı*" alanındaki dışlayıcılığın oluşturacağı risklere de işaret edilmiştir. Deklarasyon'a göre, tüm bilgi ve iletişim teknolojilerinin çoğulculuk, kültürel ve dilsel çeşitlilik ve farklı haberleşme mecralarına ayrımcılık yapılmaksızın erişim bağlamında geliştirilmesi gerekmektedir. Özellikle zararlı içeriği değerlendirebilmeleri için çocukların bilgisayar okuryazarlığına önem verilmelidir.

Deklarasyon'un ilk kısmının dördüncü alt başlığı, köleliğin ve zorla çalıştırmanın yasaklanması ile insan kaçakçılığının yasaklanmasına ilişkindir. Bilgi ve iletişim teknolojilerinin kullanımının insan kaçakçılığı olanaklarını artırdığını ve bu uygulamanın yeni sanal formunu oluşturduğunu belirten Deklarasyon, dijital ortamdaki bu tür faaliyetlerin AİHS'nin 4. maddesiyle yasaklanan gerçek hayattaki faaliyetlerle eş değer tutulması gerektiğini ifade etmiştir. Ayrıca, üye devletler, bu tür bilgi ve iletişim teknolojileri destekli insan kaçakçılığı ile mücadele için hukuki düzenlemeler yapmaya ve pratik önlemler almaya davet edilmiştir.

Deklarasyon'da ele alınan bir diğer konu ise adil yargılanma hakkı ve kanunsuz ceza olmaz ilkesidir. Deklarasyon'un ilk kısmının beşinci alt bölümünde, bilgi ve iletişim teknolojilerinin yargılamalara ilişkin şeffaflığı artırdığı ve daha iyi bir kamu denetimine imkân tanıdığı belirtilmiştir. Ancak, bu şeffaflığın, yargılama öncesi dönemde özellikle adil yargılanma hakkına olumsuz etkileri olabileceğine de işaret edilmiştir. Avrupa Konseyi, adil yargılanma hakkı ile kanunsuz ceza olmaz ilkesinin gerçek hayatta nasıl korunuyorsa dijital ortamda da aynı şekilde korunması gerektiğini belirtmiştir. Ayrıca, medya ve bilgi hizmet sağlayıcılarına ilişkin davranış kuralları geliştirilmesi çağrısı da yapılmıştır.

Bilgi ve iletişim teknolojilerinin dönüştürdüğü ve en çok etkilediği alanların başında fikrî mülkiyet hakları gelmektedir. Teknolojideki değişim hızı, ihlalin boyutunun artması, uluslararası suçla mücadeledeki güçlükler bu alanın en kronik sorunlarıdır. Avrupa Konseyi Siber Suçlar

Sözleşmesi'ne de atıfta bulunan Deklarasyon, birinci kısmın altıncı alt bölümünde, üye devletlerin bu konuda daha aktif iş birliği içerisinde olması gerektiğini belirtmiştir.

Deklarasyon'da ele alınan bir diğer konu, elektronik oylama konusudur. Deklarasyon'un "Serbest seçim hakkı" başlıklı yedinci alt bölümünde, elektronik oylamaların demokratik seçimlere ve referandumlara ilişkin kurallara uyumlu ve elektronik yöntemlerin kullanılmadığı klasik seçimler ve referandumlar kadar güvenli ve güvenilir olması gerektiği hatırlatılmıştır. Ayrıca, Avrupa Konseyinin elektronik oylamanın hukuki, işlevsel ve teknik standartlarıyla ilgili 2004 yılında yayımlamış olduğu kapsamlı tavsiye kararındaki hususların da gözetilmesi gerektiği belirtilmiştir.[273]

Deklarasyon'un birinci kısmının sekizinci ve son bölümü toplanma özgürlüğüne ayrılmıştır. Deklarasyon, üye devletlere, bilgi ve iletişim teknolojileri destekli toplanmalara yönelik gerekli hukuki güvenceyi sağlamaları ve dijital ortamdaki toplantı ve bir araya gelmelere ilişkin takip ve gözetimler yapmamaları çağrısında bulunmuştur. Bu konudaki istisnaların AİHS'nin 11. maddesinin ikinci fıkrasında yer alan ilkelere uygun olması gerektiği hatırlatılmıştır.

Deklarasyon, çoklu paydaş katılım modelini temel dijital yönetişim modeli olarak benimsemiştir. Katılımcılık öne çıkarılmaktadır. Aynı doğrultuda, öz düzenleyici ve ortak düzenleyici önlemlerde, özel hayat ile haberleşmenin mahremiyetine saygı gösterilmeli, kişisel verilerin işlenmesinde özel hayata saygı hakkı gözetilmelidir.

Özel sektör, bilhassa trafik verisinin toplanması, işlenmesi ve takibi, e-posta ve diğer elektronik haberleşme türleriyle özel haberleşmenin takibi, iş yerlerinde mahremiyete saygı, kamera kullanımı, biyometrik tanımlama, istenmeyen ileti dâhil zararlı uygulamalar, genetik verinin toplanması, kullanımı ve genetik test konularına dikkat etmelidir. Özel

---

[273] **Avrupa Konseyi**, "*Committee of Ministers' Recommendation Rec(2004)11 on legal, operational and technical standards for e-voting*", <https://www.coe.int/t/dgap/goodgovernance/Activities/Key-Texts/Recommendations/Rec(2004)11_Eng_Evoting_and_Expl_Memo_en.pdf>

sektör ayrıca internet ortamı gibi dijital ortamlarda nefret söylemi, ırkçılık ve yabancı düşmanlığı ile şiddete davete internet hizmet sağlayıcıları tarafından özel sansür (gizli sansür) uygulanması, hukuka aykırı ve zararlı içerik arasında ayrım yapılması konularında etkin olmalıdır. Bunlara ilaveten, özel sektörden çocuk pornografisinin sanal dağıtımı ve insan kaçakçılığı konularına ilişkin mücadeleye de katılmaları talep edilmektedir.

VI. Yeni Bilgi ve İletişim Ortamında Çocukların Güçlendirilmesi Tavsiye Kararı (2006)

Yeni Bilgi ve İletişim Ortamında Çocukların Güçlendirilmesi Tavsiye Kararı, Avrupa Konseyi Bakanlar Komitesinin 27 Eylül 2006 tarihli 974. Toplantısı'nda kabul edilmiştir.[274] Temel amaç, bilgi ve iletişim teknolojileri karşısında çocukların daha etkin korunmasının sağlanmasıdır. Özellikle, her zaman hukuka aykırı olarak nitelendirilemese de çocukların fiziksel, duygusal ve psikolojik gelişimlerini olumsuz etkileyecek online pornografi, şiddet ve kendine zararın tasviri ve yüceltilmesi, alçaltıcı, ayrımcı veya ırkçı ifadeler veya bu tür davranışları haklı gösterme, çocukları istismara hazırlama, zorbalık, takip ve diğer taciz türlerinin oluşturduğu zarar riski bu yönde bir karar alınmasını gerektirmiştir.

Tavsiye Kararı'nın temel noktası, çocukların bilişim okuryazarlığını artırmak, çocukları bilinçlendirmek ve bunu Avrupa Konseyine üye devletlerin eğitim müfredatlarının bir parçası hâline getirmektir. Bu doğrultuda, üye devletler, çocukların bilgi ve iletişim teknolojileri karşısında güçlendirilmesi için pedagojik içerikler ve öğrenme araçları oluşturmaya, araştırma programları geliştirmeye davet edilmektedir.

Tavsiye Kararı, tüm bu sürecin çoklu paydaş katılım modeliyle sürdürülmesini önermekte ve bu konuda kamu ile özel sektörün iş birliğinin gerektiğini belirtmektedir. Sivil topluma bu yönde denetleyici bir rol verilmelidir.

---

[274] **Avrupa Konseyi**, "*Recommendation Rec(2006)12 of the Committee of Ministers to member states on empowering children in the new information and communications environment*", <https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805af669>

VII. Yeni Bilgi ve İletişim Ortamında İfade ve Bilgi Özgürlüğünün Geliştirilmesine İlişkin Tavsiye Kararı (2007)

Yeni Bilgi ve İletişim Ortamında İfade ve Bilgi Özgürlüğünün Geliştirilmesine İlişkin Tavsiye Kararı, Avrupa Konseyi Bakanlar Komitesinin 26 Eylül 2007 tarihli 1005. Toplantısı'nda kabul edilmiştir.[275] Tavsiye Kararı'nın önemi, internete erişim ile kamu hayatına ve demokratik süreçlere katılım arasında kurduğu doğrudan bağlantıdan ileri gelmektedir.

Tavsiye Kararı, bilgi ve iletişim teknolojilerinin ve servislerinin, insan hakları ile temel hakların kullanılmasında hem pozitif hem de negatif potansiyel etkilerinin olduğu vurgusuyla başlamaktadır. Bir diğer önemli vurgu, temel hak ve hürriyetlerin kullanımı ve icrasında sadece devletlerin değil devlet dışı aktörlerin, özellikle özel sektörün önemli bir rolü olduğuna ilişkindir.

Avrupa Konseyi, yeni bilgi ve iletişim ortamında ifade ve bilgi özgürlüğünün geliştirilmesi için bireysel kullanıcıların güçlendirilmesi, güvenilir bilgi, esnek içerik oluşturma ve bilgi sürecinde şeffaflığın sağlanması için ortak standartlar ve stratejiler geliştirilmesi, bilgi teknolojileri altyapılarına makul şekilde erişim, bir kamu hizmeti olarak bilgiye erişim ve paydaşlar arasında iş birliği bağlamında üye devletleri eyleme geçmeye çağırmaktadır.

VIII. İnternetin Kamu Hizmeti Boyutunun Geliştirilmesine Yönelik Önlemlere İlişkin Tavsiye Kararı (2007)

İnternetin Kamu Hizmeti Boyutunun Geliştirilmesine Yönelik Önlemlere İlişkin Tavsiye Kararı, Avrupa Konseyi Bakanlar Komitesinin

[275] **Avrupa Konseyi**, "*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*", <https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805d4d0e>

7 Kasım 2007 tarihli 1010. Toplantısı'nda kabul edilmiştir.[276] Karar'da, önceki kararlarda olduğu gibi, bilgi ve iletişim teknolojilerinin bir yandan ifade özgürlüğü, bilgi ve iletişim hürriyeti, eğitim hakkı, toplanma hürriyeti, demokratik seçimlere ilişkin haklar gibi insan haklarının ve temel özgürlüklerin kullanılmasını esaslı şekilde kolaylaştıracağına vurgu yapılmıştır. Diğer yandan bu tür teknolojilerin özel yaşamın gizliliği, haberleşmenin mahremiyeti, insan onuru ve hatta yaşam hakkı gibi hak, özgürlük ve değerleri olumsuz etkileyebileceğine işaret edilmiştir.

Ayrıca, hayatın farklı alanlarında kullanılması sebebiyle internetin erişilebilir, makul ücretli, güvenli, güvenilir ve işler olmasına yönelik meşru bir beklentinin oluştuğu vurgulanmış; insan hakları ve demokrasi, erişim, açıklık, çeşitlilik ve güvenlik bağlamında Avrupa Konseyinin paydaş katılımını önceleyen politikalar geliştirmesine yönelik çağrı yapılmıştır.

IX. İnternet Filtreleri Bağlamında İfade ve Bilgi Özgürlüğüne Saygının Teşvik Edilmesine Yönelik Tedbirleri İçeren Tavsiye Kararı (2008)

İnternet Filtreleri Bağlamında İfade ve Bilgi Özgürlüğüne Saygının Teşvik Edilmesine Yönelik Tedbirleri İçeren Tavsiye Kararı, Avrupa Konseyi Bakanlar Komitesinin 26 Mart 2008 tarihli 1022. Toplantısı'nda kabul edilmiştir.[277] İnternet içeriğinin filtrelenmesi, hem hukuka aykırı hem de zararlı içerikle mücadele için yaygın olarak kullanılan bir yöntemdir. Avrupa Konseyinin internet filtrelerine yönelik Tavsiye Kararı bu konudaki temel sorunlara değinmekte, filtrelerin nasıl geliştirilip kullanılması gerektiği ve bir filtreleme uygulamasının hukukiliğine ilişkin idari ve yargısal etkin koruma mekanizmaları konularında yol göstermektedir.

---

[276] **Avrupa Konseyi**, *"Recommendation CM/Rec(2007)16 of the Committee of Ministers to member states on measures to promote the public service value of the Internet"*, <https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805d4a39>

[277] **Avrupa Konseyi**, *"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"*, <https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805d3bc4>

Tavsiye Kararı, üç ana bölümden oluşmaktadır:

1. İfade özgürlüğü ve bilgiye erişim hakkından tam olarak yararlanabilmek için internet filtrelerini kullanmak ve kontrol etmek
2. Çocuklar ve gençler için uygun filtreleme
3. Kamu sektörü ve özel sektör tarafından internet filtrelerinin kullanımı ve uygulanması

Tavsiye Kararı'nda ilk olarak internet filtrelerinin kullanımı ve kullanıcıların bu tür filtreleri kontrolleri ele alınmıştır. Karar'a göre, kullanıcılar uygun düştüğü ölçüde filtrelemeden haberdar edilmeli ve kullanıcılara bir içeriğe ilişkin filtreleme veya engelleme kararına itiraz etme, açıklama isteme ve sorunu giderme hakkı tanınmalıdır. İçerik engellemelerinde, içeriğin hangi sebeple engellendiği ve güncel bir iletişim kanalıyla bu engellemeye nasıl itiraz edileceği belirtilmelidir.

Tavsiye Kararı'nda değinilen bir diğer husus ise internet kullanıcılarının filtrelere, bunların nasıl kullanıldıklarına ve kapsamlarına ilişkin bilgilendirilmeleridir. Tavsiye Kararı, üye devletlere, filtreleme alanında minimum standartları geliştirme, kullanım amaçlarına göre filtrelerin etkinliklerini, ölçülülüklerini düzenli olarak gözden geçirme ve filtreleri güncelleme çağrısında bulunmaktadır.

Tavsiye Kararı, tüm bunların yanında, filtreleme teknolojisi geliştiricilerinin sosyal ve etik sorumluluklarına, bu tür teknolojilerin kullanımına yönelik eğitim, iş birliği, karşılıklı veri paylaşımı gibi konulara ve sivil toplumun filtrelemelerin potansiyel avantajları ve muhtemel tehlikeleri ile ilgili farkındalığın artırılmasındaki rolüne de değinmiştir.

Tavsiye Kararı'nda ele alınan bir diğer konu ise çocuklar ve gençler için uygun filtreleme teknolojilerinin kullanımıdır. Bu alandaki düzenlemeleri meşru kabul eden Avrupa Konseyi, aşırı korumacılığın risklerine işaret ederek ihtiyaç duyulan araştırma ve geliştirme süreçlerine destek verilmesi gerektiğini belirtmiştir.

Ayrıca Karar'da şu gibi konulara da özel olarak vurgu yapılmıştır: Ebeveynlere ve eğitimcilere gelişme çağına uygun filtrelerin seçimi ve

kullanımı konusunda destek veren inisiyatiflerin geliştirilmesi; çocuklar ve gençlerin internetin faydaları ve tehlikeleri hakkında bilgilendirilmesi; gelişme çağına uygun akıllı filtrelerin geliştirilmesi için özel sektörün teşvik edilmesi; öz düzenleme ve ortak düzenleme yapılarıyla iş birliğinin artırılması; bilinçli seçim yapılması için ortak filtreleme etiketlerinin geliştirilmesi ve içerik sağlayıcılarının öz sınıflandırmalarının birlikte çalışabilirliğinin sağlanması.

Tavsiye Kararı'nda yer alan son bir konu ise internet filtrelerinin kamu sektörü ve özel sektör tarafından kullanımı ve uygulanmasıdır. Tavsiye Kararı'na göre üye devletler:

1. Kamu otoriteleri tarafından işletilen elektronik haberleşme ağlarında internet içeriğini AİHS'nin 10. maddesinin ikinci fıkrasında belirtilen sebepler dışında filtrelemekten kaçınmalıdır.

2. Ülke çapında genel engelleme veya filtreleme tedbirlerinin sadece AİHS'nin 10. maddesinin ikinci fıkrasındaki şartların varlığı durumunda uygulamaya alınmasını temin etmelidir. Şayet bu yönde bir karar alınacaksa filtreleme gerekçesi belirli ve açıkça tanımlanabilir içeriğe yönelik olmalı, yetkili bir ulusal makam hukuka aykırılığa karar vermiş olmalı ve AİHS'nin 6. maddesindeki gerekliliklere uygun olarak bağımsız ve tarafsız bir yargı makamı veya düzenleyici makam tarafından kararın gözden geçirilmesi mümkün olmalıdır.

3. Uygun ve gerekli olduğu durumlarda ulusal mevzuata vatandaşların hukuka uygun içeriğe erişimini kısıtlamak amacıyla filtrelerin kasten kötüye kullanılmasını önleyecek hükümler getirmelidir.

4. Filtrelerin makul olmayan düzeyde içerik engellemesini önlemek ve filtrelemenin etkilerinin engellemenin maksadıyla uyumlu ve demokratik toplum gerekliliklerine göre ölçülü olmasını temin etmek amacıyla uygulanmadan önce ve uygulama sırasında değerlendirilmesini sağlamalıdır.

5. İçerik kullanıcıları ve/veya sahipleri içeriğin haklı olmayan bir gerekçeyle engellendiğini iddia ederlerse filtrelemenin askıya alınması dâhil etkili ve hemen erişilebilir denetim ve çözüm imkânları sağlamalıdır.

6. Bir filtrenin korumayı amaçladığı grupta yer almayan kullanıcıları da kapsayacak şekilde, saldırgan veya zararlı içeriğe yönelik evrensel ve genel engellemeden kaçınmalıdır. Ayrıca, araştırma amaçları gibi meşru menfaatin ortaya konulabildiği özel ve istisnai durumlarda hukuka aykırı içeriğin gösterilmesini sağlamalıdır.

7. Filtreler kullanılırken ve uygulanırken özel yaşam hakkı ile haberleşmenin mahremiyetine saygı gösterilmesini; filtreler aracılığıyla kaydedilen, muhafaza edilen ve işlenen kişisel verilerin sadece meşru ve ticari olmayan amaçlarla kullanılmasını temin etmelidir.

Tavsiye Kararı, devlet ve özel sektör oyuncuları eliyle yürütülen filtrelerin geliştirilmesi ve uygulanması süreçlerinin sivil toplumca takip edilmesi gerektiği hatırlatmasıyla sonlanmaktadır.

X. İnternet Ortamında Çocukların İtibar, Güvenlik ve Mahremiyetlerinin Korunmasına İlişkin Deklarasyon (2008)

İnternet Ortamında Çocukların İtibar, Güvenlik ve Mahremiyetlerinin Korunmasına İlişkin Deklarasyon, Avrupa Konseyi Bakanlar Komitesinin 20 Şubat 2008 tarihli 1018. Toplantısı'nda kabul edilmiştir.[278] Kısa ve temel bir metin olan bu Deklarasyon'da, öncelikle ifade özgürlüğünün ve bilgiye erişim hakkının herhangi bir kamusal kısıtlamaya veya sınıra tabi olmaksızın kullanılması gerektiği hatırlatılmıştır. Aynı doğrultuda, Birleşmiş Milletlerin 20 Kasım 1989 tarihli Çocuk Hakları Sözleşmesi'ne atıf yapılmış ve Avrupa Konseyine üye tüm devletlerin çocukların haklarının korunmasına yönelik sorumluluğu olduğu belirtilmiştir.

[278] **Avrupa Konseyi**, "*Declaration of the Committee of Ministers on protecting the dignity, security and privacy of children on the Internet*", <https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805d3d2d>

Deklarasyon, internetin çocukların haberleşme, bilgi, bilim, eğitim, eğlence gibi günlük aktiviteleri için önemli bir araç olduğunu belirtmiştir. Çocukların oluşturdukları içeriğin hem şu an hem de yetişkin oldukları dönemde onların güvenlik, mahremiyet ve itibarlarına zarar verebileceğine işaret edilmiştir. Yukarıda ele alınan İnternette İletişim Özgürlüğüne İlişkin Deklarasyon'a atıf yapılarak, internette iletişim özgürlüğünün özellikle çocukların haklarına halel getirmemesi gerektiği tekrarlanmıştır.

Deklarasyon'a göre, çocukların internet ortamındaki faaliyetlerinin takip edilmesinin onları cinsel istismar, ayrımcılık, zorbalık ve diğer tür tacizler gibi suç sayılan eylemlere maruz bırakma riski vardır. Tüm bu tespitlerin ışığında Deklarasyon, çocukların dijital okuryazarlıklarının geliştirilmesi ihtiyacına vurgu yapmaktadır.

Yeni teknolojilerin AİHS'nin 8. maddesinde güvence altına alınan özel yaşama saygı ve haberleşmenin gizliliği hakkıyla uyumlu olması gerektiğinin altını çizen Deklarasyon, çocukların bilgilerinin profilleme amaçlı kullanımı ve kişisel verilerinin ticari saiklerle saklanmasının ortaya çıkardığı endişeleri belirtmiştir. Bu konuda Birleşmiş Milletler İnternet Yönetişim Forumu kapsamında ele alınan çocukların ve gençlerin korunmasına ilişkin tartışmaları da tekrarlamıştır.

Tüm bu hatırlatmalardan sonra Deklarasyon, bir suç soruşturması hariç, çocuklar tarafından internette oluşturulan ve onların itibar, güvenlik ve mahremiyetlerini zedeleyebilecek, şimdi veya hayatlarının ilerleyen aşamalarında kendilerini saldırıya açık hâle getirebilecek içeriğin kalıcı ve süresiz şekilde erişilebilir olmaması gerektiğini belirtmiştir. Bu bağlamda, Avrupa Konseyi üyesi devletler, tüm paydaşları da dâhil ederek bu tür içeriklerin ve izlerinin (log, kayıtlar ve işlemelerin) makul bir süre içerisinde kaldırılması veya silinmesine ilişkin birlikte çalışmaya davet edilmiştir.

XI. Çocukları Zararlı İçeriğe ve Davranışlara Karşı Koruma ve Çocukların Yeni Bilgi ve İletişim Ortamına Aktif Katılımlarını Yaygınlaştırmaya İlişkin Tavsiye Kararı (2009)

Avrupa Konseyi Bakanlar Komitesi, 8 Temmuz 2009 tarihli 1063. Toplantısı'nda Çocukları Zararlı İçeriğe ve Davranışlara Karşı Koruma ve Çocukların Yeni Bilgi ve İletişim Ortamına Aktif Katılımlarını Yaygınlaştırmaya İlişkin Tavsiye Kararı'nı almıştır.[279]

Tavsiye Kararı'nda, bilgi ve haberleşme ortamlarında küçükleri zararlı içeriklerden korumak ve çocukların medya okuryazarlık becerilerini artırmak suretiyle ifade özgürlüğünü ve insan onurunu korumanın Avrupa Konseyinin bir önceliği olduğu belirtilmiştir. Bu vurgudan sonra, çocukların fiziksel, duygusal ve psikolojik gelişimlerini etkileyecek online pornografi, şiddet ve kendine zararın tasviri ve yüceltilmesi, alçaltıcı, ayrımcı veya ırkçı ifadeler yahut bu tür davranışları haklı gösterme, çocukları istismara hazırlama, zorbalık, takip ve diğer taciz türlerinin oluşturduğu risklere işaret edilmiştir.

Bu konudaki diğer Avrupa Konseyi kararlarını hatırlatan Tavsiye Kararı, çocukların temel bilgi, beceri, davranış ve insan hakları değerlerinin geliştirilmesine yönelik ihtiyaca değinmiştir. Aynı doğrultuda, internet ortamına olan güvenin ve güvenilirliğin artırılması ihtiyacına işaret edilerek, içeriklerin tarafsız bir şekilde etiketlenmesiyle hem çocukların hem de yetişkinlerin internet içeriğine ilişkin kendi öz değerlendirmelerini yapmalarının mümkün olacağı belirtilmiştir.

Üye devletlerden, özel sektör ve sivil toplum iş birliğiyle şu adımları atmaları beklenmektedir:

---

[279] **Avrupa Konseyi**, *"Recommendation CM/Rec(2009)5 of the Committee of Ministers to member states on measures to protect children against harmful content and behaviour and to promote their active participation in the new information and communications environment"*, <https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805d0b0f>

- Güvenli alanlar (duvarlı bahçeler) ile çocuklar için uygun web sitelerine ve internet içeriğine erişimi kolaylaştıran diğer araçların geliştirilmesi ve kullanılması teşvik edilmelidir.
- Etiketler ve güven damgalarının geliştirilmesi ve gönüllü kullanımı teşvik edilmelidir; böylece, ebeveynlerin ve çocukların, risk taşıyan içerikle zararsız içerik arasında ayrım yapması mümkün olacaktır.
- Çocuklar, ebeveynler ve eğitimcilerin zarar verme riski taşıyan içerikleri ve davranışları daha iyi anlama ve bunlarla baş edebilme becerileri geliştirilmelidir.

Tavsiye Kararı'nın ekinde ayrıca çocukların internet ortamında korunmasına ilişkin bir Rehber yer almaktadır. Rehber'de üç ana konu ele alınmıştır:

I. Çocuklara internet ortamında güvenli ve güvenlikli alanlar sağlanması
II. Avrupa güven damgası ve etiketleme sisteminin geliştirilmesinin teşviki
III. Çocuklar, ebeveynler ve eğitimciler için internet becerileri ve okuryazarlığının geliştirilmesi

Rehber'de, çocukların korunması için dahi olsa internet içeriğinin kısıtlanmasına yönelik her girişimin, ifade özgürlüğünün korunmasına ilişkin sorunlar ortaya çıkardığı belirtilmiştir. Üye devletlerin, bu sorunu göz önünde tutarak özel sektör, medya, sivil toplum iş birliğiyle çocuklar için güvenli ve güvenlikli alanlar oluşturmaları gerekmektedir.

Rehber, otomatik içerik oylama ve filtreleme sistemleri dışında, online içeriği gönüllülük esasına göre etiketleyen ve içerik üreticileri tarafından yapılan Internet Content Rating Association ve PEGI Online gibi girişimlerin varlığına işaret etmiştir. Rehber'e göre, online içeriğin etiketlenmesi, çocuklar için güvenli ve güvenlikli alanlar geliştirilmesine katkı sunmaktadır. Ancak, bu tür etiketleme inisiyatiflerinin etkinliği ve güvenilirliği bu sistemlerden sorumlu olanların hesap verebilirliklerine ve sistemlerin birlikte çalışabilmesine bağlıdır.

Rehber, işaretlenmemiş bir içeriğin doğrudan tehlikeli veya çocuklar, ebeveynler ve eğitimciler için daha az değerli olarak nitelendirilmemesi gerektiğini belirtmiş ve demokratik katılımı da dikkate alarak şu önerilerde bulunmuştur:

- Dijital içeriğin etiketlenmesi için Avrupa özelinde güven damgası oluşturmak;
- İnsan hakları ilkeleri ve standartlarına bağlılığı sağlamak, özellikle de kullanıcılar ve/veya müellifler/yazarlar tarafından yanlış etiketlenme yapıldığı iddiası durumunda kararın tekrar gözden geçirilmesini temin etmek;
- Etiketleme sistemlerinin hem müellifler/yazarlar hem de kullanıcılar tarafından gönüllülük esasına göre sağlanması ve kullanılması;
- İçeriğe ilişkin her türlü sansürden kaçınmak;
- Medya ve medya benzeri online içerik hizmetlerinin editoryal bağımsızlığına saygı göstermek;
- Etiketlenen içeriği düzenli olarak gözden geçirmek, örneğin etiketin maksimum geçerlilik süresini belirlemek;
- Etiket sistemlerinin birlikte çalışabilirliğine yönelik girişimleri teşvik etmek, özel bir Avrupa logosu geliştirmek ve bu kapsamda farklı yaş grupları için içeriğin uygunluğunu belirtmek;
- Üye devletlerin farklı geleneklerini de dikkate alarak içeriğin yaşa uygun derecelendirilmesi için ilkeler geliştirmek;
- Araştırma ve geliştirmeyi teşvik etmek, özellikle de içeriğin üst verisiyle etiketlenmesini temin etmek;
- Ebeveynler ve eğitimcilerin, içerik etiketlemenin çocuklar için internet ortamında güvenli ve güvenlikli alanlara erişimi kolaylaştırdığı konusunda farkındalığını artırmak;
- Etiket sistemlerini ve etkinliklerini, AİHS'nin 10. maddesine uygunluk, bu sistemlerden kaynaklanan hizmetlerin toplumun geneline erişebilirlik ve ekonomiklik bağlamında ölçmek ve değerlendirmek;

- Çocukların farkındalığını artırmak, interneti ve bilgi ve iletişim teknolojilerini özgürce kullanabilmenin fayda ve risklerine ilişkin eleştirel bakış açısı geliştirmelerini sağlamak;
- İnternet ve bilgi ve iletişim teknolojilerini en iyi şekilde kullanmaya yönelik pratik okul müfredatı geliştirmek;
- Çocukları, ebeveynleri ve eğitimcileri internette güvenli ve güvenlikli alanlar ile online içeriklere ilişkin güvenilir etiketlere ilişkin bilgilendirmek;
- Etiketleme sistemleri ve filtreleme mekanizmalarının insan hakları boyutuna, ifade ve bilgi özgürlüğüne ilişkin potansiyel risklerine ilişkin bilgiyi ve pratik anlayışı geliştirmek, diğerlerinin yanı sıra Avrupa Konseyinin bu konudaki standart belirleme enstrümanları ve araçlarına tüm paydaşların dikkatini çekmek.

XII. Ağ Tarafsızlığı Deklarasyonu (2010)

Ağ Tarafsızlığı Deklarasyonu, Avrupa Konseyi Bakanlar Komitesinin 29 Eylül 2010 tarihli 1094. Toplantısı'nda kabul edilmiştir.[280] Deklarasyon, Avrupa Konseyinin AİHS ile güvence altına alınan insan haklarının internet ortamında korunması ve geliştirilmesine ilişkin politik hedefini tekrarlamış ve İnternetin Kamu Hizmeti Boyutunun Geliştirilmesine Yönelik Önlemlere İlişkin Tavsiye Kararı'nı hatırlatmıştır.

Elektronik haberleşme ağları, fikirlerin ve bilgilerin paylaşılması için temel bir araç hâline gelmiştir. Deklarasyon'a göre, kullanıcıların online olarak bilgiye erişim ve bilgiyi yayma hakkı, yeni araçlar ve hizmetler geliştirilmesi; şeffaf olmayan trafik yönetimi, içerik ve hizmetlere yönelik ayrımcılıklar veya cihazların bağlanabilirliğinin engellenmesinden olumsuz etkilenebilecektir. Bu sebeple kullanıcıların, internet temelli içeriğe, uygulamaya veya tercih edecekleri hizmetlere bunların ücretli veya ücretsiz olmasından bağımsız olarak ve istedikleri cihazlarla en geniş

[280] **Avrupa Konseyi**, "*Declaration of the Committee of Ministers on network neutrality 29 September 2010*" <https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805ce58f>

kapsamda erişimleri mümkün olmalıdır. Altyapı veya internete bağlanmak için kullanılan ağdan bağımsız şekilde bu ilke, ağ tarafsızlığı olarak ifade edilmektedir. Avrupa Konseyine göre altyapıya erişim bu hedefin gerçekleştirilmesi için ön koşuldur.

Kullanıcı sayısının, yeni uygulamaların, içeriklerin ve hizmetlerin artması sebebiyle internet trafiğinde üstel artış vardır. Hem mevcut cihazların ağa bağlanma sayısı artmış hem de yeni tip cihazlar ağa bağlanmaya başlamıştır. Deklarasyon'a göre, elektronik haberleşme ağı işletmecileri, internet trafiğini yönetmek zorundadır. Bu yönetim; hizmetin kalitesi, yeni hizmetlerin geliştirilmesi, ağın istikrarının ve dayanıklılığının sağlanması ve siber suçlarla mücadeleyle de ilgilidir.

Deklarasyon, trafik yönetiminin ağ tarafsızlığı ilkesinden ayrılmaya mazeret teşkil etmemesi gerektiğini belirtmiştir. Bu alanda bir istisna getirilecekse üstün bir kamu menfaatinin varlığı ile gerekçelendirilmelidir. Deklarasyon, bu bağlamda AİHS'nin 10. maddesine, AİHM'nin ilgili içtihatlarına, yukarıda incelediğimiz İnternet Filtreleri Bağlamında İfade ve Bilgi Özgürlüğüne Saygının Teşvik Edilmesine Yönelik Tedbirleri İçeren Tavsiye Kararı'na ve Avrupa Birliği'nin elektronik haberleşme alanındaki yasal çerçevesine işaret etmiştir.

Deklarasyon'a göre:

- Kullanıcılar ve hizmet, uygulama veya içerik sağlayıcılar; ağ yönetim tedbirlerinin, temel hak ve özgürlüklerden (özellikle ifade ve bilgi alma özgürlüğü ve özel yaşama saygı hakları) yararlanma üzerindeki etkisini ölçebilmelidir.
- Tedbirler ölçülü, elverişli olmalı ve haksız ayrımcılıktan kaçınmalı; düzenli olarak gözden geçirilmeli ve gerçekten zorunlu olandan daha uzun bir süre devam ettirilmemelidir.
- Kullanıcılar ve hizmet sağlayıcılar; içeriklere, uygulamalara veya hizmetlere erişimlerini esaslı olarak etkileyen herhangi bir ağ yönetim tedbirinden gereğince haberdar edilmelidir.

- Hukukun üstünlüğü gereğince ve usuli güvence olarak bu tür ağ yönetim kararlarına itiraz ve bu kararların gözden geçirilmesi mümkün olmalıdır.

Avrupa Konseyi Bakanlar Komitesi, Deklarasyon'la ağ tarafsızlığı ilkesine bağlılığını beyan etmiş ve bu ilkeye ancak yukarıda belirlenen çerçevede istisnalar getirilmesi gerektiğini vurgulamıştır. Kabul edilebilir yönetim tedbirleri ve minimum hizmet kalitesi gerekliliklerinin daha net ortaya konulması için de Avrupa Konseyinin bir çerçeve çizmesi gerektiği belirtilmiştir.

XIII. İnternet Protokol Adres Kaynaklarının Kamu Yararına Uygun Yönetimine İlişkin Deklarasyon (2010)

İnternet Protokol Adres Kaynaklarının Kamu Yararına Uygun Yönetimine İlişki Deklarasyon, Avrupa Konseyi Bakanlar Komitesinin 29 Eylül 2010 tarihli 1094. Toplantısı'nda kabul edilmiştir.[281] Deklarasyon, temel haklar ile Avrupa Konseyi standartları ve değerlerinin gerçek hayatta uygulandığı gibi online ortamlarda da uygulanmasına vurgu yapmaktadır.

Deklarasyon'a göre, AİHS'nin 8 ve 10. maddelerinde yer alan hak ve özgürlükler, demokratik bir toplumda temel nitelikteki hak ve özgürlüklerdir ve online ortamlarla özellikle yakından bağlantılıdır. İnternet kaynaklarına erişim tüm bu hakların icrası için de hayati önemi haizdir. Daha önceki deklarasyon ve tavsiye kararları gibi, İnternet Protokol Adres Kaynaklarının Kamu Yararına Uygun Yönetimine İlişkin Deklarasyon da internetin kamu hizmeti niteliğinin altını çizmiştir. Keza, internet kaynaklarının kullanımının mahremiyete etkisine değinen Deklarasyon, bu bağlamda Avrupa Konseyinin 108 sayılı Sözleşmesi'nin gerekliliklerine uyumun da dikkate alınması gerektiğini hatırlatmıştır.

---

[281] **Avrupa Konseyi**, "*Declaration of the Committee of Ministers on the management of the Internet protocol address resources in the public interest*", <https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805ce5bd>

Deklarasyon'a göre, İnternet Protokolü Versiyon 4 (IPv4) adresleri kısıtlı kaynaktır ve tükenme aşamasındadır. Bu durum, internetin genişlemesine ve mevcut çalışabilirliğine risk oluşturmaktadır. Bu sebeple, dağıtılmayan veya kullanılmayan IPv4 adreslerinin kamu yararına uygun şekilde yönetilmesi arzu edilmektedir. Hedef, herkesin internet kaynaklarına stabil ve sürekli erişim sağlayabilmesini temin etmektir.

Adreslerin kıtlığı sorunu yeni İnternet Protokol Versiyon 6 (IPv6) ile çözülecektir. Deklarasyon'a göre, herkese etkin ve eşit erişim olanağı sağlayacak bu protokol, katılımcılığa da hizmet edecektir. IPv6 protokolünün geriye doğru IPv4 ile uyumlu olmaması sebebiyle, bu konudaki dönüşümün tüm paydaşların katılımı ve iş birliğiyle gerçekleştirilmesi, yeni protokolün donanım ve yazılım seviyesinde birlikte çalışabilirliğinin sağlanması gerekir.

Tüm bu gerekçelerle Bakanlar Komitesi şunları beyan etmiştir:

- İnternet protokol adresleri ortak kamu kaynağı olarak değerlendirilmeli ve kamu yararına uygun şekilde tahsis edilip yönetilmelidir. Hem mevcut hem de gelecek internet kullanıcılarının ihtiyaçları dikkate alınmalıdır.
- IPv6 protokolünün kamu sektöründe zamanında ve etkili uygulanması temin edilmeli, özel sektörün IPv6 protokolüne hızlı geçiş ve uygulama hazırlıkları teşvik edilmeli ve desteklenmelidir.
- Uygun olduğu ölçüde, internete bağlanan kullanıcılara veya aygıtlara tahsis edilen internet protokol adreslerinin içinde yer alan tanımlama özellikleri kişisel veri olarak kabul edilmeli ve bu şekilde muamele görmelidir.

XIV. Alan Adları ve İsim Dizeleri Bağlamında İfade ve Bilgi Özgürlüğü ile Toplantı ve Örgütlenme Özgürlüğünün Korunmasına İlişkin Deklarasyon (2011)

Alan Adları ve İsim Dizeleri Bağlamında İfade ve Bilgi Özgürlüğü ile Toplantı ve Örgütlenme Özgürlüğünün Korunmasına İlişkin Deklarasyon, Avrupa Konseyi Bakanlar Komitesinin 21 Eylül 2011 tarihli 1121. Toplantısı'nda kabul edilmiştir.[282]

Deklarasyon, ifade ve bilgi özgürlüğü ile toplantı ve örgütlenme özgürlüğünün temel haklar olduğunu ve Avrupa Konseyi üye devletlerinin bu hakları güvence altına almayı taahhüt ettiğini belirtmiştir. İnternetin toplumsal tartışmalar, ifade özgürlüğü ve genel olarak temel hak ve hürriyetlerin kullanılmasına sağladığı önemli katkılara vurgu yapan Deklarasyon, internet içeriğine herhangi bir müdahalede bulunulacaksa AİHS'nin 10. maddesinin ikinci fıkrasındaki koşullara riayet edilmesi gerektiğini belirtmiştir. Deklarasyon, bu bağlamda, bir sınırlama nasıl gerçekleştirilmeli sorusunun yanıtı için 2003 tarihli İnternette İletişim Özgürlüğüne İlişkin Deklarasyon'daki ilkeleri ve Avrupa Konseyi üye devletlerinin sansürden kaçınmalarına ilişkin 2005 tarihli Bilgi Toplumunda İnsan Hakları ve Hukukun Üstünlüğü Deklarasyonu'nu hatırlatmıştır.

Deklarasyon'a göre, alan adları ve isim dizelerinde yer alan ifadelerin, önsel şekilde (*a priori*), ifade özgürlüğü ile bilgi alma ve verme hakkının dışında değerlendirilmemesi gerekmektedir. Nihayetinde, bir alan adı veya isim dizesi ve bunların oluşturdukları ifade türleri, barındırılan içerikle ayrılmaz şekilde iç içe geçmiştir. Deklarasyon, belirli Avrupa Konseyi üye devletlerinin alan adlarının yönetiminde ifade özgürlüğünün korunmasına ilişkin hukuki düzenlemelere yer verdiğini belirtmiştir.

---

[282] **Avrupa Konseyi**, "*Declaration by the Committee of Ministers on the protection of freedom of expression and information and freedom of assembly and association with regard to Internet domain names and name strings*", <https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805b1059>

Deklarasyon, bazı üye devletlerin, alan adlarında veya isim dizelerinde belirli kelime veya karakterleri yasaklamasının risklerine işaret etmiştir. Sınır aşan bağlamda bu durum, diğer devletlerin egemenlik alanlarından erişilen içeriğe ilişkin de sorun teşkil etmektedir. Deklarasyon'a göre internet özgürlüklerine halel gelmemesi için, bu konudaki hassasiyetlerin hem Avrupa Konseyine üye devletler nezdinde hem de ICANN tarafından geliştirilen yeni üst düzey alan adlarında gözetilmesi gerekmektedir.

Tüm bu tartışmalar ışığında Avrupa Konseyi Bakanlar Komitesi:

- Üye devletlerin temel haklara ilişkin güvencelerin alan adlarının yönetimine uygulanması ihtiyacını tanımalarına yönelik desteğini beyan etmiştir.
- Alan adları ve isim dizeleri alanının aşırı düzenlenmesi riskine karşı uyarmış ve tüm düzenlemelerde temel hak ve hürriyetlerin temin edilmesi, düzenlemelerin AİHS'nin 10 ve 11. maddeleri ile AİHM'nin ilgili içtihatlarında yer alan kriterleri gözetmesi gerektiğini belirtmiştir.
- Üye devletlere bu konuda yol göstermek adına standart belirleme çalışmaları yapılacağını taahhüt etmiştir.
- Yetkili Avrupa Konseyi organlarını, alan adlarının yönetimiyle ilgili kurumlar, kuruluşlar ve diğer yapılarla iş birliği içerisinde olmaya, uluslararası hukuk ve uluslararası insan hakları hukukunu gözetmeye davet etmiştir.

XV. İnternet Yönetişimi İlkeleri Deklarasyonu (2011)

İnternet Yönetişimi İlkeleri Deklarasyonu, Avrupa Konseyi Bakanlar Komitesinin 21 Eylül 2011 tarihli 1121. Toplantısı'nda kabul edilmiştir.[283] Deklarasyon, önceki deklarasyonlar ve tavsiye kararlarında olduğu gibi internetin önemine ilişkin bazı tespitlerle başlamaktadır.

[283] **Avrupa Konseyi**, "*Declaration by the Committee of Ministers on Internet governance principles*", <https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cc2f6>

Deklarasyon'a göre internet; özgürlük ve kamu yararına yönelik kolektif girişimler çerçevesinde oluşan, geniş ölçekli fikir, teknoloji, kaynak ve politikanın bir toplamıdır. Devletler, özel sektör, sivil toplum ve bireyler bugünkü dinamik, kapsayıcı ve başarılı internetin gelişimine katkı sunmuştur. İnternet; özgürlük, temel hakların icrası ve kullanılması, katılımcı ve demokratik süreçler ile sosyal ve ticari faaliyetler için alan sağlamaktadır.

Deklarasyon, 2003 tarihli Dünya Bilgi Toplumu Zirvesi ile bu zirvede kabul edilen ajanda kapsamında toplanan 2005 tarihli Dünya Bilgi Toplumu Zirvesi'ndeki internet yönetişimi tanımını tekrarlamıştır: "*İlgili rolleri çerçevesinde hükûmetler, özel sektör ve sivil toplum tarafından, internetin gelişimini ve kullanımını şekillendiren ortak ilkeler, normlar, kurallar, karar alma usulleri ve programların geliştirilmesi ve uygulanmasıdır.*"

Hem ulusal hem de uluslararası seviyede gerçekleşen internet yönetişimi tartışmalarının somut sonuçları olduğunu belirten Deklarasyon, internet topluluklarının, uluslararası kuruluşların ve diğer aktörlerin internetin temel değerlerini ortaya koyan ve internet yönetişiminin çeşitli boyutlarına ilişkin rehberler geliştirdiğini belirtmiştir.

Avrupa Konseyinin de internet yönetişimi tartışmalarından uzak kalmadığını belirten Deklarasyon, Avrupa Konseyi ve üye devletlerin, AİHS'de güvence altına alınan haklarla uyumlu şekilde, *asgari kısıtlama-azami internet hakları* yaklaşımıyla, bireylere haklı olarak bekledikleri güvenlik seviyesini sağlamak için girişimleri olduğuna değinmiştir.

Deklarasyon'a göre, internete sürdürülebilir, insan merkezli ve hak temelli bir yaklaşımı mümkün kılmak için internet yönetişimi ilkelerini hâkim kılmak gerekmektedir. Bu doğrultuda Bakanlar Komitesi, şu ilkelerin hayata geçirilmesini kabul etmiştir:

İnternet Yönetişimi İlkeleri

1. İnsan hakları, demokrasi ve hukukun üstünlüğü

İnternet yönetişimi düzenlemeleri tüm temel hak ve hürriyetlerin korunmasını temin etmeli; bu hak ve hürriyetlerin evrenselliğini, bölün-

mezliğini, bağımsızlığını ve bunların uluslararası insan hakları hukuku bağlamındaki karşılıklı ilişkisini teyit etmeli; demokrasiye ve hukukun üstünlüğüne tam saygıyı temin etmeli ve sürdürülebilir kalkınmayı desteklemelidir. Tüm kamusal ve özel aktörler temel insan haklarını ve özgürlüklerini her türlü faaliyet ve işlemlerinde, bilhassa yeni teknolojiler, hizmetler ve uygulamaları dizayn ederken kabul etmeli ve gözetmelidir. Bu aktörler, temel hak ve özgürlüklerin genişletilmesi gereken durumların ve bilhassa bu tür hak ve özgürlüklere yönelen tehditlerin farkında olmalı, yeni gelişen hakların tanınmasına ilişkin girişimlerin kabul edilmesi süreçlerine tam katılım sağlamalıdır.

2. Çoklu paydaş yönetişimi

İnternet yönetişimi düzenlemelerinin geliştirilmesi ve uygulanması; açık, şeffaf ve hesap verebilir şekilde, hükûmetler, özel sektör, sivil toplum, teknik topluluklar ve kullanıcıların tam katılımını bunların özel rol ve sorumluluklarını da dikkate alarak temin etmelidir. İnternete ilişkin uluslararası kamu politikalarının ve internet yönetişimi düzenlemelerinin geliştirilmesi, tüm ülkelerden tüm paydaşların tam ve eşit katılımına imkân vermelidir.

3. Devletlerin sorumlulukları

Devletlerin internete ilişkin uluslararası kamusal politikalar bakımından hak ve sorumlulukları vardır. Egemenlikten kaynaklı haklarını icra ederken devletler uluslararası hukuku gözetmeli, kendi egemenlik alanları dışındaki kişiler veya varlıklara doğrudan yahut dolaylı zarar verecek herhangi bir eylemden kaçınmalıdır. Ayrıca, temel hakları kısıtlamaya yol açacak herhangi bir ulusal karar veya eylem; uluslararası yükümlülüklere uygun, bilhassa kanuni bir dayanağa sahip, demokratik toplumda gerekli, ölçülülük ve bağımsız denetim/yargı ilkelerine uygun olmalı ve elverişli hukuki ve yargısal süreçlere ilişkin güvenceler içermelidir.

4. İnternet kullanıcılarının güçlendirilmesi

Kullanıcılar, temel hak ve özgürlüklerini kullanmak için güçlendirilmeli, bilgilendirmeye dayalı şekilde karar almalı ve internet yönetişi-

mi düzenlemelerine, bilhassa yönetişim mekanizmalarına ve internete ilişkin kamu politikalarının geliştirilmesine tam bir güven ve özgürlük içerisinde katılmalıdırlar.

5. İnternetin evrenselliği

İnternetle bağlantılı politikalar internetin küresel niteliğini ve evrensel erişim amacını tanımalı, sınır aşan internet trafiğinin engelsiz akışını olumsuz etkilememelidir.

6. İnternetin bütünlüğü

İnternetin güvenliği, kararlılığı, dayanaklılığı, direnci ve bilhassa gelişme olanağı internet yönetişiminin temel ilkesi olmalıdır. İnternet altyapısının bütünlüğünü ve işlerliğini ve özellikle kullanıcıların internete duydukları güven ve inancı korumak için, ulusal ve uluslararası çoklu paydaş iş birliği gereklidir.

7. Merkezî olmayan yönetim

İnternetin günlük yönetiminden sorumluluğun merkezî olmayan niteliği korunmalıdır. İnternetin teknik ve yönetimsel boyutlarından sorumlu olan yapılar ve özel sektör, teknik ve operasyonel konularda öncü rollerini muhafaza ederken kamu politikasına etki eden eylemler bağlamında şeffaflığı, küresel topluluğa karşı hesap verebilirliği sağlamalıdır.

8. Mimari ilkeler

İnternetin açık standartları, birlikte çalışabilirliği ve uçtan uca niteliği muhafaza edilmelidir. Bu ilkeler tüm paydaşlara internet yönetişimine ilişkin kararlarında yol göstermelidir. Yeni kullanıcıların girişine veya meşru internet kullanımına yönelik makul olmayan engeller; teknolojiler ve hizmetler bağlamında yenilikçi potansiyele halel getirebilecek gereksiz külfetler bulunmamalıdır.

9. Açık ağ

Kullanıcılar, tercih ettikleri internet temelli içeriğe, uygulamalara ve hizmetlere, bunlar ücretli veya ücretsiz sunuluyor olsun, kendi seçtikleri

uygun araçlarla mümkün olan en geniş erişime sahip olmalıdır. Temel hak ve özgürlüklerin, bilhassa sınırlara tabi olmaksızın ifade özgürlüğü, bilgi verme ve alma hakkı ile özel yaşama saygı hakkının üzerinde etkisi olan trafik yönetim tedbirleri, bu alandaki ifade özürlüğü, bilgiye erişim hakkı ve özel yaşama saygı hakkına ilişkin uluslararası hukuk gerekliliklerine riayet etmelidir.

10. Kültürel ve dilsel çeşitlilik

Kültürel ve dilsel çeşitliliği muhafaza etmek ve dil ile alfabeden bağımsız olarak yerel içeriğin gelişimini teşvik etmek internet temelli politikaların, uluslararası iş birliğinin ve yeni teknolojiler geliştirmenin temel hedefi olmalıdır.

XVI. Yeni Bir Medya Nosyonuna İlişkin Tavsiye Kararı (2011)

Yeni Bir Medya Nosyonuna İlişkin Tavsiye Kararı, Avrupa Konseyi Bakanlar Komitesinin 21 Eylül 2011 tarihli 1121. Toplantısı'nda kabul edilmiştir.[284] Bu Tavsiye Kararı, Avrupa Konseyinin ifade ve bilgi özgürlüğü ile medya özgürlüğü alanında kriterler belirlemesi ve standartlar geliştirmesine yönelik politik çağrılar uyarınca hazırlanmıştır. Tavsiye Kararı, medya alanındaki tüm Avrupa Konseyi tavsiye kararları ile deklarasyonlarını kronolojik olarak listelemekte, Avrupa Konseyinin tüm bu metinlere ilişkin güncel yorumunu ortaya koymaktadır.

Tavsiye Kararı'nda, dijital medyanın ve yeni aktörlerin medya ekosisteminde gerçekleştirdiği gelişmelerin kademeli ve farklılaştırılmış yeni bir medya nosyonunu gerektirdiği belirtilmiştir. Müstakil bir çalışmayı hak eden bu Tavsiye Kararı'nda internete ilişkin de muhtelif atıflar yer almaktadır.

---

[284] **Avrupa Konseyi**, "*Recommendation CM/Rec(2011)7 of the Committee of Ministers to member states on a new notion of media*", <https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cc2c0>

Tavsiye Kararı, bilgi ve iletişim teknolojilerindeki gelişmelerin medya ekosisteminde önemli değişikliklere yol açtığının, bu gelişmelerin yeni aktörleri ortaya çıkardığının altını çizmiştir. Tavsiye Kararı'na göre teknoloji, doğrusal olmayan (*non-linear*) veya talep üzerine (*on-demand*) içerik teslimini, koşullu erişimi, elektronik olarak teslim edilen içeriğin ayrıştırılmasını, içeriğin kişiselleştirilmesini veya tek noktaya iletilmesini mümkün kılarak medya kavramına ve kitle iletişimine yeni bir boyut getirmiştir.

Tavsiye Kararı'nın en önemli çıktısı, internet aracılığıyla yürütülen faaliyetlerin medya faaliyetleriyle kesiştiği noktalarda onları da kapsama alarak medyanın tanımını yeni medya nosyonu altında alabildiğine genişletmesidir. Medyanın teknolojiyle etkileşimi yeni medya nosyonu olarak kavramsallaştırılmıştır.

XVII. İnternetin Evrenselliğini, Bütünlüğünü ve Açıklığını Koruma ve Geliştirmeye İlişkin Tavsiye Kararı (2011)

İnternetin Evrenselliğini, Bütünlüğünü ve Açıklığını Koruma ve Geliştirmeye İlişkin Tavsiye Kararı, Avrupa Konseyinin 21 Eylül 2011 tarihli 1121. Toplantısı'nda kabul edilmiştir.[285] Tavsiye Kararı, Avrupa Konseyinin internete yaklaşımını yansıtan önceki deklarasyon ve tavsiye kararlarının genel bir tekrarı niteliğindedir. Bu Tavsiye Kararı'nın vurgusu, Avrupa Konseyi üyelerinin insan hakları ve genel olarak temel hak ve hürriyetlerin korunmasını internet politikalarının ana unsuru hâline getirmeleri üzerindedir.

İnternete erişim ve internetin kullanımı; teknik hatlar ve ağa müdahale niteliğindeki diğer eylemlerin doğurduğu zafiyetler sebebiyle ağın stabil ve çalışır hâlde olmasının bozulması riskiyle karşı karşıyadır. Tavsiye Kararı'na göre, internetin stabil hâlde olması ve dayanıklılığı, sınır

[285] **Avrupa Konseyi**, "*Recommendation CM/Rec(2011)8 of the Committee of Ministers to member states on the protection and promotion of the universality, integrity and openness of the Internet*", <https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cc2f8>

aşan ara bağlantı ve altyapının karşılıklı bağımlılığı ve bilhassa da merkezî olmayan ve dağıtık yapısıyla doğrudan bağlantılıdır. Öyle ki bir ülkede yapılan bir müdahale, başka bir ülkedeki kullanıcıların internet üzerinden bilgiye erişimini etkileyebilmektedir. Keza, alan adları ve protokol adresleri gibi teknik alandaki düzenlemelerin de kullanıcıların bilgiye erişimine ve kişisel verilerin korunmasına etkisi vardır.

Tavsiye Kararı'na göre, internet günlük faaliyetler için çok farklı amaçlarla kullanılmaktadır. İnternet hizmetlerinin erişilebilir, makul fiyatlı, güvenli, güvenilir ve işler olmasında bireylerin haklı beklentileri vardır. Bu beklentiler, devletlere internete ilişkin politikalar geliştirirken genel kamusal yararı dikkatlice gözetme sorumluluğu yüklemektedir. Aynı doğrultuda devletlerin, internetin kamu hizmeti değerini korumak ve geliştirmek için en iyi çabanın gösterilmesine yönelik karşılıklı beklentileri vardır.

Tüm bu tespitler ışığında Bakanlar Komitesi, müteakip ilkeleri kabul etmiştir:

İnternetin evrenselliğini, bütünlüğünü ve açıklığını koruma ve geliştirmeye yönelik taahhütler

1. Genel ilkeler

1.1. Zarar vermeme

1.1.1. Devletler, uluslararası insan hakları hukukunda ve uluslararası hukukta kabul edilen standartlara ve ilkelere uygun şekilde, eylemlerinin internete erişim ve internetin kullanımına sınır aşan olumsuz bir etkide bulunmamasını temin etmekle yükümlüdür.

1.1.2. Bu yükümlülük, bilhassa devletlerin kendi egemenlik alanlarındaki eylemlerinin gayrimeşru şekilde kendi sınırları dışındaki içeriğe erişime müdahale veya internet trafiğinin sınır aşan akışına olumsuz etki oluşturmamasını içermektedir.

1.2. İş birliği

Devletler, internete ilişkin kamusal politikaların geliştirilmesi ve uygulanması aşamalarında, internete erişim ve internetin kullanımına sınır aşan olumsuz etkiyi önlemek amacıyla birbirleriyle ve ilgili diğer paydaşlarla iyi niyet çerçevesinde iş birliğinde bulunmalıdır.

1.3. Özen yükümlülüğü

Günlük teknik ve operasyonel konulara dâhil olmamaya ilişkin sınırlar çerçevesinde devletler, internet altyapısındaki sınır aşan esaslı aksaklıklara ve müdahalelere yanıt vermek, bunları önlemek, yönetmek veya herhangi bir durumda bu tür olaylardan kaynaklanan sonuçları ve riskleri minimize etmek için tüm önlemlerin alınması maksadıyla birbirleriyle ve ilgili tüm paydaşlarla iş birliği içerisinde olmalıdır.

2. İnternetin bütünlüğü

2.1. Hazırlıklı olma

2.1.1. Devletler, müştereken ve ilgili paydaşlarla istişare ederek internet altyapısındaki aksaklıklar ve müdahalelere cevap vermek ve bunları yönetmek için acil durum planları geliştirmeli ve uygulamalıdır.

2.1.2. Devletler, bilhassa internetin dengeliliğini, sağlamlığını ve dayanıklılığını muhafaza etme ve güçlendirmeye yönelik ortak standartlar, kurallar ve uygulamalar geliştirmek ve icra etmek için iş birliği içinde olmalıdır.

2.1.3. Devletler, internet altyapısında sınır aşan esaslı aksaklığa yol açma veya altyapıya müdahale etme riski barındıran eylemler bakımından, özellikle kamu-özel ortaklıkları oluşturarak, bilgi paylaşımını ve paydaşlar arasında koordinasyonu kolaylaştıracak bir ortam hazırlamalıdır.

2.2. Karşılık

2.2.1. Bildirim

Devletler, internet altyapısındaki sınır aşan esaslı aksaklıkları ve müdahaleleri etkilenme ihtimali olan devletlere gecikme olmaksızın bildirmelidir.

2.2.2. Bilgi paylaşımı

Devletler, internet altyapısındaki sınır aşan esaslı müdahale veya aksaklığa ilişkin tüm bilgileri, etkilenmesi muhtemel devletlerle zamanında paylaşmalıdır.

2.2.3. İstişare

Devletler, internet altyapısındaki sınır aşan esaslı müdahale veya aksaklığa karşı alınacak önlemlere ilişkin karşılıklı kabul görecek çözümlere ulaşmak amacıyla birbiriyle gecikme olmaksızın istişareye başlamalıdır.

2.2.4. Karşılıklı yardımlaşma

Uygun olduğu ölçüde ve yeterlilikleriyle uyumlu şekilde devletler, etkilenen diğer devletlere, internet altyapısındaki sınır aşan esaslı müdahale veya aksaklıkların olumsuz etkilerini ortadan kaldırmak için iyi niyetle desteklerini sunmalıdır.

2.3. Uygulama

Devletler, ilgili paydaşlarla istişarede bulunarak ve günlük teknik ve operasyonel hususlara müdahale etmemeye ilişkin sınırlar çerçevesinde, internetin bütünlüğünü sağlamaya yönelik özen yükümlülüğü taahhütlerinin yerine getirilmesi kapsamında makul yasal, idari ve diğer tedbirleri geliştirmelidir.

2.4. Sorumluluk

Devletler sorumluluk, yükümlülük ve ilgili uyuşmazlıkların çözümüyle alakalı uluslararası standartların daha da geliştirilmesine yönelik diyalog ve iş birliği içerisinde olmalıdır.

3. İnternetin çalışmasına yönelik kritik kaynaklar

Devletler, internetin çalışmasına yönelik kritik kaynakların yönetimiyle bağlantılı ve internet kullanıcılarının insan hakları ile temel hak ve özgürlüklerinin korunmasını uluslararası insan hakları hukukunda kabul edilen standartlara uygun şekilde temin edecek standartlar, politikalar, prosedürler ve uygulamalar geliştirmek ve icra etmek için makul tüm tedbirleri almalıdır.

XVIII. Özel Olarak İşletilen İnternet Platformları ve Online Hizmet Sağlayıcıları Bağlamında İfade Özgürlüğü ile Toplantı ve Örgütlenme Özgürlüğünün Korunması Deklarasyonu (2011)

Özel Olarak İşletilen İnternet Platformları ve Online Hizmet Sağlayıcıları Bağlamında İfade Özgürlüğü ile Toplantı ve Örgütlenme Özgürlüğünün Korunması Deklarasyonu, Avrupa Konseyi Bakanlar Komitesinin 7 Aralık 2011 tarihli 1129. Toplantısı'nda kabul edilmiştir.[286] Deklarasyon, AİHS'nin 10 ve 11. maddelerinde güvence altına alınan ifade özgürlüğü ile toplantı ve örgütlenme özgürlüğünün hem çevrim içi hem de çevrim dışı ortamda korunduğunu vurgulamıştır.

Deklarasyon sivil toplum temsilcilerinin, ihbarcıların (*whistleblowers*) ve insan hakları savunucularının bilgiye erişmek, bilgiyi paylaşmak, içeriği yayınlamak, etkileşimde bulunmak, haberleşmek ve bir araya gelmek için sosyal medya, blog siteleri ve diğer kitle haberleşme araçlarını kullandığını ve bu tür platformların yeni medya ekosisteminin ayrılmaz parçası hâline geldiğini belirtmiştir. Bu tespitten sonra Deklarasyon, her ne kadar özel kişiler tarafından işletilse de bu tür platformların kamu yararına olan tartışmaları kolaylaştırdığını, bazı durumlarda geleneksel

---

[286] **Avrupa Konseyi**, "*Declaration of the Committee of Ministers on the protection of freedom of expression and freedom of assembly and association with regard to privately operated Internet platforms and online service providers*", <https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805cb844>

basının yerine geçebildiğini, sosyal bekçilik rolü oynadığını ve gerçek hayatta pozitif değişimler sağladığını ifade etmiştir.

Deklarasyon, sunduğu imkânların yanı sıra bu tür yeni medya ekosistemine müdahalelerin temel hak ve hürriyetlere yönelik etkisine de işaret etmiştir. Bu bağlamda özellikle servis dışı bırakma gibi saldırıların oluşturduğu tehdide dikkat çekilmiştir. Deklarasyon'a göre, bu nitelikteki içerikleri barındıran şirketler saldırılar sebebiyle söz konusu içeriği barındırmaktan imtina edebilir veya sorumluluk altına girmemek adına bazı kısıtlamalara gidebilir. Keza, bu tür kararlar politik baskılar altında da ortaya çıkabilmektedir.

Deklarasyon'a göre tüm bu gelişmeler göstermektedir ki çevrim içi ifade özgürlüğü yeni yöntemlerle zorlanabilir ve özel kişilerce yönetilen internet platformlarının ve online hizmet sağlayıcıların kararlarına kurban gidebilir. Deklarasyon bu sebeple, bu aktörlerin ifade özgürlüğü ile toplantı ve örgütlenme özgürlüğünün icrasındaki kolaylaştırıcı rolünün kabul edilmesi gerektiğine dikkat çekmiştir.

Deklarasyon'a göre, bu araçlarla kamuya sunulan içeriğe müdahale edilmesi veya tüm web sitelerini erişilmez kılmaya yönelik girişimler, ifade özgürlüğü ile bilgi alma ve verme hakkını güvence altına almaya çalışan başta AİHS'nin 10. maddesi ile AİHM'nin ilgili içtihatları olmak üzere uluslararası standartlara göre muhakeme edilmelidir. Aynı değerlendirme, belirli menfaat gruplarının etkileşimine yönelik engeller bakımından da yapılmalıdır.

Tüm bu tartışmalar bağlamında Bakanlar Komitesi, üye devletleri, özel kişilerce işletilen internet platformları ve online hizmet sağlayıcıları üzerindeki politik temelli baskılardan ve bağımsız basın kuruluşlarının web sitelerine, insan hakları savunucularına, muhaliflere, ihbarcılara ve yeni basın aktörlerine yönelik diğer saldırılardan kaynaklanan AİHS'nin 10. ve 11. maddelerine ilişkin ihlallerin ağırlığı konusunda uyarmaktadır. Komite ayrıca, bu bağlamda ifade özgürlüğü, bilgi alma ve verme hakkı, toplantı ve örgütlenme hakkına ilişkin politikaları sağlamlaştırmanın öneminin altına çizmiş ve bu alandaki temel sorunları belirlemeye yönelik çalışmaları sürdürmeye yönelik taahhütleri onaylamıştır.

XIX. Arama Motorları Bağlamında İnsan Haklarının Korunmasına İlişkin Tavsiye Kararı (2012)

Arama Motorları Bağlamında İnsan Haklarının Korunmasına İlişkin Tavsiye Kararı, Avrupa Konseyi Bakanlar Komitesinin 4 Nisan 2012 tarihli 1139. Toplantısı'nda kabul edilmiştir.[287] Tavsiye Kararı'nın temel çıkış noktası, arama motorlarının bilgi toplumunda oynadığı hayati roldür.

Tavsiye Kararı'na göre, arama motorları dünya genelinde bilgi almak, tartışmalara katkı sunmak ve demokratik süreçlere katılmak için bilginin, fikirlerin ve diğer içeriklerin araştırılması, alınması ve dağıtımına imkân tanımaktadır. İnternetin kamu hizmeti niteliğine ilişkin 2007 yılındaki kararı hatırlatan Tavsiye Kararı, internet erişimdeki önemlerine binaen, arama motorlarının internet ortamında yer alan, kamuya açık ve dış erişimi amaçlanan içeriği serbestçe tarayıp indekslemesine izin verilmesinin önemli olduğunu vurgulamıştır.

Bu doğrultuda, insan hakları gerekliliklerine uyan elverişli düzenleyici çerçevelerin, arama motorlarının başkalarınca oluşturulan içeriğe bağlantı vermesine ilişkin meşru endişelere uygun yanıtlar vermesi gerektiğini belirtilmiştir. Aynı keyfiyetin, telif hukukuna ilişkin ulusal düzenlemelerde de gözetilmesi gerektiği hatırlatılmıştır.

Arama motorlarının faaliyetlerinin insan hakları ile temel hak ve özgürlüklere de etkisi vardır. Algoritmaların dizaynı, içeriğin indeksten çıkarılması ve/veya kısmi değerlendirilmesi veya yanlı sonuçlar, piyasa yoğunlaşması ve seçim süreci ile sonuçların sıralanmasına ilişkin şeffaflığın olmaması gibi sebeplerle, arama motorları ifade özgürlüğü, özel hayatın mahremiyeti ve kişisel verilerin korunması haklarına etki edebilmektedir. Bilhassa kitle iletişimine yönelmeyen içeriğin indekslenmesi veya bu tür içeriklere nüfuz edilmesi, genel olarak veri koruma süreçleri ve veri saklama süreleri sebebiyle özel yaşama etki doğabilmektedir. Tavsiye

[287] **Avrupa Konseyi**, "*Recommendation CM/Rec(2012)3 of the Committee of Ministers to member States on the protection of human rights with regard to search engines*", <https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805caa87>

Kararı'na göre, arama motorları bireysel arama geçmişleri ve davranışsal profiller gibi yeni tür kişisel veriler oluşturmaktadır.

Tavsiye Kararı, bu doğrultuda arama motorları bağlamında erişimi, çeşitliliği, tarafsız muameleyi, güvenliği ve şeffaflığı korumaya ve geliştirmeye ihtiyaç olduğunu belirtmiştir. AİHS ve kişisel verilere ilişkin 108 sayılı Avrupa Konseyi Sözleşmesi ışığında Bakanlar Komitesi arama motorlarına ilişkin şu tavsiyelerde bulunmuştur:

- Bilgi ve hizmetlere ilişkin erişimi, çoğulculuğu ve çeşitliliği temin etmek için bilgiye erişimin nasıl sağlandığına, bilhassa hangi arama sonuçlarının seçildiği, sıralandığı veya kaldırıldığına ilişkin şeffaflığın artırılması;

- Arama sıralamanın ve kitle iletişimine yönelmemiş içerikleri indekslemenin gözden geçirilmesi. İçerik arama sonuçlarında yeterince düşük listelenerek içeriğin erişilebilirliği ile üreticinin amaç ve niyetleri arasında denge sağlanabilir (örneğin, geniş dağıtımı hedefleyen yayımlanmış içerik ile sadece kamusal alanda erişilebilir olan içeriğe farklı erişilebilirlik seviyeleri oluşturmak). Varsayılan ayarlar bu hedefi gözetmelidir.

- Kişisel verilerin toplanmasında ve kişisel verilerin işlenmesine yönelik meşru amaçlara yönelik şeffaflığı artırma;

- Kullanıcılara arama motorları tarafından işlenen kişisel verilere kolay erişme ve mümkün olduğu ölçüde bu verileri düzeltme veya silme imkânı tanınması;

- Kısıtlı saklama sürelerinin uygulanması ve uygun geri döndürülemez anonimleştirme dâhil olmak üzere kişisel verinin toplanması ve işlenmesini minimuma indirecek araçlar ile verinin silinmesi için araçlar geliştirilmesi;

- Engellilerin hizmetlerine erişimini temin ederek topluma entegrasyonlarını ve tam katılımlarını artırma;

- Herhangi bir kamusal veya özel birime kullanıcıların kişisel verilerine erişim imkânı tanındığında uygun yasal korumaların mevcudiyeti temin edilerek AİHS'deki hak ve özgürlüklerin tam olarak icrasını güvence altına alma;

- AİHS'nin 10. maddesinin ikinci fıkrası doğrultusunda arama motorlarının arama sonuçlarını yok saymasını teşvik etme. Bu durumda, kullanıcı özel yaşam hakkı ile kişisel verilerin korunması hakkına konu sonuçların yok sayılmasına ilişkin talebin kaynağı hakkında bilgilendirilmelidir;

- Arama sonuçlarının seçimi, sıralanması ve önceliklendirilmesi başta olmak üzere arama motorlarının işleyişi ve kullanıcıların özel yaşam hakkı ile kişisel verilerinin korunması üzerindeki etkileri bakımından bilişim okuryazarlığının artırılması;

- Kullanıcılara bilhassa kamu değeri kriterine göre arama sonuçları bağlamında arama motoru tercihi sunulması;

- Arama motorları için özellikle bir mahkeme veya yetkili makam tarafından hukuka aykırı ilan edilen içerik ile zararlı içeriğe erişebilirlik bağlamında Avrupa Konseyinin ifade özgürlüğüne ve hakların korunmasına ilişkin standartlarına uygun, şeffaf öz düzenleme ve ortak düzenleme mekanizmalarının teşvik edilmesi.

Tüm bunlara ek olarak Tavsiye Kararı, arama motorlarına ilişkin müstakil ilkeler ortaya koymuştur. Söz konusu ilkeler şöyledir:

I. Kamunun arama motorlarını kullanırken bilinçli tercihler yapmasına yardım etme

Bağlam ve zorluklar

1. Arama motorları, internette ilk temas noktası olarak bilgiye, fikirlere, vakıalara, düşüncelere ve eğlence gibi diğer içeriklere arama ve erişme hakkını kullanırken kritik bir rol oynamaktadır. Bu tür bilgiye erişim, kişilerin şahsi düşüncelerinin inşası ve sosyal, politik, kültürel ve

ekonomik alana katılım için esaslı niteliktedir. Arama motorları, ayrıca vatandaşların elektronik gazeteler ve görsel-işitsel basın hizmetleri dâhil genel olarak basına erişimi için de önemlidir.

2. Kullanıcıların sınırlı sayıdaki dominant arama motorlarını kullanma eğiliminde olmaları sebebiyle bazı endişeler vardır. Bu -bilhassa arama motorlarının bilgi sıralaması kapsayıcı veya nötr değilse- bilgi kaynaklarına erişim ve bilgi kaynaklarının çeşitliliği bağlamında sorunlar ortaya çıkarmaktadır. Bu doğrultuda, bazı tür içerik veya hizmetlerin haksız şekilde kayırılması söz konusu olabilecektir.

3. Bilgiyi arama süreci bilginin nasıl düzenlendiğinden son derece etkilenmektedir. Öyle ki arama sonuçlarının seçimi, sıralanması ve -uygun düştüğü ölçüde- içeriğin indeksten çıkarılması da bu sürece dâhildir. Çoğu arama motoru, bu konularda ya çok kısıtlı yahut çok genel bilgiler sağlamaktadır. Özellikle, gösterilen bir sonucun o sorguya "en iyi" yanıt olarak belirlenmesinde durum böyledir.

Eylem

4. Algoritmaların rekabetle son derece alakalı olması sebebiyle, iş modelleri ve metotları ile işle ilgili kararların tamamen ifşa edilmesi uygun olmayacağı ve bu tür bilgiler arama motorlarının güvenlik açıklarını artırabileceği için (örneğin, arama manipülasyonu şeklinde) üye devletler, özel sektör ve sivil toplumla iş birliği içerisinde:

- Arama motorlarını arama sonuçlarının seçimi ve sıralanmasına ilişkin genel kriterler ve süreçler bakımından şeffaflıklarını artırmaları için teşvik etmelidir. Bu şeffaflık, arama tarafgirliğine, örneğin açık coğrafi konuma veya daha önce yapılan aramaya dayalı sonuçları göstermeyi içermelidir;

- Arama sonuçları ile kendi içerikleri dâhil herhangi bir tür ticari iletişim, tanıtım veya sponsorlu sonuçları açıkça farklılaştırma konusunda arama motorlarını teşvik etmelidir;

- Arama motorları için arama motoru hizmetlerinin kamusal değer boyutu, arama motoru piyasasındaki artan yoğunlaşma, kötüye kulla-

nım, manipülasyon ve arama sonuçlarını kısıtlama riski gibi sorunları da adresleyen dinamik piyasaya ilişkin araştırmayı teşvik etmelidir.

Özel yaşam hakkı ve kişisel verilerin korunması hakkı

Bağlam ve sorunlar

5. Arama motorları, Avrupa düzeyinde ve uluslararası düzeyde kabul edilen muhtelif düzenlemelerde de işaret edildiği üzere bireylerin arama davranışlarına ilişkin çerezler ve IP adreslerinden bireysel arama sonuçları geçmişine kadar büyük ölçekte kişisel veri işlemektedir.[**1**]

6. Bir kişinin arama sonucu; kişinin inançları, ilgi alanları, ilişkileri veya niyetlerini ifşa edebilecek bir ayak izi içermektedir. Bireysel arama geçmişi ayrıca 108 sayılı Sözleşme'nin 6. maddesinde özel olarak korunan hassas verileri (ırksal köken, politik fikirler, dinî veya diğer inançlar, sağlık, cinsel hayat veya ceza mahkûmiyetine ilişkin bilgileri) ifşa edebilir.

7. Görsel-işitsel verilerin (dijital resimler, ses ve video içeriği) çoğalması ve mobil internet erişiminin yaygınlaşması sebebiyle arama motorlarının kişisel veri işlemesi başka bir boyuta taşınmıştır. Kullanıcıların bireylere ilişkin bilgi bulmasına imkân veren, konum temelli hizmetler sunan, kullanıcılar tarafından oluşturulmuş resimleri genel amaçlı arama sonuçlarına dâhil eden ve giderek daha doğru şekilde yüz tanıma teknolojileri sunan özelleştirilmiş arama motorları mevcuttur. Bu gelişmeler, arama motorlarının, özel yaşam hakkı veya kişinin kendi tercihine göre bilgiyi arama, alma ve yayma haklarını kullanması gibi temel haklara ve ifade özgürlüğüne gelecekteki muhtemel etkilerine ilişkin endişeleri artırmaktadır.

8. Arama motorları, bir kişiye ilişkin farklı türdeki bilgileri birleştirerek o kişinin gerçeklikle bağdaşmayabilen veya kendisiyle ilgili istemediği bir imaj oluşturmaktadır. Arama sonuçlarının birleştirilmesi, bu kişiye ilişkin bilgilerin internet ortamında ayrı yerlerde kalmasına nazaran daha büyük bir risk oluşturmaktadır. Öyle ki unutulan bir kişisel veri, arama motorlarının faaliyetlerinin neticesi olarak yeniden gün ışığına çıkabilir. Medya okuryazarlığının bir unsuru olarak kullanıcılar, doğru olmayan

veya aşırı kişisel verilerin ifade özgürlüğüne halel getirmeden orijinal web sitelerinden nasıl kaldırılacağına dair bilgilendirilmelidir. Arama motorları, kullanıcıların, orijinal içerik silindikten sonra arama motorlarının -önbelleklerinde veya ufak parçalar hâlinde- saklamaya devam ettiği kişisel verilerinin web sitelerinin (seçme) kopyalarından silinmesi taleplerine gereğince yanıt vermelidir.

9. Genel olarak, kişileri özel yaşamlarına hukuka aykırı müdahalelerden koruyan, kişisel verilerin işlenmesinin kötüye kullanılmasını önleyen ve bu konuda katı kurallar getiren başta AİHS'nin 8. maddesi ile 108 sayılı Sözleşme'nin 9. maddesi olmak üzere uygulanabilir mahremiyet ve veri koruma ilkelerine uyum hayati niteliktedir.

Eylem

10. Üye devletler (belirleyecekleri kurumlar aracılığıyla) uygulanabilir veri koruma ilkelerine uyumu, bilhassa da arama motorlarının müteakip eylemleri gerçekleştirmesini temin etmelidir:

- Arama motorları tarafından minimum düzeyde kişisel veri toplanması temin edilmelidir. Meşru bir amaç için zorunlu olmadıkça ve aynı sonuçlara örnekseyerek, tahminle veya kişisel verinin anonimleştirilmesiyle de ulaşılabiliyorsa kullanıcıların IP adresleri saklanmamalıdır. Anonim arama yapmaya ilişkin yenilikçi yaklaşımlar teşvik edilmelidir.

- Kişisel verileri saklama sürelerinin, meşru ve belirli işleme amacının gerektirdiğinden fazla olmaması temin edilmelidir. Arama motoru sağlayıcıları, kişisel verileri toplama ve saklamalarını kanıtlanabilir sebeplerle gerekçelendirebilecek durumda olmalıdır. Bu bağlamdaki bilgi kamuyla paylaşılmalı ve bu bilgiye kolayca erişilebilmelidir.

- Arama motorlarının, yetkisiz üçüncü kişilere karşı kişisel verilerin korunmasına ilişkin en uygun güvenlik önlemlerini alması sağlanmalı ve ihlal bildirim planı uygulamaya alınmalıdır. Önlemler, kullanıcı ve arama motoru sağlayıcısı arasındaki haberleşmenin uçtan uca şifrelenmesini de içermelidir.

- Bireyler kişisel verilerinin işlenmesine ve bu bağlamdaki haklarını kullanmaya ilişkin anlaşılabilir, açık ve yalın bir dille, veri süjesine uygun hazırlanmış bir metinle bilgilendirilmelidir. Arama motorları, kişisel verilerin tüm kullanım amaçları (bu tür bir işlemenin ilk amacının arama talebine yanıt vermek olduğu vurgulanarak) ve kişisel verilere ilişkin hakları konusunda kullanıcılarını açıkça bilgilendirmelidir. Bireyler, kişisel verileri ele geçirildiği takdirde de bilgilendirilmelidir.

- Arama motoru sağlayıcısına ait olan farklı hizmetler ve platformlardan kaynaklanan verilerin çapraz korelasyonu, kullanıcının bu hizmete ilişkin açık rızası alınmasıyla mümkün olmalıdır. Bu kurallar, daha önce yayımlanan (2010)13 numaralı Tavsiye Kararı'nda belirtilen profil zenginleştirme faaliyetleri için de geçerlidir.

11. İlave olarak, üye devletler:

- Arama motoru sağlayıcılarını, kullanıcılara, hizmetleri kullandıkları sırada -doğrudan pazarlama amaçlarıyla oluşturulmuş herhangi bir profil dâhil- toplanmış olan kendileriyle ilgili verilere erişim, verileri düzeltme ve silme imkânı veren araçlar geliştirmeleri için teşvik etmelidir.- Kolluk kuvvetleri tarafından arama motoru sağlayıcılara yöneltilen kullanıcı verilerine ilişkin taleplerin uygun yasal ve adli usullere dayanmasını ve şeffaf iş birliği mekanizmaları uygulanmasını temin etmelidir. Bireylerin verileri ve arama kayıtları kamu otoriterleri veya özel kişilerle paylaşılmadan önce süreç, sağlam hukuki koruma mekanizmalarını ve gerekli yargısal korumaları içermelidir.

II. Filtreleme ve indeksten çıkarma

Bağlam ve zorluklar

12. Etkili arama motorlarının varlığının ön koşulu, web ortamında sunulan bilgiye özgürce erişmek ve indekslemektir. İnternet içeriğinin arama motoru sağlayıcıları tarafından filtrelenmesi ve engellenmesi, sağlayıcılar ile kullanıcıların bilgiyi dağıtma ve bilgiye erişme bağlamında

AİHS'nin 10. maddesinde güvence altına alınan ifade özgürlüklerinin ihlali riskini taşımaktadır.

13. Arama motorları, hukuka aykırı içeriği tespit etmek için ne ağlarını ve hizmetlerini önleyici şekilde gözetleme ne de uygulama öncesi filtreleme veya engelleme faaliyeti gerçekleştirme yükümlülüğü altına sokulmamalıdır; meğerki bir mahkeme kararıyla veya yetkili bir makamca bu konuda açık bir talimat verilmiş olsun. Öte yandan, diğer hakların ifade özgürlüğü ile bilgiye erişim hakkına ağır bastığı durumlarda indekslerden belirli kaynakların kaldırılmasına yönelik meşru talepler olabilir. Bu durumlarda, bilgiye erişim hakkı, kendi ifade özgürlüğünü kullanan kişinin niyetinin ötesinde içeriğe erişimi genişletecek şekilde anlaşılmamalıdır.

14. Birçok ülkede, arama motorları, belirli web sitelerini kamu otoritelerinden veya özel kişilerden gelen talepler üzerine hukuki yükümlülüklerini yerine getirmek amacıyla yahut kendi inisiyatifleriyle (örneğin, web sitesinin içeriğiyle ilgili olmayıp kötü amaçlı yazılım gibi teknik tehlikeler sebebiyle) indeksten çıkarmakta veya filtrelemektedir. Bu tür indeksten çıkarma veya filtrelemeler şeffaf olmalı, dar şekilde dizayn edilmeli ve hukuki gerekliliklere uyum çerçevesinde düzenli olarak gözden geçirilmelidir.

Eylem

15. Üye devletler:

- İndeksten çıkarma veya filtrelemeye dair her türlü yasa, politika veya bireysel talebin, ilgili yasal düzenlemelere, ifade özgürlüğü ile bilgiyi arama, alma ve yayma hakkına uygun şekilde hayata geçirilmesini temin etmelidir. Yargısal koruma ilkeleri ve bağımsız, hesap verebilir tazmin mekanizmalarına bu bağlamda riayet edilmelidir.

16. İlave olarak, üye devletler arama motoru sağlayıcılarıyla beraber çalışmalıdır ve:

- Zorunlu herhangi bir filtreleme veya engellemenin kullanıcıya şeffaf şekilde açıklanması temin edilmelidir. Belirli anahtar kelimeler için

tüm arama sonuçlarının engellenmesi, arama motorlarına ilişkin öz düzenleme ve ortak düzenleme kurallarında yer almamalı veya teşvik edilmemelidir. Öz düzenleme ve ortak düzenleme rejimleri, bireylerin ifade özgürlüğü ile bilgiyi, fikirleri veya içeriği herhangi bir mecra üzerinden arama, alma ve yayma haklarına halel getirmemelidir. Belirli kategorideki kullanıcılar için demokratik bir süreçle zararlı olarak tanımlanan içerikler bakımından üye devletler, indeksten çıkarma yöntemine başvurmamalıdır zira bu yöntem, içeriği diğer kategorideki kişiler için de erişilmez kılar. Birçok durumda, arama motorlarını uygun gönüllü bireysel filtreleme mekanizmaları sunmaya teşvik etmek bu tür grupları korumak için yeterli olacaktır.

- Kamusal alanda yer alan ve kitle iletişimine (veya bütün olarak kitle iletişimine) yöneltilmemiş içeriğin indeksten çıkarılmasına izin verilmesi imkânları araştırılmalıdır.

III. Öz Düzenleme ve Ortak Düzenleme

Bağlam ve zorluklar

17. Arama motorlarının bireylerin temel haklarını korumaya yönelik öz düzenleyici inisiyatifleri memnuniyetle karşılanmalıdır. Önemle hatırlatmak gerekir ki tüm öz düzenleme ve ortak düzenleme girişimleri başkalarının haklarına müdahaleye yol açabilir; bu sebepledir ki bu tür girişimler AİHS'nin 10. maddesine uygun şekilde şeffaf, bağımsız, hesap verebilir ve etkin olmalıdır. Devlet, özel kişiler ve sivil toplum gibi paydaşlar arasındaki verimli bir etkileşim, insan haklarının korunmasına ilişkin standartların oluşturulmasına önemli katkı sunabilir.

18. Üye devletler:

- Bu tür tedbirler uygun bulunursa arama motoru sağlayıcılarıyla ortak düzenlemenin (*co-regulation*) geliştirilmesi suretiyle başta hukuki güvenlik, ifade özgürlüğü, özel hayat hakkı olmak üzere bireylerin temel haklarının AİHS standartlarını sağlar şekilde korunmasını teşvik edecek adımları atmalıdır.

- Sektörün bireylerin başta hukuki güvenlik, ifade özgürlüğü ve mahremiyet hakkı olmak üzere temel haklarını AİHS'yi gözeterek korumayı garanti eden öz düzenleyici davranış kuralları geliştirmesi teşvik edilmelidir.

V. Medya okuryazarlığı

Bağlam ve zorluklar

19. Kullanıcılar, sunulan bilginin kaynakları hakkında bilinçli tercihler yapabilmek için farklı arama motorlarının işleyişiyle ilgili bilgilendirilmiş ve eğitilmiş olmalıdırlar (arama motoru okuryazarlığı). Özellikle, üst sıralarda çıkan bir sonucun kaynağın önemini, alakalı oluşunu veya güvenilirliğini bire bir yansıtmayabileceğini bu sayede bilebilirler. Arama motorları online ortamdaki medya ve bilgiye erişebilirlik konusunda artan önemde rol oynadıklarından medya ve bilgi okuryazarlığı stratejileri de bu doğrultuda uyarlanmalıdır. Kullanıcılar, arama motorlarının hem özelleştirilmiş hem de kendilerine ilişkin birleştirilmiş arama sonuçlarının kendi imaj ve itibarlarına etkisine ve haklarını kullanmak için mevcut araçlara ilişkin bilinçlendirilmelidir.

Eylem

20. Üye devletler:

- Arama motoru okuryazarlığı konusunu kendi ulusal medya okuryazarlığı stratejilerine dâhil etmek için uygun adımları atmalıdır.

- Kullanıcıların online kimliklerinin farkında olmalarına ve bunları yönetmelerine imkân tanıyacak uygun adımları atmalıdır. Bilhassa arama sonuçlarının kullanıcıların imaj ve itibarları üzerinde doğurabileceği etkiler ve haklarını kullanmak için etkili araçlar konusu bununla ilgilidir.

[1] Arama motorları bağlamında veri korumaya ilişkin Madde 29 Çalışma Grubu Görüşü 1/2008 (kabul edilme tarihi 4 Nisan 2008); 28. Uluslararası Veri Koruma ve Mahremiyet Yetkilileri Konferansının Mahremiyet Korunması ve Arama Motorları Kararı (Londra, 2-3 Kasım 2006).

XX. Sosyal Ağ Hizmetleri Bağlamında İnsan Haklarının Korunmasına İlişkin Tavsiye Kararı (2012)

Sosyal Ağ Hizmetleri Bağlamında İnsan Haklarının Korunmasına İlişkin Tavsiye Kararı, Avrupa Konseyi Bakanlar Komitesinin 4 Nisan 2012 tarihli 1139. Toplantısı'nda kabul edilmiştir.[288] Avrupa Konseyinin bu Tavsiye Kararı, internete ilişkin diğer kararlarla benzerlik taşımakta fakat bu kez sosyal ağ hizmetlerini merkeze almaktadır. Keza, teknik anlamdaki tavsiyeler ve eylemler arama motorlarına ilişkin yukarıda incelenen tavsiye kararıyla genel olarak benzer niteliktedir.

Tavsiye Kararı'na göre sosyal ağ veya yaygın adıyla sosyal medya, insan haklarının kullanımını mümkün kılmanın yanında demokrasi için katalizör görevindedir. Öyle ki bireyler arasında ifade ve haberleşmenin ve ayrıca kitle iletişimi veya genel olarak kitle haberleşmesinin de aracı konumundadır. Tavsiye Kararı'na göre sosyal ağlar, daha geniş halk kitlelerinin bilgiyi alma ve yaymasına yardımcı olmakta; bireylerin politik, sosyal ve kültürel hayata katılımını geliştirmektedir. Aynı doğrultuda, internetin kamu hizmeti değerinin bir uzantısı olarak sosyal ağ, demokrasiyi ve sosyal katılımı kolaylaştırmaktadır.

Tavsiye Kararı, sosyal ağların sadece sunduğu fırsatlara değil ayrıca oluşturduğu tehdit ve risklere de işaret etmiştir. Tavsiye Kararı'na göre, sosyal ağlarda ifade ve bilgi özgürlüğü, özel yaşam hakkı ve insan onuru ihlal edilebilir ve sosyal medya, ayrımcı uygulamalara ev sahipliği yapabilir. Tavsiye Kararı'na göre bu tür tehditler, bireylerin dışlanmasına yol açan süreçleri kapsayan uygun hukuki ve usuli korumaların yokluğundan kaynaklanmaktadır. Tavsiye Kararı, sosyal ağ hizmetlerinin kişilerin hak ve özgürlüklerine saygı göstermesi gerektiğine ilişkin çağrıda bulunmuştur.

---

[288] **Avrupa Konseyi**, "*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*", <https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805caa9b>

Tüm bu tespitler ışığında Bakanlar Komitesi, sosyal ağ hizmetleri bağlamında şu üç ana başlık altında belirli tedbirlerin dikkate alınmasını önermiştir:

I. Sosyal ağlarla ilgilenen kullanıcılara yardımcı olacak temel bilgiler ve tedbirler

II. Çocukların ve gençlerin zararlı içerik ve davranışlara karşı korunması

III. Kişisel veriler ve sosyal ağlarda güven

Sosyal ağların bilgiye erişim ve bilgiyi yayma konusunda sunduğu imkânlara değinen Tavsiye Kararı, sosyal ağların, kullanıcılara profillerinin varsayılan ayarlarını anlamada yardımcı olmaları; kullanıcıları profillerine açık erişimin (hem zaman hem de coğrafi olarak) neticelerine ilişkin bilgilendirmeleri; kullanıcıları, verilerini arşivler ile arama motorlarının önbelleklerinden kaldırmak dâhil kendi verilerine erişimi kısıtlama hakları olduğu konusunda aydınlatmaları; üçüncü tarafların erişimine ilişkin uygun, özel hazırlanmış rıza imkânlarını sunmaları; kullanıcılara bilgilerini kontrol etme olanağı tanımaları; kullanıcıların online kimliklerine ilişkin bilinçli tercihlerde bulunmasına destek vermeleri; kullanıcılara kullanım kuralları ve koşullarına ilişkin açık bilgilendirmeler yapmaları ve sosyal ağ hizmetinin ağlarında bulunan hukuka aykırı içerik ile uygunsuz içerik ve davranışlara ilişkin nasıl bir editoryal politikası olduğuna dair kullanıcılara açık bilgilendirmeler sağlamaları konusunda üye devletleri harekete geçmeye davet etmiştir.

Tavsiye Kararı'nda ele alınan ikinci husus ise çocukların ve gençlerin zararlı içerik ve davranışlara karşı korunmasıdır. Sosyal ağların hem çocukların hem de gençlerin hayatlarında önemli bir rol oynadığını vurgulayan Tavsiye Kararı, sosyal ağların, sundukları içeriklerin hukuki niteliğine ilişkin açık bilgiler vermesi; uygunsuz olarak nitelendirilecek içeriklere ilişkin elverişli editoryal politikalar geliştirmeleri; hukuka aykırı içerik ve davranışların bildirilmesine yönelik erişilebilir mekanizmalar geliştirmeleri; siber zorbalık ve çocukların istismarının önlenmesine ilişkin en iyi uygulamaları paylaşmaları; kolluk kuvvetleriyle şeffaf iş birliği

mekanizmaları geliştirmeleri; bir içeriğin engellenmesi veya silinmesi bağlamında Avrupa Konseyinin internet filtrelerine ilişkin prensiplerine uygun davranmaları ve bu süreçlerin tamamında AİHS'yi gözetmelerini temin etme konusunda üye devletlerin adımlar atmasını istemiştir.

Tavsiye Kararı'nda ele alınan son husus ise kişisel veriler ve sosyal ağlarda güven konusudur. Tavsiye Kararı'na göre sosyal ağlar, büyük ölçekte kişisel veri işlemektedir. Bir profildeki kişisel verilere işverenler, sigorta şirketleri, kolluk kuvvetleri ve güvenlik birimleri gibi üçüncü kişiler tarafından erişilebilir. Bu sebeple, sosyal ağ servisleri, kişisel verileri hangi meşru ve belirli amaçlar için topladıysa o amaçların ötesine geçerek işlememelidir.

Tavsiye Kararı uyarınca sosyal ağlar, kullanıcılar için en iyi uygulamaları temin etmeli; kullanıcıların haklarını etkin şekilde kullanmalarını sağlamalı; hassas verilerin artırılmış korumaya sahip olmasını temin etmeli; kişisel verilere yetkisiz üçüncü kişiler tarafından erişilmesini önleyecek en uygun güvenlik tedbirlerini sağlamalı; tasarımda mahremiyet (*privacy by design*) ilkesini uygulamalı; sosyal ağ kullanıcılarıyla bağlantılı üçüncü tarafları korumalı; hukuki yükümlülüklerin AİHS'nin 8. maddesine uygun şekilde yerine getirilmesini sağlamalı; uygulanacak hukuk ve yetkiye ilişkin açık bilgi vermeli; kullanıcıları temel haklarına yönelik tehditler hakkında bilgilendirmeli ve hakları olumsuz etkilendiğinde bunun tazmini imkânını sağlamalıdır.

XXI. İnternet Kullanıcıları İçin İnsan Hakları Rehberi (2014)

İnternet Kullanıcıları İçin İnsan Hakları Rehberi, Avrupa Konseyi Bakanlar Komitesinin 16 Nisan 2014 tarihli 1197. Toplantısı'nda kabul edilmiştir.[289] Rehber, Avrupa Konseyinin internete ilişkin önceki tüm

[289] **Avrupa Konseyi**, "*Recommendation of the Committee of Ministers to member States on a Guide to human rights for Internet users*", <https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016804d5b31>

tavsiye kararlarını ve deklarasyonlarını konsolide ederek Konseyin internete en güncel yaklaşımını ortaya koymaya çalışmıştır.

Rehber, Avrupa Konseyi üye devletlerinin insan haklarına saygı gösterme, insan haklarını koruma ve yaygınlaştırma yükümlülüklerinin özel şirketlerin denetlenmesini de kapsadığını belirtmiştir. Rehber'e göre, evrensel ve bölünemez olan insan hakları ve bununla ilgili standartlar, herhangi bir özel sektör oyuncusunun internet kullanıcıları üzerine yükleyeceği genel şartlar ve kuralların üzerindedir.

Rehber, internetin bir kamu hizmeti değeri olduğunu tekrarlamış ve kimsenin interneti kullanırken insan hakları ve temel özgürlüklerden yararlanma konusunda yasalara aykırı, gereksiz ve orantısız bir müdahaleye maruz bırakılmaması gerektiğini belirtmiştir. Aynı doğrultuda, internetin kamuya ilişkin faaliyetlerin icrasında şeffaflık ve hesap verebilirlikle ilgili sunduğu fırsatlar göz önüne alınarak kullanıcıların demokratik yaşama katılmada internetten yararlanma konusunda güçlendirilmesi gerektiğine dikkat çekilmiştir.

İnternete ilişkin tüm süreçlerde AİHS ve AİHM'nin ilgili içtihatlarının dikkate alınması gerektiğini belirten Rehber, internete uygulanacak herhangi bir kısıtlamanın yasa ile öngörülmesi, demokratik bir toplumda geçerli bir amaca ulaşılması için gerekli ve bu geçerli amaçla orantılı olması gerektiğini hatırlatmıştır. Rehber, hak ve özgürlüklerinin kısıtlandığını veya haklarının ihlal edildiğini düşündüklerinde internet kullanıcılarının etkili yasal çözümlere erişimlerinin temin edilmesini, devlet ve devletler dışındaki aktörlerle koordinasyonun yaygınlaştırılmasını, özel sektörün devlet yetkilileriyle ve sivil toplumla etkin bir diyaloğa girmesinin teşvik edilmesini ayrıca tavsiye etmektedir.

Bu genel girişten sonra Rehber, internet kullanıcılarına yönelik bir dizi hatırlatmalar içeren tavsiyeler listelemiştir. Rehber'in ekinde de bu tavsiyelerin hem gelişim süreçleri hem de kapsamına ilişkin açıklayıcı bir not yer almaktadır. Aşağıda Rehber'in ilgili tavsiyelerine yer verilmiştir:

CM/Rec(2014)6 sayılı Tavsiye Kararı'na Ek

Giriş

1. Bu kılavuz, siz internet kullanıcılarının online ortamdaki insan haklarınız, bunların muhtemel kısıtlamaları ve bu gibi kısıtlamalara karşı başvurabileceğiniz mevcut yasal çözümler hakkında bilgi edinebileceğiniz bir araçtır. İnsan hakları ve temel özgürlükler internet üzerinde online ve offline (çevrim dışı) olarak eşit bir biçimde geçerlidir. Bu ilke, diğer internet kullanıcılarının hak ve özgürlüklerine saygıyı da içerir. Kılavuzda size internet bağlamında uygulamada hak ve özgürlüklerin neler olduğu, bu hak ve özgürlüklere nasıl dayanılabileceği ve bunların nasıl kullanılabileceği, hukuksal yollara nasıl başvurulabileceğiyle ilgili bilgiler sunulmaktadır. Bu belge, belirli dönemlerde güncellemeye açık, gelişmekte olan bir dokümandır.

2. Bu kılavuz, insan haklarının korunmasına ilişkin Avrupa İnsan Hakları Sözleşmesi ile diğer Avrupa Konseyi sözleşmeleri ve belgelerine dayalıdır. Avrupa Konseyinin tüm üyeleri, imzalayıp kabul ettikleri belgelerde yer alan hak ve özgürlüklere saygı göstermek, onları korumak ve yerine getirmekle görevlidir. Kılavuz aynı zamanda bu hak ve özgürlüklerin Avrupa İnsan Hakları Mahkemesince sürekli yorumlanmasından ve Avrupa Konseyinin ilgili diğer belgelerinden esinlenmiştir.

3. Bu kılavuz yeni insan hakları ve temel özgürlükler tesis etmez. Kılavuz, mevcut insan hakları standartları ve uygulama mekanizmaları üzerine inşa edilmiştir.[290]

İnternete erişim ve bu konuda ayrım gözetilmemesi

1. İnternete erişim, hak ve özgürlüklerinizi kullanmada ve demokrasiye katılımda önemli bir vasıtadır. O nedenle mahkeme kararı olmaksızın arzunuz hilafına internet bağlantınız kesilemez. Bazı hâllerde sözleşmeye bağlı düzenlemeler sonucunda hizmet kesintiye uğrayabilir ancak bu, en son başvurulacak bir tedbir olmalıdır.

[290] Bu kılavuz, Avrupa Konseyinin 47 üye ülkesinin Bakanlar Komitesince kabul edilen bir tavsiye kararının bir parçasıdır. Kılavuzla ilgili daha fazla açıklayıcı bilgi tavsiye kararının açıklama notunda bulunabilir.

2. İnternete erişim makul bir ücret karşılığında olmalı ve ayrım gözetilmeksizin sağlanmalıdır. Kendi seçtiğiniz cihazları kullanarak internet içeriğine, uygulamalarına ve hizmetlerine mümkün olan en geniş bir biçimde erişim sağlayabilmelisiniz.

3. Kırsal ve coğrafi olarak uzak bölgelerde yaşıyorsanız, düşük gelirliyseniz ve/veya özel ihtiyaç veya engelleriniz varsa kamu makamlarının internete erişiminizi kolaylaştırmak için makul bir gayret göstermesini ve bu konuyla ilgili özel tedbirler almasını bekleyebilirsiniz.

4. Kamu yetkilileriyle, internet hizmet sağlayıcılarıyla, online içerik ve hizmet sağlayıcılarıyla veya diğer gruplarla yahut kullanıcı gruplarıyla ilişkilerinizde, toplumsal cinsiyet, ırk, renk, dil, din veya inanç, siyasi veya diğer görüş, ulusal veya sosyal köken, ulusal bir azınlıkla bağlantı, mülkiyet, doğum veya etnik köken, yaş veya cinsel yönelim gibi diğer durumlarınız nedeniyle size karşı ayrımcılık yapılmamalıdır.

İfade ve bilgi özgürlüğü

Müdahalede bulunulmadan ve ulusal sınırlar gözetilmeksizin, seçtiğiniz bilgi ve fikirleri araştırma, alma ve verme hakkına sahipsiniz. Bu, şu anlama gelmektedir:

1. İnternet üzerinden online olarak kendinizi ifade etme, diğerlerinin bilgi ve görüşlerine erişim özgürlüğüne sahipsiniz. Buna siyasi konuşmalar, dinle ilgili görüşler, olumlu kabul edilen ve incitici bulunmayan görüş ve ifadelerin yanı sıra diğerlerini rencide edebilecek, şoke edebilecek veya rahatsız edebilecek görüş ve ifadeler de dâhildir. Mahremiyet hakkı dâhil olmak üzere, başkalarının saygınlığına veya haklarına gerekli duyarlılığı göstermelisiniz;

2. Kısıtlamalar ayrımcılığı, nefret duygularını veya şiddeti tetikleyen ifadeler için uygulanabilir. Söz konusu kısıtlamalar yasalara uygun olmalı, dar kapsamlı tutulmalı ve mahkemelerin gözetiminde uygulanmalıdır;

3. Telif hakları dâhil olmak üzere, fikrî mülkiyet haklarının korunmasına saygı göstermek suretiyle içerik yaratmakta, içeriği yeniden kullanıp dağıtmakta serbestsiniz;

4. İfade özgürlüğünüze ve bilgilenme özgürlüğünüze saygı göstermek ve bu özgürlükleri korumak kamu yetkililerinin bir görevidir. Bu özgürlüklere getirilecek herhangi bir kısıtlama keyfî olmamalı, Avrupa İnsan Hakları Sözleşmesi'ne uygun olarak diğer amaçların yanı sıra ulusal güvenliğin veya kamu düzeninin, kamu sağlığının ve ahlakının korunması gibi geçerli bir amaca yönelik olmalı ve insan hakları yasasıyla uyumlu olmalıdır. Ayrıca, bu kısıtlamalar bu konuda size rehberlik edecek ve hakkınızı aramanıza yardımcı olacak bilgilerle birlikte sunulmalı ve geçerli bir amaca ulaşılması için gerekli olandan daha geniş kapsamlı veya daha uzun süreli olmamalıdır;

5. İnternet hizmet sağlayıcınızın ve online içerik ve hizmet sağlayıcılarınızın, insan haklarına saygı gösterme ve taleplerinize cevap verecek mekanizmalar tesis etme konusunda kurumsal sorumlulukları vardır. Ancak, sosyal ağlar gibi online hizmet sağlayıcılarının, içerikle ilgili politikaları nedeniyle belirli tür içerik ve davranışları kısıtlayabileceklerini bilmelisiniz. Söz konusu hizmeti kullanıp kullanmama konusunda bilgilendirilmiş bir şekilde karar verebilmeniz için muhtemel kısıtlamalardan haberdar edilmelisiniz. Bu bilgilendirme, online hizmet sağlayıcısının söz konusu hizmetten yararlanılırken neyi yasa dışı veya uygunsuz bulduğu ve bu konuyla nasıl baş edeceği konusunda spesifik bilgileri de içerir;

6. Örneğin bir takma ad kullanarak internet üzerinden kimliğinizi açıklamamayı seçebilirsiniz. Bununla birlikte, ulusal makamların kimliğinizin açığa çıkmasına yol açabilecek tedbirler alabileceğini de bilmelisiniz.

Toplanma, örgütlenme ve katılım

İnterneti kullanarak diğer bireylerle barışçı bir şekilde bir araya gelme ve örgütlenme hakkına sahipsiniz. Uygulamada bu şu anlama gelmektedir:

1. Kamu yetkililerince resmen tanınsın veya tanınmasın, sosyal gruplar ve topluluklar kurma, bunlara katılma, bunları harekete geçirme ve bunlarda yer alma amacıyla herhangi bir web sitesini, uygulamayı veya diğer hizmet oluşumunu seçme özgürlüğüne sahipsiniz. Aynı zamanda

işçi sendikası kurma ve bunlara katılma hakkınızı kullanmak için de interneti kullanabilmelisiniz;

2. İnternet üzerinden barışçı bir biçimde protesto eylemi gerçekleştirme hakkına sahipsiniz. Ancak, online protesto eyleminiz tıkanıklıklara, hizmetlerin sekteye uğramasına ve/veya başkalarının malına zarar verilmesine neden olursa bunun yasal sonuçlarıyla karşılaşabileceğinizi bilmelisiniz;

3. Dilekçeler imzalamak ve internetin nasıl yönetileceğine dair politikaların oluşturulmasına katılmak da dâhil yerel, ulusal ve küresel kamu politikaları tartışmalarına, yasama inisiyatiflerine ve karar alma süreçlerinin kamusal denetimine katılmak üzere mevcut online araçları kullanma özgürlüğüne sahipsiniz.

Mahremiyet ve verilerin korunması

İnternette özel yaşam ve aile yaşamı hakkına sahipsiniz. Buna kişisel verilerinizin korunması ile haberleşme ve iletişiminizin gizliliği de dâhildir. Bunun anlamı şudur:

1. İnterneti kullanırken kişisel verilerinizin düzenli aralıklarla işleme tabi tutulduğunu bilmelisiniz. Bu, internet tarayıcıları, elektronik posta, mesajlar, internet üzerinden sesle iletişim protokolleri, sosyal ağlar, arama motorları ve bulut (*cloud*) veri saklama hizmetlerini kullanırken gerçekleşmektedir;

2. Kamu makamlarının ve özel şirketlerin, kişisel verilerinizi işleme tabi tutarken belirli kurallara ve prosedürlere saygı gösterme yükümlülüğü vardır;

3. Kişisel verileriniz, sadece yasalar tarafından öngörüldüğünde veya sizin rızanızla işleme tabi tutulmalıdır. Hangi kişisel verilerinizin işleme tabi tutulduğu ve/veya üçüncü taraflara aktarıldığı, bu işlemin ne zaman, kim tarafından ve ne amaçla yapıldığı konusunda bilgilendirilmelisiniz. Genel olarak kişisel verileriniz üzerinde kontrol yetkinizi kullanabilmelisiniz (Verilerin doğruluğunu kontrol edebilirsiniz; düzeltme ve silme

talep edebilirsiniz; kişisel verilerinizin gereğinden uzun bir süre saklandığını tespit edebilirsiniz);

4. Genel izleme veya dinleme tedbirlerine maruz bırakılmamalısınız. Yasalarda öngörülen istisnai durumlarda, örneğin bir ceza soruşturması amacıyla kişisel verileriniz bağlamında mahremiyetinize müdahale edilebilir. Bu açıdan size ilgili yasa veya politikalar ve haklarınız konusunda erişilebilir, anlaşılabilir ve net bilgiler sağlanmalıdır;

5. İş yerinizde de mahremiyetinize saygı gösterilmelidir. Buna özel online yazışmalarınız ve iletişim mesajlarınızın mahremiyeti de dâhildir. İşvereniniz, sizinle ilgili olarak gerçekleştirilen herhangi bir gözetleme ve/veya izlemeden sizi haberdar etmelidir;

6. Veri koruma yasalarına ve ilkelerine uyulmasını sağlamak üzere, Avrupa ülkelerinin büyük çoğunluğunda mevcut olan veri koruma makamlarından yardım alabilirsiniz.

Eğitim ve okuryazarlık

Bilgiye erişim hakkı da dâhil olmak üzere eğitim hakkına sahipsiniz. Bunun anlamı şudur:

1. Resmî dillerde eğitimin yanı sıra kültürel, bilimsel, akademik ve diğer içeriğe online olarak erişime sahip olmalısınız. Fikrî mülkiyet hakkı sahiplerine eserleri karşılığında ödeme yapılabilmesi için bu erişim bazı koşullara bağlanabilir. Aynı zamanda, mevcut olduğu hâllerde, internetteki kamuya açık alanda kamu fonlarıyla oluşturulmuş araştırma ve kültür eserlerine serbestçe erişebilmelisiniz;

2. İnternet ve medya okuryazarlığının bir parçası olarak, internetteki hak ve özgürlüklerinizi kullanmak üzere dijital eğitime ve bilgiye erişim sağlayabilmelisiniz. Bunlar, çok geniş bir yelpazeyi kapsayan internet araçlarını anlamaya, kullanmaya ve bunlarla çalışmaya yönelik becerileri de içermektedir. Bu, eriştiğiniz veya erişmek istediğiniz içerik, uygulama ve hizmetlerin doğruluğunu ve güvenilirliğini eleştirel bir biçimde analiz edebilmenizi sağlayacaktır.

Çocuklar ve gençler

Bir çocuk veya genç bir insan olarak, bu kılavuzda ana hatları verilen tüm hak ve özgürlüklere sahipsiniz. Özellikle de yaşınızın küçük olması nedeniyle, interneti kullanırken özel korumaya ve rehberliğe hak kazanmış durumdasınız. Bunun anlamı şudur:

1. Görüşlerinizi özgürce ifade etme ve toplum yaşamına katılma, sesinizi duyurma ve sizi etkileyen konularda karar verme sürecine katkıda bulunma hakkına sahipsiniz. Görüşlerinize, ayrımcılık yapılmaksızın, yaşınıza ve olgunluk durumunuza göre gereken ağırlık verilmelidir.

2. Mahremiyetinizi nasıl koruyacağınız da dâhil olmak üzere, internetin emniyetli kullanımı konusunda öğretmenlerinizden, eğitimcilerinizden ve ebeveyn veya velilerinizden yaşınıza ve eğitim düzeyinize uygun bir dilde bilgi almayı bekleyebilirsiniz;

3. İnternette oluşturacağınız veya diğer internet kullanıcılarınca sizinle ilgili olarak oluşturulacak içeriğe dünyanın her tarafından erişilebileceğini ve bunun itibarınızı, güvenliğinizi ve özel hayatınızın gizliliğini tehlikeye atabileceğini, şimdi veya hayatınızın daha sonraki bir evresinde size veya haklarınıza bir şekilde zarar verebileceğini bilmelisiniz. Talebiniz üzerine bu içerikler makul kabul edilebilecek kısa bir süre içinde kaldırılmalı veya silinmelidir;

4. Yasa dışı online içerik ve davranışlar (örneğin online taciz) ile yasa dışı olduğu iddia edilen içeriğin ilgili makamlara bildirilebileceği konusunda size açık ve anlaşılır bilgiler verilmesini bekleyebilirsiniz. Bu bilgiler yaşınıza ve içinde bulunduğunuz şartlara uyarlanmalı ve bilgilerinizin gizliliğine ve kimliğinizin açıklanmamasına gereken saygı gösterilerek bu konuda size tavsiyelerde bulunulmalı ve destek verilmelidir;

5. Özellikle internette cinsel istismar ve tacizle ve diğer siber suçlarla ilgili olarak fiziksel, zihinsel ve ahlaki esenliğinize yönelik müdahalelere karşı size özel bir koruma sağlanmalıdır. Bilhassa bu tür tehditlere karşı kendinizi korumak üzere eğitim alma hakkına sahipsiniz.

Etkili çözüm yolları

1. İnsan haklarınız ve temel özgürlükleriniz kısıtlandığında veya ihlal edildiğinde etkili bir çözüm yoluna başvurma hakkına sahipsiniz. Etkili bir çözüme ulaşmak için doğrudan yasal işlemlere başlamanıza gerek olmayabilir. Etkili çözüm yolları; mevcut, bilinir, erişilebilir ve makul maliyetli olmalı, uygun tazmin ve telafiyi sağlayabilmelidir. Etkili çözüm yolları doğrudan doğruya internet hizmet sağlayıcılarından, kamu yetkililerinden ve/veya ulusal insan hakları kurumlarından sağlanabilir. Söz konusu ihlale bağlı olmak üzere, etkili çözüm yolları arasında soruşturma, açıklama, yanıt, düzeltme, özür dileme, hakların eski hâline getirilmesi, internet bağlantısının yeniden sağlanması ve tazminat yer alabilir. Uygulamada bunun anlamı şudur:

1.1. İnternet hizmet sağlayıcınız, online içerik ve hizmet sağlayıcılarınız veya diğer şirket ve/veya kamu makamları sizi haklarınız, özgürlükleriniz, muhtemel çözüm yolları ve bunları nasıl elde edeceğiniz konusunda bilgilendirmelidir. Bu bilgilendirmeye, haklarınıza müdahaleyle ilgili bildirim ve şikâyette bulunma ve haklarınızın telafisi konusunda bilgiye kolayca erişim de dâhildir;

1.2. İlave bilgiler ve rehberlik kamu makamları, ulusal insan hakları kurumları (ombudsmanlar gibi), veri koruma makamları, yurttaş danışma büroları, insan hakları veya dijital haklar dernekleri veya tüketici örgütlerince sağlanabilir;

1.3. Ulusal makamlar, sizi internette veya internet kullanılarak işlenen suç faaliyetlerine veya ceza gerektiren suçlara karşı korumakla yükümlüdürler. Bu yükümlülük, bilhassa dijital kimliğinize, bilgisayarınıza ve bilgisayarınızdaki bilgilere yasa dışı erişim, müdahale, bunlarda sahtecilik veya bunlarla ilgili diğer dolandırma amaçlı manipülasyonlar söz konusu olduğunda geçerlidir. Dijital kimliğinize ve dijital varlıklarınıza bir zarar geldiği veya bir müdahale yapıldığına dair şikâyetiniz durumunda, yetkili kanuni merciler olayı soruşturmak ve yaptırım uygulamak dahil uygun eylemleri almakla yükümlüdür.

2. İnternetle ilgili olarak hak ve özgürlüklerinizin veya hakkınızdaki herhangi bir suç isnadının belirlenmesinde:

2.1. Bağımsız ve tarafsız bir mahkeme tarafından makul bir süre içinde adil yargılanma hakkına sahipsiniz;

2.2. Tüm iç hukuk yollarını tükettikten sonra Avrupa İnsan Hakları Mahkemesine bireysel başvuru hakkına sahipsiniz.

XXII. Bilginin İnternet Ortamında Sınır Ötesine Serbestçe Akışına İlişkin Tavsiye Kararı (2015)

Bilginin İnternet Ortamında Sınır Ötesine Serbestçe Akışına İlişkin Tavsiye Kararı, Avrupa Konseyi Bakanlar Komitesinin 1 Nisan 2015 tarihli 1224. Toplantısı'nda kabul edilmiştir.[291] Tavsiye Kararı'nda belirtildiği üzere herhangi bir müdahale olmaksızın ve sınırlardan bağımsız olarak ifade özgürlüğü, bilhassa da bilgiyi alma ve yayma hakkının kullanılması demokratik bir toplumun temel taşı, sürdürülebilirliğin ve her insanın gelişiminin temel koşuludur. Keza, AİHS'de yer alan hak ve özgürlükler ile Kişisel ve Siyasal Haklar Uluslararası Sözleşmesi'nin 19. maddesi hem çevrim içi hem de çevrim dışı alana eşit olarak uygulanmaktadır.

Tavsiye Kararı'nda vurgulandığı üzere, AİHS'nin 10. maddesi bilginin sadece içeriğine değil, yayılmasına ve barındırılmasına ilişkin araçlara da uygulanmaktadır. Nihayetinde, bilginin yayılmasına getirilen herhangi bir kısıtlama bilgiyi alma ve yayma hakkına da müdahale oluşturmaktadır. Aynı kurallar, toplantı ve örgütlenme özgürlüğü için de geçerlidir.

Tavsiye Kararı'na göre, internet trafiğine kasıtlı veya kasıtsız müdahale eden veya internet içeriğine yahut hizmetlerine ülke içinde sınırlamalar getiren ulusal politikalar, önlemler, ticari faaliyetler, teknolojik uygulamalar o devletin sınırları dışında ifade özgürlüğü ile toplantı ve örgütlenme haklarının kullanımı üzerinde de sonuçlar doğurabilir. Tavsiye Kararı,

[291] **Avrupa Konseyi**, "*Recommendation CM/Rec(2015)6 of the Committee of Ministers to member States on the free, transboundary flow of information on the Internet*", <https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c3f20>

bu durumda başka bir devletin egemenlik hakkının etkilenebileceğinin altını çizmiştir. Teknolojideki gelişmeler, örneğin içerik dağıtım ağları ve verileri bilginin sahibi, sorumlusu veya alıcısına yakın bir konumda değil uzak noktalarda (bulut hizmetleri gibi) barındıran ve işleyen hizmetlerin yaygınlaşması, bu alandaki karmaşıklığı artırmaktadır.

Tavsiye Kararı, uluslararası ortak bir anlayış geliştirilmesi gerektiğini, internet ortamında bilginin sınır ötesine serbest akışına ilişkin kuralların konsolide hâle getirilmesinin zorunlu olduğunu, tüm bunlar yapılırken çocukların online ortamlarda korunmasına, siber suçlarla mücadeleye ve kişisel verilerin korunmasına ilişkin uluslararası sözleşmelerle uyumun temin edilmesi gerektiğini belirtmiştir. Avrupa Konseyinin (2011)8 referans numaralı İnternetin Evrenselliğini, Bütünlüğünü ve Açıklığını Koruma ve Geliştirmeye İlişkin Tavsiye Kararı'nı da hatırlatan bu Karar, devletlerin kendi egemenlik alanlarındaki eylemlerinin diğer devletlerde bilgi erişimine gayrimeşru şekilde müdahale etmeme veya internet üzerindeki sınır aşan bilgi akışını olumsuz etkilememe sorumluluğuna dikkat çekmiştir.

1. Bilginin internet ortamında serbest ve sınır aşan akışına ilişkin ilkeler

1. Genel ilkeler

1.1. Devletler kendi egemenlik alanlarındaki herkesin AİHS'nin 10 ve 11. maddelerine uygun şekilde ifade özgürlüğü ile toplantı ve örgütlenme özgürlüğünü temin etmeye yönelik yükümlülüğü vardır. Bu yükümlülük aynı şekilde internet ortamı için de geçerlidir. Bu haklar ve özgürlükler cinsiyet, cinsel eğilim, ırk, renk, dil, din, politik veya başka fikir, ulusal veya sosyal köken, ulusal bir azınlıkla bağlantı, mülkiyet, doğum veya diğer statüler gibi gerekçelerle ayrımcılığa tabi tutulmaksızın temin edilmelidir.

1.2. Devletler, bilginin internet ortamındaki küresel serbest akışını korumalı ve geliştirmelidir. Devletler, kendi egemenlik alanlarında internet trafiğine müdahalelerinin AİHS'nin 10. maddesinde ve ilgili diğer uluslararası sözleşmelerde belirtilen meşru amaçlarla gerçekleştirilmesini

ve bilginin internet ortamında sınır aşan akışına gereksiz ve ölçüsüz etki oluşturmamasını temin etmelidir.

2. Gerekli özen ilkeleri

Devletler ulusal politikalarını değerlendirirken, geliştirirken veya uygularken bilginin internet ortamında sınır aşan serbest dolaşımına olumsuz etki edebilecek internet trafiğine müdahaleleri tanımlama ve bunlardan kaçınma yaklaşımı içinde gerekli özeni göstermelidir. Bu yaklaşım, müteakip hususların gözetilmesini gerektirmektedir.

- **Değerlendirme:** Bu tür bir etki doğurma imkânı olan düzenleyici veya diğer tedbirler, devletlerin, AİHS'de teminat altına alınan insan haklarına ve temel özgürlüklere saygı gösterme, bunları koruma ve geliştirme sorumluluğu kapsamında değerlendirilmelidir.

- Şeffaflık, öngörülebilirlik, hesap verebilirlik: Bilginin internet ortamında serbest dolaşımına etki edebilecek politikalar ve düzenleyici çerçeveler geliştirirken devletler, yukarıdaki değerlendirmelerin neticeleri dâhil şeffaflığı, uygulamalarının öngörülebilirliğini ve hesap verebilirliği temin etmelidir. Bilhassa, teklif edilen düzenleyici çerçeveler, uygun usuller takip edilerek ve kamusal görüş bildirmeye yeterli süre tanıyacak şekilde yayımlanmalıdır.

- Ölçülülük ve tedbirlerin gözden geçirilmesi: Devletler, hukuka aykırı olarak nitelendirilen içeriğin veya hizmetlerin engellenmesinin AİHS'nin 8, 10 ve 11. maddeleriyle uyumlu olmasını temin etmelidir. Bilhassa, internet ortamındaki hukuka aykırı içerik veya faaliyetlerle mücadele için devlet otoriteleri tarafından alınan tedbirler, devletin sınırlarının ötesinde gereksiz ve ölçüsüz etkilere sebebiyet vermemelidir. Devletler, en az müdahaleci ve en az zarar verici tedbirleri geliştirmeye çaba göstermeli ve bunları şeffaf ve hesap verebilir süreçler izleyerek uygulamalıdır. Devletler tarafından hayata geçirilen veya desteklenen tedbirlerin uygulamadaki etkililikleri ve hâlâ gerekli veya ölçülü olup olmadıkları düzenli şekilde gözden geçirilmelidir.

3. Öz düzenlemenin değeri

Devletler, uygun öz düzenleyici davranış kurallarının geliştirilmesini teşvik etmeli, kolaylaştırmalı ve desteklemelidir. Böylece tüm paydaşların, internet trafiğinin serbest akışı bağlamında AİHS'nin 8, 10 ve 11. maddelerine tam uyumlu şekilde özel hayata ve aile hayatına saygı, ifade özgürlüğü, toplantı ve örgütlenme özgürlüğü haklarına saygı göstermesi sağlanır.

4. Teknik en iyi uygulamaların teşviki

4.1. Devletler, ifade özgürlüğü, toplantı ve örgütlenme özgürlüğü ve özel hayat ile aile hayatına saygı hakkını gözeten, bilhassa internet trafiği üzerinde sınır aşan etkisi olan eylemlerin gerekliliğine ve tedbirlerin ölçülülüğüne ilişkin değerlendirmeleri içeren teknik en iyi uygulamaları hayata geçirirken çoklu paydaş iş birliğini teşvik etmelidir.

4.2. Devletler, ulusal politikalarının küresel internet mimarisine uyumlu olmasını sağlamalıdır. Bu yükümlülük, alan adı sistemine ilişkin en iyi uygulamalara bağlılığı da kapsar.

5. Uluslararası diyalog ve politika

5.1. Ulusal politikalar ve ticari faaliyetler bir devletin sınırlarının ötesindeki internet trafiğine müdahale niteliği taşırsa bu müdahaleden etkilenen tarafların bu devlet nezdinde itiraz etme imkânları olmayabilir. Devletler bu tarafların şikâyetlerinin dinlenilmesi ve çözüme kavuşturulmasını mümkün kılan yapılar ve usullerin mevcudiyetini temin etmelidir. Bu bağlamda devletler, ortak anlayışların, uluslararası standartların ve kuralların artan bir şekilde geliştirilmesi ve yarışan (çatışan) hukuk kurallarının ifade özgürlüğü ile bilgiye erişime uygulandığı durumlarda uygulanabilir hukuka ve yetkili yargı alanına ilişkin en iyi uygulamalara dâhil olmak için uluslararası diyalog içerisinde bulunmalıdır.

5.2. İnternete ilişkin uluslararası politika ve düzenlemelerin geliştirilmesi bağlamında devletler, internete bağlanabilirliği, bilhassa çeşitli ve çoğulcu bilginin mevcudiyeti ile erişilebilirliğini korumalı ve teşvik

edilmelidir; zira, bunlar bilginin internet ortamında serbest ve sınır aşan akışını etkilemektedir.

5.3. Uzak lokasyonlarda bilgiyi saklayan veya işleyen hizmetlere ilişkin olarak devletler, 108 sayılı Sözleşme ve AİHS'nin 8. maddesi doğrultusunda özel hayat ile aile hayatına saygı hakkı uyarınca kişisel verilerin korunması hakkını himaye etmelidir. Bu husus, AİHS'nin 10 ve 11. maddelerinde teminat altına alınan hakların eksiksiz kullanılması için de önemli arz eder. Devletler, bu tür hizmetlerle ilgili olarak yetki alanı ve uygulanabilir hukuka ilişkin soruları adresleyen ortak normlar, uygulamalar ve anlayışlar geliştirmek için uluslararası diyalog içerisinde bulunmalıdır.

XXIII. Ağ Tarafsızlığı Bağlamında İfade Özgürlüğü Hakkı ile Özel Hayat Hakkının Korunması ve Geliştirilmesine İlişkin Tavsiye Kararı (2016)

Ağ Tarafsızlığı Bağlamında İfade Özgürlüğü Hakkı ile Özel Hayat Hakkının Korunması ve Geliştirilmesine İlişkin Tavsiye Kararı, Bakanlar Komitesinin 13 Ocak 2016 tarihli 1244. Toplantısı'nda kabul edilmiştir.[292] Ağ tarafsızlığı, Avrupa Konseyinin gündeminde kalmaya devam etmektedir. Konu, ifade özgürlüğünden kişisel verilerin korunmasına kadar çok farklı hakları ve alanları ilgilendirmektedir. Nihayetinde bilgi toplumunda neredeyse tüm hakların kullanımı, erişilebilir ve kaliteli bir internet bağlantısının varlığını gerektirmektedir. Aynı doğrultuda, engelleme ve filtreleme ile içeriği önceliklendirme uygulamaları kullanıcıların internete olan güvenini zayıflatmaktadır.

Ağ tarafsızlığı ilkesi, internet trafiğinin ayrımcılık yapılmaksızın işlerliği, kullanıcıların bilgi alma ve yayma hakkı ile dilediği hizmeti kullanma hakkı üzerine kuruludur. AİHS'nin 10. maddesinin, bilginin sadece içeriğini değil mecrasını da güvence altına aldığını belirten Tav-

[292] **Avrupa Konseyi**, "*Recommendation CM/Rec(2016)1 of the Committee of Ministers to member States on protecting and promoting the right to freedom of expression and the right to private life with regard to network neutrality*", <https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c1e59>

siye Kararı, ağ tarafsızlığının, teknik yenilikçiliği ve ekonomik gelişmeyi desteklediğini belirtmiştir. Bu alandaki eski kararlarını tekrar hatırlatan Avrupa Konseyi, ağ tarafsızlığına ilişkin bir rehber yayımlamıştır.

Ağ tarafsızlığı rehberi

1. Genel ilkeler

1.1. İnternet kullanıcılarının kendi tercih ettikleri hizmetler, uygulamalar ve cihazlar aracılığıyla AİHS'nin 10. maddesine uygun şekilde bilgiyi alma ve yayma hakkı da dâhil ifade özgürlüğü vardır. Bu haklar, cinsiyet, ırk, renk, dil, din veya inanç, siyasi veya diğer görüş, ulusal veya sosyal köken, ulusal bir azınlıkla bağlantı, mülkiyet, doğum veya benzeri statü gibi nedenlerle bir ayrımcılık yapılmadan kullanılabilmelidir.

1.2. İnternet kullanıcılarının bilgiyi alma ve yayma hakkı engelleme, yavaşlatma, belirli içeriğe, hizmete, uygulamaya veya cihaza ilişkin internet trafiğinin veya özel bir anlaşma veya tarife esasına göre sağlanan hizmetlerle bağlantılı trafiğin bozulması veya ayrımcılığa tabi tutulması gibi sebeplerle kısıtlanmamalıdır.

1.3. İnternet kullanıcıları, koşulları internet erişim hizmet sağlayıcılarla akdettikleri sözleşmede belirlenen ve bu sözleşmenin internete erişimleri ile bilgiyi alma ve yayma haklarını etkileyecek tüm hususlara ilişkin özel ve yeterli bilgi sağlayan hükümleriyle internet bağlantısına sahip olmalıdır.

2. İnternet trafiğine eşit muamele

2.1. İnternet trafiğine, gönderen, alıcı, içerik, uygulama, hizmet veya cihaza bakılmaksızın kısıtlama veya müdahale olmadan eşit muamele edilmelidir. Ağ tarafsızlığı ilkesi bu tavsiye bağlamında böyle anlaşılmalıdır. Ağ tarafsızlığı ilkesi, altyapı veya internet bağlantısı için kullanılan ağa ve sinyalleri iletmek için kullanılan teknolojiye bakılmaksızın tüm internet erişim hizmetlerine uygulanır.

2.2. Bu kural, gerekli ve ölçülü olan şu tür internet trafik tedbirlerine halel getirmemektedir:

- Bir mahkeme kararının veya bir düzenleyici makamın kararının yerine getirilmesi;

- Ağın, ağ üzerinden sağlanan hizmetlerin ve son kullanıcıların terminal cihazının bütünlüğünün ve güvenliğinin muhafaza edilmesi;

- Ağ tıkanıklığının önlenmesi ve tıkanıklık olduğu zaman trafik yönetiminin optimize edilmesi.

3. Çoğulculuk ve bilginin çeşitliliği

3.1. İnternet hizmet sağlayıcıları, kendi ürünleriyle rekabet içerisinde olan başka içerik, uygulama ve hizmet sağlayıcılarının trafiğine ayrımcılık yapmamalıdır. Bu, trafik yönetim kararlarının, işletmecinin içeriğe ilişkin karar alma süreçlerinden Bakanlar Komitesinin Medya Yoğunlaşması Bağlamında Demokraside Medyanın Rolünün Korunmasına İlişkin Deklarasyon'unun (2007) ruhuna uygun olarak katı şekilde ayrıştırılmasını gerektirmektedir.

3.2. İnternet hizmet sağlayıcıları ile içerik, uygulama ve hizmet sağlayıcıları arasındaki anlaşmalar temelinde tercihli trafik muamelesine, ağ tarafsızlığı ilkesinin bir istisnası olarak sadece kullanıcıların bilgiye erişim, bilgiyi kullanma ve yayma haklarına ilişkin yeterli koruma mekanizmaları mevcutsa izin verilmelidir. Tercihli trafik muamelesi bilhassa kullanıcıların internet erişiminin ekonomikliğini, performansını veya kalitesini düşürmemeli veya etkilememelidir. İnternet kullanıcıları, tercihli trafik muamelesinin olmadığı bir internet bağlantısı konusunda gerçek bir tercih imkânına sahip olmalıdır. Kullanıcılar, bu tür bir muamelenin bilgiye, kamuya açık çeşitli ve çoğulcu içeriğe, uygulamalara ve tercih edecekleri hizmetlere erişim, bunları kullanma ve yayma imkânlarına olan etkisi konusunda bilgilendirilmelidir.

3.3. Fiziki internet bağlantısı internet trafiği ve diğer hizmetler arasında paylaştırılmışsa devletler, internet hizmet sağlayıcılara kamu yararı amacını karşılayacak içeriğin taşınması için makul, şeffaf ve ölçülü yükümlülükler getirebilir.

4. Mahremiyet

4.1. İnternet trafik yönetim tedbirleri, bu rehberin ikinci bölümünde belirtilen amaçlara ulaşmak için gerekli ve ölçülü olduğu sürece kişisel veri işlemeyi içermelidir. Bu tedbirler, 108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'nin 8. maddesinin ikinci fıkrası ile özel hayat ve kişisel verilerin korunmasına ilişkin uygulanabilir mevzuata uygun olmalıdır.

4.2. Haberleşmenin içeriğini değerlendirme kapasitesi olan internet trafik yönetim teknikleri, özel hayat ve aile hayatına saygı hakkına bir müdahale niteliğindedir. Bu sebeple, bu tür bir kullanım AİHS'nin 8. maddesiyle tam uyumlu olmalı, özel hayat ve kişisel verilerin korunmasına ilişkin mevzuata uygunluk yönünden test edilmeli ve her bir üye devletin yetkili makamları tarafından mevzuata uyum bağlamında gözden geçirilmelidir.

5. Şeffaflık

5.1. İnternet hizmet sağlayıcıları; içeriğe, uygulamalara veya hizmetlere erişmelerine ve bunları yaymalarına etki edebilecek trafik yönetimi uygulamaları konusunda kullanıcıları sarih, tam ve kamuya açık bilgilerle donatmalıdır. İnternet kullanıcıları, internet hizmet sağlayıcılarından internet trafik yönetimi ve internet hızlarına ilişkin bilgi alabilmelidir.

5.2. Her bir devletin yetkili makamları internet trafik yönetimi uygulamalarını takip etmeli ve raporlamalıdır. Raporlar açık ve şeffaf şekilde hazırlanmalı ve kamuyla ücretsiz olarak paylaşılmalıdır.

6. Hesap verebilirlik

6.1. İnternet hizmet sağlayıcıları, internet kullanıcılarının yukarıdaki hükümlerde belirtilen ilkelerin ihlali iddiasıyla yaptıkları şikâyetlere makul sürede yanıt verecek uygun, sarih, açık ve etkili prosedürleri uygulamaya koymalıdır. İnternet kullanıcılarının, konuyu her bir üye devletin yetkili makamlarının doğrudan dikkatine sunabilme imkânı ve sorunun vakitlice çözülmesine ilişkin hakkı olmalıdır.

6.2. Devletler, politika çerçevelerinde internet hizmet sağlayıcılarının ağ tarafsızlığı ilkesine saygı gösterme konusundaki hesap verebilirliğini temin etmelidir. Hesap verebilirlik ayrıca ağ tarafsızlığına ilişkin şikâyetlere cevap verecek uygun mekanizmaların varlığını gerektirir.

XXIV. İnternet Özgürlüğüne İlişkin Tavsiye Kararı (2016)

İnternet Özgürlüğüne İlişkin Tavsiye Kararı, Avrupa Konseyi Bakanlar Komitesinin 13 Nisan 2016 tarihli 1253. Toplantısı'nda kabul edilmiştir.[293] Tavsiye Kararı, AİHS'nin hem online hem de offline ortama uygulandığı ve Avrupa Konseyine üye devletlerin, insan haklarına saygı göstermek, onları korumak ve geliştirmek için hem negatif hem de pozitif yükümlülükleri bulunduğu vurgusuyla başlamaktadır.

İnternet özgürlüğü; insan hakları ve temel özgürlüklerin internet ortamında AİHS'ye ve Kişisel ve Siyasal Haklar Uluslararası Sözleşmesi'ne uygun şekilde icrası, kullanılması ve korunması olarak tanımlanmıştır. Tavsiye Kararı ulusal, bölgesel veya küresel tüm internet yönetişimi düzenlemelerinin, internet özgürlüğü anlayışı üzerine inşa edilmesi gerektiğini belirtmektedir. Keza devletlerin, internet özgürlüğü için uygun ortamı hazırlamakla yükümlü olduğu da ifade edilmiştir.

Tavsiye Kararı, Avrupa Konseyi üye devletlerinin internet özgürlüğüne ilişkin düzenlemelerini ve uygulamalarını ölçümlemek adına ayrıca bir dizi ölçü ve referans göstergeler ortaya koymuştur.

İnternet özgürlüğü göstergeleri

İnternet özgürlüğü, insan haklarının ve temel özgürlüklerin internet ortamında AİHS'ye uygun şekilde icrası, kullanılması ve korunmasıdır. Bu internet özgürlüğü göstergeleri; ifade özgürlüğü, toplantı ve örgütlenme özgürlüğü, özel yaşam hakkı ve etkili başvuru hakkına odaklan-

[293] **Avrupa Konseyi**, "*Recommendation CM/Rec(2016)5 of the Committee of Ministers to member States on Internet freedom*", <https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016806415fa>

maktadır. Göstergeler, mevcut ve resmîleşmiş insan hakları standartları ve icra mekanizmalarının üzerine inşa edilmiştir. İnternet özgürlüğüne kapsamlı bir yaklaşım için tüm göstergeler, Avrupa Konseyi üye devletlerinde internet özgürlüklerinin niteliksel ve objektif değerlendirilmesi ve raporlanmasına rehberlik etmeyi amaçlamaktadır. Bu göstergeler, ülkeleri birbirleriyle kıyaslamanın aracı olarak ya da internet özgürlükleri seviyelerini sınıflandırmak için tasarlanmamıştır.

1. İnternet özgürlüğü için uygun ortamın sağlanması

1.1. İnsan hakları ve temel özgürlüklerin internet ortamında korunması AİHS'ye uygun şekilde kanunla güvence altına alınır.

1.2. İnsan hakları ve temel özgürlüklerin kullanmasına herhangi bir devlet müdahalesi AİHS ile uyumludur.

1.3. İnternetle alakalı hukuki düzenlemeler ve politikalar, henüz tasarı aşamasındayken insan hakları ve temel özgürlüklerin kullanılmasına olası etkileri bağlamında değerlendirilir.

1.4. İnternetle alakalı hukuki düzenlemeler ve politikalar devlet makamları tarafından kapsayıcı ve şeffaf şekilde, özel sektör, sivil toplum, akademi ve teknik topluluk dâhil tüm paydaşların katılımı temin edilerek geliştirilir.

1.5. İnternet konularında düzenleyici veya farklı bir yetkisi olan herhangi bir devlet organı, faaliyetlerini politik veya ticari müdahaleden uzak şekilde ve şeffaf olarak sürdürür; internet özgürlüğünü korur ve geliştirir.

1.6. Devlet, bireyleri siber suçlara karşı etkili ceza adaleti veya diğer tedbirlerle korur. Bu tür tedbirler özel yaşama, ifade özgürlüğüne, barışçıl şekilde toplantı ve örgütlenme özgürlüğüne müdahale oluşturma riski doğurursa kötüye kullanımı önleyecek mekanizmalara ve koruyucu tedbirlere tabi tutulur. Bu tedbirler AİHS'nin 8, 10 ve 11. maddeleriyle uyumludur. Özellikle erişilebilir, belirli, açık ve öngörülebilir bir yasa ile düzenlenir; meşru bir amaç güder; demokratik bir toplumda gerekli ve ölçülüdür; etkin tazmin mekanizmalarına imkân verir.

1.7. Devlet, "Birleşmiş Milletler İş Dünyası ve İnsan Haklarına Dair Rehber İlkeler: Birleşmiş Milletler 'Koruma, Saygı Gösterme ve Telafi Edici Çözüm Üretme' Çerçevesinin Uygulanması" için politikalar geliştirir ve tedbirler alır.

1.8. Devlet, bilinçli karar alabilme yeteneklerini geliştirmek ve başkalarının hak ve özgürlüklerine saygı göstermelerini temin etmek için kullanıcılara medya okuryazarlığı ve dijital okuryazarlık programları sunar. Devlet eğitsel, kültürel, bilimsel, akademik ve diğer içeriklere erişimi ve bunların kullanımını destekler.

2. İfade özgürlüğü hakkı

2.1. İnternete erişim özgürlüğü

2.1.1. İnternet, ayrımcılık yapılmaksızın nüfusun tüm grupları için elde edilebilir, erişilebilir ve makul fiyatlıdır.

2.1.2. Halkın, kamu idareleri (internet erişim noktaları), eğitim kurumları ve özel kişiler tarafından desteklenen alanlarda (evrensel topluluk hizmeti) internete erişimi vardır.

2.1.3. Devlet; geliri düşük olanlar, kırsal veya coğrafi olarak uzak alanlarda yaşayanlar ve engelliler gibi özel ihtiyaçları olanların internete erişimi için makul tüm tedbirleri alır.

2.1.4. AİHS'nin 10. maddesiyle uyumlu kısıtlamalar hariç, internete erişimde genel, ülke çapında bir kısıtlama yoktur.

2.1.5. Devlet, mevzuatta ve uygulamada, kişilerin internet bağlantısını kesmenin, genel bir ilke olarak, ifade özgürlüğü hakkına yönelen ölçüsüz bir kısıtlama olduğunu kabul eder.

2.1.6. Hapishane gibi kurumlar dâhil herhangi bir internet erişim kısıtlaması, AİHS'nin ifade özgürlüğünün kısıtlanmasına ilişkin kanunla öngörülme, meşruluk ve ölçülülük koşulları ile devletin ifade özgürlüğünü korumaya yönelik pozitif yükümlülüğüne uygun olmalıdır.

2.1.7. İnternet erişimine ilişkin kısıtlayıcı tedbirler uygulanmadan önce, bir mahkeme veya bağımsız idari bir makam internet bağlantısını kesmenin, ulaşılmaya çalışılan meşru amaç için en az müdahaleci tedbir olduğuna karar verir. Kısıtlayıcı tedbirin devam eden gerekliliği, bu makamlar tarafından sürekli bir şekilde değerlendirilir. Bu koşullar, kullanıcıların internet hizmetleri karşılığında ödeme yapmaması durumlarına uygulanmaz.

2.1.8. Kısıtlayıcı tedbirler uygulandığında ilgili kişinin bir mahkeme veya kararları yargısal denetime tabi bağımsız bir idari otorite önünde AİHS'nin 6. maddesine uygun bir hukuki hak arama hakkı vardır.

2.2. Düşünce özgürlüğü ve bilgi alma ve verme hakkı

2.2.1. Devlet makamları veya özel sektör aktörleri tarafından bir internet platformunu (sosyal medya, sosyal ağlar, bloglar veya başka diğer web siteleri) veya bilgi ve haberleşme teknolojileri (BT) araçlarını (anlık mesajlaşma ve diğer uygulamalar) engelleyen veya erişimi başka şekilde kısıtlayan her türlü tedbir veya devlet makamlarının bu tür eylemlere yönelik talepleri, kısıtlamaların kanunla öngörülme, meşruluk ve ölçülülük koşullarına uygun olmasını öngören AİHS'nin 10. maddesiyle uyumlu olmalıdır.

2.2.2. Devlet makamları veya özel sektör tarafından alınan internet içeriğini engelleme, filtreleme veya kaldırmaya yönelik her türlü tedbir veya bu tür bir işlem için devlet makamları tarafından gerçekleştirilen her türlü talep, kısıtlamaların kanunla öngörülme, meşruluk ve ölçülülük koşullarına uygun olmasını öngören AİHS'nin 10. maddesiyle uyumlu olmalıdır.

2.2.3. İnternet hizmet sağlayıcıları, genel bir ilke olarak, internet trafiğine eşit ve gönderen, alıcı, içerik, uygulama, hizmet veya cihaz temelli ayrımcılık yapmayacak şekilde muamele eder. İnternet trafik yönetim tedbirleri, AİHS'nin 10. maddesine uygun şekilde üstün kamusal yarara ulaşmak için şeffaf, gerekli ve ölçülü olmalıdır.

2.2.4. İnternet kullanıcılarının veya ilgili diğer tarafların, internete erişim, içerik veya bilgiyi alma ve yayma imkânlarını sınırlamaya yönelik işlemlere karşı AİHS'nin 6. maddesine uygun şekilde mahkemelere erişimi vardır.

2.2.5. Devlet, bilgi alma ve yayma özgürlüğüne uyguladığı engellenen veya içerdiği bilgiler kaldırılan web sitelerini göstermek gibi kısıtlamalar hakkında bunların hukuki dayanağı, gerekliliği ve gerekçesi, bu işleme izin veren mahkeme kararı ve bu karara itiraz hakkını içerecek şekilde kamuoyunu zamanında ve uygun şekilde bilgilendirmelidir.

2.3. Medya özgürlüğü

2.3.1. İnternette faaliyet gösteren medyanın editoryal bağımsızlığı hukuken, politik olarak ve uygulamada güvence altına alınmıştır. Haberlerine bilgi ekleme veya bunlardan bilgi çıkarmaya yahut belirli bir yayın politikası izlemeye yönelik bir baskıya maruz bırakılamazlar.**2.3.2.** Medya, genel işletme kaydı dışında, internet ortamında veya blog olarak faaliyet gösterebilmek için hükûmetten veya devlet makamlarından izin veya lisans almak zorunda değildir.

2.3.3. İnterneti kullanan gazeteciler ve diğer medya aktörleri, devlet tarafından tehdit veya taciz edilmemelidir. Cezalandırılma, taciz veya saldırı korkusuyla kendilerine otosansür uygulamamalıdır.

2.3.4. Gazetecilerin ve diğer medya aktörlerinin kaynaklarının gizliliği hukuken korunmaktadır ve uygulamada buna saygı gösterilmelidir.

2.3.5. Medya web siteleri ve yeni medya aktörlerinin web siteleri siber saldırılar veya diğer engelleyici eylemlerden (örneğin, hizmet dışı bırakma saldırıları) etkilenmemelidir.

2.3.6. Gazeteciler ve yeni medya aktörlerine yönelik tehditler ve suçlar hızlıca ve etkin olarak soruşturulmalıdır. Bir cezasızlık ortamı oluşmamalıdır.

2.4. Kısıtlamaların kanuniliği, meşruluğu ve ölçülülüğü

2.4.1. İnternet ortamında ifade özgürlüğüne yönelik herhangi bir kısıtlama AİHS'nin 10. maddesindeki gerekliliklere uygun olmalıdır. Bu kısıtlamalar:

- Bireylerin davranışlarını düzenlemelerine imkân verecek şekilde erişilebilir, açık, müphem olmayan ve yeterince belirli olan kanunlarda öngörülmüştür. Kanun, kısıtlamanın kapsamına ilişkin katı bir kontrol ve herhangi bir kötüye kullanımı önlemek için yargısal denetimi temin eder. Kanun, sınırlamaların uygulanması konusunda kamu otoritelerine verilen takdir yetkisinin kapsamını ve kullanım tarzını yeterince açık şekilde gösterir.

- AİHS'nin 10. maddesinde tahdidî olarak belirtilen şekilde meşru bir amaç güder.

- Demokratik bir toplumda gereklidir ve ulaşılmaya çalışılan amaçla orantılıdır. Kısıtlama için ivedi bir sosyal ihtiyaç vardır ve bu kısıtlama bir mahkeme veya yargısal denetime tabi olan bağımsız bir idari makam tarafından uygulanmıştır. Karar belirli bir hedefe yönelmeli ve spesifik olmalıdır. Ayrıca, kısıtlamanın etkinliği ve aşırı engelleme risklerine göre yapılacak bir değerlendirmeye dayanmalıdır. Bu değerlendirme, kısıtlamanın internet içeriğine veya belirli tip içeriğe erişimi ölçüsüz engelleyip engellemeyeceğini ve ayrıca belirtilen meşru amaca ulaşmak için en az kısıtlayıcı araç olup olmadığını içermelidir.

2.4.2. Devlet, mevzuatında internet ortamında ifade özgürlüğüne ölçüsüz kısıtlamalar dayatmaz. Hakarete ilişkin düzenlemeler spesifiktir ve uygulama kapsamlarına göre dar şekilde tanımlanır. Bu düzenlemeler, kamusal tartışmaları veya devlet organlarının eleştirilmesini yasaklamaz ve aşırı ceza veya ölçüsüz tazminat tutarları yahut hukuki giderler uygulamaz. Hapis gibi sert yaptırımlar, yalnızca başkalarının temel hakları şiddete veya nefrete teşvik gibi durumlarda ciddi olarak ihlal edildiği zaman uygulanır.

2.4.3. Nefret söylemini düzenleyen veya kamu düzenini, genel ahlakı, küçükleri, ulusal güvenliği, devlet sırlarını koruyan yasalar ve veri koruma yasaları kamusal tartışmaları yasaklayacak şekilde uygulanmaz.

Bu tür yasalar, ifade özgürlüğü kısıtlamalarını sadece acil bir kamu yararı durumunda uygular, kamu yararını karşılamak için mümkün olduğunca dar tanımlanır ve orantılı yaptırımlar içerir.

3. Barışçıl şekilde toplanma ve örgütlenme özgürlüğü

3.1. Bireyler, bir araya gelmek ve birlikler kurmak, bunların amaçlarını belirlemek, işçi sendikaları kurmak ve uluslararası standartlarla uyumlu kanunların çizdiği sınırlar içinde faaliyetlerde bulunmak üzere sosyal medya ve diğer BT uygulamaları gibi internet platformlarını kullanmakta özgürdür.

3.2. Birlikler, ifade özgürlüklerini kullanmak, siyasal ve kamusal tartışmalara katılmak için interneti kullanmakta özgürdür.

3.3. Bireyler, barışçıl şekilde toplanmak amacıyla organize olmak için sosyal medya ve diğer BT uygulamaları gibi internet platformlarını kullanmakta özgürdür.

3.4. Barışçıl şekilde toplanma hakkının icrası bağlamında uygulanan ve internet platformlarının engellenmesi veya kısıtlanmasını netice veren devlet tedbirleri AİHS'nin 11. maddesiyle uyumlu olmalıdır.

3.5. İnternet bağlamında barışçıl şekilde toplanma özgürlüğü ve örgütlenme özgürlüğünün icrasına ilişkin herhangi bir kısıtlama AİHS'nin 11. maddesiyle uyumlu olmalıdır. Sınırlamalar:

- Bireylerin davranışlarını düzenlemelerine imkân verecek şekilde erişilebilir, açık, sarih ve yeterince belirli olan kanunlarda öngörülür.

- AİHS'nin 11. maddesinde tahdidî olarak sayılmış meşru bir amaç güder.

- Demokratik bir toplumda gerekli ve ulaşılmaya çalışılan meşru amaçla orantılıdır. Kısıtlama için acil bir sosyal ihtiyaç olmalıdır. Toplanma özgürlüğü ve örgütlenme özgürlüğünün kullanımı ile tüm toplumun menfaatleri arasında adil bir denge gözetilmelidir. Şayet daha az müdahaleci bir tedbir aynı amaca erişmeyi sağlıyorsa o uygulanmalıdır. Kısıtlama

dar bir şekilde yorumlanmalı ve uygulanmalı; toplantı ve örgütlenme özgürlüğünün özüne zarar vermemelidir.

4. Özel hayat ve aile hayatı hakkı

4.1. Kişisel verilerin korunması

4.1.1. Özel hayat ve aile hayatı hakkı, AİHS'nin 8. maddesine uygun şekilde güvence altına alınır. Bu hakka getirilen herhangi bir kısıtlama AİHS'nin 8. maddesinde tahdidî olarak sayılan meşru amaçlardan birini gütmeli, demokratik bir toplumda gerekli ve hedeflenen meşru amaçla orantılı olmalıdır.

4.1.2. Mevzuat, tüm kişisel verilerin AİHS'nin 8. maddesine ve Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'ni (Sözleşme No. 108) onaylayan devletlerde bu Sözleşme'ye uygun şekilde korunduğunu garanti etmelidir.

4.1.3. Kişisel veriler, hukuka uygun şekilde (veri süjesinin açık rızasıyla veya kanuna dayalı olarak) meşru amaçlarla, bu amaçlar aşılmadan, doğru ve güvenli şekilde işlenir. Bu koşullar ayrıca profillemeye (bir birey hakkında onun kişisel tercihlerini, davranışlarını ve tavırlarını tanımlamak, analiz ve tahmin etmek amacıyla bilgi toplayan ve bu bilgiyi kullanan otomatik kişisel veri işleme tekniklerine) de uygulanır.

4.1.4. Bireyler, kendilerini esaslı şekilde etkileyen ve görüşleri dikkate alınmaksızın tamamen otomatik veri işlemeye dayalı bir karara maruz bırakılamazlar. Her bir bireyin, talebi hâlinde, kişisel verilerinin işlenmesine ve bunun dayandığı sebebe ilişkin bilgi alabileceği; işlemeye itiraz edebileceği; talebi hâlinde, kişisel verinin düzeltilmesini veya silinmesini isteyebileceği; veri işlemeye veya profillemeye rıza verebileceği, itiraz edebileceği veya rızasını geri alabileceği etkili süreçler mevcut olmalıdır. Bu haklara saygı duyulmadığında bireylerin işletebilecekleri etkili bir itiraz imkânı bulunmalıdır. Kişisel verileri korumaya yönelik hukuki çerçeveler, bilgiye erişim ve ifade özgürlüğüne ilişkin yeterli güvenceleri içermelidir.

4.1.5. Mevzuat, kamusal ve özel kuruluşların kişisel verileri işlemeye ilişkin sorumluluklarını tanımlar.

4.1.6. Tam bağımsız ve tarafsız hareket eden bir denetleme makamı, kişisel verilerin korunmasına ilişkin hukuki çerçeveye uyumluluğu temin eder.

4.1.7. Devlet, hukuken veya uygulamada, anonimliği, takma adları, özel haberleşmenin gizliliğini veya şifreleme teknolojilerinin kullanımını yasaklamaz. Anonimlik ve haberleşmenin gizliliğine müdahale, AİHS'nin 8. maddesindeki kanunilik, meşruluk ve orantılılık şartlarına uygun olmalıdır.

4.2. Gözetim

4.2.1. Kamu otoriteleri (güvenlik hizmetleri gibi) tarafından uygulanan gözetim tedbirleri AİHS'nin 8. maddesindeki gerekliliklerle uymalı; etkili, bağımsız ve tarafsız bir denetime tabi tutulmalıdır.

4.2.2. Gözetim tedbirleri erişilebilir, açık, belirli ve öngörülebilir bir kanuni dayanağa uygun şekilde gerçekleştirilmelidir. Kanun, kamu otoriteleri tarafından kullanılacak takdir yetkisine yönelik koruma mekanizmalarını içermeli ve şunları yeterli açıklık ve netlikte tanımlamalıdır:

- Gözetim tedbirlerine mahal verebilecek ihlallerin niteliği;

- Gözetim tedbirlerini uygulayan yetkili makamlar, bu tür makamlara verilen takdir yetkisinin kapsamı ve bu takdir yetkisinin tedbirin ulaşmaya çalıştığı meşru amaç bakımından kullanım tarzı;

- Gözetim tedbirlerine tabi tutulması muhtemel bireylerin kategorileri;

- Gözetim tedbirlerini uygulamaya ilişkin zaman sınırlamaları;

- Gözetim tedbirleri neticesinde elde edilen verinin incelenmesi, kullanılması ve muhafazasına ilişkin usuller;

- Gözetim tedbirleri neticesinde elde edilen verinin diğer taraflara iletimi esnasında alınacak önlemler ve iletim sırasında veri güvenliğini sağlamak için uygulanabilecek tedbirler;

- Gözetim tedbirlerinden elde edilen verinin yok edilmesi ve silinmesine yönelik şartlar;

- Gözetim tedbirlerini denetlemekten sorumlu organlar.

4.2.3. Gözetim tedbirleri, AİHS'nin 8. maddesinde tahdidî olarak sayılan meşru bir amaç güder, demokratik bir toplumda gerekli ve güdülen meşru amaçla orantılıdır.

4.2.4. Devlet makamlarınca doğrudan veya özel sektör teşekküleriyle iş birliği içerisinde uygulanan gözetim tedbirleri, kanunla kurulmuş bağımsız ve tarafsız bir mahkeme veya hem söz konusu tedbirleri uygulayan makamlardan hem de yürütme organından bağımsız başka bir devlet makamı tarafından onaylanmalıdır.

4.2.5. Devlet makamlarınca doğrudan veya özel sektör teşekküleriyle iş birliği içerisinde uygulanan gözetim tedbirleri, şifreleme sistemlerini ve haberleşme altyapısını zayıflatacak faaliyetler (güvenlik, bilgi ve iletişim sistemlerindeki yerleşik kusurlar ve arka kapılar) içeremez.

4.2.6. Gözetim tedbirleri, adli bir makam tarafından güvence altına alınan etkili bir incelemeye veya söz konusu tedbirleri uygulayan makamlar ile yürütmeden bağımsız ve tarafsız bir başka devlet organının denetimine tabidir.

4.2.7. Mevzuat, bir denetim organının, kendisine verilen görevin ifasıyla ilgili tüm bilgiye erişim hakkını, bilgi sınıflandırma düzeyine bakılmaksızın, teminat altına alır. Denetim organının bilgiye erişimi, yabancı kuruluşlar tarafından sağlananlar dâhil kamu otoritelerince tutulan ilgili tüm bilgileri kapsar.

4.2.8. Denetim organları yetkilerini, gizli bilgiler ve kişisel verileri araştırma ve kullanma dahil profesyonelce ve tam olarak kanunla verilen amaçlar doğrultusunda kullanır; aynı zamanda bilginin bu tür organların

yetki alanı dışında kalan herhangi bir amaçla kullanılmasından ve ifşa edilmesinden korur.

4.2.9. Denetim organları, kamu otoriteleri tarafından alınan gözetim tedbirlerinin insan haklarına uygunluklarını yetkileri dâhilinde titizlikle inceler. Bu incelemeye, yabancı makamlarla iş birliği içinde bilgi değişimi veya ortak operasyonlar marifetiyle alınan tedbirler de dâhildir.

4.2.10. Adli makamlar ve denetim organları, gözetim tedbirlerinin hukuka aykırı olduğunu tespit ettiğinde bu tedbirleri kaldırma veya durdurma yetkisini ve bu tür tedbirler kullanılarak elde edilen bilginin silinmesini talep etme yetkisini haizdir.

4.2.11. Gözetim tedbirlerini uygulayan kamu otoriteleri ve denetim organları bilgi edinme yasalarının alanından muaf değildir. Bilgi sağlamamaya ilişkin kararlar olay bazında değerlendirilir, uygun şekilde gerekçelendirilir ve bağımsız bilgi veya veri koruma yetkilisinin denetimine tabidir. Denetim organları dönemsel raporlar ve soruşturma raporlarının bilgilendirici versiyonlarını kamunun erişimine sunar.

5. Başvuru yolları

5.1. Devlet, bireylerin online insan hakları ihlallerine ilişkin iddialarının bağımsız şekilde karara bağlanmasını sağlayan adli veya idari prosedürlere erişimini AİHS'nin 6. maddesine uygun şekilde temin eder.

5.2. Devlet, AİHS'nin 13. maddesine uygun şekilde etkili başvuru hakkı sağlar. Bu hak, etkili yargı dışı mekanizmalar, idari ve ulusal insan hakları kurumları gibi çözüm bulunmasını sağlayan diğer yolları kapsar. Bireyler, etkili bir çözüm ararken hukuki, usuli, finansal veya diğer pratik engellerle karşılaşmamalıdır.

5.3. Devlet, birinci sorumlu varlık olarak, özel sektör aktörleri tarafından gerçekleştirilen internete ilişkin insan hakları ihlallerine karşı koruma sağlamak ve etkilenenlerin etkin bir hak arama yoluna erişimini temin etmek için uygun adımları atar.

5.4. Devlet, faaliyetleri kapsamında tüm özel sektör aktörlerinin internet bağlamında insan haklarına saygı göstermesi için politikalar ve tedbirler uygular. Bilhassa internet ortamında insan hakları ve temel özgürlükleri olumsuz etkilenebilecek bireylerin, şikâyetlerini erkenden ve doğrudan iletebilecekleri etkin şikâyet mekanizmaları kurar. Mekanizmalar meşru (şikâyet süreçlerinin adil bir şekilde yürütülmesini temin eden güveni sağlar), erişilebilir (ilgililer tarafından bilinir, erişimin önünde engel yoktur), öngörülebilir (her bir adım için belirtici zaman dilimi, süreç türlerine ilişkin netlik ve muhtemel sonuç içeren açık ve bilinen bir usul ve uygulamayı takip etme imkânı veren araçlar sağlar), adil (bilgi kaynaklarına makul erişim, bir şikâyet sürecine dâhil olmak için gerekli tavsiye ve uzmanlık), şeffaf (bir şikâyetin sürecine ilişkin tarafları sürekli bilgilendirir) ve AİHS'nin 13. maddesiyle uyumludur.

[**1**] Bu Tavsiye Kararı kabul edilirken Rusya Federasyonu'nun Daimî Temsilcisi, İç Tüzük'ün Bakanlar Komitesi toplantılarına ilişkin 10.2c maddesine uygun şekilde, Rus Hükûmetinin, ulusal düzeyde uygulanması için metodolojiye atıf yapılmasından ötürü Tavsiye Kararı'na uyup uymama konusundaki hakkını saklı tuttuğunu beyan etmiştir.

XXV. İnternet Aracı Platformlarının Rolleri ve Sorumluluklarına İlişkin Tavsiye Kararı (2018)

İnternet Aracı Platformlarının Rolleri ve Sorumluluklarına İlişkin Tavsiye Kararı, Bakanlar Komitesinin 7 Mart 2018 tarihli 1309. Toplantısı'nda kabul edilmiştir.[294] Tavsiye Kararı, AİHS'nin hem online hem de offline temel hak ve özgürlüklere uygulanacağına ilişkin klasik hâline gelen vurguyla başlamaktadır. Aynı doğrultuda, internetin temel hak ve özgürlüklerin kullanımına katkısı ve kişisel veriler ile mahremiyetin korunmasının önemi hatırlatılmıştır.

[294] **Avrupa Konseyi**, "*Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries*", <https://rm.coe.int/1680790e14>

Tavsiye Kararı'na göre, yaygın, çeşitli ve hızla değişen nitelikte "internet aracıları" olarak adlandırılan oyuncular, çeşitli işlevler ve hizmetler sunmak ve sağlamak suretiyle internette gerçek ve tüzel kişiler arasındaki etkileşimi kolaylaştırmaktadır. Bu tür aktörlerin bazıları kullanıcıları internete bağlamakta, bilgi ve verinin işlenmesine imkân tanımakta veya kullanıcılar tarafından oluşturulan içerikler dâhil web tabanlı hizmetleri barındırmaktadır. Bazıları bilgiyi toplamakta ve arama yapılmasına imkân vermekte, üçüncü taraflarca tasarlanan ve/veya işletilen içerik ve hizmetlere erişim sağlamakta, bunları barındırmakta ve indekslemektedir. Bazıları ise görsel-işitsel hizmetler dâhil mal ve hizmetlerin satışını kolaylaştırmakta ve ödeme dâhil başka ticari işlemlere imkân tanımaktadır.

Tavsiye Kararı'na göre, aracılar paralel olarak başka fonksiyonlar da yerine getirebilir: Kişisel veriyi otomatik işlemek suretiyle içeriğe moderasyon sağlayabilir, içeriği derecelendirebilir ve muhtelif kontrol türleri uygulayarak kullanıcıların bilgiye erişimini medyaya kıyasen etkileyebilir veya bu tür yayıncılara benzer fonksiyonlar yerine getirebilir. Keza, aracı hizmetler, örneğin platformlarında kullanıcılar tarafından oluşturulan içeriklere alan sağlamak suretiyle geleneksel medya tarafından da sunulabilir ve bu fonksiyonu bağlamında aynı kuruluşun tabi olduğundan farklı bir düzenleyici kurallara tabi olabilir.

Aracı platformları tanımladıktan sonra Tavsiye Kararı, hukukun üstünlüğünün hem insan haklarının korunması ve geliştirilmesi hem de çoğulcu ve katılımcı demokrasi için bir ön koşul olduğunu belirtmiştir. Karar'a göre, çeşitli ağ etkileri ve birleşmeler daha az sayıda ve daha büyük teşebbüslerin oluşmasına yol açmış, bu teşebbüsler küçük aracılar veya girişimlerin fırsatlarını tehdit edecek şekilde pazara hâkim olmuş ve onları etki edecek konuma ve hatta kamusal iletişimin ana biçimini kontrol edecek bir noktaya getirmiştir. Tavsiye Kararı'na göre, çevrim içi ifadenin baş aktörü olarak bu tür aracı platformların gücü, bunların rollerinin ve insan hakları üzerindeki etkilerinin, keza ilgili görev ve sorumluluklarının açıklığa kavuşturulmasını zorunlu kılmaktadır. Aracı platformların hizmetlerinin ve altyapılarının suçlular tarafından kötüye kullanılması riski de buna dâhildir.

Tavsiye Kararı, dijital alana erişim ve bu alanın yönetimi için medya ve bilgi okuryazarlığı becerilerinin geliştirilmesinin önemli olduğunu vurgulayarak bu konuda devletlere çağrıda bulunmuştur. Tavsiye Kararı'na göre, aracılar tarafından veya onların vasıtasıyla yönetilen ve sağlanan hizmetlere ilişkin düzenleyici çerçeveler çeşitli, çok katmanlı ve sürekli gelişim hâlindedir. Devletler, özel kişilerin önemli kamu hizmeti değeri olan hizmetleri sunmada kritik bir rol oynadığı bir ortamı düzenlemenin karmaşıklığı ve zorluğuyla karşı karşıya kalmaktadır. Bu görev, internet ve ilgili hizmetlerin küresel niteliğiyle, aracıların çeşitliliğiyle, internet trafiğinin hacmiyle ve bu trafiğin üretilme ve işlenme hızıyla daha fazla karmaşık hâle gelmektedir. Aracı platformların farklı ülkelerde faaliyet göstermesi veya kullanılmasının (bulut bilişim dâhil) bir neticesi olarak, bu tür aracıların faaliyetleri bazı durumlarda farklı yargı yetkisi alanlarının birden fazla -ve kimi zaman çatışan- kanunları altında etki doğurmaktadır.

Tavsiye Kararı'na göre internet aracıları, genellikle hizmet koşulları ve topluluk standartları şeklinde, içerik kısıtlama politikalarını da içeren kendi kurallarını geliştirmektedir. Ayrıca, aracılar kullanıcıdan ve kullanıcı hakkında çok yüksek oranda bilgi ve veri toplamakta, üretmekte, saklamakta ve işlemektedir. Bu faaliyetlerle, diğer hakların yanında, kullanıcıların mahremiyet ve ifade özgürlüğü haklarına müdahale edilebilmektedir. Yine Tavsiye Kararı'na göre, etkili raporlama ve şikâyet mekanizmaları bulunmayabilmekte, şeffaflık ve etkinlik düzeyleri yetersiz kalabilmekte veya bunlar sadece otomatik şekilde sunulabilmektedir.

Tavsiye Kararı, "Birleşmiş Milletler İş Dünyası ve İnsan Haklarına Dair Rehber İlkeler: Birleşmiş Milletler 'Koruma, Saygı Gösterme ve Telafi Edici Çözüm Üretme' Çerçevesi"ne uygun şekilde, aracı platformların, tüm eylemlerinde kullanıcılarının ve etkilenen tarafların insan haklarına saygı göstermesi gerektiğinin altını çizmiştir. Bu, ilgili kanunlara ve düzenleyici çerçevelere uygun hareket etme sorumluluğunu da içermektedir. Tavsiye Kararı'na göre, aracıların oynadığı çoklu roller sebebiyle, buna tekabül eden görev ve sorumlulukları ile bunların hukuken korunmaları, icra edilen özel hizmet ve fonksiyonlar dikkate alınarak belirlen-

melidir. Tavsiye Kararı, bu değerlendirmeleri yaptıktan sonra müteakip kılavuz ilkeleri kabul etmiştir:

Devletlerin İnternet Aracılarının Rol ve Sorumluluklarıyla İlgili Atacakları Adımlara Dair Kılavuz İlkeler

1. Devletlerin dijital ortamda insan haklarını ve temel özgürlükleri koruma ve geliştirmeye ilişkin yükümlülükleri

1.1. Kanunilik

1.1.1. Kamu makamları tarafından internet aracılarına yöneltilen ve insan hakları ile temel özgürlüklere müdahale niteliği taşıyan her türlü istem, talep veya başkaca bir eylem kanunda öngörülmeli, kanunda belirtilen sınırlar içerisinde icra edilmeli ve demokratik bir toplumda gerekli ve ölçülü bir tedbir olmalıdır. Devletler, internet aracılarına hukuki olmayan yollarla baskı uygulamamalıdır.

1.1.2. İnternet aracılarına yönelik kanunlar, düzenlemeler ve politikalar ticari veya gayriticari olmasına, amaç ve kapsamına bakılmaksızın AİHS'de yer bulan insan hakları ve temel özgürlükleri etkin şekilde korumalı ve keyfî uygulamalara karşı uygun teminatları içermelidir.

1.1.3. Devletlerin dijital ortamda insan haklarını ve temel özgürlükleri mutlak koruma yükümlülüğü vardır. Tüm düzenleyici çerçeveler -öz düzenleyici ve ortak düzenleyici yaklaşımlar dâhil- bu yükümlülüğe ilişkin etkili denetim mekanizmaları içermeli ve uygun tazmin imkânlarıyla desteklenmelidir.

1.1.4. İnternet aracılarına uygulanacak kanun veya düzenlemelerin yapım süreci, şeffaf ve katılımcı olmalıdır. Devletler kamu yararı, kullanıcıların ve etkilenen tarafların yararı ile aracıların yararı arasında uygun dengenin kurulmasını temin etmek amacıyla tüm paydaşlarla düzenli olarak istişarede bulunmalıdır. Kanun ve düzenlemeleri kabul etmeden önce devletler, insan haklarına muhtemel olumsuz etkileri anlamak, önlemek ve azaltmak için insan hakları etki analizi yapmalıdır.

1.1.5. İnternet aracılarına yönelik kanunlar, düzenlemeler ve politikalar çoklu ve kesişen ayrımcılık türlerini de dikkate alarak ayrım gözetmeksizin yorumlanmalı, uygulanmalı ve icra edilmelidir. Ayrımcılık yasağı, bazı durumlarda özel ihtiyaçları dikkate almak veya mevcut eşitsizlikleri gidermek için özel tedbirler gerektirebilir. Devletler ayrıca, hukuki mevzuatı tasarlarken, yorumlarken ve uygularken muhtemel ayrımcı etkileri önlemek adına aracıların büyüklük, nitelik, fonksiyon ve organizasyon yapısı bakımından esaslı farklılıklarını dikkate almalıdır.

1.1.6. Devletler, internet aracılarına yönelik kanun, düzenleme ve politikaların etkili şekilde uygulanabilir ve icra edilebilir olduğunu ve sınır aşan haberleşmenin işleyişini ve serbest akışını haksız yere kısıtlamamasını temin etmelidir.

1.2. Hukuki belirlilik ve şeffaflık

1.2.1. İnternet aracılarına ve bunların devletler ve kullanıcılarla olan ilişkilerine yönelik her türlü mevzuat, erişilebilir ve öngörülebilir olmalıdır. Tüm mevzuat, aracılar, kullanıcılar ve etkilenen tarafların kendi davranışlarını düzenlemelerine imkân verecek şekilde açık ve yeterince belirli olmalıdır. Mevzuat, özel haberleşmeler ve kamusal tartışmalar için güvenli ve destekleyici bir online ortam oluşturmalı, ilgili uluslararası standartlara uygun olmalıdır.

1.2.2. Her yasal düzenleme, kamu makamlarına internet aracılarıyla ilgili verilen yetkileri -bilhassa bu tür yetkiler kolluk kuvvetleri tarafından kullanıldığında- açıkça tanımlamalıdır. Bu tür yasal düzenlemeler, keyfî uygulamalara karşı koruma sağlamak için takdir yetkisinin kapsamını belirtmelidir.

1.2.3. Devletler uluslararası karşılıklı adli yardımlaşma anlaşmalarına dayananlar dâhil belirli bir zaman diliminde internet aracılarına yöneltilen talepler vasıtasıyla uygulanan içerik kısıtlamalarının veya kişisel veri açıklamalarının sayısı, niteliği ve hukuki dayanağı ve bu taleplerin sonucu olarak atılan adımlar hakkında kapsamlı bilgiyi kamuya açık olarak ve düzenli şekilde yayımlamalıdır. Şeffaflık amacıyla devletler, aracıların, mahkeme kararları, idari kararlar, özel şikâyet talepleri veya kendi içerik

kısıtlama politikalarının uygulanmasına dayanan dijital ortamdaki hak ve özgürlüklerin kullanımına yönelik müdahalelerine ilişkin açık (basit ve makine tarafından okunabilir), kolayca erişilebilir ve anlamlı bilgileri yayımlamasını zorunlu tutmalıdır.

1.2.4. Hukuki belirsizliği ve hukuk kurallarının çelişmesini önlemek amacıyla devletler, farklı hukuk kurallarının uygulandığı durumlarda birbirleriyle ve ilgili tüm paydaşlarla iş birliği içerisinde olmayı taahhüt etmeli ve uygun devlet dışı yargı mercilerinin aracılığı dâhil ortak yaklaşımların ve yetkiye ait ilkelerin geliştirilmesini desteklemelidir.

1.3. İfade özgürlüğü için korumalar

1.3.1. Kamu makamları tarafından internet aracılarına yöneltilen erişimi kısıtlamaya yönelik (içeriğin engellenmesi veya içeriğin kaldırılması dâhil) her türlü istem, talep, eylem veya ifade özgürlüğünün kısıtlanmasına yol açabilecek diğer tedbirler kanunda öngörülmeli, AİHS'nin 10. maddesinde yer alan meşru amaçlardan birini gütmeli, demokratik bir toplumda gerekli olmalı ve hedeflenen amaç ile orantılı olmalıdır. Devlet makamları, amaçladıkları politika hedefine ulaştıracak en az müdahaleci tedbiri tespit edebilmek için, herhangi bir kısıtlamayı uygulamadan önce ve uyguladıktan sonra kısıtlamanın istenmeyen etkileri dâhil muhtemel etkilerini dikkatlice değerlendirmelidir.

1.3.2. Devlet makamları, aracılardan bir içeriğe erişimi kısıtlamayı talep ettikleri zaman, bir mahkeme kararı veya kararları yargı denetimine tabi bağımsız bir idari makamın kararını almalıdırlar. Bu kural, çocukların cinsel istismarına yer veren içeren içerikler gibi, bağlamından bağımsız şekilde hukuka aykırı olan içerikler söz konusu olduğunda veya AİHS'nin 10. maddesinde belirtilen koşullara uygun şekilde hızlandırılmış tedbirlere ihtiyaç duyulan durumlarda uygulanmayacaktır.

1.3.3. İnternet aracıları devlet kararı üzerine üçüncü taraflara ait içerikleri kısıtladıklarında devlet makamları etkin tazmin mekanizmalarının ve bunlara bağlı uygulanabilir usuli güvencelerin varlığını temin etmelidir. Aracılar içeriği kendi hizmet kural ve koşullarına dayalı olarak

kaldırdıkları takdirde bu, aracıları, erişim sağladıkları üçüncü tarafa ait içerikten sorumlu kılan bir kontrol türü olarak nitelendirilmemelidir.

1.3.4. Devlet makamları; kullanıcılara, içerik sağlayıcılara ve aracılara karşı, ifade özgürlüğünü zedeleme niyetiyle kamunun katılımını önleme amaçlı stratejik davalar (SLAPP - *strategic lawsuits against public participation*) veya kötü niyetli ve bezdirme amaçlı davaları engellemeye ilişkin uygun yasal düzenlemeleri yapmayı değerlendirmelidir.

1.3.5. Devlet makamları, aracılara -otomatik yollarla olsun veya olmasın- salt erişim sağladıkları, aktardıkları veya sakladıkları içeriği kontrol etmeye yönelik doğrudan veya dolaylı bir genel yükümlülük getirmemelidir. Devlet makamları, internet aracılarına herhangi bir talep iletirken veya tek başına, diğer devletlerle yahut uluslararası kuruluşlarla birlikte internet aracılarının ortak düzenleme yaklaşımlarını teşvik ederken genel içerik kontrolüne yol açacak eylemlerden kaçınmalıdır. Tüm ortak düzenleme yaklaşımları, hukukun üstünlüğü ve şeffaflık önlemlerine uygun olmalıdır.

1.3.6. Devlet makamları, düzenleyici çerçevelere uymadıkları gerekçesiyle aracılara uyguladıkları yaptırımların orantılı olduğunu temin etmelidir; zira, orantısız tedbirler hukuka uygun içeriğin kısıtlanmasına ve ifade özgürlüğü hakkı üzerinde caydırıcı bir etkiye yol açabilir.

BEŞİNCİ KISIM

AVRUPA İNSAN HAKLARI MAHKEMESİ VE İNTERNET

§7. AVRUPA İNSAN HAKLARI MAHKEMESİNİN İNTERNET HUKUKUNA İLİŞKİN KARARLARI

Bilgi ve iletişim teknolojilerinin kullanımının AİHS'ye uygunluğu, AİHM tarafından farklı bağlamlarda değerlendirmeye alınmıştır. AİHM'nin mahremiyetten kişisel verilerin korunmasına kadar bu konuda çok sayıda içtihadı vardır.[295] Daha ziyade, AİHS'nin özel hayata ve aile hayatına saygıya ilişkin 8. maddesi ile ifade özgürlüğüne ilişkin 10. maddesi bağlamında verilen bu kararlar, mahremiyet ile diğer çatışan haklar arasında nasıl bir denge kurulması gerektiği konusunda yol gösterici niteliktedir.

İnternetin yaygınlaşması ve ifade özgürlüğünün temel bir aracı hâline dönüşmesiyle birlikte internete erişimin engellenmesi konusu da AİHM'i meşgul etmeye başlamıştır. Benzer şekilde, özellikle sosyal medyanın toplumun geniş kesimlerince kullanılmaya başlanmasıyla beraber arama motorlarının bilgi toplumunda özgün fonksiyonlar yerine getirmesi, üçüncü kişilerin platformlarda çok farklı niteliklerde içerik üretmesi ve paylaşması, içeriklerden kimin hangi esasa göre sorumlu tutulacağı, bağlantıların sorumluluk doğurup doğurmayacağı gibi internet hukukuna özgü sorunlar ortaya çıkmış ve bu konudaki uyuşmazlıklar nihai olarak AİHM'nin önüne gelmiştir.

Aralık 2020 itibarıyla AİHM'nin doğrudan internet hukukuna özgü vermiş olduğu on yedi kararı bulunmaktadır. Söz konusu kararlar (kabul veya kabul edilmezlik) internet ortamındaki içeriğe erişimin engellenmesi, içeriğin kaldırılması, internet ortamında kişilik haklarının korunması, internet platformlarının hukuki sorumluluğu, unutulma hakkı, üçüncü kişilere ait internet içeriğinden sorumluluk, üçüncü kişilere ait internet bağlantılarından sorumluluk gibi farklı konulara ilişkindir.

---

[295] AİHM'nin kişisel verilere ilişkin temel içtihatları için bkz. **AİHM**, "*Case Law of the European Court of Human Rights Concerning the Protection of Personal Data*" <https://www.echr.coe.int/Documents/FS_Data_ENG.pdf>

Müteakip bölümlerde AİHM'nin doğrudan internet hukukuyla ilgili on yedi kararı detaylı şekilde incelenecek ve bu inceleme neticesinde AİHM'nin internete ilişkin içtihatlarının gelişimi gözlemlenerek Mahkemenin en güncel yaklaşımı tespit edilmeye çalışılacaktır.

İncelenecek kararlar şunlardır:

- Ahmet Yıldırım v. Türkiye (18 Aralık 2012 - No. 3111/10)
- Akdeniz v. Türkiye (11 Mart 2014 - No. 20877/10)
- Cengiz ve diğerleri v. Türkiye (1 Aralık 2015 - No. 48226/10 ve 14027/11)
- Delfi AS v. Estonya (16 Haziran 2015 - No. 64569/09)
- Kalda v. Estonya (19 Ocak 2016 - No. 17429/10)
- MTE ve Index.Hu Zrt v. Macaristan (2 Şubat 2016 - No. 22947/13)
- Jankovskis v. Litvanya (17 Ocak 2017 - No. 21575/08)
- Rolf Anders Daniel Pihl v. İsveç (9 Mart 2017 - No. 74742/14)
- Tamiz v. Birleşik Krallık (19 Eylül 2017 - No. 3877/14)
- M.L. ve W.W. v. Almanya (28 Haziran 2018 - No. 60798/10 ve 65599/10)
- Magyar Jeti Zrt v. Macaristan (4 Aralık 2018 - No. 11257/16)
- Høiness v. Norveç (19 Mart 2019 - No. 43624/14)
- Kablis v. Rusya (30 Nisan 2019 - No. 48310/16 ve 59663/17)
- Bulgakov v. Rusya (23 Haziran 2020 - No. 20159/15)
- Engels v. Rusya (23 Haziran 2020 - No. 61919/16)
- OOO Flavus ve Diğerleri v. Rusya (23 Haziran 2020 - No. 12468/15, 23489/15 ve 19074/16)
- Vladimir Kharitonov v. Rusya (23 Haziran 2020 - No. 10795/14)

Kararlar üç farklı kategoride sınıflandırılabilir:

1. **İnternet İçeriğine Erişimin Engellenmesi veya İçeriğin Filtrelenmesine İlişkin Kararlar**
    - Ahmet Yıldırım v. Türkiye

- Akdeniz v. Türkiye
- Cengiz ve diğerleri v. Türkiye
- Kalda v. Estonya
- Jankovskis v. Litvanya
- Kablis v. Rusya
- Bulgakov v. Rusya
- OOO Flavus ve Diğerleri v. Rusya
- Vladimir Kharitonov v. Rusya

2. İçeriğin Kaldırılmasına İlişkin Kararlar

- M.L. ve W.W. v. Almanya
- Engels v. Rusya

3. Hukuki Sorumluluğa İlişkin Kararlar

- Delfi AS v. Estonya
- MTE ve Index.Hu Zrt v. Macaristan
- Rolf Anders Daniel Pihl v. İsveç
- Tamiz v. Birleşik Krallık
- Magyar Jeti Zrt v. Macaristan
- Høiness v. Norveç

Takip eden bölümlerde bu kararlar, karar tarihine göre (kronolojik olarak) incelenecektir. Kararlarda adı geçen ilgili deklarasyon ve tavsiye kararlarından bilinçli olarak geniş alıntılar yapılmıştır. Bu şekilde, yumuşak hukuk kurallarının nihai kararlara ne derece etki ettiği gözlemlenmeye çalışılmıştır.

§8. AHMET YILDIRIM V. TÜRKİYE

AİHM tarafından internet içeriğine erişimin engellenmesine ilişkin verilmiş ilk karar, 18 Aralık 2012 tarihli *Ahmet Yıldırım v. Türkiye* kararıdır.[296] AİHM, Web 2.0 olarak nitelendirilen etkileşimli internet içeriğinin hukuki statüsünü ve bu tür platformlardaki ifade özgürlüğü konusunu ilk defa bu kararında etraflıca ele almıştır.

I. Davanın gelişimi

Başvurucu Ahmet Yıldırım, akademik çalışmalarını ve farklı konulara ilişkin görüşlerini paylaşmak amacıyla Google Sites hizmetini kullanmak suretiyle http://sites.google.com/a/ahmetyildirim.com.tr/academic/ URL adresinde bir blog sayfası oluşturmuştur. Google Sites hizmetini kullanan başka bir kullanıcı ise http://sites.google.com/site/kemalizminkarinagrisi/benimhikayem/atauerk-koessi/at adresinde Atatürk'ün hatırasına hakaret içeren bir blog sayfası hazırlamıştır.[297]

Denizli Asliye Ceza Mahkemesi, 23 Haziran 2009 tarihinde, 5651 sayılı Kanun'un 8. maddesinin birinci fıkrasının (b) bendi uyarınca, Atatürk aleyhine içerikler barındıran bloğa erişimin engellenmesi kararı almıştır.[298] Karar, uygulanmak üzere Telekomünikasyon İletişim Başkanlığına (TİB) gönderilmiştir.

TİB, uyuşmazlık konusu blog sayfasının engellenmesinin, bu sayfanın sahibi *hosting* belgesine sahip olmadığı ve yurt dışında bulunduğu için ancak Google Sites isimli yer sağlayıcısı sitenin tamamının engellenmesi suretiyle mümkün olacağını belirtmiştir. 24 Haziran 2009 tarihinde, TİB'in talebi üzerine, Denizli Asliye Ceza Mahkemesi 23 Haziran tarihli kararını düzelterek Google Sites sitesinin tamamına erişimin engellen-

---

[296] **AİHM**, *Ahmet Yıldırım v. Türkiye*, Başvuru No: 3111/10, 18.12.2012.

[297] *Ahmet Yıldırım v. Türkiye*, para. 7.

[298] *Ahmet Yıldırım v. Türkiye*, para. 8.

mesine karar vermiştir.[299] Karar üzerine TİB, DNS engelleme tekniğini kullanarak Google Sites sitesinin tamamına erişimi engellemiştir.[300] Bu şekilde, sadece tedbire konu olan blog değil, tüm bloglar engellenmiştir.

Başvurucu, 1 Temmuz 2009 tarihinde, 24 Haziran 2009 tarihli erişimin engellenmesi kararına itiraz etmiş ve kendi internet sitesine ilişkin olarak bu tedbirin kaldırılmasını talep etmiştir.[301] Başvurucu, söz konusu siteyi düzenli olarak akademik çalışmalarını ve farklı konulara ilişkin görüşlerini yayınlamak için kullandığını, yasa dışı içerik nedeniyle engellenen siteye karşı alınan tedbir sonucunda, bu site ile hiçbir bağlantısı olmayan kendi sitesine erişimin de tamamen engellendiğini belirtmiştir.[302]

Başvuran, tedbir kararından diğer sitelerin etkilenmemesi için münhasıran uyuşmazlık konusu siteye erişimi imkânsız kılan bir yöntemin seçilmesi gerektiğini belirtmiş ve URL engelleme tedbirini örnek olarak göstermiştir. Denizli Ceza Mahkemesi ise başvuranın bu talebini, 13 Temmuz 2009 tarihinde, uyuşmazlık konusu siteye erişimin engellenmesinin tek yolunun suça konu içeriği yayınlayan http://sites.google.com sayfasına erişimin engellenmesi olduğuna yönelik TİB görüşü uyarınca reddetmiştir.[303]

Başvuran Yıldırım, AİHM'ye sunduğu 25 Nisan 2012 tarihli mektubunda, sitenin sahibine karşı yürütülen adli soruşturmanın 25 Mart 2011 tarihinde, yurt dışında bulunan şüphelinin kimliğinin ve adresinin tespitinin imkânsız olması sebebiyle, bildiği kadarıyla, takipsizlikle sonuçlanmasına rağmen kendi internet sitesine hâlen erişemediğini belirtmiştir.[304]

---

[299] *Ahmet Yıldırım v. Türkiye*, para. 10.
[300] *Ahmet Yıldırım v. Türkiye*, para. 11.
[301] *Ahmet Yıldırım v. Türkiye*, para. 12.
[302] *Ahmet Yıldırım v. Türkiye*, para. 12.
[303] *Ahmet Yıldırım v. Türkiye*, para. 13.
[304] *Ahmet Yıldırım v. Türkiye*, para. 14.

II. Hukuki arka plan

Konunun esasına girmeden evvel AİHM; temel Türk internet hukuku düzenlemesini (5651 sayılı Kanun), 1 Temmuz 2004 tarihinde yürürlüğe giren Avrupa Konseyi Siber Suç Sözleşmesi'ni, ilgili Avrupa Konseyi tavsiye kararı metnini, Avrupa Birliği Adalet Divanı (ABAD) kararını ve Birleşmiş Milletler metnini alıntılamıştır.

4/5/2007 tarihli ve 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un 8. maddesi şöyledir:

"*Madde 8*

Erişimin engellenmesi kararı ve yerine getirilmesi

(1) İnternet ortamında yapılan ve içeriği aşağıdaki suçları oluşturduğu hususunda yeterli şüphe sebebi bulunan yayınlarla ilgili olarak erişimin engellenmesine karar verilir:

a) 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununda 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.

(…)"

(2) Erişimin engellenmesi kararı, soruşturma evresinde hâkim, kovuşturma evresinde ise mahkeme tarafından verilir. Soruşturma evresinde, gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısı tarafından da erişimin engellenmesine karar verilebilir. Bu durumda Cumhuriyet savcısı kararını yirmidört saat içinde hâkimin onayına sunar ve hâkim, kararını en geç yirmidört saat içinde verir. Bu süre içinde kararın onaylanmaması halinde tedbir, Cumhuriyet savcısı tarafından derhal kaldırılır. Koruma tedbiri olarak verilen erişimin engellenmesine ilişkin karara 4/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanunu hükümlerine göre itiraz edilebilir.

(3) Hâkim, mahkeme veya Cumhuriyet savcısı tarafından verilen erişimin engellenmesi kararının birer örneği, gereği yapılmak üzere Başkanlığa gönderilir.

(4) İçeriği birinci fıkrada belirtilen suçları oluşturan yayınların içerik veya yer sağlayıcısının yurt dışında bulunması halinde (…) erişimin engellenmesi kararı re'sen Başkanlık tarafından verilir. Bu karar, erişim sağlayıcısına bildirilerek gereğinin yerine getirilmesi istenir.

(5) Erişimin engellenmesi kararının gereği, derhal ve en geç kararın bildirilmesi anından itibaren yirmidört saat içinde yerine getirilir.

(7) Soruşturma sonucunda kovuşturmaya yer olmadığı kararı verilmesi halinde, erişimin engellenmesi kararı kendiliğinden hükümsüz kalır (…)

(8) Kovuşturma evresinde beraat kararı verilmesi halinde, erişimin engellenmesi kararı kendiliğinden hükümsüz kalır (…)

(9) Konusu birinci fıkrada sayılan suçları oluşturan içeriğin yayından çıkarılması halinde; erişimin engellenmesi kararı (…) kaldırılır."

AİHM'ye göre 5651 sayılı Kanun'da yer alan "yayın" terimi, doktrinde de bir tartışma konusu olmuştur. Bazı yorumculara göre, 2. maddenin (ğ) bendinde "*internet ortamında yer alan ve içeriğine belirsiz sayıda kişilerin ulaşabileceği veriler*" şeklinde tanımlanan "*internet ortamında yapılan yayın*" terimi ile "*internet ortamında yapılan yayın*" şeklinde tanımlanan,

aynı maddenin (1) bendinde yer alan "*yayın*" terimi birbiriyle çelişmektedir.[305] Esasen, burada zorluk "internet ortamında yapılan yayın" ifadesinin kullanılmasından kaynaklanmaktadır zira bu ifade internette yer alan her türlü veriyi kapsayabilecektir.

AİHM'nin atıf yaptığı bir diğer belge ise 13 Mayıs 2005 tarihli Bilgi Toplumunda İnsan Hakları ve Hukukun Üstünlüğü Deklarasyonu'dur.[306] Söz konusu Deklarasyon'da vurgulandığı üzere:

"1. İfade, Bilgi ve İletişim Özgürlüğü Hakkı

BT'ler herkese ifade özgürlüğünden yararlanmak konusunda emsali olmayan imkânlar sunmaktadır. Bununla birlikte, bu özgürlüğü devlet veya özel sektör sansürü gibi ciddi tehditlere de maruz bırakmaktadır.

İfade, bilgi ve iletişim özgürlüğüne dijital olmayan ortamda gösterilen saygının aynısı dijital ortamda da gösterilmelidir. Bu özgürlüğün, dijital bir form içinde vücut bulması sebebiyle, AİHS'nin 10.maddesinde yer alan kısıtlamalardan farklı kısıtlamalara tabi tutulması doğru olmayacaktır.

Üye devletler, bir yandan ifade özgürlüğünü güvence altına alırken öte yandan ırkçı nitelik taşıyan veya ırk ayrımcılığı ve çocuk pornosu içeren yasa dışı içerikler ile mücadeleye ilişkin yerel mevzuatlarının TBT yoluyla işlenen suçlara da uygulanmasını gözetmelidir.

Üye devletler, devlet ve özel sektör sansürünün önlenmesi için hukuki ve pratik önlemleri muhafaza etmeli ve güçlendirmelidir. (…)"

Mahkemenin alıntıladığı bir diğer Avrupa Konseyi metni ise 28 Mayıs 2003 tarihli İnternette İletişim Özgürlüğüne İlişkin Deklarasyon'dur.[307] Bu Deklarasyon'da, internette iletişimin üzerinde uygulanacak sınır gözetmeyen bir *apriori* kontrolün istisnai olması ve bireylerin internete erişiminin önündeki engellerin ortadan kaldırılması gerektiği belirtilmektedir.

---

[305] *Ahmet Yıldırım v. Türkiye*, para. 18.

[306] *Ahmet Yıldırım v. Türkiye*, para. 20.

[307] *Ahmet Yıldırım v. Türkiye*, para. 21.

"(…)

İlke 1: İnternet için içerik kuralları

Üye devletler, internet içeriğine, diğer içerik dağıtım araçlarına getirilen düzenlemelerin ötesinde bir sınırlama getirmemelidir.

(…)

İlke 3: Devletin ön kontrolünün bulunmaması

Kamu otoriteleri, engelleme veya filtreleme gibi genel önlemler vasıtasıyla, sınır tanımayan bir şekilde toplumun bilgiye veya internet ortamındaki diğer iletişim olanaklarına erişiminin önüne geçmemelidir. Bu durum küçüklerin bulunabileceği okul veya kütüphane gibi yerlerde onların korunması amacıyla filtreleme yapılmasını engellemeyecektir.

Yetkili ulusal makamlar bunun yasal olmadığı hususunda geçici veya nihai bir karar verdikleri takdirde, İnsan Hakları ve Temel Özgürlüklerin Korunmasına İlişkin Sözleşme'nin 10.2 maddesinde yer alan güvencelere saygı gösterilmesi kaydıyla, açıkça tespit edilebilen bir internet içeriğinin silinmesi için veya alternatif olarak, buna erişimin engellenmesi için gerekli önlemler alınabilir.

(…)"

22. Deklarasyon'un açıklayıcı notunda, 3 numaralı ilkeye ilişkin aşağıdaki yoruma yer verilmiştir:

"Devletin ön kontrolünün bulunmaması

Bu ilke, toplumun internet ortamındaki aramalarında devletin ön kontrolünün bulunmamasının öneminin altını çizmektedir. Birtakım devletler gerçekten de vatandaşlarının bazı yabancı veya yerel internet sitelerinin içeriklerine erişimlerini siyasi gerekçelerle engelleme eğilimi içindedir. Bu uygulama ve devletin ön kontrolüne ilişkin her türlü benzer uygulama sert bir şekilde kınanmalıdır.

Her ne kadar devletler istenmeyen içeriğe erişimi engelleyici geniş çaplı önlemleri hiçbir koşulda almamalılar ise de küçüklerin korunması için gerekli

istisnalara izin verilmelidir. Küçüklerin internete örneğin okul veya kütüphanelerde erişimleri sırasında, kamu kurumları zarar verici içeriklere erişimin engellenmesi için bilgisayarlara filtre kurulmasını talep edebilir.

Devletin ön kontrolünün bulunmaması, bir içeriğin, yalnızca ceza hukuku değil, idare hukuku ve medeni hukuk gibi diğer hukuk dalları açısından da yasal olmadığına ilişkin yetkili ulusal makamlar tarafından alınan geçici veya nihai bir karar sonucunda silinmesi veya buna erişimin engellenmesi için gerekli önlemlerin alınması imkânını şüphesiz ki ortadan kaldırmaz. Yasa dışı bir içeriğe toplumun erişiminin engellemesi, bu şekilde alınabilecek önleyici tedbirlerden sayılabilir. Ön kontrole sebep olabilecek bu tarz önlemler, İnsan Hakları ve Temel Özgürlüklerin Korunmasına İlişkin Sözleşme'nin 10.2 maddesinin hükümlerine uygun olmalı ve açıkça tespit edilebilen bir internet içeriğine yönelmelidir."

AİHM ayrıca, Avrupa Konseyi Bakanlar Komitesinin 7 Kasım 2007 tarihli İnternetin Kamu Hizmeti Boyutunun Geliştirilmesine Yönelik Önlemlere İlişkin Tavsiye Kararı'na, 26 Eylül 2007 tarihli Yeni Bilgi ve İletişim Ortamında İfade ve Bilgi Özgürlüğünün Geliştirilmesine İlişkin Tavsiye Kararı'na, 26 Mart 2008 tarihli İnternet Filtreleri Bağlamında İfade ve Bilgi Özgürlüğüne Saygının Teşvik Edilmesine Yönelik Tedbirleri İçeren Tavsiye Kararı'na ve 4 Nisan 2012 tarihli Arama Motorları Bağlamında İnsan Haklarının Korunmasına İlişkin Tavsiye Kararı'na atıf yapmıştır.

Mahkeme, Avrupa Birliği'nin 2008/2160(INI) sayılı Tavsiye Kararı ile Avrupa Birliği Adalet Divanının C-70/10 sayılı *Scarlet Extended SA v. SABAM* (*Belçikalı Yazar, Bestekâr ve Editörler Derneği)* kararına da değinmiştir. Öte yandan, Birleşmiş Milletler İnsan Hakları Komitesinin 11-29 Temmuz 2011 tarihleri arasında gerçekleşen 102. oturumunda Medeni ve Siyasi Haklara İlişkin Uluslararası Sözleşme'nin 19. maddesiyle ilgili olarak kabul ettiği 34 numaralı Genel Yorum'a vurgu yapılmış ve akabinde muhtelif karşılaştırmalı hukuk[308] örneklerine yer verilmiştir.

[308] *Ahmet Yıldırım v. Türkiye*, para. 31-37.

Birleşmiş Milletler İnsan Hakları Komitesinin söz konusu Genel Yorum'unda belirtildiği üzere:

"43. Web sayfalarının, blogların veya internet temelli, elektronik veya diğer bilgi yaygınlaştırma sistemlerinin, ayrıca örneğin internet hizmet sunucuları veya arama motorları gibi bu tür iletişimi destekleyen sistemlerin işleyişine getirilecek herhangi bir kısıtlama, ancak 3'üncü paragrafa uygun gerekçelerle kabul edilebilir. İzin verilebilir kısıtlamalar genellikle içeriğe özgü olmalıdır; belirli sitelerin ve sistemlerin işleyişine getirilecek genel yasaklar paragraf 3'le bağdaşmaz. Ayrıca, bir siteye veya enformasyon yaygınlaştırma sistemine yalnızca hükûmete veya hükûmetin temsil ettiği siyasal sisteme yönelik eleştirel tutum alabileceği ve bu yönde yayınlar yapabileceği gerekçesiyle yasak getirilmesi de 3'üncü paragrafla bağdaşmaz."

III. AİHM'nin tespit ve değerlendirmeleri

Davanın konusu, kendi sitesiyle ilgisi bulunmayan bir ceza davası kapsamında alınan tedbir sonucu başvurucunun sitesinin engellenmiş olmasıdır. Hukuka aykırı içerikle mücadele için kullanılan tekniğin ölçüsüz olduğu, hedeflenen amaçla orantılı olmadığı iddia edilmiştir. AİHM, uyuşmazlığı çözerken internet ile ifade özgürlüğüne ilişkin önceki içtihatlarına atıfta bulunmuştur. Mahkeme *"[E]rişebilirliklerinin yanı sıra büyük miktarda veriyi muhafaza etme ve dağıtma imkânları sayesinde, internet siteleri kamunun güncele erişiminin iyileştirilmesine ve bilginin iletilmesinin kolaylaştırılmasına önemli derecede katkıda bulunmaktadır."*[309] şeklindeki tespitinin yer aldığı içtihadına atıf yapmış; akabinde Google Sites hizmetinin, ifade özgürlüğünün kullanılması açısından bir araç olduğunu belirtmiştir.[310] Bu tespit, bilgi dağıtma araçlarına yönelik korumaların yer aldığı diğer içtihatlarla desteklenmiştir.

AİHM tarafından haklı olarak tespit edildiği üzere, erişimin engellenmesi tedbirinin nispeten sınırlı etkilerinin olması, kısıtlamanın

[309] **AİHM**, *Times Newspapers v. Birleşik Krallık* (1 ve 2 sayılı), Başvuru No: 3002/03 ve 23676/03, 10.3.2009.

[310] *Ahmet Yıldırım v. Türkiye*, para. 49.

önemini azaltmamaktadır.[311] Üçüncü kişiye ait bir içeriğe yönelik tedbir için TİB'in talebi üzerine Denizli Asliye Ceza Mahkemesinin siteye bütünüyle erişimi engelleme kararı vermiş olması; bilgi ve fikir alma ve verme özgürlüğünün ihlali sayılarak, "kamu makamlarının müdahalesi" olarak nitelendirilmiştir.[312]

Mahkeme; "yasa tarafından öngörülmüş" olmadığı, meşru bir hedefi/hedefleri gütmediği veya bu hedef/hedeflere ulaşmak için "demokratik bir toplumda zorunlu" olmadığı durumlarda böyle bir engellemenin (DNS engellemesi) AİHS'nin 10. maddesine aykırı olacağı tespitini yapmıştır.[313]

Peki, yasayla öngörülmüş olmanın kriterleri nelerdir? Mahkemeye göre, bir düzenleme, iç hukukta dayanağı bulunması, erişilebilir olması ve aydınlatıcı tavsiyelere ilişkin ihtiyacı karşılamak suretiyle herkesin kendi davranışını ayarlamasına izin verecek açıklıkta yazılması hâlinde öngörülebilir olarak nitelendirilebilecektir.[314]

AİHM, erişimin engellenmesine imkân veren 5651 sayılı Kanun'un 8. maddesinin birinci fıkrasına atıf yaparak müdahalenin yasal bir temeli olduğunu tespit etmiştir. Bu düzenleme erişilebilirlik ve öngörülebilirlik kriterlerini sağlamakta mıdır? AİHM, hukuki belirliliğin sağlanabilmesi için, kamu gücünün AİHS'de güvence altına alınan haklara keyfî müdahalelerine karşı birtakım korumaların olması ve yasanın bu gücün kullanılmasının yöntemini ve kapsamını yeterli netlikte düzenlemesi gerektiğini vurgulamıştır.[315]

AİHM, 5651 sayılı Kanun'da geçen "internet ortamında yapılan yayın" kavramı son derece geniş kapsamlı ve internet üzerinde yayımlanan her türlü veriyi kapsayacak nitelikte olsa dahi somut olayda Ahmet Yıldırım'a ait blog ve Google Sites'ın hukuka uygunluğunun özel bir değerlen-

[311] *Ahmet Yıldırım v. Türkiye*, para. 54.
[312] *Ahmet Yıldırım v. Türkiye*, para. 55.
[313] *Ahmet Yıldırım v. Türkiye*, para. 56.
[314] *Ahmet Yıldırım v. Türkiye*, para. 56.
[315] *Ahmet Yıldırım v. Türkiye*, para. 59.

dirme konusu yapılmadığını belirtmiştir.[316] Mahkeme, aynı doğrultuda, 5651 sayılı Kanun'un yer sağlayıcılara ilişkin 5. maddesinin ikinci fıkrasında yer alan, hukuka aykırı içeriği yayından kaldırmaya ilişkin hükmü de değerlendirmiş; somut olayda Google Sites'ın bilgilendirildiği veya aleyhine ceza soruşturması açılmış bir siteye ilişkin tedbir niteliğindeki kararın gereklerini yerine getirmediği sonucuna varacak bir bilgi bulunmadığını da beyan etmiştir.[317]

AİHM'nin özellikle üzerinde durduğu konu, TİB'in yetkileri ve esas hakkında davaya bakan mahkemenin konuyu nasıl muhakeme ettiğidir. Erişimin engellenmesinin içeriğinden ziyade usulü özel olarak mütalaa edilmiştir. AİHM, TİB'in kapsamlı yetkileri olduğunu ve erişimin engellenmesine ilişkin tedbirin genişletilmesini talep edebileceğini vurgulamıştır.[318] Ayrıca, Denizli Asliye Ceza Mahkemesinin kapsamlı bir araştırma yapmaksızın salt TİB'in görüşüyle hareket ettiğinin de altı çizilmiştir.

AİHM, yerel mahkeme kararında erişimin engellenmesinin gerekliliğinin tartışıldığına işaret eden hiçbir olgunun bulunmamasını; daha önemlisi, 5651 sayılı Kanun'un 8. maddesinin, ölçülülük başta olmak üzere AİHS'nin 10. maddesinde yer alan ilkelerin değerlendirilmesini zorunlu kılan, bu konuda bir sorumluluk yükleyen bir nitelikte olmamasını; büyük miktarda bilgiye erişimi engelleyen tedbirlerin internet kullanıcılarının haklarını önemli derecede etkilemesi ve bunun üzerinde önemli bir yan etkisi olması sebebiyle hâkimlerin bunu değerlendirmemesini eksiklik olarak görmüştür.[319]

Tüm bu tespitlerin neticesinde AİHM, 5651 sayılı Kanun'un 8. maddesinin öngörülebilirlik şartını karşılamadığı ve başvuranın demokratik bir toplumda hukukun üstünlüğünün emrettiği ölçüde korumadan yararlanmasına izin vermediği hükmüne varmıştır.[320] Ayrıca, bu düzenlemenin, güvence altına alınan hakların "ülke sınırları gözetilmeksizin"

[316] *Ahmet Yıldırım v. Türkiye*, para. 61.
[317] *Ahmet Yıldırım v. Türkiye*, para. 62.
[318] *Ahmet Yıldırım v. Türkiye*, para. 63.
[319] *Ahmet Yıldırım v. Türkiye*, para. 66.
[320] *Ahmet Yıldırım v. Türkiye*, para. 67.

geçerli olduğunu belirten AİHS'nin 10. maddesinin birinci fıkrasına da açıkça aykırı olduğuna hükmedilmiştir.

Özetle AİHM, erişimi engelleme tedbirinin keyfî sonuçlar doğurduğuna, yalnızca uyuşmazlık konusu siteye erişimi engelleme hedefi gütmediğine, tüm içeriğe erişimin engellenmesine yol açtığına; internet sitelerine erişimin engellenmesinin hukuki kontrolü için bir mekanizma öngörülmediğinden tedbirin istismar edilmesinin önüne geçmek için gerekli şartların bulunmadığına; yerel hukuk düzenlemesinin, bir siteyi hedefleyen erişim engeli tedbirinin genel bir erişim engeli olarak kullanılmasından kaçınılması için hiçbir güvence öngörmediğine hükmetmiştir.[321] Bu doğrultuda, AİHS'nin 10. maddesinin ihlal edildiğine karar verilmiştir.

IV. Yargıç Paulo Pinto de Albuquerque'nin mutabık görüşü

AİHM Yargıcı Paulo Pinto de Albuquerque, *Ahmet Yıldırım* kararında karara katılan ancak gerekçe bakımından ayrışan bir mutabık görüş yazmıştır. Yargıç Pinto de Albuquerque, dağınık hatta çelişkili bir içtihat oluşmasının önüne geçmek için Mahkemenin, bu kararında, yeni ve çetrefil sorunlar karşısında ilkesel bir yaklaşım sergilemesi gerektiğini ve mevcut yasal mevzuattaki boşlukları dikkate alarak bu konuda uyguladığı prensiplere uygun açık kılavuz ilkeler koyması gerektiğini belirtmiştir.[322] Avrupa Konseyinin internet ortamındaki özgürlüğe ilişkin muhtelif kararlarına atıf yapan Yargıç Pinto de Albuquerque, mevcut hukuki ve politik çerçeve ışığında şu kriterleri önermiştir:[323]

(1) Yayınlarının engellenmesi muhtemel olan kurum ve kişi kategorilerinin tanımı: yasa dışı içeriklerin, internet sitelerinin ve platformlarının yerli ve yabancı sahibi, bu internet sitelerinin veya platformlarının

[321] *Ahmet Yıldırım v. Türkiye*, para. 68.

[322] *Ahmet Yıldırım v. Türkiye*, Yargıç Pinto de Albuquerque'nin Mutabık Görüşü.

[323] *Ahmet Yıldırım v. Türkiye*, Yargıç Pinto de Albuquerque'nin Mutabık Görüşü.

kullanıcıları veya bu yasa dışı site ve platformları link olarak verenler ve bu içeriklere abone olanlar

(2) Engelleme emirlerinin kategorilerinin tanımlanması, örnek olarak internet sitelerinin, IP adreslerinin, portların, ağ protokollerinin veya sosyal ağ gibi kullanım tiplerinin engellenmesine yönelik tedbirler

(3) Bölgesel, ulusal veya küresel düzeyde etkisi olabilecek engelleme emrinin yer bakımından uygulanmasına ilişkin hüküm

(4) Böyle bir engelleme tedbirinin süre sınırının olması

(5) Engelleme tedbirini AİHS'nin 10.2 maddesinde belirtilen meşru hâle getirebilecek "menfaatlerin" sayılması

(6) İfade özgürlüğünün esasına (çekirdek özüne) saygı gösterilmesini sağlarken ifade özgürlüğü ile yarışan diğer menfaatlerin dengelenmesini öngören orantılılık kriterine uyum

(7) İfade özgürlüğüne yapılan müdahalenin, güdülen menfaati uygun bir şekilde geliştirip geliştirmediğinin ve söz konusu "sosyal ihtiyacı" gerçekleştirmek için gerekli olandan daha ileri gidilip gidilmediğinin tespitini mümkün kılan gereklilik ilkesine saygı gösterilmesi

(8) Gerekçeli bir engelleme kararı vermeye yetkili makamların belirtilmesi

(9) Ulaşılmak istenilen amaçlarla ifadenin çatıştığı ya da imkânsız olduğu hâller dışında, zarar görmüş bir kuruluş ya da kişinin ifadesi ve karar talebine dayanan dosyanın yetkili makam tarafından incelenmesini içeren bu kararı vermek için takip edilmesi gereken usul

(10) Zarar gören kişi ve kuruma engelleme emrinin ve gerekçesinin tebliği

(11) Engelleme tedbirine karşı yasal bir itiraz yolu

Yargıç Pinto de Albuquerque, bu şekilde objektif bir ölçülülük testi geliştirmeye çalışmıştır. Yargıç Pinto de Albuquerque'ye göre, internet içeriğine müdahale için özel kanunlarla düzenleme yapılmalıdır. İnter-

net sitelerine veya platformlarına karşı uygulanan ve süresiz veya uzun süre geçerli olan engellemeler sansür olarak nitelendirilecektir. İstisnai durumların yasa dışı bir içeriğin engellenmesini meşru kılması hâlinde, yasa dışı yayından ne *de jure* ne *de facto* sorumlu olan veya onun içeriğine abone olmayan kişi ve kurumların hedef alınmasından kaçınılması ve yasa dışı içeriğe yönelen tedbirlere ayar yapılması gerekir.[324]

5651 sayılı Kanun'u ve uygulamasını da değerlendiren Yargıç Pinto de Albuquerque'ye göre, Türk hâkimlerin, 5651 sayılı Kanun'un 8. maddesi uyarınca kendilerine verilen yetkileri dar yorumlamaları gerekirdi. [325] Ayrıca, Ahmet Yıldırım'ın yaptığı itirazı da daha az müdahaleci herhangi bir tedbirin bulunmadığından bahisle reddetmemeleri lazım gelirdi. Devletlerin internet ortamında ifade özgürlüğüne ilişkin her türlü müdahaleden kaçınma konusundaki olumsuz yükümlülüğünü hatırlatan Yargıç Pinto de Albuquerque, ana kararda 5651 sayılı Kanun'un ilgili hükümlerinin tadil edilmesi gerektiğine vurgu yapılmasını önermiştir.

V. Değerlendirme

AİHM, *Ahmet Yıldırım* kararında internetin ifade özgürlüğünün kullanılması ve geliştirilmesi açısından önemini vurgulamıştır. AİHM, yukarıda da belirtildiği üzere, erişimin engellenmesi usulünü ve bu kararların alınması ile icra edilmesi süreçlerindeki eksiklikleri dikkate alarak bir karara varmıştır.

Öte yandan, Yargıç Pinto de Albuquerque tarafından da eleştirildiği üzere, kararda Web 2.0 dünyasına uygulanacak genel bir ölçülülük metodolojisi yer almamaktadır. *Ahmet Yıldırım* kararı önemli bir başlangıçtır ancak kapsamlı bir yol gösterici değildir. Kararın en önemli çıktıları şunlardır: (i) İnternet içeriğine müdahale için açık bir düzenlemenin varlığı şarttır ve (ii) internet içeriğine tedbir uygulayacak makamlar bir yerindelik denetimi yaparak, kullandıkları araçların ulaşmayı amaçladıkları amaç için elverişli ve ölçülü olup olmadığını değerlendirmek zorundadır.

---

[324] *Ahmet Yıldırım v. Türkiye*, Yargıç Pinto de Albuquerque'nin Mutabık Görüşü.

[325] *Ahmet Yıldırım v. Türkiye*, Yargıç Pinto de Albuquerque'nin Mutabık Görüşü.

Öte yandan, kararın, erişimin engellenmesi konusunun teknik boyutlarını gereğince ele alındığını söylemek pek mümkün değildir. Gerçekten de TİB'in 2009 yılında uyguladığı DNS engelleme yöntemi yerinde miydi? URL engellemesi yapılması, diğer bir deyişle, sadece ilgili blog sayfasına erişimin engellenmesi mümkün müydü? Dördüncü bölümde açıklandığı üzere, DNS engelleme tekniğinin altyapıda kapsamlı bir dönüşüm gerektirmeden, minimum maliyetle, pratik şekilde kullanılması mümkündür. URL engelleme tekniği ise maliyetli bir tekniktir.

Dördüncü Bölümde incelendiği üzere bir kullanıcısının hukuka aykırı veya zararlı olarak etiketlenmiş bir URL adresine erişmesini kontrol edebilmek için İSS'nin kullanıcının tüm internet trafiğini incelemesi gerekmektedir.[326] Bu teknik, "derin paket analizi" (DPI) olarak da bilinmektedir ve daha önceden belirlenmiş bir ağ politikası gereğince işletmecilerin sabit veya mobil ağları üzerinden iletilen tüm paketlerin içeriklerinin incelenmesi esasına dayanmaktadır.

2009 yılında Türkiye'de DPI analizi yapacak ve URL engellemesi gerçekleştirecek bir internet altyapısının olmadığı bilinmektedir. 2009'un dünyasında altyapıda hukuka aykırı içerikle mücadele için kullanılabilecek teknikler, DNS veya IP engelleme teknikleriydi. Hâliyle, TİB tarafından verilen görüş teknik olarak doğruydu. Ancak, Denizli Asliye Ceza Mahkemesinin AİHM'nin *Ahmet Yıldırım* kararının özünde belirtildiği üzere bir denge testi yapması ve Türkiye'nin taraf olduğu uluslararası sözleşmeleri de dikkate alarak çatışan menfaatleri dengelemesi ve daha az müdahaleci bir yöntemi benimsemesi gerekirdi. Teknik bir tercihin ne denli büyük etkileri olabileceğinin öngörülmesi beklenirdi. Nihayetinde, DNS engelleme tekniğinin bir bütün hâlinde tüm bilgi kaynağını engelleyerek ölçüsüz bir kısıtlamaya yol açtığı ve bir kişinin hukuka aykırı fiili sebebiyle başkalarının cezalandırılmasını netice vererek ifade özgürlüğüne ve ceza sorumluluğunun şahsiliği ilkesine aykırılık oluşturduğu aşikârdır.

Peki, URL engelleme yöntemi daha az müdahaleci bir yöntem midir? URL engelleme tekniğiyle spesifik bir sayfaya erişimin engellenmesi mümkündür. Bu yönüyle DNS ve IP engelleme tekniklerine nazaran

[326] **§4(X)(C)**[URL engellemesi].

ifade özgürlüğüne daha az müdahale eden bir yöntemdir. Ancak URL engelleme tekniğinin mahremiyet anlamında ağır bir yan etkisi vardır. Dördüncü bölümde etraflıca incelendiği üzere, URL engelleme tekniğinin uygulanabilmesi için ülke genelinde tüm internet çıkış noktalarında DPI tekniğinin kullanılması gerekir. Bu, ağdaki tüm iletişimin teker teker kontrol edilmesi anlamına gelir.

Kişisel verilerin ve de mahremiyetin bu aşamada korunmasına ilişkin etkin bir hukuki çerçeve yoksa URL engelleme tekniği AİHS'nin 10. maddesine hizmet ederken 8. maddesi bağlamında özel yaşama ve genel olarak mahremiyete yönelik ölçüsüz bir müdahale doğurabilir. Dolayısıyla, internet içeriğine müdahalede tedbirleri iyi veya kötü şeklinde sınıflandırmak mümkün değildir. Her tekniğin kendisine göre avantajı ve dezavantajı vardır.

§9. AKDENİZ V. TÜRKİYE

Ahmet Yıldırım kararından sonra AİHM önünde tartışılan bir diğer internet hukuku kararı, 11 Mart 2014 tarihli *Akdeniz v. Türkiye* kabul edilmezlik kararıdır.[327] Başvurunun temelini, last.fm ve myspace.com web sitelerinde yer alan içeriklerin fikrî mülkiyet haklarını ihlal etmesi sebebiyle bu sitelere uygulanan erişimin engellenmesi tedbirinin AİHS'nin 10. maddesi bağlamında bilgi alma hürriyetini ihlal ettiği iddiası oluşturmaktadır.

I. Kararın detaylı incelemesi

Hukukçu akademisyen Yaman Akdeniz tarafından AİHM önüne getirilen ihtilafın konusu last.fm ve myspace.com sitelerine uygulanan erişim engellemesidir. MÜ-YAP (Bağlantılı Hak Sahibi Fonogram Yapımcıları Meslek Birliği) tarafından yapılan başvuru üzerine, 26 Haziran 2009 tarihinde, telif haklarını ihlal ederek müzik eserlerini yaydıkları gerekçesi ile 5846 sayılı Fikir ve Sanat Eserleri Kanunu'nun (FSEK) ek 4. maddesinde yer alan usul işletilerek Beyoğlu Cumhuriyet Savcılığı kararıyla last.fm ve myspace.com sitelerine erişim engellenmiştir.[328] Söz konusu karara, ilgili sitelerin temsilcileri tarafından süresi içerisinde herhangi bir itiraz yapılmamıştır.

Sitelere erişim DNS engelleme tekniği kullanılarak engellenmiştir. Hâliyle, siteler tüm Türkiye'de erişilmez duruma gelmiştir. Söz konusu siteleri düzenli olarak kullanan bir kullanıcı sıfatıyla Yaman Akdeniz, tedbirlerin bilgiye erişim ve ifade özgürlüğünü ölçüsüzce kısıtladığı ve daha önemlisi Savcılık kararının bir hâkim onayına sunulmadığı iddialarıyla karara itiraz etmiştir.[329] Ayrıca, FSEK'nin ek 4. maddesinin üçüncü

---

[327] **AİHM**, *Akdeniz v. Türkiye*, Başvuru No: 20877/10, 11.3.2014.

[328] *Akdeniz v. Türkiye*, para 3.

[329] *Akdeniz v. Türkiye*, para 5.

fıkrasının Anayasa'ya aykırı olduğundan bahisle bu düzenlemenin iptal istemiyle Anayasa Mahkemesine taşınmasını talep etmiştir.

Kararı inceleyen Beyoğlu Sulh Ceza Mahkemesi, Yaman Akdeniz'in kullanıcı sıfatıyla savcılık kararına itiraz hakkı olmadığını, böyle bir hakkı olsaydı bile itirazını 7 günlük itiraz süresi içerisinde yapmış olması gerektiğini ileri sürerek talebi 30 Eylül 2009 tarihinde reddetmiştir.

Yaman Akdeniz, bu karara üst mahkemede itiraz etmiştir. İtirazı inceleyen mahkeme de 12 Ekim 2009 tarihinde Yaman Akdeniz'in itirazını farklı gerekçelerle reddetmiştir. [330] Mahkeme, AİHS ve Ticaretle Bağlantılı Fikrî Mülkiyet Anlaşması (TRIPS) hükümlerine atıf yapmış ve artan bilişim suçlarını da gerekçe göstererek telif ihlallerinin önlenmesi için sitelere erişimin engellenmesinin tek etkili yöntem olduğunu belirtmiştir. Mahkeme, ayrıca, merkezleri yurt dışında bulunan ihtilafa konu web sitelerinin, içeriklere yönelik taleplere duyarsız kaldığına dikkat çekmiştir. Son olarak, mevcut internet altyapısı internet ortamındaki belirli bir içeriğe erişimi engellemeye olanak tanımadığı için, somut olayda uygulanan engelleme yönteminin tek çare olduğuna işaret edilmiştir.

Başvurucu, iç hukuktaki ilgili hak arama yollarını tükettikten sonra AİHM'ye başvurmuştur. Başvuruyu değerlendiren AİHM, öncelikle başvuranın AİHS'nin 34. maddesi bakımından mağdur olarak değerlendirilip değerlendirilemeyeceğini -kişi bakımından yetki (*ratione personae*) konusunu- incelemiştir.

Türk Hükûmeti, başvurucunun, kullanıcı sıfatıyla mağdur olarak nitelendirilemeyeceğini; müzik dinlemek ve indirmek için alternatif yöntemleri olduğunu; Savcılık kararından itibaren 7 gün içerisinde itirazını gerçekleştirmediği için iç hukuk yollarını gereğince tüketmiş sayılamayacağını iddia etmiştir.[331]

Başvurucu, davaya taraf olması, diğer bir deyişle mağdur olarak nitelendirilmesi bakımından, web sitelerine erişimin engellenmesi özelinde genel menfaat ihlali kavramına işaret etmiştir.[332] Usul konularında

[330] *Akdeniz v. Türkiye*, para 8.

[331] *Akdeniz v. Türkiye*, para 15.

[332] *Akdeniz v. Türkiye*, para 15.

ise aşırı şekilciliğin AİHS kapsamında korunan hakları etkisiz kılacağını iddia etmiştir.

Başvurucu, last.fm sitesinde üye hesabının bulunduğunu tekrarlamış ve bu hesapta özgün bir içeriğin olduğunu belirtmiştir. Türk Hükûmetinin alternatif yöntemlerin varlığına yönelik iddiasına ise bu önermenin kabul görmesi durumunda, bir içerik türüne yönelik alternatifin varlığı durumunda kamu otoritelerinin her türlü web sitesini engellemeyi meşru sayacağı argümanıyla cevap vermiştir.

AİHM, başvurucunun mağdur olarak nitelendirilmesi sorunsalını çözmek için AİHS'nin mağdur tanımına ilişkin 34. maddesinin ve mağdur kavramının müstakil olarak değerlendirilmesi gerektiğine; AİHS'nin halk davası (*actio popularis*) açma imkânı vermediğine, kişinin bireysel başvuruda bulunabilmek için sözleşmeci devlete yüklenebilir bir eylem ya da ihmal sonucu AİHS'nin ihlal edilmesi nedeniyle doğrudan ya da dolaylı olarak mağdur olduğunu makul bir şekilde ifade etmesi gerektiğine; istisnai bazı durumlarda doğrudan mağdurun yakınlarının mağdur olarak nitelendirilebileceğine; her durumda, iddia edilen ihlal sonucu oluşan zararla başvuru yapan arasında doğrudan, dolaylı veya muhtemel bir bağın bulunması gerektiğine ilişkin muhtelif içtihatlarına atıf yapmıştır.[333] AİHM, MÜ-YAP tarafından last.fm ve myspace.com sitelerine FSEK ek madde 4 kapsamında ihtar yapıldığını, sitelerin ihtara rağmen iş birliğine gitmediğini ve sitelerin ilgililerinin söz konusu erişimin engellenmesi kararlarına itiraz etmediklerini belirtmiştir.

AİHM, başvurucunun talebinin fikir ve sanat eserleri alanındaki bir ihlal sebebiyle verilen erişimin engellenmesi kararının tali bir etkisine dayandığını belirtmiştir.[334] Mahkeme, internete erişimin ifade özgürlüğüne, bilgiye erişime ve bilginin yayılmasına olan katkısını yok saymamaktadır. Ancak Mahkeme, yapılan başvuru bakımından başvuranın mağdur olarak nitelendirilemeyeceğine hükmetmiştir.[335]

---

[333] *Akdeniz v. Türkiye*, para. 19.

[334] *Akdeniz v. Türkiye*, para. 23.

[335] *Akdeniz v. Türkiye*, para. 23.

Karar inşa edilirken öncelikle söz konusu sitelerin niteliği değerlendirilmiştir. AİHM, söz konusu sitelerin engellenmesinin, başvuranı müzik dinlemenin diğer pek çok yolu arasında yalnızca birinden yoksun bıraktığı; başvuranın, herhangi bir güçlük yaşamaksızın çok sayıda müzik eserine telif hakkı kuralları ihlal edilmeden, çeşitli yollardan erişim sağlayabileceği tespitini yapmıştır. Diğer bir deyişle, AİHM, internet içeriğine yönelik alternatifler bulunduğu ve bu alternatiflerin varlığının kişiye yönelik hak kısıtlaması bakımından kişiyi genel menfaati ilgilendiren bir konudaki tartışmaya girmekten alıkoymadığını belirtmiştir.

AİHM, bu kararı verirken önceki içtihatlarıyla karşılaştırmalar da yapmıştır. Mahkeme, *Tanrıkulu ve Diğerleri v. Türkiye* davasında, yayın yasağı tedbiri uygulanan günlük gazetenin okuyucularının mağdur sıfatını kabul etmediğini hatırlatmıştır.[336] Başvurana yönelik kararının da bu doğrultuda önceki içtihadıyla çelişmediğini belirtmiştir.[337]

Benzer şekilde, başvuran, last.fm ve myspace.com sitelerinin yayınlarının kendisi için özel bir önemi olduğunu ve sitelerin engellenmesinin kendisini önemli bir iletişim kaynağından mahrum bırakacağını iddia etmediği için kararın *Khurshid Mustafa ve Tarzibachi v. İsveç*[338] içtihadıyla da çelişmediğini belirtmiştir.[339] Bunun yanı sıra, sitelere erişimin engellenmesi başvuranı genel tartışmalara katılmaktan alıkoymadığı için kararın *Ashby Donald ve Diğerleri v. Fransa*[340] içtihadından farklı nitelikte olduğunu belirtmiştir.[341] Benzer kıyaslamalar *Monnat v. İsviçre*[342] ve *Ahmet Yıldırım v. Türkiye* kararlarıyla da yapılmış ve başvuran, yayıncı değil bir kullanıcı olduğu için söz konusu kararlarda varılan içtihatlarla çelişki oluşmadığına hükmedilmiştir.[343]

---

[336] **AİHM**, *Tanrıkulu ve Diğerleri v. Türkiye*, Başvuru No: 40150/98, 40153/98 ve 40160/98, 6.11. 2001.

[337] *Akdeniz v. Türkiye*, para. 25.

[338] **AİHM**, *Khurshid Mustafa ve Tarzibachi v. İsveç*, Başvuru No: 23883/06, 16.12.2008.

[339] *Akdeniz v. Türkiye*, para. 26.

[340] **AİHM**, *Ashby Donald ve Diğerleri v. Fransa*, Başvuru No: 36769/08, 10.1.2013.

[341] *Akdeniz v. Türkiye*, para. 26.

[342] **AİHM**, *Monnat v İsviçre*, Başvuru No: 73604/01, 21.9.2006.

[343] *Akdeniz v. Türkiye*, para. 27.

II. Değerlendirme

Erişimi engellemenin ölçüsüzlüğü perspektifinden bakıldığında *Yaman Akdeniz* kararının *Ahmet Yıldırım* kararından temel farkları nelerdir? AİHM, *Ahmet Yıldırım* kararındaki tespitlerine atıf yaparak bir web sitesine erişimi engelleyen her türlü tedbirin, suistimallerin önüne geçmek için kapsamı üzerinde hem sıkı bir denetim hem de etkili bir yargı kontrolü sağlayan katı bir yasal çerçevenin bir parçası olması gerektiğine, zira bunun "dolaylı sansürün" önemli etkilerini taşıyabileceğine yönelik değerlendirmesini tekrar etmiştir.[344] Ayrıca, "*bilgi alma özgürlüğü*" ve "*telif haklarının korunması*" gibi çatışan menfaatlerin dengelenmesine ilişkin olarak da yerel mahkemelere özellikle geniş bir takdir yetkisi verildiğine yönelik içtihatlarını vurgulamıştır.

Kararın, bu hâliyle *Ahmet Yıldırım* kararından ayrıldığına, başvurucu Yaman Akdeniz'in söz konusu engelleme sebebiyle mağdur sıfatı taşımadığına hükmetmiştir. Diğer bir deyişle AİHM, AİHS'nin 34. maddesi bağlamında mağdur sıfatını dar yorumlamıştır.[345]

Bir internet içeriğinin başka sitelerde de bulunuyor olması yani platformun alternatifinin varlığı, engellemeleri haklı kılar mı? AİHM, bilgi alma özgürlüğü ve telif haklarının korunması arasındaki dengede, telif haklarının korunmasını öne çıkarmış ve bu soruya telif haklarının korunması lehine geniş bir yanıt vermiş durumdadır.

Aynı kıyaslama *Ahmet Yıldırım* kararı için yapılabilir mi? Ahmet Yıldırım'ın o dönemde akademik çalışmalarını yüklemek için Google Sites dışında ücretsiz blog hizmeti alabileceği alternatifler mevcuttu. Alternatiflerin varlığının engellemeleri *ipso iure* manasız kıldığı şeklindeki bir yorumun yerindeliği tartışmalıdır. Nihayetinde, her bir sitenin kendine özgü yayın ilkeleri, içerik politikaları, barındırıldığı altyapının getirdiği farklılıkları, kullanıcı deneyimi bakımından artıları ve eksileri vardır. İki

---

[344] *Akdeniz v. Türkiye*, para. 28.

[345] Benzer konuda Avrupa Birliği Adalet Divanı farklı bir yaklaşım ortaya koymuştur. Bu konuda bkz. **Geiger, Christophe /Izyumenko, Elena** (2020) *"Blocking Orders: Assessing Tensions with Human Rights"*: Frosio, G (Editör) *Oxford Handbook of Online Intermediary Liability*, Oxford, Oxford University Press, s. 596-597.

web sitesinin bire bir alternatif olması teknik olarak neredeyse imkânsızdır. Bu sebeple, internet ortamında her bir içerik için alternatifin varlığı hususunu hassasiyetle değerlendirmek gerekir.

Haklı olarak belirtildiği üzere alternatif mecranın varlığı yorumu, ifade özgürlüğüne yönelik ciddi riskler barındırmaktadır.[346] Bu sebeple, erişimin engellenmesi kararlarından dolayı internet kullanıcılarının mağdur olarak nitelendirilmemesi, bilgi toplumunun veya daha özel bir ifadeyle ağ toplumunun ruhuna uygun bir yaklaşım değildir.

[346] **Taşkın, Cankat** (2016) *İnternete Erişim Yasakları*, Ankara, Seçkin, s. 105.

§10. CENGİZ VE DİĞERLERİ V. TÜRKİYE

AİHM'nin internet hukukuyla alakalı bir diğer kararı, 1 Aralık 2015 tarihli *Cengiz ve Diğerleri v. Türkiye* kararıdır.[347] Karar, 1 Mart 2016 tarihinde kesinleşmiştir. İki farklı başvurunun -Serkan Cengiz'in 20 Temmuz 2010 ve Yaman Akdeniz ile Kerem Altıparmak'ın 27 Aralık 2010 tarihli başvurularının- birleştirilmesi neticesinde verilmiş bir karardır. Kararın temelini, Atatürk'e hakaret nitelikli içerikler sebebiyle YouTube sitesine erişimin mahkemece engellenmesi oluşturmaktadır.

I. Davanın gelişimi

Ankara Sulh Ceza Mahkemesi, YouTube sitesinde yer alan 10 farklı sayfadaki videoların 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanun'u ihlal ettiği iddiasıyla 5 Mayıs 2008 tarihinde 5651 sayılı Kanun'un 8. maddesinin birinci fıkrasının (b) bendi uyarınca YouTube.com sitesine ve bu sitenin IP adreslerine erişimin engellenmesine karar vermiştir.

Serkan Cengiz, YouTube sitesinin kullanıcısı sıfatıyla söz konusu karara 21 Mayıs 2010 tarihinde itiraz etmiştir.[348] Talep, Ankara Sulh Ceza Mahkemesi tarafından reddedilmiştir. Aynı doğrultuda, Yaman Akdeniz ve Kerem Altıparmak tarafından da YouTube sitesinin kullanıcısı sıfatıyla 31 Mayıs 2010 tarihinde, adı geçen Mahkemenin kararına itiraz edilmiştir. İtirazda, engellemeye konu olan on videodan altısının kaldırıldığı; geriye kalan dört tanesine de Türkiye'den erişilemediği vurgulanmıştır.

İtirazı inceleyen Ankara Sulh Ceza Mahkemesi, videolara her ne kadar Türkiye'den erişilemiyor olsa da bunların hâlâ sitede barındırıldığını ve dünyadaki kullanıcıların erişimine açık olduğunu belirtmiştir. Ayrıca, soruşturma aşamasında taraf olmayan Yaman Akdeniz ve Kerem Altı-

---

[347] **AİHM**, *Cengiz ve diğerleri v. Türkiye*, Başvuru No: 48226/10 ve 14027/11, 1.12.2015.

[348] Davanın gelişimi için bkz. *Cengiz ve diğerleri v. Türkiye*, para. 6-11.

parmak'ın karara itiraz etme haklarının bulunmadığına hükmedilmiştir. Neticede, 9 Haziran 2010 tarihinde itiraz reddedilmiştir. Bu karara yapılan itiraz da Ankara Asliye Ceza Mahkemesi tarafından 2 Temmuz 2010 tarihinde reddedilerek Ankara Sulh Ceza Mahkemesinin 9 Haziran 2010 tarihli kararı hukuka uygun bulunmuştur.

Bir web sitesinin, kesintisiz yayını temin etmek adına farklı sunucularda ve IP adresleri altında yayın yapması mümkündür. YouTube sitesi de bu şekilde faaliyet göstermektedir. Beşinci bölümde etraflıca açıklandığı üzere, IP adresleri yenilenerek erişimin engellenmesi kararlarının bertaraf edilmesi pekâlâ mümkündür.[349] YouTube sitesinin farklı IP adreslerini kullanması üzerine Ankara Sulh Ceza Mahkemesi 17 Haziran 2010 tarihinde bu kez YouTube sitesi tarafından kullanılan kırk dört yeni IP adresine erişimi engellemiştir.[350]

Yaman Akdeniz ve Kerem Altıparmak, erişimin engellenmesinin kapsamını genişleten bu karara da itiraz etmişlerdir. Karara ayrıca, YouTube sitesinin temsilcileri ve İnternet Teknolojileri Derneğinin temsilcileri de itiraz etmişlerdir. İtirazı inceleyen Mahkeme, içeriklerin yayından çıkarılmadığı, sadece Türkiye'den erişimin kısıtlandığı, dünyadaki internet kullanıcılarının söz konusu videolara hâlâ erişebildiği şeklindeki tespitini tekrarlamıştır. Aynı minvalde, itirazı yapan kişilerin davaya taraf olmamaları sebebiyle itiraz haklarının bulunmadığına hükmetmiş ve itirazları 1 Temmuz 2010 tarihinde reddetmiştir. Somut olayda uygulanan 5651 sayılı Kanun'un ilgili hükmünün Anayasa'ya aykırılığı iddiasını ise nazara almamıştır. Bu karara karşı yapılan itiraz da Ankara Asliye Ceza Mahkemesi tarafından 2 Temmuz 2010 tarihinde reddedilmiştir.

Türk Hükûmeti, ilgili siteye erişimin engellenmesine ilişkin 5 Mayıs 2008 tarihli karardan önce de hukuka aykırı içerikler yer aldığı gerekçesiyle bu site hakkında verilmiş 34 adet yerel mahkeme kararı bulunduğunu; TİB'in YouTube yetkilileriyle irtibat hâlinde olduğunu; uyar-kaldır yöntemiyle bazı videoların YouTube platformundan kaldırıldığını ancak davaya konu dört videonun hâlâ global veri tabanında yer aldığını be-

[349] **§5(I)(A)**[IP değişikliği].

[350] *Cengiz ve diğerleri v. Türkiye*, para. 12-15.

lirtmiştir.[351] URL engellemesinin o dönemki altyapıda uygulanmasının teknik olarak mümkün olmadığı gerekçesiyle TİB tarafından YouTube sitesinin tamamına erişimin engellenmesinden başka bir çözüm yolu bulunmadığı da iddia edilmiştir.

Başvurucular ise Türkiye'den YouTube'a erişimin TİB tarafından 5 Mayıs 2008 tarihi ile 30 Ekim 2010 tarihleri arasında engellendiğini belirtmişlerdir.[352] Başvurucular, telif ihlali iddiasıyla yapılan bir başvuru neticesinde YouTube'a erişim engelinin 30 Ekim 2010 tarihinde kaldırıldığını; ancak, YouTube tarafından yapılan değerlendirme neticesinde söz konusu videoların tekrar yayımlandığını; çeşitli videolara yönelik detaylı inceleme yapıldığı zaman bir kısmının Atatürk'ün manevi hatırasına hakaret olarak nitelendirilebilecek içerikte olmadığını; geriye kalan kısmı için ise kapsamlı bir hukuki değerlendirme yapılmadığını iddia etmişlerdir.

II. Hukuki arka plan

AİHM, hukuki ihtilafı çözerken internet hukuku alanında öncü niteliğinde olan ve dava konusu ihtilafla aynı kanundan (5651 sayılı Kanun'dan) kaynaklanan *Ahmet Yıldırım* içtihadına atıf yapmıştır.

İlk başvurudan (2010) son karar aşamasına kadar (2015) geçen süre içerisinde Türk hukukunda farklı gelişmeler olmuştur. 5651 sayılı Kanun'da 2014 yılında yapılan bir değişiklikle, erişimin engellenmesinin belirli bir süre ile verilmesine imkân tanınmıştır. 2015 yılında yapılan başka bir değişiklikle de 5651 sayılı Kanun'a 8/A maddesi eklenerek Başbakanın ya da bir Bakanlığın bu yöndeki talebi üzerine, internet ortamındaki içeriğin kaldırılması ve/veya içeriğe erişimin engellenmesi için TİB yetkilendirilmiştir. Bu düzenlemeyle, engellemenin kural olarak URL engellemesiyle yapılması, ihlalin önlenememesi durumunda sitenin tamamına erişimin engellenmesi kararı verilmesi sağlanmıştır.

---

[351] *Cengiz ve diğerleri v. Türkiye*, para. 17.

[352] *Cengiz ve diğerleri v. Türkiye*, para. 18.

Öte yandan Türk Hükûmeti, URL filtreleme teknolojisinin Türkiye'de mevcut olmadığını; sürecin uyar-kaldır yöntemine dayalı olarak yürütüldüğünü; bu konuda çok şikâyet olmasına rağmen etkin bir koruma mekanizmasının getirilmediğini iddia etmiştir.[353]

AİHM, Türk yargısının yeni içtihatlarına da atıf yapmıştır.[354] T.C. Anayasa Mahkemesi 2 Nisan 2014 tarihinde Twitter, 29 Mayıs 2014 tarihinde ise YouTube siteleri hakkında karar vermiştir. Söz konusu kararların maddi konuları *Ahmet Yıldırım* kararı ile *Cengiz ve Diğerleri* kararıyla benzerlik göstermektedir. Anayasa Mahkemesi bu kararlarda özetle Twitter ve YouTube sitelerinin tamamına erişimin engellenmesini ölçülü bir tedbir olarak görmemiştir.

AİHM, son olarak Birleşmiş Milletler İnsan Hakları Komitesinin, Medeni ve Siyasi Haklara İlişkin Uluslararası Sözleşme'nin 19. maddesiyle ilgili olarak kabul ettiği ve internet içeriğinin kısıtlanmasına yönelik görüşlerini içeren 34 numaralı Genel Yorum'una atıf yapmıştır.[355]

III. Tarafların iddiaları

Başvuruyu inceleyen AİHM, öncelikle davanın kabul edilebilirliğine ilişkin hüküm vermiştir. Başvurucular, YouTube sitesinin engellenmesinin AİHS'nin 10. maddesinde güvence altına alınan ifade özgürlüklerine müdahale niteliğinde olduğunu iddia etmektedirler.

Türk Hükûmeti, iddialarını iki temelde ortaya koymuştur. Türk Hükûmeti, önceki bölümde etraflıca incelenen *Akdeniz v. Türkiye*[356] kararı ile *Tanrıkulu ve Diğerleri v. Türkiye* kararına atıf yaparak başvurucuların salt kullanıcı sıfatıyla bu davayı AİHM'nin önüne getiremeyeceğini ileri sürmüştür.[357]

---

[353] *Cengiz ve diğerleri v. Türkiye*, para. 23.

[354] *Cengiz ve diğerleri v. Türkiye*, para. 25-28.

[355] *Cengiz ve diğerleri v. Türkiye*, para. 27.

[356] *Akdeniz v. Türkiye* kararı için bkz. §9.

[357] *Cengiz ve diğerleri v. Türkiye*, para. 31.

Türk Hükûmetinin ikinci iddiası süre açısındadır. Türk Hükûmeti, başvurucuların, AİHM'ye YouTube'a erişimin engellenmesi kararından iki yıl sonra başvurduklarını, şayet bu tedbirler nedeniyle gerçekten mağdur olduklarını düşünselerdi bu kadar uzun süre beklememeleri gerektiğini iddia etmiştir.[358] AİHM, her iki iddiayı da yerinde görmeyerek başvuruyu kabul edilebilir bulmuştur. Özellikle *Akdeniz v. Türkiye* kararındaki kabul edilemezlik gerekçeleri dikkate alındığında Mahkemenin önemli bir içtihat değişikliğine gittiği fark edilmektedir.

Tüm başvurucular, YouTube sitesinin aktif kullanıcısı olduklarını, siteyi hem akademik amaçla hem de genel anlamda vakit geçirmek maksadıyla etkin olarak kullandıklarını belirtmişlerdir.[359] Özel olarak da "vatandaş gazeteciliği" kavramına atıf yapmışlardır. Sadece bilgi alma değil bilgi verme haklarının da etkilendiğine vurgu yapmışlardır. Kendi başvurularının *Akdeniz v. Türkiye* kararından farkını ise söz konusu kararın telif haklarına ilişkin bir ihlale dayalı olduğunu belirterek ve genel menfaati etkileyen tartışmalara katılma söz konusu olduğunda devletin daha az manevra alanı olması gerektiğine ilişkin muhtelif AİHM içtihatlarına atıf yaparak izah etmeye çalışmışlardır.[360] Başvuruculardan Yaman Akdeniz ve Kerem Altıparmak, erişimi engellenen diğer siteleri örnek göstermek suretiyle, erişimin engellenmesi tedbirinin, genel engelleme yöntemi olarak kullanılmasını sınırlayacak herhangi bir mekanizma içermediğini tartışmışlardır.[361]

Türk Hükûmeti, konu bakımından (*ratione materiae*) itirazlarını yenilemiştir.[362] Türk Hükûmeti, uygulanan tedbirin hukuka uygun nitelikte, gerekli, gerekçeli, adil bir yargılama neticesinde alınmış ve demokratik bir toplumda gerekli nitelikte olduğunu belirtmiştir.[363] Ayrıca, tedbirin en son çare olarak kullanıldığını, uyar-kaldır yöntemine de başvurulduğunu

[358] *Cengiz ve diğerleri v. Türkiye*, para. 35.
[359] *Cengiz ve diğerleri v. Türkiye*, para. 36-38.
[360] *Cengiz ve diğerleri v. Türkiye*, para. 39.
[361] *Cengiz ve diğerleri v. Türkiye*, para. 41.
[362] *Cengiz ve diğerleri v. Türkiye*, para. 42.
[363] *Cengiz ve diğerleri v. Türkiye*, para. 43.

ve 5651 sayılı Kanun'da esaslı değişiklikler yapılarak metnin iyileştirildiğini iddia etmiştir.[364]

IV. AİHM'nin tespit ve değerlendirmeleri

A. Kabul edilebilirliğe yönelik tespit ve değerlendirmeler

AİHM, bir müdahalenin varlığına yönelik tartışmaları yaptığı noktada, AİHS'nin halk davası (*actio popularis*) açma imkânı vermediğini; kişinin, bireysel başvuruda bulunabilmek için sözleşmeci devlete yüklenebilir bir eylem ya da ihmal sonucu AİHS'nin ihlal edilmesi nedeniyle doğrudan ya da dolaylı olarak mağdur olduğunu makul bir şekilde ifade etmesi gerektiğini tekrarlamıştır.[365] Mahkeme, tıpkı *Akdeniz v. Türkiye* kararında yaptığı gibi, *Tanrıkulu ve Diğerleri v. Türkiye* davasına atıf yaparak yayın yasağı tedbiri uygulanan günlük gazetenin okuyucularının mağdur sıfatını kabul etmediğini hatırlatmıştır.[366]

Cengiz ve Diğerleri v. Türkiye kararında en kapsamlı tartışma, bu kararın *Akdeniz v. Türkiye* kararından farkının ortaya konulduğu kısımda yapılmıştır. *Akdeniz v. Türkiye* kararında AİHM, bir internet sitesinin kullanıcısını, salt kullanıcı sıfatıyla AİHS bağlamında mağdur kabul etmemiştir. *Cengiz ve Diğerleri v. Türkiye* kararında AİHM, bir metodoloji geliştirmeye çalışmıştır. Mahkemeye göre, bir internet sitesi kullanıcısının mağdur olarak nitelendirilip nitelendirilemeyeceği, her davanın somut koşullarına göre müstakil olarak değerlendirilmelidir.[367] Aynı doğrultuda, kullanıcının internet sitesini kullanma şekline ve benzer tedbirin kendisi üzerinde doğurabileceği sonuçların ağırlığına da dikkat edilmelidir. Tüm bu değerlendirmeler yapılırken, internetin bireyler tarafından haber ve görüş alma ve verme özgürlüğü haklarını kullanmada başlıca araçlardan biri hâline geldiğinin de gözden kaçırılmaması gerektiği vurgulanmıştır.

---

[364] *Cengiz ve diğerleri v. Türkiye*, para. 44-45-46.

[365] *Cengiz ve diğerleri v. Türkiye*, para. 49.

[366] *Cengiz ve diğerleri v. Türkiye*, para. 49.

[367] *Cengiz ve diğerleri v. Türkiye*, para. 49.

AİHM, aktif kullanıcı-pasif kullanıcı ayrımı yapmıştır. AİHM, *Akdeniz v. Türkiye* kararına konu olan last.fm ve myspace.com siteleri ile YouTube sitesini ve başvuruculaların kullanım alışkanlıklarını karşılaştırmıştır.[368] Mahkeme, başvuruculaların YouTube sitesinin pasif kullanıcıları olmadığını; akademik faaliyetleriyle ilgili videolar paylaştıklarını belirtmiştir. Bu yönüyle AİHM, somut başvurunun *Ahmet Yıldırım v. Türkiye* kararıyla benzeştiği, aktif kullanım açısından *Akdeniz v. Türkiye* kararından ayrıştığı tespitini yapmıştır.[369]

AİHM, incelemesini bir adım öteye taşıyarak konuyu bu kez kullanıcı açısından değil, platform açısından yani YouTube sitesinin niteliğini dikkate alarak tetkik etmiştir. Bu aşamada Mahkeme, mevcut başvurunun *Akdeniz v. Türkiye* kararından farkını tartışmıştır. AİHM, *Akdeniz v. Türkiye* kararında başvurucunun, telif haklarını korumaya ilişkin kuralları ihlal etmeksizin ve herhangi bir güçlük yaşamadan çok sayıda müzik eserine farklı yöntemlerle erişebilmesinin hukuki neticeyi belirleyen esaslı unsur olduğunu hatırlatmıştır.[370] Diğer bir deyişle, Mahkeme, hizmetin ikame edilebildiğini, alternatiflerin var olduğunu kastetmiştir.

AİHM, YouTube sitesinin sanat ve müzik eserlerinin yanı sıra siyasi ve sosyal içerikler barındırdığını hatta herkesin farklı ilgilerine cevap verecek bilgiler de içerdiğini[371] belirtmiş; 5651 sayılı Kanun uyarınca YouTube sitesi aleyhine uygulanan tedbirin başvurucular için spesifik bilgiler içeren bir siteyi erişilmez kıldığı ve söz konusu spesifik bilgilere başka yöntemlerle kolayca erişilemeyeceği tespitini yapmıştır.[372] Mahkeme ayrıca, YouTube sitesinin ilgililer açısından önemli bir iletişim kaynağı olduğunun altını çizmiştir.

AİHM, YouTube sitesinin video barındıran bir web sitesi olduğunu, kullanıcıların bu site üzerinden video gönderebildiklerini, seyredebil-

---

[368] *Cengiz ve diğerleri v. Türkiye*, para. 50.

[369] *Cengiz ve diğerleri v. Türkiye*, para. 50.

[370] *Cengiz ve diğerleri v. Türkiye*, para. 51.

[371] Bu husus *Akdeniz v. Türkiye* kararında da etraflıca tartışılmıştır. Ayrıca bkz. *Khurshid Mustafa ve Tarzibachi v. İsveç* kararı.

[372] *Cengiz ve diğerleri v. Türkiye*, para. 51.

diklerini ve paylaşabildiklerini, bunun haber ve görüş alma ve verme özgürlüğünün kullanılmasında önemli bir araç olduğu hususunda şüphe duyulmadığını tekrarlamıştır.[373] Akabinde, YouTube sitesinin vatandaş gazeteciliğinin doğmasına olanak tanıdığı tespiti yapılarak bu çerçevede özellikleri, erişilebilirlik düzeyi ve bilhassa potansiyel etkisinin yanı sıra herhangi bir muadili bulunmaması dikkate alındığında başvurucular için alternatifsiz olduğunun kabul edilmesi gerektiği hükmüne varılmıştır.[374]

AİHM, kabul edilebilirlik konusunu hükme bağlarken T.C. Anayasa Mahkemesinin Twitter ve YouTube sitelerine yönelik kararlarına da atıf yapmıştır.[375] AİHM, Anayasa Mahkemesinin, aralarında Yaman Akdeniz ve Kerem Altıparmak'ın da bulunduğu aktif kullanıcıların mağdur sıfatı taşıdığını kabul etmesine yönelik tespitine ve yapılan muhakemenin neticesine katıldığını belirtmiştir.

AİHM'ye göre, mağdur sıfatını kabul etme kriterleri esnek şekilde uygulanmalı ve davanın özel koşulları dikkate alınmalıdır.[376] AİHM, tüm bu tespitler ışığında Türk Hükûmetinin başvuruculaların mağdur sıfatına yönelik itirazını reddetmiştir. Mahkeme, AİHS'nin 10. maddesinin sadece bilgilerin içeriğiyle değil, aynı zamanda bu bilgileri yayınlama araçlarıyla da ilgili olduğunu, nihayetinde araçlara yönelik her türlü sınırlamanın haber alma ve verme hakkını etkilediğini belirtmiştir.[377] *Ahmet Yıldırım v. Türkiye* kararına tekrar atıf yapılarak AİHS'nin 10. maddesinin yalnızca haber verme hakkını değil fakat aynı zamanda halkın haber alma hakkını da güvence altına aldığı vurgulanmıştır.

AİHM, yasal dayanağı her ne olursa olsun, YouTube sitesinin tamamına yönelik erişimin engellenmesi tedbirinin internetin erişilebilirliğini etkileyecek düzeyde olduğunu ve bu nedenle AİHS'nin 10. maddesi bağlamında Türk Devleti'ne sorumluluk yüklediğini; tedbirin, AİHS'nin 10. maddesiyle güvence altına alınan hakların kullanılmasında "kamu

[373] *Cengiz ve diğerleri v. Türkiye*, para. 52.
[374] *Cengiz ve diğerleri v. Türkiye*, para. 52.
[375] *Cengiz ve diğerleri v. Türkiye*, para. 53.
[376] *Cengiz ve diğerleri v. Türkiye*, para. 55.
[377] *Cengiz ve diğerleri v. Türkiye*, para. 56.

makamlarının müdahalesi" olduğunu belirtmiştir.[378] Nihayetinde başvuru kabul edilebilir bulunmuştur.

B. Müdahalenin haklılığına ilişkin tespit ve değerlendirmeler

Kabul edilebilirliğe ilişkin kararından sonra AİHM, müdahalenin haklılığını müdahaleye olanak veren düzenlemenin aşırı derecede belirsiz olduğu iddiasıyla ele almıştır. AİHM, bu bağlamda, AİHS'nin 10. maddesinin ikinci fıkrasında yer alan "kanunla öngörülme" şartını etüt etmiş; müdahalenin salt bir yasal temelinin olmasının yetmediğini, yasal düzenlemenin niteliğinin de önemli olduğunu belirtmiştir.[379] Mahkeme, daha önceki içtihatlarına atıf yaparak kanunla öngörülme şartının yerine getirilmesi için kanunun erişime açık ve etkileri bakımından öngörülebilir olması yani bu kanunun, uygulanacağı her kişinin davranışlarını düzenlemesine imkân verecek açıklıkta yazılması gerektiğini hatırlatmıştır.

Bilindiği üzere *Ahmet Yıldırım v. Türkiye* kararında da *Cengiz ve Diğerleri v. Türkiye* kararına konu olan 5651 sayılı Kanun ele alınmıştır. AİHM, *Ahmet Yıldırım v. Türkiye* kararına çapraz atıf yaparak 5651 sayılı Kanun'un, bir internet sitesinin tamamına yönelik erişim engellemesine yetki vermediğine ilişkin yorumunu *Cengiz ve Diğerleri v. Türkiye kararında* da muhafaza ettiğini göstermiştir.[380] AİHM, tespitinin, Twitter ve YouTube sitelerine ilişkin kararlarda Anayasa Mahkemesi tarafından da benimsendiğine işaret etmiştir.

AİHM nihai hükme varırken *Ahmet Yıldırım v. Türkiye* kararındaki sistematiğin neredeyse aynısını takip etmiştir: Kısıtlamalar önsel olarak (*apriori*) AİHS'ye uyumsuz değildir; yeter ki muhtemel kötüye kullanma durumlarına karşı sunulan hukuki güvence konusunda etkili olsun ve yasağın sınırlandırılması hususunda katı bir yasal çerçeve mevcut bulunsun.[381]

---

[378] *Cengiz ve diğerleri v. Türkiye*, para. 57.

[379] *Cengiz ve diğerleri v. Türkiye*, para. 59.

[380] *Cengiz ve diğerleri v. Türkiye*, para. 59.

[381] *Cengiz ve diğerleri v. Türkiye*, para. 60-62.

AİHM, yerel mahkeme tarafından YouTube sitesine erişimin tamamen engellenmesine karar verilirken mahkemeye bu yönde yetki tanıyan bir yasal hükmün bulunmadığı; Türkiye'de URL filtreleme teknolojisi olmadığından TİB'in kendisine iletilen adli kararların icrası için sitelerin tamamına erişimin engellenmesi yoluna gittiği; 5651 sayılı Kanun'un 8. maddesinde öngörülen müdahalenin, AİHS'nin gerektirdiği yasallık koşulunu karşılamadığı ve bu maddenin, başvuruculların demokratik bir toplumda hukukun üstünlüğünün gerektirdiği ölçüde yeterli bir koruma imkânına sahip olmalarına olanak tanımadığı sonucuna varmıştır.[382] AİHM, AİHS'nin 10. maddesinin birinci fıkrasında yer alan hakların "ülke sınırları gözetilmeksizin" korunduğundan hareketle, 5651 sayılı Kanun'un 8. maddesini bu hükme aykırı bulmuş ve söz konusu hükmün ihlal edildiğine karar vermiştir.[383]

V. Yargıç Paul Lemmens'in mutabık görüşü

AİHM Yargıcı Paul Lemmens, *Cengiz ve Diğerleri v. Türkiye* kararında heyetin kararına katılmakla birlikte, AİHS'nin 10. maddesinin ihlal edildiği yönündeki çoğunluk kararının gerekçesine yönelik bazı eleştiriler sunmuştur.

Yargıç Paul Lemmens, dava konusu olan müdahalenin herhangi bir yasal dayanağı bulunmamakta mıydı; ya da uygulanmasına karar verilen tedbir, yasal dayanağın sınırlarını aşmış mıydı; ya da tedbirin dayanağını oluşturan yasal hüküm yeterince açık/belli değil miydi; ya da bu yasal dayanak, yetkili makama çok geniş bir yetki mi vermekteydi sorularını sormuştur.[384] Yargıç Paul Lemmens'e göre, erişimin engellenmesi tedbiri kanunla öngörülmemiştir. İç hukuku yorumlama ve uygulama görevinin öncelikle ulusal makamlara ve özellikle mahkemelere düştüğünü hatırlatan Yargıç Paul Lemmens, T.C. Anayasa Mahkemesinin, 29 Mayıs 2014 tarihli YouTube kararında 5651 sayılı Kanun'un 8. maddesinin bir sitenin tamamına erişimin engellenmesine açıkça izin vermediğine hükmettiğini

[382] *Cengiz ve diğerleri v. Türkiye*, para. 63-65.

[383] *Cengiz ve diğerleri v. Türkiye*, para. 65.

[384] *Cengiz ve diğerleri v. Türkiye*, Yargıç Paul Lemmens'in Mutabık Görüşü.

ifade etmiştir. Buradan hareket eden Yargıç Paul Lemmens, AİHM'nin tedbirin kanunla öngörülmediği sonucuna varması gerektiğini ve 5651 sayılı Kanun'un öngörülebilirliğini veya ifade özgürlüğüne yönelik keyfî müdahalelere karşı sunduğu korumayı inceleme aşamasına geçmesine gerek olmadığını belirtmiştir.[385]

Yargıç Paul Lemmens'in değindiği bir diğer konu, *Cengiz ve Diğerleri v. Türkiye* kararına yönelik başvuru yapıldıktan sonra 5651 sayılı Kanun'da gerçekleştirilen değişikliklerin, özelde 8/A maddesinin, incelenmesi hususudur. AİHM, mevcut dava açıldıktan sonra 5651 sayılı Kanun'da değişiklik yapıldığını not etmiş, ancak olayların meydana geldiği sırada veya hâlihazırda internet sitelerine erişimin engellenmesinin hukuki dayanaklarının AİHS ile uyumluluğu hususunda soyut olarak (*in abstracto*) karar vermekle görevli olmadığını belirtmiştir.[386] AİHM, buna karşılık, söz konusu hükümlerin uygulanmasının, başvuranların AİHS'nin 10. maddesiyle güvence altına alınan ifade özgürlüğü haklarına etkisinin somut olarak (*in concreto*) değerlendirilmesi gerektiği sonucuna varmıştır.

Yargıç Paul Lemmens'e göre, AİHM, başvuru sonrası yapılan yasal değişiklikleri incelemeliydi; zira, AİHM 5651 sayılı Kanun'a eklenen 8/A maddesi hakkında soyut olarak (*in abstracto*) karar vermek zorunda değildir. Keza Yargıç Paul Lemmens'e göre AİHM ihtilaf konusu müdahalenin amacı ve gerekliliğini, en azından *obiter dictum* olarak incelemiş olsaydı verdiği karar, 5651 sayılı Kanun'un 8. maddesine dayalı uygulamalar gibi yeni 8/A maddesine dayanan uygulamaların da karşılaması gereken ilkeler hakkında Türk makamlarını ve vatandaşlarını aydınlatabilirdi.[387]

VI. Değerlendirme

AİHM'nin *Cengiz ve Diğerleri v. Türkiye* kararı *Ahmet Yıldırım v. Türkiye* kararıyla paralellik arz ederken, *Akdeniz v. Türkiye* kararından esaslı hatta AİHS'nin yorumlanması bakımından radikal sayılabilecek farklılıklar içermektedir.

---

[385] *Cengiz ve diğerleri v. Türkiye*, Yargıç Paul Lemmens'in Mutabık Görüşü, para. 3.

[386] *Cengiz ve diğerleri v. Türkiye*, para. 75.

[387] *Cengiz ve diğerleri v. Türkiye*, Yargıç Paul Lemmens'in Mutabık Görüşü, para. 4.

Ahmet Yıldırım v. Türkiye kararıyla benzerlik, 5651 sayılı Kanun'un yasayla öngörülme şartını sağlamasına ilişkindir. AİHM'nin bu konudaki yorumu tutarlıdır. AİHM, kanunla öngörülme şartının yerine getirilmesi için kanunun erişime açık ve etkileri bakımından öngörülebilir olmasını yani bir kanunun uygulanacağı her kişinin bu yasa uyarınca davranışlarını düzenlemesine imkân verecek açıklıkta yazılması gerektiğini hatırlatmıştır.

Öte yandan AİHM, AİHS bağlamında mağdur kavramını *Cengiz ve Diğerleri v. Türkiye* kararında yeniden tanımlamış, *Akdeniz v. Türkiye* kararından radikal şekilde sapmıştır. AİHM, her ne kadar AİHS'nin halk davası (*actio popularis*) açma imkânı vermediği kararını tekrarlasa da mağdur kavramının içine bir web sitesinin aktif kullanıcılarını da katarak *de jure* olmasa bile *de facto* olarak halk davasının önünü açmıştır. "*Actio popularis*" yeniden yorumlanmış ve genişletici bir yorum yapılmıştır. Tabii ki bu muhakemenin çok sistematik ve güçlü olduğunu söylemek zordur, eleştirilecek yönleri vardır.

AİHM, basit kullanıcı-aktif kullanıcı ayrımı yapmıştır. İnteraktif kullanımla pasif kullanıma birbirinden farklı hukuki statüler vermiştir. Şayet bir kullanıcı YouTube gibi çok amaçlı bir platformu bilgiye erişim, bilgiyi/fikri yayma ve iletişim amaçlarıyla kullanıyorsa ve bu platforma yönelik kamusal ve esaslı bir müdahale yapılırsa bu kullanıcı için AİHS'nin 34. maddesinde düzenlenen mağdur kavramının unsurları oluşmuştur. Bu durumda başvurunun kabul edilebilirliği pekâlâ mümkündür. AİHM, *Akdeniz v. Türkiye* kararında müziğe erişimi engellenen kullanıcıyı mağdur olarak kabul etmezken *Cengiz ve Diğerleri v. Türkiye* kararında YouTube sitesini interaktif şekilde kullanan başvuruculari mağdur olarak kabul etmiştir.

Akdeniz v. Türkiye kararında bir müzik paylaşım sitesine yönelik kısıtlama sebebiyle yapılan başvuruda sitenin aktif kullanıcısının başvurusunu kabul edilebilir görmeyen AİHM, engellemeye konu site YouTube sitesi olunca çok farklı bir yorum geliştirmiştir. *Akdeniz v. Türkiye* kararında bir sitenin alternatifinin bulunmasını müdahalenin haklılığını tespit ederken temel bir kriter olarak gözeten AİHM, YouTube sitesini çok farklı bir yerde konumlandırmış ve fonksiyonlarını dikkate alarak sitenin başvurucular için alternatifsiz olduğu hükmüne varmıştır. AİHM'nin *Cengiz ve Diğerleri v. Türkiye* kararındaki esasa ilişkin tüm değerlendir-

melerine katılmakla birlikte YouTube sitesine yönelik böyle bir yorum yapılmasının yerinde olmadığı kanaatindeyiz.

YouTube sitesi alternatifsiz değildir. İnternet ortamında bu sitenin ikame edilmesi mümkündür, bire bir[388] olmasa da alternatifleri vardır. *Akdeniz v. Türkiye* kararında müzik sitesi için alternatiflerin mevcudiyetine işaret edip, kabul edilebilirliği hükme bağlarken bunu dikkate alan AİHM, YouTube sitesi için farklı bir yorum getirmiştir.

AİHM'nin *Ahmet Yıldırım v. Türkiye* ve *Cengiz ve Diğerleri v. Türkiye* kararlarında değinmediği bir husus ise erişimin engellenmesi tedbirlerinin etkisidir. Beşinci bölümde detaylı olarak incelendiği üzere, erişimin engellenmesi tedbirlerinin kolayca aşılması mümkündür. YouTube sitesi, erişimin engellendiği dönemde bile Türkiye'de en çok ziyaret edilen siteler arasında yer almaya devam etmiştir. Engellemenin etkisi AİHM tarafından verilen kararın sonucuna etki etmeyecek olsa da erişimin engellenmesi konusu ikinci kez ele alınıyorken Mahkemenin bu konuda daha yol gösterici olması beklenirdi.

AİHM'nin T.C. Anayasa Mahkemesinin Twiter ve YouTube kararlarına atıf yapması yerinde bir yaklaşım olmuştur.[389] Nihayetinde, Yargıç Lemmens tarafından da vurgulandığı üzere iç hukuku yorumlama ve uygulama görevi öncelikle ulusal makamlara ve özellikle mahkemelere düşmektedir.

---

[388] Önceki bölümde *Akdeniz v. Türkiye* kararında da belirtildiği üzere her bir sitenin kendine özgü yayın ilkeleri, içerik politikaları, barındırıldığı altyapının getirdiği farklılıkları, kullanıcı deneyimi bakımından artıları ve eksileri vardır. İki web sitesinin bire bir alternatif olması teknik olarak neredeyse imkânsızdır.

[389] *Cengiz ve Diğerleri v. Türkiye* kararının 25. paragrafında Türk Anayasa Mahkemesinin Twitter kararına yer verilmiştir. Bu kısmın son cümlesinde, Anayasa Mahkemesinin hükme varırken AİHM'nin *Ahmet Yıldırım* kararına atıf yaptığı ifadesi geçmektedir. Hâlbuki, 2 Nisan 2014 tarihli Anayasa Mahkemesi kararında *Ahmet Yıldırım v. Türkiye* kararına herhangi bir atıf yer almamaktadır. Anayasa Mahkemesinin ilgili kararının da teknik olarak en çok eleştirilen kısımlarından birisi budur. Nihayetinde, Anayasa Mahkemesi ilk kez erişimin engellenmesi tedbirine yönelik karar verirken bu alandaki ilk karar olan ve 5651 sayılı Kanun'la doğrudan ilgisi bulunan AİHM içtihadına yer vermemiştir. Anayasa Mahkemesi kararında birçok AİHM içtihadına atıf vardır ancak *Ahmet Yıldırım* kararına bir atıf yoktur. Hâliyle bu bir eksikliktir.

§11. DELFİ AS V. ESTONYA

AİHM'nin bu aşamaya kadar incelenen kararları, internet ortamında yer alan içeriğe erişimin engellenmesinin hukukiliğine ilişkindir. AİHM'nin internet ortamındaki içerikten dolayı hizmet sağlayıcıların hukuki sorumluluğuna ilişkin ilk kararı ise *Delfi AS v. Estonya* kararıdır.[390] AİHM, bir internet haber portalının hakaret niteliğindeki anonim yorumlardan sorumlu tutulmasını AİHS'nin 10. maddesinin ihlali olarak görmemiştir.

İnternet haber portallarının sorumluluğunu AİHS'nin 10. maddesinin ikinci fıkrası bağlamında ele alan Mahkeme, hakaret niteliğinde veya diğer tür hukuka aykırı ifadeler kullanılması durumunda ilgili kişilere etkin bir tazmin yolu sunulması gerektiğinin altını çizmiştir.

Haber portalının sahipleri, sadece yer sağlama hizmeti sunduklarından bahisle, barındırdıkları içerikleri kontrol etmekle yükümlü olmadıklarını ve özellikle verinin büyüklüğü dikkate alındığında bunun teknik bakımdan uygulanabilir olmadığını ileri sürmüşlerdir.

İç hukukun, kullanıcı yorumları sebebiyle haber portallarının sorumlu tutulmasına ilişkin öngörülebilir bir hüküm içerdiği tespitini yapan AİHM, internet haber portallarının ekonomik nitelikte bir faaliyet yürüttüğünü, kullanıcı yorumları bakımından pasif, salt teknik bir hizmet sağlayıcı niteliğinde olmadığını ve bu sebeple içerikten sorumlu tutulacağını belirtmiştir. Bu hükme varılırken, anonim yorumların yazarlarına karşı hak arama imkânlarının teknik sebeplerle kısıtlı olması gerçeği de dikkate alınmıştır.

AİHM, kararının özel sansüre (*private censorship*) yol açıp açmayacağını da tartışmış ve nefret söylemi ile şiddet çağrısı barındıran içeriklerin

---

[390] **AİHM**, *Delfi AS v. Estonya*, Başvuru No: 64569/09, 16.6.2015.; Kararın Adalet Bakanlığı tarafından yapılan Türkçe tercümesi için bkz. <http://www.inhak.adalet.gov.tr/ara/karar/delfias_karari.pdf>

filtrelenmesinin bu bağlamda bir sansür olarak nitelendirilemeyeceğini, başkalarının hak ve menfaatlerini dengelemek için uygun bir araç olduğunu belirtmiştir. Tüm bu sebeplerle, üçüncü kişiler tarafından yazılan hukuka aykırı yorumlardan dolayı bir internet haber portalının sahiplerinin tazminata mahkûm edilmesinin AİHS'nin 10. maddesi bağlamında ölçüsüz bir müdahale olmadığına karar verilmiştir.

I. Davanın gelişimi

Delfi AS, Estonya'da kurulu bir şirket olup, işletmiş olduğu internet haber sitesinde yer alan üçüncü kişi yorumlarından sorumlu tutulması sebebiyle AİHS'nin 10. maddesinde koruma altına alınan ifade özgürlüğü hakkının ihlal edildiğini iddia etmiştir. Delfi AS, Estonya'nın internet üzerindeki en büyük haber sitelerinden biridir. Estonya'da Estonca ve Rusça haberler yayınlamakta ve ayrıca Letonya ile Litvanya'da faaliyet göstermektedir.

Delfi AS sitesi, Web 2.0 özelliği olan klasik bir internet portalıdır. Site editörleri tarafından haberler paylaşılmakta, kullanıcılar bu haberlere yorum yapmakta, hem haberler hem de bu yorumlar internet ortamında yayımlanmaktadır. Hukuki sorumluluğa ışık tutmak adına, sitenin ihtilafa konu olan dönemde nasıl çalıştığının açıklanmasında fayda vardır. Kararda açıklandığı üzere söz konusu dönemde:[391]

- Haberlerin sonunda, "yorum ekle" ibaresi ile yorumlar, yorum sahibinin ismi ve e-posta adresi (isteğe bağlı) için ayrılmış alanlar bulunmaktaydı. Bu alanların altında, "yorumu yayınla" ve "yorumları oku" ibareleri bulunan butonlar yer almaktaydı.
- Başka kişilerce eklenen yorumları okumaya ayrılan kısım, "yorumları oku" butonuna tıklamak suretiyle erişilebilen ayrı bir alandı.
- Yorumlar otomatik olarak yüklenmekte ve dolayısıyla başvuran şirketin düzeltme veya denetiminden geçmemekteydi.

[391] *Delfi AS v. Estonya*, para. 12.

- Haber makaleleri günde yaklaşık 10.000 okuyucu yorumu almakta ve bu yorumların çoğunluğu rumuzlar altında gönderilmekteydi.

Kısacası, herhangi bir internet kullanıcısı rastgele bir rumuz belirtmek suretiyle, herhangi bir haberin altında dilediği içeriği paylaşabilmekteydi. Bu sistemin kötüye kullanılmasını önlemek adına Delfi AS şirketi tarafından bir mekanizma geliştirilip geliştirilmediği sorunsalı da kararda etüt edilmiştir. Kararın ilgili kısmında açıklandığı üzere:[392]

- Sitede bir uyar-kaldır sistemi mevcuttu. Bu sistem sayesinde herhangi bir okuyucu bir yorumu *leim* (Estoncada internet üzerindeki hakaret içerikli, alaycı veya nefret uyandırıcı iletiler için kullanılan bir sözcük) olarak işaretleyebilmekte ve ilgili yorum, sayfadan hızlı bir şekilde kaldırılmaktaydı.
- Dahası, edebe aykırı bir kısım sözcük köklerini içeren yorumların otomatik olarak silinmesine yönelik bir sistem bulunmaktaydı.
- Bunun yanı sıra, hakaret içerikli bir yorumdan mağdur olan kişi şirkete doğrudan ihbarda bulunabilmekte ve bu durumda, bahse konu yorum derhâl siteden kaldırılmaktaydı.

Delfi AS şirketi, sitede yayımlanacak yorumlara ilişkin bir içerik politikası belirlemiştir. Bu politikada yorumların kendi kurumsal görüşünü yansıtmadığını belirtmiş, yorumların herhangi bir editoryal süreçten geçmediğinin altını çizmiş, içeriklerden kullanıcıların bizzat sorumlu olduğunu vurgulamış, uyar-kaldır mekanizmasını izah etmiştir.[393] Bu bağlamda, sitede düşmanlığa, şiddete ve yasa dışı faaliyetlere teşvik eden; tehdit, hakaret, konu dışı bağlantılar, istenmeyen e-postalar ya da reklamlar, asılsız ve/veya konu dışı olan, edebe aykırı ifadeler ve kaba sözler içeren yorumlar yasaklanmıştır.

Estonya Hükûmeti, Delfi AS'nin hakaret içerikli ve aşağılayıcı yorumlar yayınlama konusunda Estonya'da kötü bir geçmişinin olduğunu

[392] *Delfi AS v. Estonya*, para. 13.

[393] *Delfi AS v. Estonya*, para. 14.

iddia etmiş ve hakarete uğrayan kişilerin, Delfi AS aleyhine dava açıp tazminat talep etme suretiyle onur ve itibarlarını savunma haklarının bulunduğu konusuna vurgu yapmıştır.[394]

24 Ocak 2006 tarihinde Delfi AS haber sitesinde, halka açık feribot taşımacılığı hizmeti sağlayan SLK şirketine atfen "SLK, Planlanan Buz Yolunu Yok Etti" başlıklı bir haber yayımlanmıştır. Bu haber, yayımlanmasının ardından 24 ve 25 Ocak 2006 tarihlerinde 185 yorum almıştır. Yorumlardan yaklaşık 20 tanesi SLK şirketinin hissedarı Bay L'ye yönelik tehdit içermekte ve onur kırıcı nitelikteydi.[395]

9 Mart 2006 tarihinde Bay L, avukatı aracılığıyla ilgili haberin altında yer alan ve kişilik haklarına saldırı niteliğindeki yorumların kaldırılması ve bu yorumlar sebebiyle kendisine manevi tazminat ödenmesi talebinde bulunmuştur. Talebin yapıldığı aynı gün (ki içeriğin yayımlanmasından altı hafta sonrasına tekabül etmektedir), Delfi AS şirketi tarafından hakaret niteliğindeki tüm yorumlar kaldırılmış; Bay L'ye uyar-kaldır kapsamındaki süreçle ilgili bilgi verilmiş ancak Bay L'nin tazminat talebi reddedilmiştir.

A. Harju İlk Derece Mahkemesinde tazminat davasına ilişkin ilk inceleme

Bay L, 2006 yılında Delfi AS şirketi aleyhine tazminat davası açmıştır. Harju İlk Derece Mahkemesi, 25 Haziran 2007 tarihli kararıyla tazminat talebini reddetmiştir.[396] Mahkeme, Delfi AS şirketinin, AB e-Ticaret Direktifi'ne dayalı olarak hazırlanan ve Estonya'da yürürlükte bulunan Bilgi Toplumu Hizmetleri Kanunu'na göre sorumluluktan muaf olduğuna hükmetmiştir. Mahkeme, sitenin haber alanıyla yorum alanı arasında ayrım yaparak Delfi AS şirketinin yorum kısmındaki faaliyetinin temelde mekanik ve pasif nitelikte olduğunu, şirketin yorumların yayınlayıcısı

[394] *Delfi AS v. Estonya*, para. 15.
[395] *Delfi AS v. Estonya*, para. 16.
[396] *Delfi AS v. Estonya*, para. 23.

olarak düşünülmesi mümkün olmadığı gibi yorumları denetlemek gibi bir yükümlülüğünün de bulunmadığını belirtmiştir.[397]

B. Harju İlk Derece Mahkemesinde tazminat davasına ilişkin ikinci inceleme

Bay L, yerel mahkemenin kararına itiraz etmiştir. İtirazı inceleyen Tallinn İstinaf Mahkemesi, somut olaydaki sorumsuzluğun Bilgi Toplumu Hizmetleri Kanunu kapsamında olmadığına karar vermiş ve itiraz kabul edilerek dosya tekrar yerel mahkemenin önüne gelmiştir. Harju İlk Derece Mahkemesi, istinaf mahkemesinin tespitleri çerçevesinde dosyayı baştan muhakeme etmiştir.

Harju İlk Derece Mahkemesi öncelikle şu belirlemeleri yapmıştır: Delfi AS şirketi, internet sitesinde yayımlanan yorumların düzeltilmediğine, içerik politikasına aykırı yorum eklemenin yasak olduğuna ve bu tür yorumları kaldırma hakkını saklı tuttuğuna dair bir not koymuştur. Şirket ayrıca kullanıcıların, her türlü uygunsuz yorum hakkında kendisine bildirimde bulunabildiği bir sistem kurmuştur. Mahkeme, bu uygulamanın yetersiz olduğuna ve başkalarının kişilik haklarına yönelik yeterli koruma sağlamadığına kanaat getirmiştir.[398] Mahkeme, yorumları yayınlayanın Delfi AS şirketinin kendisi olduğunun değerlendirilmesi gerektiğine ve şirketin yorumların içeriğinden sorumlu olmadığına dair bir sorumsuzluk beyanı yayınlayarak sorumluluğu üzerinden atamayacağına hükmetmiştir.

Bu tespitleri yaptıktan sonra Harju İlk Derece Mahkemesi, yorumların çoğunun kaba, aşağılayıcı ve hakaret içerikli olduğunu ve L'nin onur, haysiyet ve itibarını zedelediğini kaydetmiştir. Bu yorumların, haklı eleştiri sınırlarını aştığını ve adi hakaret derecesine vardığını tespit eden Mahkeme, ifade özgürlüğünün mevzubahis yorumları kapsayacak kadar geniş olmadığını belirterek Bay L'nin kişilik haklarının ihlal edildiği sonucuna varmıştır.[399]

---

[397] *Delfi AS v. Estonya*, para. 23.

[398] *Delfi AS v. Estonya*, para. 26.

[399] *Delfi AS v. Estonya*, para. 27.

C. Tallinn İstinaf Mahkemesinin kararı

Tallinn İstinaf Mahkemesi, Harju İlk Derece Mahkemesinin kararını 16 Aralık 2008 tarihinde onamıştır. İstinaf Mahkemesi, haber sitesine eklenen yorumlar üzerinde Delfi AS şirketinin ön denetim gerçekleştirmeye mecbur olmadığını vurgulamış; bununla birlikte, ön denetim gerçekleştirmemeyi tercih ettiği için, hukuka aykırı yorumların siteden hızla kaldırılmasını sağlayacak etkili başka bir sistem kurması gerektiğini belirtmiştir.[400] İstinaf Mahkemesi, Delfi AS tarafından alınan tedbirlerin yetersiz olduğuna ve yorumları denetleme külfetinin olası mağdurlar üzerine yüklenmesinin iyi niyet ilkesine aykırı olduğuna kanaat getirmiştir.

İstinaf Mahkemesi, Delfi AS şirketinin, Bilgi Toplumu Hizmetleri Kanunu'na istinaden sorumluluğunun ortadan kalkmış olduğu yönündeki iddiasını reddetmiştir. Mahkeme, Delfi AS'nin söz konusu yorumlar bakımından sadece teknik bir aracı konumunda bulunmadığını, faaliyetlerinin yalnızca teknik, otomatik ve pasif olarak nitelendirilemeyeceğini, zira kullanıcıları yorum eklemeye davet ettiğini kaydetmiştir.[401] İstinaf Mahkemesine göre Delfi AS şirketi teknik hizmetlerden ziyade bir içerik hizmetleri sağlayıcısı olarak nitelendirilmelidir.

D. Estonya Yüksek Mahkemesinin kararı

Delfi AS, Tallinn İstinaf Mahkemesinin kararını temyiz etmiştir. Estonya Yüksek Mahkemesi, şirketin temyiz başvurusunu 10 Haziran 2009 tarihinde reddetmiştir. İstinaf Mahkemesinin kararı esas yönünden onanmış ancak gerekçesi kısmen değiştirilmiştir.[402] Yüksek Mahkemeye göre konu, Bilgi Toplumu Hizmetleri Kanunu değil, Borçlar Kanunu bağlamında ele alınmalıdır. Mahkeme, bilgi toplumu hizmet sağlayıcısı olarak nitelendirilmek için hizmet sağlayıcının, aktardığı veya sakladığı içeriğe ilişkin ne bilgisinin ne de kontrolünün olması gerektiğini, mevcut olayda Delfi AS şirketinin bir içerik sağlayıcı olarak nitelendirilmesi gerektiğini belirtmiştir.

---

[400] *Delfi AS v. Estonya*, para. 28.

[401] *Delfi AS v. Estonya*, para. 29.

[402] *Delfi AS v. Estonya*, para. 31.

Yüksek Mahkeme, kararını verirken haberlere yapılan yorumların işleyişini, Delfi AS şirketinin bu yorumlara ilişkin yaklaşımını ve sistemin teknik boyutunu etraflıca değerlendirmiştir. Yüksek Mahkemeye göre, Delfi AS'nin yorumların yayımlanmasındaki dahli sadece teknik, otomatik ve pasif nitelikte olmayıp şirektin hedefi salt aracılık hizmeti sağlamak değildir. Yüksek Mahkeme bu yargıya Delfi AS'nin, haberlere yorum yapmaları için kullanıcılarını aktif şekilde davet etmesinden ulaşmaktadır. Nihayetinde, Delfi AS haber sitesinin ziyaret edilme sayısı, yapılmış olan yorumların sayısına bağlı olup sitede yayımlanan reklamlardan elde edilen gelir de dolayısıyla ziyaretçi sayısına bağlıdır. Buradan yola çıkan Yüksek Mahkeme, Delfi AS'nin, yorumlardan sağladığı ekonomik bir menfaatinin olduğunu; yorumları kendisinin yazmamış olmasının yorum alanı üzerinde Delfi AS'nin hiçbir denetimi bulunmadığı anlamına gelmediğini belirtmiştir.

Yüksek Mahkeme, Delfi AS'nin hizmetlerinden faydalanan bir kimsenin, eklemiş olduğu yorum üzerinde değişiklik yapamadığını ya da yorumunu silemediğini, kullanıcıların yalnızca uygunsuz yorumları bildirme olanağına sahip olduğunu, bu nedenle Delfi AS'nin eklenen yorumların hangilerinin yayımlanıp hangilerinin yayımlanmayacağını belirlediğinin altını çizmiştir. Ayrıca, Delfi AS şirketinin bu imkânı hiç kullanmamasının, yorumların yayımlanması üzerinde denetiminin olmadığı anlamına gelmediğini vurgulamıştır. Basılı medya ile dijital medya arasında bir karşılaştırma da yapan Yüksek Mahkeme, hem basılı medya yayıncısının hem internet sitesi operatörünün, girişimci sıfatıyla, yorumların yayımlanmasından ekonomik menfaatlerinin bulunması sebebiyle yayımlayıcı/ifşa eden kişi olacaklarını belirtmiştir.

Delfi AS şirketinin, internet sitesinde üçüncü kişiler tarafından yapılan yorumlar sebebiyle sorumlu olduğu tespitini yapan Yüksek Mahkeme, hukuki sorumluluğun Estonya Borçlar Kanunu'na göre çözülmesi gerektiğini belirterek esasa ilişkin değerlendirmeler yapmıştır. Somut olaydaki içeriklerin açıkça Bay L'nin onur ve şerefine saldırı niteliğinde olduğu, bu ifadelerin basın özgürlüğü kapsamında korunamayacağı, Bay L'nin hem yorumları yapanlar hem Delfi AS şirketi aleyhine tazminat talebinde bulunmasının mümkün olduğu belirtilmiştir.

Mahkeme, Delfi AS şirketinin, yorumların kanuna aykırı niteliğinin farkında olmadığı ve farkında olmasına gerek de bulunmadığı yönündeki iddiasını mesnetsiz görmüştür. Mahkemeye göre Delfi AS'nin, zarara yol açmaktan kaçınılmasına ilişkin kanuni yükümlülük nedeniyle, açıkça kanuna aykırı içerik taşıyan yorumların yayımlanmasına engel olması gerekirdi. Delfi AS'nin bu hususta herhangi bir eylemde bulunmamasının hukuka aykırı olduğuna hükmeden Yüksek Mahkeme, şirketin, kusursuzluğunu ispat edemediğine karar vermiştir.

E. Hükmün Delfi AS şirketi tarafından yerine getirilmesi ve şirketin iş modelindeki değişiklikler

Delfi AS şirketi, davayı kaybettikten sonra, tekrar bir hukuki sorumluluk altına girmemek adına haber sitesindeki yorum bölümünün işleyişini esaslı olarak değiştirmiştir. Kararda aktarıldığı üzere, 1 Ekim 2009 tarihinde kendi internet sitesinde yayımladığı bilgiye göre:[403]

- Delfi AS, yorum sahibi yorum kurallarını okuyup kabul edinceye dek onur kırıcı yorumlarda bulunan kişilerin yeni bir yorum eklemesine izin vermemeye başlamıştır.
- Delfi AS, siteye eklenen yorumlar üzerinde ek denetim gerçekleştiren moderatörlerden oluşan bir ekip kurmuştur.
- Moderatörler öncelikle uygunsuz yorumlara ilişkin tüm kullanıcı bildirimlerini gözden geçirmekte; bunun yanı sıra, yorumların yorum kurallarına uygunluğunu da denetlemektedirler.

Yayımlanan bilgilere göre, 2009 yılının Ağustos ayında Delfi AS okuyucularınca eklenen yorumların sayısı 190.000'dir. Delfi AS moderatörleri, ağırlıklı olarak istenmeyen veya yersiz içeriklere sahip 15.000 yorumu (yaklaşık %8) silmiştir. Yine aynı istatistiklere göre, hakaret içerikli yorumlar, toplam yorum sayısının %0,5'inden daha azdır.

[403] *Delfi AS v. Estonya*, para. 32.

II. Hukuki arka plan

AİHM, *Delfi AS v. Estonya* kararını verirken Avrupa Konseyinin muhtelif politik deklarasyonlarına, Avrupa Birliği düzenlemelerine ve Avrupa Birliği Adalet Divanı kararlarına atıf yapmıştır. Mahkeme, Avrupa Konseyinin 28 Mayıs 2003 tarihli İnternette İletişim Özgürlüğüne İlişkin Deklarasyon'una, 7 Kasım 2007 tarihli İnternetin Kamu Hizmeti Boyutunun Geliştirilmesine Yönelik Önlemlere İlişkin Tavsiye Kararı'na, 21 Eylül 2011 tarihli Yeni Bir Medya Nosyonuna İlişkin Tavsiye Kararı'na, 16 Nisan 2014 tarihli İnternet Kullanıcıları İçin İnsan Hakları Rehberi'ne, Birleşmiş Milletler İnsan Hakları Konseyi Özel Raportörü Frank La Rue'nün düşünce ve ifade özgürlüğü hakkının desteklenmesi ve korunmasına ilişkin 16 Mayıs 2011 tarihli Rapor'una (A/HRC/17/27)[404] atıf yapmıştır.

Mahkeme, ayrıca, B e-Ticaret Direktifi'ne, (mülga) 98/34/AT sayılı Bilgi Toplumu Hizmetleri Direktifi'ne[405] ve Avrupa Birliği Adalet Divanının muhtelif kararlarına[406] atıf yapmıştır. Mukayeseli hukuka da değinen Mahkeme, operatörün, ister ön sansür, redaksiyon, alıcıların seçilmesi, daha önce tanımlanmış bir konu üzerinde yorum yapılması talebi yoluyla ister içeriği kendi içeriği olarak kabul etmesi yoluyla olsun, çevrim içi yayınlama öncesinde üçüncü taraf içeriklerine müdahale seviyesi arttıkça, çevrim içi yayımlanan herhangi bir içerikten sorumlu tutulma olasılığının da aynı ölçüde artacağı tespitini yapmıştır.[407]

---

[404] **Birleşmiş Milletler**, "*The UN Human Rights Council's Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression of 16 May 2011 to the Human Rights Council (A/HRC/17/27)*" <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G11/132/01/PDF/G1113201.pdf?OpenElement>

[405] Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations OJ L 204, 21.7.1998.

[406] **Avrupa Birliği Adalet Divanı**, Birleştirilen C-236/08 - C-238/08 Google Fransa ve Google davaları, L'Oréal ve Diğerleri, C-324/09, Scarlet Extended C-70/10 davası, SABAM, C-360/10 davası, Google İspanya ve Google, C-131/12 davası, Papasavvas, C-291/13 davası.

[407] *Delfi AS v. Estonya*, para. 58.

III. AİHM Birinci Dairenin kararı

Delfi AS v. Estonya ihtilafı, Büyük Dairenin önüne gelmeden evvel Birinci Daire tarafından karara bağlanmıştır. Büyük Daire, Birinci Dairenin müdahalenin kanunda öngörülmesine, ifade hürriyetine müdahalenin ölçülülüğüne ve yorumlardan sorumluluğa ilişkin değerlendirmelerine atıf yapmıştır.[408] Birinci Dairenin kararı, bire bir olmasa da Estonya Yüksek Mahkemesinin tespitleriyle örtüşmektedir.

IV. Delfi AS şirketinin iddiaları

Delfi AS şirketi, kullanıcılar tarafından oluşturulan içeriklerin kişilerin toplumsal tartışmalara katılmasına, bu sayede demokrasi ve ifade özgürlüğünün gerçekleştirilmesine katkı sağladığına vurgu yapmıştır.[409] Delfi AS şirketi, uyar-kaldır yönteminin etkili bir koruma yöntemi olduğunu ileri sürmüş; AİHM tarafından etkili bir yöntem olarak değerlendirilmezse kimliği bilinmeyen kişilerce yapılan açıklamaların yasaklanmasının ya da aracıların, sonradan doğabilecek olası bir sorumluluktan kaçınmak adına tedbirli davranarak yorumcuların iletişim özgürlüklerini keyfî olarak kısıtlamasının söz konusu olacağını vurgulamıştır.[410]

Delfi AS şirketi, yorumlarla ilgili faaliyetlerinin aracılık faaliyeti olarak nitelendirilmesi gerektiğini belirtmiştir. Şirket, bu bağlamda çok önemli ve haklı bir argüman ileri sürmüştür: İnternet ortamında aracılık faaliyeti gösteren hizmet sağlayıcılar, kullanıcılar tarafından oluşturulan içeriklerin yasalara uygunluğuna karar verecek konumda değildir; nihayetinde, hakaret nitelikli içerikler bağlamında itibarına neyin zarar verdiğini ancak kişinin kendisi belirleyebilecektir.[411]

Delfi AS şirketi, başkalarına ait içerikten sorumlu tutulmasının, ifade özgürlüğüne yönelik bir müdahalenin kanunla öngörülmesi gerek-

[408] *Delfi AS v. Estonya*, para. 58.
[409] *Delfi AS v. Estonya*, para. 66.
[410] *Delfi AS v. Estonya*, para. 67.
[411] *Delfi AS v. Estonya*, para. 68.

tiği şartını taşımadığını iddia etmiştir.[412] Delfi AS, bir aracının, haberdar olmadığı içeriğin yayıncısı olarak değerlendirilebileceğini öngören herhangi bir mevzuat ya da içtihadın bulunmadığını; aksine, geçerli düzenlemelerin, hizmet sağlayıcılara üçüncü taraf içerikleri nedeniyle sorumluluk yüklenmesini açık bir şekilde yasakladığını ileri sürmüştür.[413] Aynı doğrultuda şirket, müdahalenin demokratik bir toplumda gereklilik kriterini sağlamadığını, aksine bir sansüre yol açtığını, müdahale için baskın bir sosyal ihtiyaç bulunmadığını, zaten hukuka aykırılığı ortadan kaldırmak için yeterli önlemleri aldığını ileri sürmüştür.[414]

V. Estonya Hükûmetinin savunması

Estonya Hükûmeti, yerel mahkemelerin, hukuk kurallarını gereği gibi uyguladığını belirtmiştir.[415] Hükûmet, Delfi AS şirketinin anonim yorumları iptal etme veya benzeri şekilde iş modelinde değişikliğe gidilmesine yol açacak bir durumun ortaya çıkmadığını iddia etmiştir.[416] Delfi AS şirketinin sorumluluğuna ilişkin düzenlemelerin kanunlarda öngörüldüğü; düzenlemelerin, başkalarının şerefini koruma gibi meşru bir amaç güttüğü belirtilmiştir. Estonya Hükûmetinin savunmasında yer alan, Delfi AS'nin karar sonrasında beş moderatör istihdam ederek etkin bir moderasyon yapmaya başladığının vurgulandığı kısmın özel olarak not edilmesi gerekir.[417]

VI. Müdahil üçüncü tarafların görüşleri

Delfi AS davasına, Helsinki İnsan Hakları Vakfı, Article 19, Access, yirmi sekiz ortaklık kuruluşu ile birlikte hareket eden Medya Hukuki Savunma Girişimi (MLDI - Media Legal Defence Initiative), müşterek hareket eden Avrupa Dijital Medya Derneği (EDiMA), Bilgisayar ve

[412] *Delfi AS v. Estonya*, para. 68.
[413] *Delfi AS v. Estonya*, para. 69.
[414] *Delfi AS v. Estonya*, para. 72-80.
[415] *Delfi AS v. Estonya*, para. 81.
[416] *Delfi AS v. Estonya*, para. 83.
[417] *Delfi AS v. Estonya*, para. 91.

İletişim Endüstrisi Derneği (CCIA Avrupa) ve Avrupa İnternet Servis Sağlayıcıları Derneklerinden Pan-Avrupa Derneği (EuroISPA) müdahil olarak görüşlerini paylaşmıştır. Bu görüşlerden öne çıkanları şöyledir:

Helsinki İnsan Hakları Vakfı: Aracı hizmet sağlayıcılarının, geleneksel medya muamelesi görmemesi ve onlarla aynı sorumluluk rejimine tabi tutulmaması gerektiğini savunmuştur.[418]

Article 19: Web sitelerini kullanıcılar tarafından eklenen yorumlardan sorumlu tutmanın bu siteler üzerine katlanılamaz bir yük getireceğini ileri sürmüştür.[419]

Access: İnternet kullanıcılarına ifadelerini kimlikleri belli olacak şekilde iletme zorunluluğu getirilmesinin internet ekonomisine zarar vereceğini iddia etmiş ve internet ortamına en önemli çevrim içi katkıyı rumuz kullanan kişilerin sağladığını ortaya koyan araştırmaya atıfta bulunmuştur.[420]

Medya Hukuki Savunma Girişimi (MLDI): Erişim ile içerik arasındaki sınırların gittikçe artan oranda belirsizleştiğini ve gelişmiş arama hizmetlerinin, çevrim içi pazarların, web 2.0 uygulamalarının ve sosyal paylaşım sitelerinin "aracılar" arasında yer aldığını kaydetmiştir.[421]

EDiMA, CCIA Avrupa ve EuroISPA: Delfi AS gibi bir çevrim içi haber tartışma forumuna yönelik teknolojinin ve işletim süreçlerinin, sosyal medya paylaşım platformları ve bloglar/mikrobloglar gibi yer verme hizmetlerinden teknolojik açıdan ayırt edilemez nitelikte olduğunu iddia etmiştir.[422]

---

[418] *Delfi AS v. Estonya*, para. 94.
[419] *Delfi AS v. Estonya*, para. 96.
[420] *Delfi AS v. Estonya*, para. 99.
[421] *Delfi AS v. Estonya*, para. 102.
[422] *Delfi AS v. Estonya*, para. 108.

VII. AİHM'nin tespit ve değerlendirmeleri

AİHM, *Delfi AS* davasının farklı haklar arasında hassas bir denge kurulması üzerine olduğunun bilincindedir. AİHM, bir yandan ifade özgürlüğünün kullanılması bakımından internetin emsalsiz bir platform olduğunu kaydetmiş; diğer yandan da nefret söylemi ve şiddete teşvik eden söylemler dâhil olmak üzere, karalayıcı ve açıkça hukuka aykırı içeriklerin daha önce hiç olmadığı gibi birkaç saniye içerisinde dünya çapında yayılabildiğine ve bazen sürekli olarak internette kaldığına işaret etmiştir.[423] Mahkeme tarafından vurgulandığı üzere mevcut davanın temelinde çelişen bu iki hakikat yer almaktadır.[424]

AİHM, Estonya Yüksek Mahkemesinin tespitlerinin yerindeliğini inceleyerek davayı ele almaya başlamıştır. AİHM, Estonya Yüksek Mahkemesinin Delfi AS şirketinin faaliyetlerine yönelik tespitlerinin sorgulanmasına yönelik bir gerekliliğin bulunmadığını belirtmiştir.[425] Ayrıca, somut olaydaki içeriklerin nefrete ya da şiddete teşvik anlamına geldiğini de kabul etmiştir.[426]

AİHM, kararının internet platformları üzerindeki etkilerini dikkate alarak davanın, büyük, profesyonel olarak yönetilen, ticari temelde faaliyet gösteren, kendi haber yazılarını yayımlayan ve okuyucularını bu haberlere yorum yapmaya davet eden bir internet haber portalıyla ilgili olduğunu vurgulama gereği duymuştur.[427] Bu vurgunun ardından, davanın, üçüncü taraflarca oluşturulan yorumların yayımlandığı diğer internet forumlarına ilişkin olmadığının altı bir kez daha çizilmiştir. Örnek olarak da 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 sağlayanın herhangi bir içerik sunmadığı ve içerik sağlayıcısı-

---

[423] *Delfi AS v. Estonya*, para. 110.

[424] *Delfi AS v. Estonya*, para. 110.

[425] *Delfi AS v. Estonya*, para. 113.

[426] *Delfi AS v. Estonya*, para. 114; Aynı yönde bir tespit için bkz. *Delfi AS v. Estonya*, para. 117.

[427] *Delfi AS v. Estonya*, para. 115.

nın bir internet sitesini ya da bir bloğu hobi olarak işleten sıradan bir kişi olduğu bir sosyal medya platformu gösterilmiştir.[428]

A. Kanunilik

Mevcut uyuşmazlığın hukuka uygunluğunu incelemeye başlayan AİHM, bir müdahalenin hukuka uygunluğunun ilk şartının "yasayla öngörülme" olduğunu ve bu şartın, öngörülebilirlik koşulunu beraberinde getirdiğini belirtmiştir.[429] Bu konudaki yerleşik içtihatlarına atıf yapan AİHM, yerel mevzuatın gerektirdiği bütün olasılıkları öngöremeyen kesinlik derecesinin, büyük oranda söz konusu yasanın içeriğine, kapsadığı alana ve kapsama alınan kişilerin sayı ve statüsüne bağlı olduğunu hatırlatmıştır. Aynı doğrultuda AİHM, mesleklerini icra ederken son derece temkinli hareket etme alışkanlığına sahip olan kişilerden (medya çalışanlarından), bu türden faaliyetin yaratacağı riskleri değerlendirirken özel önem göstermelerinin beklenebileceğini kaydetmiştir.[430]

AİHM'ye göre taraflar arasındaki uyuşmazlığın esasını, Delfi AS şirketinin faaliyetlerinin nasıl sınıflandırılması gerektiği oluşturmaktadır. Delfi AS, üçüncü taraflarca yapılan yorumlar açısından kendisinin aracı olarak sınıflandırılması gerektiğini değerlendirirken, Estonya Hükûmeti başvurucu şirketin söz konusu yorumlar bakımından da medya yayıncısı olarak görülmesi gerektiğini ileri sürmüştür.[431] Estonya yerel mahkemelerinin hukuki nitelendirmelerini tekrar eden AİHM, ulusal hukukun yorumlanması ve uygulanmasının öncelikle ulusal makamların özellikle de mahkemelerin görevi olduğunu belirtmiştir. Ayrıca, AİHM'nin, davalı bir devletin yasama organının belirli bir alanın düzenlenmesi bakımından seçtiği yöntemlerin uygunluğuna ilişkin bir görüş belirtme görevi bulunmadığı da tekrar edilmiştir.[432]

---

[428] *Delfi AS v. Estonya*, para. 116.
[429] *Delfi AS v. Estonya*, para. 120.
[430] *Delfi AS v. Estonya*, para. 122.
[431] *Delfi AS v. Estonya*, para. 125.
[432] *Delfi AS v. Estonya*, para. 127.

Tüm bu tespitlerini somut olaya uygulayan AİHM; Estonya Anayasası, Borçlar Kanunu ve ilgili içtihatların, yorumlardan doğan sorumluluk bakımından hukuki öngörülebilirlik kriterini sağladığına hükmetmiştir.[433] Hatta bir adım öteye giden Mahkeme, Delfi AS haber sitesinin Estonya'daki en büyük haber sitesi olduğunu belirterek profesyonel bir yayıncı olan şirketin, mevzuatı ve içtihadı daha iyi bilmesi ve yasal danışmanlık alması gerektiğini kaydetmiştir.[434] AİHM bu nedenle, başvurucu şirketin, faaliyetleriyle ilgili riskleri değerlendirebilecek bir konumda olduğunu ve bu faaliyetlerin yol açabileceği sonuçları makul bir dereceye kadar öngörebileceğini ifade etmiş ve söz konusu müdahalenin AİHS'nin 10. maddesinin ikinci fıkrası anlamında "yasayla öngörülmüş olduğu" sonucuna varmıştır.[435]

B. Meşru amaç

AİHM, başvurucu şirketin ifade özgürlüğüne yönelik kısıtlamanın, başkalarının şöhret ve haklarının korunması meşru amacını taşıdığı hususuna itiraz edilmediği için müstakil bir meşru amaç değerlendirmesi yapmamıştır.[436]

C. Demokratik bir toplumda gereklilik

AİHM, Delfi AS şirketine yönelik müdahalenin demokratik bir toplumda gerekliliğini değerlendirdiği aşamada, bu konudaki yerleşik içtihatlarına atıf yapmıştır. Ayrıca, basının demokratik bir toplumda yerine getirdiği temel fonksiyona da değinmiştir.[437] Bu tespitlerin yanında, *Ahmet Yıldırım v. Türkiye* gibi kararlarına da atıf yaparak internetin toplumun gündemdeki olaylara erişimini sağladığını ve genel anlamda bilginin dağıtılmasını büyük ölçüde kolaylaştırdığını belirtmiştir.[438] Tüm

[433] *Delfi AS v. Estonya*, para. 128.
[434] *Delfi AS v. Estonya*, para. 129.
[435] *Delfi AS v. Estonya*, para. 129.
[436] *Delfi AS v. Estonya*, para. 130.
[437] *Delfi AS v. Estonya*, para. 132.
[438] *Delfi AS v. Estonya*, para. 133.

bu hakların yanında, özel yaşama saygı gösterilmesini isteme hakkının bir parçası olan şöhretin korunması hakkının, AİHS'nin 8. maddesi tarafından korunan bir hak olduğunu vurgulamıştır.[439] AİHM, bu bağlamda, AİHS'nin 10. maddesinde korunan ifade özgürlüğüyle 8. maddesinde korunan özel hayata saygı hakkı arasında denge kurulması gerektiğini belirtmiştir.

AİHM, somut olaydaki müdahalenin ölçülülüğünün değerlendirilebilmesi için yorumların bağlamı, karalayıcı yorumların önlenmesi ya da kaldırılması amacıyla Delfi AS şirketi tarafından uygulanan tedbirler, Delfi AS şirketinin yükümlülüğüne alternatif olarak yorumların gerçek yazarlarının yükümlülüğü ve yerel yargılamaların başvurucu şirket açısından sonuçları gibi faktörlerin ayrı ayrı değerlendirilmesi gerektiğine karar vermiş ve incelemesini bu yönde detaylandırmıştır.[440]

Yorumların bağlamını inceleyen AİHM, Delfi AS şirketinin, yorum yapmaları için kullanıcıları teşvik ettiğini, yorumlara ilişkin içerik kuralları yürürlüğe koyulmuşsa da bir yorumun, Delfi AS sitesinde yayımlanmasından sonra yorumu yapan tarafından kaldırılamadığını, ancak Delfi AS şirketinin müdahalesi neticesinde bu yorumların teknik olarak silinebildiğini, bu işleyiş kapsamında Delfi AS şirketinin, internet sitesinde yayımlanan yorumlara ilişkin esaslı bir kontrol gerçekleştirmiş olması gerektiğini belirtmiştir.[441] AİHM, Estonya Yüksek Mahkemesinin Delfi AS şirketinin haberlerin altında yer alan yorumlar bakımından pasif bir teknik hizmet sağlayıcı olmanın ötesine geçtiği yönündeki tespitine katıldığını belirtmiş ve müdahalenin AİHS'nin 10. maddesi çerçevesinde uygun temellere dayandırıldığına hükmetmiştir.[442]

Yorumları yazan kişilerin sorumluluğunun Delfi AS şirketinin sorumluluğuna etkisi nedir? Bu sorunun yanıtını arayan AİHM, internet ortamında anonimliğin fikir ve bilgilerin paylaşılmasında önemi oldu-

[439] *Delfi AS v. Estonya*, para. 134-137.
[440] *Delfi AS v. Estonya*, para. 142.
[441] *Delfi AS v. Estonya*, para. 144-145.
[442] *Delfi AS v. Estonya*, para. 146.

ğunu yadsımamaktadır.[443] Mahkeme, anonim içeriklerin klasik medyaya kıyasla internet ortamında hukuka aykırılıkları artırdığını da yok saymamaktadır. AİHM, bu noktada Avrupa Birliği Adalet Divanının, unutulma hakkı olarak da anılan *Google v. İspanya* kararına da atıf yapmış ve bireylerin temel haklarının arama motorlarının ekonomik menfaatleri ile başka internet kullanıcılarının menfaatlerinden daha önde olduğuna yönelik Adalet Divanı tespitini hatırlatmıştır.[444]

AİHM, internet ortamında farklı tür ve seviyelerde anonimliğin var olduğunu, bazı durumlarda kısıtlı bir onaylama (e-posta onayı gibi) bazı durumlarda ise tam bir kimlik doğrulaması yapıldığını, soruşturma ve yargı makamlarının içerik sahiplerinin tespiti için bazı özel kısıtlamalarla karşı karşıya kalabildiğini belirtmiştir.[445] Konunun teknik boyutuna da atıf yapan AİHM, IP adreslerinin çoğu zaman karışık sonuçlar doğurduğunu, bazı durumlarda yorumun yazıldığı bilgisayarın tespitine imkân verdiğini, bazı durumlarda ise teknik sebeplerle bir neticeye ulaşmaya elverişli olmadığını belirtmiştir.[446]AİHM, Estonya Yüksek Mahkemesi kararına göre, zarar gören kişinin başvurucu şirket ya da yorumların yazarları aleyhine dava açma olanağına sahip olduğunu belirtmiştir. AİHM, yorumların yazarlarının kimliğinin tespitine imkân sağlayan tedbirlerin belirsiz etkililiği ve nefret söylemi mağdurunun, yorumların yazarları hakkında etkili bir şekilde dava açmasını mümkün kılacak enstrümanların Delfi AS şirketi tarafından devreye konulmamış olması hususlarını dikkate alarak Estonya Yüksek Mahkemesinin kararını yerinde görmüştür.[447] AİHM, varmış olduğu bu hükmü, basınla ilgili daha önce vermiş olduğu bir kararı da gerekçe göstererek desteklemiştir. *Krone Verlag*[448] kararında AİHM, hakarete maruz kalan kişinin hakaret davasında tazminat elde

---

[443] *Delfi AS v. Estonya*, para. 147.

[444] *Delfi AS v. Estonya*, para. 147.

[445] *Delfi AS v. Estonya*, para. 148; Servis sağlayıcıların bu bağlamda sorumluluğuna ilişkin daha önce hüküm altına alınmış 2008 tarihli *K.U. v. Finlandiya*, Başvuru No:2872/02, 2.12.2008 içtihadına atıf yapılmıştır. Bkz. *Delfi AS v. Estonya*, para. 149.

[446] *Delfi AS v. Estonya*, para. 150.

[447] *Delfi AS v. Estonya*, para. 151.

[448] **AİHM**, *Krone Verlags GmbH & Co. KG v. Avusturya (No. 4)*, Başvuru No: 72331/01, 9.11.2006.

etmesine yönelik riskin, genelde hakaret eden kişiden daha iyi ekonomik koşullara sahip olan medya şirketine kaydırılmasının, söz konusu medya kuruluşunun ifade özgürlüğüne orantısız bir müdahale teşkil etmediği sonucuna varmıştır.[449]

AİHM'nin, demokratik bir toplumda gereklilik unsurunu değerlendirdiği son nokta ise Delfi AS tarafından alınan önlemlerdir. AİHM, Estonya mahkemeleriyle benzer bir yaklaşımla, Delfi AS şirketinin, hukuka aykırı nitelikteki yorumları kendi inisiyatifiyle fark edip kaldırmış ve bu minvalde esaslı bir kontrol sağlamış olması gerektiğinden hareket etmiştir.[450] AİHM; nefret söylemi içeren, şiddete çağıran, hukuka aykırılığı aşikâr olan içeriklerin kaldırılması noktasında platform yöneticisine yükümlülük getirilmesini ifade özgürlüğüne yönelik ölçüsüz bir müdahale olarak nitelendirmemiştir.

AİHM, Delfi AS'nin hukuka aykırı yorumları önlemek için belirli ölçüde teknik tedbirler aldığını not etmektedir.[451] Otomatik filtrelemenin belirli ölçüde bir koruma getirdiğini, editörlerin kendi inisiyatifleriyle bazı yorumları bir uyar-kaldır süreci işletilmesine gerek olmaksızın kaldırdığını kabul etmektedir. Ancak, spesifik kelimeler içermeyen, karmaşık metaforlar, gizli anlamlar veya nükteler barındıran içeriklere karşı bu mekanizmanın etkisiz kaldığını belirtmiştir.[452]

Platformun daha aktif bir şekilde içerik kaldırması "özel bir sansüre" yol açar mı? AİHM, bu durumun özel bir sansüre yol açmayacağı kanaatindedir.[453] Mahkeme, internetin "halkın habere erişiminin artırılması ve genel olarak bilginin yayılmasının kolaylaştırılması" konusundaki "önemli rolünü" kabul etmekle birlikte internetteki içerik ve iletişimin ortaya çıkardığı zarar riskini de önemsediğini belirtmiştir.[454]

---

[449] *Delfi AS v. Estonya*, para. 151.
[450] *Delfi AS v. Estonya*, para. 153.
[451] *Delfi AS v. Estonya*, para. 155.
[452] *Delfi AS v. Estonya*, para. 155.
[453] *Delfi AS v. Estonya*, para. 157.
[454] *Delfi AS v. Estonya*, para. 157.

AİHM'nin bu yaklaşımının arkasında hassas bir denge yatmaktadır. Saptanabilir bireysel bir mağdurun olmadığı, genel bir gruba yönelen nefret söylemi veya şiddete teşvik eden söylemler gibi içerikleri de dikkate alan AİHM, potansiyel bir nefret söylemi mağdurunun interneti sürekli olarak kontrol edebilme imkânının, büyük bir ticari internet haber sitesinin bu tür yorumları engelleme ya da hızla kaldırabilme imkânından daha sınırlı olduğu değerlendirmesini önemsediğini belirtmiştir.[455]

AİHM, uyar-kaldır mekanizmasının etkinliğini de değerlendirmiştir. Delfi AS, uyar-kaldır mekanizmasının, hakları dengeleyen bir çözüm olduğunu iddia etmiştir. AİHM'ye göre, bu yöntem birçok vakada etkin bir yol olarak nitelendirilebilirse de mevcut davada olduğu gibi nefret söylemi ve kişilerin vücut bütünlüğüne yönelik şiddet söylemleri söz konusu olduğunda etkin değildir. Hatta Mahkeme bir adım ileriye giderek, internet haber sitelerinin, açıkça hukuka aykırı olan yorumları mağdur olduğu iddia edilen kişi ya da üçüncü tarafların bildirimine gerek olmaksızın derhâl kaldırmaya yönelik tedbirler almaması durumunda, başkalarının ve bir bütün olarak toplumun hak ve menfaatlerinin, AİHS'ye taraf devletlere AİHS'nin 10. maddesi çerçevesinde internet haber sitelerine sorumluluk getirme hakkını verebileceğini değerlendirmiştir.[456]

AİHM, Delfi AS aleyhine hükmedilen tazminatın ölçülü bir yaptırım niteliğinde olduğunu; Delfi AS kararından sonra Estonya mahkemelerinin bu konuda yeknesak bir uygulama geliştirdiğini not etmiştir.[457] AİHM, kararın Delfi AS'nin iş modelini değiştirmesine yol açmadığını, sitenin hâlâ Estonya'nın en büyük internet haber sitesi olduğunu, sadece şirketin hukuka aykırı içerikle mücadele için daha aktif bir moderatör ekibi kurduğunu belirtmiştir.[458]

Sonuç olarak, yukarıda belirtilen hususlara ilişkin somut değerlendirme temel alınarak, Estonya Yüksek Mahkemesinin mevcut davadaki gerekçesi, özellikle söz konusu yorumların aşırı niteliği, yorumların baş-

[455] *Delfi AS v. Estonya*, para. 158.
[456] *Delfi AS v. Estonya*, para. 159.
[457] *Delfi AS v. Estonya*, para. 160.
[458] *Delfi AS v. Estonya*, para. 161.

vurucu şirket olan Delfi AS tarafından ticari temelde işletilen ve profesyonel olarak yönetilen haber sitesinde yayımlanan bir habere tepki olarak yayımlandığı, nefret söylemi teşkil eden ve şiddete teşvik eden söylemler barındıran yorumların derhâl kaldırılması ve söz konusu yorumların yazarlarının sorumlu tutulmaları bakımından gerçekçi bir imkân sağlanmasına yönelik olarak Delfi AS şirketi tarafından alınan tedbirlerin yetersizliği ile Delfi AS şirketi aleyhine uygulanan ölçülü yaptırım dikkate alındığında, AİHM davalı Estonya Devleti'ne sağlanan takdir payını göz önünde bulundurarak ulusal mahkemeler tarafından başvurucu şirkete sorumluluk yüklenmesinin ilgili ve yeterli gerekçelere dayandırıldığı sonucuna varmıştır. Bu nedenle, ilgili tedbirin, başvurucu şirketin ifade özgürlüğüne orantısız bir sınırlama teşkil etmediğine ve dolayısıyla AİHS'nin 10. maddesinin ihlal edilmediğine hükmedilmiştir.

VIII. Yargıçlar Raimondi, Karakaş, De Gaetano ve Kjølbro'nun müşterek mutabık görüşü

AİHM Yargıçları Raimondi, Karakaş, De Gaetano ve Kjølbro karara farklı gerekçelerle katılmışlardır. Yargıçlar, özellikle *Delfi AS* kararındaki bazı müphem hususların netleştirilmesi gerektiğini ileri sürmüşlerdir. Yargıçlara göre Delfi AS'nin Estonya Yüksek Mahkemesi tarafından sorumlu tutulması iki şekilde yorumlanabilir: (1) Hukuka aykırı yorumların yayımlanmasını "engellemediğinden" Delfi AS şirketi sorumludur ve bu sorumluluk, yorumları daha sonra "kaldırmaması" nedeniyle artmıştır veya (2) Delfi AS şirketi hukuka aykırı yorumların yayımlanmasını "engellememiştir" ve yorumları daha sonra "kaldırmaması" nedeniyle söz konusu yorumlardan sorumludur.[459]

Yargıçlar Raimondi, Karakaş, De Gaetano ve Kjølbro, AİHM'nin konuyu ikinci yoruma göre değerlendirdiği kanaatindedirler. Yargıçlar, birinci yorumun esas alınması durumunda mevcut davanın neticesinin farklı olacağı görüşündedirler.[460] Yargıçlara göre, ilk yorumun esas alın-

[459] *Delfi AS v. Estonya*, Yargıçlar Raimondi, Karakaş, De Gaetano ve Kjølbro'nun Müşterek Mutabık Görüşü, para. 4.

[460] *Delfi AS v. Estonya*, Yargıçlar Raimondi, Karakaş, De Gaetano ve Kjølbro'nun Müşterek

ması, ulusal mevzuatın Delfi AS gibi bir haber portalına aşırı yük getirme riskine yol açacak şekilde yorumlanmasına sebep olabilecektir. Diğer bir ifadeyle, bir haber sitesi, okuyucular tarafından yazılan ve bariz şekilde hukuka aykırı olan yorumların yayımlanmasını engellemek amacıyla yorumları ön denetlemeye tabi tutmak ve bunun için gerekli tedbirleri almak zorunda kalabilecektir.[461]

Yargıçlara göre, haber sitesini kullanıcılar tarafından yazılan yorumların yayımlanmasını "engellemediği" için sorumlu tutmak, sitenin hukuka aykırı yorumlardan doğacak sorumluluktan kaçınmak için bütün kullanıcı yorumlarını tek tek ön denetlemeye tabi tutması anlamına gelecektir. Bu durum, uygulamada, haber sitesinin AİHS'nin 10. maddesi ile güvence altına alınan ifade özgürlüğüne orantısız bir müdahaleye yol açabilecektir.[462]

Yargıçlara göre, AİHM mevcut dava gibi bir davanın değerlendirilmesine ilişkin ilkeleri daha açık bir şekilde belirtme imkânını kullanmalıydı. Yargıçlara göre, haber sitesinin, açık bir şekilde hukuka aykırı olan yorumların sitede yayımlanmış olabileceğini veya yayımlandığını bilip bilmediği ya da bilmesi gerekip gerekmediği konusunda yapılacak bir değerlendirmede; söz konusu yorumların niteliği, yayımlanma koşulları, üzerine yorum yazılan makalenin konusu, ilgili haber sitesinin niteliği, sitenin geçmişi, makaleye yapılan yorum sayısı, sitenin aktifliği ve yorumların ne kadar süre sitede kaldığı hususları da dâhil olmak üzere, davanın kendine özgü bütün koşulları dikkate alınmalıdır.[463]

Yargıçlar, mevzubahis yorumların açıkça hukuka aykırı niteliği ve bu yorumların silinmeden önce altı hafta boyunca haber sitesinde kaldığı dikkate alındığında Estonya Yüksek Mahkemesinin, "hukuka aykırı içeriğinin farkında olunması gereken yorumları kendi inisiyatifiyle siteden

Mutabık Görüşü, para. 5.

[461] *Delfi AS v. Estonya*, Yargıçlar Raimondi, Karakaş, De Gaetano ve Kjølbro'nun Müşterek Mutabık Görüşü, para. 6.

[462] *Delfi AS v. Estonya*, Yargıçlar Raimondi, Karakaş, De Gaetano ve Kjølbro'nun Müşterek Mutabık Görüşü, para. 7.

[463] *Delfi AS v. Estonya*, Yargıçlar Raimondi, Karakaş, De Gaetano ve Kjølbro'nun Müşterek Mutabık Görüşü, para. 12.

kaldırmadığı" gerekçesiyle Delfi AS'yi sorumlu tutmasını orantısız bulmadıklarını; aslında bu kadar uzun bir süre boyunca bu tür açıkça hukuka aykırı yorumların farkında olmamanın, neredeyse hukuki sorumluluktan kaçınmak için esas teşkil edemeyecek olan kasıtlı ihmal anlamına geldiğini belirtmişlerdir.[464]

IX. Yargıç Boštjan Zupančič'in mutabık görüşü

AİHM Yargıcı Boštjan Zupančič de müstakil bir mutabık görüş yazmıştır. Davanın neticesine katılan Yargıç Zupančič, tarihî ve etik bazı ilaveler paylaşmıştır. Yargıç Zupančič'e göre kişilik haklarının ihlali konusuna ilişkin temel sorun *common law* ve Kıta Avrupası arasındaki yaklaşımdan kaynaklanmaktadır.[465] Bu iki hukuk sisteminin kişilik haklarının korunmasına yönelik kurallarını karşılaştıran Yargıç Zupančič, internet ortamındaki anonim içeriklere yönelik görüşünü açıklamıştır.

Yargıç Zupančič, bir internet sitesinin ya da başka bir kitle iletişim aracının herhangi bir anonim yorumu yayımlamasına izin verilmesini tamamen kabul edilemez görmektedir.[466] Anonim yorumlara ilişkin bu katı değerlendirmesini, çok uzak olmayan bir geçmişte "editöre gönderilen mektupların" yayımlanabilir olarak görülmeden önce yazarın kimliği bakımından iki kere kontrol edildiğine yönelik örnekle izah etmeye çalışmıştır. AİHM'nin *Print Zeitungsverlag GmbH v. Avusturya*[467] kararına da atıf yapan Yargıç Zupančič, basılı bir anonim mektubun yayımlanması nedeniyle haklı olarak tazminata hükmedilmesinin önceki içtihatlarla uyumlu bir yaklaşım olduğunu belirtmiştir.

Yargıç Zupančič'e göre kitlesel medya, "basının yararlandığı geniş özgürlük, buna uygun sorumluluk düzeyini gerektirir" ilkesine göre işletilmekteydi. Ticari çıkarlar için son derece saldırgan karalama şekillerinin yayımlanmasını teknik olarak mümkün kılmak ve bir internet servis

---

[464] *Delfi AS v. Estonya*, Yargıçlar Raimondi, Karakaş, De Gaetano ve Kjølbro'nun Müşterek Mutabık Görüşü, para. 15.

[465] *Delfi AS v. Estonya*, Yargıç Zupančič'in Mutabık Görüşü.

[466] *Delfi AS v. Estonya*, Yargıç Zupančič'in Mutabık Görüşü.

[467] **AİHM**, *Print Zeitungsverlag GmbH / Avusturya*, Başvuru No: 26547/07, 10.10.2013.

sağlayıcısının başkalarının kişilik haklarına yönelik bu saldırılardan hiçbir sorumluluğu bulunmadığını ileri sürmek tamamen kabul edilemezdir.

Yargıç Zupančič, *Print Zeitungsverlag GmbH v. Avusturya* kararı ile kıyaslama yaparak 300 avroluk tazminat tutarını da düşük görmüş ve ifade özgürlüğünün, diğer özgürlükler gibi, başkalarının özgürlükleri ve kişisel bütünlüğü negatif olarak etkilendiğinde açıkça sona ermesi gerektiği vurgusuyla mutabık görüşünü tamamlamıştır.

X. Yargıçlar Sajó ve Tsotsoria'nın müşterek muhalif görüşü

AİHM Yargıçları Sajó ve Tsotsoria müşterek muhalif görüş sunmuşlardır. Bu karşı görüşlerini; tamamlayıcı sansür, genel bağlam, neticeler, Delfi AS'nin aracı hizmet sağlayıcı olarak rolü, yorumların niteliği, müdahale ve aktif aracı hizmet sağlayıcıların hakları, müdahalelerin öngörülebilirliği (öngörülebilirlik problemi), demokratik bir toplumda gereklilik, "gerekli ve yeterli gerekliliklerin" analizine yönelim, yayıncıların sorumluluğunun genişletilmesi (temel ekonomik menfaat), sorumluluk seviyesi, dengeleme (olmaması) alt başlıklarında kapsamlı bir şekilde ortaya koymuşlardır.

AİHM Yargıçları Sajó ve Tsotsoria'ya göre, Delfi AS kararının muhtemel sonucu olarak her türlü karalama fiilinin ve belki "yasa dışı" faaliyetin önlenmesi adına, tüm yorumlar yazılır yazılmaz denetlemeye tabi tutulmak zorunda kalacaktır.[468] Yargıçlar, bu durumun aktif aracılar ve blog operatörlerine, yorum özelliğine son vermek bakımından birçok neden sunacağını ve sorumluluk korkusunun operatörler tarafından ek otosansür uygulanmasına yol açabileceğini, bu durumun da en kötü ihtimalle otosansüre davetiye çıkarmak olduğunu ileri sürmüşlerdir. AİHM Yargıçları Sajó ve Tsotsoria, AİHM'nin, kararının kamu politikaları alanındaki etkilerini gereğince değerlendirmediğini, tehlikelere vurgu

[468] *Delfi AS v. Estonya*, Yargıçlar Sajó ve Tsotsoria'nın Müşterek Muhalif Görüşü, para. 1.

yapılırken internetin demokrasinin gelişimine olan katkılarına yeterince değinilmediğini belirtmişlerdir.[469]

Yargıçların eleştirdiği bir diğer husus ise AİHM'nin mukayeseli hukuktaki örnekleri çok kısıtlı incelemiş olması, Avrupa Konseyi üye devletleriyle dünyadaki demokratik devletlerin düzenlemelerini yeterince incelememesidir. Yargıçlar, ortak yaklaşımın gerçekten de bilgiye vâkıf olma üzerine kurulduğunu ve esas olanın uyar-kaldır yöntemi olduğunu belirtmişlerdir.[470] Yargıçlar, aracı platformlara ilişkin güvenli liman ilkesinin manasız hâle geldiğini belirtmişlerdir. Yargıçlar, herhangi bir sorumluluk altına girmemek ve sorun yaşamamak adına platformların yorumlar için varsayılan yaklaşımının "otomatik silme" olacağını ileri sürmüşlerdir.[471]

AİHM kararının incelendiği ilk bölümde belirtildiği üzere AİHM, kararının, sosyal medya platformlarına veya internet sitesini kişisel amaçlarla kuran veya hobi amacıyla kullanan kişilere uygulanmayacağını belirtmiştir. Yargıçlar haklı olarak, "hasar kontrolünün" nasıl katkı sağlayacağını anlamanın oldukça zor olduğunu belirtmiş ve "*İfade özgürlüğü bir hobi konusu olamaz.*" demek suretiyle AİHM'yi açıkça eleştirmişlerdir.[472]

Yargıçlar, Estonya Yüksek Mahkemesinin, Delfi AS'nin haklarına yönelen oldukça yoğun müdahaleyle ilgili yeterli gerekçeler sunamadığı ve bu durumun, AİHS'nin ihlali anlamına geldiğini ileri sürmüşlerdir.[473] Yargıçlar, her şeyden evvel AİHM'nin, kullanıcı yorumlarını ayrı ayrı ele almadığını ve bunların hukuka aykırılıklarını müstakil olarak tartışmadığını, bunun da önemli bir eksiklik olduğunu belirtmişlerdir.[474]

Yargıçlara göre, Delfi AS'nin basın hürriyeti ihlal edilmiştir. Nihayetinde, kullanıcı yorumları haberleri zenginleştirmektedir. Aktif bir aracı

---

[469] *Delfi AS v. Estonya*, Yargıçlar Sajó ve Tsotsoria'nın Müşterek Muhalif Görüşü, para. 6.

[470] *Delfi AS v. Estonya*, Yargıçlar Sajó ve Tsotsoria'nın Müşterek Muhalif Görüşü, para. 7.

[471] *Delfi AS v. Estonya*, Yargıçlar Sajó ve Tsotsoria'nın Müşterek Muhalif Görüşü, para. 8.

[472] *Delfi AS v. Estonya*, Yargıçlar Sajó ve Tsotsoria'nın Müşterek Muhalif Görüşü, para. 9.

[473] *Delfi AS v. Estonya*, Yargıçlar Sajó ve Tsotsoria'nın Müşterek Muhalif Görüşü, para. 10.

[474] *Delfi AS v. Estonya*, Yargıçlar Sajó ve Tsotsoria'nın Müşterek Muhalif Görüşü, para. 12-14.

platformun bir hakkı da başkalarına haber alma ve verme olanağı sağlama hakkıdır.[475]

Yargıçlar, AİHM'nin öngörülebilirlik sorununa ilişkin yorumunu da eleştirmişlerdir. Delfi AS şirketinin davadaki asıl ihtilaf konusu olan kullanıcı yorumlarından sorumlu tutulabilmesi için Estonya Borçlar Kanunu mu, Bilgi Toplumu Hizmetleri Kanunu mu uygulanmalıdır? Bilindiği üzere Bilgi Toplumu Hizmetleri Kanunu, servis sağlayıcılarını sorumluluktan muaf tutmaktadır; servis sağlayıcı hukuka aykırı içeriğin farkına varınca söz konusu içeriği hemen kaldırırsa Kanun "güvenli bir liman" sağlamakta ve servis sağlayıcı sorumlu tutulamamaktadır. AİHM Yargıçları Sajó ve Tsotsoria'ya göre, Avrupa Birliği hukukunun veya özel düzenlemenin neden uygulanmadığına ilişkin kapsamlı bir inceleme yapılmaması eksikliktir.[476] Yargıçlara göre, veri depolamanın ticari niteliğinin, söz konusu faaliyeti yayıncılara uygulanabilen sorumluluk sistemi alanına soktuğunu ileri sürmek ikna edici değildir. Depolama ticari bir faaliyet olarak görülmektedir ancak bu durum, "güvenli bir liman" sistemine olanak sağlayan Bilgi Toplumu Hizmetleri Kanunu açısından eşitliği değiştirmemektedir.[477]

Birbiriyle çelişkili içtihatlara da atıf yapan Yargıçlar, hukuki sorumluluğun tespitinin zorluğuna ve kullanıcı yorumları sebebiyle platforma uygulanacak kuralların belirsizliğine dikkat çekmişlerdir. İronik bir üslupla, sadece kâhin bir hukuk danışmanının (*divine legal counsel*), bütün yayınlama sürecine ilişkin tam bilgi sahibi olarak faaliyet gösteren yayıncılara (editörler) uygulanan bir tür mutlak sorumluluk altında bir site operatörünün, farkında olmadığı bir yorum bakımından sorumlu tutulacağından emin olabileceğini belirtmişlerdir.[478]

AİHM'nin, platformların sorumluluğuna ilişkin farklılaştırılmış bir yaklaşım getirilebileceğine ilişkin tespitine değinen Yargıçlar, ticari amacı

[475] *Delfi AS v. Estonya*, Yargıçlar Sajó ve Tsotsoria'nın Müşterek Muhalif Görüşü, para. 16.
[476] *Delfi AS v. Estonya*, Yargıçlar Sajó ve Tsotsoria'nın Müşterek Muhalif Görüşü, para. 17.
[477] *Delfi AS v. Estonya*, Yargıçlar Sajó ve Tsotsoria'nın Müşterek Muhalif Görüşü, para. 17.
[478] *Delfi AS v. Estonya*, Yargıçlar Sajó ve Tsotsoria'nın Müşterek Muhalif Görüşü, para. 20.

doğrudan bir sorumluluk doğuran unsur olarak nitelendiren AİHM kararına karşı şu haklı tespiti yapmışlardır:

"Son üç yüz yıl boyunca, para konusunda fikirler üretilmiş ve bu hiçbir zaman ifadeye sağlanan koruma düzeyinin düşürülmesine bağlı olmamıştır. Fikirlerin mali getirisini önemsememeye gücü yetebilecek Roma otoritesinin (her ne kadar genellikle imparatorluğunun memnuniyetine bağlı olsa da) aristokratik dünyasında yaşamıyoruz. Bir gazete ya da yayıncının herhangi bir satış kanalını ticari bir girişim olarak işletmesi onun aleyhinde kullanılamaz. Fikir üretiminin ücretsiz olması beklenemez. Yeterli mali imkânlar olmadan hiçbir fikir üretilemez; maddi karşılık ve basın kuruluşunun ticari niteliği, basına sağlanan koruma düzeyinin azaltılmasına yönelik gerekçeler değildir (ve olamaz). Bilgi değerlidir; bilginin etkili bir şekilde nakledilmesi sadece bir hobi değildir. Ticari görülen ve bu nedenle yüksek sorumluluğa tabi tutulan aynı platform ayrıca kamu menfaati konusunda geliştirilmiş ve interaktif görüşme sağlayan bir platformdur. Dengeleme uygulamasında bu husus dikkate alınmamıştır."[479]

Bu tespitten sonra Yargıçlar, klasik bir yayıncı (gazete editörü gibi içeriği kontrol eden) ve aktif platform arasındaki farkı şu şekilde ortaya koymuştur: (a) Bir gazetede, gazeteci tipik bir çalışandır (her ne kadar bir gazeteciyi editörüne/işverenine karşı korumak için iyi nedenler olsa bile); ve (b) editör, ilke olarak, yayımlanacak bir haberin içeriğini önceden bilebilecek konumdadır ve yayının kontrol edilmesi kapsamında önceden karar verme yetkisine ve imkânına sahiptir.[480] Yargıçlara göre, aktif platform, ancak filtreleme mekanizması ile mümkün kılındığında ön denetleme olanağı bulmaktadır.[481] Ayrıca, aktif aracı, bir iletiyi silme ya da iletiye erişimi engelleme yetkisine de sahiptir. Ancak, olağan durumlarda aktif aracı, iletiyi yayımlayan kişi üzerinde kişisel kontrole sahip değildir. Yorumcu, yayıncının çalışanı değildir ve çoğunlukla yayıncı tarafından tanınmamaktadır. Yayın, editörün kararı olmadan gerçekleşir. Bu nedenle, bilginin ve kontrolün düzeyi önemli ölçüde değişiklik göstermektedir.

---

[479] *Delfi AS v. Estonya*, Yargıçlar Sajó ve Tsotsoria'nın Müşterek Muhalif Görüşü, para. 29.

[480] *Delfi AS v. Estonya*, Yargıçlar Sajó ve Tsotsoria'nın Müşterek Muhalif Görüşü, para. 31.

[481] *Delfi AS v. Estonya*, Yargıçlar Sajó ve Tsotsoria'nın Müşterek Muhalif Görüşü, para. 31.

Bu bağlamda, kontrol, bilgiyi gerektirmektedir ve editör/yayıncı ile aktif aracı arasındaki fark barizdir.[482]

Sorumluluk konusuna da değinen Yargıçlar, bir yayıncı olarak tanımlanamasa da Delfi AS'nin insanların yorum yapması için gönüllü olarak imkân sağladığını ve bu faaliyetin, basın nitelikli ifade özgürlüğü konusu olsa bile sorumluluktan muaf tutulmadığını belirtmiştir. Yargıçlar, Bilgi Toplumu Hizmetleri Kanunu'nun, diğer hususların yanı sıra mevcut davada olduğu gibi depolama açısından da bu yönde bir sorumluluk öngördüğünü; Kanun'un, sorumluluğu "fiilî bilgiye" dayandırdığını ve hızlı kaldırma görevi getirdiğini vurgulamışlardır.[483] AİHM'nin ise bu hususu yetersiz bulduğunu tekrarlamışlardır.

Yargıçların altını defalarca çizdiği husus; saldırgan yorumları, bu tür yorumların bulunduğuna dair fiilî bilgi olmadan ve yayımlandıktan hemen sonra kaldırma görevinin, aktif platformun 7/24 denetleme sağlaması gerektiği anlamına geldiğidir.[484] Yargıçlara göre, hangi açıdan bakılırsa bakılsın, bu, kesin ve mutlak sorumluluk olup geniş kapsamlı ön sınırlamadan hiçbir şekilde farklı değildir ve ilgili menfaatlerin korunmasını neden sadece bu düzeyde bir sorumluluğun sağlayabileceği konusunda herhangi bir gerekçe gösterilmemiştir.[485]

AİHM Yargıçları Sajó ve Tsotsoria, AİHM'nin, filtreleme mekanizmasının çalışmadığına yönelik tespitle yetinip kapsamlı bir değerlendirme yapmamasını da eleştirmiştir.[486] Aynı doğrultuda, özel bir moderatör ekibi kurmanın "özel medya kuruluşlarına uygulanan bir sansür" olarak değerlendirilmemesini ve daha az müdahale içeren tedbirlerin uygulanabileceğine yönelik herhangi bir değerlendirme yapılmamasını ağır şekilde eleştirmişlerdir.[487] Yargıçlara göre, atıfta bulunulan tüm uluslararası belgelere uygun olarak, yorumlar için alan sağlayan aktif bir aracının

---

[482] *Delfi AS v. Estonya*, Yargıçlar Sajó ve Tsotsoria'nın Müşterek Muhalif Görüşü, para. 32.
[483] *Delfi AS v. Estonya*, Yargıçlar Sajó ve Tsotsoria'nın Müşterek Muhalif Görüşü, para. 33.
[484] *Delfi AS v. Estonya*, Yargıçlar Sajó ve Tsotsoria'nın Müşterek Muhalif Görüşü, para. 35.
[485] *Delfi AS v. Estonya*, Yargıçlar Sajó ve Tsotsoria'nın Müşterek Muhalif Görüşü, para. 35.
[486] *Delfi AS v. Estonya*, Yargıçlar Sajó ve Tsotsoria'nın Müşterek Muhalif Görüşü, para. 36.
[487] *Delfi AS v. Estonya*, Yargıçlar Sajó ve Tsotsoria'nın Müşterek Muhalif Görüşü, para. 37.

mutlak sorumluluğu olamaz ve e ifade özgürlüğünün korunması görevi yüklenemez.[488] Yargıçlar, dengeleyici bir yaklaşım uygulandığında bu dengeleme testinin diğer unsurlarının da (basın ve gazeteciliğe müdahaleye yönelik tartışmalar başta olmak üzere) dikkate alınması gerektiğini vurgulamışlardır.[489]

Yargıçlar, nefret söylemi sorununa gözlerini kapama gibi bir niyetleri olmadığını belirtmişlerdir.[490] Yargıçlara göre, yorum kısmının ırkçılığın yayılmasına teknik olarak imkân tanıdığı hususu orantılılık incelemesinin bir parçası olmalıdır. Bu noktada Yargıçlar aslında, yorum kısmının tüm görüşlerin eşit olarak yayılmasına imkân tanımakta olduğu tespitini de yapmıştır. Buna karşılık, spesifik bir kanıt olmasa da daha çok yorum yapılmasının ırkçı yorumların yapılma olasılığını artıracağını kabul eden Yargıçlar, yargılamalarda bu yönde bir delil bulunmadığından veya AİHM tarafından bu yönde bir atıf yapılmadığından bu durumu bir hipotez olarak kabul ettiklerini belirtmişlerdir.[491]

Yargıçlara göre AİHM'nin görevi, ulusal yetkililerce gerçekleştirilen müdahalenin gerçekten uygun ve güvenilir temellere dayandırılıp dayandırılmadığını belirlemektedir.[492] Bu hususun mevcut davada eksik olduğunu belirten AİHM Yargıçları Sajó ve Tsotsoria, bu nedenle AİHS'nin ihlal edildiğini ileri sürmüşlerdir.

XI. Değerlendirme

AİHM'nin *Delfi AS v. Estonya* kararı birçok açıdan sorunlu ve de çelişkili bir karardır. AİHM, derinlemesine bir incelemeye girişmeksizin, varsayımlardan yola çıkarak, mevcut müdahaleye ilişkin gereğince bir ölçülülük testi yapmaksızın ve bir internet haber sitesinin gün içerisinde teknik olarak nasıl işlediğini, ne ölçekte bir bilgiyi yönetmesi gerektiğini değerlendirmeksizin bir hükme varmıştır. Tekrara düşmemek adına

[488] *Delfi AS v. Estonya*, Yargıçlar Sajó ve Tsotsoria'nın Müşterek Muhalif Görüşü, para. 38.
[489] *Delfi AS v. Estonya*, Yargıçlar Sajó ve Tsotsoria'nın Müşterek Muhalif Görüşü, para. 39.
[490] *Delfi AS v. Estonya*, Yargıçlar Sajó ve Tsotsoria'nın Müşterek Muhalif Görüşü, para. 42.
[491] *Delfi AS v. Estonya*, Yargıçlar Sajó ve Tsotsoria'nın Müşterek Muhalif Görüşü, para. 42.
[492] *Delfi AS v. Estonya*, Yargıçlar Sajó ve Tsotsoria'nın Müşterek Muhalif Görüşü, para. 43.

AİHM Yargıçları Sajó ve Tsotsoria'nın muhalefet şerhlerinde işaret etmiş oldukları tüm hususlar yerindedir ve AİHM'nin kararının tutarsızlığını göstermek için kâfidir.

AİHM'nin *Delfi AS v. Estonya* kararının tek neticesi otosansürdür. Dördüncü bölümde sosyal engelleme teknikleri kısmında incelendiği üzere, platformların sorumluluğuna ilişkin ölçüsüz her kuralın ve düzenlemenin tüm ekosistem üzerinde öngörülemez etkileri vardır.[493] AİHM, meseleye düz bir mantıkla yaklaşmaktadır. Mahkemeye göre, kayıtlı olmayan kullanıcılar tarafından yorum eklenmesine müsaade edilmesi Delfi AS şirketinin tercihiydi. Buna müsaade ettiğine göre şirketin bu türden yorumlar için belli bir sorumluluğu üzerine almış olduğu düşünülmelidir.

Mahkeme, mesleklerini icra ederken son derece temkinli hareket etme alışkanlığına sahip olan kişilerden, bu türden faaliyetin yaratacağı riskleri değerlendirirken özel önem göstermelerinin beklenebileceğini kaydetmiştir. Kısacası, AİHM, interneti klasik bilgiye erişim ve iletişim mecralarıyla eş değer tutmuş ve internetin kendine has özelliklerini, demokrasiye ve fikir özgürlüğüne katkılarını belirttiği kendi içtihatlarını (*Ahmet Yıldırım*, *Cengiz ve Diğerleri* gibi) dahi yok saymıştır.

Delfi AS şirketi, belirli kelimelerin yorumlarda yer almasını engelleyen bir filtreleme sistemi kurmuştur. Hangi tür içeriklerin yorumlarda paylaşılabileceğine ilişkin kapsamlı bir içerik politikası hazırlamış ve bunu ilgili sayfalarda duyurmuştur. Herhangi bir yoruma ilişkin bir şikâyet geldiği zaman da bu içeriği internet ortamından anında kaldırmıştır. Diğer bir ifadeyle, etkin bir uyar-kaldır mekanizması kurmuş ve işletmiştir. Bir internet haber sitesi olarak, kullanıcıları haberlere yorum yazmaya teşvik etmesi, AİHM tarafından bir bakıma cezalandırılması gereken bir davranış olarak nitelendirilmiştir. Öyle ki kullanıcıları yorum yapmaya teşvik etmek, ticari bir faaliyette bulunmak bu bağlamda içerikten sorumlu tutulmaya yol açan bir neticeye varmaktadır.

[493] **§4(X)(J)**[Sosyal teknikler].

Delfi AS şirketi daha fazla ne yapabilirdi? AİHM, kararının, yorumların proaktif bir şekilde denetlenmesine yol açacak nitelikte olmadığını belirtse de kararında kendisiyle çelişmektedir. Karardan öğrenildiği kadarıyla, Delfi AS şirketi hukuki sorumluluk altına girmemek adına moderatörler istihdam ederek her bir yorumu incelemek durumunda kalmıştır. AİHM, buna rağmen, kararının Delfi AS şirketinin iş modeline etkisi olmadığını iddia etmektedir. Haklı olarak belirtildiği üzere AİHM'nin değerlendirmesi, uyar-kaldır yöntemini etkisizleştirmiştir.[494] Keza, yer sağlayıcıların veya geniş tabiriyle hizmet sağlayıcıların log tutma gibi en temel yükümlülüklerini dahi yerine getirmesi anlamsızlaşmaktadır.[495]

AİHM, vermiş olduğu kararın sosyal medya sitelerine, kişisel veya hobi amaçlı sitelere uygulanamayacağını söylese de kararın tahlilinden bu tür platformlara bu kararın uygulanmamasını gerektirecek bir sonuç çıkarmak zordur. AİHM'nin takip ettiği hukuki metodoloji takip edilirse bir sosyal medya platformu da ticari bir yapıdır ve ne kadar çok içerik paylaşılırsa platformun ticari değeri de o kadar fazla artar. Bir internet haber sitesi yorum sayfası bakımından Web 2.0 sitesidir, tıpkı kullanıcı yorumları bakımından bir sosyal medya sitesi gibi. Aynı hukuki statüde bulunan iki platformdan birisini kullanıcı yorumlarından sorumlu tutarken diğerinin bu hukuki rejimden muaf olduğunu iddia etmek, hukukun temel ilkeleriyle ve en önemlisi eşitlik ilkesiyle bağdaşmamaktadır. Eşitlik ilkesinin bir neticesi olarak aynı veya benzer statüde olanlara aynı veya benzer kuralların işletilmesi zaruridir.

AİHM, Estonya yargısının Estonya Bilgi Toplumu Hizmetleri Kanunu'nda yer alan güvenli liman kurallarını, platformun salt veriyi aktardığı durumlardaki muafiyet kurallarını uygulamamasını gereğince etüt etmemiştir. Daha önemlisi, internet hukukunun bir nevi en temel normu hâline gelen uyar-kaldır[496] yöntemini işlevsiz hâle getirmiştir. Nihayetinde, internet platformları bu kadar hızlı yaygınlaşıyorsa, kullanıcı odaklı şekilde farklı nitelikte ve türde içerik internet ortamında dolaşıma

[494] **Taşkın**, s. 195.

[495] **Taşkın**, s. 196.

[496] Uyar-kaldır yöntemi için bkz. **§4(III)(B)**[Uyar-kaldır yöntemiyle engelleme].

girebiliyorsa bunun katalizörü uyar-kaldır yöntemi ve bu yöntemin getirdiği koşullu sorumluluk rejimidir.

Kararda tartışıldığı üzere Delfi AS şirketi, uyar-kaldır mekanizmasının hakları dengeleyen bir çözüm olduğunu iddia etmiştir. AİHM'ye göre bu yöntem birçok vakada etkin bir yol olarak nitelendirilebilirse de mevcut davadaki gibi nefret söylemi ve kişilerin vücut bütünlüğüne yönelik doğrudan şiddet söylemlerinin olduğu durumlarda bu mekanizma etkin değildir. Hatta Mahkeme bir adım ileriye giderek, internet haber sitelerinin, açıkça hukuka aykırı olan yorumları, mağdur olduğu iddia edilen kişi ya da üçüncü tarafların bildirimine gerek olmaksızın derhâl kaldırmaya yönelik tedbirler almaması durumunda, başkalarının ve bir bütün olarak toplumun hak ve menfaatlerinin, AİHS'ye taraf devletlere AİHS'nin 10. maddesi çerçevesinde internet haber sitelerine sorumluluk getirme hakkını verebileceğini değerlendirmiştir.

AİHM, *Delfi AS v. Estonya* kararında internet ortamındaki anonim yorumlara karşı mahremiyetin korunmasında yol gösterici olmayı başaramamıştır.[497] Keza, internetin kendine has özel kuralları olduğunu belirtmesine rağmen bunun ne manaya geldiğini, bu politikaların neler olduğunu ortaya koyamamıştır.[498] Mahkeme, *Ahmet Yıldırım* kararındaki özgürlükçü yaklaşımını bu kararda sürdürememiştir.[499]

İsabetle belirtildiği üzere *Delfi AS v. Estonya* kararı, kendi koşullarında değerlendirilmesi gereken istisnai bir karardır.[500] AİHM daha sonra almış olduğu kararlarda (örneğin, *MTE ve Index.hu Zrt v. Macaristan* kararı gibi) *Delfi AS* kararındaki katı tutumunu yumuşatmaya çalışmıştır. Ancak, cin bir kez şişeden çıkmıştır. Müteakip içtihatlar *Delfi AS* kararının isabetsizliğini teyit etmiş ve AİHM hatadan bir ölçüde dönmeye çalışmıştır ancak bunu başaramamıştır.

---

[497] **Susi, Mart** (2014) "*Delfi AS AS v. Estonia*" The American Journal of International Law, Cilt: 108, Sayı: 2, s. 295-302, s. 302.

[498] **Susi**, s. 302.

[499] Bu yöndeki bir değerlendirme için ayrıca bkz. **Taşkın**, s. 71.

[500] Benzer görüş için bkz. **Köksal, Tuğçe Duygu** (2018) *"İnternet sağlayıcılarının üçüncü kişiler tarafından yapılan yorumlar bakımından hukuki sorumluluğu üzerine: Avrupa İnsan Hakları Mahkemesi'nin Delfi AS Kararı"* Suç ve Ceza, Sayı: 1, s. 95-114, s. 110.

§12. KALDA V. ESTONYA

AİHM'nin, internete erişim hakkı kapsamındaki bir diğer önemli kararı *Kalda v. Estonya* kararıdır.[501] Karar, aynı konudaki iki ayrı başvurunun birleştirilmesiyle verilmiştir. *Kalda v. Estonya* kararının konusu, hapishanelerde mahkûmların internete erişimine koyulan kısıtlamaların hukukiliğine ilişkindir.

I. Davanın gelişimi

Başvurucu; Romeo Kalda isimli, müebbet hapse mahkûm bir Estonya vatandaşıdır. Bay Kalda, 2005 yılında Pärnu Hapishane yönetimine başvurarak, Estonya Resmî Gazetesi'ne (*Riigi Teataja*), Yüksek Mahkeme ve idare mahkemelerinin internet ortamındaki kararlarına ve AİHM'nin içtihatlarının yer aldığı HUDOC veri tabanına erişim talep etmiştir. Ancak, talebi Hapishane yönetimi tarafından reddedilmiştir.

Bay Kalda, hapishane yönetiminin kararına karşı idari yargı yoluna başvurmuştur. İlk derece idare mahkemesi, talebi reddetmiştir. Bunun üzerine başvurduğu Temyiz Mahkemesi, Resmî Gazete'nin kâğıt versiyonunun mevcut olması sebebiyle Bay Kalda'nın talebinin yerinde olmadığına ve bilgiye erişim hakkının kısıtlanmadığına hükmetmiştir.[502] Ancak, Yüksek Mahkeme, Resmî Gazete'nin 1 Ocak 2007'den itibaren kâğıt olarak basılmadığını, sadece dijital ortamda yer aldığını not ederek tutukluların hukuki metinlere makul şekilde erişiminin sağlanması gerektiğini belirtmiştir.[503]

Öte yandan, Estonya Yüksek Mahkemesi, Pärnu Hapishane yönetiminin, Estonya idare mahkemelerinin kararları ile AİHM kararlarına erişimi kısıtlamasını kişilerin bilgiye erişim hakkının kısıtlanması olarak

---

[501] **AİHM**, *Kalda v. Estonia*, Başvuru No: 17429/10, 19.1.2016.

[502] *Kalda v. Estonya*, para. 7.

[503] *Kalda v. Estonya*, para. 8.

görmüştür. Mahkeme, bu hükme Estonya Anayasası'nın 44. maddesinin birinci fıkrasının bilgiye erişim hakkı açısından özel bir kısıtlama getirmediğini ve bu sebeple, tutuklular ile özgür kişiler arasında ayrımcılık yapılmasının açık bir dayanaktan yoksun olduğunu dikkate alarak ulaşmıştır.[504]

Bay Kalda, daha sonra nakledildiği Tartu Hapishanesinde de benzer sorunlar yaşamış ve 18 Ekim 2007 tarihinde, www.coe.ee (Avrupa Konseyi İletişim Ofisinin Tallinn'deki yerel sitesi), www.oiguskantsler.ee (Adalet Bakanlığı sitesi) ve www.riigikogu.ee (Estonya Parlamentosu sitesi) sitelerine erişim sağlayamadığı için Tartu Hapishane yönetimine başvurmuş ancak bu başvuru Hapishane yönetimi tarafından reddedilmiştir.[505] Bay Kalda'nın bu talebinin temelini Hapishane yönetimiyle yaşadığı hukuki ihtilaflar oluşturmuştur.[506] Bay Kalda, haklarını mahkemede savunabilmek için söz konusu hukuki metinlere erişmeyi amaçlamıştır.

23 Kasım 2007 tarihinde Bay Kalda'nın başvurusu Adalet Bakanlığı tarafından da reddedilmiştir. Bay Kalda, bu karara itiraz etmiştir. İtirazı inceleyen Tartu İdare Mahkemesi, talebi yerinde görmüş ve Tartu Hapishanesi yönetimine Bay Kalda'ya bu amaçla kullanılan özel bir bilgisayarda, gözetim altında www.coe.ee sitesine erişim imkânı tanıması talimatı vermiştir.[507] Öte yandan, 1 Haziran 2008 tarihli Estonya İnfaz Kanunu'nun 31. maddesinin birinci fıkrasında dayanağı olmadığı için www.oiguskantsler.ee ve www.riigikogu.ee sitelerine erişim verilmesi talebi reddedilmiştir. Hem Bay Kalda hem de Hapishane yönetimi söz konusu karara itiraz etmişler, Temyiz Mahkemesi itirazları reddetmiş ve konu son aşamada Estonya Yüksek Mahkemesinin önüne gelmiştir.

Yüksek Mahkeme, hapishanelerde sadece belirli sitelere erişime izin veren Estonya İnfaz Kanunu'nun 31. maddesinin birinci fıkrasının Anayasa'ya ve özel olarak herkesin kamusal erişime açılmış bilgiye erişim

---

[504] *Kalda v. Estonya*, para. 9.

[505] *Kalda v. Estonya*, para. 10.

[506] *Kalda v. Estonya*, para. 10.

[507] *Kalda v. Estonya*, para. 12.

hakkına uygunluğunu değerlendirmiştir.[508] Mahkeme, kişilerin hapis cezası ile cezalandırılmasının amacının kamu düzenini korumak ve tutukluları hukuka uyan bireyler hâline getirmek olduğunu belirtmiştir. Tutuklulara internet erişimi verilmesinin kötüye kullanımlara yol açabileceğini vurgulayan Yüksek Mahkeme, İnfaz Kanunu'nun 31. maddesinin birinci fıkrasında sayılan hukuk veri tabanlarına erişimin, tutukluların haklarını koruyabilmeleri adına tanındığını kaydetmiştir.[509] Mahkeme, tutukluların söz konusu hukuki metinlere sadece internet ortamında erişebileceğini de not etmiştir.

Yüksek Mahkeme, tutuklulara uygulanan internet erişimi yasağının, tutukluluk amaçlarıyla bağdaşmayan bir iletişim kurulmasını engellemek amacıyla getirildiğini belirtmiş, internet ortamındaki bilgilerin hapishanenin güvenliğini tehlikeye atabileceğini veya tutukluların hukuka uyan bireyler olmasına halel getirebileceğini ifade etmiştir.[510] Mahkeme, bu kısıtlamaların tutukluluğun amacına ulaşması ve kamu güvenliğini sağlamak için gerekli olduğunu belirtmiştir.

Yüksek Mahkeme, konuyu ölçülülük açısından da incelemiştir. Mahkeme, tutukluların internete geniş şekilde erişiminin bu kişilerin yasaklanmış iletişimler kurmasına yol açacağını, bu durumun da artırılmış bir kontrol seviyesi ve hâliyle maliyet gerektireceğini belirtmiştir.[511] Mahkeme, tutukluların basılı içeriklere erişim talep edebildiği gerçeğini de dikkate alarak engelleme ile amaçlanan hedefi ölçülü olarak görmüş ve Anayasa'da yer alan bilgiye erişim hürriyetinin ihlali olmadığı tespitini yapmıştır.[512]

II. Hukuki arka plan

AİHM, kararı incelerken Estonya Anayasası'nın herkesin kamusal bilgiye özgürce erişim hakkı olduğunu düzenleyen 44. maddesinin birinci

[508] *Kalda v. Estonya*, para. 15.
[509] *Kalda v. Estonya*, para. 15.
[510] *Kalda v. Estonya*, para. 16.
[511] *Kalda v. Estonya*, para. 17.
[512] *Kalda v. Estonya*, para. 17.

fıkrasına, Kamusal Bilgi Kanunu'na ve İnfaz Kanunu'nun 31. maddesinin birinci fıkrasına atıf yapmıştır. Ayrıca, Avrupa Konseyinin ve Birleşmiş Milletlerin[513] internete erişimle ilgili temel hak ve hürriyet eksenli muhtelif belgelerine atıf yapmıştır.[514]

III. Tarafların iddiaları

Bay Kalda, internet ortamında hukuki konularda araştırma yapmasının engellenmiş olmasının, AİHS'nin 10. maddesinde koruma altına alınan ifade özgürlüğüne bir müdahale olduğunu iddia etmiştir. Estonya Hükûmeti ise söz konusu bilgilere alternatif erişimin mümkün olması sebebiyle AİHM'nin başvuruyu reddetmesini talep etmiştir.[515] AİHM, başvuruyu kabul edilebilir görmüştür.

Bay Kalda, Estonya hapishane sistemiyle ilgili çeşitli davaları bulunduğunu, ihtilaf konusu web sitelerine erişme amacının kendi haklarını korumak olduğunu iddia etmiştir.[516] Bay Kalda, internette yer alan içtihatlara getirilen erişim kısıtlamasının, bilgiye erişim hakkına toptan bir yasaklama teşkil ettiğini belirtmiştir. Bay Kalda, hukuki araştırma yapmakla spesifik bir bilgiyi talep etmenin birbirinden farklı hususlar olduğunu ileri sürmüştür.[517]

Bay Kalda, Estonya Hükûmetinin söz konusu sitelere erişim sebebiyle oluşan bilişim tehditleri iddiasını da reddetmiştir.[518] Bu sitelerin referanslar, arama motorları, bağlantılar (sosyal medya bağlantıları dâhil) içerdiğini ve bunların Adalet Bakanlığı sistemlerince etkin şekilde engellendiğini belirtmiştir. Bu doğrultuda, erişim talep ettiği sitelerle hâliha-

---

[513] Bkz. **Birleşmiş Milletler**, "*The UN Human Rights Council's Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression of 16 May 2011 to the Human Rights Council (A/HRC/17/27)*"

[514] *Kalda v. Estonya*, para. 19-25.

[515] *Kalda v. Estonya*, para. 28-30.

[516] *Kalda v. Estonya*, para. 31.

[517] *Kalda v. Estonya*, para. 32.

[518] *Kalda v. Estonya*, para. 34.

zırda eriştiği siteler arasında ayrım yapılmasının dayanağı olmadığını ileri sürmüştür.[519]

Son olarak Bay Kalda, internet erişimine alternatif olarak sunulan basılı içtihatlara erişimin zahmetli olduğunu ve makul olmadığını iddia etmiştir.[520] Bay Kalda, bu iddiasını, tutukluların kâğıt belgeler dâhil en fazla 30 kilogramlık eşyaya sahip olabileceği ve ücretsiz en fazla 21 sayfalık yazıcı çıktısı alabileceği kısıtlamasıyla gerekçelendirmiştir.

Estonya Hükûmeti, öte yandan, AİHS'nin 10. maddesinin ihlal edilmediğini iddia etmiştir. Hükûmet, devletin belirli grup kişilere (mahkûmlar gibi) bilgiye erişim kanallarına yönelik kısıtlama getirmede takdir yetkisi olduğunu ve mahkûmların özgür kişilerle aynı statüde olmadığı için Estonya Anayasası'nda yer alan bilgiye erişim hakkından eşit olarak yararlanamayacağını ileri sürmüştür.[521] Bu kısıtlamanın, İnfaz Kanunu'nun 31. maddesinin birinci fıkrasında açıkça yeri olduğu belirtilmiştir.

Estonya Hükûmetine göre, internete kısıtlama getirmenin temel amacı, hapishane güvenliğinin temin edilmesi, hapishane dışındakilerin korunması, özellikle suçla mücadelenin sağlanması ve mağdurların korunmasıdır.[522] İçeriğin teknik olarak engellenmesinin maliyetine ve zorluğuna da vurgu yapan Estonya Hükûmeti, izin verilen ve yasaklanan sitelerin, başvurucu Bay Kalda'nın hakları ve kamusal güvenlik dikkate alındığında ölçülü olarak belirlendiğini belirtmiştir.[523] Aynı doğrultuda, alternatif yöntemlerin varlığı (yazışma ve telefon görüşmesi yapma gibi) karşısında, Bay Kalda'nın bilgiye erişiminin tamamen kısıtlandığından bahsedilemeyeceğini tekrar etmiştir.[524] Estonya Hükûmeti ayrıca muhtelif içtihatları tercüme etmeye ve erişilebilir kılmaya yönelik diğer inisiyatiflerine de atıf yapmıştır.[525]

---

[519] *Kalda v. Estonya*, para. 34.
[520] *Kalda v. Estonya*, para. 35.
[521] *Kalda v. Estonya*, para. 36.
[522] *Kalda v. Estonya*, para. 37.
[523] *Kalda v. Estonya*, para. 38.
[524] *Kalda v. Estonya*, para. 39.
[525] *Kalda v. Estonya*, para. 40.

IV. AİHM'nin tespit ve değerlendirmeleri

Davanın esasına giren AİHM, öncelikle bilgiye erişim hakkının sınırlarını ortaya koymaya çalışmıştır. AİHM, kamuyu ilgilendiren bilgilere erişimin temel bir hak olduğuna yönelik tespitlerini tekrarlamış ve kamusal tartışma için ortamlar hazırlamanın sadece basınla sınırlı olmadığını vurgulayarak bu yöndeki temel içtihatlarını hatırlatmıştır.[526] Bu tespitinden sonra AİHM, mevcut uyuşmazlığın niteliğinin farklılığına dikkat çekmiş ve uyuşmazlığın, bir mahkûmun internet ortamında konusu belirli bir içeriğe ulaşması ile ilgili olduğunu belirtmiştir.[527]

AİHM, hapis cezasının, tutukluların dış dünyayla iletişimine kısıtlama getirmesinin kaçınılmaz olduğunun farkındadır.[528] Bu doğrultuda, AİHS'nin 10. maddesinin tutuklular için genel bir bilgiye erişim imkânı sağlanması yükümlülüğü getirmediğini belirtmiştir. Ancak AİHM, Estonya hukukunda tutuklulara kısıtlı bir erişim hakkı tanındığını belirtip bu hakka ilişkin kısıtlamanın hukukiliğini değerlendirmeye almıştır. Açıkça kanunda yer aldığı için söz konusu kısıtlamanın kanunla öngörülme şartını taşıdığını ve müdahalenin başkalarının haklarını korumak, düzensizliği ve suçu önlemek amacıyla getirildiğini kabul etmiştir.[529]

Kanunda öngörülme şartını değerlendirdikten sonra AİHM, müdahaleyi ölçülülük açısından incelemiştir. AİHM, Bay Kalda'nın erişmeye çalıştığı sitelerin esas olarak mahkûmların hakları dâhil hukuki bilgiler içeren siteler olduğunu not etmiştir.[530] Mahkeme, bir bilgiye özel olarak erişim için öncelikle o bilgiden haberdar olunması gerektiğini belirtmiş ve Estonya mahkemelerin bilgiye erişim için farklı yöntemlerin maliyetini kıyaslamadığı tespitini yapmıştır.[531]

---

[526] *Kalda v. Estonya*, para. 41-42.

[527] *Kalda v. Estonya*, para. 43.

[528] *Kalda v. Estonya*, para. 45.

[529] *Kalda v. Estonya*, para. 46-47.

[530] *Kalda v. Estonya*, para. 50.

[531] *Kalda v. Estonya*, para. 50.

AİHM, internete erişimin bir hak olarak tanınması gerektiğinin altını çizmiştir.[532] Mahkeme, birçok bilginin artık sadece internet ortamında yer aldığını belirtmiştir. Buna örnek olarak Estonya Resmî Gazete'sinin sadece online olarak yayımlanmasını göstermiştir. Ayrıca, online olarak yayımlanan bu Resmî Gazete'nin AİHM kararlarının Estonca özetlerini ve çevirilerini paylaştığını da belirtmiştir.

Tüm bu tespitlerden sonra Mahkeme, Estonya İnfaz Kanunu uyarınca tutuklulara hapishane yönetiminin gözetiminde özel olarak tahsis edilmiş ve sınırlı erişimi olan bilgisayarlar temin edildiğini hatırlatmıştır.[533] Mahkeme, tüm bu süreçlerin masraflarının/yüklerinin kamu otoriteleri tarafından üstlenildiğini, güvenlik ve maliyete ilişkin itirazların özünde konuyla ilgili olduğunu kabul etmiştir. AİHM burada önemli bir nüansa vurgu yapmıştır. AİHM, yerel mahkemelerin, davaya konu ilave üç web sitesine daha erişim sağlanmasının getireceği riske ilişkin kapsamlı bir güvenlik analizi yapmadığını ve söz konusu sitelerin devlet otoriteleri ile uluslararası organizasyonlara ait olduğunu dikkate almadığını belirtmiştir.[534]

AİHM, bu bağlamda, gerekli etki analizinin yapılmadığı kanaatindedir. Bu koşullar altında AİHM, mevcut olayda başvurucu Bay Kalda'nın bilgiye erişim hakkına müdahaleyi meşru kılacak yeterli gerekçelerin ortaya konulmadığına hükmetmiştir. Nihayetinde AİHM, müdahalenin demokratik toplum gerekliliklerine uygun olmadığına karar vermiş ve Bay Kalda'nın talebini haklı görmüştür.[535] AİHS'nin 10. maddesinin ihlal edildiğine hükmedilmiştir.

V. Yargıç Jon Fridrik Kjølbro'nun muhalif görüşü

AİHM Yargıcı Jon Fridrik Kjølbro, AİHM'nin *Kalda v. Estonya* kararına katılmamış ve müstakil bir muhalif görüş kaleme almıştır.[536] Yargıç

[532] *Kalda v. Estonya*, para. 52.

[533] *Kalda v. Estonya*, para. 53.

[534] *Kalda v. Estonya*, para. 53.

[535] *Kalda v. Estonya*, para. 54.

[536] *Kalda v. Estonya*, Yargıç J.F. Kjølbro'nun Muhalif Görüşü.

Kjølbro, başvuranın üç web sitesine erişiminin kısıtlanmasının, AİHS'nin 10. maddesiyle teminat altına alınan bilgiye erişim özgürlüğüne müdahale olduğu yönündeki çoğunluk görüşüne katılmaktadır.[537] Yargıç Kjølbro, aynı doğrultuda, çoğunluğun müdahalenin kanunla öngörüldüğü ve meşru amaçlar güttüğüne ilişkin görüşüne de katılmaktadır.[538] Fakat Yargıç Kjølbro, müdahalenin demokratik bir toplumun gerekliliklerine uymadığına yönelik çoğunluk görüşüne katılmamaktadır.[539]

Yargıç Kjølbro, AİHM'nin tutukluların internete erişim hakkı konusunu -genel veya sınırlı bir formda- ilk defa ele aldığını ve bir mahkûmun internete erişiminin yasaklanmasının AİHS'nin 10. maddesinin ihlali olduğuna ilk kez karar verdiğini ifade etmiştir. Yargıç Kjølbro'ya göre, çoğunluk, başvuranın müebbet hapis cezasına çarptırılmış ve kapalı cezaevinde yatan bir kişi olduğu gerçeğini yeterince değerlendirmemiştir.[540] Yargıç Kjølbro, AİHM'nin bu yaklaşımının, Mahkemenin kendi içtihatlarıyla çelişen bir durum olduğunu ileri sürmüştür. Nitekim Yargıç Kjølbro, AİHM'nin, muhtelif kararlarında, tutukluluğun kaçınılmaz bir neticesi olarak suç işlenmesinin ve asayişin bozulmasının önlenmesi amaçlarıyla tutukluların AİHS'deki haklarının güvenlik gerekçesiyle kısıtlanmasını haklı bulduğunu hatırlatmıştır.[541]

Yargıç Kjølbro, tutukluların internete erişiminin engellenmesi tedbirinin, güvenlik risklerini bertaraf etmek amacıyla alındığını tekrarlamıştır. Yargıç Kjølbro, kötüye kullanım ve güvenlik riskleri sebebiyle tutukluların bilgiye erişim hakkını kısıtlayan Estonya kanun koyucusunun, tutuklular ile toplumun yarışan menfaatleri arasında bir denge gözettiğini belirtmiştir.[542] Yargıç, mevcut kararın, bir içeriğe erişim sağlayan âkit devletlere başka sitelere de erişim sağlama yükümlülüğü getireceğini vurgulamıştır.

---

[537] *Kalda v. Estonya*, Yargıç J.F. Kjølbro'nun Muhalif Görüşü, para. 2.

[538] *Kalda v. Estonya*, Yargıç J.F. Kjølbro'nun Muhalif Görüşü, para. 3.

[539] *Kalda v. Estonya*, Yargıç J.F. Kjølbro'nun Muhalif Görüşü, para. 3.

[540] *Kalda v. Estonya*, Yargıç J.F. Kjølbro'nun Muhalif Görüşü, para. 4.

[541] *Kalda v. Estonya*, Yargıç J.F. Kjølbro'nun Muhalif Görüşü, para. 4.

[542] *Kalda v. Estonya*, Yargıç J.F. Kjølbro'nun Muhalif Görüşü, para. 7.

Yargıç Kjølbro, AİHM'nin konuya, engellenen sitelerin içeriği açısından yaklaştığını, yerel otoritelerin İnfaz Kanunu'nun 31. maddesinin birinci fıkrasını ihdas etme amacı olan güvenlik gerekçelerinin göz ardı edildiğini, hâliyle bu durumun yerel otoritelerin yerindelik değerlendirmesinin bir denetimi niteliğinde olduğunu tartışmıştır.[543]

Yargıç Kjølbro, AİHM'nin atıf yaptığı internetle ilgili uluslararası metinlerin yorumuna da eleştiri getirmiştir.[544] İnternetin topluma faydasını yadsımayan Yargıç Kjølbro, internete erişimi temel hak olarak gören ilgili metinlerin hiçbirinin tutukluların internete erişimine ilişkin bir husus içermediğinin altını çizmiştir. Atıf yapılan tüm uluslararası belgelerin internetin genel önemine vurgu yaptığını fakat hiçbirinin AİHS'nin 10. maddesinin tutuklulara genel olarak veya kısıtlı şekilde bir erişim sağlanması yönünde yorumlanmasını destekleyecek nitelikte olmadığını belirtmiştir.[545]

Yargıç Kjølbro, AİHM'nin mukayeseli hukuka atıf yapmamasını da eleştirmiştir.[546] Karardaki bilgilerin, hapis cezalarını çeken kişilere genel olarak veya kısıtlı şekilde bir internet erişimi sağlanması yönünde bir Avrupa konsensüsü olduğuna yönelik yeterli bir temel oluşturmadığı belirtilmiştir.[547]

Yargıç Kjølbro, önemli bir hatırlatma yapmaktadır. Yargıç Kjølbro'ya göre, kötüye kullanma riski ve özünde var olan güvenlik riskleri o kadar mühimdir ki AİHM, bir devlete tutuklulara internet erişimi sağlamaya yönelik bir yükümlülük yüklerken dikkatli olmalıdır. Zira erişim sağlama yükümlülüğünün devletler bakımından kontrol önlemleri alma gibi pratik ve finansal sonuçları olacaktır.[548] Öyle ki gerekli denetim mekanizmasını kurmak her zaman mümkündür fakat bunun yükü ve maliyeti devletler için aşırı olabilir.

---

[543] *Kalda v. Estonya*, Yargıç J.F. Kjølbro'nun Muhalif Görüşü, para. 8.

[544] *Kalda v. Estonya*, Yargıç J.F. Kjølbro'nun Muhalif Görüşü, para. 9.

[545] *Kalda v. Estonya*, Yargıç J.F. Kjølbro'nun Muhalif Görüşü, para. 9.

[546] *Kalda v. Estonya*, Yargıç J.F. Kjølbro'nun Muhalif Görüşü, para. 10.

[547] *Kalda v. Estonya*, Yargıç J.F. Kjølbro'nun Muhalif Görüşü, para. 10.

[548] *Kalda v. Estonya*, Yargıç J.F. Kjølbro'nun Muhalif Görüşü, para. 11.

Yargıç Kjølbro, içeriğe erişime ilişkin alternatif yöntemleri dikkate alarak Estonya idari makamlarınca gerçekleştirilen uygulamayı ölçülü olarak nitelendirmektedir.[549] Yargıç Kjølbro, AİHM'nin kararının, mahkûmların başka web sitelerine de erişim talep etmesine yol açacağını hatırlatmaktadır.[550]

Yargıç Kjølbro, yukarıda belirtilen tüm gerekçeleri tekrarlayarak devletlerin tutukluların internete erişimini kısıtlama konusunda daha geniş takdir yetkisini haiz olması gerektiğini, mevcut uyuşmazlıkta AİHS'nin 10. maddesinin ihlal edilmediğini belirtmiştir.[551] Konunun önemi ve etkilerini dikkate alarak bu kararın Büyük Daire tarafından verilmiş olması gerektiğini de tartışmıştır.[552]

VI. Değerlendirme

AİHM'nin, *Delfi AS v. Estonya* kararı sonrası internetle ilgili ele aldığı önemli bir karar olan *Kalda v. Estonya* kararında internetin düzenlenmesi konusunda isabetli ve sağlam temelli bir yaklaşım ortaya koyamadığı gözlemlenmektedir. Bunun temelinde AİHM'nin, vermiş olduğu kararların neticelerinin etki analizini yapmaması ve interneti tek taraflı ele alması yatmaktadır.

AİHM, interneti AİHS'deki tüm hakları perçinleyen sihirli bir değnek olarak görmekte ve internete demokratik toplumun mutlak dönüştürücüsü olarak yaklaşmaktadır. İnternetin faydaları, demokratik toplumdaki tartışmaların oluşumuna etkisi, bilgiye erişim ile insan hakları aktivizmine katkıları yok sayılamaz. Ancak, internet bundan ibaret değildir. İnternet, toplum için büyük bir fırsattır; aynı internet, gerekli denge sağlanmazsa toplumsal barışın temellerini sarsma potansiyeline sahiptir. Bunun birçok örneğine dünyanın çok farklı coğrafyalarında şahit olunmuştur.

---

[549] *Kalda v. Estonya*, Yargıç J.F. Kjølbro'nun Muhalif Görüşü, para. 12.

[550] *Kalda v. Estonya*, Yargıç J.F. Kjølbro'nun Muhalif Görüşü, para. 13.

[551] *Kalda v. Estonya*, Yargıç J.F. Kjølbro'nun Muhalif Görüşü, para. 14.

[552] *Kalda v. Estonya*, Yargıç J.F. Kjølbro'nun Muhalif Görüşü, para. 15.

AİHM, internetin teknik işleyişini içselleştirememektedir. Bunun en bariz örnekleri *Akdeniz v. Türkiye*, *Cengiz ve Diğerleri v. Türkiye* ile *Delfi AS v. Estonya* kararlarında gözlemlenmiştir. Aynı hatalı yaklaşım *Kalda v. Estonya* kararında da sürdürülmüştür. AİHM, konu internet olunca kendi içtihatlarıyla ve temel insan hakları kurallarıyla çelişmekte, temel hak ve hürriyetlerin meşru sınırlarının olduğunu gereğince etüt edememektedir.

İnternet, dinamik bir alandır. Beşinci bölümde etraflıca incelendiği üzere, en kompleks filtreleme ve erişimi engelleme sisteminin bile aşılması mümkündür. Mükemmel bir sistem yoktur ve internetin gelişim dinamikleri dikkate alındığında hiçbir zaman da olmayacaktır. AİHS'nin sihirli değneği bile olsa, getirilen çözüm kısa bir sürede demode olacaktır. DPI teknolojilerinin kısa sürede başına gelenler bunun en güzel örneğidir.

Yargıç Kjølbro'nun tüm tespitleri yerindedir. Hapishane gibi özel bir alanda, tutuklular gibi özel statülü bireylerin bilgiye erişim haklarını incelerken AİHM, madalyonun diğer yüzünü, güvenlik risklerini yok saymaktadır. Devletlere aşırı bir külfet yüklenerek mağdurların hakları, güvenlikleri, hapishane güvenliği, suç işlenmesinin önlenmesi (ki hepsi meşru taleplerdir) riskleri göz ardı edilmektedir.

§13. MTE VE INDEX.HU ZRT V. MACARİSTAN

AİHM'nin *Delfi AS v. Estonya* kararı büyük tartışmalar başlatmıştır. Kararın internet platformlarına ölçüsüz bir yükümlülük getirdiği ileri sürülmüştür. AİHM, bu tartışmalar hararetini korurken benzer bir konudaki başka bir başvuruyu karara bağlamıştır. *MTE ve Index.hu Zrt v. Macaristan* kararı,[553] bir nevi *Delfi AS v. Estonya* kararının şerhi gibidir. Bu kararda AİHM, internet platformlarının sorumluluğuna açıklık getirmeye çalışmıştır fakat AİHM'nin bu konuda başarılı olduğunu söylemek zordur. *MTE ve Index.hu Zrt v. Macaristan* kararı da tartışmalı bir karardır.

I. Davanın gelişimi

MTE ve Index.hu, Macaristan'da kurulu tüzel kişilerdir. *MTE ve Index.hu Zrt v. Macaristan* kararı, MTE ve Index.hu tarafından sunulan sitelerde yer alan kullanıcı yorumlarına, bu tüzel kişilerin aktif şekilde moderasyon yapmalarına ilişkin kuralların AİHS'nin 10. maddesinde yer alan ifade özgürlüğü ile internet ortamında yorum yapma özgürlüğünü ihlal ettiği iddiasını konu edinmektedir.[554]

MTE, Budapeşte'de kurulu bir dernek olup Macaristan internet içerik sağlayıcılarının öz düzenleyici kurumu olarak faaliyet göstermektedir. İnternet içerik sağlayıcılarının özel mesleki ilkelere ve etik kurallara riayetini kontrol etmekte ve on bir üyesi arasında doğabilecek ihtilaflarda özel bir uyuşmazlık çözüm/tahkim komisyonu olarak hareket etmektedir.[555] Index.hu da Budapeşte'de kurulu bir limitet şirket olup Macaristan'daki en büyük internet portalını işletmektedir.

---

[553] **AİHM**, *Magyar Tartalomszolgáltatók Egyesülete (MTE) ve Index.hu Zrt v. Macaristan*, Başvuru No: 22947/13, 2.5.2016.

[554] *MTE/Index.hu Zrt v. Macaristan*, para. 3.

[555] *MTE/Index.hu Zrt v. Macaristan*, para. 5.

Her iki kuruluşun işlettiği internet portallarında kullanıcıların yorum yapmasına imkân tanıyan bir altyapı vardır. Yorum yapma izni ancak üye olan kullanıcılara veriliyorsa da yorumlar bir ön kontrolden geçirilmemekte veya düzenlenmemektedir.[556] Her iki portalda da yorumların portal sahiplerinin görüşünü yansıtmadığı ve tüm sorumluluğun kullanıcılarda olduğuna dair birer uyarı vardır.[557] Ayrıca, olası bir kötüye kullanımı önlemek adına uyar-kaldır sistemi işletilmektedir.[558] Index.hu portalında yalnızca kısmi bir moderasyon vardır ve gerektiğinde yorumlar silinebilmektedir.[559] Tüm bunların yanında, her iki portalda, başkalarının kişilik haklarını ihlal eden içeriklerin platformlarına yüklenemeyeceğine dair uyarılar vardır.[560] Index.hu sitesinde ayrıca detaylı moderasyon kuralları yer almaktadır.[561]

5 Şubat 2010 tarihinde MTE "*İnternet ortamında etik olmayan bir diğer ticari davranış*" başlığı altında, iki emlak yönetim sitesine ilişkin bir görüş paylaşmıştır.[562] Söz konusu siteler, ücretsiz üyelik sonunda kullanıcılardan ücret talep etmeleri, sözleşme koşullarını tek taraflı olarak değiştirme haklarını saklı tutmaları ve içerikler ile kişisel verileri silmek için üyelik ücretinin ödenmesini zorunlu kılmaları sebebiyle MTE tarafından eleştirilmiştir.

MTE'nin haberinin altına, rumuz kullanılarak söz konusu sitelerin saçma, eşkıya şirket (*mug company*) olduğu şeklinde yorumlar yazılmıştır.[563] MTE tarafından kaleme alınan haber, Zöld Újság Zrt tarafından yönetilen vg.hu sitesince olduğu gibi kopyalanmıştır.[564] Index.hu da aynı

[556] *MTE/Index.hu Zrt v. Macaristan*, para. 6.
[557] *MTE/Index.hu Zrt v. Macaristan*, para. 7.
[558] *MTE/Index.hu Zrt v. Macaristan*, para. 8.
[559] *MTE/Index.hu Zrt v. Macaristan*, para. 8.
[560] *MTE/Index.hu Zrt v. Macaristan*, para. 9.
[561] *MTE/Index.hu Zrt v. Macaristan*, para. 10.
[562] *MTE/Index.hu Zrt v. Macaristan*, para. 11.
[563] *MTE/Index.hu Zrt v. Macaristan*, para. 12.
[564] *MTE/Index.hu Zrt v. Macaristan*, para. 13.

haberi sitesinin tüketicilerin korunması kısmında paylaşmış ve yine içeriğin altına takma adla küfür ve hakaret içeren yorumlar yazılmıştır.[565]

17 Şubat 2010 tarihinde söz konusu emlak yönetim sitelerini yöneten şirket; MTE, Index.hu ve Zöld Újság Zrt aleyhine yanlış, saldırgan içerikler sebebiyle itibarının zedelendiğinden bahisle tazminat davası açmıştır.[566] Davalılar, davanın açıldığını haber alır almaz söz konusu içerikleri sitelerinden kaldırmıştır.

MTE, Index.hu ve Zöld Újság Zrt'nin temel iddiaları, aracı platformlar oldukları ve kullanıcı yorumlarından sorumlu tutulamayacakları yönündedir.[567] Bu iddialarını, Macar hukuku düzenlemesi olan 108 (CVIII) sayılı Elektronik Ticari Hizmetler Kanunu'na dayandırmışlardır. Bu iddia yerel mahkeme tarafından kabul edilmemiş, mahkeme söz konusu içeriklerin değiştirilmiş/editoryal süreçten geçirilmiş içerikler olduğundan bahisle davalıların sorumlu olduklarına hükmetmiştir.[568] Kullanıcı yorumlarını maddi olarak da ele alan yerel mahkeme, söz konusu içeriklerin bazılarının kabul edilebilir eleştiri seviyesini aştığı tespitini de yapmıştır.[569]

Tüm taraflar bu karara itiraz etmiştir. MTE, Index.hu ve Zöld Újság Zrt, içeriklere ilişkin bir uyarı almadıklarını, davadan haberdar olur olmaz içerikleri kaldırdıklarını, kullanıcı yorumlarının editoryal içerik olarak değerlendirilemeyeceğini ve bu yorumlar bakımından bilgi depolayan hizmet sağlayıcılar olarak hareket ettiklerini ileri sürmüşlerdir.[570]

Budapeşte Temyiz Mahkemesi, 27 Ekim 2011 tarihli kararıyla yerel mahkemenin kararını farklı bir gerekçeyle onamıştır.[571] Temyiz Mahkemesi, Elektronik Ticari Hizmetler Kanunu'nun, AB e-Ticaret Direktifi'ni iç hukuka aktaran bir düzenleme olduğunu ve sadece ticari nitelikteki

[565] *MTE/Index.hu Zrt v. Macaristan*, para. 14.
[566] *MTE/Index.hu Zrt v. Macaristan*, para. 15.
[567] *MTE/Index.hu Zrt v. Macaristan*, para. 16.
[568] *MTE/Index.hu Zrt v. Macaristan*, para. 17.
[569] *MTE/Index.hu Zrt v. Macaristan*, para. 17.
[570] *MTE/Index.hu Zrt v. Macaristan*, para. 18.
[571] *MTE/Index.hu Zrt v. Macaristan*, para. 19.

elektronik hizmetlere özellikle de internet üzerinden yapılan alışverişlere uygulandığını belirtmiştir.[572] Temyiz Mahkemesi, yorum faaliyetinin bu hizmetler kapsamına girmediğini belirtmiş ve bu sebeple yer sağlayıcı ve aracı kavramlarını detaylı inceleme gereği görmemiştir. Tüm bu tespitler ışığında Temyiz Mahkemesi, yorumları söz konusu emlak yönetim şirketlerinin haklarını ihlal eder nitelikte görmüş, yorumları sonradan kaldırmış olsalar da MTE, Index.hu ve Zöld Újság Zrt'nin objektif olarak bu içeriklerden sorumlu olduğuna hükmetmiştir.[573]

MTE, Index.hu ve Zöld Újság Zrt, bu karara itiraz ederek konuyu Macaristan Yüksek Mahkemesine (Kúria) taşımışlardır.[574] Macaristan Yüksek Mahkemesi, önceki tüm yerel mahkeme ve temyiz mahkemesi kararlarını onamıştır.[575] Macaristan Yüksek Mahkemesi, ilgili site yöneticilerinin sitelerinde kullanıcıların yorum yapmasına olanak tanıyarak objektif olarak her türlü incitici ve hukuka aykırı içerikten sorumlu olduğunu belirtmiştir. Macaristan Yüksek Mahkemesi, Budapeşte Temyiz Mahkemesinin gerekçelerini tekrarlayarak başvurucuların yer sağlayıcı istisnasına dayanamayacaklarına hükmetmiştir.[576] Karar, 2 Ekim 2012 tarihinde verilmiştir.

MTE, Index.hu ve Zöld Újság Zrt, son aşamada bu kararı 3 Ocak 2013 tarihinde şikâyet yoluyla Anayasa Mahkemesine taşımışlardır.[577] MTE, Index.hu ve Zöld Újság Zrt'nin temel iddiası, yorumlardan dolayı sorumlu tutulmalarının ifade özgürlüklerine ölçüsüz bir kısıtlama getirdiğidir. Anayasa Mahkemesi 11 Mart 2013 tarihinde şikâyeti kabul edilebilir görmüştür.[578]

Macaristan Anayasa Mahkemesi, yaptığı inceleme neticesinde şikâyeti 27 Mayıs 2014 tarihinde reddetmiştir.[579] Anayasa Mahkemesi,

[572] *MTE/Index.hu Zrt v. Macaristan*, para. 20.
[573] *MTE/Index.hu Zrt v. Macaristan*, para. 20.
[574] *MTE/Index.hu Zrt v. Macaristan*, para. 21.
[575] *MTE/Index.hu Zrt v. Macaristan*, para. 22.
[576] *MTE/Index.hu Zrt v. Macaristan*, para. 22.
[577] *MTE/Index.hu Zrt v. Macaristan*, para. 23.
[578] *MTE/Index.hu Zrt v. Macaristan*, para. 24.
[579] *MTE/Index.hu Zrt v. Macaristan*, para. 25.

blogların ve yorumların, ifade özgürlüğü altında korunan faaliyetler olduğunu belirtmiştir. Anayasa Mahkemesi de neredeyse önceki tüm yerel mahkemelerin ve üst mahkemelerin kararlarını tekrar ederek, benzer bir yaklaşımla internet sitelerinin sorumlu olduğuna hükmetmiştir. Mahkeme, yakın tarihli bir kararında kişilik haklarını korumak için yazarların değil, bilfiil basın organlarının sorumlu tutulmasını Anayasa'ya uygun bulduğunu hatırlatmıştır.[580]

II. Hukuki arka plan

AİHM, yerel hukuki düzenlemelerden Macaristan Medeni Kanunu'nun 75. maddesini alıntılamıştır.[581] Söz konusu hüküm, herkesin, kişilik haklarının korunmasını talep etme hakkı olduğunu düzenlemektedir. Hüküm, tüzel kişilere de niteliği örtüştüğü ölçüde kişilik haklarının korunması imkânını tanımaktadır. AİHM'nin alıntıladığı bir diğer düzenleme ise Elektronik Ticari Hizmetler Kanunu'dur.[582] Bu düzenleme, AB e-Ticaret Direktifi'ne benzer şekilde bilgi toplumu hizmet sağlayıcılarını tanımlamaktadır.

İlgili uluslararası ve mukayeseli hukuk örneklerinde ise AİHM, *Delfi AS v. Estonya* kararının ilgili kısmına atıf yapmakla yetinmiştir.[583] Bu yaklaşım bile *MTE ve Index.hu Zrt v. Macaristan* davasının *Delfi AS v. Estonya* kararıyla ne kadar ilintili olduğunu göstermektedir.

III. Tarafların iddiaları

Başvuruculların temel iddiası, Macar mahkemelerinin, kullanıcı yorumları sebebiyle internet siteleri yöneticilerine objektif sorumluluk getiren kararlarının AİHS'nin 10. maddesinde güvence altına alınan ifade özgürlüğüne ölçüsüz bir müdahale olduğu yönündedir.[584] Macar

[580] *MTE/Index.hu Zrt v. Macaristan*, para. 25.
[581] *MTE/Index.hu Zrt v. Macaristan*, para. 26.
[582] *MTE/Index.hu Zrt v. Macaristan*, para. 27.
[583] *MTE/Index.hu Zrt v. Macaristan*, para. 28.
[584] *MTE/Index.hu Zrt v. Macaristan*, para. 29.

Hükûmeti, bu iddiaya itiraz etmiştir.[585] AİHM, iddiayı temelli görerek başvuruyu kabul edilebilir bulmuştur.[586]

Başvurucular, Avrupa Birliği hukukunun muhtelif düzenlemelerine, Avrupa Konseyi Bakanlar Komitesinin kararlarına ve BM Özel Raportörü'nün ifade özgürlüğüne ilişkin raporlarına atıf yapmıştır.[587] Başvurucular, iç hukuktaki düzenlemeler sebebiyle bu tür bir sorumluluğa muhatap olduklarını tartışmışlardır.[588]

Yorumların kamusal tartışmalara katkı sunduğunu ve paylaşımların ifade özgürlüğüyle korunduğunu iddia eden başvurucular, yorumların editoryal içeriklerle eş tutulmaması gerektiğini belirtmişlerdir.[589] Başvuruculara göre asıl mesele, iç hukuk uygulamalarındaki çelişkilerdir.[590]

Başvurucular, sorumluluktan kurtulmanın tek yolunun ya tüm yorumları bir ön denetime tabi tutmak veya yorumları toptan şekilde engellemek olduğunu belirtmişlerdir.[591] Üçüncü taraflara ait içerikler sebebiyle siteleri sorumluluk altına sokmanın, yorumların yayımlanmasını engelleyeceğini ve esaslı bir sansüre yol açacağını iddia etmişlerdir.[592] Bu sorumluluk rejiminin ölçüsüzlüğüne değinen başvurucular, uyar-kaldır yönteminin başkalarının şöhretini korumak için en uygun yöntem olduğunun altını çizmişlerdir.[593] Hukuki sorumluluğun ifade özgürlüğü üzerinde caydırıcı bir etki (*chilling effect*) doğuracağını hatırlatmışlardır.[594] Nihayetinde, editoryal sorumluluğun, diğer bir deyişle sıkı sorumluluk rejiminin dijital çağdaki sorunlara bir yanıt olmadığını tekrar etmişlerdir.[595]

---

[585] *MTE/Index.hu Zrt v. Macaristan*, para. 30.
[586] *MTE/Index.hu Zrt v. Macaristan*, para. 31.
[587] *MTE/Index.hu Zrt v. Macaristan*, para. 32.
[588] *MTE/Index.hu Zrt v. Macaristan*, para. 33.
[589] *MTE/Index.hu Zrt v. Macaristan*, para. 34.
[590] *MTE/Index.hu Zrt v. Macaristan*, para. 35.
[591] *MTE/Index.hu Zrt v. Macaristan*, para. 36.
[592] *MTE/Index.hu Zrt v. Macaristan*, para. 37.
[593] *MTE/Index.hu Zrt v. Macaristan*, para. 38.
[594] *MTE/Index.hu Zrt v. Macaristan*, para. 39.
[595] *MTE/Index.hu Zrt v. Macaristan*, para. 40.

IV. Macaristan Hükûmetinin savunması

Macaristan Hükûmeti, başvuruculaların genel olarak ifade özgürlüklerinin ihlal edildiğini kabul etmekle beraber, bunun kanunla öngörülen ve başkalarının haklarının korunması gibi meşru bir amaçla gerçekleşen bir eylem olduğunu belirtmiştir.[596] Hükûmet, başvuruculaların objektif sorumluluğu başkaları tarafından ifade edilen yorumları iletmekten kaynaklandığı için internet hizmet sağlayıcılarına tanınan sorumsuzluk istisnasının burada uygulanamayacağını ileri sürmüştür.[597]

Aynı doğrultuda, Hükûmet başvuruculaların kendi fikirlerini ve görüşlerini yayma haklarının zedelenmediğini iddia etmiştir.[598] Hükûmete göre, kontrolsüz yorumları internet sitelerinde yayımlayan kişilerin, bu yorumlar arasında hukuka aykırı olanların da bulunacağını ve medeni hukuk bağlamında bir sorumluluğun doğacağını öngörmesi gerekir.[599] Tüm bu tespitler ışığında Hükûmet, ihtilafın özünü ifade özgürlüğü ile başkalarının onuru ve haklarının korunması arasındaki dengenin teşkil ettiğini ve yorumların açıkça hukuka aykırı olması sebebiyle ölçüsüz bir müdahalenin bulunmadığını belirtmiştir.[600] Hükûmet, ölçülülüğün varlığının ispatı olarak Macaristan mahkemelerinin tazminata değil, sadece yargılama giderlerine hükmetmesini göstermiştir.[601]

V. AİHM'nin tespit ve değerlendirmeleri

A. Kanunla öngörülme açısından inceleme

AİHM, taraflar arasında başvuruculaların ifade özgürlüğünün ihlal edildiğine yönelik bir ihtilaf olmadığını ve bu tespite kendisinin de katıldığını belirtmiştir.[602] AİHM'ye göre asıl ihtilaf, başvuruculaların ifade

[596] *MTE/Index.hu Zrt v. Macaristan*, para. 41.
[597] *MTE/Index.hu Zrt v. Macaristan*, para. 42.
[598] *MTE/Index.hu Zrt v. Macaristan*, para. 43.
[599] *MTE/Index.hu Zrt v. Macaristan*, para. 43.
[600] *MTE/Index.hu Zrt v. Macaristan*, para. 44.
[601] *MTE/Index.hu Zrt v. Macaristan*, para. 44.
[602] *MTE/Index.hu Zrt v. Macaristan*, para. 45.

özgürlüğüne müdahalenin "kanunla öngörülme" şartını karşılayıp karşılamadığıdır.[603]

AİHM, tarafların iddiasına ve Macaristan mahkemelerinin tespitlerine değinmiş ve ardından kendi görevinin yerel mahkemelerin yerine geçmek veya bir taraf devletin kanun koyucusunun bir alanı düzenlerken kullandığı yöntemin yerindeliğini incelemek olmadığını vurgulamıştır.[604] AİHM, kendi görevinin, kabul edilen metotların ve bunların etkilerinin AİHS'ye uyumluluğunu incelemek olduğunu not etmiştir. Bu tespitleri yapan AİHM'ye göre, asıl incelenmesi gereken husus, Macaristan Yüksek Mahkemesinin (Kúria) Medeni Kanun'un ilgili hükümlerini uygulamasının AİHS'nin 10. maddesinin ikinci fıkrası bağlamında öngörülebilir olup olmadığıdır.[605]

AİHM'ye göre Macaristan Yüksek Mahkemesi, 108 sayılı Kanun'u yorumlarken AB e-Ticaret Direktifi'ni dikkate alıp almadığına ilişkin açıklama yapmamıştır.[606] Buna rağmen AİHM, Macaristan Medeni Kanunu'nun başvurucular için açık olduğuna ve başvurucuların üçüncü kişilerin hukuka aykırı yorumlarından sorumlu tutulmalarının kendileri için öngörülebilir olduğuna kanaat getirmiştir.[607] AİHM, Macaristan Hükûmetinin söz konusu müdahalenin başkalarının haklarını korumak gibi meşru bir amaçla yapıldığına yönelik görüşüne de katılmıştır.[608] Bu bağlamda, müdahalenin demokratik toplum düzeninin gerekliliklerine uygunluğunu incelemeye geçmiştir.

[603] *MTE/Index.hu Zrt v. Macaristan*, para. 47.
[604] *MTE/Index.hu Zrt v. Macaristan*, para. 47.
[605] *MTE/Index.hu Zrt v. Macaristan*, para. 49.
[606] *MTE/Index.hu Zrt v. Macaristan*, para. 50.
[607] *MTE/Index.hu Zrt v. Macaristan*, para. 51.
[608] *MTE/Index.hu Zrt v. Macaristan*, para. 52.

B. Demokratik toplum düzeninin gerekliliklerine uygunluk

AİHM, somut olayı incelemeden evvel demokratik toplum düzeninin gerekliliklerine ilişkin yerleşik içtihatlarını tekrarlamıştır.[609] Ardından, medyanın demokratik bir toplumda oynadığı temel fonksiyona vurgu yapmıştır.[610] Bu tespitlerden sonra internetin kamunun haberlere erişimini ve genel olarak bilginin yayılmasını kolaylaştırma fonksiyonunu öne çıkaran *Ahmet Yıldırım v. Türkiye* ile *Delfi AS v. Estonya* gibi kararlarına atıf yapmıştır.[611]

AİHM, şöhretin korunması hakkının AİHS'nin 8. maddesi bağlamında kişilerin özel hayatının gizliliğine saygının bir unsuru olduğunu hatırlatmıştır.[612] AİHM, demokratik bir toplumda başkalarının şöhretini ve haklarını korumak mülahazasıyla ifade özgürlüğüne müdahalenin gerekliliği incelenirken, yerel makamların çatışan hakları makul şekilde dengeleyip dengelemediğini incelemek gerektiğini belirtmiştir.[613] AİHM, ilke olarak, AİHS'nin 8 ve 10. maddelerinde yer alan haklara eşit şekilde muamele edilmesi ve yerel makamların bu tür durumlarda dengelemeyi nasıl gerçekleştirdiklerine dair güçlü gerekçeler ortaya koyması gerektiğini hatırlatmıştır.[614]

C. Genel tespitler ve uygulanabilir kriter

AİHM, tespitlerini somut olaya uygulama aşamasına geçtiğinde öncelikle Macar mahkemelerinin belirlemelerinin isabetli olup olmadığını incelemeye başlamıştır.[615] AİHM, Macar Anayasa Mahkemesinin başvu-

[609] *MTE/Index.hu Zrt v. Macaristan*, para. 54.
[610] *MTE/Index.hu Zrt v. Macaristan*, para. 55.
[611] *MTE/Index.hu Zrt v. Macaristan*, para. 56.
[612] *MTE/Index.hu Zrt v. Macaristan*, para. 57.
[613] *MTE/Index.hu Zrt v. Macaristan*, para. 58.
[614] *MTE/Index.hu Zrt v. Macaristan*, para. 59.
[615] *MTE/Index.hu Zrt v. Macaristan*, para. 60.

rucuların faaliyetinin basına uygulanan kurallar ışığında yorumlanması gerektiği tespitine katıldığını belirtmiştir.[616]

AİHM, öncelikle bu davanın *Delfi AS v. Estonya* davasıyla benzerliğini ve farklılığını ele almıştır. AİHM, internetin doğası gereği internet haber sitelerinin görev ve sorumluluklarının özellikle üçüncü taraflara ait içerikler sebebiyle klasik yayıncılarınkinden farklı olacağına ilişkin *Delfi AS v. Estonya* kararındaki çıkarımını tekrarlamıştır.[617] Ayrıca AİHM, söz konusu kararda, kullanıcılar tarafından yapılan yorumlara ekonomik amaçlarla platform sağlanması ve bu tür platformları kullananların açıkça hukuka aykırı ifadeler kullanarak nefret söylemi ve şiddete teşvik barındıran içerikler paylaşması durumunu incelediğini hatırlatmıştır.[618]

AİHM, iki gerekçeyle *MTE ve Index.hu Zrt v. Macaristan* davasının *Delfi AS v. Estonya* kararından farklı olduğunu ortaya koymuştur:[619] (1) Mevcut davada da hukuka aykırı yorumlar söz konusudur ancak bunlar nefret söylemi veya şiddete teşvik seviyesinde değildir, dolayısıyla *Delfi AS* kararından farklıdır. (2) Büyük bir medya şirketi olması hasebiyle ikinci başvurucunun (Index.hu) ekonomik menfaati var ise de internet hizmet sağlayıcılarının kâr amacı gütmeyen öz düzenleyici birliği niteliğinde olan ilk başvurucunun (MTE) bu tür bir ekonomik menfaati bulunmadığından *Delfi AS* kararından farklıdır.

AİHM, tüzel kişilerin AİHS bağlamında mağdur ve başvurucu olarak kabul edilip edilemeyeceği hususunu da değerlendirmiştir. AİHM, tüzel kişilerin, kişilik haklarının ihlali sebebiyle AİHS kapsamında mağdur olarak değerlendirilemeyeceğine dair önceki içtihadına atıf yapmıştır.[620] AİHM, ticari itibara ilişkin menfaatlerin manevi boyutunun olmadığına ilişkin içtihadını da hatırlatmıştır.[621] Buna rağmen, şirketlerin ticari başarılarını ve varlığını sürdürmesinde genel bir toplumsal menfaat

---

[616] *MTE/Index.hu Zrt v. Macaristan*, para. 61.

[617] *MTE/Index.hu Zrt v. Macaristan*, para. 62.

[618] *MTE/Index.hu Zrt v. Macaristan*, para. 63.

[619] *MTE/Index.hu Zrt v. Macaristan*, para. 64.

[620] **AİHM**, *Sdružení Jihočeské Matky v. Czech Republic*, Başvuru No: 19101/03, 10.07.2006.

[621] **AİHM**, *Uj v. Hungary*, Başvuru No: 23954/10, 19.07. 2011.

olduğunun altını çizmiştir.[622] Bu tespitlerinin ışığında AİHM, bu davanın başvurucu şirketin itibarının korunması hakkına yönelik olmadığını; yerel mahkeme kararlarını da esas alarak aslında hakaretamiz içeriklerin dolaylı olarak o şirketin arkasındaki gerçek kişilerin haklarına yönelik bir ihlal niteliğinde olduğunu belirtmiştir.[623] AİHM, tüzel kişilerin, menfaatlerinin korunmasına yönelik bir hakkı olduğuna ilişkin Macar mahkemelerinin tespitlerini yeterli görmüştür.

AİHM, AİHS'nin 10. maddesinde koruma altına alınan ifade özgürlüğü ve 8. maddesinde koruma altına alınan özel hayatın gizliliğine saygı hakları arasında denge kurulması için şu kriterleri geliştirmiştir:[624]

(1) Kamusal yararı ilgilendiren bir tartışmaya katkı
(2) Raporun konusu
(3) İlgili kişinin eski davranışları
(4) İçerik
(5) Yayının şekli ve sonuçları
(6) Gazeteciler veya yayıncılara verilen cezanın ağırlığı

AİHM'ye göre tüm bu kriterlerin somut olayda göz önünde bulundurulması gerekmektedir.

AİHM, internet haber sitelerinin sorumluluğunun tespitinde *Delfi AS v. Estonya* kararında geçen şu kriterlerin esas alınması gerektiğini hatırlatmıştır:[625]

(1) Yorumların bağlamı
(2) Başvurucu şirket tarafından hakaret içeren yorumların önlenmesi için uygulanan tedbirler
(3) Aracı platforma alternatif olarak gerçek yazarların sorumluluğu
(4) Başvurucu şirket aleyhine sürdürülen yerel yargılamaların neticeleri

---

[622] *MTE/Index.hu Zrt v. Macaristan*, para. 66.
[623] *MTE/Index.hu Zrt v. Macaristan*, para. 67.
[624] *MTE/Index.hu Zrt v. Macaristan*, para. 68.
[625] *MTE/Index.hu Zrt v. Macaristan*, para. 69.

AİHM, mevcut uyuşmazlıkta nefret söylemi içeriği olmasa da bu kriterlerin (*Delfi AS* kriterleri) mevcut uyuşmazlık için de uygulanması gerektiğine karar vermiştir.[626]

1. İhtilafa konu yorumların içerik ve bağlamı

AİHM, ihtilafa konu yorumların, tüketicileri ve internet kullanıcılarını alakadar eden bir konuya ilişkin ve kamusal menfaati ilgilendiren nitelikte bir tartışma kapsamında olduğunu belirtmiştir.[627] AİHM, başvurucular arasında (MTE ve Index.hu) bir ayrım yaparak MTE'nin durumunun, ticari faaliyet gösteren bir girişim olan ve platformunda birçok yorum yapılmasını sağlayan Index.hu şirketinden farklı olduğunu belirtmiş; her iki sitenin yöneticilerinin durumunun yerel mahkemeler tarafından gereğince etüt edilmemiş olmasını bir eksiklik olarak görmüştür.[628]

AİHM, yorumların niteliğini de dikkate alarak ifade özgürlüğü şemsiyesi altına girip girmeyeceğini müstakil olarak değerlendirmiştir.[629] Kolaylık, kapsam ve hız açısından internetin hakaret dolu içeriğin yayılmasında oynadığı rolü dışlamayan AİHM, bu bağlamda internet portallarındaki spesifik iletişim türlerinin dikkate alınması gerektiğini belirtmektedir.[630] AİHM, yorumlarda kullanılan ifadelerin, her ne kadar düşük seviyeli bir üyelik stiline bağlı olsa da, internet portalları arasında yaygın bir uygulama olduğuna, bunun da ifadelere atfedilecek etkiyi azalttığına hükmetmiştir.[631]

2. Yorumların asıl yazarlarının sorumluluğu

AİHM, yerel mahkemelerin, yorumları yazanların sorumluluğuna gidilip gidilemeyeceğini tartışmadığını; Macaristan Anayasa Mahkeme-

[626] *MTE/Index.hu Zrt v. Macaristan*, para. 70.
[627] *MTE/Index.hu Zrt v. Macaristan*, para. 72.
[628] *MTE/Index.hu Zrt v. Macaristan*, para. 73.
[629] *MTE/Index.hu Zrt v. Macaristan*, para. 74-76.
[630] *MTE/Index.hu Zrt v. Macaristan*, para. 77.
[631] *MTE/Index.hu Zrt v. Macaristan*, para. 77.

sinin bir varsayımdan hareketle mağdur tarafın böyle bir tazmin yoluna gidemeyeceğini belirttiğini; yerel mahkemelerin ayrıca yorum yazmak için kullanılan kayıt usulünü gereğince tartışmadığını belirtmiştir.[632] AİHM, *Delfi AS v. Estonya* kararına tekrar atıf yaparak, başvuruculların, üçüncü kişilerin yorum yaparak ifade özgürlüğünü icra edebilmeleri için platform sağlamış olmalarının özünde bir basın faaliyeti olduğunu hatırlatmıştır.[633]

AİHM, sorumluluk konusunda, basın hürriyeti ve özelde gazetecilik faaliyetine ilişkin önceki içtihatlarına atıf yaparak yerleşik içtihadı çerçevesinde bir değerlendirme yapmıştır. AİHM'ye göre, yerel mahkemelerin başvuruculların faaliyetini "hakaret içeren ifadelerin yayılması" olarak nitelendirmesi bir an için kabul edilse bile, başvuruculların sorumluluğunu şu yerleşik içtihatla bağdaştırmak mümkün değildir:[634] "*[B]ir gazetecinin bir röportajda başkası tarafından yapılan açıklamaların yayılmasına yardım etmesi nedeniyle cezalandırılması, basının kamunun yararına olan tartışmalara katkı sunmasına ciddi şekilde engel olacaktır ve gerçekten güçlü gerekçeler olmadığı sürece bu yola başvurulmamalıdır.*"

3. Başvurucular tarafından alınan tedbirler ve mağdur tarafın tutumu

AİHM, yerel mahkemelerin nihai karara varırken başvuruculların aldığı içeriğin kaldırılmasına yönelik tedbirleri bir kriter olarak dikkate almadığını hatta Budapeşte Temyiz Mahkemesinin içeriğin kaldırılmış olmasının sorumluluğun doğmasına etki etmeyeceğini belirttiğini hatırlatmıştır.[635] AİHM, başvurucular tarafından internet sitelerinde hakaret içeren yorumları önlemek adına uygulanan yorum sistemi, uyar-kaldır mekanizması, içerik kuralları, kısmi kontrol gibi tedbirlerin, başvurucunun veya yerel mahkemelerde onların aleyhine dava açan davacının tutumlarının Macar mahkemeleri tarafından değerlendirmeye alınma-

[632] *MTE/Index.hu Zrt v. Macaristan*, para. 78.
[633] *MTE/Index.hu Zrt v. Macaristan*, para. 79.
[634] *MTE/Index.hu Zrt v. Macaristan*, para. 79.
[635] *MTE/Index.hu Zrt v. Macaristan*, para. 80.

mış olmasını ve salt zararlı ve onur kırıcı yorumlara alan sağladığı için başvurucunun objektif sorumluluğuna gidilmesini eleştirmiştir.[636]

Hatırlatmak gerekirse, ilgili davacı herhangi bir şekilde uyar-kaldır mekanizmasını işletmemiş, doğrudan tazminat davası açmış ve başvurucular söz konusu yorumların davacının haklarını ihlal ettiğinden ancak davanın açılmasıyla haberdar olmuşlardır. Dolayısıyla, bu tutumun da değerlendirilmemiş olmasını AİHM'nin eksiklik olarak görmesi bütüncül bir değerlendirme açısından yerindedir.

4. Yorumların mağdur taraf üzerindeki sonuçları

AİHM, tüzel kişilerin itibar kaybı ve dolayısıyla kişilik haklarının ihlali durumunda tazminata hak kazanmalarına ilişkin içtihatlarını tekrarlamıştır.[637] AİHM, somut olayda emlak yönetim şirketlerinin iş yapış tarzı yüzünden hâlihazırda farklı incelemeler/soruşturmalar yürütüldüğünü, başvurucuların sitelerinde yer alan yorumların tüketiciler nezdinde ek ve önemli bir etki doğurucu nitelikte olmadığını, yerel mahkemelerin söz konusu yorumların ciddiyet düzeyini ve tüzel kişilerin ticari itibarına halel getirip getirmediğini ele almadığını belirtmiştir.[638]

5. Başvurucular üzerindeki neticeler

AİHM'nin incelediği son kriter ise yerel mahkeme kararlarının başvurucular üzerindeki neticeleridir. Başvurucular, sadece yargılama giderleri ile vekâlet ücreti ödemişler, herhangi bir manevi tazminat ödememişlerdir. AİHM, somut davada başvurucular aleyhine tazminata hükmedilmemiş olmasının neticeyi değiştirmeyeceğini, nihayetinde müstakbel taleplerde bu sorumluluk rejimi sebebiyle başvuruculara tazminat ödemek durumunda kalabileceklerini belirtmiştir.[639] Ancak, AİHM'ye göre asıl sorun tazminat ödeme veya tazminat riski değildir. Asıl sorun, sorumluluğun internet portallarının işleyişi üzerindeki genel

[636] *MTE/Index.hu Zrt v. Macaristan*, para. 81-83.
[637] *MTE/Index.hu Zrt v. Macaristan*, para. 84.
[638] *MTE/Index.hu Zrt v. Macaristan*, para. 85.
[639] *MTE/Index.hu Zrt v. Macaristan*, para. 86.

etkisidir.[640] AİHM'ye göre bu yaklaşım, nihayetinde tüm yorum alanlarının kapatılmasına yol açabileceği gibi, doğrudan veya dolaylı olarak internet ortamındaki özgürlüklere ket vurabilecektir.[641] AİHM, bu doğrultuda internet portallarının demokratik toplumda oynadığı önemli rolün altını tekrar çizmiştir.[642]

İnternet platformlarını özgür elektronik medyanın kahramanı olarak nitelendiren AİHM, Macar yerel mahkemelerinin, hukuki sorumluluğa ilişkin kararlarının internet özgürlükleri üzerindeki etkilerini gereğince değerlendirmemesini, tüm menfaatler ve haklar arasında denge kurmamasını ifade özgürlüğünün korunmasında bir eksiklik olarak nitelendirmiştir.[643]

D. Sonuç

AİHM'ye göre, Macar mahkemelerinin katı tutumu AİHM'nin içtihatlarıyla ortaya konulan yarışan hakları dengelemeye ilişkin kriterleri fiilen dışlayan sorumluluk yaklaşımını yansıtmaktadır.[644] AİHM, amacının davalı devletin iç hukukta bir alanı düzenlerken seçtiği yöntemin yerindeliğini incelemek olmadığını tekrarlamıştır.[645]

AİHM, *Delfi AS v. Estonya* kararına atıf yaparak, uyar-kaldır yönteminin hızlı dönüş yapmak için gerekli etkinlikte kullanıldığı birçok durumda hakları ve menfaatleri dengelemek adına uygun bir araç olduğunu belirtmiştir.[646] AİHM, bu yöntemin mevcut davada da ilgili şirketin ticari itibarını korumak için etkin bir yöntem olarak kullanılmasının önünde bir engel bulunmadığını ifade etmiştir.[647]

---

[640] *MTE/Index.hu Zrt v. Macaristan*, para. 86.
[641] *MTE/Index.hu Zrt v. Macaristan*, para. 86.
[642] *MTE/Index.hu Zrt v. Macaristan*, para. 87.
[643] *MTE/Index.hu Zrt v. Macaristan*, para. 88.
[644] *MTE/Index.hu Zrt v. Macaristan*, para. 89.
[645] *MTE/Index.hu Zrt v. Macaristan*, para. 90.
[646] *MTE/Index.hu Zrt v. Macaristan*, para. 91.
[647] *MTE/Index.hu Zrt v. Macaristan*, para. 91.

AİHM tekrar *Delfi AS v. Estonya* kararına dönerek, nefret söylemi veya başkalarının fiziksel bütünlüğüne yönelik tehditler söz konusu olduğunda üye devletlerin, mağdur veya üçüncü kişilerin talebi olmasa dahi içeriğin gecikmeksizin kaldırılmasına yönelik tedbirleri almayan internet haber portallarına sorumluluk yükleyebileceğini vurgulamıştır.[648] AİHM, mevcut davada bu tür bir söylemin olmadığına hükmetmiştir. Bu doğrultuda, AİHS'nin 10. maddesinde güvence altına alınan ifade özgürlüğünün ihlal edildiğine karar vermiştir.

VI. Yargıç Egidijus Kūris'in mutabık görüşü

AİHM yargıcı Egidijus Kūris, karara katılmakla beraber müstakil bir mutabık görüş yazmıştır. Yargıç Kūris, *MTE ve Index.hu Zrt v. Macaristan* kararının, *Delfi AS v. Estonya* kararında ortaya koyulan esasların uygulandığı ilk dava olduğunu belirtmiştir.[649] Mevcut davadaki içeriklerin, *Delfi AS v. Estonya* kararına konu olan içeriklerin aksine açıkça hukuka aykırılık taşımadığını belirten Yargıç Kūris, bu kararın nefret söylemini ele alan *Delfi AS* kararından farklı olduğunu belirtmiştir. Yargıç Kūris, bu doğrultuda, mevcut kararın *Delfi AS* kararındaki ilkelerden bir sapma niteliğinde olmadığını ifade etmiştir.[650]

Yargıç Kūris, internet platformlarının iş modellerine eleştirel yaklaşmaktadır. Yargıç, bu kararın, içeriklerine bakılmaksızın yorumların yayılmasından ekonomik fayda sağlayanlar başta olmak üzere internet platformları tarafından, sorunlu ifadelere karşı gerekli tedbirleri almaktan kaçınmak amacıyla kullanılmaması gerektiğini vurgulamaktadır.[651] Bir adım ileriye giderek, bu şekilde kullanılması durumunda, bu kararın her şey pahasına kârı amaçlayan internet iş modellerini aklama aracı olabileceğinin altını çizmektedir.[652] Bu durumda sorumluluğun kurumsal olarak AİHM'ye ait olacağını belirtmektedir.

---

[648] *MTE/Index.hu Zrt v. Macaristan*, para. 91.

[649] *MTE/Index.hu Zrt v. Macaristan*, Yargıç Kūris'in Mutabık Görüşü, para. 1.

[650] *MTE/Index.hu Zrt v. Macaristan*, Yargıç Kūris'in Mutabık Görüşü, para. 2.

[651] *MTE/Index.hu Zrt v. Macaristan*, Yargıç Kūris'in Mutabık Görüşü, para. 3.

[652] "tekrar!" vurgusu Yargıç Kūris'e aittir. Bkz. *MTE/Index.hu Zrt v. Macaristan*, Yargıç

Yargıç Kūris, bu kararın *Delfi AS* kararından sonraki ilk karar olduğunu ama son karar olmayacağını belirtmiştir.[653] *MTE ve Index.hu Zrt v. Macaristan* kararı, *Delfi AS* kararından bir nebze geri adım olarak görülse de bu davanın ince detaylar içeren müteakip davalar için bir kanıt oluşturacağını ifade etmiştir.

VII. Değerlendirme

AİHM, çatışan haklar arasında denge kurarken basın özgürlüğüne ilişkin yaklaşımını temel alarak *Delfi AS v. Estonya* kararına nispetle bir ölçüde farklı bir karar vermiştir. *Delfi v. Estonya* kararından farklı olarak nefret söylemi ve şiddete teşvik içeriğinin söz konusu olmaması, genel kaba ifadelerin yer alması sebebiyle bu kez AİHM farklı bir karara hükmetmiştir.[654] Lakin AİHM, *MTE ve Index.hu Zrt v. Macaristan* kararında da internet platformlarının sorumluluğunun çerçevesini ölçülü olarak çizmeyi başaramamıştır.

Delfi AS sonrası bu karar da birçok belirsizlik içermektedir ve internetin ulusal ve uluslararası yönetişimi bağlamında pek çok tartışmayı beraberinde getirmiştir. Her iki kararın ortak paydası ve sorumluluk tespitinde temel kriter, başvuruya konu yorumların içeriğinin ve atfedilen sorumluluğun internet sitesi üzerindeki caydırıcı etkisinin değerlendirilmesi gerekliliğidir.[655]

AİHM, ticari olarak faaliyette bulunmayı ve internet ortamında tartışma yapılmasına olanak tanımayı, tartışmaları kolaylaştıran bir altyapı sunmayı bir nevi mutlak sorumluluk doğuran faaliyet olarak görmektedir.

Kūris'in Mutabık Görüşü, para. 3.

653 *MTE/Index.hu Zrt v. Macaristan*, Yargıç Kūris'in Mutabık Görüşü, para. 4.

654 Nefret söylemi ile genel kaba veya incitici nitelikteki ifadelerin ayrıştırılması her zaman kolay değildir. Uygulamada bu ayrıma ilişkin ciddi sorunlar vardır. Bu kadar yorum farklılıklarının olduğu bir hususta tüm sorumluluğu platformlara yüklemenin yerindeliği ayrıca tartışılmalıdır. Bu konudaki tartışmalar için bkz. **McGonagle, Tarlach** (2020). "*Free Expression and Internet Intermediaries: The Changing Geometry of European Regulation*": Frosio, Giancarlo (Editör) *Oxford Handbook of Online Intermediary Liability*, Oxford, Oxford University Press, s. 474.

655 **Köksal**, s. 112.

Karar, gerekli koruma mekanizmalarına ilişkin kriterleri net olarak ortaya koymadığı ve *Delfi AS* kararının muğlaklıklarını ortadan kaldırmadığı için dijital demokrasi bakımından da endişe verici bir karardır. Ayrıca, vatandaş gazeteciliği açısından da platformların sansür yapmasına, sosyal teknikleri kullanmasına davetiye çıkarmaktadır.

AİHM, Macar yerel mahkemelerini eleştirmektedir ancak hem *Delfi AS* hem de *MTE ve Index.hu ZRT v. Macaristan* kararında kendisi de tutarlı bir kriter geliştirememiş, konuya tüm boyutlarıyla bakamamıştır. AİHM'nin kararı, Macar yerel mahkemelerinin kararından metodolojik olarak pek de farklı değildir.

AİHM'ye göre, incelenen kararın *Delfi AS v. Estonya* kararından farkı, *Delfi AS* kararında ticari amaçla yürütülen bir faaliyet ve nefret söylemi ile şiddete teşvik içeren yorumlar bulunmasıdır. Nefret söylemini veya şiddete teşvik eden içeriği tespit etmek kolay mıdır? İnternetin teknik işleyişini içselleştirmeden tüm internet ekosistemini ters yüz edecek bir karar vermek ne kadar makuldür? Bu kararların tüm Web 2.0 platformlarına uygulanmayacağının garantisi nedir?

AİHM, internet gibi karmaşık bir sistem karşısında kendi teknik kapasitesini ileriye taşıyarak derinlemesine bir inceleme yapmak yerine sorunu sadeleştirmeye ve hâliyle detayları yok saymaya çalışmaktadır. Sorunun tüm boyutlarını yansıtamayacak kısıtlı bir çözüm sunmaktadır. Bu da hakkaniyetli bir yaklaşım değildir. Disiplinler arası bakış gerektiren, hukuk, yönetişim ve tekniğin iç içe geçtiği bir alana klasik kurallarla yükümlülükler getirmek ve kısıtlamalar koymak ne kadar makuldür?

AİHM, internetin genel bir kamusal bilgiye erişim ve iletişim aracı hâline gelmediği dönemde kurulmuş bir yargı organıdır. AİHM, gelişen teknoloji karşısında kendisini yenilemeyi başaramamıştır. *Delfi AS v. Estonya* ile *MTE ve Index.hu Zrt v. Macaristan* kararları bunun en bariz örnekleridir. AİHM, klasik medya rejimi ile ilgili vermiş olduğu kararlardan kıyas yaparak internet ortamında hakların dengelenmesine çalışmaktadır. Lakin bu metodoloji internete katkı sunan değil, yenilikçi modellere ket vuran bir metodolojidir.

AİHM, bizzat kendisi kurumsal olarak ifade özgürlüğünün kısıtlanmasına dolaylı olarak yeşil ışık yakmıştır. Dördüncü bölümde etraflıca incelenen sosyal tekniklerin kullanımına, otosansüre, platformların sorumluluk altına girmemek adına sakıncalı görebilecekleri tüm içerikleri, yorumları sansürlemesine, diğer bir deyişle platform sansürüne (*private censorship*) zemin hazırlamaktadır.

§14. JANKOVSKİS V. LİTVANYA

AİHM'nin *Jankovskis v. Litvanya*[656] kararı, *Kalda v. Estonya* kararına benzer şekilde hapishane gibi belirli bir alanda internet içeriğine erişim hakkıyla ilgilidir. Karar, Henrikas Jankovskis isimli Litvanyalı bir mahkûmun, eğitim bilgileri içeren bir internet sitesine erişiminin kısıtlanması sebebiyle AİHS'nin 10. maddesinde yer alan ifade özgürlüğünün ihlal edildiği iddiasını konu almaktadır.

I. Davanın gelişimi

Bay Jankovskis, Pravieniškės Islahevinde (*Correctional Home*) hapis cezasını çekmektedir. 1996 yılında Vilnius Üniversitesi Tıp Fakültesinden mezun olmuştur. 30 Mayıs 2006 tarihinde Litvanya Eğitim ve Bilim Bakanlığına başvurarak, insan hakları hukuku alanında uzmanlaşmak amacıyla uzaktan eğitim yöntemiyle ikinci bir üniversite okuma talebinde bulunmuştur.[657]

Litvanya Eğitim ve Bilim Bakanlığı, 12 Haziran 2006 tarihinde göndermiş olduğu yanıtta, eğitim programlarıyla ilgili bilginin Bakanlığa ait olan ve bir kamu kurumu tarafından işletilen www.aikos.smm.lt isimli siteden bulunabileceğini belirtmiştir.[658] Bay Jankovskis, Pravieniškės Islahevi idaresine başvurarak www.aikos.smm.lt sitesi ile kişisel e-postalarının barındırıldığı www.one.lt ile www.yahoo.com sitelerine erişim sağlanmasını talep etmiştir.[659] Talebi inceleyen Islahevi İdaresi, Eğitim ve Bilim Bakanlığının başvurucunun mahkûm olduğu hususunu dikkate almadığını belirtmiş ve bilgilendirmeyi yeterli görmemiştir.[660]

---

[656] **AİHM**, *Jankovskis v. Litvanya*, B. No. 21575/08, 17.4.2017.

[657] *Jankovskis v. Litvanya*, para. 6.

[658] *Jankovskis v. Litvanya*, para. 7.

[659] *Jankovskis v. Litvanya*, para. 8.

[660] *Jankovskis v. Litvanya*, para. 9.

Islahevi İdaresi, mahkûmlara internet kullanma veya bir e-posta kutusuna erişim hakkı tanıyan yasal bir düzenleme olmadığı için Bay Jankovskis'in talebini reddetmiştir.[661] Bunun üzerine Bay Jankovskis, Litvanya Eğitim ve Bilim Bakanlığının yanıtını gerekçe göstererek bu karara karşı bir üst idari makam niteliğindeki Cezaevleri Otoritesine itiraz başvurusunda bulunmuştur.[662]

İtirazı inceleyen Cezaevleri Otoritesi, 26 Temmuz 2006 tarihinde, hükmün infazının mahkûmlara internete erişimi sağlanmasına izin vermediğini belirterek itirazı reddetmiştir.[663] Bay Jankovskis, 1 Ağustos 2006 tarihinde bu kararın iptali için yargı sürecini başlatmıştır.[664]

Pravieniškės Islahevi İdaresi, ilgili yasal mevzuat uyarınca mahkûmların sadece geleneksel posta hizmetinden yararlanabileceğini, e-posta kullanmalarına izin verilmediğini belirtmiştir.[665] Ayrıca, mahkûmların internete erişmeleri durumunda güvenlik açısından sorunlar ortaya çıkacağı, mahkûmların suça konu faaliyetlerini hapishanede de sürdürebileceği, hapishanede yasa dışı şekilde cep telefonu kullanımı yoluyla bile birçok ihlalin gerçekleştiği ifade edilmiştir.

Cezaevleri Otoritesi de başvurunun reddedilmesi gerektiğini, Ceza İnfaz Kanunu'nun 96. maddesinin mahkûmlara belirli koşullarda bilgisayar kullanma imkânı tanısa da internete erişim olanağı tanımadığını belirtmiştir.[666] Ayrıca, Litvanya hukukunda mahkûmlara internet erişimi sağlanmasına olanak tanıyan bir hukuki düzenleme bulunmadığını tekrarlamıştır.

İtirazları inceleyen Kaunas Bölge İdare Mahkemesi, 2 Şubat 2007 tarihinde Bay Jankovskis'in talebini reddetmiştir.[667] Mahkeme, mahkûmların idareyle sadece posta yoluyla iletişime geçebileceğini, telefon ve

[661] *Jankovskis v. Litvanya*, para. 10.
[662] *Jankovskis v. Litvanya*, para. 11.
[663] *Jankovskis v. Litvanya*, para. 12.
[664] *Jankovskis v. Litvanya*, para. 13.
[665] *Jankovskis v. Litvanya*, para. 14.
[666] *Jankovskis v. Litvanya*, para. 15.
[667] *Jankovskis v. Litvanya*, para. 16.

radyo gibi iletişim araçlarına yönelik yasağın interneti de kapsadığını, bu yasağın amacının hapishanelerde suç işlenmesinin önlenmesi olduğunu kararına gerekçe olarak göstermiştir.

Bay Jankovskis, Kaunas Bölge İdare Mahkemesinin kararını temyiz etmiştir. İtiraz gerekçesi olarak, ilk derece mahkemesinin ilgili kanunu hatalı yorumladığını ileri sürmüştür.[668] Bay Jankovskis, başvurusunun temelinin eğitim hakkının ve bilgiye erişim hakkının kısıtlanmasına dayandığı görüşündedir. Bu bağlamda, Litvanya Anayasası'nın 25. maddesi ile AİHS'nin 10 ve 14. maddelerine atıf yapmıştır. Pravieniškės Islahevi İdaresi, hapishanede bir okul ve ayrıca mahkûmların da katılmasının mümkün olduğu bilgisayar okuryazarlığı alanında eğitim veren bir meslek yüksekokulu (*Elektrėnai Vocational Educational Centre*) bulunduğunu, bu eğitim olanaklarından yararlanmak için internet erişimine gerek olmadığını belirtmiştir.[669]

Temyiz talebini inceleyen Yüksek İdare Mahkemesi, 11 Aralık 2007 tarihli kararıyla Bay Jankovskis'in talebini reddetmiştir.[670] Yüksek İdare Mahkemesi de ilk derece idare mahkemesiyle benzer gerekçelere dayanmıştır. Yüksek İdare Mahkemesine göre, internetin, eğitim amacı dışında farklı amaçlarla kullanılması mümkündür; internete erişim hakkı mutlak bir hak değildir ve belirli sosyal gruplar için bu hak kısıtlanabilir; mahkûmlara internete erişim hakkı sağlanması durumunda suçla mücadele alanında hapishane idareleri büyük güçlükler yaşayacak ve mahkûmların faaliyetlerini tam olarak takip edemeyecektir.

Tüm bu süreçler devam ederken Bay Jankovskis, 30 Haziran 2006 tarihinde Elektrėnai Meslek Yüksekokulundaki bilgisayar okuryazarlığı programından diplomasını almıştır.[671] Litvanya Hükûmetinin verdiği bilgiye göre, Bay Jankovskis ayrıca 2007-2008 yılları arasında Kaunas bölgesindeki bir orta dereceli okul tarafından düzenlenen İngilizce dil

[668] *Jankovskis v. Litvanya*, para. 17.
[669] *Jankovskis v. Litvanya*, para. 18.
[670] *Jankovskis v. Litvanya*, para. 19.
[671] *Jankovskis v. Litvanya*, para. 20.

kursu ile bilgisayar okuryazarlığı kursunu da tamamlamıştır.[672] Bay Jankovskis'in çeşitli dönemlerde, mahkûmiyet koşullarının kötülüğüne ve keyfî disiplin yaptırımlarına karşı muhtelif şikâyetleri de olmuştur.[673]

II. Hukuki arka plan

AİHM, yerel hukuki düzenlemelerden Litvanya Anayasası'nın ifade özgürlüğünü düzenleyen 25. maddesini[674], 1 Haziran 2006 tarihi ile 28 Şubat 2010 tarihleri arasında yürürlükte olan Ceza İnfaz Kanunu[675] ile Eğitim Kanunu'nun[676] ilgili hükümlerini alıntılamıştır. Uluslararası hukuk bağlamında ise Avrupa İşkenceyi ve İnsanlık Dışı veya Aşağılayıcı Muamele ve Cezayı Önleme Komitesinin 13 Aralık 1992 tarihinde yayımlanan İkinci Genel Rapor'una (CPT/Inf (92) 3 [EN]) atıf yapmıştır.[677] AİHM ayrıca *Kalda v. Estonya* kararında alıntıladığı Avrupa Konseyi ve diğer uluslararası hukuk belgelerine de çapraz atıf yapmıştır.[678]

III. Tarafların iddiaları

Bay Jankovskis'in temel iddiası, eğitim hakkı ve ifade özgürlüğünün kısıtlandığıdır.[679] Bay Jankovskis, Ceza İnfaz Kanunu'nun 1. Ek'inin altıncı kısmında yer alan ve hapishanede bulundurulamayacak telefon ve diğer iletişim araçlarını (radyo vb.) sayan hükmün belirsiz olduğunu, internete erişime ilişkin bir yasaklamanın kanunda öngörülmediğini ileri sürmüştür.[680] Söz konusu kısıtlamanın suçu önleme amacıyla bağlantılı olmadığını belirtmiştir.[681]

---

[672] *Jankovskis v. Litvanya*, para. 21.
[673] *Jankovskis v. Litvanya*, para. 22-27.
[674] *Jankovskis v. Litvanya*, para. 28.
[675] *Jankovskis v. Litvanya*, para. 29.
[676] *Jankovskis v. Litvanya*, para. 34.
[677] *Jankovskis v. Litvanya*, para. 35.
[678] *Jankovskis v. Litvanya*, para. 36.
[679] *Jankovskis v. Litvanya*, para. 37.
[680] *Jankovskis v. Litvanya*, para. 38.
[681] *Jankovskis v. Litvanya*, para. 39.

Bay Jankovskis, yasaklamanın ölçüsüz olduğunu da ileri sürmüştür.[682] Bay Jankovskis'e göre, eğitim programlarıyla ilgili web sitesini bizzat Eğitim ve Bilim Bakanlığı önermiştir. Bay Jankovskis, eğitimle ilgili en güncel bilginin internet ortamında yer aldığını ve çalışmaları için gerekli bilgiyi internet ortamı dışında temin etmesinin mümkün olmadığını belirtmiştir. İddiasını, başka ülkelerin, internet erişimine izin veren uygulamalarıyla desteklemiştir.

IV. Litvanya Hükûmetinin savunması

Litvanya Hükûmeti, iç hukuk yollarının tüketilmediğini ileri sürmüştür.[683] Ayrıca, Bay Jankovskis'in Litvanya'da bulunan diğer eğitim kurumlarına eğitim amacıyla bir başvuru yapmadığını da belirtmiştir. Hükûmet, alternatif yolların varlığı sebebiyle bu başvurunun temelsiz olduğunu tartışmıştır.[684] Bunun yanı sıra, hâlihazırda almış olduğu eğitimleri dayanak gösteren Litvanya Hükûmeti, Bay Jankovskis'in dezavantajlı bir konuma gelmediğini iddia etmiştir.[685] Ayrıca, AİHS'nin 10. maddesinin mahkûmlara internet erişimi sağlanması konusunda devlete pozitif bir yükümlülük getirmediğine dair bir AİHM içtihadına da atıf yapmıştır.

Litvanya Hükûmeti, AİHM başvurucunun bilgiye erişim hakkının kısıtlandığına dair bir tespit yapsa dahi bu müdahalenin hukuki bir dayanağı olduğu görüşündedir.[686] Zira 2010 yılında yapılan açık bir kanuni değişiklikle mahkûmların her türlü elektronik araçla iletişimi yasaklanmıştır. Litvanya Hükûmeti, yasağın amacının, telefon dolandırıcılığı gibi suçları ve ceza yargılamasında kişilerin etkilenmesini önlemek olduğunu tekrarlamıştır.[687]

---

[682] *Jankovskis v. Litvanya*, para. 40.
[683] *Jankovskis v. Litvanya*, para. 41.
[684] *Jankovskis v. Litvanya*, para. 42.
[685] *Jankovskis v. Litvanya*, para. 43.
[686] *Jankovskis v. Litvanya*, para. 44.
[687] *Jankovskis v. Litvanya*, para. 44.

Hükûmet, müdahalenin gerekli ve ölçülü olduğu görüşündedir.[688] Hükûmete göre, mahkûmlara internet erişimi sağlanması, başkalarının haklarına bir tehdit oluşturabilecek ve hukuka aykırılıkları önlemek için ciddi bir maliyet ortaya çıkacaktır. Dahası Litvanya Hükûmeti, Bay Jankovskis'in talep ettiği belgelerin, yakınları tarafından çıktı alınarak temin edilebileceği görüşündedir. Hükûmet, eğitim hakkına müdahale etmediği yönündeki iddialarını, mahkûmlara sunulan eğitim programlarıyla desteklemiştir.

Son olarak Litvanya Hükûmeti, Bay Jankovskis'in sadece ilgili eğitim sitesine değil, internete genel bir erişim talep ettiğini, ayrıca e-postalarına erişmek istediğini, bunlara yönelik kısıtlamaların ise mahkûmların yazışmalarının sınırlanmasına ilişkin AİHM içtihatlarıyla uyumlu olduğunu belirtmiştir.[689] Litvanya Hükûmeti, ayrıca Avrupa Konseyine üye birçok devletin mahkûmların internete erişimini kısıtladığını belirtmiştir.[690]

V. AİHM'nin tespit ve değerlendirmeleri

İnternete eğitim amaçlı erişimin kısıtlanmasını dikkate alan ve ayrıca birçok hizmetin artık sadece dijital ortamda sunuluyor olmasına ilişkin *Kalda v. Estonya* kararındaki tespitlerine atıf yapan AİHM, başvuruyu kabul edilebilir görmüş ve esastan incelemiştir.[691]

AİHM, toplumun genel olarak bilgiye erişmekte menfaati olduğunu belirtmiştir. Ancak, somut olaydaki ihtilaf, bir devletin bilgiyi kamuyla paylaşmasından ziyade, başvurucu gibi özel statülü bir kişinin yani mahkûmun Eğitim ve Bilim Bakanlığına ait bir internet sitesine erişmesine ilişkindir.[692] *Delfi AS v. Estonya*, *Ahmet Yıldırım v. Türkiye* gibi kararlarına atıf yapan AİHM, internetin, genel olarak bilginin yayılması ve kamunun bilgiye erişmesindeki rolünün önemini hatırlatmıştır.[693]

---

[688] *Jankovskis v. Litvanya*, para. 46.
[689] *Jankovskis v. Litvanya*, para. 47.
[690] *Jankovskis v. Litvanya*, para. 48.
[691] *Jankovskis v. Litvanya*, para. 49.
[692] *Jankovskis v. Litvanya*, para. 52-53.
[693] *Jankovskis v. Litvanya*, para. 54.

AİHM, mahkûmiyetin genel olarak belirli haklardan yoksunluğa yol açtığının farkındadır. Ayrıca, *Kalda v. Estonya* kararına tekrar atıf yaparak AİHS'nin 10. maddesinin mahkûmlara genel bir internete erişim hakkı tanıdığı şeklinde yorumlanmaması gerektiğini belirtmiştir.[694] Bu tespitlere rağmen, Litvanya hukukunda eğitime erişim hakkı tanındığı için mevcut kısıtlamanın bu hakka ve genel olarak bilgiye erişim hakkına bir müdahale niteliği taşıyıp taşımadığının incelenmesi gerektiğine karar vermiştir.[695]

A. Kanunla öngörülme açısından inceleme

AİHM, başvurunun yapıldığı 2006 yılında, internet erişimine ilişkin açık bir kısıtlama olmadığını, "diğer yöntemlerle iletişim" şeklindeki kısıtlamanın 2010 yılında getirildiğini belirtmiştir.[696] Bununla birlikte AİHM, makul bir şekilde yorumlandığında radyo ve elektronik haberleşme araçlarına yönelik kısıtlamanın internete erişim kısıtlamasını da içerdiği görüşündedir. Bu doğrultuda, mahkûmlara uygulanan internete erişim kısıtlamasının kanunla öngörülme şartını karşıladığına karar vermiştir.[697]

B. Müdahalenin meşru amaç için gerçekleştirilip gerçekleştirilmediği

AİHM, Litvanya Hükûmetinin bu kısıtlamayı getirme amacını dayandırdığı başkalarının haklarını koruma, suç işlenmesini ve düzeni bozabilecek davranışları önleme gerekçelerine katılmıştır.[698]

C. Demokratik toplum düzeninin gerekliliklerine uygunluk

Kanunla öngörülme ve meşru amaç kriterlerini inceledikten sonra AİHM, müdahalenin demokratik toplum düzeninin gerekliliklerine

[694] *Jankovskis v. Litvanya*, para. 55.
[695] *Jankovskis v. Litvanya*, para. 55.
[696] *Jankovskis v. Litvanya*, para. 57.
[697] *Jankovskis v. Litvanya*, para. 57.
[698] *Jankovskis v. Litvanya*, para. 58.

uygun olup olmadığını değerlendirmeye almıştır. Bu aşamada, öncelikle Bay Jankovskis'in erişmeye çalıştığı internet sitelerinin niteliklerini ele almıştır. AİHM, erişim talebinin esasının eğitim alma, infaz süresince rehabilitasyon ve sonrasında topluma tekrar entegre olma amacı taşıdığını tespit etmiştir.[699] AİHM, ayrıca ilgili siteye erişerek doğrudan inceleme yapmanın spesifik bir bilgiye yönelik tek tek talepte bulunmaktan daha etkili bir yöntem olduğunu belirtmiştir.[700] Mahkeme, ayrıca bu alandaki bilgilerin sıklıkla güncellenmesi sebebiyle internet sitesine erişmenin önemli olduğunu dikkate almıştır.[701]

Yukarıda ifade edildiği üzere, Pravieniškės Islahevinde hem bir orta dereceli okul hem de bir meslek yüksekokulu vardır. AİHM, başvurucu ikinci bir üniversite derecesi almak amacını taşıdığından bu imkânların bir alternatif olarak değerlendirilemeyeceğine kanaat getirmiştir.[702]

AİHM, yerel otoritelerin ve mahkemelerin, mahkûmlara internet erişimi sunulmasının oluşturacağı ilave maliyetleri gereğince ele almadığı düşüncesindedir.[703] En önemlisi, başvurucunun erişim talep ettiği sitenin Litvanya Eğitim ve Bilim Bakanlığına yani bir kamu otoritesine ait olduğu yok sayılmış, bu konuda sessiz kalınmıştır.[704]

Kalda v. Estonya kararına tekrar atıf yapan AİHM, internetin "dijital uçurumu" ortadan kaldırmak için toplumda oynadığı rolü hatırlatmıştır.[705] Bay Jankovskis'in erişmek istediği AIKOS'un kamu otoriteleri tarafından sunulan ve güvenlik riski oluşturması zor bir site olduğunun Litvanya makamları tarafından dikkate alınmamasını AİHM bir eksiklik olarak nitelendirmiştir.[706]

---

[699] *Jankovskis v. Litvanya*, para. 59.
[700] *Jankovskis v. Litvanya*, para. 60.
[701] *Jankovskis v. Litvanya*, para. 60.
[702] *Jankovskis v. Litvanya*, para. 61.
[703] *Jankovskis v. Litvanya*, para. 61.
[704] *Jankovskis v. Litvanya*, para. 61.
[705] *Jankovskis v. Litvanya*, para. 62.
[706] *Jankovskis v. Litvanya*, para. 62.

Tüm bu gerekçelerle AİHM, mevcut davada başvurucunun bilgiye erişim hakkının kısıtlanmasına ilişkin makul gerekçeler ortaya koyulmadığına kanaat getirmiş ve bu kısıtlamanın demokratik toplum gerekliliklerine uymadığına karar vermiştir.[707] Bu doğrultuda, AİHS'nin 10. maddesinin ihlal edildiğine hükmetmiştir.

VI. Değerlendirme

Kalda v. Estonya kararına ilişkin değerlendirmeler, bu karar için de aynen geçerlidir. AİHM'nin, *Jankovskis v. Litvanya* kararında da internetin niteliğini gereğince ele aldığını ve isabetli bir değerlendirme yaptığını söylemek pek mümkün değildir. Bunun temelinde AİHM'nin, vermiş olduğu kararların neticelerinin etki analizini yapmaması ve interneti tek taraflı ele alması yatmaktadır.

Yargıç Kjølbro'nun *Kalda v. Estonya* kararına ilişkin muhalif görüşünde isabetle vurgulandığı üzere hapishane gibi özel bir alanda, tutuklular gibi özel statülü bireylerin bilgiye erişim hakları incelenirken madalyonun diğer yüzü yani güvenlik riskleri dikkate alınmalı ve devletlere aşırı bir külfet yüklenerek mağdurların hakları, güvenlikleri, hapishane güvenliği, suç işlenmesinin önlenmesi (ki hepsi meşru taleplerdir) riskleri yok sayılmamalıdır.

AİHM, AIKOS sitesi kamu tarafından işletilen bir site olduğu için bu siteye erişim sağlanmamasını demokratik toplum düzeninin gerekliliklerine aykırı görmüştür. Bir internet sitesinin kamu tarafından işletilmesi, güvenlikle ilgili tüm risklerin bertaraf edildiği manasına gelmemektedir. Beşinci bölümde etraflıca incelendiği üzere, içerik engelleme sistemleri bazen bir çeviri sitesi gibi veya çoğu zaman tarayıcılara gömülü olarak gelen eklentilerle çok kolay şekilde aşılabilir. Burada ortaya çıkan teknik denetim ve kontrol sorunlarını ve olası bir ihlalin ortaya çıkaracağı güvenlik risklerini yok saymak, makul bir yaklaşım değildir.

AİHM, internete erişimin kısıtlanması için kanunda öngörülme ve meşru amaç kriterlerinin sağlandığını belirtmiş fakat kısıtlamayı demok-

[707] *Jankovskis v. Litvanya*, para. 63.

ratik toplum düzeninin gerekliliklerine aykırı görmüştür. Ancak AİHM, demokratik toplum düzeninin gerekliliklerini incelerken bu alandaki mukayeseli hukuku ele almamış, uluslararası ortak paydayı gereğince ortaya koymamıştır. *Kalda v. Estonya* kararındaki eksik yorum tekrarlanmıştır.

Öte yandan, hapishane gibi özel alanlarda internete erişimi kısıtlamanın başkalarının hak ve menfaatlerini korumak gibi meşru bir amacı vardır. Bu tür alanlarda, mahkûmların rehabilitasyonu ve topluma tekrar kazandırılması gibi amaçlarla özel "intranet" sistemlerinin kurulması durumunda şüphesiz farklı yorum yapılacaktır.

§15. ROLF ANDERS DANİEL PİHL V. İSVEÇ

AİHM'nin *Rolf Anders Daniel Pihl v. İsveç*[708] kararı, internet içeriğinden sorumluluğun ele alındığı bir karardır. Mahkemenin, *Delfi AS v. Estonya* ile *MTE ve Index.hu Zrt v. Macaristan* kararlarının ardından vermiş olduğu, sorumluluk hukuku bağlamında önemli bir karardır. Başvurunun temelini, bir blog sitesindeki kullanıcı yorumlarından blog sitesini işleten tarafın hukuken sorumlu tutulmamasının, AİHS'nin 8. maddesinde güvence altına alınan özel hayata saygı hakkını ihlal ettiği iddiası oluşturmaktadır.

I. Davanın gelişimi

Başvurucu Rolf Anders Daniel Pihl, İsveç vatandaşıdır. 29 Eylül 2011 tarihinde bir blog sayfasında kendisini Nazilerle ilişkilendiren bir içerik yayımlanmıştır. Blog sayfasında, ön onay mekanizması işletilmeyen bir yorum sekmesi bulunmaktadır. Ön onay mekanizması olmadığı için, yorum yapan kişilerden düzgün hareket etmeleri ve hukuk kurallarına uymaları beklenmektedir.[709]

Bay Pihl ile ilgili içerik yayımlandıktan sonra, aynı içeriğin altında, Bay Pihl'in kişilik haklarına saldırı niteliğinde bir yorum paylaşılmıştır.[710] 8 Ekim 2011 tarihinde Bay Pihl, ilgili blog içeriğinin ve yapılan yorumun altına, söz konusu içeriğin yanlış olduğunu belirten ve kaldırılmasını talep eden bir yorum yazmıştır.[711] Akabinde, söz konusu içerik blog sayfasının yöneticisi tarafından kaldırılmış; yeni bir sayfada, Bay Pihl ile ilgili o içeriğin doğru olmayan bilgiler ihtiva ettiği belirtilmiş ve hatadan dolayı özür dilenmiştir.[712] Bay Pihl, kaldırılmasına rağmen söz konu içeriğin in-

---

[708] **AİHM**, *Rolf Anders Daniel PIHL v. İsveç*, Başvuru No: 74742/14, 7.2.2017.

[709] *Rolf Anders Daniel PIHL v. İsveç*, para. 3.

[710] *Rolf Anders Daniel PIHL v. İsveç*, para. 4.

[711] *Rolf Anders Daniel PIHL v. İsveç*, para. 5.

[712] *Rolf Anders Daniel PIHL v. İsveç*, para. 6.

ternet ortamında ve arama motorlarında yer almaya devam ettiğini ileri sürmüş ve blog sitesini işleten kâr amacı gütmeyen birliğin söz konusu içeriği ve yorumu derhâl kaldırmaması sebebiyle bu durumu tazminat davasına konu etmiştir.[713]

İç hukuktaki çeşitli usuli aşamaların, temyiz ve itirazların ardından talepleri reddedilen[714] Bay Pihl, blog sitesini işleten birliğin içerikten dolayı sorumlu tutulmaması sebebiyle haklarının ihlal edildiğini ve bu durumun devletin AİHS'nin 8. maddesinde yer alan pozitif yükümlülüklerinin ihlali niteliğinde olduğunu öne sürerek Adalet Şansölyesi'ne başvurmuştur.[715]

Talebi inceleyen Adalet Şansölyesi, AİHM'nin *Delfi AS v. Estonya* gibi içtihatlarını da dikkate alarak AİHS'nin 8 ve 10. maddeleri arasında bir denge gözetilmesi gerektiğini, bu konuda devletlerin bir takdir alanı olduğunu belirtmiş ve mevcut ihtilafta Bay Pihl'in AİHS'nin 8. maddesi altında korunan haklarının ihlal edilmediğine karar vermiştir.[716]

II. Hukuki arka plan

Hakaret, İsveç Ceza Kanunu'nun 5. Bölümü'nün 1. Kısmı'nda suç olarak düzenlenmiştir.[717] Elektronik Bültenlerin Sorumluluğu Hakkında Kanun'un (*Act on Responsibility for Electronic Bulletin Boards)* 5. maddesi de bloglar dâhil internet ortamında forum sayfası gibi faaliyet gösteren hizmet sağlayıcılara bazı içerikleri derhâl kaldırma yükümlülüğü getirmektedir.[718] Bu Kanun, bazı katalog suçlar (çocuk pornografisinden telif ihlallerine) belirleyerek bunların internet ortamından kaldırılması için özel bir usul öngörmektedir. Yasa, bu alanda faaliyet gösteren hizmet sağlayıcılara platformlarını denetleme konusunda aktif bir yükümlülük

[713] *Rolf Anders Daniel PIHL v. İsveç*, para. 7.
[714] *Rolf Anders Daniel PIHL v. İsveç*, para. 8-14.
[715] *Rolf Anders Daniel PIHL v. İsveç*, para. 15.
[716] *Rolf Anders Daniel PIHL v. İsveç*, para. 16.
[717] *Rolf Anders Daniel PIHL v. İsveç*, para. 17.
[718] *Rolf Anders Daniel PIHL v. İsveç*, para. 18-19.

getirmektedir.[719] Önemle belirtmek gerekir ki hakaret suçu bu içerikler arasında yer almamaktadır.

III. AİHM'nin tespit ve değerlendirmeleri

Başvurucu, blog sitesini işleten birliği hakaret nitelikli içerikten sorumlu tutmasına İsveç hukukunun izin vermemesi sebebiyle AİHS'nin 8. maddesiyle korunan özel hayata saygı hakkının ihlal edildiğini ileri sürmüştür.[720]

Başvuruyu ele alan AİHM, öncelikle AİHS'nin 8. maddesi bağlamında özel hayatın tanımına ilişkin muhtelif içtihatlarına atıf yapmıştır. *MTE ve Index.hu Zrt v. Macaristan* kararında yapmış olduğu bir kişinin itibarının korunması hakkının 8. maddede düzenlenen özel hayatın korunması hakkı kapsamında olduğuna ilişkin tespitini tekrarlamıştır.[721] Akabinde, 8. maddenin işletilebilmesi için ihlalin belirli bir seviyeye ulaşması gerektiğine ilişkin içtihatlarını hatırlatmıştır.[722]

AİHM, yerel mahkemelerin içeriğin hakaret niteliği taşıdığına ilişkin tespitlerine katılmış ve bu içeriğin 8. madde kapsamında olduğunu belirtmiştir.[723] Burada özellikle *Delfi AS v. Estonya* kararındaki sorumluluk rejiminin işletilip işletilemeyeceğine de bakan AİHM, davaya konu yorumun nefret söylemi veya şiddete teşvik niteliğinde olmadığını belirtmiştir.[724]

AİHM'ye göre mevcut uyuşmazlık, devletin eyleminden kaynaklanan bir ihlalden ziyade yerel mahkemelerin başvurucunun özel hayatının korunması için sundukları korumanın yetersizliği iddiasından kaynaklanmaktadır.[725] Devletlerin bu konudaki pozitif ve negatif yükümlülüklerine

[719] *Rolf Anders Daniel PIHL v. İsveç*, para. 20.
[720] *Rolf Anders Daniel PIHL v. İsveç*, para. 21.
[721] *Rolf Anders Daniel PIHL v. İsveç*, para. 23.
[722] *Rolf Anders Daniel PIHL v. İsveç*, para. 24.
[723] *Rolf Anders Daniel PIHL v. İsveç*, para. 25.
[724] *Rolf Anders Daniel PIHL v. İsveç*, para. 25.
[725] *Rolf Anders Daniel PIHL v. İsveç*, para. 26.

değinen AİHM, her iki durumda da sorumlulukların benzer olduğunu belirtmiştir. Bu doğrultuda, yarışan haklar arasında makul bir denge kurulması gerektiğini ve her bağlamda devletlerin belirli ölçüde takdir alanı olduğunu hatırlatmıştır.[726] Bu çerçevede, *Delfi AS v. Estonya* kararındaki tespitlerine atıf yapmıştır.[727]

Peki, sorumluluk rejimi tesis edilirken nasıl bir yol izlenmelidir? AİHM, bu noktada *MTE Index.hu Zrt v. Macaristan* kararındaki kriterleri hatırlatmıştır.[728] Buna göre, sorumluluk tesisinde, yorumların bağlamı, şirketin hakaret içeren yorumları önlemek veya kaldırmak için aldığı tedbirler, aracı platformun sorumluluğuna alternatif olarak gerçek içerik sağlayıcı kişilerin sorumluluğu ve şirket aleyhine iç hukuktaki yargılamaların neticesi gibi kriterler dikkate alınmalıdır.

Tüm bu tespitlerden sonra AİHM, mevcut uyuşmazlıkta başvurucunun AİHS'nin 8. maddesi tahtında güvence altına alınan özel hayata saygı gösterilmesi hakkı ile blog sitesini işleten birliğin AİHS'nin 10. maddesiyle güvence altına alınan ifade özgürlüğü hakkının İsveç Devleti tarafından makul şekilde dengelenip dengelenmediğini değerlendirmeye almıştır.[729]

AİHM, blog sitesini işleten birliğin küçük ve kâr amacı gütmeyen bir yapıda olduğunu, internet ortamında çok fazla yoruma zemin hazırlayacak veya çok kişi tarafından görüntülenebilecek nitelikte olmadığını belirtmiştir.[730] AİHM, her tespitinden sonra mevcut durumu *Delfi AS v. Estonya* kararıyla karşılaştırmıştır. Bu aşamada da mevcut uyuşmazlığın maddi unsurlarının *Delfi AS v. Estonya* ile aynı olmadığını vurgulamıştır.[731]

Hatırlanacağı üzere, Delfi AS portalı Estonya'nın en çok ziyaret edilen siteleri arasında yer almakta ve içeriklerine çok sayıda kullanıcı yorum yapmaktaydı. AİHM'ye göre, *MTE ve Index.hu Zrt v. Macaristan*

---

[726] *Rolf Anders Daniel PIHL v. İsveç*, para. 26.

[727] *Delfi AS v. Estonya*, para. 139.

[728] *MTE/Index.hu Zrt v. Macaristan*, para. 69.

[729] *Rolf Anders Daniel PIHL v. İsveç*, para. 29.

[730] *Rolf Anders Daniel PIHL v. İsveç*, para. 30-31.

[731] *Rolf Anders Daniel PIHL v. İsveç*, para. 31.

kararında hüküm altına alındığı üzere, filtrelenmemiş yorumların hukuka aykırı nitelikte olabileceğinden hareketle platformu sorumluluk altına sokmak aşırı ve pratik olmayan bir öngörü/tedbir gerektiren ve hâliyle internet ortamında bilgiye erişim hakkını zedeleyen bir yaklaşımdır.[732]

AİHM, blogda yapılan yorumlara ön denetim uygulanmadığını, içerikleri üretenlerin içerikten sorumlu olduklarının belirtildiğini, mevcut ihtilafta hukuka aykırı nitelikteki içeriğin bildirimin ertesi gününde blog tarafından kaldırıldığını tespit etmiştir.[733] Yine *Delfi AS v. Estonya* kararıyla karşılaştırma yapan AİHM, hukuka aykırı içeriklerin Delfi AS sitesinde altı hafta boyunca yayında kaldıktan sonra kaldırıldığını hatırlatmıştır.[734]

İçeriklerin kaldırılmasına rağmen arama motorları üzerinden erişilebilir olmasının hukuki bir etkisi var mıdır? AİHM, bu noktada, AB Adalet Divanının "unutulma hakkı kararı" olarak da bilinen *Google v. İspanya* kararına atıf yapmış; bu kararda, başvurucuya arama motorundan ilgili yorumların izlerini kaldırmayı talep etme olanağı tanındığını belirtmiştir.[735]

Bahse konu yorumu yazan kişinin sorumluluğunu da tartışan AİHM, içeriğin yayımlandığı bilgisayara ait IP adresi tespit edilmiş olmasına rağmen başvurucunun söz konusu kişinin tespitine yönelik bir girişimde bulunup bulunmadığına dair bilgi verilmediğini belirtmiştir.[736]

AİHM, üçüncü taraflara ait yorumlar sebebiyle platformların sorumluluğuna gidilmesinin genel olarak internet aracılığıyla ifade özgürlüğünün sağlanması üzerindeki etkisine vurgu yapmıştır.[737] *MTE ve Index.hu ZRT v. Macaristan* kararında da tespit edildiği üzere, bu tür bir sorumluluk özellikle ticari olmayan web siteleri için daha zarar verici olacaktır.[738] AİHM, iç hukukta sorumluluk konusunu düzenleyen hüküm-

[732] *Rolf Anders Daniel PIHL v. İsveç*, para. 31.
[733] *Rolf Anders Daniel PIHL v. İsveç*, para. 32.
[734] *Rolf Anders Daniel PIHL v. İsveç*, para. 32.
[735] *Rolf Anders Daniel PIHL v. İsveç*, para. 33.
[736] *Rolf Anders Daniel PIHL v. İsveç*, para. 34.
[737] *Rolf Anders Daniel PIHL v. İsveç*, para. 35.
[738] *Rolf Anders Daniel PIHL v. İsveç*, para. 35.

lerin varlığına işaret etmiş ve yorumun niteliği veya ağırlığı daha farklı olsaydı, söz konusu içeriği kaldırmadığı için blog sitesini işleten derneğin sorumlu tutulabileceğini belirtmiştir.[739]

AİHM, somut olaydaki yorumun nefret söylemi veya şiddete teşvik niteliğinde olmadığını dikkate almıştır. İçeriğin kâr amacı gütmeyen bir dernek tarafından işletilen küçük bir blogda yayımlandığını gözetmiştir. Yorumun, bildirim yapıldıktan sonraki gün hemen ve ilk yayımlanma tarihinden dokuz gün sonra dernek tarafından kaldırıldığını değerlendirmiştir. Bu tespitler ışığında AİHM, İsveç yerel mahkemelerinin, başvurucunun AİHS'nin 8. maddesinde güvence altına alınan hakkıyla derneğin AİHS'nin 10. maddesiyle korunan ve karşı hak niteliğinde olan ifade özgürlüğü hakkı arasında makul bir denge gözettiklerine hükmetmiştir.[740] Bu doğrultuda, başvuruyu açıkça temelsiz görmüş ve kabul edilebilirlik kriterini sağlamadığından başvurunun reddedilmesine hükmetmiştir.[741]

IV. Değerlendirme

Rolf Anders Daniel Pihl v. İsveç kararı, AİHM'nin *Delfi AS v. Estonya* kararıyla geliştirdiği sorumluluk rejiminin tekrar test edildiği bir karar olmuştur. AİHM, internet platformlarının üçüncü taraflara ait içeriklerden sorumlu tutulmalarının, internet ortamında ifade özgürlüğüne yönelik caydırıcı bir etki (*chilling effect*) oluşturmasıyla ilgili temkinli ifadeler kullanmaktadır. Ancak, AİHM bu caydırıcı etkinin asıl nedeninin *Delfi AS v. Estonya* kararı dolayısıyla bizzat kendisi olduğunun farkına varmamaktadır. *MTE ve Index.hu Zrt v. Macaristan* kararında da bu konuda bir düzeltme yapılmak şöyle dursun, sorumluluk rejimi perçinlenmiştir.

AİHM, mevcut uyuşmazlıktaki gibi bir blog sitesinin yorumlardan dolayı hukuki sorumluluktan nasıl kurtulacağına dair objektif bir metodoloji geliştirememiştir. *Rolf Anders Daniel Pihl v. İsveç* kararının çeşitli kısımlarında *Delfi AS v. Estonya* kararıyla kıyaslama yapılarak maddi

---

[739] *Rolf Anders Daniel PIHL v. İsveç*, para. 36.

[740] *Rolf Anders Daniel PIHL v. İsveç*, para. 37.

[741] *Rolf Anders Daniel PIHL v. İsveç*, para. 38.

vakıaların farklılığına vurgu yapılmaya çalışılsa da sorumluluğun hangi aşamada başladığını hangi aşamada bittiğini kestirmek zordur. Ayrıca, bir yorumun salt hakaret niteliğinde mi, nefret söylemi niteliğinde mi olduğunun tespiti kapsamlı bir muhakeme gerektirir. Ancak, hukuki nitelendirmedeki bu nüans, platformun ön denetim mekanizması kurup kurmaması ve yorumlardan hukuki sorumluluğa kadar birçok hususu etkilemektedir. AİHM, platformların hem öngörülü olmasını hem de doktrinde bile birçok yönüyle tartışmalı konuları hemen çözümleyip hareket etmesini beklemektedir. Bu yaklaşım, Web 2.0 sisteminin doğasına aykırıdır.

AİHM, ticari faaliyette bulunmamayı sorumluluğun tespitinde bir kriter olarak kullanmaya devam etmiştir. Daha önce de belirtildiği üzere, internet ortamında içeriklerin oluşturulması ve platformların sürdürülebilirliğinde ticari amaç çok önemli bir yer tutmaktadır. Buna rağmen, AİHM ticari faaliyet durumunda ölçüsüz bir sorumluluk rejimi uygulamaktadır.

AİHM'nin *Rolf Anders Daniel Pihl v. İsveç* kararının satır aralarında, sitenin farklı bir statüde değerlendirilmesine gerekçe olarak küçük bir blog olması, görece az sayıda ziyaretçiye içerik ulaştırması ve blogda az yorum yapılması gösterilmektedir. Diğer bir deyişle, mevcut uyuşmazlığı *Delfi AS v. Estonya* kriteri dışında nitelendirmeye çalışmaktadır. Küçük blog, büyük site, az kullanıcı yorumu, çok ziyaretçi ayrımı ne kadar objektif ve makuldür? Bir içerik, ticari olmayan bir blog sitesinde, kalabalık olmayan ancak spesifik bir kitleye yönelmiş olabilir. Bu durum, içeriğin, somut olaydaki niteliği gereği büyük bir hukuka aykırılığa yol açmayacağı anlamına gelmez. AİHM, internet ekosistemini ve Web 2.0 dünyasını gereğince içselleştiremediğinden kıyas yoluyla bir yorum yapmaya çalışmakta ancak bu da hakkaniyete uygun bir sonuç vermemektedir.

§16. TAMİZ V. BİRLEŞİK KRALLIK

AİHM'nin *Tamiz v. Birleşik Krallık* kararı, blogger.com gibi bir internet platformunun kullanıcı içeriklerinden sorumluluğuna ilişkin bir karardır.[742] Başvuru, temel olarak, kişi aleyhine hakaret ve iftira niteliğindeki içeriklerin Google Inc. şirketi tarafından barındırılan blogger.com platformunda üç buçuk ay boyunca yayımlanmasından doğan zararı ortadan kaldırmak için yerel mahkemelerin gerekli hukuki korumayı sağlamadığından bahisle Birleşik Krallık devletinin AİHS'nin 8. maddesi bağlamındaki pozitif yükümlülüğünü ihlal ettiği iddiasına ilişkindir.

I. Davanın gelişimi

Başvurunun ana konusu blogger.com sitesinde barındırılan bir blog içeriğidir. Blogger platformu, ABD'de kurulu ve ABD merkezli bir şirket olan Google Inc. şirketi tarafından yönetilmektedir. Site, dünyanın herhangi bir yerindeki kullanıcının ücretsiz şekilde blog oluşturmasına imkân vermektedir.[743] Ayrıca, kullanıcılarına bloglarının görünümünü şekillendirmek için tasarım araçları sağlamakta ve web siteleri yoksa bloglarını blogger.com sitesinde barındırmaya imkân tanımaktadır.

Blogger.com, "İçerik Politikası" uygulamakta ve kullanıcıların, hizmetleri kullanarak neler yapabileceğini belirlemektedir.[744] Örneğin, çocuk pornografisi, ırkçılık temelli nefret söylemi yasaklanmıştır. İçerik Politikası şu şekilde açıklanmıştır:[745]

"*Blogger ücretsiz bir haberleşme, kendini ifade etme ve ifade özgürlüğü hizmetidir. Blogger'ın bilginin mevcudiyetini artırdığına, sağlıklı tartışmaları*

---

[742] **AİHM**, *Tamiz v. Birleşik Krallık*, Başvuru No: 3877/14, 19.9.2017.

[743] *Tamiz v. Birleşik Krallık*, para. 4.

[744] *Tamiz v. Birleşik Krallık*, para. 5.

[745] *Tamiz v. Birleşik Krallık*, para. 5.

teşvik ettiğine ve insanlar arasında yeni bağlantılar kurulmasına imkân tanıdığına inanıyoruz.

Kullanıcılarımızın paylaşmayı tercih ettikleri içeriğin sahipliğine ve sorumluluğuna saygı göstermekteyiz. İnancımız şudur ki içeriği sansürlemek, kendisini ifade özgürlüğü üzerine inşa eden bir hizmete aykırı olacaktır.

Bu değerleri ayakta tutabilmek için, bu hizmeti sunma imkânımızı ve teşvik ettiğimiz ifade özgürlüğünü tehdit eden kötüye kullanımları önlemeliyiz. Sonuç olarak, Blogger üzerinde barındırılabilecek içeriğin sınırları vardır. Tanımladığımız sınırlar hukuki gerekliliklerle uyum sağlayacak ve hizmetin bütün olarak gelişmesine katkı sunacak şekildedir."

Google, bu politikanın yanı sıra "Kötüye Kullanımı Bildir" özelliği sunmaktadır ve bu kanal aracılığıyla "*Hakaret/İftira/Karalama*" dâhil sekiz farklı gerekçeyle ihlal bildirimi yapmak mümkündür.[746] Kullanıcı "*Hakaret/İftira/Karalama*" seçeneğini işaretlediği zaman karşısına ikinci bir ekran çıkmakta, bu ekranda blogger.com hizmetinin Amerikan Hukukuna göre faaliyet gösterdiği ve hakları ihlal ettiği iddia edilen içeriklerin, ancak bir mahkeme kararıyla iftira niteliğinde (hukuka aykırı) olduğu tespit edilirse kaldırılacağı uyarısı yer almaktadır.[747] Google şirketi, blogger.com hizmetine yüklenen kullanıcı içeriğinin miktarını bu politikanın gerekçesi olarak göstermiştir. Google, hukuka aykırılığı bir mahkeme tarafından tespit edilmediği sürece bir içeriğin kaldırılmasının pratik olmadığını, bu tür ihtilaflar hakkında kendi başına hüküm veremeyeceğini belirtmiştir.[748]

Başvurucu Bay Payam Tamiz, Birleşik Krallık vatandaşı olup Maidstone'da yaşamaktadır. 27 Nisan 2011 tarihinde blogger.com sitesinde barındırılan "Londra Müslümanı" isimli bir blog sayfasında başvurucunun fotoğrafı ve hakkında çeşitli iddialar içeren bir gönderi yayımlanmıştır.[749] Bu gönderiye cevap olarak, Bay Payam'ın çeşitli suçlara karıştığı, hüküm giydiği, ikiyüzlü olduğu, aşırı bir ırkçı olduğu, iltica sürecinde gerçek

[746] *Tamiz v. Birleşik Krallık*, para. 6.

[747] *Tamiz v. Birleşik Krallık*, para. 6.

[748] *Tamiz v. Birleşik Krallık*, para. 6.

[749] *Tamiz v. Birleşik Krallık*, para. 7.

yaşını gizlediği ve cinsel hayatına ilişkin muhtelif iddiaların yer aldığı anonim yorumlar yapılmıştır.[750]

Başvurucu, 28-29 Nisan 2011 tarihinde, blogger.com sitesinde yer alan "Kötüye Kullanımı Bildir" seçeneğini kullanarak hakaret niteliğinde gördüğü belirli yorumları şikâyet etmiştir.[751] Başvurucu, bir yandan da Google Inc. şirketinin Birleşik Krallık'taki bağlı şirketi olan Google UK Ltd. şirketine 29 Haziran 2011 tarihinde başvurmuş ve Yorum A referanslı yorumun kaldırılması için talepte bulunmuştur.[752] Google UK Ltd. başvuruyu Google Inc. şirketine yönlendirmiştir. Google Inc. ise başvuru metninden açıkça anlaşılamadığı gerekçesiyle başvurucudan söz konusu yorumun gerçek olup olmadığına yönelik açıklama talep etmiştir. Başvurucu, Yorum A'nın "yanlış ve iftira" niteliğinde olduğunu belirtmiş ve ayrıca Yorum B'yi de şikâyet konusu yapmıştır.[753]

19 Temmuz 2011 tarihinde Google Inc. şirketi bünyesindeki "Blogger Takımı" başvurucuya bir e-posta göndererek, şikâyetini blog sayfasının yazarına iletmek için başvurucunun iznini talep etmiş ve ihtilaf konusu yorumları kendilerinin kaldırmayacaklarını belirtmiştir.[754] Bu isteğe onay veren başvurucu, ayrıca C, D, E, F ve G referanslı yorumları da şikâyetine dâhil etmiştir.

11 Ağustos 2011 tarihinde Google Inc., şikâyeti ilgili blog sayfasının yöneticisine iletmiştir.[755] 14 Ağustos 211 tarihinde gönderi ve tüm yorumlar blog sayfasının yöneticisi tarafından kaldırılmış ve ertesi gün başvurucu bilgilendirilmiştir.[756]

---

[750] *Tamiz v. Birleşik Krallık*, para. 8-16.

[751] *Tamiz v. Birleşik Krallık*, para. 17.

[752] *Tamiz v. Birleşik Krallık*, para. 18.

[753] *Tamiz v. Birleşik Krallık*, para. 18.

[754] *Tamiz v. Birleşik Krallık*, para. 19.

[755] *Tamiz v. Birleşik Krallık*, para. 20.

[756] *Tamiz v. Birleşik Krallık*, para. 21.

II. Yerel yargılama süreci

Başvurucu, Google Inc. şirketi aleyhine A ila G referanslı tüm yorumlara ilişkin tazminat davası açmıştır.[757] Bilahare H referanslı yorumu da talebine ekleyerek Google Inc. şirketine karşı açmış olduğu davaya dâhil etmiştir.[758]

Google Inc. şirketi, Yerel Yüksek Mahkemenin davaya ilişkin yargılama yetkisinin olmadığını ileri sürmüş ve şu iddialarda bulunmuştur:[759]

i. Talep formu, ilgili yargılama alanında yorumlara önemli sayıda okuyucu tarafından erişildiğine dair bir iddia içermemektedir. Hâliyle "gerçek ve esaslı" bir haksız fiil söz konusu değildir.

ii. Google Inc. şirketi İngiliz hukuku bağlamında hakaret içeren içeriklerin yayıncısı değildir, bloglar üzerindeki içerikleri üretmediği gibi bunlar üzerinde kontrolü de yoktur, tarafsız bir hizmet sağlayıcısıdır.

iii. Google Inc. yayıncı olarak kabul edilse bile 2002 tarihli Elektronik Mahremiyet Direktifi'nin 19. maddesi gereğince sorumluluktan muaf bulunmaktadır.

22 Mart 2012 tarihinde Yüksek Mahkeme, kararını vermiştir.[760] Kararı veren hâkim öncelikle "*gerçek ve esaslı bir haksız fiil*" olup olmadığını değerlendirmeye almıştır.[761] Hâkim, C, E, F, G ve H referanslı yorumları "*salt kaba taciz*"; A, B ve D referanslı yorumları ise hakaret olarak değerlendirmiştir.[762]

Google Inc. şirketinin "*yayıncı*" olarak nitelendirilip nitelendirilemeyeceği konusunda hâkim, hukuki sorumluluğun, bildirim anından itibaren değerlendirilmesi gerektiğini belirtmiştir.[763] Hâkim, Google Inc.

---

[757] *Tamiz v. Birleşik Krallık*, para. 22.

[758] *Tamiz v. Birleşik Krallık*, para. 22.

[759] *Tamiz v. Birleşik Krallık*, para. 23.

[760] *Tamiz v. Birleşik Krallık*, para. 24.

[761] *Tamiz v. Birleşik Krallık*, para. 25.

[762] *Tamiz v. Birleşik Krallık*, para. 25.

[763] *Tamiz v. Birleşik Krallık*, para. 26.

şirketinin, rencide edici nitelikte olduğu ileri sürülen içeriği kaldırmamasının bu yönde geliştirdiği ve uyguladığı politikadan kaynaklandığını ve şirketin kendisini söz konusu içeriği soruşturmak veya içerik hakkında hüküm vermek konumunda görmediğini not etmiştir.[764] Bunun özünde pratiklik yatmaktadır: Google Inc. şirketi bilgilerin ve fikirlerin paylaşımı için platform sağlayarak sansürden kaçınmaya çalışmaktadır. Öte yandan, blogger.com platformu üzerinde yarım trilyondan fazla kelime yer almakta ve her dakika 250.000 yeni kelime eklenmektedir. Hâkime göre bu durum karşısında içerik üzerinde kurumsal bir editoryal kontrol sağlanması neredeyse imkânsızdır.[765]

Davayı ele alan hâkime göre AİHS'nin 10. maddesi bağlamında zorunlu ve ölçülü olmadığı sürece bir hukuki sorumluluğun oluşturulmasından kaçınılmalıdır.[766] Hâkim, yorumların yazarları ve blog sayfasının yazarına yönelik dava açma imkânının varlığına işaret etmiştir. Anonimliğe ilişkin sorunlar sebebiyle bu yaklaşımın gerçeklikten öte teorik olduğunu kabul etmekle birlikte yine de kolaylıkla göz ardı edilemeyeceğini vurgulamıştır.[767] Hâkim, asıl hukuki sorunun söz konusu kişilere dava açılabilmesinden ziyade Google Inc. şirketinin bir yayıncı olarak nitelendirilip nitelendirilemeyeceği olduğunu tekrarlamıştır.[768]

Hâkime göre, Google Inc. şirketi (her zaman büyük bir süratle olmasa da) söz konusu blog sahiplerine bildirimde bulunma sorumluluğunu üstlenmekte fakat tüm şikâyetleri araştırması gerektiğini kabul etmemektedir.[769] Yine de Google şirketinin durumundaki bir şirket, kendisine şikâyet bildirimi gelmesi durumunda derhâl yayıncı statüsüne dönüşmemektedir.

Hâkime göre, bir hizmet sağlayıcıya veya kolaylaştırıcıya ilişkin statünün kendiliğinden bir yayını onaylayan veya yayına muvafakat eden

---

764 *Tamiz v. Birleşik Krallık*, para. 27.

765 *Tamiz v. Birleşik Krallık*, para. 27.

766 *Tamiz v. Birleşik Krallık*, para. 28.

767 *Tamiz v. Birleşik Krallık*, para. 28.

768 *Tamiz v. Birleşik Krallık*, para. 28.

769 *Tamiz v. Birleşik Krallık*, para. 29.

statüsüne dönüşmesi yerinde değildir. Nihayetinde, Google kendisine bildirim yapıldığı zaman önceden olduğu gibi tarafsız kalmaya çalıştığı iddiasındadır. Hâkime göre, içeriği kaldırma (gerçek manada sansür uygulama) teknik kapasitesi olsa da içeriğin yazarı veya onaylayanı olduğu anlamına gelmez.[770] Hâkim bu durumu, gece bir duvara grafiti çizilmesi sebebiyle duvar sahibinin duvardaki içerikten sorumlu tutulmasına benzetmektedir.[771] Tüm bu tespitler ışığında hâkim, Google Inc. şirketinin rolünün bir platform sağlayıcı olarak tamamen pasif olduğunu belirtmiş ve İngiliz hukuku uyarınca yayıncı olarak sorumlu tutulamayacağına hükmetmiştir.[772] Hâkime göre, Google Inc. şirketi bir an için yayıncı olarak kabul edilse bile kendisine bildirim gelmesinden içeriği kaldırmasına kadar o denli kısa bir süre geçmiştir ki şirketin sorumluluğu gündeme gelmeyecektir. Zira 2002 tarihli Elektronik Haberleşme Tüzüğü'nün 19. maddesi hükümleri şirkete gerekli savunma imkânını tanıyacaktır.[773]

Başvurucu, Google Inc. şirketinin yayıncı olarak kabul edilmemesi kararına itiraz etmiş ve ifade özgürlüğü karşısında şöhretin de AİHS'nin 8. maddesi bağlamında korunduğunu belirtmiştir.[774] Bu itiraz da 14 Şubat 2013 tarihinde reddedilmiştir.[775]

İtirazı inceleyen İstinaf Mahkemesi, Yüksek Mahkemenin A, B ve D referanslı yorumların nitelendirilmesine yönelik tespitine katıldığını belirtmiştir.[776] İstinaf Mahkemesi, Google Inc. şirketinin yayıncı olup olmadığına dair tespite ise yorumların bildirime rağmen yayında kaldığı süre ile şirketin tüm sistem üzerindeki kontrol yetkilerini dikkate alarak farklı yaklaşmışsa da[777] alt derece mahkemesinin haksız fiilin gerçek ve esaslı olması gerektiğine ilişkin tespitlerine katılarak istinaf talebini red-

[770] *Tamiz v. Birleşik Krallık*, para. 29.
[771] *Tamiz v. Birleşik Krallık*, para. 29.
[772] *Tamiz v. Birleşik Krallık*, para. 29.
[773] *Tamiz v. Birleşik Krallık*, para. 30.
[774] *Tamiz v. Birleşik Krallık*, para. 31.
[775] *Tamiz v. Birleşik Krallık*, para. 32.
[776] *Tamiz v. Birleşik Krallık*, para. 33-34.
[777] *Tamiz v. Birleşik Krallık*, para. 35-38.

detmiştir.[778] Bu karara yönelik temyiz talebi de 1 Temmuz 2013 tarihinde reddedilmiştir.[779]

III. Hukuki arka plan

Konunun esasına girmeden evvel AİHM, muhtelif İngiliz hukuku düzenlemesi ve içtihadı ile Avrupa Birliği hukuku düzenlemesi ve insan hakları belgesine atıf yapmıştır. İngiliz hukukuna göre, hakaret niteliğindeki ifadelerin yayımlanmasından hukuki sorumluluğun doğması ve hakaret sebebiyle haksız fiilden dolayı sorumlu tutulabilmek için en azından yayın sürecine bilerek dâhil olmak gerekmektedir.[780] Keza, rolü, tartışmalı içeriği dağıtmakla sınırlı olan kişiyi yayıncı olarak nitelendirilebilmek için kişinin hakaret niteliğindeki içerikten haberdar olması veya makul bir özen göstererek bunu öğrenebilecek olması gerekmektedir.[781]

AİHM, İngiliz mahkemelerinin, hakarete ilişkin içerikler sebebiyle bilgi toplumu hizmet sağlayıcılarının sorumluluğuna dair özel bir içtihat geliştirdiğini not etmiştir.[782] İngiliz mahkemeleri, üçüncü taraflara ait içeriklere salt pasif ortam sağlayan bilgi toplumu hizmet sağlayıcılarıyla, veriyi kısa süreli veya geçici olarak saklamanın ötesine geçen ve içeriği diğer internet kullanıcılarına eriştirenler arasında bir ayrım yapmaktadır. Söz konusu içtihada göre, ikinci kategorideki hizmet sağlayıcılar, hakaret niteliğinde olduğu belirtilen içeriği bildirime rağmen ihmal veya kasıtlarıyla kaldırmazlarsa ve somut olayın özelliklerinden bu durumun yayının devamına ilişkin bir tür rıza veya muvafakat olarak nitelendirilmesi mümkünse sorumlu tutulabileceklerdir.[783]

AİHM, ayrıca 1996 tarihli İngiliz Hakaret Yasası[784], AB e-Ticaret Direktifi'nin bazı hükümlerinin uygulamasını gösteren İngiliz Elektronik

[778] *Tamiz v. Birleşik Krallık*, para. 39-40.
[779] *Tamiz v. Birleşik Krallık*, para. 41-42.
[780] *Tamiz v. Birleşik Krallık*, para. 43.
[781] *Tamiz v. Birleşik Krallık*, para. 43.
[782] *Tamiz v. Birleşik Krallık*, para. 44.
[783] *Tamiz v. Birleşik Krallık*, para. 44.
[784] *Tamiz v. Birleşik Krallık*, para. 45-48.

Ticaret Tüzüğü[785] ile "gerçek ve esaslı haksız fiil" tanımlamasına ilişkin muhtelif İngiliz yargı içtihadını alıntılamıştır.[786] Aynı doğrultuda, Avrupa Konseyinin 28 Mayıs 2003 tarihli İnternette İletişim Özgürlüğüne İlişkin Deklarasyon'una, 21 Aralık 2005 tarihli Birleşmiş Milletler İfade Özgürlüğü Özel Raportörü, Basın Özgürlüğüne İlişkin OSCE Temsilcisi ve OAS İfade Özgürlüğü Özel Raportörü'nün ortak deklarasyonuna ve Avrupa Birliği e-Ticaret Direktifi'nin 14 ve 15. maddelerine yer verilmiştir.[787]

IV. Tarafların iddiaları

Başvurucu, temel olarak AİHS'nin 8. maddesiyle güvence altına alınan şöhretinin korunması hakkını çiğneyen hakaret ve iftira niteliğindeki içeriklerin Google Inc. şirketi tarafından barındırılan bir web sitesinde üç buçuk ay boyunca yayımlanması karşısında yerel mahkemelerin, uğradığı zararı ortadan kaldırmak için gerekli hukuki korumayı sağlamadığından bahisle Birleşik Krallık devletinin AİHS'nin 8. maddesi bağlamındaki pozitif yükümlülüğünü ihlal ettiğini ileri sürmüştür.[788] Yayımlanan yorumlara ilişkin "*gerçek veya esaslı bir haksız fiil*" testini uygulayan yerel mahkemelerin, kendisinin hukuki korumaya erişimini reddettiklerini ve bu durumun AİHS'nin 8. maddesinde güvence altına alınan haklarına müdahale niteliğinde olduğunu iddia etmiştir.

A. Birleşik Krallık Hükûmetinin görüşleri

Birleşik Krallık Hükûmeti, başvurucunun şikâyetinin temelsiz olduğunu ileri sürerek reddedilmesi gerektiğini belirtmiştir.[789] Hükûmet, başvurucunun haklarına ilişkin dikkatli bir inceleme yapıldığını; yerel mahkemelerin ve temyiz makamlarının, yorumlara ilişkin gerekli değerlendirmeleri yaptığını; başvurucunun, bazı yorumları istinaf süre-

[785] *Tamiz v. Birleşik Krallık*, para. 49.

[786] *Tamiz v. Birleşik Krallık*, para. 50

[787] *Tamiz v. Birleşik Krallık*, para. 54-56.

[788] *Tamiz v. Birleşik Krallık*, para. 57-59.

[789] *Tamiz v. Birleşik Krallık*, para. 60.

cinde usulüne uygun olarak itiraza konu etmediğini belirtmiştir.[790] Aynı doğrultuda, başvurucunun taleplerinin yerine getirilmesinin Google Inc. şirketinin ve kullanıcılarının haklarına zorunlu olmayan ve ölçüsüz bir müdahale niteliğinde olacağını ileri sürmüştür.[791] Ayrıca, haksız fiil testinin de yarışan hakları dengelemek için etkin bir araç olduğunu ifade etmiştir.[792]

Hükûmet, son olarak, Google Inc. şirketinin bildirimden önce ve sonra şeklinde sorumluluğunun ayrıştırılarak bir karar verilmesinin AİHM'nin *Delfi AS v. Estonya* içtihadıyla uyumlu olduğunu vurgulamış ve yerel mahkemelerin, kararlarını ilgili ve yeterli gerekçelere dayandırdığını belirtmiştir.[793] Google Inc. şirketi "uyar-kaldır" mekanizması kurmuştur ve uyarı sonrası etkin bir süreç işletmiştir. Hükûmete göre, uyarı öncesi süreç için Google Inc. şirketinin sorumlu tutulması, AİHS'nin 10. maddesi kapsamındaki hakları ölçüsüz kısıtlayan, internet ortamında özgür ve samimi bilgi, görüş ve fikir paylaşımının üzerinde olumsuz etki doğuracak bir durum ortaya çıkaracaktır.[794]

B. Başvurucunun iddiaları

Başvurucu, A'dan H'ye kadar olan yorumların yayımlanmasının şahsına karşı açık bir saldırı olduğunu ve AİHS'nin 8. maddesiyle korunan özel hayata saygı hakkını ihlal ettiğini ileri sürmüştür.[795] Ayrıca C, E, F, G ve H referanslı yorumların yerel mahkemelerce hakaret niteliği taşımadığı tespiti yapılmışsa da bu yorumların yayımlanmasının, itibarına halel getirip getirmediğinin değerlendirmeye alınmadığını ileri sürmüştür.[796]

Başvurucu, mahkemelerin 8 ve 10. maddeler kapsamındaki hakları dengelerken geniş bir takdir yetkisi bulunduğunu kabul etmekle birlikte

---

[790] *Tamiz v. Birleşik Krallık*, para. 61.
[791] *Tamiz v. Birleşik Krallık*, para. 62.
[792] *Tamiz v. Birleşik Krallık*, para. 63.
[793] *Tamiz v. Birleşik Krallık*, para. 64.
[794] *Tamiz v. Birleşik Krallık*, para. 65.
[795] *Tamiz v. Birleşik Krallık*, para. 66.
[796] *Tamiz v. Birleşik Krallık*, para. 66.

mevcut ihtilafta bir denge testi yapılmadığını ve bu bağlamda Google şirketinden yorumların ne kadar görüntülendiği gibi gerekli delillerin alınmadığını ileri sürmüştür.[797] Ayrıca, yorumların yayında kaldığı süreyi gerekçe göstererek itibarına esaslı ölçüde zarar gelmediğine yönelik ilgili ve yeterli gerekçe ortaya konmadığını iddia etmiştir.[798] Son olarak *Delfi AS v. Estonya* içtihadındaki kriterlere atıf yapan başvurucuya göre, Google Inc. şirketinin uyar-kaldır mekanizması yetersiz kalmıştır; içerik, kötüye kullanımın bildirilmesinden dört ay sonra kaldırılmıştır; yorumlar, itibarı üzerinde ağır ve olumsuz etki oluşturmuştur; ihlal olduğunun tespiti Google Inc. gibi şirketler üzerinde "*caydırıcı etki*" doğurmayacaktır.[799]

C. Müdahil üçüncü tarafların görüşleri

Tamiz v. Birleşik Krallık davasına Google Inc., Media Legal Defence Initiative (MLDI) ve Article 19 müdahil olmuş, başvuruya ilişkin görüşlerini paylaşmıştır.

1. Google Inc.

Google Inc. şirketine göre blogger.com platformu, kişilerin politik, sosyal ve kültürel konularda geniş bir çerçevede ifade özgürlüğünü kullanmasına imkân vermektedir.[800] Şirket, bu sebeple, mevcut başvurunun hem kendisinin hem de blogger.com platformunu her gün kullanan milyonlarca bireyin AİHS'nin 10. maddesindeki haklarını ilgilendirdiği kanaatindedir.

Google Inc. şirketine göre, yorumları yayımlamadan bir ön filtrelemeye tabi tutmak, bilgi toplumu hizmet sağlayıcılarına ölçüsüz ve altından kalkılamayacak bir külfet getirecektir.[801] Şirket, platformlara belirli bir süre tanınması gerektiğini düşünmektedir. Şirkete göre, bilgi toplumu hizmet sağlayıcılarını bir şikâyet talebi geldiği anda sorumlu tut-

[797] *Tamiz v. Birleşik Krallık*, para. 67.
[798] *Tamiz v. Birleşik Krallık*, para. 68.
[799] *Tamiz v. Birleşik Krallık*, para. 69.
[800] *Tamiz v. Birleşik Krallık*, para. 70.
[801] *Tamiz v. Birleşik Krallık*, para. 71.

mak; şikâyetin içeriğini soruşturmak, blog sayfalarının veya yorumların yazarlarıyla iletişime geçmek ve kaldırmayı kolaylaştırıcı gerekli teknik ve pratik tedbirleri almak için makul bir süre tanımamak bilgi toplumu hizmet sağlayıcılarının AİHS'nin 10. maddesi tahtındaki haklarına ölçüsüz bir müdahale oluşturacaktır.[802] Keza, hakları zedelenen kişi ve blog platformunun sağlayıcısının hakları arasında adil bir denge kurulabilmesi için bilgi toplumu hizmet sağlayıcılarına makul bir süre tanınmalıdır. Şirkete göre, aksi bir durumda, bildirim gelir gelmez yorumların kaldırılması gerekecek ve bu da meşru ifadeler ile kamuyu ilgilendiren önemli bilgilerin yayımlanmasını baskılayacaktır.[803]

2. Media Legal Defence Initiative (MLDI)

Media Legal Defence Initiative (MLDI) isimli sivil toplum örgütü, yer sağlayıcı platformların bireylere ifade özgürlüklerini kullanmaları için dijital alan sağladığını belirtmiştir.[804] MLDI'ya göre, aracı platformlar için mutlak bağışıklık, son kullanıcıları tarafından paylaşılan içeriğin hukuka uygunluğunun tespitinde platformlar yerine mahkemelerin karar vermesi, içeriği kontrol etmeye ilişkin yükümlülüğün olmaması, yargı yetkisine ilişkin eşikler konulması -egemenlik alanıyla ilgisi kurulmayan kişilere dava hakkı tanınmaması- yoluyla yargılama turizminin önüne geçilmesi örnek güvencelerdir.[805]

MLDI'ya göre, gerekli koruma sağlanmazsa aracı platformlar sansür yapmaya zorlanabilir ve bu şekilde sorumluluk altına girmemek adına son kullanıcıların ifade özgürlüklerini kısıtlayabilir.[806] MLDI'ya göre aracı platformlar, sadece mahkeme kararının veya yetkili bir makam tarafından alınan içeriğin kaldırılması veya engellenmesi kararının gereğini yerine getirmemeleri durumunda, barındırdıkları içerikten dolayı sorumlu tutulabilirler.[807] Keza, sorumluluğun doğabilmesi için en azından tartışmalı

[802] *Tamiz v. Birleşik Krallık*, para. 71.
[803] *Tamiz v. Birleşik Krallık*, para. 71.
[804] *Tamiz v. Birleşik Krallık*, para. 72.
[805] *Tamiz v. Birleşik Krallık*, para. 72.
[806] *Tamiz v. Birleşik Krallık*, para. 73.
[807] *Tamiz v. Birleşik Krallık*, para. 73.

içeriği kaldırmama veya engellememenin hukuki bir sorumluluğa yol açacağının açıkça belirtilmiş olması gerekir.[808]

3. Article 19

Article 19 isimli sivil toplum örgütü, bloglara ve internet ortamındaki yorumların niteliğine dikkat çekmiştir ve yorumların yayımlanmasının çoğu zaman başkalarının itibarına önemli bir zarar verme imkânının kısıtlı olduğunu belirtmiştir.[809] Bu bağlamda Article 19'a göre, bir içeriğin kaldırılmasına yönelik talepte bulunabilmesi için zararın önemli ve ciddi seviyede olması gerekmektedir.[810] İç hukukta böyle bir kriter aramak suretiyle, AİHS'nin 8. maddesince korunan itibar hakkına yönelik gerçek bir ihlal olması durumunda kişiye hak arama imkânı verilerek sistemin kötüye kullanılması engellenecek ve genel olarak AİHM'nin içtihatlarıyla uyumlu bir durum ortaya çıkacaktır.[811]

V. AİHM'nin tespit ve değerlendirmeleri

Başvuruyu esastan inceleyen AİHM, öncelikle AİHS'nin 8. maddesinde güvence altına alınan özel hayata saygı gösterilmesini talep hakkına ve ihlalin belirli bir seviyede olmasına ilişkin önceki içtihatlarını alıntılamıştır.[812] Mahkemeye göre, bir kişinin şahsi onuru ve itibarına saldırı belirli bir ciddiyet seviyesine ulaşmalı ve kişinin özel hayatına ilişkin haklarını kullanmasına halel getirecek nitelikte olmalıdır.[813] Article 19'un tespitlerine çapraz atıf yapan AİHM, internet ortamında kişilere rahatsızlık oluşturan çok fazla sayıda içerik bulunsa da bunların çoğunun önemsiz nitelikte olduğunu veya çok kısıtlı şekilde yayımlandığını ve başkalarının itibarına önemli bir zarar oluşturmaktan uzak olduğunu belirtmiştir.[814]

---

[808] *Tamiz v. Birleşik Krallık*, para. 74.
[809] *Tamiz v. Birleşik Krallık*, para. 75.
[810] *Tamiz v. Birleşik Krallık*, para. 76.
[811] *Tamiz v. Birleşik Krallık*, para. 76.
[812] *Tamiz v. Birleşik Krallık*, para. 77-79.
[813] *Tamiz v. Birleşik Krallık*, para. 80.
[814] *Tamiz v. Birleşik Krallık*, para. 80.

Somut olaydaki yorumların söz konusu eşiği aşıp aşmadığını inceleyen AİHM, yerel mahkemelerin genel tespitlerine katılarak yorumların söz konusu ciddiyet seviyesini karşılamadığını belirtmiştir.[815] Ayrıca, Mahkemeye göre bu başvurunun özü, başvurucunun AİHS'nin 8. maddesinde tanınan haklarını korumak için başvurabileceği hiçbir önlem olmamasıyla ilgili değildir.[816] Başvurucu; yorumların yazarlarına, "London Muslim" blog sayfasının yazarına veya Google Inc. şirketine dava açabilecekken talebini sadece Google Inc. şirketine yöneltmiştir.[817] Keza, yerel mahkemeler de Google Inc. şirketinden talepte bulunulmasını ilkesel olarak reddetmemiş; sadece, somut olayda gerçek ve esaslı bir haksız fiilin niteliklerinin oluşmadığını tespit etmiştir.[818] Ayrıca, yerel mahkemelere göre, Google Inc. şirketinin sorumluluğu; yorumların yayımlanması ve içeriklerin hakaret niteliğinde olduğu konusunda bilgilendirilmesinin üzerinden makul bir süre geçtikten sonra söz konusu olacaktır.[819]

AİHM'ye göre yerel mahkemelerin yaklaşımı, tamamen uluslararası hukuka uyum gözetmek amacıyladır.[820] Avrupa Konseyi, Avrupa Birliği, Birleşmiş Milletler ve OECD'nin muhtelif düzenlemelerine ve kararlarına atıf yapan AİHM, bilgi toplumu hizmet sağlayıcılarının, üçüncü taraflara ait içeriklerden söz konusu içerikleri hukuka aykırılıklarının farkına varmaları üzerine derhâl kaldırdıkları veya bunlara erişimi kısıtladıkları takdirde sorumlu tutulamayacağını vurgulamıştır.[821] Benzer şekilde, Avrupa Birliği e-Ticaret Direktifi'ne atıfta bulunan AİHM, üye devletlerin, bilgi toplumu hizmet sağlayıcılarına genel bir içerik kontrolü veya hukuka aykırı aktiviteyi takip etme yükümlülüğü getirmemesi gerektiğini hatırlatmıştır.[822]

---

[815] *Tamiz v. Birleşik Krallık*, para. 81.
[816] *Tamiz v. Birleşik Krallık*, para. 82.
[817] *Tamiz v. Birleşik Krallık*, para. 82.
[818] *Tamiz v. Birleşik Krallık*, para. 82.
[819] *Tamiz v. Birleşik Krallık*, para. 83.
[820] *Tamiz v. Birleşik Krallık*, para. 84.
[821] *Tamiz v. Birleşik Krallık*, para. 84.
[822] *Tamiz v. Birleşik Krallık*, para. 84.

Yukarıda belirtildiği üzere başvurucu, genel olarak *Delfi AS v. Estonya* kararına atıf yapmıştır.[823] AİHM, *Delfi AS v. Estonya* kararındaki içtihadını tekrarlamıştır. *Delfi AS* kararının konusunu büyük ölçekli, ticari amaçla işletilen, hem haber yayımlayan hem de kullanıcıları bu haberlere yorum yapmaya davet eden bir portal oluşturmaktadır. AİHM, bu kararın, sosyal medya platformları gibi herhangi bir içerik sunmayan sosyal medya siteleri ile içerik sağlayıcısının bir web sitesini veya blog sitesini hobi amaçlı işlettiği diğer internet mecralarına uygulanamayacağına dikkat çekmiştir.[824]

AİHM, yerel mahkemelerin başvurucunun itibarının korunmasına ilişkin haklarıyla Google Inc. şirketi ve son kullanıcıların ifade özgürlüğü haklarını açıkça dengelemeye ilişkin bir inceleme yapmadığının farkındadır.[825] AİHM'ye göre bunun temel nedeni, başvurucunun yerel mahkemeler nezdinde bu hususu dile getirmemesi ve istinaf ile temyiz aşamasında ise bunun usulen mümkün olmamasıdır.[826]

Buna rağmen AİHM konunun esasını tekrar incelemiş ve "*gerçek ve esaslı bir haksız fiil*" testinin, özünde AİHS'nin 8 ile 10. maddeleri arasında bir dengeleme amacı güttüğünü belirtmiştir.[827] Keza, yerel mahkemelerin kıyas yoluyla *Delfi AS* kararının kriterlerini uyguladığını ifade etmiştir.[828] Başvurucu ise, aksine, ilgili usul kurallarıyla ispat külfetine ilişkin gerekliliklerı yerine getirmemiştir.[829] Bu doğrultuda Mahkeme, yerel mahkemelerin gerekli dengeleme testini yaptığına ikna olmuş, verdikleri kararın gerekçelerinin ilgili ve yeterli olduğuna hükmetmiştir.[830]

Tüm bu tespitler ışığında ve özellikle Google Inc. gibi bir bilgi toplumu hizmet sağlayıcısının bilgiye ve politik, sosyal, kültürel tartışmalara erişimi kolaylaştırma konusunda oynadığı önemli rolü dikkate alarak

[823] *Tamiz v. Birleşik Krallık*, para. 85.
[824] *Tamiz v. Birleşik Krallık*, para. 85.
[825] *Tamiz v. Birleşik Krallık*, para. 86.
[826] *Tamiz v. Birleşik Krallık*, para. 86.
[827] *Tamiz v. Birleşik Krallık*, para. 87.
[828] *Tamiz v. Birleşik Krallık*, para. 87.
[829] *Tamiz v. Birleşik Krallık*, para. 88.
[830] *Tamiz v. Birleşik Krallık*, para. 89.

AİHM, Birleşik Krallık devletinin mevcut davadaki takdir marjının geniş olduğunu tespit etmiştir.[831] Mahkeme, yerel mahkemelerin incelemelerini ve değerlendirmelerini yeterli görmüştür. AİHM, yerel mahkemelerin yerindelik konusunda takdir yetkisinin sınırları içinde kaldıklarına ve başvurucunun AİHS'nin 8. maddesinde korunan özel hayatına saygı hakkıyla Google Inc. şirketi ve son kullanıcıların AİHS'nin 10. maddesinde güvence altına alınan ifade özgürlüğü hakları arasında adil bir dengenin kurulduğuna karar vermiştir.[832] Netice olarak, açıkça dayanaksız olduğundan bahisle başvurucunun AİHS'nin 8. maddesi bağlamındaki başvurusunun reddedilmesine hükmetmiştir.[833] Keza, AİHS'nin 13. maddesinde güvence altına alınan etkili başvuru hakkının da ihlal edilmediğine karar vermiştir.[834] Sonuç olarak, başvuruyu kabul edilmez bulmuştur.

VI. Değerlendirme

AİHM'nin *Tamiz v. Birleşik Krallık* kararı, bilgi toplumu hizmet sağlayıcısı statüsünde olan Google Inc. şirketinin üçüncü kişilerin içeriklerinden dolayı sorumluluğuna ilişkin usul ve esasları ortaya koymuştur. Önceki içtihatlarıyla paralel karar veren Mahkemeye göre, aracı platformların sorumluluğuna gidilebilmesi için bunların hukuka uygun şekilde bilgilendirilmesi ve hukuka aykırılığın tespitinden sonra söz konusu içeriğin makul sürede kaldırılmaması gerekmektedir.

Bu kararın en önemli çıktısı, internete müdahaleye dayanak teşkil eden mevzuatta hukuki belirliliğin sağlanmış olmasının önemidir.[835] İngiliz Mahkemelerinin çatışan hak ve menfaatleri kapsamlı şekilde tartmış ve müdahalenin gerekliliği konusunda tatmin edici nitelikte bir değerlendirme yapmış olmaları AİHM'nin kararının da belirleyici faktörü olmuştur.

---

831 *Tamiz v. Birleşik Krallık*, para. 90.

832 *Tamiz v. Birleşik Krallık*, para. 90.

833 *Tamiz v. Birleşik Krallık*, para. 91.

834 *Tamiz v. Birleşik Krallık*, para. 92-93.

835 Bu yönde bkz. **Dinwoodie, Graeme B** (2017). *A Comparative Analysis of the Secondary Liability of Online Service Providers*, Cham, Springer, s. 44.

Tamiz v. Birleşik Krallık davasında *Delfi AS v. Estonya* kararı tekrar gündeme gelmiştir. AİHM'nin bu karardaki çıkmazı da yine *Delfi AS* kriterlerinin neden uygulanamayacağını açıkladığı noktada olmuştur. Tekrar etmek gerekirse, AİHM'nin yorumuyla *Delfi AS* kararının konusunu büyük ölçekli, ticari amaçla işletilen, hem haber yayımlayan hem de kullanıcıları haberlere yorum yapmaya davet eden bir portal oluşturmaktadır. AİHM'ye göre bu karar, sosyal medya platformları gibi herhangi bir içerik sunmayan sosyal medya siteleri ile içerik sağlayıcısının bir web sitesini veya blog sitesini hobi amaçlı işlettiği diğer internet mecralarına uygulanmamaktadır

AİHM, her kararında *Delfi AS* kararındaki bu kriterleri tekrarlayarak objektif bir kriter geliştirdiğini ortaya koymaya çalışmaktadır. Hâlbuki AİHM, sübjektif bir kriter geliştirmiştir. Sosyal medya platformlarını sorumluluk açısından kapsam dışında bırakırken temelde kullanıcı yorumları bakımından yer sağlayıcı niteliğinde olan haber portallarını sorumluluk kapsamına almaktadır. Keza, bireysel blogları kapsam dışında bırakarak kriterini daha belirsiz hâle getirmektedir. *Tamiz v. Birleşik Krallık* sonrasındaki kararlarda da benzer tartışmalar tekrar alevlenmiş ve AİHM bu konudaki çelişkileri gideremiştir.

§17. M.L. VE W.W. V. ALMANYA

AİHM'nin 28 Haziran 2018 tarihli *M.L. ve W.W. v. Almanya* kararı, unutulma hakkının AİHM tarafından ilk defa açıkça ele alındığı karar olması sebebiyle önemlidir.[836] AB Adalet Divanının *Google v. İspanya* kararına da muhtelif atıflar içeren bu karar, unutulma hakkının AİHS bağlamındaki hukuki dayanağı ve kapsamını görmek açısından üzerinde durulması gereken bir karardır.

I. Davanın gelişimi

AİHM'nin *M.L. ve W.W. v. Almanya* kararı, M.L. ve W.W. isimli iki Alman vatandaşının başvurularının birleştirilmesiyle verilmiş bir karardır. Başvurunun temel konusunu, M.L. ve W.W.'nin, ceza mahkûmiyetlerine ilişkin bilgilerin bazı medya kuruluşlarına ait (Spiegel online, Deutschlandradio ve Mannheimer Morgen) internet sitelerinden kaldırılmasına yönelik taleplerinin Alman Federal Mahkemesi tarafından reddedilmesi sebebiyle AİHS'nin 8. maddesi bağlamında haklarının ihlal edildiği iddiası oluşturmaktadır. Başvurucular M.L. ve W.W. üvey kardeşler olup 1991 yılında W.S. isimli bir aktörü öldürmeleri sebebiyle ömür boyu hapse mahkûm edilmişlerdir.[837] Muhtelif temyiz girişimleri başarısızlıkla sonuçlanmıştır. Sırasıyla 2007 ve 2008 yıllarında şartlı salıverilmişlerdir.

M.L. ve W.W., çeşitli mecralarda kendileriyle ilgili yayımlanan içeriklerin kaldırılması veya en azından içeriklerde isimlerinin anonim hâle getirilmesi için girişimlerde bulunmuşlardı. Çeşitli ilk derece ve temyiz mahkemelerinde her bir taleplerine ilişkin kararlar verilmiştir.

---

[836] **AİHM**, *M.L. ve W.W. v. Almanya*, Başvuru No: 60798/10 ve 65599/10, 28.6.2018.

[837] *M.L. ve W.W. v. Almanya*, para. 7.

A. Birinci talep ve yargılama

14 Temmuz 2000 tarihinde, *Deutschlandradio* isimli radyo istasyonunda "W.S. 10 yıl önce öldürüldü" başlıklı bir haber yayımlanmış ve rapor içeriğinde katil zanlısı olarak M.L. ve W.W.'nin isimlerine yer verilmiştir.[838] Bu rapor, söz konusu radyonun internet sitesinin arşiv kısmında en azından 2007 yılına kadar yayında kalmıştır.[839]

2007 yılında başvurucular, radyo istasyonu aleyhine Hamburg Bölge Mahkemesinde dava açarak kendileriyle ilgili içeriklerin anonim hâle getirilmesini talep etmiştir.[840] 29 Şubat 2008 tarihinde, Bölge Mahkemesi talebi yerinde görmüştür. Mahkeme, başvurucuların, mahkûmiyetlerinden çok uzun süre sonra fiilleriyle artık karşılaşmama konusundaki menfaatlerinin kamunun başvurucuların söz konusu olaylara dahli hakkında bilgilendirilme menfaatinden ağır bastığına hükmetmiştir.[841]

Hamburg İstinaf Mahkemesi, 29 Temmuz 2008 tarihli iki kararıyla ilk derece mahkemesinin kararını onamış ve eski haber içeriklerinin başvurucuların kişilik haklarını ihlal ettiğine hükmetmiştir.[842] Hamburg İstinaf Mahkemesi, bu kararını başvurucuların topluma tekrar entegre olma haklarını da gözeterek vermiştir. Mahkemeye göre, yargılama neticesinde hüküm giydirilerek toplum tarafından gerekli yaptırım uygulanmış ve toplum dava konusunda yeterince bilgi sahibi olmuştur.

Hamburg İstinaf Mahkemesi, radyo istasyonunun ifade özgürlüğünün zedelenip zedelenmediği sorununu da ele almıştır. Mahkemeye göre, radyo istasyonunun ifade özgürlüğüne müdahale asgari seviyede kalmıştır zira içeriğin yayımlanması/yayılması yasaklanmamış, sadece başvurucuların isminin zikredilmesi kısıtlanmıştır.[843]

---

[838] *M.L. ve W.W. v. Almanya*, para. 10.
[839] *M.L. ve W.W. v. Almanya*, para. 11.
[840] *M.L. ve W.W. v. Almanya*, para. 12.
[841] *M.L. ve W.W. v. Almanya*, para. 12.
[842] *M.L. ve W.W. v. Almanya*, para. 14.
[843] *M.L. ve W.W. v. Almanya*, para. 14.

Hamburg İstinaf Mahkemesi, kapsamlı bir karar vermiş ve internet ortamında içerik yayımlanmasının neticeleri konusunu neredeyse tüm boyutlarıyla mütalaa etmiştir.[844] Mahkeme tarafından vurgulandığı üzere, bir içerik internet ortamında yayımlanmasıyla birlikte artık daimî surette bu ortamda yer almakta ve içeriğin eski veya yeni tarihli olması bu neticeyi değiştirmemektedir. Öyle ki anonimlik talep eden bir kişi için içeriğin eski veya yeni bir tarihte yayımlanması arasında fark yoktur. Meseleyi bir mahkûmun sosyalleşmesi, tekrar topluma kazandırılması konusun bağlamında da tartışan Temyiz Mahkemesi; bir komşusu, işvereni veya iş arkadaşının, başvuruculların isimlerini inceleyerek cinayete karıştıklarına ilişkin eski haberlerin daha fazla yayılmasına sebep olabileceğini ve bunun da başvuruculların yeniden sosyalleşmesini tehlikeye uğratacağını belirtmiştir.

Hamburg İstinaf Mahkemesi, radyo istasyonunun başvuruculların haklarına müdahaleden dolayı sorumlu olduğunu ve içeriğin sadece dijital arşivlerde yer alıyor olmasının bu bağlamda sorumsuzluk için geçerli bir gerekçe olmadığı düşüncesindedir.[845] Mahkemeye göre, arşiv içeriğine, radyo istasyonunun web sitesindeki diğer içeriklerle aynı şekilde erişilebilmektedir. İstinaf Mahkemesi, içerikte kişi bilgilerinin anonim hâle getirilmesinin tarihî gerçekliği tahrif etmek değil, sadece rapordaki bir detayı çıkarmak anlamına geldiği kanaatindedir.

Radyo istasyonu, kararı temyiz etmiş ve Federal Mahkeme, 15 Aralık 2009 tarihli kararıyla temyiz başvurusunu yerinde görerek İstinaf Mahkemesi ile Bölge Mahkemesinin kararlarını iptal etmiştir.[846] Federal Mahkeme, davaya konu olan içeriğin başvuruculların kişilik hakları ile mahremiyetlerinin korunması haklarına bir müdahale niteliğinde olduğu ve AİHS'nin 8. maddesi kapsamına girdiği tespitini yapmıştır. Bu tespitten sonra bir hatırlatma yaparak, kişilik hakları ile mahremiyet haklarının AİHS'nin 10. maddesinde güvence altına alınan ifade özgürlüğü ve basın özgürlüğü ile dengelenmesi gerektiğini belirtmiştir.[847] Federal Mahkeme,

[844] *M.L. ve W.W. v. Almanya*, para. 15.

[845] *M.L. ve W.W. v. Almanya*, para. 16.

[846] *M.L. ve W.W. v. Almanya*, para. 18.

[847] *M.L. ve W.W. v. Almanya*, para. 18.

kişilik haklarının hangi kapsamda korunacağının önceden tanımlanmadığını ve bu tür bir dengeleme için somut olayın özellikleri ile AİHS'de korunan hakların beraber dikkate alınması gerektiğini belirtmiştir.

Federal Mahkeme, radyo istasyonunun ifade özgürlüğü ve kamunun bilgi alma hakkının İstinaf Mahkemesi tarafından gereğince ele alınmadığı düşüncesindedir.[848] Federal Anayasa Mahkemesinin bu konudaki içtihatlarına atıf yapan Federal Mahkeme, ceza mahkûmiyetine ilişkin bilgilerin aktüel bir konu olduğunu ve medyanın bu konuda haber yapma sorumluluğunun bulunduğunu belirtmiştir.[849] Mahkemeye göre, bir dava sıradan bir davanın ötesine geçerse kamunun daha fazla bilgi edinme menfaati söz konusu olur ve kamunun bilgiye erişme hürriyeti, kişisel hakların korunmasına ilişkin menfaatin önüne geçer. Federal Mahkeme, hukuku ihlal eden ve başkalarına zarar verenlerin, sadece cezai yaptırımı değil ayrıca basına konu olacaklarını da öngörmeleri gerektiğini vurgulamaktadır.[850]

Peki, bir suçun faili hüküm giyer ve kamu bu konuda yeterince bilgi sahibi olursa kişinin topluma yeniden entegrasyonu bağlamında kişilik haklarına yönelik tekrar eden müdahale nasıl gerekçelendirilecektir? Federal Mahkeme, bu durumda artık basitçe bir gerekçelendirme yapılamayacağı kanaatindedir.[851] Federal Anayasa Mahkemesinin içtihatları ile AİHM'nin *Österreichischer Rundfunk v. Avusturya*[852] kararına atıf yapan Federal Mahkeme, cezasını çeken kişilerin bile kendi suçlarıyla yüzleşmekten kaçınmaya yönelik mutlak bir hakları olmadığını belirtmiştir.[853] Yine de Federal Mahkeme, bir denge kurulacaksa mevcut haber içeriğinin sunuluş şekli ile yayılma derecesine bakılması gerektiğini belirtmiştir.

Tüm bu tespitlerini somut olaya uygulayan Federal Mahkeme, başvurucuların kişiliklerinin korunması haklarının, radyo istasyonunun

[848] *M.L. ve W.W. v. Almanya*, para. 19.
[849] *M.L. ve W.W. v. Almanya*, para. 19.
[850] *M.L. ve W.W. v. Almanya*, para. 19.
[851] *M.L. ve W.W. v. Almanya*, para. 20.
[852] **AİHM**, *Österreichischer Rundfunk v. Avusturya*, Başvuru No: 35841/02, 7.12. 2006.
[853] *M.L. ve W.W. v. Almanya*, para. 20.

ifade özgürlüğü hakkı ve kamunun bilgilendirilme menfaati karşısında korunacak nitelikte olmadığına hükmetmiştir.[854] Federal Mahkeme, bu hükme içeriğin radyo istasyonunun internet sitesinde sunuluş şeklinden yola çıkarak varmıştır. Federal Mahkeme, başvuruculaın suçlarının cezasını çektiği ve aradan da esaslı bir süre geçtiği gerçeğini yok saymamaktadır. İçeriğin sunuluş şeklini dikkate alan Federal Mahkeme, içeriğin başvuruculaın kişilik haklarını esaslı şekilde etkilemediğini, başvuruculaı her zaman bir ceza boyunduruğu altında bırakacak nitelikte olmadığını, başvuruculaı sabıkalı olarak damgalayacak ve dikkatleri üzerlerine çekecek şekilde olmadığını değerlendirmiştir.

Federal Mahkeme, dava konusu içeriğin ünlü bir aktöre ilişkin gerçek bir cinayete dair olduğunu ve kamunun dikkatini çekme amacı taşıdığını not etmiştir. Haberin sunuluş şekline detaylıca ışık tutan Federal Mahkeme, haberin başvuruculaı suçlu olarak damgalamadığı kanaatini tekrarlamıştır.[855] İçeriğin yayılma derecesini de tekrar ele alan Federal Mahkeme, diğer mecralarla bir kıyaslama yaparak internet sitesinde yer alan içeriğin daha kısıtlı bir kitleye, somut olaydaki bilgiyi arayan internet kullanıcılarına, daha az görünür arşiv sayfalarında eriştirildiği görüşündedir.[856]

Federal Mahkeme, kamunun, mevcut olaylar hakkında bilgilendirilmeye yönelik meşru menfaatinin yanında geçmişteki olayları araştırabilmeye yönelik bir menfaatinin de olduğunu vurgulamıştır.[857] Bu bağlamda, medyanın, eski içerikleri internet kullanıcılarına ulaştırmak da dâhil ifade özgürlüğünü kullanırken kamuyu bilgilendirme ve demokratik fikrin şekillenmesine yardımcı olma görevini yerine getirdiği kanaatindedir.[858] Radyo istasyonunun, kamu hukukuna tabi bir tüzel kişilik olduğunun altını çizen Federal Mahkeme, istasyonun bir misyonunun da arşiv oluşturmak olduğunu belirtmiştir. Federal Mahkeme, battaniye bir yasaklamanın veya suçluların isimlerinin internet arşivindeki raporlardan

[854] *M.L. ve W.W. v. Almanya*, para. 21.
[855] *M.L. ve W.W. v. Almanya*, para. 22.
[856] *M.L. ve W.W. v. Almanya*, para. 23.
[857] *M.L. ve W.W. v. Almanya*, para. 24.
[858] *M.L. ve W.W. v. Almanya*, para. 24.

silinmesinin tarihi silmek ve bu bağlamda suç faillerine tam bir bağışıklık sağlamak anlamına geleceği kanaatindedir. Bu sebeple Federal Mahkeme, suçluların böyle bir hak talep edemeyeceğinin altını çizmiştir.[859]

Federal Mahkeme, başvurucular tarafından talep edilen yasağın, diğer bir deyişle hukuka uygunluğu bakımından herhangi bir değişiklik olmamış arşiv yayınlarını kaldırmanın, ifade özgürlüğü ile basın hürriyeti üzerinde caydırıcı bir etki (*chilling effect*) oluşturacağını ileri sürmüştür.[860] Mahkemeye göre, radyo istasyonlarının eski arşivlerini düzenli olarak kontrol etmekle yükümlü tutulmalarına sebep olacak bir netice, ifade özgürlüğü ile basın hürriyetini gereğinden fazla kısıtlamış olacaktır. Bunun sonucunda, kamunun bu tür bilgilere erişimin korunmasında menfaati olmasına rağmen raporların arşivlenmesinin durdurulması veya ilgili kişilerin isimlerinin yok sayılması gibi bir risk doğacak ve nihayetinde raporlar hukuka aykırı hâle gelecektir.

Federal Mahkeme, son olarak, konuyu kişisel verilerin korunması bağlamında ele almıştır. Federal Mahkemeye göre, kişisel verilerin korunması alanındaki yasal düzenlemeler de aynı hukuki sonuca varılmasını sağlamaktadır.[861] Mahkeme, ihtilaf konusu içeriğin medyaya sunulan istisna kapsamına girdiği görüşündedir. Bunun bir neticesi olarak ilgili kişinin rızasına veya kanunla açıkça öngörülmesi gereken bir hâle ihtiyaç duyulmaktadır. Federal Mahkeme, kişisel veriyi toplama, işleme ve kullanma konusunda ilgili kişilerin rızasına ihtiyaç duyulması durumunda basının ve radyo istasyonlarının gazetecilik faaliyetlerini yerine getiremeyeceğinin altını çizmiştir.[862] Bunların görevinin içeriği internet ortamına göndermekle sınırlı olmadığını, ayrıca internet ortamında sürekli şekilde erişilebilirliği temin etmeyi de kapsadığını belirtmiştir. Bu doğrultuda, radyo istasyonunun başvurusunu yerinde görmüştür. Federal Mahkemenin kararı Federal Anayasa Mahkemesinin önüne götürülmüş, Federal Anayasa Mahkemesi başvuruyu reddetmiştir.[863]

---

[859] *M.L. ve W.W. v. Almanya*, para. 24.

[860] *M.L. ve W.W. v. Almanya*, para. 25.

[861] *M.L. ve W.W. v. Almanya*, para. 26.

[862] *M.L. ve W.W. v. Almanya*, para. 26.

[863] *M.L. ve W.W. v. Almanya*, para. 27.

B. İkinci talep ve yargılama

İkinci talep ve yargılama Der Spiegel dergisine yönelmiştir.[864] Haftalık bir dergi olan Der Spiegel, internet sitesinde "W.S. - ölümüne dövüldü" şeklinde bir dosya yayımlamıştır. Söz konusu dosyaya erişim için ödeme yapılması şartı vardır. Derginin 1992 yılına ait bir sayısında başvurucuların hayatlarına, ailelerine, yaşantılarına ilişkin detaylı bilgiler ve isimleri yer almıştır. Dosyada yer alan iki haberde ayrıca başvurucuları mahkeme salonunda bir gardiyanla ve ikinci başvurucuyu W.S. ile gösteren fotoğraflar yer almaktadır.[865]

Başvurucular, 2007 yılında Der Spiegel'e karşı dava açmak için adli yardıma başvurmuşlarsa da talepleri reddedilmiştir.[866] Benzer bir başvuruyu Hamburg Bölge Mahkemesine yapmışlar ve adli yardım talepleri kabul edilmiştir. Bu doğrultuda açmış oldukları davada Hamburg Bölge Mahkemesi, başvurucuların taleplerini yerinde görmüş, isimlerinin ve fotoğraflarının yer aldığı dosyalara kamusal erişimin kısıtlanmasına karar vermiş ve dergiye talimat göndermiştir.[867] 29 Temmuz 2008 tarihinde Hamburg İstinaf Mahkemesi, Hamburg Bölge Mahkemesinin kararını daha öncekine benzer gerekçelerle onamıştır.[868]

Tıpkı birinci talep gibi ikinci talep de temyiz edilmiştir. Federal Mahkeme, birinci talepte olduğu gibi Der Spiegel'in başvurusunu kabul ederek başvurucuların taleplerini reddetmiştir.[869] Federal Mahkeme, birinci talepteki yaklaşımını muhafaza etmiş ve neredeyse aynı gerekçeyle karar vermiştir.

Federal Mahkeme, ikinci talebin hukukiliğini incelerken de Der Spiegel'in haberi sunuş tarzını detaylı olarak incelemiştir. Federal Mahkemeye göre, dergi, başvurucuları proaktif bir söylemle katil olarak nitelendirmemiş, iddiaları temel alarak cinayetten hüküm giydiklerini ve

[864] *M.L. ve W.W. v. Almanya*, para. 28.
[865] *M.L. ve W.W. v. Almanya*, para. 29.
[866] *M.L. ve W.W. v. Almanya*, para. 30-31.
[867] *M.L. ve W.W. v. Almanya*, para. 32-33.
[868] *M.L. ve W.W. v. Almanya*, para. 34.
[869] *M.L. ve W.W. v. Almanya*, para. 35.

henüz aydınlatılmamış hususların olduğundan bahisle bu konuda nihai kararın okuyuculara bırakıldığını belirtmiştir.[870]

Federal Mahkeme ikinci kriter olarak ise yine içeriğin yayılma derecesini değerlendirmeye almıştır. Mahkeme, içeriğin sadece ödeme yapılması durumunda okunuyor olmasını erişime yönelik bir kısıtlama olarak nitelendirmiştir.[871] Federal Mahkeme, suçluların kendileriyle ilgili bilgilerin veya raporların silinmesine yönelik genel bir kısıtlama talep edemeyeceklerini tekrarlamıştır. Özellikle böyle bir kısıtlamanın kamunun dikkatini çeken önemli bir cinayette söz konusu olamayacağını vurgulamıştır.

Federal Mahkeme, fotoğrafların hukuki durumunu da detaylı olarak ele almıştır.[872] Bu konudaki iç hukuk düzenlemelerine (Telif Hakkı Kanunu gibi) ve içtihatlara atıf yapan Federal Mahkeme, kademeli koruma yaklaşımını uyguladığını belirtmiştir.[873] Buna göre, güncel bir vakıa bakımından önemi olan kişilerin fotoğraflarının yayımlanması durumunda, Telif Hakkı Kanunu'nun madde 23(1)(1) kısmı uyarınca, ilgili kişinin meşru menfaatlerine bir zarar gelmiş olmaması hâlinde fotoğraflarının yayımlanmasında daha toleranslı olması gerekmektedir.[874] Bu bağlamda, bahse konu kişiden rıza alınması yükümlülüğüne bir istisna tanınmamaktadır meğerki önemli güncel bir vakıaya ilişkin bir içerik olsun.[875]

Federal Mahkeme, bu kriterleri ortaya koyduktan sonra onları somut olaya uygulamıştır. Mahkeme, somut olayda başvurucuların fotoğraflarının uygunsuz şekilde kullanılmadığını veya özel alanına izinsiz bir müdahale niteliğinde olmadığını ve fotoğrafların kamuya genel olarak başvurucuları sabıkalı olarak damgalayacak şekilde sunulmadığını belirtmiştir.[876] Federal Mahkeme, bu doğrultuda başvurucuların Telif Hakkı

[870] *M.L. ve W.W. v. Almanya*, para. 36.
[871] *M.L. ve W.W. v. Almanya*, para. 36.
[872] *M.L. ve W.W. v. Almanya*, para. 37.
[873] *M.L. ve W.W. v. Almanya*, para. 37.
[874] *M.L. ve W.W. v. Almanya*, para. 37.
[875] *M.L. ve W.W. v. Almanya*, para. 37.
[876] *M.L. ve W.W. v. Almanya*, para. 38.

Kanunu'nun 23(2) maddesi kapsamında, fotoğrafların yayımlanmasının yasaklanmasında meşru bir menfaatinin olmadığına hükmetmiştir.[877] Birinci talep gibi ikinci talep de Federal Anayasa Mahkemesi önüne getirilmeye çalışılsa da birinci taleple aynı gerekçeyle reddedilmiştir.[878]

C. Üçüncü talep ve yargılama

2007 yılında başvurucular günlük gazete Mannheimer Morgen aleyhine Hamburg Bölge Mahkemesi nezdinde dava açmıştır.[879] Gazetenin internet sitesinin (www.morgenweb.de) "Eski haber içerikleri" kısmında 2001 tarihli bir içerik yer almaktadır ve bu içerik 2007 yılına kadar o kısımda yer almıştır.[880] İçerik sadece üyelere veya belirli içerikleri satın alanların erişimine açıktır. Fakat tüm internet kullanıcılarının haber içeriklerinin başlıklarına genel bir erişimi vardır. 22 Mayıs 2001 tarihli bir içerikte başvurucuların isimleri ve cinayetle ilgili kısa bir haber yer almaktadır.

Başvurucular, bu içerikler için de yasal süreci işletmişlerdir. 16 Kasım 2007 tarihinde Bölge Mahkemesi başvurucuların talebini kabul etmiş, 19 Ağustos 2008 tarihinde Hamburg İstinaf Mahkemesi aynı gerekçelerle kararı onamıştır.[881] 20 Nisan 2010 tarihinde ise Federal Mahkeme, ikinci talepte geliştirmiş olduğu aynı gerekçeyle ilk derece mahkemesi kararlarını bozmuştur.[882] Yine benzer şekilde, 23 Haziran 2010 tarihinde Federal Anayasa Mahkemesi, başvurucuların başvurusunu önceki taleplerle aynı gerekçelerle reddetmiştir.[883]

---

[877] *M.L. ve W.W. v. Almanya*, para. 38.
[878] *M.L. ve W.W. v. Almanya*, para. 39.
[879] *M.L. ve W.W. v. Almanya*, para. 40.
[880] *M.L. ve W.W. v. Almanya*, para. 40.
[881] *M.L. ve W.W. v. Almanya*, para. 41-42.
[882] *M.L. ve W.W. v. Almanya*, para. 43.
[883] *M.L. ve W.W. v. Almanya*, para. 44.

D. Diğer talepler

Başvurucular, farklı gazetelerde (Frankfurter Allgemeine Zeitung gibi) yer alan içerikler için de hukuki süreç başlatmışsa da Federal Mahkeme söz konusu içerikler bakımından kamunun bilgilendirilme menfaatinin azalmadığına hükmetmiştir.[884]

II. Hukuki arka plan

AİHM, *M.L. ve W.W. v. Almanya* kararını incelemeden önce muhtelif Alman iç hukuk düzenlemesi, Avrupa Konseyi düzenlemesi, Avrupa Birliği düzenlemesi ve özellikle de Avrupa Birliği Adalet Divanının unutulma hakkı kararı olarak da bilinen *Google v. İspanya* kararına atıf yapmış ve bunlardan çeşitli alıntılar yapmıştır.[885]

İç hukuk düzenlemelerinden alıntılananlar, Alman Anayasası (The Basic Law), Medeni Kanun ve Telif Hakkı Kanunu'dur. AİHM, Avrupa Konseyinin 108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi ve muhtelif Bakanlar Komitesi tavsiye kararlarına atıf yapmıştır. Avrupa Birliği kısmında ise, 95/46 sayılı AB Direktifi'ne, AB Genel Veri Koruma Tüzüğü'ne atıfta bulunmuş, Madde 29 Çalışma Grubu'nun unutulma hakkıyla ilgili tavsiye kararını ve Avrupa Birliği Adalet Divanının *Google v. İspanya* kararını alıntılamıştır.

III. Tarafların iddiaları

AİHM, iki başvurunun da aynı nitelikte olması sebebiyle birleştirilmesine karar vermiştir.[886] Başvuruculaların temel iddiasına göre, isimlerinin geçtiği arşivlerin internet ortamında yer alması, suçlu olarak damgalanmalarının devam etmesine neden olmaktadır.[887] Alman Federal Mahkemesinin *Lebach* kararına yapılan atfı da eleştiren başvurucular,

---

[884] *M.L. ve W.W. v. Almanya*, para. 45.

[885] *M.L. ve W.W. v. Almanya*, para. 46-63.

[886] *M.L. ve W.W. v. Almanya*, para. 64.

[887] *M.L. ve W.W. v. Almanya*, para. 68.

bir televizyon yayını ile internet yayını arasında mukayese yapılamayacağını, televizyon yayınının bir süre sonra unutulacağını lakin belirli bir olay hakkındaki bilginin özellikle arama motorları aracılığıyla ücretsiz ve hızlı şekilde herhangi bir yerden ve sürekli olarak erişilir olacağını ileri sürmüşlerdir. Bu nedenle bir içeriğin internet ortamında yayılması, özel hayata saygı hakkının sürekli şekilde ihlali anlamına gelecektir.[888]

Başvurucular asıl amaçlarının sosyal ilişkilerine zarar verecek şekilde suçlu olarak damgalanmayı önlemek olduğunu, Federal Mahkemenin haberin anonim hâle getirilmesinin bir bakıma tarihi silmek manasına geldiği görüşünün yersizliğini tartışmışlardır.[889] Benzer şekilde, Federal Mahkemenin ve Alman Hükûmetinin basına arşivleri kontrol etme yükümlülüğü getirilmesinin ifade özgürlüğünü ölçüsüz şekilde kısıtlayacağı şeklindeki görüşünün de temelsiz olduğunu iddia etmişlerdir.[890] Bu görüşlerini, basının, arşiv içeriklerini sürekli düzeltmek zorunda olmadığı, sadece talep durumunda hareket etmesi gerektiği argümanıyla temellendirmeye çalışmışlardır.[891] Ayrıca, burada bir maliyet ortaya çıkarsa bu maliyetin talepte bulunanlara yükletilmesi suretiyle bir denge kurulabileceğini belirtmişlerdir.[892] En önemli iddiaları ise basına yüklenecek bir arşiv düzeltmesi yükümlülüğünün caydırıcı etki (*chilling effects*) oluşturmayacağı, nihayetinde AİHS'de güvence altına alınan iki hakkın dengelenmesi durumunda caydırıcı etki konusunun uygulanamayacağıdır.[893]

Başvurucular, içeriklere yirmi yıl sonra hâlâ erişilebiliyor olmasında toplumsal bir faydanın kalıp kalmadığının da sorgulanması gerektiği görüşündedirler.[894] Arama motorlarının içerikleri eriştirmedeki rolleri ve bu konudaki zorluklar bağlamında internet ortamında mutlak bir anonimlik mümkün olmasa bile anonim kalmaya yönelik taleplerin otomatik

[888] *M.L. ve W.W. v. Almanya*, para. 69.
[889] *M.L. ve W.W. v. Almanya*, para. 70.
[890] *M.L. ve W.W. v. Almanya*, para. 71.
[891] *M.L. ve W.W. v. Almanya*, para. 71.
[892] *M.L. ve W.W. v. Almanya*, para. 71.
[893] *M.L. ve W.W. v. Almanya*, para. 71.
[894] *M.L. ve W.W. v. Almanya*, para. 72.

olarak dışlanmaması gerektiğini tartışmışlardır.[895] Basının, en azından, anonimliği sağlamak amacıyla imkân dâhilindeki her şeyi yapmak zorunda olduğunu ileri sürmüşlerdir. Tüm bunların dışında, iç hukuk yollarını tükettiklerini iddia etmişlerdir.[896]

IV. Alman Hükûmetinin savunması

Alman Hükûmeti, dijital arşivlerin yakın tarihi belgelemeye yardımcı olduğundan bahisle kolektif hafıza için öneminin altını çizmiş ve dijital arşivlerin doğrulanmasına yönelik bir yükümlülüğün ölçüsüz bir müdahale olacağını ileri sürmüştür.[897] Dijital arşivlerin artan büyüklüğünü, ölçüsüzlük iddiasına kanıt olarak göstermiştir.

Alman Hükûmeti, bir arşiv içeriğine müdahale edilebilmesi için somut olaydaki her bir raporun özellikli durumunun ve müdahalenin yarışan haklar üzerindeki etkisinin dikkate alınması gerektiği kanaatindedir.[898] Alman Hükûmetine göre böyle bir inceleme için, gerekli dengeleme testini yapabilecek yetkinlikte kişiler olması gerekir. Alman Hükûmetinin bir diğer itirazı, bu tür bir yükümlülüğün dijital arşivlerin veya kişiselleştirilmiş raporların tamamen ortadan kalkmasına yol açma riskine ilişkindir.[899] Hükûmet, bu alanı düzenlemede devletlerin geniş bir takdir marjı olduğunun altını çizmiştir.[900]

Yukarıda belirtildiği üzere, başvurucular, kişi ismi girildiğinde arama motorlarının kişiyle ilgili tüm sonuçları çok hızlı şekilde erişilebilir kıldığını tartışmıştır. Bu konuya ilişkin olarak Alman Hükûmeti, arama motorları sayesinde internet ortamındaki içeriklere daha hızlı ve pratik şekilde erişilebildiğini, arama motorları olmasaydı içeriği konumlandırmanın büyük bir emek gerektireceğini vurgulamıştır.[901]

---

[895] *M.L. ve W.W. v. Almanya*, para. 73.
[896] *M.L. ve W.W. v. Almanya*, para. 74.
[897] *M.L. ve W.W. v. Almanya*, para. 75.
[898] *M.L. ve W.W. v. Almanya*, para. 76.
[899] *M.L. ve W.W. v. Almanya*, para. 77.
[900] *M.L. ve W.W. v. Almanya*, para. 78.
[901] *M.L. ve W.W. v. Almanya*, para. 79.

Alman Hükûmeti, internet hukuku bağlamında önemli bir soruna da işaret etmiştir: içeriklerin ve paydaşların çokluğu. Nihayetinde bir içerik internet ortamına koyulduktan sonra arama motorları tarafından kopyası alınmakta ve içerik kaynak sitesinde silinse bile bir kopyası farklı mecralarda var olmaya devam etmektedir. Alman Hükûmeti, bu nedenle, içeriğin silinmesi için birçok paydaşa başvurulmasının gerekli olduğuna işaret etmiştir.[902]

İçeriğin hukukiliğine yönelik eleştiriye de yanıt veren Alman Hükûmeti, başvuruculların topluma yeniden entegre olmalarını meşru bir hak olarak kabul etmekle birlikte, Federal Mahkemenin yarışan hakları gereğince tartıştığını belirtmiştir.[903] Alman Hükûmeti, ayrıca başvuruculların olayı medyanın gündemine tekrar taşıyarak olaya güncellik kazandırdığının altını çizmiş, fotoğrafların hukuka uygun şekilde ve tarafsız bir formatta yayımlandığını tartışmıştır.[904] Davaya müdahil olan üçüncü taraflar da benzer tartışmaları yapmıştır.[905]

V. AİHM'nin tespit ve değerlendirmeleri

A. Genel olarak

Konunun esasına giren AİHM, öncelikle "özel hayat" kavramını nasıl tanımladığına ilişkin yerleşik içtihatlarını tekrarlamıştır. Mahkeme, özel hayatın tahdidî olarak tanımlanamayacak geniş bir kavram olduğunu, kişinin maddi ve manevi varlığına yönelik çok farklı unsurları içerdiğini belirtmiş ve bu kavramın, kişisel bilgilerin rıza olmaksızın yayımlanmamasını talep etmeye yönelik meşru bir beklentiyi kapsadığını tekrarlamıştır.[906]

---

[902] *M.L. ve W.W. v. Almanya*, para. 79.

[903] *M.L. ve W.W. v. Almanya*, para. 80.

[904] *M.L. ve W.W. v. Almanya*, para. 81-82.

[905] *M.L. ve W.W. v. Almanya*, para. 83-85.

[906] *M.L. ve W.W. v. Almanya*, para. 86.

Mahkeme, belirli bir bireye ilişkin verilerin derlenmesi, kişisel verilerin işlenmesi veya kullanılması yahut söz konusu materyalin öngörülebilir olanın ötesinde bir şekilde veya derecede yayımlanması durumunda, özel hayatla ilgili endişelerin ortaya çıktığını yinelemiştir. AİHM, bu durumda kişisel verinin korunmasının AİHS'nin 8. maddesinde de güvence altına alındığı üzere kişinin özel hayatına ve aile hayatına ilişkin haklarını kullanması bakımından ciddi önem arz ettiğine ilişkin içtihadına atıf yapmıştır.[907] AİHM, söz konusu içtihadında AİHS'nin 8. maddesinin bir nevi bilgisel selfdeterminasyon imkânı tanıdığını, bireylerin nötr olarak da olsa toplanan, işlenen ve toplu olarak yayılan verilere ilişkin mahremiyet haklarına dayanmalarına ve AİHS'nin 8. maddesindeki haklarının bu tür form ve şekilde gündeme gelmesine izin verdiğini karara bağladığını hatırlatmıştır.[908]

AİHM, 8. maddenin uygulanma koşullarının sınırlarının altını tekrar çizmiştir. Mahkemeye göre, 8. maddenin gündeme gelebilmesi için kişinin şahsına yönelik saldırı belirli bir ağırlığa ve kişinin özel hayatına saygı hakkını kullanmasına halel getirecek bir niteliğe ulaşmalıdır.[909] Aynı şekilde, bir suç işlenmesi gibi kişinin kendi eylemlerinin öngörülebilir bir neticesi sebebiyle 8. maddeye dayanılması da mümkün değildir.[910]

AİHM, mevcut ihtilafın, başvuruculların AİHS'nin 8. maddesinde güvence altına alınan özel hayata saygı hakları ile radyo istasyonunun, yayıncıların ve kamunun AİHS'nin 10. maddesiyle koruma altına alınan ifade özgürlüğü hakları arasında makul bir denge sağlanıp sağlanmadığına ilişkin olduğunu belirtmiştir.[911] Mahkeme, bu dengenin incelenmesinde devletlerin pozitif yükümlülüklerinin, basının demokratik bir toplumda oynadığı rolün, kamunun bu tür bilgiye erişmedeki menfaatlerinin dik-

---

[907] *M.L. ve W.W. v. Almanya*, para. 87; İlgili içtihat için bkz. **AİHM**, *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland*, Başvuru No: 931/13, 27.06. 2017.

[908] *M.L. ve W.W. v. Almanya*, para. 87.

[909] *M.L. ve W.W. v. Almanya*, para. 88.

[910] *M.L. ve W.W. v. Almanya*, para. 88; Bu konuda ayrıca bkz. **AİHM**, *Axel Springer AG v. Germany*, Başvuru No: 39954/08, 7.02. 2012.

[911] *M.L. ve W.W. v. Almanya*, para. 89.

kate alınması gerektiğine değinerek bu konudaki muhtelif içtihatlarına atıf yapmıştır.[912]

AİHM, basının birinci fonksiyonunun kamuyu bilgilendirmek olduğunu belirttikten sonra basının ikinci ve önemli bir fonksiyonunun ise daha önce yayımlanmış haberlerin arşivlerini tutmak ve bu arşivleri kamu için erişilebilir kılmak olduğunu vurgulamıştır.[913] Bu tespitten sonra internet arşivlerinin önemine değinmiştir. AİHM, internet arşivlerinin haberlerin ve bilgilerin muhafaza edilmesi ve kullanılabilir hâle getirilmesi konusundaki esaslı katkısının altını çizmiş, bu arşivlerin bilhassa kamu tarafından hızlıca erişilebilir ve genel olarak ücretsiz olması sebebiyle eğitim ve tarihsel araştırma için önemli bir kaynak oluşturduğunu belirtmiştir.[914]

AİHM, internet sitelerinin bilgiye erişim ve haberleşme aracı olduğunun, bilgiyi muhafaza etme ve iletme kapasitesi bakımından basılı medyadan farklı bir nitelik arz ettiğinin ve internet ortamı üzerindeki içerik ve iletişimin başta özel hayatın gizliliği olmak üzere temel hak ve özgürlükler üzerinde oluşturduğu zarar riskinin bilhassa arama motorlarından dolayı geleneksel basının oluşturduğundan açıkça daha yüksek olduğunun altını çizmiştir.[915]

AİHM, devletlerin AİHS'nin 8 ve 10. maddeleri bağlamındaki yükümlülüğüne, genel olarak kendi yetkilerine, yarışan hakların nasıl dengelenmesi gerektiğine ilişkin genel kurallarına atıf yapmıştır.[916] Özellikle yarışan hakların nasıl dengeleneceğine ilişkin geliştirdiği kriterleri tekrarlamıştır. Bu kriterler şöyledir: tartışmanın kamusal menfaate katkısı, ilgili kişinin bilinirliğinin derecesi, haber içeriklerinin konusu, ilgili kişinin önceki davranışları, yayının içeriği, şekli ve sonuçları, fotoğrafların hangi koşullarda alındığı.[917]

---

[912] *M.L. ve W.W. v. Almanya*, para. 89.

[913] *M.L. ve W.W. v. Almanya*, para. 90.

[914] *M.L. ve W.W. v. Almanya*, para. 90.

[915] *M.L. ve W.W. v. Almanya*, para. 91.

[916] *M.L. ve W.W. v. Almanya*, para. 92-94.

[917] *M.L. ve W.W. v. Almanya*, para. 95.

B. Kriterlerin somut uyuşmazlığa uygulanması

Oluşturduğu kriterleri somut uyuşmazlığa uygulayan AİHM, başvurucular hakkındaki içeriklerin internet ortamında kolayca bulunabilmesinin temel nedeninin arama motorları olduğunu ve arama motorlarının varlığının başvuruya konu içerikleri daha görünür kıldığını belirtmiştir.[918] Akabinde Mahkeme, içeriği görünür/bulunur kılma özelliği sebebiyle arama motorunun sorumluluğunun, içeriği ilk elden yayımlayandan farklı olabileceği tespitini yapmıştır.[919] Avrupa Birliği Adalet Divanının *Google v. İspanya* kararına atıf yapan AİHM'ye göre, tehlikede olan menfaatlerin dengelenmesi, silme talebinin, içeriğin asıl yayımlayıcısına mı yoksa arama motoruna mı yöneltileceğine göre değişik sonuçlara yol açabilecektir. Asıl yayımlayıcının faaliyeti, ifade özgürlüğünün korumaya niyetlendiği değerin merkezinde yer alırken arama motorunun asıl menfaati söz konusu kişiye ilişkin ilk bilgiyi yayımlamak olmayıp özellikle bu kişiyle ilgili mümkün olan tüm bilginin tespit edilmesini kolaylaştırmak ve onunla ilgili bir profil oluşturmaktır.[920]

C. Kamu yararını ilgilendiren bir tartışmaya katkı

Kamu yararını ilgilendiren tartışmanın varlığına ilişkin olarak AİHM, Federal Mahkemenin kamunun bir ceza yargılaması hakkında bilgilendirilmeye ve bu tür bilgileri alabilmeye yönelik menfaati olduğu tespitine katılmıştır.[921] Mahkemeye göre asıl tartışma, içeriklerin ilk aşamada yayımlanması değil, aradan geçen süreden sonra hâlâ yayında olmasının kamusal menfaati ilgilendiren tartışmaya katkı sunup sunmadığına ilişkindir.[922]

AİHM, belirli bir süre geçtikten sonra -özellikle de hapishaneden çıktıktan sonra- topluma yeniden entegrasyon bağlamında hükümlülerin, eylemleriyle tekrar yüzleştirilmemelerine yönelik menfaatleri olduğunu

[918] *M.L. ve W.W. v. Almanya*, para. 97.
[919] *M.L. ve W.W. v. Almanya*, para. 97.
[920] *M.L. ve W.W. v. Almanya*, para. 97.
[921] *M.L. ve W.W. v. Almanya*, para. 98.
[922] *M.L. ve W.W. v. Almanya*, para. 99.

ve kamunun ceza yargılamalarına ilişkin bilgi edinme menfaatinin somut olayın özellikleri dâhil çeşitli faktörlere göre değişiklik göstereceğini kabul etmektedir.[923] AİHM'nin bu yöndeki içtihatlarının istikrarlı olduğu söylenebilir.

Yukarıda belirtildiği üzere Federal Mahkeme başvuruculaın, suçlarıyla tekrar yüzleştirilmeme bakımından esaslı menfaatleri olduğunu kabul etse de kamunun da bu bağlamda olay hakkında bilgilendirilme dışında geçmiş olayları araştırabilmeye yönelik bir menfaati olduğunu kabul etmiştir. Federal Mahkeme, basının, arşivlerinde yer alan eski haber içeriklerini kamusal erişime sunarak demokratik fikrin şekillenmesine katkı sağlama fonksiyonunu yerine getirdiğinin altını çizmiştir. AİHM, Federal Mahkemenin tüm tespitlerine katılmaktadır.[924]

AİHM, basının hem web siteleri hem de dijital arşivler kurmak suretiyle demokratik toplumda oynadığı rolü vurgulayan içtihatlarına tekrar atıf yaparak kamunun erişim hakkı olan bilgiye erişimin kısıtlanmasına yönelik her türlü tedbirin güçlü gerekçeleri olması gerektiğinin altını çizmiştir.[925] AİHM, Federal Mahkemenin, dijital arşivlere yönelik kısıtlamanın ifade özgürlüğü üzerinde caydırıcı etki doğuracağına yönelik tespitlerine de katıldığını belirtmiştir.[926]

AİHM, başvuruculaın, basının arşiv içeriklerini sürekli düzeltmek zorunda olmadığı, sadece talep durumunda hareket etmesi gerektiğine yönelik iddialarını da ele almıştır. Mahkeme, bu iddiaya ilişkin olarak, Federal Mahkemenin işaret ettiği risklerin varlığına katıldığını belirterek bu iddiayı yerinde görmemiştir.[927] Mahkeme, Alman Hükûmeti tarafından ortaya koyulan riskleri de makul görerek, bir içeriğin hukukiliğinin sonradan incelenmesinin tüm menfaatlerin dengelenmesini zorunlu kıldığı ve bunun online arşivlerin veya kişiselleştirilmiş raporların tamamen or-

[923] *M.L. ve W.W. v. Almanya*, para. 100.
[924] *M.L. ve W.W. v. Almanya*, para. 101-102.
[925] *M.L. ve W.W. v. Almanya*, para. 102.
[926] *M.L. ve W.W. v. Almanya*, para. 103.
[927] *M.L. ve W.W. v. Almanya*, para. 104.

tadan kalkmasına yol açma riski taşıdığı görüşüne katılmıştır.[928] AİHM, bu aşamada kamunun bilgiye erişme hakkını yarışan haklar arasında üstün tutmuştur.

Başvuruculların isimlerinin silinmesi yerine anonim hâle getirilmesi konusuna da AİHM benzer şekilde yaklaşmıştır. AİHM, içeriğin silinmesi yerine anonim hâle getirilmesi suretiyle muhafaza edilmesinin ifade özgürlüğüne daha az müdahaleci bir yöntem olduğu konusunda hemfikirdir. Bununla birlikte Mahkeme, içeriğin nasıl haberleştirileceğinin bir gazetecilik faaliyeti olduğunu ve AİHS'nin 10. maddesinin gazetecilere verdiği özgürlük çerçevesinde gazetecilerin haberlerinin güvenilirliğini sağlamak adına mesleklerinin etik kuralları ile davranış kurallarına uydukları sürece neyi nasıl yayımlayacaklarına kendilerinin karar vermesi gerektiğini hatırlatmıştır.[929] Mahkeme ilgili kişinin adı gibi bireyselleştirilmiş bilgilerin , haber raporuna eklenmesinin bir gazetecilik işi olduğu ve bunun özellikle hatırı sayılır derecede dikkat çeken ceza davalarında daha da geçerli olduğu görüşündedir.[930] AİHM, konuyla ilgili farklı basın mecralarındaki muhtelif içerikleri de dikkate alarak yıllar geçmiş olsa da haberlerin kamusal menfaati ilgilendiren tartışmalara katkı sağladığı görüşündedir.[931]

D. İlgili kişinin bilinirliğinin derecesi ve raporun konusu

AİHM, başvuruculların ceza yargılaması sırasında kamuoyu nezdinde bilinir hâle geldiklerini, geçen zaman içerisinde bilinirlikleri azalsa da yeniden yargılama talepleri ve basına yönelik çeşitli bilgilendirmeleri sebebiyle tekrar kamuoyunun gündemine geldiklerini ve haberlerde anonim olmak için başvuru yaptıkları sırada hâlâ aynı durumda olduklarını belirtmiştir.[932] Mahkeme, özellikle yeniden yargılama talepleriyle

[928] *M.L. ve W.W. v. Almanya*, para. 104.
[929] *M.L. ve W.W. v. Almanya*, para. 105.
[930] *M.L. ve W.W. v. Almanya*, para. 105.
[931] *M.L. ve W.W. v. Almanya*, para. 105.
[932] *M.L. ve W.W. v. Almanya*, para. 106.

konunun demokratik bir toplumdaki tartışmaya katkı sunacak niteliğe kavuştuğunu tartışmıştır.[933]

E. İlgili kişinin medyaya yönelik önceki davranışları

AİHM, başvuruculaların yeniden yargılama için gerekli tüm yolları işlettiklerini ve süreci basına da bilgi vererek yürüttüklerini belirtmiştir.[934] Mahkeme, bir kişinin masumiyetini ispat için yapmış olduğu girişimlerden dolayı kınanamayacağını belirtmekle birlikte, başvuruculaların basınla iletişim süreçlerini dikkate alarak, yaptıklarının hukuk yollarını tüketmekten öte olduğunu ileri sürmüştür.[935] Bu sebeple AİHM, başvuruculaların, haber raporlarında anonim olmak veya online mecrada unutulma hakkı talep etmek için sınırlı bir meşru beklentisi olabileceğine hükmetmiştir.[936]

F. Yayının içeriği, şekli ve sonuçları

AİHM; yayının içeriği, şekli ve sonuçlarının da değerlendirmeye alınması gerektiğini belirterek haber içeriğinin ve fotoğrafın yayılma kapsamı, gazetenin ulusal veya yerel olması, geniş veya kısıtlı bir sirkülasyonunun olması gibi faktörlerin önemli olduğunu tekrarlamıştır.[937] Her bir içeriği teker teker değerlendiren AİHM, Alman Federal Mahkemesinin içeriklere yönelik değerlendirmelerini yerinde bulduğunu, yayın içeriğinin ve şeklinin basının ifade özgürlüğünü icrası kapsamında olduğunu belirtmiştir.[938]

Başvurucular, yukarıda belirtildiği üzere, Alman Federal Mahkemesinin televizyon yayınıyla ilgili değerlendirmesinin ve yaptığı karşılaştırmanın internet çağına uygun olmadığını iddia etmişlerdir. AİHM, bu konuyu da değerlendirmiş ve içeriğe Spiegel online örneğinde sadece

[933] *M.L. ve W.W. v. Almanya*, para. 107.
[934] *M.L. ve W.W. v. Almanya*, para. 108.
[935] *M.L. ve W.W. v. Almanya*, para. 109.
[936] *M.L. ve W.W. v. Almanya*, para. 109.
[937] *M.L. ve W.W. v. Almanya*, para. 110.
[938] *M.L. ve W.W. v. Almanya*, para. 111.

ödeme yapanlarca, Mannheimer Morgen örneğinde ise sadece üyeler tarafından erişilebiliyor olmasını bu bağlamda kısıtlı bir erişim olarak nitelendirmiştir.[939]

Başvuruculların tartıştığı bir diğer husus, arama motorlarının içeriğin yayılmasına ve daha fazla görünür olmasına etkisidir. AİHM, başvuruculların, içeriğin daha az görünür kılınması için arama motorlarına bir başvuru yaptıklarına ilişkin bilgi paylaşmadıklarına işaret etmiştir.[940] Mahkeme ayrıca, ifade özgürlüğüne daha az müdahale edecek bir tedbire yönelik yerel mahkemeler nezdinde de bir başvuru yapılmadığını veya bu hususun tartışılmadığını belirtmiştir.[941]

G. Fotoğrafların hangi koşullarda alındığı

AİHM, son olarak, fotoğrafların hukukiliğini ele almıştır. Mahkeme, fotoğrafların hangi koşullarda çekildiğine dair başvurucular ve Alman mahkemeleri tarafından bir bilgi paylaşılmadığını not etmiştir. Fotoğrafların başvuruculların 1994 yılındaki yani salıverilmelerinden on üç yıl önceki hâllerini gösterdiğini dikkate alan Mahkemeye göre, bu durum üçüncü kişilerin fotoğraflardan yola çıkarak başvuruculları tanıma ihtimalini düşürmektedir.[942]

H. Sonuç

AİHM, yukarıda belirtilen tüm tespitler ışığında, çatışan menfaatleri dengelemede yerel makamların sahip olduğu takdir yetkisini, yayını tarihinde hukukiliği tartışma konusu olmayan haber raporlarına erişimin muhafaza edilmesinin önemini ve başvuruculların basına yönelik hareketlerini dikkate alarak Alman Federal Mahkemesinin kararını yerinde görmüştür.[943] Bu doğrultuda, başvuruculların taleplerinin Federal Mahkeme tarafından kabul edilmemesinin Alman Devleti'nin başvuruculların

[939] *M.L. ve W.W. v. Almanya*, para. 112-113.
[940] *M.L. ve W.W. v. Almanya*, para. 114.
[941] *M.L. ve W.W. v. Almanya*, para. 114.
[942] *M.L. ve W.W. v. Almanya*, para. 115.
[943] *M.L. ve W.W. v. Almanya*, para. 116.

özel hayatlarına saygı haklarını korumaya yönelik pozitif yükümlülüğünü ihlal ettiği anlamına gelmediğine ve AİHS'nin 8. maddesinin de bu doğrultuda ihlal edilmediğine hükmetmiştir.

VI. Değerlendirme

AİHM'nin *M.L. ve W.W. v. Almanya* kararı ilk bakışta bir unutulma hakkı kararı gibi gözükse de kararda teknik olarak unutulma hakkına ilişkin derinlemesine bir inceleme yapılmamıştır. AİHM, unutulma hakkına ilişkin Avrupa Birliği Adalet Divanının kararını alıntılasa bile kararın asıl kısmında neredeyse bu kararın çıktılarına tekrar dönüp bir değerlendirme yapmamaktadır. Konu, unutulma hakkının AİHS çerçevesinde sınırlarının ne olduğunu görmek adına uygun bir örnek teşkil etse de Mahkeme, unutulma hakkını ilk kez kurumsallaştırmak adına önemli bir fırsatı kaçırmıştır.

AİHM, konuya demokratik bir toplumda kamusal tartışmaya katkı dar çerçevesinden bakmıştır. İçeriğin sunuluş şekli, basın hürriyeti, kapsamlı bir dengeleme yapılması zorunluluğu gibi unsurlar çerçevesinde bir değerlendirme yapılmıştır. Bu karar, klasik bir basın hakkına müdahale kararının ötesine geçememiştir.

AİHM, klasik medya ve internet medyası arasındaki temel farklılığı ve bunların haklar üzerindeki müdahale etkisini daha iyi şekilde ortaya koyabilirdi. En önemlisi, kişisel verilerin korunması mülahazasıyla artık demokratik toplum düzeninin bir gerekliliği hâline gelmiş olan ve arama motorlarını da yakından ilgilendiren unutulma hakkı yaklaşımı çerçevesinde hem özel hayata saygı hakkının hem de ifade hürriyetinin dengelenmesi mümkün olabilirdi. AİHM, içerik sağlayıcısı konumundaki medya kuruluşlarının içeriği kaynağında düzeltmesini odak noktasına aldığı için hakları gereğince dengeleme konusunda yeni bir yaklaşım geliştirememiştir.

Unutulma hakkı, niteliği itibarıyla hukuka uygun olan içeriğin internet ortamından kaldırılmasını veya bu içeriğe erişimin kısıtlanmasını talep etme hakkıdır. Unutulma hakkını kişilik haklarının korunmasına

ilişkin temel talep hakkından ayıran şey, unutulma hakkının yöneldiği içeriğin internet ortamında bulunmasının hukuki ve meşru bir sebebinin olmasıdır. İçeriğin internet ortamında yayımlanmasının temeli; basın, bilim, sanat faaliyeti veya temel bir ifade özgürlüğü eylemi olabilir.

Temel olarak unutulma hakkı, internet ortamında yer alan içeriğin arama motorlarında listelenmemesini (*de-listing* veya *the right to de-referencing*) talep hakkıdır. Unutulma hakkı, internet ortamı başta olmak üzere her türlü dijital ortamda belirli kişisel verilerin erişime kısıtlanması hakkı olarak ortaya çıkmış istisnai bir hak iken zaman içerisinde genel bir hakka doğru evrilmiştir.

Unutulma hakkının asıl amacı belirli veriyi veya bilgiyi internet ortamında daha az görünür kılmaktır. Öyle ki, mevcut bir sitede veya arama motorunda uygulanan tekniklerle bu amaca ulaşılması mümkündür. Örneğin, robots.txt dosyalarında yapılacak bir ayar sayesinde bir web sitesindeki içeriğin fiilen silinmeden arama motorları indekslerinden çıkartılması pekâlâ mümkündür. Keza, belirli içeriğin teknik olarak genel ziyarete kısıtlanmasıyla da verinin silinmeden daha az görünür kılınması mümkündür.

Avrupa Birliği Adalet Divanının 13 Mayıs 2014 tarihli *Google v. İspanya* içtihadı sayesinde dünyaca bilinirliği artan bu hak, birçok ülke hukukunu etkileyerek güçlü normatif dayanaklar kazanmıştır.[944] AB Veri Koruma Tüzüğü'nde unutulma hakkı açıkça yer bulmuştur. Avrupa Birliği Adalet Divanının yeni kararlarıyla unutulma hakkının kapsamı ve teknik olarak nasıl uygulanması gerektiğine yönelik yeni ilkeler ortaya koyulmaya devam edilmektedir.[945]

Unutulma hakkı, sadece bugünün değil geleceğin de konusudur. Alman Hükûmeti isabetli bir şekilde dijital arşivlerin yakın tarihi belge-

---

[944] **Avrupa Birliği Adalet Divanı**, Case C-131/12, *Google Spain SL & Google Inc. v. Agencia Española de Proteccción de Datos. (AEPD) & Mario Costeja González*, 13.5.2014.

[945] Avrupa Birliği Adalet Divanının güncel kararları için bkz. Case C-136/17, GC, AF, BH, ED v. Commission nationale de l'informatique et des libertés (CNIL), 24 Eylül 2019; Case C-507/17, *Google LLC, successor in law to Google Inc., v Commission nationale de l'informatique et des libertés (CNIL)*, 24.9.2019.

lemeye yardımcı olduğundan bahisle kolektif hafıza için öneminin altını çizmiş ve dijital arşivlerin doğrulanmasına yönelik bir yükümlülüğün, ölçüsüz bir müdahale olacağını belirtmiştir.

Alman Hükûmeti, internet hukuku bağlamında önemli bir soruna da işaret etmiştir: içeriklerin ve paydaşların çokluğu. Nihayetinde bir içerik internet ortamına koyulduktan sonra arama motorları tarafından bir kopyası alınmakta ve kaynak sitesinde silinse bile farklı mecralarda var olmaya devam etmektedir. Unutulma hakkına ilişkin objektif bir kriter geliştirilmez ve hakkın uygulanmasındaki takdir tamamen platformlara bırakılırsa platformlar sorumluluk altına girmemek adına her talebi kabul etme şeklinde bir uygulamaya yönelebileceğinden platform sansürünün oluşması riski vardır.

Unutulma hakkı temel bir hak niteliğindedir.[946] Ancak unutulma hakkının mümkün olduğunca dar şekilde yorumlanması ve üstün kamusal bir yarar olmadığı sürece kullanılmasına izin verilmemesi gerekir. Bu bakış açısıyla, gelecek nesillerin bilgiye erişim haklarına halel getirmeyen, en dengeli yaklaşımın ortaya koyulması gerekir.

Yukarıda belirtilen teknik eleştirilere rağmen AİHM'nin bu dengeyi gözetmesi ve unutulma hakkını dar yorumlaması kararın en önemli çıktısıdır. Ayrıca, klasik verilerin korunması düzenlemelerinin basın faaliyetlerine doğrudan uygulanmasının sakıncalarının da tartışılmış olması bu kararın diğer bir önemli çıktısıdır. Karar, kişisel verilerin korunması düzenlemelerinin basın ve ifade özgürlüğüne ilişkin istisnalarının nasıl yorumlanacağı konusunda yol gösterici olacaktır.[947]

Unutulma hakkı alanındaki düzenlemelerin ifade özgürlüğü, basın özgürlüğü, kamunun bilgiye erişim hakkı ve en önemlisi de gelecek nesillerin bilgiye erişim hakkını dikkate alarak ölçülü ve hakkaniyetli olması

---

[946] Unutulma hakkının insan hakları bağlamında gelişimine ilişkin kapsamlı bir inceleme için bkz. **Sözüer, Eren** (2017) *Unutulma Hakkı - İnsan Hakları Hukuku Perspektifinden Bir İnceleme*, İstanbul, On İki Levha Yayıncılık.

[947] İstisnaların yorumlanması konusunda bkz. **Taştan, Furkan Güven** (2017) *Türk Sözleşme Hukukunda Kişisel Verilerin Korunması*, İstanbul, On İki Levha.

zaruridir. Nihayetinde, bugünün siyasal konjonktürüne göre alınabilecek bir karar, gelecek nesillerin bilgiye erişim hakkını kısıtlayabilecektir.

Unutulma hakkı, internet ortamının dinamikliği, her geçen gün ortaya çıkan yeni teknolojiler ve iş modelleri sebebiyle tartışılmaya devam edecektir. Değerlendirme yapılırken bilgiye erişim bakımından hem mevcut hem de gelecek nesillerin haklarının aynı derecede gözetilmesi hakkaniyetli bir yaklaşım olacaktır.

§18. MAGYAR JETİ ZRT V. MACARİSTAN

AİHM'nin 4 Aralık 2018 tarihinde karara bağladığı *Magyar Jeti Zrt v. Macaristan*[948] kararı, internet hukukunun içerik hukuku alt kırılımında önemli bir tartışma konusu olan başkalarına ait içerikten dolayı sorumluluğa ilişkin bir karardır. Başvurunun özünü, başvurucu şirketin web sitesinde paylaştığı ve hakaret içerikli bir içeriğe yönlendiren bir bağlantı sebebiyle yerel mahkemeler tarafından sorumlu tutulmasının AİHS'nin 10. maddesi bağlamında ifade özgürlüğünü kısıtladığı iddiası oluşturmaktadır.

I. Davanın gelişimi

AİHM'ye başvuru Macar hukukuna göre kurulmuş bir limitet şirket olan Magyar Jeti Zrt tarafından 2016 yılında yapılmıştır. Başvurucu şirket, Macaristan'da 444.hu alan adlı popüler bir online haber sitesini işletmekte, günde yaklaşık 250.000 tekil ziyaretçi almakta, yirmi dört personel ile hizmet sunmakta ve politikadan teknolojiye, spordan popüler kültüre kadar muhtelif konularda günde yaklaşık yetmiş beş haber yayımlamaktadır.[949]

5 Eylül 2013 tarihinde, otobüsle futbol takımının maçına giden bir taraftar grubu Konyár beldesinde bulunan bir ilköğretim okulunun önünde durmuş, ırkçı bazı söylemlerde bulunmuş, öğrencilere tehditler savurmuş ve fiziksel taşkınlıklar sergilemiştir.[950] 8 Eylül 2013 tarihinde, Bay J.Gy. isimli bir yerel yönetici, olayla ilgili açıklama yaparak o dönemde Macar Parlamentosunda üçüncü büyük parti olan Jobbik isimli partiyi suçlayan ifadeler kullanmıştır.[951] Bu röportaj, muhtelif medya organlarında yer almış ve ayrıca YouTube sitesine yüklenmiştir.

---

[948] **AİHM**, *Magyar Jeti Zrt v. Macaristan*, Başvuru No: 11257/16, 4.12.2018.

[949] *Magyar Jeti Zrt. v. Macaristan*, para. 6.

[950] *Magyar Jeti Zrt. v. Macaristan*, para. 7.

[951] *Magyar Jeti Zrt. v. Macaristan*, para. 8.

Başvurucu şirket de 6 Eylül 2013 tarihinde Konyár'daki olay hakkında 444.hu sitesinde, B.H. isimli gazetecinin imzasıyla "*Romanya'ya gitmekte olan futbol taraftarları Çingene öğrencileri tehdit etmek için durdu*" şeklinde bir haber yayımlamıştır.[952] Haber içeriğinde, Bay J.Gy. ile yapılan röportajın YouTube'a yüklendiği de belirtilmiştir. "YouTube'a yüklendi" kelimeleri yeşille gösterilerek YouTube videosuna bir bağlantı olduğuna işaret edilmiştir. Haber içeriği üç defa güncellenmiştir.[953] Başka üç haber sitesi tarafından da aynı YouTube içeriğine bağlantı sağlanmıştır.[954]

13 Ekim 2013 tarihinde, Jobbik Partisi, Macar Medeni Kanunu'nun 78. maddesine dayanarak Debrecen Yüksek Mahkemesi nezdinde Bay J.Gy., Roma Produkciós Iroda Alapítvány, başvurucu şirket ve ilgili videoya bağlantı sağlayan diğer haber siteleri aleyhine dava açmıştır.[955] Jobbik Partisi, futbol taraftarları için Jobbik mensubu denilmesinin ve YouTube'da yer alan videoya bağlantı sağlanmasının itibarını zedelediğini iddia etmiştir.[956]

30 Mart 2014 tarihinde Yüksek Mahkeme, Bay J.Gy.'nin ifadelerinin Jobbik Partisinin Konyár'daki olayda dahli olduğu izlenimi yarattığını belirtmiş ve talebi yerinde görmüştür.[957] Yüksek Mahkeme aynı zamanda hakaret dolu içerikleri yaymaktan dolayı başvurucu Magyar Jeti Zrt şirketinin objektif olarak sorumlu olduğuna karar vermiş; siyasi partinin itibar hakkının ihlal edildiğini belirtmiş; şirketin, mahkeme kararını 444.hu sitesinde yayımlamasına ve YouTube videosuna bağlantıyı siteden kaldırmasına hükmetmiştir.[958]

Başvurucu şirket, "Jobbik" kelimesinin bir siyasi partiden çok Roman karşıtlığını ifade etmek ve bu tür kolektif örgütlenmeleri betimlemek için yaygın olarak kullanılan bir kavram olduğunu, Jobbik Partisinin kamuo-

---

[952] *Magyar Jeti Zrt. v. Macaristan*, para. 9.
[953] *Magyar Jeti Zrt. v. Macaristan*, para. 10.
[954] *Magyar Jeti Zrt. v. Macaristan*, para. 11.
[955] *Magyar Jeti Zrt. v. Macaristan*, para. 12.
[956] *Magyar Jeti Zrt. v. Macaristan*, para. 12.
[957] *Magyar Jeti Zrt. v. Macaristan*, para. 13.
[958] *Magyar Jeti Zrt. v. Macaristan*, para. 13-14.

yunda nefreti ve suçu teşvik eden söylemlerle bilindiğini iddia etmiştir.[959] Ayrıca, içeriğe bağlantı sağlamak suretiyle ifadeleri tekrarlamadığını ve yalan içeriği yaymadığını belirtmiştir. Bu itiraza rağmen Debrecen İstinaf Mahkemesi 25 Eylül 2014 tarihinde, başvurucu şirketin Macar Medeni Kanunu'nun 78. maddesinin ikinci fıkrası uyarınca içeriğin yayılmasından sorumlu olduğuna hükmederek ilk derece mahkemesinin kararını onaylamıştır.[960]

İki davalı, yerel mahkemelerin kararını Macaristan Yüksek Mahkemesi (Kúria) önüne taşımış ve bu kararların basın özgürlüğünü ölçüsüz şekilde kısıtladığını ileri sürmüştür.[961] Macaristan Yüksek Mahkemesi (Kúria) 10 Haziran 2015 tarihli kararında yerel mahkemelerin kararını yerinde görmüş, "jobbikos" kelimesinin günlük konuşma dilinde söz konusu siyasi partiyi ifade edecek şekilde kullanıldığı tespitini yapmış ve başvurucu şirketlerin faaliyetlerinin bilginin yayılması niteliğinde olduğuna hükmetmiştir.[962]

Başvurucu şirket, 1 Aralık 2014 tarihinde Anayasa Mahkemesine bireysel başvuru yapmış ve Medeni Kanun bağlamında basın kuruluşlarının yanlış bilgilerin yayılmasından dolayı üçüncü kişilere ait içeriklerden dolayı objektif olarak sorumlu tutulmasına itiraz etmiştir.[963] Başvurucu şirkete göre bu durumda basın kuruluşu, kamu yararını ilgilendiren dengeli ve tarafsız bir haberden dolayı bile hukuka aykırılıktan sorumlu tutulabilecektir. Bu durumun yayıncılar için aşırı bir külfet oluşturacağını, yayıncıların sadece doğruluğu açıkça tartışmasız olan içerikleri yayımlamak zorunda kalacağını, tartışmalı konularla ilgili haber yapmanın imkânsız hâle geleceğini iddia etmiştir. Başvurucu, yerel mahkemelerin yayıncıların gazetecilik etiği ve meslek kurallarına uygun hareket edip etmediğini değerlendirmeden sadece gerçeğe aykırı ifadelerin yayılıp yayılmadığı perspektifinden dar bir değerlendirme yaptığını belirtmiştir. Başvurucunun en önemli iddiası, bilginin haber değerinin çok kısa ol-

[959] *Magyar Jeti Zrt. v. Macaristan*, para. 15.
[960] *Magyar Jeti Zrt. v. Macaristan*, para. 16.
[961] *Magyar Jeti Zrt. v. Macaristan*, para. 18.
[962] *Magyar Jeti Zrt. v. Macaristan*, para. 19.
[963] *Magyar Jeti Zrt. v. Macaristan*, para. 17.

duğu internet alanında her ifadenin gerçekliğini doğrulamak için zaman olmadığıdır.[964]

Bireysel başvuruyu inceleyen Macaristan Anayasa Mahkemesi, 19 Aralık 2017 tarihinde başvuruyu reddetmiştir.[965] İlk derece mahkemesinin bir içeriğe bağlantı sağlamanın içeriğin yayılması manasına geldiğine yönelik tespitine katılan Anayasa Mahkemesi, içeriği yayanın, üçüncü tarafa ait ifadeyi benimsemese ve açıklamanın gerçekliğine sehven inanmış olsa bile salt içeriği yaymaktan sorumlu olduğunu belirtmiştir.[966]

Anayasa Mahkemesi, haberlere ilişkin önceki içtihatlarına atıf yapmıştır. Mahkemeye göre, toplumsal figürlere ilişkin konuşmaların haberleştirilmesi durumunda eğer ki haber tarafsız ve objektifse, açıklama kamu menfaatini ilgilendiren bir konuya ilişkinse, yayıncı açıklamanın kaynağını belirtmişse ve ilgili kişiye, muhtemel zarar verici açıklamalara yanıt verme olanağı tanındıysa bu tür eylemler içeriği yayma olarak nitelendirilmeyecektir.[967] Mahkemeye göre böyle durumlarda gazeteciler ne kendi ifadelerini ortaya koymuşlardır ne de kamuoyunu kendi düşünceleriyle etkileme niyetine sahiplerdir. Mahkeme, basın içeriğinin editörlerin ve gazetecilerin kendi kararları ve tercihleriyle tanımlandığı durumlardaki sorumluluğu ayrıştırmaya çalışmış ve kamusal tartışmaya ilişkin menfaatin basın toplantılarının doğru şekilde haberleştirilmesini gerektirdiğini vurgulamıştır.[968] Bu tespitlerini mevcut olaya uygulayan Anayasa Mahkemesi, ihtilaf konusu içeriklerin başvurucu şirketlerin kendi ifadelerini içermesi dolayısıyla yayılma (*dissemination*) durumunun oluştuğuna hükmetmiştir.[969]

[964] *Magyar Jeti Zrt. v. Macaristan*, para. 17.
[965] *Magyar Jeti Zrt. v. Macaristan*, para. 20.
[966] *Magyar Jeti Zrt. v. Macaristan*, para. 20.
[967] *Magyar Jeti Zrt. v. Macaristan*, para. 21.
[968] *Magyar Jeti Zrt. v. Macaristan*, para. 21.
[969] *Magyar Jeti Zrt. v. Macaristan*, para. 22.

II. Hukuki arka plan

AİHM, konunun esasına girmeden evvel muhtelif iç hukuk düzenlemelerine, uluslararası belgelere, Avrupa Birliği Adalet Divanının bazı kararlarına ve demokratik toplum düzeninin gerekliliklerini ortaya koymak adına çeşitli ülke düzenlemelerine atıf yapmıştır. İç hukuk düzenlemelerinden Macaristan Anayasası (Fundamental Law),[970] Anayasa Mahkemesi Kanunu[971] ve Medeni Kanun'un[972] başta ifade özgürlüğüne ilişkin olmak üzere ilgili düzenlemelerini alıntılamıştır. Avrupa Konseyinin internete ilişkin 2007 ve basına ilişkin 2011 yılına ait iki Bakanlar Komitesi kararından ve Birleşmiş Milletler alt metinlerinden alıntılar yapmıştır.[973]

AİHM'nin alıntıladığı bir diğer içerik ise Avrupa Birliği Adalet Divanının 8 Eylül 2016 tarihli kararıdır.[974] Bunlar dışında alıntıladığı diğer içtihatlar ise sırasıyla Alman Federal Anayasa Mahkemesinin 15 Aralık 2011 tarihli kararı,[975] Kanada Yüksek Mahkemesinin 2011 yılına ait bir kararı[976] ve Amerika Birleşik Devletleri Temyiz Mahkemesinin 26 Temmuz 2012 tarihli[977] kararıdır.

III. Tarafların iddiaları

Başvurunun özünü, başvurucu şirketin web sitesinde paylaştığı ve hakaret içerikli bir içeriğe yönlendiren bir bağlantı sebebiyle yerel mahkemeler tarafından sorumlu tutulmasının AİHS'nin 10. maddesi bağla-

---

970 *Magyar Jeti Zrt. v. Macaristan*, para. 23.

971 *Magyar Jeti Zrt. v. Macaristan*, para. 24.

972 *Magyar Jeti Zrt. v. Macaristan*, para. 25.

973 İnternetin Kamu Hizmeti Boyutunun Geliştirilmesine Yönelik Önlemlere İlişkin Tavsiye Kararı için bkz. **§6(VIII)**; Yeni Bir Medya Nosyonuna İlişkin Tavsiye Kararı için bkz. **§6(XVI)**.

974 **Avrupa Birliği Adalet Divanı**, Case C-160/15 *GS Media BV v. Sanoma Media Netherlands BV, Playboy Entreprises International Inc., Britt Geertruida Dekker*.

975 **German Federal Constitutional Court**, No. 1 BvR 1248/11 of 15 December 2011.

976 **Supreme Court of Canada**, Crookes v. Newton (2011, SCC 47, [2011] 3.S.C.R. 269).

977 26 July 2012 the United States Court of Appeals for the Third Circuit held in Philadelphia Newspapers, LLC (No. 11-3257, 2012 U.S. App. LEXIS 15419 (3d Cir. July 26, 2012).

mında ifade özgürlüğünü kısıtladığı iddiasıdır. AİHM, başvurucunun iç hukuk yollarını tükettiğine ve başvurunun kabul edilebilir olduğuna karar vermiş, başvuruyu esastan incelemiştir.[978]

Başvurucu şirket, ifade özgürlüğüne müdahalenin kanunla öngörülmediğini, Medeni Kanun'un 78. maddesinin ikinci fıkrasının zararlı yalan içeriklerin yayılmasına yönelik bir sorumluluk getirdiğini fakat bağlantının bilginin yayılması olarak kabul edileceğine ilişkin bir yasal düzenleme veya içtihat bulunmadığını ileri sürmüştür.[979] Aynı doğrultuda, Macar mahkemelerinin kararlarında bağlantı sağlamanın spesifik özelliklerinin dikkate alınmadığını, daha ziyade mevcut içeriğin geleneksel yöntemlerle paylaşılmasına ilişkin standartların olaya uygulandığını, bunun da öngörülebilir bir durum olmadığını iddia etmiştir.[980] Başvurucu şirket, bağlantı sağlamanın, içeriğin kendisini nakletmediği veya iletmediğini, sadece varlığına işaret ettiğini vurgulamıştır.

Başvurucu şirket, bağlantıların çalışmasına yönelik önemli bir teknik hususa işaret etmiştir: Yerel mahkemelerce geliştirilen kriter, bağlantının işaret ettiği web sitesinin içerik sağlayıcısının içeriği değiştirmesi ve orijinalinde yer almayan hakaret barındıran yeni bir içerik oluşturması durumunda dahi şirketin sorumluluğuna yol açacaktır.[981]

Başvurucu şirket, bir siyasi partinin itibarının korunmasının müdahale için meşru kabul edilmesine de itiraz etmiştir.[982] AİHM'nin kendi içtihatlarına vurgu yapan başvurucu şirket, kabul edilebilir kamu denetiminin sınırlarının, eleştiriye daha fazla tolerans göstermesi gereken politikacılar için daha geniş olduğunu belirtmiştir.

Başvurucunun iddiasını temellendirdiği bir diğer dayanak ise müdahalenin demokratik toplumda gerekli olmadığıdır.[983] Başvurucu şirkete göre, yerel mahkemeler, korunan iki değer arasında bir dengeleme yap-

[978] *Magyar Jeti Zrt. v. Macaristan*, para. 33-37.
[979] *Magyar Jeti Zrt. v. Macaristan*, para. 38.
[980] *Magyar Jeti Zrt. v. Macaristan*, para. 39.
[981] *Magyar Jeti Zrt. v. Macaristan*, para. 39.
[982] *Magyar Jeti Zrt. v. Macaristan*, para. 40.
[983] *Magyar Jeti Zrt. v. Macaristan*, para. 41.

mamış; objektif sorumluluk kuralını işletmek suretiyle içeriğin yayılması bağlamında başvurucu şirketin iyi niyet veya kötü niyet çerçevesinde hareket edip etmediğini değerlendirmemiştir.[984]

Başvurucu şirket, bir dengeleme yapılmış olsaydı başvurucu şirketin ifade özgürlüğü hakkının Jobbik Partisinin itibar hakkından üstün tutulacağı görüşündedir.[985] Bağlantı, kamu yararını ilgilendiren dengeli bir haber raporunda yer almıştır.[986] Başvurucu şirkete göre, haber verirken bağlantı sağlamak tamamen basının kendi takdir alanında kalan bir yöntemdir. Bağlantıyı veren gazeteciler, YouTube'da yer alan bilgiyi doğrulamak suretiyle mesleki yükümlülükleri kapsamında hareket etmişlerdir. Kaldı ki Jobbik Partisinin yorumların asıl sahibine dava açma imkânı bulunmaktadır. Keza YouTube videosuna bağlantı vererek erişim sağlamak Jobbik Partisinin itibarına önemli bir etkide bulunmamıştır. Aksine, üçüncü kişilere ait içerikten başvurucu şirketin sorumlu tutulması, basının online gazetecilik içeriği oluşturması noktasında önemli kısıtlamalar doğurmuştur. Bağlantı sağlama durumunda, hakaretten otomatik sorumluluk doğması caydırıcı bir etki oluşturmaktadır. Gazeteciler ile online haber siteleri bu nedenle yayınlarında bağlantı kullanmaktan imtina edeceklerdir. Bu durum, internetin çapraz referans (*cross-referential*) yapısını ve kullanıcıların bilgiye erişimini kısıtlayacaktır.

IV. Macar Hükûmetinin savunması

Macar Hükûmeti, müdahale kanunla öngörüldüğü ve başkalarının haklarının korunması meşru amacı güdüldüğü için başvurucunun ifade özgürlüğüne halel gelmediğini, ilgili makamların kendilerine tanınan takdir alanında hareket ettiğini ileri sürmüştür.[987] Medeni Kanun'da bu konuda açık bir yasal dayanak olduğunu belirten Macar Hükûmeti, baş-

[984] *Magyar Jeti Zrt. v. Macaristan*, para. 41.
[985] *Magyar Jeti Zrt. v. Macaristan*, para. 42.
[986] *Magyar Jeti Zrt. v. Macaristan*, para. 43.
[987] *Magyar Jeti Zrt. v. Macaristan*, para. 44.

kalarının itibarının korunması gibi bir mülahazayla ifade özgürlüğünün kısıtlanabileceğini belirtmiştir.[988]

Macar Hükûmeti, başvurucu şirketin, özenli davranmış ve video kaydına ilişkin bağlantıyı paylaşmamış olsaydı sorumluluk altına girmeyeceğini belirtmiş; somut içeriğin hukuka aykırılığını ve söz konusu siyasi partinin itibar hakkını ihlal ettiğini tartışmıştır.[989] Macar Hükûmeti, yayıncıların, doğrulamada başarısız oldukları içeriklerden sorumlu tutulacağını öngörmesi gerektiğini ileri sürmektedir.[990] Aksi hâlde ciddi insan hakkı ihlallerinin yaptırımsız kalacağını iddia etmiştir. Keza hukuka aykırı içeriğe sadece erişim sağlanmasının dahi bilginin yayılması anlamına geleceğini, yayımlayanın bu konudaki objektif sorumluluğu bakımından iyi niyet veya kötü niyet ile başkalarının haklarının ihlalinin ciddiyetinin önemi olmadığını belirtmiştir. Macar Hükûmeti, bu durumun ifade özgürlüğüne bir kısıtlama veya yayıncılar üzerinde ölçüsüz bir külfet oluşturmadığı görüşündedir.[991]

Macar Hükûmeti, kâr amacı güden internet sitesi olan başvurucu şirketin, video kayıtlarına erişim sağlamanın hukuki neticelerini öngörebilecek durumda olduğunu; kendisinden özenli davranmasının beklenebileceğini ve bağlantıyı herhangi bir zorluk yaşamadan kaldırabileceğini ileri sürmüştür.[992] Hükûmete göre, yerel mahkemelerin, başvurucu şirketin mahkeme masraflarını ödemesine ve yerel mahkeme kararının ilgili kısımlarını internet sitesinde yayımlamasına hükmetmesi yarışan haklar arasında dengeleyici bir tutum sergilendiğini göstermektedir.[993]

---

[988] *Magyar Jeti Zrt. v. Macaristan*, para. 45.
[989] *Magyar Jeti Zrt. v. Macaristan*, para. 46.
[990] *Magyar Jeti Zrt. v. Macaristan*, para. 47.
[991] *Magyar Jeti Zrt. v. Macaristan*, para. 47.
[992] *Magyar Jeti Zrt. v. Macaristan*, para. 48.
[993] *Magyar Jeti Zrt. v. Macaristan*, para. 49.

V. Müdahil tarafların görüşleri

Magyar Jeti Zrt v. Macaristan yargılamasına muhtelif sivil toplum örgütleri müdahil olmuş ve internet ortamında bağlantılardan dolayı sorumluluğa ilişkin görüş paylaşmıştır.

Article 19, bir web sayfasına bağlantı sağlamakla, bağlantı sağlanan web sayfasındaki içeriği yayımlamak arasında temel bir fark olduğunu, bağlantıların okuyuculara içeriğin başka bir yerde yayımlandığına dair referans teşkil ettiğini belirtmiştir.[994] Article 19'un isabetle belirttiği üzere, internet ortamında bağlantılar olmaksızın içeriği bulmak zor veya imkânsız hâle gelir ve bilgiye erişim azalır.[995] Article 19; Kanada, İngiltere, Avustralya ve Amerika Birleşik Devletleri'ne ait mahkeme kararlarından içerikler paylaşarak bağlantıların tek başına bir yayın teşkil etmediğini, dipnotlar gibi bir referans aracı olduğunu, müstakil yayınların okunması için imkân sağladığını belirtmiştir.[996]

Bağlantı sebebiyle neden sorumluluk oluşmaz sorunsalıyla ilgili olarak Article 19, başvurucular tarafından da işaret edilen önemli bir teknik detayı ortaya koymuştur: Bağlantı sağlanan içerik, bağlantı sağlayanın bilgisi dışında zamanla değişebilmektedir.[997] Article 19, bağlantı sağladığı içeriğin hukuka aykırı olduğunu açıkça bilmeyen ve içeriği açıkça benimsemeyen bağlantı sağlayanın sorumlu tutulmaması gerektiği görüşündedir. Zira başkalarına ait içerikten dolayı bağlantı sağlayanın sorumlu tutulması durumunda caydırıcı bir etki oluşacak ve kontrolleri altında olmayan web sitelerinin içerikleri sebebiyle çok geniş bir kitle cezalandırılacak, internet kullanıcılarının bilgiye erişimleri sınırlandırılacaktır.[998]

Yargılamaya müdahil olan The European Publishers' Council, The Media Law Resource Center Inc., The Newspaper Association of America, Buzzfeed, Electronic Frontier Foundation, Index on Censorship, Profesör Lorna Woods, Dr. Richard Danbury ve Dr. Nicole Stremlau ortak

[994] *Magyar Jeti Zrt. v. Macaristan*, para. 50.
[995] *Magyar Jeti Zrt. v. Macaristan*, para. 50.
[996] *Magyar Jeti Zrt. v. Macaristan*, para. 50.
[997] *Magyar Jeti Zrt. v. Macaristan*, para. 50.
[998] *Magyar Jeti Zrt. v. Macaristan*, para. 50.

bir görüş paylaşmıştır.[999] Müdahil taraflar, bağlantı sağlamanın muhtelif kamusal faydaları olduğunu, içeriğin daha hızlı şekilde sunulmasını temin etmek suretiyle gazetecilik sürecini kolaylaştırdığını, gazetecilerin haberi daha öz ve kolayca erişilebilir şekilde sunmalarını kolaylaştırdığını, okuyucuların haber içeriğinin orijinal kaynaklarını kontrol ederek yayının doğruluğunu teyit etme imkânı bulduklarını belirtmişlerdir.[1000] Bağlantı sağlamanın basında çeşitliliğe katkı sunduğunu, bilgi ve fikirlerin özgürce ifade edilmesi ve bunlara erişilmesinin aydınlatılmış toplumsal tartışmaları kolaylaştırdığını eklemişlerdir.

Tıpkı başvurucu şirket ve Article 19 gibi bu müdahil taraflar da bağlantı sağlamaya katı bir sorumluluk rejimi uygulanmasının caydırıcı etki doğuracağını vurgulamışlardır.[1001] Aynı şekilde, bağlantı sağlanan içeriğin değişmesi pekâlâ mümkün olduğundan sorumluluk esasının temelinin sağlam olmadığını belirtmişlerdir. Müdahil taraflara göre, içeriği oluşturan tarafından içeriğin kaldırılması veya söz konusu kişinin içerikten doğrudan sorumlu tutulması mümkün olduğu için bağlantı sebebiyle bir sorumluluk rejimi getirilmesi zorlayıcı bir sosyal ihtiyaç değildir.

Bağlantı sağlama durumunda hiç mi sorumluluk doğmayacaktır? Müdahil taraflar, bir gazeteci veya basın kuruluşunun, hukuka aykırı içeriğin doğru olduğunu açıkça beyan etmesi veya çok fazla hukuka aykırı içerik ihtiva ettiği bir mahkeme kararıyla tespit edilen içeriğe bağlantıyı kaldırmayı reddetmesi durumunda sorumluluğun doğacağını kabul etmektedirler.[1002] Yani içeriğin benimsenmesi durumu söz konusuysa farklı bir yorum yapılabileceği kanaatindedirler.

Diğer müdahil taraflar olan Access Now, the Collaboration on International ICT Policy in East and Southern Africa ve European Digital Rights tarafından müşterek sunulan görüşte internetin tasarımının bilgiye özgürce bağlantı kurulması fikrine dayandığı, bağlantının kendisinin tek başına editoryal açıklama niteliğinde olmadığı ve bir yayının diğerini

[999] *Magyar Jeti Zrt. v. Macaristan*, para. 51.
[1000] *Magyar Jeti Zrt. v. Macaristan*, para. 51.
[1001] *Magyar Jeti Zrt. v. Macaristan*, para. 51.
[1002] *Magyar Jeti Zrt. v. Macaristan*, para. 51.

benimsediği anlamına gelmek zorunda olmadığı belirtilmiştir.[1003] Adı geçen taraflara göre, bağlantılar sadece diğer sayfaları veya web kaynaklarını işaret etmekte ve ilk bağlantı paylaşıldıktan sonra içerik tam aksi yönde değiştirilebilmektedir. Bu sebeple, bireysel kullanıcıların paylaştıkları herhangi bir bağlantının, doğrulayabilecekleri bir içeriğe işaret ettiğine yönelik bir varsayıma dayanan objektif sorumluluk standardının işlemeyeceğini ileri sürmüşlerdir.

Mozilla Foundation ve Mozilla Corporation (beraber Mozilla) ise bağlantının sadece kullanıcıların bilgiden bilgiye gezinti yapmalarına imkân sağlama amacı olduğunu belirtmişlerdir.[1004] Diğer müdahil taraflar gibi Mozilla da bağlantıların kullanıcılara başka bir yerde bulunan bilgiye erişmek için sunulan teknik ve otomatik araçlar olduğunu ve bilginin yayımlanması olarak nitelendirilemeyeceğini ifade etmiştir. Mozilla, ayrıca, bağlantı kullanmaya yönelik bir kısıtlamanın *world wide web* sisteminin bilgiyi birbirine bağlayarak erişilebilir kılma ana amacına zarar vereceğini vurgulamış ve bağlantı sağlamanın sorumluluk doğurması durumunda insanların sayısız web sayfası arasında bilgiyi nasıl aktaracağına yönelik kuşkularını paylaşmıştır.[1005] Son olarak, bağlantılar olmazsa okuyucuların daha fazla bilgiye erişebilmeleri için yayıncıların alternatif talimatlar sağlaması gerekeceğini belirtmiştir.

Avrupa Bilgi Toplumu Enstitüsü (the European Information Society Institute), bağlantıların dijital gezintinin ana aracı olduğunu ve klasik atıf yöntemlerinin aksine başka metinlere hızlıca ulaşmayı sağladığını belirtmiştir.[1006] Enstitüye göre bağlantılar, (a) gazeteciler ve okuyucular arasında etkileşimi, (b) bilgiyi desteklemek için vakıalar, olaylar ve kaynaklar sağlayarak güvenilirliği, (c) okuyuculara haberin kaynağına ve haber toplama süreçlerine dönme imkânı sağlayarak şeffaflığı, (d) gazetecilere ve okuyuculara çelişen kaynakları karşılaştırma imkânı sağlayarak eleştirel okumayı artırarak yeni bir medyanın gelişmesine katkı sunmuş-

[1003] *Magyar Jeti Zrt. v. Macaristan*, para. 52.

[1004] *Magyar Jeti Zrt. v. Macaristan*, para. 53.

[1005] *Magyar Jeti Zrt. v. Macaristan*, para. 53.

[1006] *Magyar Jeti Zrt. v. Macaristan*, para. 54.

tur.[1007] Enstitü, bağlantılar için katı sorumluluk kuralları işletilmesinin kaçınılmaz olarak otosansüre yol açacağı fikrindedir.

Son müdahil taraf olan the European Roma Rights Centre ise konuya azınlıkların nefret suçları veya nefret söylemiyle bağlantılı eylemlere maruz kalmaları ve bu bağlamda AİHS'nin 10. maddesinin sağladığı koruma açısından yaklaşmıştır.[1008] Adı geçen müdahil taraf, hakarete ilişkin yasaların Roman azınlığın siyasi partilerin ırkçı temelli uygulamalarını dile getirmesini önlemek amacıyla kullanılmasının bu tür siyasi partileri azınlık gruplara karşı koruma neticesini doğuracağını iddia etmiş; online yayıncıların bağlantı sağlanan içerikten dolayı sorumluluğunun caydırıcı bir etkisi olacağını ve ırkçılıkla mücadele eden sivil topluma ve azınlıklara aşırı bir yük getireceğini ileri sürmüştür.[1009]

VI. AİHM'nin tespit ve değerlendirmeleri

A. Bir müdahale olup olmadığı

Taraflar arasındaki ihtilafın temeli, yerel mahkemelerin kararlarıyla başvurucu şirketin AİHS'nin 10. maddesinde güvence altına alınan ifade özgürlüğüne müdahale edilip edilmediğidir. AİHM, aksini değerlendirmeyi gerektirecek bir durum olmadığı kanaatindedir.[1010] Bu tespitinden sonra AİHM, müdahalenin kanunla öngörülüp öngörülmediğini, 10. maddenin ikinci fıkrası uyarınca meşru bir veya birkaç amaca dayanıp dayanmadığını ve demokratik bir toplumda gerekli olup olmadığını incelemeye başlamıştır.

B. Kanunilik

AİHM'nin klasik metodolojisiyle ilk incelediği husus, yapılan müdahalenin kanunilik ilkesinin şartlarını yerine getirip getirmediği olmuş-

[1007] *Magyar Jeti Zrt. v. Macaristan*, para. 54.
[1008] *Magyar Jeti Zrt. v. Macaristan*, para. 55.
[1009] *Magyar Jeti Zrt. v. Macaristan*, para. 55.
[1010] *Magyar Jeti Zrt. v. Macaristan*, para. 56.

tur. AİHM, tarafların müdahalenin bir kanunla öngörülme şartını yerine getirip getirmediği konusunda farklı görüşleri olduğunu belirtmiştir: Başvurucu şirket, bir bağlantı paylaşmanın hukuka aykırı veya hakaret niteliğindeki bilgiyi yayma olarak nitelendirilmesinin için hukukta öngörülmediğini iddia ederken, Macar Hükûmeti Medeni Kanun'un ilgili hükümleri uyarınca başvurucu şirketin üçüncü taraflarca ifade edilen fikirleri açıklamak ve yaymak suretiyle sorumlu olduğunu savunmuştur.[1011]

AİHM, önceki içtihatlarına atıf yaparak AİHS'nin 10. maddesinin ikinci fıkrasında yer alan "kanunla öngörülme" ifadesinin sadece söz konusu tedbirin iç hukukta yasal bir temelinin olmasını emretmediğini, aynı zamanda söz konusu kanunun niteliğini de hedeflediğini hatırlatmıştır.[1012] Keza Mahkeme, mesleklerini icra ederken son derece temkinli hareket etme alışkanlığına sahip olan kişilerden, bu türden bir faaliyetin yaratacağı riskleri değerlendirirken özel önem göstermelerinin beklenebileceğine ilişkin içtihatlarını alıntılamıştır.[1013]

AİHM, yerel mahkemelerin bağlantı paylaşmayı hakaret niteliğindeki ifadeleri yayma olarak görüp Medeni Kanun'un 78. maddesini uyguladıklarını belirtmiş, bağlantıların geçerliliğine ve sınırlarına ilişkin ne açık bir düzenleme ne de bir içtihat olduğunu not etmiştir.[1014] Bu tespite rağmen, müdahalenin gerekliliğine çapraz atıf yapan AİHM, AİHS'nin 10. maddesinin ikinci fıkrası bağlamında, Medeni Kanun'un ilgili hükümlerinin uygulanmasının başvurucu şirket açısından öngörülebilir olup olmadığını incelemeye gerek olmadığına hükmetmiştir.[1015]

C. Meşru amaç

AİHM, Macar Hükûmetinin müdahalenin başkalarının haklarını koruma meşru amacına dayandığına ilişkin görüşüne katılmıştır.[1016]

[1011] *Magyar Jeti Zrt. v. Macaristan*, para. 58.
[1012] *Magyar Jeti Zrt. v. Macaristan*, para. 59.
[1013] *Magyar Jeti Zrt. v. Macaristan*, para. 59.
[1014] *Magyar Jeti Zrt. v. Macaristan*, para. 60.
[1015] *Magyar Jeti Zrt. v. Macaristan*, para. 61.
[1016] *Magyar Jeti Zrt. v. Macaristan*, para. 62.

D. Demokratik toplum düzeninin gerekliliği

AİHM, ifade özgürlüğüne müdahalede demokratik toplum düzeninin gerekliliğine ilişkin temel ilkeleri *Delfi AS v. Estonya* kararında etraflıca belirlediğini ifade etmiştir.[1017] Ayrıca kamu menfaatine ilişkin konularda haber yapmayla ilgili olarak AİHS'nin 10. maddesi ile gazetecilere sağlanan güvencenin, gazetecilerin iyi niyetle ve doğru, somut temelde hareket etmeleri, gazetecilik ahlakı gereğince "güvenilir ve kesin" bilgi sağlamaları koşuluna tabi tutulduğunu belirtmiş ve büyük bilgi sirkülasyonuna işaret ederek gazetecilik etiğinin artan önemine işaret etmiştir.[1018]

Aynı doğrultuda, başkalarının şöhret veya haklarının korunmasındaki menfaatleri kapsamında, demokratik bir toplumda ifade özgürlüğüne müdahale edilmesine yönelik bir ihtiyaç olup olmadığını incelerken AİHM, yerel makamların AİHS tarafından güvence altına alınan ve başka davalarda birbiriyle çatışabilen iki değer yani bir yanda 10. madde tarafından korunan ifade özgürlüğü ile diğer yanda 8. maddede belirtilen özel hayata saygı hakkı arasında adil bir denge kurup kurmadığının belirlenmesi gerektiğine ilişkin içtihatlarını tekrarlamıştır.[1019]

AİHM *Ahmet Yıldırım v. Türkiye* kararına da atıf yaparak, büyük miktarda veriyi saklama ve yayımlama kapasitesi ile internetin toplumun gündemdeki olaylara erişimini sağlamaya ve genel anlamda bilginin dağıtılmasını kolaylaştırmaya büyük katkı sunduğunu hatırlatmıştır.[1020] Bununla birlikte, internetteki içerik ve iletişimin başta özel hayata saygı hakkı olmak üzere insan hak ve özgürlüklerinin kullanılmasına yönelik doğurduğu zarar riskinin basının doğurduğu riskten daha yüksek olduğunun altını çizmiştir.[1021] İçtihatlarındaki istikrarı göstermek adına AİHM, internetin doğası gereği internet haber sitelerinin görev ve sorumluluklarının klasik yayıncılarınkinden -özellikle de üçüncü taraflara ait içerikler sebebiyle- farklı olacağına ilişkin *MTE ve Index.hu Zrt v. Macaristan*

[1017] *Magyar Jeti Zrt. v. Macaristan*, para. 63.
[1018] *Magyar Jeti Zrt. v. Macaristan*, para. 64.
[1019] *Magyar Jeti Zrt. v. Macaristan*, para. 65.
[1020] *Magyar Jeti Zrt. v. Macaristan*, para. 66.
[1021] *Magyar Jeti Zrt. v. Macaristan*, para. 66.

kararındaki çıkarımını tekrarlamıştır.[1022] AİHM, önceki içtihatlarıyla uyumlu şekilde, bilgi toplumu hizmet sağlayıcılarının üçüncü taraflara ait içeriklerden dolayı söz konusu içeriğin hukuka aykırılığının farkına varıp içeriği hızlıca kaldırmada veya içeriğe erişimi kısıtlamada başarısız olmadıkları sürece sorumlu olmamaları gerektiği kanaatindedir.[1023]

Son olarak AİHM, içeriğin basılı bir ortamda tekrar üretilmesi ve internet ortamında tekrar üretilmesi bakımından uygulanacak kuralların farklı olabileceğini kabul etmektedir.[1024] Mahkemeye göre, içeriğin internet ortamında tekrar üretilmesi durumunda söz konusu hak ve menfaatleri korumak ve güvence altına almak için öngörülen kuralların teknolojinin kendine özgü kurallarına uygun şekilde düzenlenmesi gerektiği görüşündedir.[1025] AİHM, yerel düzeyde gazetecilerin internet ortamında elde ettikleri bilgiyi herhangi bir yaptırıma uğrama korkusu olmaksızın kullanmalarına izin veren yeterli bir hukuki düzenleme olmamasının, basının son derece önemli olan "kamu denetçiliği" fonksiyonunu ciddi şekilde engelleyeceği kanaatindedir.[1026]

Mahkeme, mevcut davayı, özellikle online bir haber metninde internet ortamındaki hakaret nitelikli içeriğe bağlantı veren internet haber sitelerinin AİHS'nin 10. maddesi bağlamındaki yükümlülükleri ve sorumluluklarına ilişkin bir dava olarak ele almıştır.[1027]

AİHM, *Delfi AS v. Estonya*, *MTE ve Index.hu Zrt v. Macaristan*, *Rolf Anders Daniel Pihl v. İsveç* kararlarında yaptığı gibi *Magyar Jeti Zrt v. Macaristan* kararında da somut olaydaki internet sitesinin niteliğini, nasıl işlediğini ve hizmet sunduğunu incelemiştir. AİHM, mevzubahis internet haber sitesinin profesyonel olarak işletildiğini, farklı konulara ilişkin

[1022] *Magyar Jeti Zrt. v. Macaristan*, para. 66.
[1023] *Magyar Jeti Zrt. v. Macaristan*, para. 67.
[1024] *Magyar Jeti Zrt. v. Macaristan*, para. 68.
[1025] *Magyar Jeti Zrt. v. Macaristan*, para. 68.
[1026] *Magyar Jeti Zrt. v. Macaristan*, para. 68.
[1027] *Magyar Jeti Zrt. v. Macaristan*, para. 69.

her gün yetmiş beşe yakın haber yayımladığını ve günde 250.000'e yakın ziyaretçi aldığını belirtmiştir.[1028]

AİHM, yerel mahkemelerin bir basın toplantısına ilişkin haberin naklinin hangi durumda sorumluluk doğurup doğurmadığına ilişkin tespitlerini incelemiş, yalan veya hakaret niteliğindeki bilgilerin aktarılmasında sorumluluktan bağışıklık getirilmediği tespitini yapmıştır.[1029]

AİHM, üçüncü taraflara ait içeriklere ilişkin geleneksel medya ile internet haber sitelerini işletenlerin sorumluluğunun farklılaşacağına dair *Delfi AS v. Estonya* kararındaki tespitini tekrarlamıştır.[1030] İnternetin kamunun haberlere ve bilgiye erişimini artırma rolüne dikkat çeken Mahkeme, başka web sayfalarına ve internet kaynaklarına bağlantı vermekteki amacın, mevcut bilginin çokluğuyla şekillenen bir ağda internet kullanıcılarına bir içerikten diğerine gezinti yapma imkânı sağlamak olduğunu belirtmiştir.[1031] Mahkemeye göre bağlantılar bilgiyi birbirine eklemleyerek erişilebilir kılar ve internetin etkin işlemesine katkı sunar.[1032]

AİHM, bağlantıların niteliğini derinlemesine incelemiştir. Mahkemeye göre bağlantılar, bir tür haber yapma tekniğidir ve geleneksel yayın yöntemlerinden esaslı olarak farklıdır. Zira genel bir kural olarak kullanıcıları internet ortamında başka bir yerde bulunan içeriğe yönlendirirler.[1033] Aynı doğrultuda, bağlantı sağlanan açıklamalar veya bunların içeriği kullanıcıya ulaştırılmaz, sadece içeriğin başka bir web sitesindeki varlığına okuyucuların dikkati çekilir.

AİHM'ye göre, bilginin yayılması yollarıyla kıyaslandığında bağlantıları farklı kılan diğer bir özellik, bağlantı aracılığıyla bir içeriğe işaret eden kişinin o içerik üzerinde bir kontrol icra etmemesidir. Zira içerik, bağlantı oluşturulduktan sonra değiştirilebilir meğerki bağlantının işa-

[1028] *Magyar Jeti Zrt. v. Macaristan*, para. 70.
[1029] *Magyar Jeti Zrt. v. Macaristan*, para. 71.
[1030] *Magyar Jeti Zrt. v. Macaristan*, para. 72.
[1031] *Magyar Jeti Zrt. v. Macaristan*, para. 73.
[1032] *Magyar Jeti Zrt. v. Macaristan*, para. 73.
[1033] *Magyar Jeti Zrt. v. Macaristan*, para. 74.

ret ettiği içerik bağlantı sağlayan kişi tarafından oluşturulmuş olsun.[1034] Mahkeme, bağlantının işaret ettiği içeriğin zaten ilk yayıncı tarafından erişilebilir kılındığını ve kamunun sınırsız erişimine açıldığını da vurgulamıştır.

AİHM, bağlantıların teknik özelliklerini dikkate alarak, Macar mahkemelerinin yalnızca bağlantının paylaşılmasını hakaret niteliğindeki bilgiyi yayma ile eş değer tutan ve otomatik olarak içerikten sorumlu kılan yaklaşımına katılmadığını belirtmiştir.[1035] Mahkeme tam aksine, bir bağlantının AİHS'nin 10. maddesi kapsamında sorumluluğa vücut verip vermediğinin her somut olay özelinde birçok kriter dikkate alınarak değerlendirilmesi gerektiği görüşündedir.[1036]

AİHM, başvurucu şirketin bağlantının yayıncısı olarak sorumluluğu bakımından müteakip kriterleri belirlemiştir:[1037]

(i) Gazeteci ihtilaflı içeriği benimsemiş midir?

(ii) Gazeteci ihtilaflı içeriği benimsemeden tekrarlamış mıdır?

(iii) Gazeteci ihtilaflı içeriği benimsemeden veya tekrarlamadan içeriğe salt bağlantı mı sağlamıştır?

(iv) Gazeteci, içeriğin hakaret barındırdığını veya hukuka aykırı olduğunu bilmekte midir veya makul şekilde bilmiş olması kendisinden beklenebilir mi?

(v) Gazeteci iyi niyetle hareket etmiş midir, gazetecilik etiğine saygı göstermiş midir ve sorumlu gazetecilikten beklenen gerekli özeni sergilemiş midir?

Geliştirmiş olduğu bu kriterleri somut olaya uygulayan AİHM, dava konusu makalede sadece Bay J.Gy. ile yapılan ve YouTube sitesinde bulunan bir röportajdan bahsedildiğini, söz konusu içeriğe ulaşmak amacıyla bir bağlantı sağlandığını, içeriğin herhangi bir kısmından ilave bir yorum veya tekrar içermediğini ve ilgili siyasi partiden bahsedilmediğini

[1034] *Magyar Jeti Zrt. v. Macaristan*, para. 75.

[1035] *Magyar Jeti Zrt. v. Macaristan*, para. 76.

[1036] *Magyar Jeti Zrt. v. Macaristan*, para. 76.

[1037] *Magyar Jeti Zrt. v. Macaristan*, para. 77.

belirtmiştir.[1038] İçeriği daha yakından etüt eden Mahkeme, haberin hiçbir yerinde yazarın bağlantı sağlanan içeriğin doğru olduğuna veya içeriği onayladığına yahut bu içerikten dolayı sorumluluğu kabul ettiğine dair bir ifade bulunmadığının altını çizmiş ve bu sebeple, sağlanan bağlantının, hukuka aykırılığı belirlenmiş bir içeriğin benimsenmesi niteliğinde olmadığına karar vermiştir.[1039]

İçeriğin tekrar edilmesi sorununa ilişkin olarak Mahkeme, gazetecilik faaliyetleriyle ilgili önceki içtihatlarını alıntılamıştır. AİHM, bir röportajda yer alan başkalarına ait ifadelerin yayılması sebebiyle bir gazetecinin cezalandırılmasının, basının kamu yararını ilgilendiren tartışmalara katkısına esaslı darbe vuracağını tekrarlamış ve güçlü gerekçeler olmadığı takdirde bu yola başvurulmaması gerektiğini belirtmiştir.[1040] AİHM, gazetecilerin haber alıntılamalarının önemini tekrar tekrar vurgulamıştır.

AİHM, birtakım unsurların varlığı hâlinde, örneğin bir bağlantıya ilave olarak içerik aktarılması durumunda, sorumluluğun doğma ihtimalini göz ardı etmemektedir.[1041] Mahkeme, gazetecinin iyi niyetle ve gazetecilik etiğine uygun hareket etmediği, kamu yararını ilgilendiren sorumlu bir gazetecilikten beklenen özeni göstermediği durumları bu tür sorumluluk hâline örnek göstermektedir.[1042] Mahkeme, somut olayda haberin hakaret içeren ifadeleri tekrarlamadığını ve yayının sadece bağlantıyı sağlamakla sınırlı olduğunu belirtmiştir.[1043]

Yerel mahkemelerde gazeteci ile başvurucu şirketin bağlantı sağlanan içeriğin hukuka aykırılığı konusunda bilgi sahibi olup olmadığı tartışılmamıştır. Bu noktada AİHM, bir kişinin şöhretine yönelik saldırının belli seviyede ciddiyete ulaşması ve kişinin özel hayatına saygı gösterilmesini isteme hakkını kullanmasına halel getirecek şekilde gerçekleştirilmesi gerektiğine dair içtihatlarına atıf yapmıştır. Mahkeme, sıradan kişilere nazaran politikacılara yönelik eleştirilerde kabul edilebilir eleştiri sınırı-

[1038] *Magyar Jeti Zrt. v. Macaristan*, para. 78.
[1039] *Magyar Jeti Zrt. v. Macaristan*, para. 79.
[1040] *Magyar Jeti Zrt. v. Macaristan*, para. 80.
[1041] *Magyar Jeti Zrt. v. Macaristan*, para. 80.
[1042] *Magyar Jeti Zrt. v. Macaristan*, para. 80.
[1043] *Magyar Jeti Zrt. v. Macaristan*, para. 80.

nın daha geniş olduğunu, politikacıların daha fazla tolerans göstermesi gerektiğini belirtmiştir.[1044]

Tüm bu tespitler ışığında AİHM, mevcut başvurudaki gazeteciyi, erişim sağladığı içeriklerin -bu içerikler tartışmalı dahi olsa- siyasi partilere ilişkin izin verilen eleştiri kapsamında kalacağını ve bu itibarla da hukuka aykırı olmadığını sanmakta haklı görmüştür.[1045] Her ne kadar J.Gy.'nin açıklamalarının maddi dayanaktan yoksun şekilde Jobbik ile bağlantılı kişilerin ırkçı nitelikte eylemler yaptığı iması içermesinden dolayı hakaret niteliğinde olduğu tespit edilmişse de AİHM, bu tür sözlerin başından itibaren açıkça hukuka aykırı kabul edilemeyeceği yönündeki görüşü benimsemiştir.[1046]

AİHM, yetkili yerel mahkemeler tarafından yorumlandığı şekliyle ilgili Macar hukukunun, kısıtlamaların en üst düzeyde incelemeyi gerektirdiği bir durumda, başvurucu şirketin AİHS'nin 10. maddesi kapsamındaki ifade özgürlüğü haklarına ilişkin anlamlı bir değerlendirmeyi dışladığı görüşündedir.[1047] *MTE ve Index.hu Zrt v. Macaristan* kararına tekrar atıf yapan AİHM, Macar mahkemelerinin bağlantı sağlamanın bilgiyi yaymaya sebep olması ve objektif sorumluluk doğurması şeklindeki kararının, bir tarafta siyasi partinin itibarı diğer tarafta başvurucu şirketin ifade özgürlüğü gibi yarışan haklar arasında bir dengeleme yapılmasını etkin şekilde dışlamış olduğunu belirtmiştir.[1048]

AİHM, bu tür objektif bir sorumluluğun internet ortamında bilginin akışı üzerinde öngörülebilir olumsuz etkileri olacağı görüşündedir. Haber yazarları ve yayıncılar, üzerinde kontrolleri bulunmayan, değişebilir içerikli materyallere bağlantı sağlamaktan çekinebilecektir. Mahkeme, bunun internet ortamında ifade özgürlüğü üzerinde doğrudan veya dolaylı olarak caydırıcı etki doğuracağı kanaatindedir.[1049] Bu gerekçelerle

[1044] *Magyar Jeti Zrt. v. Macaristan*, para. 81.
[1045] *Magyar Jeti Zrt. v. Macaristan*, para. 82.
[1046] *Magyar Jeti Zrt. v. Macaristan*, para. 82.
[1047] *Magyar Jeti Zrt. v. Macaristan*, para. 83.
[1048] *Magyar Jeti Zrt. v. Macaristan*, para. 83.
[1049] *Magyar Jeti Zrt. v. Macaristan*, para. 83.

AİHM, yerel mahkemelerin başvurucu şirket üzerine objektif sorumluluk yüklemesinin makul ve yeterli sebeplere dayanmadığına ve önlemin ifade özgürlüğü üzerinde ölçüsüz bir müdahale teşkil ettiğine karar vermiştir.[1050] Bu doğrultuda, AİHS'nin 10. maddesinin ihlal edildiğine hükmetmiştir.

E. Yargıç Paulo Pinto de Albuquerque'nin mutabık görüşü

AİHM Yargıcı Paulo Pinto de Albuquerque, karara katılmakla beraber müstakil bir mutabık görüş yazmıştır. Yargıç Pinto de Albuquerque, Avrupa insan hakları hukukunun, interneti, uluslararası olarak korunan insan hakları -özellikle ifade özgürlüğü ve basın hürriyeti hakları-kapsamına dâhil etme lehine güçlü bir şekilde geliştiğini, internet ortamında yayımlanan üçüncü şahıslara ait içerikler sebebiyle sorumluluk yüklenmesinin korunan bu haklara halel getireceğini belirtmiştir.[1051] Yargıç Pinto de Albuquerque'ye göre, mevcut davadaki hukuki mesele, bağlantı sağlamanın objektif bir sorumluluk doğurması standardının bu haklarla uyumlu olup olmadığıdır. Bağlantıların önemine değinen Yargıç Pinto de Albuquerque, bu davanın neticesinin internetin günlük işleyişi üzerinde etkileri olacağını vurgulamıştır. Bu bağlamda, karara katıldığını belirtmekle birlikte, bağlantılara ilişkin sorumluluğa dair ilkeleri vurgulamak amacıyla AİHM'nin yapmış olduğu muhakemeyi etüt etmiştir.

AİHM'nin bağlantıları bir yayının tekrarlanmasından farklı gören tespitlerini alıntılayan Yargıç Pinto de Albuquerque, bağlantıları farklı kılan özelliklere vurgu yapmış ve Mahkemenin yaklaşımının Alman Federal Anayasa Mahkemesi, Kanada Temyiz Mahkemesi ile Amerika Birleşik Devletleri Temyiz Mahkemesinin -AİHM'nin de atıf yaptığı- kararlarıyla uyumlu olduğunu belirtmiştir.[1052] Yargıç Pinto, World Wide Web'in mucidi Tim Berners-Lee'nin bağlantılara ilişkin şu görüşünü de alıntılamıştır:

[1050] *Magyar Jeti Zrt. v. Macaristan*, para. 84.

[1051] *Magyar Jeti Zrt. v. Macaristan*, Yargıç Pinto de Albuquerque'nin Mutabık Görüşü, para. 1.

[1052] *Magyar Jeti Zrt. v. Macaristan*, Yargıç Pinto de Albuquerque'nin Mutabık Görüşü, para. 2-3.

"Webin dizayn edilmesinin gayesi, normal bağlantıların herhangi bir zımni anlam barındırmayan referanslar olmasıdır. Normal bir bağlantı, bir belgenin diğer bir belgeyi onayladığı veya bir belgenin diğer belgeyi hazırlayan kişi tarafından oluşturulduğu yahut bir belgenin diğer belgenin parçası olduğu anlamına gelmek zorunda değildir."[1053]

Yargıç Pinto de Albuquerque, sistemin dizaynına ilişkin iki ilkenin webin yapısının ve işleyiş modunun temelini oluşturduğunu ve ifade özgürlüğünü mümkün kıldığını belirtmiştir.[1054] Tim Berners-Lee tarafından belirtildiği üzere:

"Webin kullanışlılığının ve büyümesinin altında yatan temel ilke evrenselliktir. Bir bağlantı oluşturduğunuzda herhangi bir şeye bağlantı verebilirsiniz. Bu da insanların hangi bilgisayara sahip olduğu, hangi yazılımı kullandığı, hangi dili konuştuğundan, internet bağlantısının kablolu veya kablosuz oluşundan bağımsız şekilde webe herhangi bir şeyi koyabilmeleri manasına gelmektedir. Merkezden yönetilmeme de önemli bir tasarım özelliğidir. Bir sayfa eklemek veya bağlantı kurmak için merkezî bir otoritenin onayına ihtiyaç duyulmaz. Yapmanız gereken şey, basit ve standart üç protokolü kullanmaktır: Bir sayfayı HTML formatında yazın, bunu URL yazım kurallarına göre adlandırın ve HTT kullanarak internet ortamına sunun. Merkezden yönetilmeme alabildiğine geniş bir yenilikçiliği mümkün kılmıştır ve gelecekte de böyle olmaya devam edecektir."[1055]

Son olarak Berner-Lee'nin bilginin verimli ve evrensel bir şekilde bağlanmasına duyulan ihtiyaca ilişkin görüşlerinden alıntı yapmıştır:

"Web, bilgi için evrensel bir alan olarak dizayn edilmiştir, bir yer imi veya bağlantı oluşturduğunuzda bu bağlantıyı kesinlikle ağlar vasıtasıyla erişilen herhangi bir bilgi yerine bağlayabilirsiniz. Evrensellik web için çok önemlidir: Bazı tür şeylere bağlantı veremezseniz gücünü kaybeder… "[1056]

[1053]**Berners-Lee, Tim**, *"Links and Law: Myths"* <https://www.w3.org/DesignIssues/LinkMyths.html>

[1054]*Magyar Jeti Zrt. v. Macaristan*, Yargıç Pinto De Albuquerque'nin Mutabık Görüşü, para. 4.

[1055]**Berners-Lee, Tim**, *"Long Live the Web: A Call for Continued Open Standards and Neutrality"* <https://www.scientificamerican.com/article/long-live-the-web/>

[1056]**Berners-Lee, Tim/Fischetti, Mark** (1999) *Weaving the web : the original design and*

Yargıç Pinto de Albuquerque'ye göre bağlantılar webi bir arada tutan tutkaldır; zira, bağlantılar insanların kolayca ve hızlıca diğer web sayfalarını gezmelerini, bilgi almalarını, görüntülemelerini ve bilgiyi tekrar paylaşmalarını sağlamaktadır.[1057] Bağlantılar olmaksızın bilgiyi bulabilmeleri için yayıncıların kullanıcılara alternatif talimatlar sağlamaları gerekmektedir. Yargıç Pinto de Albuquerque'ye göre güçlü bir teknik bilgi olmaksızın ortalama bir insan için bunu gerçekleştirmek imkânsız değilse de zor olacaktır.[1058] Tüm bu tespitlerin ışığında Yargıç Pinto de Albuquerque, evrensellik ve merkezden yönetilmeme prensiplerinin özellikle gazetecilik alanındaki etkilerine vurgu yapmış[1059] ve Kanada Temyiz Mahkemesinin de bağlantılarla ilgili benzer bir yaklaşımı benimsediğini belirtmiştir.[1060]

AİHM'nin kararındaki bağlantıların sorumluluk doğurmasına ilişkin kriterleri tekrar ele alan Yargıç Pinto de Albuquerque,[1061] bu kriterleri şu şekilde özetlemiştir:[1062]

İlke 1: Bir gazeteci, bağlantının yönlendirdiği karalayıcı veya başka şekilde hukuka aykırı olan içeriği açık ve net bir dille benimser veya tekrar ederse bağlantı kullanılması geleneksel yayın türleriyle eş tutulur.

İlke 2: Bir gazetecinin (mevcut ve pozitif bir bilgiyle) bağlantının yönlendirdiği içeriğin hukuka aykırı olduğunu bildiği ve kötü niyetle hareket ettiği durumlarda hukuki sorumluluğa hükmedilmelidir. İstisnai olarak, bir gazetecinin içeriğin hukuka aykırı olduğunu mesleki etik ve sorumlu bir gazetecinin özen yükümlülüğü ışığında makul şekilde bilmesi

ultimative destiny of the World Wide Web by its inventor, New York, HarperCollins.

[1057] *Magyar Jeti Zrt. v. Macaristan*, Yargıç Pinto De Albuquerque'nin Mutabık Görüşü, para. 4.

[1058] *Magyar Jeti Zrt. v. Macaristan*, Yargıç Pinto De Albuquerque'nin Mutabık Görüşü, para. 4.

[1059] *Magyar Jeti Zrt. v. Macaristan*, Yargıç Pinto De Albuquerque'nin Mutabık Görüşü, para. 5.

[1060] *Magyar Jeti Zrt. v. Macaristan*, Yargıç Pinto De Albuquerque'nin Mutabık Görüşü, para. 6-7.

[1061] *Magyar Jeti Zrt. v. Macaristan*, Yargıç Pinto De Albuquerque'nin Mutabık Görüşü, para. 8-19.

[1062] *Magyar Jeti Zrt. v. Macaristan*, Yargıç Pinto De Albuquerque'nin Mutabık Görüşü, para. 20.

(müspet/varsayılan bir bilgi) gereken durumlarda da hukuki sorumluluk gündeme gelebilir.

İlke 3: Bir gazeteci bağlantı kullanır ama bu bağlantının yönlendirdiği karalayıcı veya başka şekilde hukuka aykırı olan içeriği onaylamaz veya tekrar etmezse, bağlantı kullanılması geleneksel yayın türleriyle eş tutulmaz ve -bu tür bir içeriğin hukuka aykırı olduğunu ilan eden ve kullanımını yasaklayan bir mahkeme kararına uyulmaması durumu hariç- sorumluluk doğurmaz.

İlke 4: İçeriğin asıl yayıncısına tanınan tüm savunma imkânları, bağlantı sağlanan içerikten hukuken sorumlu tutulmaları durumunda gazetecilere de tanınmalıdır. Gazetecilerin bağlantının yönlendirdiği karalayıcı veya başkaca şekilde hukuka aykırı olan içerikle aralarına mesafe koyma yükümlülükleri yoktur.

İlke 5: Yukarıda belirtilen Sözleşme (AİHS) ilkeleri, yerel mahkemelerin kararlarında ortaya konulan tespitlere dayalı olarak geriye dönük bir bakıştan ziyade söz konusu zamanda yazara sunulan durumun ışığında her bir olay için müstakil bir değerlendirme yapılmasını gerektirir.

İlke 6: Bağlantıların kullanılmasına ilişkin objektif veya katı sorumluluk rejimi, bizatihi yukarıda zikredilen Sözleşme (AİHS) hükümlerine aykırıdır.

İlke 7: Bu ilkeler hem gerçek kişilere (gazeteciler) hem de tüzel kişilere (medya şirketleri) uygulanır.

AİHM'nin yukarıda sayılan ilkelerini mevcut olaya tekrar uygulayan Yargıç Pinto de Albuquerque,[1063] Berners-Lee'nin bağlantıların sadece dijital devrim için değil refahımızın ve hatta özgürlüğümüzün devamı için kritik önemde olduğuna dair görüşünü tekrarlamıştır.[1064] Berners-Lee'nin ifadesiyle, bağlantıların tıpkı demokrasi gibi savunulma-

---

[1063] *Magyar Jeti Zrt. v. Macaristan*, Yargıç Pinto De Albuquerque'nin Mutabık Görüşü, para. 21-24.

[1064] *Magyar Jeti Zrt. v. Macaristan*, Yargıç Pinto De Albuquerque'nin Mutabık Görüşü, para. 26.

sı gerekmektedir.[1065] Yargıç Pinto de Albuquerque'ye göre AİHS'nin 10. maddesinin ihlal edildiğini tespit etmek suretiyle AİHM bu "savunma"yı gerçekleştirmiştir.

VII. Değerlendirme

Magyar Jeti Zrt. v. Macaristan kararı, AİHM'nin internetin teknik işleyişini gözeterek internet hukukuyla ilgili vermiş olduğu en isabetli karardır. AİHM'nin *Delfi AS v. Estonya*, *MTE ve Index.hu Zrt v. Macaristan* ve *Rolf Anders Daniel Pihl v. İsveç* kararları içerikten dolayı sorumluluğa dair iken, AİHM ilk defa bağlantıların hukuki statüsünü ve bağlantılar sebebiyle içerikten dolayı sorumluluğu ele almıştır.[1066]

AİHM, çatışan hakları yerinde dengeleyen bir karar vermiştir. Bağlantılar için doğrudan ve mutlak bir sorumluluğu reddettiği gibi belirli koşullar altında sorumluluğun mutlak bir sorumsuzluk anlayışını da benimsememiştir. Her somut olayın özelliklerine göre bir değerlendirmenin yapılmasını ve buna göre bir karar verilmesini belirtmiştir.

İlke 7: Bu ilkeler hem gerçek kişilere (gazeteciler) hem de tüzel kişilere (medya şirketleri) uygulanır.

Bağlantılar, interneti internet yapan en temel fonksiyonlardır. Bağlantılar, kullanıcılara başka bir yerde bulunan bilgiye erişmek için sunulan teknik ve otomatik araçlardır ve bu özgün işlevleri sebebiyle ayrı bir hukuki statüde değerlendirilmeleri gerekir. Bağlantılar, internetin devinimiyle paralel şekilde değişmektedir. Uzun URL adreslerini kısaltma amacıyla kullanılan özel bağlantılar bunun bir örneğidir.

[1065] **Berners-Lee / Fischetti**, s. 174.

[1066] Bağlantılardan dolayı sorumluluğun tespiti Avrupa Birliği hukukunun da en temel tartışma konularından birisidir. Bu konuda, telif hukukundan ceza hukukuna çok farklı alanlarda tartışmalar sürmektedir. 2000 yılında kabul edilen E-Ticaret Direktifi, bu sorunları çözmekte yetersiz kalmaktadır. Bu konudaki güncel tartışmalar için bkz. **Schulze, Reiner/Staudenmayer, Dirk** (2020) *EU Digital Law Article-by-Article Commentary*, Baden, Nomos Verlagsgesellschaft, s. 481.

Bağlantı vermeyi içeriğin otomatik yayımlanması olarak nitelendirmek, internet sisteminin bilgiyi birbirine bağlayarak erişilebilir kılma ana amacına zarar verecektir. Bağlantılar olmazsa yayıncılar, daha fazla bilgi bulmaları için okuyuculara alternatif talimatlar sağlamak zorunda kalacak ve internet işlevsellikten uzak bir ağ hâline gelecektir. AİHM'nin bağlantı sağlayanın bağlantının yönlendirdiği hukuka aykırı içerikten objektif olarak sorumlu tutulamayacağına dair yaklaşımı bu sebeple yerindedir. *Delfi AS v. Estonya* başta olmak üzere, internet içerikleriyle ilgili vermiş olduğu önceki kararlar ile kıyaslandığında AİHM, ilk defa internetin teknik işleyişinin özüne ve ruhuna uygun bir karar vermiştir.

Karar, bağlantıları demokrasi için hayati önemde gören Berners-Lee'nin hassasiyetine uygundur. İnternet hukuku bağlamında uygulanabilir ve detaylı ilkeler ortaya koyan bir karardır. Web 2.0 içeriklerine ilişkin kararlarındaki isabetsizlikten sonra AİHM, makul ve hakkaniyetli bir içtihat geliştirebilmiştir.

§19. HØİNESS V. NORVEÇ

AİHM'nin 19 Mart 2019 tarihli *Høiness v. Norveç* kararı, internet platformunun sorumluluğunun ele alındığı bir karardır.[1067] Başvurucu, bir online tartışma platformunda kendisiyle ilgili yayımlanan yorumları gereğince önlemedikleri veya hızlıca kaldırmadıkları gerekçesiyle açtığı bir tazminat davasında yerel mahkemelerin bazı basın kuruluşlarını ve editörlerini tazminata mahkûm etmemesi sebebiyle AİHS'nin 8. maddesinde güvence altına alınan özel hayata saygı hakkının ihlal edildiğini iddia etmiştir.

I. Davanın gelişimi

AİHM'ye başvuru, Norveç vatandaşı Bayan Mona Høiness tarafından 3 Haziran 2014 tarihinde yapılmıştır.[1068] Bayan Høiness, Oslo'da yaşayan, ceza ve çocuk velayet davalarıyla tanınan bir avukattır. Eskiden bir *talk-show* sunucusu ve kamusal tartışmaların aktif katılımcısı olan Bayan Høiness, şu an bir iş adamı ile evlidir.[1069]

Bayan Høiness, 2010 yılında Basın Şikâyetleri Komisyonuna, Bay Trygve Hegnar'a ait ve onun tarafından kontrol edilen haftalık ve günlük gazeteler Kapital ve Finansavisen aleyhine iki başvuru yapmıştır. Aynı kişi, Hegnar Online adlı internet sitesinin de sahibidir ve siteyi yönetmektedir.[1070] Her üç yayın da 2010 yazının sonlarından itibaren, başvurucunun, kendisine miras bırakacak olan zengin ve yaşlı bir dul kadınla ilişkisine dair makaleler yayımlamıştır. Şikâyetin esası, bu yayınların, başvurucunun bahsi geçen kadını duygusal veya finansal olarak istismar ettiğine dair doğrudan veya dolaylı iddialarına ilişkindir. [1071] Dul hanıme-

---

[1067] **AİHM**, *Høiness v. Norveç*, Başvuru No: 43624/14, 19.6.2019.

[1068] *Høiness v. Norveç*, para. 1.

[1069] *Høiness v. Norveç*, para. 5.

[1070] *Høiness v. Norveç*, para. 6.

[1071] *Høiness v. Norveç*, para. 7.

fendi 2011 yılında öldükten sonra mirasçılarının açmış olduğu vasiyetin iptali davaları başvurucu lehine sonuçlanmış ve yukarıda adı geçen yayınlarda bu davaların içerikleri paylaşılmıştır.[1072]

Hegnar Online web sitesi, okuyucuların tartışmalar başlatabileceği ve yorum gönderebileceği -ayrı bir web adresinde fakat online gazete aracılığıyla erişim sağlanan- bir forum kurmuştur.[1073] Tüm içerikler kullanıcılar tarafından oluşturulmakta, forumda herhangi bir editoryal içerik bulunmamaktadır. Kullanıcıların anonim şekilde yorum yapmaları mümkündür ve kayıt yapma yükümlülüğü yoktur. İstatistiklere göre ayda 200.000 yorumun paylaşıldığı söz konusu forum Norveç'te türünün en büyüğü niteliğindedir. Denizcilik, BT, Finans, Emlak, Medya, Günün Teması şeklinde alt forum bölümleri mevcuttur.

5 Kasım 2010 tarihinde, forumda "Günün Teması" başlığında "*Bayan Høiness – Kapital'e göre dava büyüyor*" başlıklı bir içerik yayımlanmış ve bu başlık altında Bayan Høiness ile ilgili eleştirel ve hakaret içeren muhtelif içerikler paylaşılmıştır.[1074] İçeriklere anonim olarak farklı günlerde yorumlar yapılmış ve bu içerikler farklı sayılarda okunmuştur.

Başvurucu, 8 Kasım 2010 tarihinde Basın Şikâyet Komisyonuna başvurarak Hegnar Online sitesinde "Günün Teması" olarak yayımlanan içerikle ilgili şikâyette bulunmuştur.[1075] Bu süreçte bazı yorumlar silinmiştir. Tüm yorumların kaldırılmasına ilişkin uyarı neticesinde tespit edilen başka yorumlar da silinmiştir.[1076] Hegnar Online editörleri, platformlarının açık bir forum niteliğinde olduğunu ve içeriklerin ön kontrol gerçekleşmeksizin yayımlandığını belirtmiştir.[1077] Konuyu ele alan Basın Şikâyet Komisyonu, Kapital gazetesinin yanıltıcı başlığı ve Finansavisen gazetesinin başvurucuya cevap hakkı tanımaması sebebiyle gazetecilik meslek ilkelerini ihlal ettiğine karar vermiştir.[1078]

[1072] *Høiness v. Norveç*, para. 7.

[1073] *Høiness v. Norveç*, para. 8.

[1074] *Høiness v. Norveç*, para. 9.

[1075] *Høiness v. Norveç*, para. 10.

[1076] *Høiness v. Norveç*, para. 13.

[1077] *Høiness v. Norveç*, para. 14.

[1078] *Høiness v. Norveç*, para. 15.

28 Kasım 2010 tarihinde "Basın" başlığı altında başvurucuyla ilgili başka bir forum tartışması başlatılmış ve muhtelif tarihlerde bu başlık altında anonim şekilde içerikler paylaşılmaya devam etmiştir.[1079] Forumdaki bu yorumlar, paylaşılan verilere bakılırsa epeyce okunmuştur.[1080] Yapılan uyarı neticesinde bu içerikler de forumdan kaldırılmıştır.[1081]

7 Ocak 2011 tarihinde söz konusu forum sayfalarıyla ilgili Basın Şikâyet Komisyonuna müstakil bir başvuru yapılmış ve yayınların basın meslek ilkelerine aykırı olduğu ileri sürülmüştür.[1082]

7 Nisan 2011 tarihinde başvurucu, Hegnar Online'a bir bildirimde bulunarak hem Hegnar Online hem de sitenin editörü Bay H. hakkında tazminat davası açacağını; söz konusu içeriklerin hem Ceza Kanunu bağlamında hakaret suçunu teşkil ettiğini hem de Tazminat Kanunu uyarınca haksız fiil olduğunu ileri sürmüştür.[1083] Keza, içeriklerin cinsel saldırı niteliğinde olduğu ve özellikle kadınlara yönelik cinsiyetçi içerikleri sebebiyle AİHS'nin 10. maddesi bağlamında korunamayacağını belirtmiştir.[1084]

Hegnar Online ve Bay H., bu iddialar hakkında, sitelerinde uygun görülmeyen forum yorumlarına ilişkin basit bir şikâyet usulü geliştirdiklerini; her gönderinin yanına site yönetimine bildirim gönderen bir bağlantı koyulduğunu; bu tür bir şikâyet alındığında yorumun silindiğini; ayda 1.800 ila 2.000 arasında yorumun bu yöntemle silindiğini; tüm önlemlerin yanı sıra şirketin kendi moderatörlerinin şahsi inisiyatifleriyle forum yayın kurallarını ihlal eden içerikleri sildiğini; başvurucunun şikâyeti üzerine söz konusu yorumların sadece sekiz dakika içinde silindiğini; bir yorumun ise bizzat moderatörün tespitiyle kaldırıldığını belirtmiştir.[1085] Yorumların kendileri tarafından oluşturulmadığını, editoryal sorumluluklarına gidilemeyeceğini, şirkete sorumluluk atfedilemeyeceğini

[1079] *Høiness v. Norveç*, para. 16.
[1080] *Høiness v. Norveç*, para. 17.
[1081] *Høiness v. Norveç*, para. 18.
[1082] *Høiness v. Norveç*, para. 19.
[1083] *Høiness v. Norveç*, para. 20.
[1084] *Høiness v. Norveç*, para. 20.
[1085] *Høiness v. Norveç*, para. 21.

belirten Hegnar Online ve Bay H., başvurucuda oluşan hoşnutsuzluk sebebiyle kısmi bir ödeme önermiştir.

Başvurucu, Oslo Şehir Mahkemesinde Hegnar Media AS ve editör Bay H. aleyhine tazminat davası açmıştır.[1086] Öte yandan hakaret suçu iddiasıyla Norveç Ceza Kanunu çerçevesinde cezai süreci başlatmıştır. Bu iddialara karşı davalılar, konunun e-Ticaret Kanunu bağlamında çözülmesi gerektiğini; kasıtları olmadığı için Ceza Kanunu hükümlerinin uygulanamayacağını; yorumlardan haberdar olmadıklarından dolayı da editoryal sorumluluklarına gidilemeyeceğini ileri sürmüşlerdir.[1087]

4 Ocak 2012 tarihinde Oslo Şehir Mahkemesi davalılar lehine karar vermiş ve dava konusu üç yorumun hakaret niteliğinde olmadığına, başvurucunun onuruna ve şöhretine halel getirmediğine hükmetmiştir.[1088] Birinci yorumun, içerik olarak tatsız ve kaba olsa da başvurucunun kişilik haklarını ihlal etmediğini belirtmiştir.[1089] İkinci yorumu da tatsız ve gayriciddi olarak nitelendiren Şehir Mahkemesi benzer gerekçelerle bir ihlal olmadığına hükmetmiştir.[1090] Başvurucunun üçüncü bir kişiyle cinsel ilişkide bulunduğu iddiasına ilişkin olarak ise bunun kişinin şöhreti veya onurunu ihlal eden nitelikte sayılamayacağını, yorumda olumsuz bir nitelik olmadığını belirtmiştir.[1091] Mahkeme, diğer yorumlara da benzer şekilde yaklaşmış ve tüm talepleri reddetmiştir.[1092] Başvurucunun, yargılama giderlerini ve vekâlet ücretini ödemesine hükmetmiştir.

Başvurucu 31 Ocak 2012 tarihinde Şehir Mahkemesinin kararına Borgarting Yüksek Mahkemesinde itiraz etmiştir.[1093] İtirazı inceleyen Yüksek Mahkeme, kararını 24 Ekim 2013 tarihinde vermiştir.[1094] Yüksek Mahkeme, başvurucunun Hegnar Grubu ve diğer basın kuruluşlarında

[1086] *Høiness v. Norveç*, para. 22.
[1087] *Høiness v. Norveç*, para. 23.
[1088] *Høiness v. Norveç*, para. 24.
[1089] *Høiness v. Norveç*, para. 25.
[1090] *Høiness v. Norveç*, para. 26.
[1091] *Høiness v. Norveç*, para. 27.
[1092] *Høiness v. Norveç*, para. 28.
[1093] *Høiness v. Norveç*, para. 30.
[1094] *Høiness v. Norveç*, para. 31.

çok fazla sayıda habere konu edildiğini kabul etmekle beraber, başvurucunun neden kamuoyunun dikkatini çektiğini ele almak gerektiğini belirtmiş ve kapsamlı bir değerlendirme yapmıştır.[1095]

Dava konusu içeriklerin gayriciddi ve cinsiyetçi olduğunu kabul eden Yüksek Mahkeme, yine de bu içeriklerin tazminata yol açması konusunda Basın Şikâyet Komisyonundan farklı düşündüğünü belirtmiştir.[1096] Yüksek Mahkeme, başvurucunun tazminat talebinin ancak davalıların makul bir kusuru olduğu durumda gündeme gelebileceğini belirtmiştir.[1097] Bu kusurun ise yorumların tespiti ve akabinde kaldırılması için gerekenin yapılıp yapılmadığına göre belirlenmesi gerektiğine işaret etmiştir.[1098]

Yorumlar, herhangi bir ön sansür uygulanmadan, gerçek zamanlı olarak yayımlanmıştır. Bu bağlamda, Yüksek Mahkeme kontrolün ancak içerik yayımlandıktan sonra yapılacağını belirtmiştir.[1099] Diğer bir deyişle, *ex-ante* değil *ex-post* bir denetim yapılabileceğini ifade etmiştir.

İçeriğin kontrol edilmesi hususunda ise Yüksek Mahkeme, uyarı düğmelerinin bulunduğunu, yorumlara reaksiyon gösterilmesinin mümkün olduğunu not etmiştir.[1100] Editör olarak çalışanların da kendi inisiyatifleriyle içerikleri kontrol ettiklerini ve yorumları kaldırdıklarını belirtmiştir. Forumdaki içeriğin fazlalığına dikkat çeken Yüksek Mahkeme, sınırlı sayıda içeriğin kaldırılabildiğine işaret etmiştir.[1101] Mahkeme, öne çıkan üç yorumla ilgili de benzer bir değerlendirme yapmış ve itirazı reddetmiştir.[1102]

Başvurucu, Yüksek Mahkemenin kararını Temyiz Mahkemesine götürmüş ancak temyiz talebi yerinde görülmeyerek 7 Şubat 2014 tarihinde reddedilmiştir.[1103]

[1095] *Høiness v. Norveç*, para. 32-33.
[1096] *Høiness v. Norveç*, para. 34.
[1097] *Høiness v. Norveç*, para. 35.
[1098] *Høiness v. Norveç*, para. 35.
[1099] *Høiness v. Norveç*, para. 36.
[1100] *Høiness v. Norveç*, para. 37.
[1101] *Høiness v. Norveç*, para. 37.
[1102] *Høiness v. Norveç*, para. 38-40.
[1103] *Høiness v. Norveç*, para. 41-42.

II. Hukuki arka plan

AİHM, konunun esasına girmeden evvel hakaret suçunu düzenleyen Ceza Kanunu, hukuki sorumluluğun esaslarını düzenleyen Tazminat Kanunu, Cinsiyet Eşitliği Kanunu gibi muhtelif iç hukuk düzenlemesine ve AİHS'ye atıf yapmıştır.[1104] Keza, 23 Mayıs 2003 tarihli e-Ticaret Kanunu'nun 18. maddesine atıf yapmıştır. "Belirli barındırma hizmetlerinin sorumluluktan muafiyeti" başlıklı söz konusu hüküm şöyledir:

"Bir hizmet alıcısının talebi üzerine bilgi barındıran bir hizmet sağlayıcısı yalnızca

(a) kasten hareket ederek hukuka aykırı bilgiyi barındırmış veya hukuka aykırı bilgiyi barındırarak hukuka aykırı faaliyetlere katkı sunmuşsa cezalandırılır, veya

(b) kasten veya ağır ihmalle hareket ederek hukuka aykırı bilgiyi barındırmışsa veya hukuka aykırı bilgiyi barındırarak hukuka aykırı faaliyetlere katkı sunmuşsa tazminat ödemekle yükümlüdür.

Hizmet sağlayıcı, birinci fıkrada belirtilen kasıt veya ağır ihmal durumunda, gecikme olmaksızın bilgiyi kaldırmak veya bilgiye erişimi engellemek için gerekli önlemleri alırsa cezai ve hukuki sorumluluktan her koşulda muaftır.

Bir hizmet sağlayıcısı, eğer ki hizmet alıcısı onun adına hareket ediyor veya onun kontrolü altındaysa bu maddede öngörülen sorumluluktan muaf değildir."

III. Başvurucunun iddiaları

Başvurucu, AİHS'nin 8. maddesiyle güvence altına alınan özel hayata saygı hakkının ihlal edildiğini iddia etmiştir. Norveç Hükûmeti, bu iddiaya itiraz etmiştir. AİHM, başvuruyu temelli görmüş ve kabul edilebilir bularak esası incelemiştir.[1105]

[1104] *Høiness v. Norveç*, para. 43-47.

[1105] *Høiness v. Norveç*, para. 50.

Başvurucu, mevzubahis yorumların açıkça hukuka aykırı olduğunu ve yerel mahkemelerin, AİHS'nin 8 ve 10. maddesiyle korunan haklarının dengelenmesi hususunu gereğince gözetmediğini ileri sürmüştür.[1106] Başvurucu, miras davasının kamuyu ilgilendirdiğini kabul etmektedir fakat Hegnar Online ve diğer iki yayıncının makalelerinin dengeli olmadığını belirtmiştir.[1107] Başvurucu, bu iddiasını Basın Şikâyetleri Komisyonunun gazetecilik ilkelerini ihlale ilişkin tespitine dayandırmıştır.

Hegnar Online tarafından bir uyarı düğmesi koyulmuş ve bazı çalışanlar forumdaki içerikleri takip etmek için görevlendirilmişse de bu açıkça yetersizdir. Başvurucuya göre forumda paylaşılan büyük ölçekteki yorumları ele almada bu sistem yetersiz kalmıştır.[1108] Başvurucu, anonim yorum yapanları bizzat kendisi tespit edebilecek durumda değildir.[1109]

Üçüncü kişilerin yorumlarından dolayı sorumluluğun internet ortamında ifade özgürlüğü üzerinde olumsuz etki göstereceğine ilişkin olarak ise başvurucu, söz konusu sitenin Norveç'teki en büyük platform ve tartışma forumu olduğunu ve sorumluluğun olumsuz bir etki doğurmayacağını iddia etmiştir.[1110] Başvurucunun yerel mahkemelerce yargılama giderleri ile vekâlet ücretini ödemeye mahkûm edilmesi ise AİHS'nin 8. maddesinin müstakil ihlal sebebi olarak gösterilmiştir.[1111]

IV. Norveç Hükûmetinin savunması

Norveç Hükûmeti, yorumların AİHS'nin 8. maddesinde güvence altına alınan özel hayata saygı hakkını ihlal edecek seviyede olmadığını ileri sürmüştür.[1112] Norveç Hükûmeti, bu iddiasını başvurucunun şöhreti ve söz konusu miras davasının kamuoyunda bilinirliği üzerine inşa etmiş, Yüksek Mahkemenin yerel yargılamada konuyu gereğince ele aldığını belirtmiş-

[1106] *Høiness v. Norveç*, para. 51.
[1107] *Høiness v. Norveç*, para. 52.
[1108] *Høiness v. Norveç*, para. 53.
[1109] *Høiness v. Norveç*, para. 54.
[1110] *Høiness v. Norveç*, para. 55.
[1111] *Høiness v. Norveç*, para. 56.
[1112] *Høiness v. Norveç*, para. 57.

tir.[1113] Başvurucu tarafından yorumları oluşturan anonim hesaplara yönelik hukuki bir süreç başlatılmadığına işaret eden Norveç Hükûmeti, *Pihl v. İsveç* kararına atıf yaparak mevcut davada da benzer bir durumun olduğunu ve bir ihlal bulunmadığını ileri sürmüştür.[1114] Keza, yargılama giderleri açısından da hukuka aykırı bir uygulama olmadığını tekrarlamıştır.[1115]

V. AİHM'nin tespit ve değerlendirmeleri

Başvuruyu ele alan AİHM, öncelikle AİHS'nin 8. maddesi bağlamında özel hayatın tanımına ilişkin muhtelif içtihatlarına atıf yapmış ve bir kişinin itibarının korunması hakkının 8. maddede düzenlenen özel hayatın korunması hakkı kapsamında olduğuna ilişkin tespitini tekrarlamıştır.[1116] Bu tekrardan sonra ise 8. maddenin işletilebilmesi için ihlalin belirli bir seviyeye ulaşması gerektiğine ilişkin içtihatlarını hatırlatmıştır.[1117]

AİHM'ye göre mevcut uyuşmazlık, bir devlet eylemi sebebiyle ihlalden öte, başvurucunun özel hayatının korunmasına ilişkin olarak yerel mahkemelerin sunduğu korumanın yetersizliği ile ilgilidir.[1118] Devletlerin bu konudaki pozitif ve negatif yükümlülüklerine değinen AİHM, her iki durumda da sorumlulukların benzer olduğunu belirtmiştir. Bu doğrultuda, ilgili yarışan haklar arasında makul bir denge kurulması gerektiğini ve her bağlamda devletlerin belirli ölçüde takdir alanı olduğunu hatırlatmıştır.[1119] Bu çerçevede, *Delfi AS v. Estonya* kararındaki tespitlerine atıf yapmıştır.[1120]

Peki, sorumluluk rejimi tesis edilirken nasıl bir yol izlenmelidir? AİHM, bu bağlamda, *MTE ve Index.hu Zrt v. Macaristan* kararındaki kri-

---

[1113] *Høiness v. Norveç*, para. 58-59.
[1114] *Høiness v. Norveç*, para. 60-61.
[1115] *Høiness v. Norveç*, para. 62.
[1116] *Høiness v. Norveç*, para. 63.
[1117] *Høiness v. Norveç*, para. 64.
[1118] *Høiness v. Norveç*, para. 65.
[1119] *Høiness v. Norveç*, para. 65.
[1120] *Høiness v. Norveç*, para. 66.

terleri hatırlatmıştır.[1121] Bu bağlamda, sorumluluk tesisinde, yorumların bağlamı, şirketin hakaret içeren yorumları önlemek veya kaldırmak için aldığı tedbirler, aracı platformun sorumluluğuna alternatif olarak gerçek içerik sağlayıcı kişilerin sorumluluğu ve şirket aleyhine iç hukuktaki yargılamaların neticesi gibi kriterler dikkate alınmalıdır.

Tüm bu tespitlerden sonra AİHM, mevcut uyuşmazlıkta başvurucunun AİHS'nin 8. maddesiyle güvence altına alınan özel hayatına saygı hakkı ile online haber ajansı ve forum işleteninin AİHS'nin 10. maddesiyle korunan ifade özgürlüğü hakkının makul şekilde dengelenip dengelenmediğini değerlendirmeye almıştır.[1122]

AİHM, *Delfi AS v. Estonya* kararının aksine ve *Rolf Anders Daniel Pihl v. İsveç* içtihadına benzer şekilde, ihtilaf konusu olan yorumlar nefret söylemi veya şiddete teşvik niteliğinde olmadığı için içeriklerin derinlemesine incelenmesine gerek olmadığını belirtmiştir.[1123] Mahkeme, yorumları yazan anonim kişi veya kişilerle hukuki anlamda mücadele etmenin önündeki külfetin ve engellerin varlığına işaret ederek buna itiraz etmediğini belirtmiştir.[1124]

Hegnar Online sitesinin popüler ve ticari bir haber platformu olduğunu belirten AİHM, forum sayfalarındaki tartışmaların editoryal haberlerin bir devamı olarak nitelendirilemeyeceğine kanaat getirmiştir.[1125]

Mahkeme, Hegnar Online sitesinde yorum kısmının kötüye kullanılmasını engellemek için alınan önlemleri incelemiştir. Tekrarlamak gerekirse, içerikleri izlemek için moderatör sistemi kurulmuş, hukuka aykırı nitelikteki içeriklerin ihbar edilmesi için uyarı mekanizması geliştirilmiş ve e-posta gibi yöntemlerle uyarı verilmesi sağlanmıştır.[1126] Bu tespitler-

[1121] *Høiness v. Norveç*, para. 67.
[1122] *Høiness v. Norveç*, para. 68.
[1123] *Høiness v. Norveç*, para. 69.
[1124] *Høiness v. Norveç*, para. 70.
[1125] *Høiness v. Norveç*, para. 71.
[1126] *Høiness v. Norveç*, para. 72.

den sonra AİHM, Yorum 1 ve Yorum 2 içeriklerinin kaldırılması sürecine ve yerel mahkemelerin kararlarına atıfta bulunmuştur.[1127]

AİHM, yerel mahkemelerin başvurucunun talebini incelediğini ve değerlendirdiğini, tüm iddiaları gereğince ele aldığını belirtmiş ve *Delfi AS v. Estonya* kararında belirtilen ilkeler doğrultusunda, yerel mahkemelerin görüşünün aksine bir görüş benimsemeyi gerektirecek bir durum olmadığına kanaat getirmiştir.[1128]

AİHM, mevcut uyuşmazlıkta başvurucunun AİHS'nin 8. maddesi tahtında güvence altına alınan özel hayatına saygı hakkı ile online haber ajansı ile forum işleteninin AİHS'nin 10. maddesi tahtında güvence altına alınan ifade özgürlüğü hakkının yerel mahkemelerce makul şekilde dengelendiğine hükmetmiştir.[1129] Keza, yargılama giderlerine ilişkin hak ihlali iddiasını da yerinde bulmamıştır.[1130] Tüm bu tespitler ışığında AİHM, oy birliğiyle başvuruyu kabul edilebilir görmüş, AİHS'nin 8. maddesinin ihlal edilmediğine hükmetmiştir.

VI. Değerlendirme

AİHM'nin *Høiness v. Norveç* kararı, Mahkemenin önceki içtihatlarından *Rolf Anders Daniel Pihl v. İsveç* kararı ile uyumlu bir karardır. *Delfi AS v. Estonya* kararındaki kriterleri tekrar eden Mahkeme, platformların, kullanıcıları tarafından oluşturulan içeriklerden dolayı sorumluluğunu nefret söylemi veya şiddete davet içerme ve içermemeye göre farklı şekilde ele almaktadır. Şayet nefret söylemi içeren veya şiddete davet eden bir içerik var ise platformun içeriklerle proaktif şekilde mücadele edecek bir mekanizma kurması zorunludur. Bu hatalı yaklaşım, Web 2.0 platformlarının işleyişiyle bağdaşmasa da AİHM bu konudaki yaklaşımını istikrarlı olarak sürdürmektedir.

[1127] *Høiness v. Norveç*, para. 73.

[1128] *Høiness v. Norveç*, para. 74.

[1129] *Høiness v. Norveç*, para. 75.

[1130] *Høiness v. Norveç*, para. 76-77.

§20. KABLİS V. RUSYA

AİHM'nin 30 Nisan 2019 tarihli *Kablis v. Rusya* kararı, internet içeriğine erişimi engellemek için idari makamlara yetki verilmesinin hukuka uygunluğunun tartışıldığı bir karardır.[1131]

I. Davanın gelişimi

AİHM'ye başvuru, Rus vatandaşı Bay Grigoriy Nikolayevich Kablis tarafından 28 Temmuz 2016 ve 30 Temmuz 2017 tarihlerinde yapılmış ve Mahkeme, bu iki başvuruyu birleştirmiştir.[1132] Başvurucu, ifade özgürlüğü ile toplanma hürriyetinin ihlal edildiğini ve kendisine etkin bir hukuki koruma sağlanmadığını iddia etmiştir.[1133]

19 Eylül 2015 tarihinde Rus Federal Güvenlik Teşkilatı ve Rusya Federasyonu Soruşturma Komitesi tarafından Komi Cumhuriyeti yöneticileri hakkında suç çetesine üyelik ve dolandırıcılık şüphesiyle bir soruşturma açılmış ve söz konusu kişiler aynı gün tutuklanmıştır.[1134] 21 Eylül 2015 tarihinde başvurucu, Bayan S. ile birlikte Syktyvkar İlçe İdaresine müracaat ederek 25 Eylül 2015 tarihinde Komi Cumhuriyeti tutuklamalarına ilişkin gösteri yapma niyetlerini bildirmiştir.[1135] Aynı gün, bu gösteri talebine ilişkin bilgileri blog sitesinde yayımlamıştır.[1136]

Syktyvkar İlçe İdaresi talebi reddederek başvurucuya alternatif bir toplanma alanı önermiştir.[1137] Başvurucu, talebinin reddedildiğini ve ilgili diğer gelişmeleri de 22 Eylül 2015 tarihinde blog sitesinde yayım-

---

[1131] **AİHM**, *Kablis v. Rusya*, Başvuru No: 48310/16 ve 59663/17, 30.4.2019.

[1132] *Kablis v. Rusya*, para. 1.

[1133] *Kablis v. Rusya*, para. 3.

[1134] *Kablis v. Rusya*, para. 6.

[1135] *Kablis v. Rusya*, para. 7.

[1136] *Kablis v. Rusya*, para. 8.

[1137] *Kablis v. Rusya*, para. 9.

lamıştır.[1138] Ayrıca, 23 Eylül 2015 tarihinde Facebook sitesine benzer Rus sosyal medya sitesi olan VKontakte sitesinde, kamusal tartışmalara katılmaya çağıran bir içerik paylaşmıştır.[1139]

İçeriğin yayımlanmasından sadece bir gün sonra, 24 Eylül 2015 tarihinde, başvurucunun VKontakte hesabı, Rusya Federal Haberleşme, Bilgi Teknolojileri ve Kitle İletişim Denetleme Kurumu (Roskomnadzor) ve bir Rusya Federasyonu başsavcı vekilinin talimatları doğrultusunda VKontakte site yönetimi tarafından kapatılmıştır.[1140] Kamusal Etkinlikler Kanunu'nun 10. maddesi bağlamında hukuka aykırı şekilde gösteri düzenlemeye çağrı yapılması sebebiyle Bilgi Kanunu'nun 15. maddesinin üçüncü fıkrası uyarınca hesabın engellendiği belirtilmiştir.[1141]

Başvurucu, müteakip günlerde, blog sayfasına kişileri halk meclisine davet eden üçüncü bir içerik eklemiştir.[1142] Başsavcılığın talebi üzerine, söz konusu blog sitesini barındıran hizmet sağlayıcı tarafından ilgili blog sayfalarına erişim engellenmiş ve bu durum başvurucuya e-postayla bildirilmiştir.[1143] 25 Eylül 2015 tarihinde elliye yakın kişi Lenin heykelinin yanında toplanarak herhangi bir olay çıkmadan dağılmıştır.[1144]

Başvurucu, gösteri yapma talebinin reddine ilişkin karara Syktyvkar Yerel Mahkemesinde itiraz etmiş ve idare tarafında önerilen yerin uygun olmadığını ileri sürmüştür.[1145] Syktyvkar Yerel Mahkemesi 18 Kasım 2015 tarihinde talebi reddetmiştir. Kararın iptali için açılan iptal davası da reddedilmiştir.[1146] Başvurucu, gösteri yapmak istedikleri alanın yasaklı alan olmadığını, ilgili idare tarafından yasaklı alanları belirleyen genelgenin yayımlanmadığını ve dolayısıyla kamu tarafından erişilebilir

[1138] *Kablis v. Rusya*, para. 10.
[1139] *Kablis v. Rusya*, para. 11.
[1140] *Kablis v. Rusya*, para. 12.
[1141] *Kablis v. Rusya*, para. 12.
[1142] *Kablis v. Rusya*, para. 13.
[1143] *Kablis v. Rusya*, para. 14.
[1144] *Kablis v. Rusya*, para. 15.
[1145] *Kablis v. Rusya*, para. 16.
[1146] *Kablis v. Rusya*, para. 17.

olmadığını ileri sürerek kararı temyiz etmiştir.[1147] 28 Kasım 2016 tarihli kararıyla Komi Cumhuriyeti Temyiz Mahkemesi, temyiz talebini benzer gerekçelerle reddetmiştir.[1148] Bu karara itiraz da reddedilmiştir.[1149]

Başvurucu, diğer yandan VKontakte sitesindeki hesabının kapatılması ve üç içeriğe erişimin engellenmesi kararlarına karşı da hukuki süreç başlatmıştır.[1150] Başvurucu, engellemelerin demokratik bir toplumda gerekli olmadığını, ifade özgürlüğünün ihlal edildiğini belirtmiş ve manevi olarak zarar gördüğünü ileri sürmüştür.

Syktyvkar Yerel Mahkemesi, başvurucunun talebini 5 Nisan 2016 tarihinde reddetmiştir.[1151] Mahkemeye göre, engellemenin hukuki dayanağı vardır ve bilginin yayılması bağlamında hukuka aykırılığı önlemeyi amaçlamaktadır.[1152] Keza, belirli bir gönderi yerine VKontakte hesabının tamamına erişimin engellenmesinin de hukuki dayanağı bulunduğu, bu dayanağın internet ortamında gerçek zamanlı erişilebilir içeriklerin paylaşılmasının doğası dikkate alınarak tüm hesaba erişimi engellemeye imkân tanıdığı belirtilmiştir.[1153] Başvurucunun manevi haklarının da ihlal edilmediğini belirten Mahkeme, talebin reddedilmesi gerektiğine hükmetmiştir.

Yerel mahkemenin kararına itirazı inceleyen Komi Cumhuriyeti Temyiz Mahkemesi, 7 Temmuz 2016 tarihli kararıyla, yerel mahkeme kararının hukuka uygun olduğunu, makul ve yerinde bir gerekçesi bulunduğunu belirterek talebi reddetmiştir.[1154] Bu karara karşı yapılan tüm itirazlar da reddedilerek iç hukuk yolları tüketilmiştir.[1155]

[1147] *Kablis v. Rusya*, para. 18.
[1148] *Kablis v. Rusya*, para. 19.
[1149] *Kablis v. Rusya*, para. 20-21.
[1150] *Kablis v. Rusya*, para. 22.
[1151] *Kablis v. Rusya*, para. 23.
[1152] *Kablis v. Rusya*, para. 23.
[1153] *Kablis v. Rusya*, para. 23.
[1154] *Kablis v. Rusya*, para. 24.
[1155] *Kablis v. Rusya*, para. 24-25.

II. Hukuki arka plan

AİHM, konunun esasına girmeden evvel muhtelif iç hukuk düzenlemesine, idari karara ve mahkeme içtihadına atıf yapmıştır. Mahkeme, toplantı ve gösteri hakkının kısıtlandığı iddialarına ilişkin Temyiz Mahkemesinin 28 numaralı ve 26 Haziran 2018 tarihli kararına, 91-RZ numaralı ve 29 Kasım 2012 tarihli Komi Cumhuriyeti Kanunu'nun "Komi Cumhuriyeti'nde kamusal etkinliklerin düzenlenmesiyle" ile ilgili 5. bölümüne, Syktyvkar İlçe İdaresinin 9/3483 tarihli ve 4 Eylül 2013 tarihli genelgesine ve İdari Usul Kanunu'na atıfta bulunmuştur.

Erişimin engellenmesinin hukukiliğine ilişkin ise 149-FZ numaralı 27 Temmuz 2006 tarihli Bilgi, Bilgi Teknolojileri ve Bilginin Korunması Kanunu'nun 15.3 bölümüne atıf yapmıştır. Söz konusu düzenleme şöyledir:

"1. *İnternet dâhil telekomünikasyon ağlarında kitlesel düzensizliğe, radikal faaliyetlere veya mevcut usullere aykırı bir şekilde kitlesel (kamusal) etkinliklere katılmaya çağıran bir bilgi tespit edilirse -federal Devlet makamları, bölgesel Devlet otoriteleri, belediyeler, teşkilatlar veya vatandaşlar tarafından tespit dâhil- Rusya Federasyonu Başsavcısı veya vekilleri bilgiyi yayan bilgi ortamına erişimin engellenmesine yönelik tedbirlerin alınması için kitlesel medya, kitlesel haberleşme ve bilgi teknolojileri konusunda yetkili kolluk kuvvetine talimat verir.*

2. Birinci fıkra kapsamındaki talimatı alan kitlesel medya, kitlesel haberleşme ve bilgi teknolojileri konusunda yetkili federal kolluk kuvveti derhâl şunları yapmalıdır:

(1) *Hizmet sağlayıcıya, kitlesel düzensizliğe, aşırılık yanlısı faaliyetlere veya mevcut usullere aykırı bir şekilde kitlesel (kamusal) etkinliklere katılmaya çağıran bilgi içeren web sitesine veya web sitesinde yer alan bilgi ortamına erişimin kısıtlanmasına yönelik tedbirleri alması için talimat verir. Talimat web sitesinin alan adını, ağ adresini ve bilginin tespit edilmesini sağlayacak web sayfasının yeknesak kaynak belirleyici (URL) adresini içermelidir.*

(2) *Kitlesel düzensizliğe, aşırılık yanlısı faaliyetlere veya mevcut usullere aykırı bir şekilde kitlesel (kamusal) etkinliklere katılmaya çağıran bilgi içeren internet gibi telekomünikasyon ağında yer sağlayıcıyı veya bilgi ortamını barındıran kişiyi veya bu tür içerikleri barındıran web sitesinin sahibine hizmet sağlayanları tespit etmelidir.*

(3) *Yer sağlayıcı veya ikinci fıkrada belirtilen kişiye bilgi yayımlama kurallarının ihlallerine ilişkin, kitlesel düzensizliğe, aşırılık yanlısı faaliyetlere veya mevcut usullere aykırı bir şekilde kitlesel (kamusal) etkinliklere katılmaya çağıran bilgi içeren web sitesinin tanımlanmasına imkân verecek ilgili alan adını ve ağ adresini belirten ve bu tür bilginin silinmesi talimatını da içeren Rusça ve İngilizce elektronik bir bildirim göndermelidir.*

(4) *Yer sağlayıcıya veya ikinci fıkrada belirtilen kişiye iletilen bildirimin tarih ve zamanının kaydını özel bir elektronik sicilde tutmalıdır.*

3. İnternet telekomünikasyon ağına erişim izni veren haberleşme hizmet sağlayıcısı, kitlesel medya, kitlesel haberleşme ve bilgi teknolojileri konusunda yetkili federal birimden erişimin engellenmesine ilişkin tedbirleri uygulama talimatı aldığı zaman, kitlesel düzensizliğe, aşırılık yanlısı faaliyetlere veya mevcut usullere aykırı bir şekilde kitlesel (kamusal) etkinliklere katılmaya çağıran bilgi içeren web sitesine veya web sitesinde yer alan bilgi ortamına erişimi derhâl engellemelidir.

4. Yer sağlayıcı veya ikinci fıkranın ikinci bendinde belirtilen kişi, ikinci fıkranın üçüncü bendinde zikredilen bildirimi almasından itibaren yirmi dört saat içerisinde, bilgi kaynağının sahibine bildirimle ilgili ve kitlesel düzensizliğe, aşırılık yanlısı faaliyetlere veya mevcut usullere aykırı bir şekilde kitlesel (kamusal) etkinliklere katılmaya çağıran bilgiyi gecikmeksizin silmesinin gerekli olduğuna dair bilgi vermelidir.

5. Bilgi ortamının sahibi, kitlesel düzensizliğe, aşırılık yanlısı faaliyetlere veya mevcut usullere aykırı bir şekilde kitlesel (kamusal) etkinliklere katılmaya çağıran bilgiyi silerse kitlesel medya, kitlesel haberleşme ve bilgi teknolojileri konusunda yetkili federal birime bir bildirim göndermelidir. Bu tür bildirim elektronik olarak da gönderilebilir.

6. Beşinci fıkrada belirtilen bildirimi aldıktan ve doğruluğunu teyit ettikten sonra, kitlesel medya, kitlesel haberleşme ve bilgi teknolojileri konusunda yetkili federal birim, internet telekomünikasyon ağına erişim izni veren haberleşme hizmet sağlayıcısına, web sitesi gibi bilgi ortamına erişimi tekrar açabileceğine dair derhâl bir bildirim göndermelidir.

7. Haberleşme hizmet sağlayıcısı, altıncı fıkrada belirtilen bildirimi alması üzerine web sitesi gibi bilgi ortamına erişimi derhâl tekrar açmalıdır."

III. Tarafların iddiaları

AİHM, *Kablis v. Rusya* kararında iki farklı hukuki meseleyi karara bağlamıştır. İlk mesele, yukarıda belirtildiği üzere, başvurucunun toplantı ve gösteri hakkına bir kısıtlama getirildiği iddiasına ilişkindir. AİHM, kararının ilk bölümünü bu meseleye ayırmış ve başvurucunun AİHS'nin 11. maddesinde güvence altına alınmış olan toplantı ve örgütlenme özgürlüğü ile 13. maddesinde güvence altına alınmış olan etkili başvuru hakkının ihlal edildiğine hükmetmiştir.[1156]

İkinci mesele ise başvurucunun VKontakte sosyal ağındaki hesabının kapatılmasının ve blog içeriklerine erişimin engellenmesinin AİHS'nin 10. maddesinde güvence altına alınmış olan ifade özgürlüğünü ihlal edip etmediği ile ilgilidir.[1157]

AİHM, söz konusu şikâyetin AİHS'nin 35. maddesinin üçüncü fıkrası anlamında açıkça dayanaktan yoksun olmadığını tespit etmiş ve başkaca bir kabul edilemezlik engeli de bulunmayan işbu şikâyetin kabul edilebilir olduğuna karar vermiştir.[1158]

Başvurucu, VKontakte hesabını ve blog sayfasını kamusal konularda görüşlerini ifade etmek için kullandığını ve yapılan engellemelerin ifade özgürlüğünü kısıtladığını ileri sürmüştür.[1159] Aynı doğrultuda, engel-

[1156] İnternet hukuku konusuyla doğrudan bağlantılı olmadığı için söz konusu kısımlar detaylıca incelenmemiştir. Bu konuda bkz. *Kablis v. Rusya*, para. 39-72.

[1157] *Kablis v. Rusya*, para. 73.

[1158] *Kablis v. Rusya*, para. 74.

[1159] *Kablis v. Rusya*, para. 75.

lemeye dayanak oluşturan Bilgi Kanunu'nun 15. maddesinin üçüncü fıkrasının öngörülebilir bir düzenleme olmadığını, "*mevcut usullere aykırı bir şekilde*" ibaresinin açıklıktan uzak olduğunu, kötüye kullanımı önlemek için gerekli mekanizmaları içermediğini belirtmiştir.[1160] Keza, blog sayfasına yönelik erişim engellemesi tedbirinin yargısal bir ön denetim olmaksızın kolluk kuvvetlerince uygulanmasının ve spesifik sayfa URL engellemesi mümkünken tüm hesabının engellenmesinin hukuka aykırı olduğunu iddia etmiştir.[1161]

Başvurucu, ifade özgürlüğüne yönelen müdahalenin meşru bir amaç gütmediğini ve demokratik bir toplumda gerekli olmadığını belirtmiştir.[1162] Rus makamlarının bu bağlamda kendisine sıfır tolerans gösterdiğini ileri sürmüştür. En önemlisi, VKontakte hesabına erişim tamamen kesilmek suretiyle, sadece hukuka aykırı görülen değil diğer tüm içeriğe de erişimin engellendiğini, mahkemelerin engelleme kararına yüzeysel olarak baktığını, ölçülülük ve demokratik toplumda gereklilik testlerini gereğince uygulamadıklarını iddia etmiştir.[1163]

Rus Hükûmeti ise bu iddialara karşı çıkmış ve söz konusu içeriklerin, başvurucunun kamusal etkinliğe yönelik görüşlerinden ziyade izinsiz bir kamusal etkinliğe çağrı içerdiğini, hukuka aykırı niteliğinden dolayı engellendiğini ileri sürmüştür.[1164] Aynı doğrultuda, VKontakte hesabının tamamen engellenmesinin iç hukukta kanuni dayanağı olduğunu ve bunun internet ortamında gerçek zamanlı veri paylaşımıyla meşru kılındığını belirtmiştir.[1165] Ayrıca, içeriğin silinmesi durumunda başvurucunun hesabının tekrar açılabileceğini tartışmış, dilerse alternatif bir sosyal ağ hesabı oluşturabileceğini vurgulamış ve bu sebeplerle ifade özgürlüğünün ölçüsüzce kısıtlanmadığını iddia etmiştir.[1166]

[1160] *Kablis v. Rusya*, para. 76.
[1161] *Kablis v. Rusya*, para. 76.
[1162] *Kablis v. Rusya*, para. 77.
[1163] *Kablis v. Rusya*, para. 77.
[1164] *Kablis v. Rusya*, para. 78.
[1165] *Kablis v. Rusya*, para. 78.
[1166] *Kablis v. Rusya*, para. 78.

IV. AİHM'nin tespit ve değerlendirmeleri

AİHM, ifade özgürlüğünün demokratik bir toplumun temelini ve her bireyin kendini geliştirmesi ve tatmin olması için en önemli şartlardan birini oluşturduğuna; AİHS'nin 10. maddesinin ikinci fıkrasının sadece zararsız olan düşünceler için değil, aynı zamanda rahatsızlık veren düşünceler için de geçerli olduğuna; bütün bunların da demokratik bir toplumun özellikleri olan çoğulculuk ve hoşgörünün gerekleri olduğuna dair içtihatlarını alıntılamıştır.[1167] Mahkeme, aynı doğrultuda, AİHS'nin 10. maddesinin ifade özgürlüğünü "herkes" açısından güvence altına aldığını; maddede, amaçlanan hedefin doğasına yahut gerçek veya tüzel kişilerin bu özgürlüğün kullanılmasında oynadıkları rollere göre bir ayrım yapılmadığını; bilgi dağıtım araçlarına getirilen her türlü kısıtlamanın bilgi alma ve verme özgürlüğüne dokunduğunu; maddenin yalnızca bilgilerin iletilmesi hakkını değil, aynı zamanda toplum açısından bilgi alma hakkını da güvence altına aldığını belirten *Ahmet Yıldırım v. Türkiye* gibi içtihatlarını tekrarlamıştır.[1168]

İfade özgürlüğüne ilişkin bu genel hatırlatmalardan sonra AİHM, internete ilişkin yaklaşımını tekrarlamıştır. İnternet sitelerinin ifade özgürlüğünün kullanılması açısından önemine ilişkin "*[E]rişilebilirliğinin yanı sıra büyük miktarda veriyi muhafaza etme ve dağıtma kapasitesi sayesinde internet, kamunun güncele erişiminin iyileştirilmesine ve bilginin iletilmesinin kolaylaştırılmasına önemli derecede katkıda bulunmaktadır.*" içtihadını hatırlatan Mahkeme, internette kullanıcılar tarafından gerçekleştirilen anlatım faaliyetinin, interneti ifade özgürlüğünün kullanılması bakımından emsalsiz bir platform kıldığını vurgulayan *Delfi AS v. Estonya* gibi içtihatlarını alıntılamıştır.[1169]

AİHM'ye göre AİHS'nin 10. maddesinin ikinci fıkrası çerçevesinde "gereklilik", "acil toplumsal ihtiyacın" varlığını ifade etmektedir. AİHS'ye taraf devletler, bu tür bir ihtiyacın mevcut olup olmadığını değerlendirmede belli bir takdir payına sahiptir. Ancak bu, gerek yasaları gerek

[1167] *Kablis v. Rusya*, para. 79.

[1168] *Kablis v. Rusya*, para. 80.

[1169] *Kablis v. Rusya*, para. 81.

bağımsız bir mahkeme tarafından alınmış olanlar da dâhil bu yasaları uygulamaya yönelik kararları kapsayan Avrupa denetimi ile bir arada yürümektedir.[1170] Bu hatırlatmasından sonra Mahkeme, "bir kısıtlamanın" 10. madde tarafından korunan ifade özgürlüğüyle bağdaştırılabilir olup olmadığı konusunda nihai kararı verme yetkisinin kendisinde olduğunu hatırlatmıştır.[1171]

AİHM son olarak bir ihlale ilişkin inceleme yaparken nasıl bir usul takip ettiğini şöyle açıklamıştır: Denetleyici yargı yetkisini kullanırken Mahkemenin görevi yetkili ulusal makamların yerini almak değil, daha ziyade bu makamların takdir yetkileri uyarınca vermiş olduğu kararları 10. madde kapsamında yeniden gözden geçirmektir.[1172] Mahkemenin söz konusu denetimi, davalı devletin, takdir payını makul, dikkatli bir şekilde ve iyi niyet içerisinde kullanıp kullanmadığını belirlemekle sınırlı değildir. Mahkeme, hakkında şikâyette bulunulan müdahaleye davanın bütünü ışığında bakmalı, müdahalenin "güdülen meşru amaçla orantılı"lığını, ulusal makamların söz konusu müdahaleyi haklı çıkarmak için ileri sürdüğü gerekçelerin "ilgili ve yeterli" olup olmadığını belirlemelidir. Bunu yaparken Mahkeme, ulusal makamların, 10. maddede yer alan ilkelerle bağdaşan standartlar uygulamış ve dahası ilgili olaylar hakkında kabul edilebilir bir değerlendirmeye dayanmış olduğuna kanaat getirmelidir.[1173]

Mahkeme, başvurucunun İlçe İdaresi tarafından onaylanmamış bir kamusal etkinliğe çağrı içeren sosyal medya hesabı ile üç blog gönderisinin Başsavcı vekili tarafından engellenmesinin, başvurucunun ifade özgürlüğüne kamusal bir müdahale niteliğinde olduğunu ve başvurucunun başka bir hesap oluşturması ve içerik paylaşması imkânının bulunmasının bu nitelendirmeyi etkilemediğini belirtmiştir.[1174] Bu tür bir müdahalenin AİHS'nin 10. maddesi bağlamında ihlal teşkil edip etmediğinin

[1170] *Kablis v. Rusya*, para. 82.
[1171] *Kablis v. Rusya*, para. 82.
[1172] *Kablis v. Rusya*, para. 83.
[1173] *Kablis v. Rusya*, para. 83.
[1174] *Kablis v. Rusya*, para. 84.

tespitinde kanunla öngörülme, demokratik bir toplumda gereklilik gibi kriterlerin incelenmesi gerekmektedir.[1175]

AİHM, somut olaydaki müdahalenin Bilgi Kanunu'nun 15. maddesinin üçüncü fıkrasına dayalı olarak gerçekleştirildiğini belirtmiştir.[1176] Yerel mahkemelerin tespitlerine değinen AİHM, amaç kamu düzeni ihlallerini önlemek olsa da AİHS'nin diğer maddelerinin aksine 10 ve 11. maddenin kamu düzeninin sağlanması ve korunmasını amaçlayan sınırlamalara izin vermediğini belirtmiştir.[1177] Mahkemeye göre, esasında Rus Hükûmeti bu amaca dayanmamıştır.

AİHM'ye göre, Rus Hükûmeti kanunun bilgi dağıtımı suretiyle ihlalini önlemek amacıyla bir kısıtlama getirmiş olsa da bu müdahaleyi AİHS'nin 10. maddesinin ikinci fıkrasında yer alan hangi meşru amaca dayalı olarak gerçekleştirdiğini izah edememiştir.[1178] Mahkemeye göre, kamunun güvenliğinin sağlanması ve düzensizliğin veya suçun önlenmesi mülahazaları da mevcut olay için uygulanabilir değildir.[1179] Keza, gizli bilginin ifşasını önleme amacı da uygulama alanı bulmamaktadır. Mahkeme, bu bağlamda müdahalenin hukuki dayanağının yetersiz olduğunu vurgulamıştır.[1180]

Rus Anayasa Mahkemesinin kamusal etkinliklere ilişkin düzenlemelerin amacını irdeleyen kararına çapraz atıf yapan AİHM, kamusal etkinliklerin ön bir bildirim ve onaya tabi tutulmasıyla hem etkinliğe katılan hem de diğer kişilerin güvenliğinin sağlanması amaçlanmaktadır.[1181] AİHM de bu bağlamda, müdahalenin amacının başkalarının haklarının korunması olduğunu not etmiştir. Ayrıca, mevcut olayda engellemenin yayımlanmış içeriğin hukuka aykırılığına ilişkin bir yargı kararı verilmeden önce yapıldığı, bir ön müdahale niteliği taşıdığı tespitini yapmıştır.[1182]

[1175] *Kablis v. Rusya*, para. 85.
[1176] *Kablis v. Rusya*, para. 86.
[1177] *Kablis v. Rusya*, para. 87.
[1178] *Kablis v. Rusya*, para. 88.
[1179] *Kablis v. Rusya*, para. 88.
[1180] *Kablis v. Rusya*, para. 88.
[1181] *Kablis v. Rusya*, para. 89.
[1182] *Kablis v. Rusya*, para. 90.

AİHM, AİHS'nin 10. maddesinin bu tür yayınlar için ön kısıtlama tedbirlerini yasaklamadığını hatırlatmış ancak bunların çok dikkatli bir şekilde ve sadece istisnai durumlarda uygulanması gerektiğini ifade etmiştir.[1183] *Ahmet Yıldırım v. Türkiye* kararında da belirtildiği üzere, önleyici kısıtlamalarda, yetkilerin kötüye kullanılmasını önlemek amacıyla yasaklamaların kapsamı üzerinde sıkı bir kontrole ve etkin yargısal denetime olanak sağlayan bir yasal çerçeve gerekmektedir.[1184]

Bu doğrultuda AİHM, başvurucunun Bilgi Kanunu'nun 15. maddesinin üçüncü fıkrasında yer alan *"mevcut usullere aykırı bir şekilde gerçekleştirilen kitlesel (kamusal) etkinlikler"* ibaresinin çok geniş ve müphem olduğuna dair iddiasının üzerinde durmuştur.[1185] Mahkeme, somut olayda kapsamlı bir değerlendirme yapılmadığını ve başkalarının haklarına etki hususunun gereğince tartışılmadığını, Başsavcılığın salt bir gösteriye çağrıyı esas alarak erişimi engelleme kararı verdiğini belirtmiştir.[1186]

Bilgi Kanunu'nun yukarıda bahsedilen hükmünü irdeleyen AİHM, söz konusu hükmün, AİHS'nin 10. maddesindeki kriterlere uygun şekilde web sitesinin veya sayfanın değil de sadece belirli içeriğin engellenmesine ilişkin bir zorunluluk taşımadığını belirtmiştir.[1187] Keza, yerel mahkemelerin de bu konuda bir değerlendirme yaptığına dair bir delilin olmadığını ifade etmiştir.[1188] Mahkemeye göre, bu düzenleme Başsavcı ve vekillerine önleyici tedbirler almak ve kapsamını belirlemek hususunda çok geniş yetkiler vermektedir.[1189]

Başsavcının internet içeriklerini engelleme yetkisine karşı yargı yolu açıktır. Fakat AİHM kanun yollarının varlığından ziyade etkinliğinin incelenmesi gerektiği görüşündedir.[1190] Her şeyden evvel, bir kamusal etkinliğe yönelik yayının engellenmesi üzerine yapılan itirazın söz konusu

[1183] *Kablis v. Rusya*, para. 91.
[1184] *Kablis v. Rusya*, para. 92.
[1185] *Kablis v. Rusya*, para. 93.
[1186] *Kablis v. Rusya*, para. 93.
[1187] *Kablis v. Rusya*, para. 94.
[1188] *Kablis v. Rusya*, para. 94.
[1189] *Kablis v. Rusya*, para. 95.
[1190] *Kablis v. Rusya*, para. 96.

etkinlik gerçekleşmeden yargı tarafından karara bağlanması gerekir ki bu karar bir anlam ifade edebilsin.[1191]

AİHM, tüm bu tespitler ışığında erişimi engelleme hususunu düzenleyen Bilgi Kanunu'nun 15. maddesinin üçüncü fıkrasının Mahkemenin yerleşik içtihatlarında belirlenmiş olan kötüye kullanıma karşı gerekli teminatları içermediğini, özellikle de yasakların kapsamına ilişkin denetim ve etkili yargısal denetimden yoksun olduğunu belirtmiştir.[1192] Ayrıca, yerel mahkemelerin içeriklere ilişkin müstakil değerlendirmeler yapmadığı ve gerekçelerini ortaya koymadığı görüşündedir.[1193]

Her üç içeriği ayrı ayrı ele alan AİHM, birinci gönderinin kamuyu ilgilendiren güncel bir konuya ilişkin bir ifade olduğunu[1194], toplantı yerine ilişkin bilgilendirmenin de kamu yararını ilgilendiren bir hususta bilgi paylaşımı niteliğinde olduğunu[1195] belirtmiş; açıkça hukuka aykırı bir içerik taşımayan bu gönderilerin neden engellendiğine dair kamu otoritelerinin makul bir gerekçe ortaya koymadığını ifade etmiştir.[1196] İfade özgürlüğü ile toplantı ve gösteri hakkına ilişkin muhtelif içtihatlarına atıf yapan AİHM, üçüncü gönderi ile sosyal medya gönderisi bakımından kamu otoritelerinin barışçıl hukuka aykırı toplanmalara da belirli ölçüde tolerans göstermesi gerektiği kanaatindedir.[1197] kişileri

AİHM, başvurucunun kanuni bir kısıtlamaya aykırı olarak kişileri kamusal gösteriye katılmaya çağırmasının ifade özgürlüğünün kısıtlanması için tek başına gerekçe olamayacağı görüşündedir.[1198] Mahkemeye göre kısıtlamanın hukuka uygun olması için demokratik bir toplumda gerekli olup olmadığının incelenmesi gerekmektedir.

[1191] *Kablis v. Rusya*, para. 96.
[1192] *Kablis v. Rusya*, para. 97.
[1193] *Kablis v. Rusya*, para. 98.
[1194] *Kablis v. Rusya*, para. 99.
[1195] *Kablis v. Rusya*, para. 100.
[1196] *Kablis v. Rusya*, para. 101.
[1197] *Kablis v. Rusya*, para. 102.
[1198] *Kablis v. Rusya*, para. 103.

Demokratik toplum düzeninin gerekliliği penceresinden konuyu ele alan AİHM, başvurucunun toplumsal bir olaya ilişkin görüşlerini kamuyla paylaştığını, bir toplantı tertipleyerek insanları bir araya gelmeye çağırmasının herhangi bir şiddete, düzensizliğe veya başka bir hukuka aykırı eyleme davet içermediğini, sadece elli kişilik dar bir çevrede barışçıl bir gösteri yapma niteliğinde olduğunu, etkinliğe ilişkin davette henüz izin alınmadığını belirterek kişileri yanıltmadığını dikkate almış, bu tür bir eyleme yönelik müdahalenin demokratik toplum düzeninin gerekliliklerıyle bağdaşmadığını belirtmiştir.[1199] Keza, etkinliğin kamu güvenliği veya başkalarının hakları üzerinde zararlı bir neticesi olmadığını, söz konusu kısıtlamaları meşru gösterecek ve ihtilaf konusu içeriklere erişimi kısıtlayacak baskın bir toplumsal ihtiyacın olmadığını ifade etmiştir.[1200]

Tüm bu tespitlerin ve konuyla ilgili içtihatların ışığında AİHM, iç hukuktaki düzenlemenin, kendisinin önleyici tedbirlerin istismar edilmesini önlemek için aradığı gerekli teminatlardan yoksun olduğuna karar vermiştir.[1201] Ayrıca, yerel mahkemeler tarafından uygulanan standartların AİHS'nin 10. maddesinde vücut bulan ilkelerle uyumlu olmadığına ve başvurucunun ifade özgürlüğüne müdahale için "ilgili ve yeterli" gerekçeler sunulmadığına hükmetmiştir.[1202] Bu doğrultuda, başvurunun kabul edilebilir olduğuna, AİHS'nin 11. maddesinin ihlal edildiğine, 11. maddesiyle bağlantılı olarak 13. maddesinin de ihlal edildiğine, erişimi engelleme sebebiyle 10. maddesinin ihlal edildiğine, başvurucuya manevi tazminat ödenmesine hükmetmiştir.

V. Değerlendirme

AİHM, *Kablis v. Rusya* kararında, ilk defa *Ahmet Yıldırım v. Türkiye* kararıyla ele aldığı erişimin engellenmesi konusunda yaklaşımını koruduğunu göstermiştir. AİHM, bir mahkeme kararı olmaksızın idari makamlarca internet içeriğine yönelik önleyici tedbirler uygulanmasını

[1199] *Kablis v. Rusya*, para. 104.
[1200] *Kablis v. Rusya*, para. 105.
[1201] *Kablis v. Rusya*, para. 106.
[1202] *Kablis v. Rusya*, para. 106.

ilkesel olarak yasaklamamaktadır. Ancak, bu tür bir durumda AİHS'nin genel sistematiğine ve ruhuna uygun olarak, önleyici kısıtlamalarda, yetkilerin kötüye kullanılmasını önlemek amacıyla yasaklamaların kapsamı üzerindeki sıkı bir kontrole ve etkin yargısal denetime olanak sağlayan bir yasal çerçeve gerekmektedir.

Kablis v. Rusya kararının bir diğer önemli vurgusu ise internet içeriğine erişimi engellemek için kullanılması meşru olan engelleme tekniği üzerinedir. AİHM'nin, *Ahmet Yıldırım v. Türkiye* kararıyla ilk kez ele aldığı, *Cengiz ve Diğerleri v. Türkiye* kararıyla sürdürdüğü yaklaşımına göre internet içeriğine müdahalede en az kısıtlayıcı yöntem tercih edilmelidir. Mahkemenin, URL engellemenin asıl yöntem olduğu ancak istisnai hâllerde DNS engelleme tekniğinin de kullanılabileceğine yönelik içtihadı artık istikrarlı bir hâl almıştır. Ayrıksı durumlarda, meşru sebeplerle ve gerekçeleri ortaya koyularak bir web sitesine külli bir engelleme getirilebilecektir. Her koşulda, verilen kararların etkin yargısal denetimi sağlanmalıdır.

§21. BULGAKOV V. RUSYA

AİHM, 23 Haziran 2020 tarihinde Rusya'ya ilişkin dört karar vermiştir. Bunların tamamı, erişimin engellenmesi tedbirlerinin ve içeriğin kaldırılması kararlarının AİHS'ye uygunluğuna ilişkindir. İlk karar, *Bulgakov v. Rusya* kararıdır.[1203] *Bulgakov v. Rusya* başvurusunun ana konusu, aşırılık barındıran bir içeriğe uygulanan engelleme kararı sebebiyle web sitesinin tamamına erişimin engellenmesidir.

I. Davanın gelişimi

Başvurucu Bay Yevgeniy Vladimirovich Bulgakov, "Worldview of the Russian Civilization" isimli ve www.razumei.ru alan adında barındırılan bir web sitesinin sahibi ve yöneticisidir. Bay Bulgakov, Kasım 2013'te, web sitesine erişimin Kirovskiy Bölge Mahkemesinin 3 Nisan 2012 tarihli kararına istinaden yerel İSS tarafından engellendiğini tespit etmiştir.

2011 yılının sonlarında Rostov Bölge savcısı, internet ortamında daha önceden aşırılık içeren bir yayın olarak sınıflandırılan bir kitabın kopyasına başvurucunun web sitesinde elektronik formatta erişildiğini belirtmiş ve bu içeriğin yer aldığı sitenin IP adresine erişimin engellenmesi için Kirovskiy Bölge Mahkemesine başvurmuştur. Savcılığın talebini inceleyen Mahkeme, Aşırıcılığın Bastırılması Kanunu ile Bilgi Kanunu'nun 10(1) ve (6). bölümlerine dayanarak İSS'nin savcılığın önerdiği yöntemle başvurucunun web sitesini engellemesini talep etmiştir.

Kirovskiy Bölge Mahkemesinin kararından haberdar olması üzerine başvurucu, ilgili e-kitabı sitesinden silmiş ve web sitesine erişimin açılması için talepte bulunmuştur. Moskova'da bulunan Savelovskiy Yerel Mahkemesi 25 Mart 2014 tarihinde bu talebi uygun bulmuş ve aşırılık barındıran içeriğin çıkarılması sebebiyle erişimin engellenmesi tedbirinin kaldırılmasına hükmetmiştir.

[1203] **AİHM**, *Bulgakov v. Rusya*, Başvuru No: 20159/15, 23.6.2020.

Bu karara yapılan itiraz neticesinde Moskova Şehir Mahkemesi kararı bozmuştur. Mahkeme, İSS'ye web sitesinin spesifik bir sayfasına değil sitenin yayın yaptığı IP adresine erişimi engellemesi talimatı verildiğini, bu sebeple içerik silinmiş olsa bile erişimin engellenmesi kararının kaldırılmasının ilgili hükme aykırılık teşkil edeceğine karar vermiş ve başvurucunun temyiz mahkemesine itiraz etme izni talebini reddetmiştir.

Başvurucu, 2012 yılındaki kararı temyiz edebilmek için Kirovskiy Bölge Mahkemesinde tekrar itirazda bulunmuş ve Anayasa Mahkemesinin içtihatlarına atıf yaparak ilgili kişiyi yargılamaya dâhil etmeyen ve ilgili kişinin hak ve yükümlülüklerini belirleyen veya haklarına kısıtlama getiren bir yargılamanın adil olarak nitelendirilemeyeceğini ileri sürmüştür.[1204] Başvurucu, asıl engelleme yargılamasından haberdar olmadığını ve haklarını savunamadığını ileri sürmüştür. Keza, e-kitabın kaldırıldığına dair delilleri de paylaşmıştır.

Rostov Bölge Mahkemesi, 29 Ocak 2015 tarihinde temyizi reddetmiştir. Mahkeme, 2012 yılına ait kararın başvurucunun yargılamaya katılamadığı gerekçesiyle iptal edilemeyeceğini zira bu davanın başvurucuya değil İSS'ye karşı açıldığını belirtmiştir.[1205] Ayrıca, başvurucunun delillerini değerlendirmeksizin, e-kitabın kaldırıldığının ortaya konulmadığına karar vermiştir. Akabinde, sırasıyla Bölge Mahkemesi ve Yüksek Mahkeme, temyiz taleplerini reddetmiştir.

II. Hukuki arka plan

AİHM, konunun esasını incelemeden evvel muhtelif ulusal ve uluslararası hukuk metinlerine atıf yapmıştır. Bilgi Kanunu'nun (27 Temmuz 2006 tarihli Federal Yasa no. 149-FZ) 2. bölümü internet sitesini "alan adı veya ağ adresi ile erişilebilen bilgisayar yazılımı ve diğer içeriklerin toplamı" olarak, internet sitesinin sayfasını (web sayfası) "internet sitesinin, alan adı ve ilave karakterlerden oluşan referans ile erişilen parçası" olarak

[1204] *Bulgakov v. Rusya*, para. 7.

[1205] *Bulgakov v. Rusya*, para. 9.

tanımlanmıştır.[1206] Aynı düzenlemenin 10. maddesi uyarınca bilgi Rusya Federasyonu'nda Rus mevzuatına uygun olarak özgürce paylaşılabilir. Cezai veya idari olarak yasaklanmış olan bilginin paylaşımı yasaktır.

Rus mahkemelerinin internet içeriğine erişimin engellenmesine ilişkin muhtelif kararlarına atıf yapan AİHM, Nisan 2020 itibarıyla, yargı kararlarına ilişkin online veri tabanında, Rus mahkemelerinin IP engelleme tekniği kullanarak erişimi engelleyen 12.000 kararının bulunduğunu not etmiştir.[1207]

AİHM, Avrupa Konseyinin 28 Mayıs 2003 tarihli İnternette İletişim Özgürlüğüne İlişkin Deklarasyon'unu zikrederek Deklarasyon'un internet ortamındaki içeriğe devletlerin ön kontrol uygulamaması gerektiğine ilişkin maddesini alıntılamıştır.[1208] Aynı şekilde, Birleşmiş Milletler İnsan Hakları Konseyinin düşünce ve ifade özgürlüğü hakkının korunması ve desteklenmesine ilişkin Özel Raportörü'nün İnsan Hakları Konseyine gönderdiği 16 Mayıs 2011 tarihli Rapor'una (A/HRC/17/27),[1209] Birleşmiş Milletler Fikir ve İfade Özgürlüğü Özel Raportörü, Avrupa Güvenlik ve İşbirliği Teşkilatı Medya Özgürlüğü Temsilcisi, Amerikan Devletleri Örgütü İfade Özgürlüğü Özel Raportörü, Afrika İnsan ve Halkların Hakları Komisyonu İfade Özgürlüğü ve Bilgiye Erişim Özel Raportörü'nün 1 Haziran 2011 tarihli Ortak Deklarasyonu'na,[1210] Birleşmiş Milletler İnsan Hakları Komitesinin 11-29 Temmuz 2011 tarihleri arasında gerçekleşen 102. oturumunda Medeni ve Siyasi Haklara İlişkin Uluslararası Sözleşme'nin 19. maddesiyle ilgili olarak kabul ettiği ve internet içeriğinin kısıtlanmasında dikkat edilecek hususlara yönelik tavsiyeler içeren 34 sayılı Genel Yorum'una[1211] atıf yapmıştır. Ayrıca Avrupa Konseyinin 13 Nisan 2016 tarihli İnternet Özgürlüğüne İlişkin Tavsiye Kararı'ndan alın-

[1206] *Bulgakov v. Rusya*, para. 10.

[1207] *Bulgakov v. Rusya*, para. 12-15.

[1208] İnternette İletişim Özgürlüğüne İlişkin Deklarasyon için bkz. **§6(IV)**.

[1209] *Bulgakov v. Rusya*, para. 17.

[1210] *Bulgakov v. Rusya*, para. 18.

[1211] *Bulgakov v. Rusya*, para. 19.

tılar yapmıştır.[1212] Söz konusu Tavsiye Kararı'nın ilgili kısımlarını tekrar etmek gerekirse:

2.2.1. Devlet makamları veya özel sektör aktörleri tarafından bir internet platformunu (sosyal medya, sosyal ağlar, bloglar veya başka diğer web siteleri) veya bilgi ve haberleşme teknolojileri (BT) araçlarını (anlık mesajlaşma ve diğer uygulamalar) engelleyen veya bunlara erişimi başkaca şekilde kısıtlayan her türlü tedbir veya devlet makamlarının bu tür eylemlere yönelik talepleri, kısıtlamaların kanunla öngörülme, meşruluk ve ölçülülük koşullarına uygun olmasını öngören AİHS'nin 10. maddesiyle uyumlu olmalıdır.2.2.2. Devlet makamları veya özel sektör tarafından alınan internet içeriğini engelleme, filtreleme veya kaldırmaya yönelik her türlü tedbir veya bu tür bir işlem için devlet makamları tarafından gerçekleştirilen her türlü talep, kısıtlamaların kanunla öngörülme, meşruluk ve ölçülülük koşullarına uygun olmasını öngören AİHS'nin 10. maddesiyle uyumlu olmalıdır.

Bu Tavsiye Kararı'na Rusya Federasyonu tarafından özel çekince koyulmuş olduğunu belirtmek gerekir.

III. Tarafların iddiaları

Başvurucu, içerik yayından kaldırılmış olmasına rağmen yerel mahkemeler tarafından İSS seviyesinde tüm web sitesine erişimin engellenmesinin AİHS'nin 10. maddesinde güvence altına alınan ifade özgürlüğünü ihlal ettiğini ileri sürmüştür.[1213] AİHM, başvuruyu kabul edilebilir görmüştür.[1214]

IV. Rus Hükûmetinin savunması

Rus Hükûmeti, başvurucuya ait web sitesinin Kirovskiy Bölge Mahkemesinin kararı uyarınca İSS tarafından engellendiğini, kararın telekomünikasyon düzenleyicisi Roskomnadzor'a gönderilmediğini ve

[1212] İnternet Özgürlüğüne İlişkin Tavsiye Kararı için bkz. **§6(XXIV)**.

[1213] *Bulgakov v. Rusya*, para. 21.

[1214] *Bulgakov v. Rusya*, para. 22.

Roskomnadzor tarafından başvurucunun web sitesine yönelik bir tedbir alınmadığını belirtmiştir.[1215] Aşırılık barındıran içerik kaldırıldıktan sonra başvurucunun web sitesine yönelik bir erişimi engelleme tedbiri alınmadığını ileri sürmüştür.

V. Başvurucunun iddiaları

Başvurucu, mevcut davada erişimin engellenmesi amacıyla kullanılan ve Yüksek Mahkemenin 10 Mayıs 2011 tarihli kararıyla da tekrar gündeme gelen İSS seviyesinde IP engelleme tekniğinin nasıl uygulandığını izah etmiştir.[1216] Başvurucu, Rus mahkemelerinin yasaklı içerik bir veya birden fazla web sayfasında olsa da site ve sayfa şeklinde bir ayrım yapmadan tüm web sitesine erişimin engellenmesi kararı verdiklerini ileri sürmüştür. Başvurucu, bu tür durumlarda mahkemelerin, kararlarını sadece hukuka aykırı içerikle sınırlamaya yönelik bir yükümlülükleri olmadığını iddia etmiştir.

Başvurucu, mahkemeler tarafından verilen erişimin engellenmesi kararlarının teknik uygulamasının kaçınılmaz olarak tüm web sitesine erişimi engellemeyle sonuçlandığını; web sitelerinin IP adresi olmasına rağmen münferit web sayfalarının IP adresi olmadığı için kararın IP temelli verildiğini ileri sürmüştür. Başvurucu, bir web sayfasına erişimin IP temelli engellenmesinin tüm web sitesine erişimi engellemeye yol açacağına dair sadece bir mahkeme kararına rastgeldiğini ve bu kararın -iki ay sonra, başvurucunun davasında bunun tam zıttı bir sonuca varan- Rostov Bölge Mahkemesi tarafından onaylandığını belirtmiştir.

Başvurucuya göre, yargısal uygulama gerekli hukuki koruma kriterlerini sağlamamıştır. Öyle ki "web sitesi" ile "web sayfası" arasındaki ayrım yapılamamış ve sorunlu bir içerik barındırması durumunda bir web sitesinin tamamına erişimin engellenmesi söz konusu olmuştur. Daha önemlisi, bu uygulama, hukuka uygun bir içeriğin bu tür tedbirlerden nasıl etkileneceğine yönelik bir değerlendirme yapma ihtiyacını da ortadan kaldırmaktadır. Başvurucu, IP engelleme tekniğini, 5 numaralı

[1215] *Bulgakov v. Rusya*, para. 23.

[1216] *Bulgakov v. Rusya*, para. 24.

duruşma salonuna erişimi kısıtlamak için adliye binasının ana girişinin kapatılmasına benzetmiştir.[1217]

VI. Müdahil tarafların görüşleri

Davaya farklı taraflar ve sivil toplum örgütleri müdahil olmuş ve görüş paylaşmışlardır. Bu taraflardan ilki Birleşmiş Milletler Fikir ve İfade Özgürlüğü Özel Raportörü'dür.[1218] Raportör, bireylerin çevrim içi ortamda da çevrim dışı ortamda olduğu gibi ifade özgürlüğünden faydalanmasına izin verilmesi gerektiğini vurgulamıştır. Web sitelerinin tamamen engellenmesi konusuna da değinen Raportör, bu tür engellemelerin, ifade özgürlüğünün izin verilen sınırlarına ilişkin kriterleri sağlaması, içeriğe özgü olması ve web sitelerinin salt hükûmeti veya siyasal sistemi eleştiriyor diye hedef alınmaması durumunda istisnai olarak uygulanabileceği görüşündedir.

Davaya müdahil olarak görüş veren diğer taraflar ise Article 19, EFF, Access Now ve Reporters without Borders isimli sivil toplum örgütleridir.[1219] Söz konusu kuruluşlara göre, bir web sitesinin tamamına erişimi engelleme, hukuka uygun-hukuka aykırı içerik arasında ayrım yapma imkânı tanımadığı ve bu sebeple hukuken asla gerekli olamayacağı için aşırı ve ölçüsüz bir tedbirdir. Şayet erişimi engelleme tedbirine izin verilirse kanun şu minimum standartları sağlamalıdır: (i) Bir mahkeme veya bağımsız bir yargısal organ tarafından engellemeye karar verilmelidir; (ii) ilgili taraflara engelleme kararının arandığı yargılamalara müdahale hakkı tanınmalıdır; (iii) engelleme kararlarının tüm mağdurlarına engelleme kararlarına itiraz hakkı tanınmalıdır; (iv) engellenen web sitelerine erişmeye çalışan herkes engelleme kararının hukuki dayanağı ve gerekçeleri ile bu karara itiraz yollarına ilişkin bilgiyi görebilmelidir.

Son müdahil, Avrupa Bilgi Toplumu Enstitüsü isimli sivil toplum örgütüdür.[1220] Söz konusu kuruluş, hedefini aşan ve meşru içeriği aşırı

[1217] *Bulgakov v. Rusya*, para. 24.

[1218] *Bulgakov v. Rusya*, para. 25.

[1219] *Bulgakov v. Rusya*, para. 26.

[1220] *Bulgakov v. Rusya*, para. 27.

şekilde engelleyen bir tedbirin demokratik toplumda kabul edilebilir olmadığını belirtmiş ve yetkili makamların aynı sonuca daha az müdahaleci bir tedbirle ulaşılıp ulaşılamayacağına dair bireyselleştirilmiş bir değerlendirme yapması gerektiğini vurgulamıştır. Bu doğrultuda, hedef alınan web sitesinin bilgilendirilmesi gerektiğini, hukuka aykırı içeriği kaldırması ve bu karara ilişkin beyanlarda bulunması için kendisine makul bir süre verilmesi lazım geldiğini beyan etmiştir.

VII. AİHM'nin tespit ve değerlendirmeleri

Konunun esasına giren AİHM öncelikle *Ahmet Yıldırım v. Türkiye* kararında internetin niteliğiyle ilgili tespitlerine atıfta bulunmuştur.[1221] Tekrar etmek gerekirse, AİHM söz konusu kararında erişilebilirliğin yanı sıra büyük miktarda veriyi muhafaza etme ve dağıtma imkânları sayesinde internet sitelerinin kamunun güncele erişiminin iyileştirilmesine ve bilginin iletilmesinin kolaylaştırılmasına önemli derecede katkıda bulunduğunu; internetin politik veya kamu menfaatine ilişkin tartışma ve eylemlere katılım konusunda asli vasıtaları barındırdığını ve AİHS'nin 10. maddesinin yalnızca bilgilerin iletilmesi hakkını değil aynı zamanda toplumun bilgi alma hakkını da güvence altına aldığını belirtmiştir.

AİHM, başvurucunun, web sitesinin hem sahibi hem de yöneticisi olduğu ve Kasım 2013'te web sitesine erişimin mahkeme kararına dayalı olarak yerel bir İSS tarafından engellendiği tespitini paylaşmıştır. Bu tespitten sonra Mahkeme tekrar *Ahmet Yıldırım v. Türkiye* kararına atıf yaparak, yasal temeli ne olursa olsun, böyle bir tedbirin internete erişimi etkileyebilme potansiyeli olduğunu, bu sebeple de davalı devletin 10. madde kapsamında sorumluluğunu doğurduğunu hatırlatmıştır.[1222] Mahkeme tarafından verilen engelleme kararının bu bağlamda bir kamusal makamın AİHS'nin 10. maddesiyle güvence altına alınan bilgi alma ve yayma hakkına müdahalesi niteliğinde olduğunu belirtmiştir.[1223]

[1221] *Bulgakov v. Rusya*, para. 28.

[1222] *Bulgakov v. Rusya*, para. 29.

[1223] *Bulgakov v. Rusya*, para. 29.

Müdahalenin kapsamı bakımından konuyu ele alan AİHM, başvurucunun ihtilaf konusu e-kitabın yasaklı içerik olduğuna ilişkin bir itirazda bulunmadığını belirtmiş; itirazın temel olarak hukuka aykırı bir içerik sebebiyle -bu içerik yayından kaldırıldıktan sonra dahi- tüm web sitesine erişimin engellenmesine yönelik olduğunu tespit etmiştir.[1224] Mahkemeye göre bu müdahalenin iki temel bağlamda ele alınması gerekir: (i) kanunla öngörülme ve (ii) AİHS'nin 10. maddesinin ikinci fıkrasında belirtilen meşru amaçlardan bir veya birden fazlasını gütme ve bu amaçlara erişmek için demokratik bir toplumda gerekli olma.

AİHM'ye göre "kanunla öngörülen" ifadesi, 10. maddenin ikinci fıkrası bağlamında, uygulanan tedbirin iç hukukta bir dayanağı olması gerektiğinin yanı sıra söz konusu yasanın niteliğiyle de ilgilidir. Bu bakımdan yasanın, ilgilinin kendisi açısından ortaya çıkabilecek sonuçları ve hukukun üstünlüğü ilkesiyle uyumunu önceden değerlendirebilmesi için erişilebilir olması gerektiğini ifade etmektedir.[1225] Yasa yürütme organına temel haklara ilişkin konularda sınırsız bir takdir yetkisi veriyorsa AİHS'nin benimsediği demokratik bir toplumu oluşturan ana ilkelerden biri olan hukukun üstünlüğü ilkesine aykırılık söz konusu olacaktır. Bu sebeple yasa, bu gücün kullanılmasının yöntemini ve kapsamını yeterli netlikte düzenlemelidir.

AİHM bu içtihatlarını somut uyuşmazlığa uygulamıştır.[1226] Bölge Mahkemesinin 3 Nisan 2012 tarihli kararının Bilgi Kanunu'nun 10(6) bölümüne dayandığını, bu hükmün idari veya cezai olarak müeyyideye bağlanmış herhangi bir içeriğin dağıtımını engellemeye izin verdiğini, e-kitabın bu kategoride aşırılık içeren bir yayın olarak sınıflandırıldığını, bu tür içeriğin yayımlanmasının İdari Kabahatler Kanunu'nun 20.29. maddesinde bir kabahat olarak düzenlendiğini dikkate alan AİHM, müdahalenin "kanunla öngörülme" şartını yerine getirdiğini tespit etmiştir.[1227]

[1224] *Bulgakov v. Rusya*, para. 30.

[1225] *Bulgakov v. Rusya*, para. 31.

[1226] *Bulgakov v. Rusya*, para. 32.

[1227] *Bulgakov v. Rusya*, para. 32.

AİHM, yine de Bölge Mahkemesinin kararının, hukuka aykırı nitelikteki içeriğin engellenmesiyle sınırlı şekilde uygulanmadığı görüşündedir.[1228] Bölge Mahkemesi, savcılığın başvurusunda talep ettiği engelleme tekniğinin kullanılmasına yani hukuka aykırı içeriğin tüm web sitesi erişime kapatılmak suretiyle engellenmesine karar vermiştir. Peki, Mahkeme neden bu şekilde davranmıştır? Başvurucu, bu yöntemin kullanılmasının sebebi olarak bir web sitesindeki sayfa ile web sitesinin tamamı arasındaki ayrıma ilişkin hâkimlerin teknik uzmanlık eksikliği olmasını göstermiştir. İddiasını desteklemek için Rus mahkemelerinin bu konudaki çelişkili içtihatlarını göstermiştir. Bu tür IP temelli engellemenin binlerce farklı olayda uygulandığı bir vakıadır.

AİHM, bir web sitesinin tamamının engellenmesinin bir gazete veya televizyon istasyonunun engellenmesiyle kıyaslanabilecek aşırı ve keyfî bir tedbir olduğunu vurgulamıştır.[1229] Zira, bu tür bir tedbir AİHM'ye göre, hukuka uygun ve hukuka aykırı bilgi arasında bir ayrım yapmamakta, hukuka aykırı kabul edilmeyen birçok içeriği de erişilmez kılmaktadır. *Ahmet Yıldırım v. Türkiye* kararını tekrar hatırlatan AİHM, IP engelleme tekniğinin hedeflenen hukuka aykırı içeriği engellemeyi aşan bir tedbir olduğunu belirtmiştir. AİHM, Bilgi Kanunu'nun 10. maddesinin esasında tüm web sitesine değil hedeflenen içeriğe yönelik tedbire izin verdiğini ifade etmiş; Mahkemenin uyguladığı engelleme formülünün mevzuatta dayanağı olmadığına kanaat getirmiştir.

Peki yerel düzenleme, engelleme tedbirlerinin aşırı ve keyfî uygulanmasına yönelik bir koruma mekanizması içermekte midir? Bu sorunun yanıtını arayan AİHM, savcının engelleme kararının, hakları etkilenmesi muhtemel kişilere önceden bildirim yapılmaksızın alındığını belirtmiştir.[1230] Keza, Bölge Mahkemesinin başvurucuyu davalara müdahil olmaya veya beyanda bulunmaya davet etmediğini, tüm sürecin savcı ve yerel İSS arasında gerçekleştiğini not etmiştir.

[1228] *Bulgakov v. Rusya*, para. 33.

[1229] *Bulgakov v. Rusya*, para. 34.

[1230] *Bulgakov v. Rusya*, para. 35.

AİHM'ye göre, yerel İSS'nin davalı olarak belirlenmiş olması, sürecin İSS'nin aleyhine bir etkisi olmaması sebebiyle yeterli değildir.[1231] Mahkemeye göre İSS, içeriği hakkında bilgi sahibi olmadığı milyonlarca web sitesine erişim için kullanıcılara gerekli teknolojiyi sağlamaktadır. İSS, içerikler hakkında içeriklerin sahipleri kadar detaylı bilgiye sahip değildir ve engellemeye konu her web sitesini savunabilecek hukuki kaynaklardan da mahrumdur. Keza İSS'nin yargılamaların neticelerine ilişkin hukuki bir menfaati yoktur. Engelleme kararlarının, bağlantı sağlama ticari hizmeti üzerinde bir yansıması yoktur ve bu kararlar kesinleştiği zaman tüm Rus İSS'lerinin aynı engelleme kararını uygulamasını gerektirmektedir. Tüm bu tespitler ışığında AİHM, başvurucunun yokluğunda gerçekleştirilen yargılamaların ilgili tarafların kendilerini ifade edebilmeleri için gerekli ortamı sağlamadığına karar vermiştir.[1232]

AİHM, mevcut uyuşmazlıkta Rus iç hukukunun itirazlara ilişkin mekanizmalarının da gereğince işletilmediğine işaret etmiştir.[1233] Aynı doğrultuda, daha az müdahaleci nitelikte bir tedbire yönelik araştırma gerçekleştirilmediğini, engellemeye konu web sitesinin sahibinin şeffaf bir şekilde bilgilendirilmediğini, başvurucunun engelleme gerçekleşene kadar web sitesi aleyhine alınan karardan haberdar olmadığını belirtmiştir. Başvurucunun iddialarının temel boyutlarından bir diğeri, hukuka aykırı olduğu ileri sürülen içerik kaldırılmasına rağmen web sitesinin erişime açılmayıp engellemenin sürdürülmesidir.[1234] Hatırlanacağı üzere, ilk derece mahkemesi erişimin açılması yönünde bir karar vermişse de üst mahkemeler bu kararı bozmuş ve engellemenin devamına hükmetmiştir.

Tüm bu tartışmalar ışığında AİHM, Bilgi Kanunu'nun 10(6) bölümüne dayalı olarak gerçekleştirilen müdahalenin aşırı ve keyfî bir etki doğurduğuna, Rus mevzuatının başvurucuya hukuk devletinde ve demokratik toplumda gereken düzeyde bir koruma sağlamadığına, müdahalenin kanunla öngörülmediğine hükmetmiş ve AİHS'nin 10. maddesinin ikinci fıkrasındaki koşulların varlığını tartışmaya gerek olmadığına

[1231] *Bulgakov v. Rusya*, para. 36.

[1232] *Bulgakov v. Rusya*, para. 36.

[1233] *Bulgakov v. Rusya*, para. 37.

[1234] *Bulgakov v. Rusya*, para. 38.

karar vermiştir.[1235] Bu doğrultuda, AİHS'nin 10. maddesinin ihlal edildiği sonucuna varmıştır.[1236]

10. madde ihlaline ilişkin tespitinden sonra Mahkeme, 13. maddenin ihlal edilip edilmediğini ele almıştır. Başvurucu, Rus mahkemelerinin AİHS'nin 13. maddesinde güvence altına alınan etkili başvuru hakkını ihlal ettiğini ileri sürmüştür.[1237] 13. madde şu şekildedir: *"Bu Sözleşme'de tanınmış olan hak ve özgürlükleri ihlal edilen herkes, ihlal fiili resmî görev yapan kimseler tarafından bu sıfatlarına dayanılarak gerçekleştirilmiş olsa dahi ulusal bir makama etkili bir başvuru yapabilme hakkına sahiptir."* AİHM, açıkça dayanaktan yoksun olmadığına kanaat getirerek bu iddiayı kabul edilebilir görmüştür.[1238]

Rus Hükûmeti, başvurucunun tüm etkili iç hukuk yollarını kendi inisiyatifiyle sonuna kadar tükettiğini ve uygulanabilir hukuk kuralları çerçevesinde taleplerinin mahkemelerce dikkate alındığını iddia etmiştir.[1239] Hükûmet, web sitesi idari bir makam olan Roskomnadzor tarafından engellenmediği için bir hak ihlali olmadığını ileri sürmüştür.

Başvuran ise kendisine kararlara itiraz ve temyiz duruşmasına katılma olanağı sağlandığından bahisle Rus hukukunun, iddia ettiği ihlale ilişkin -teorik olarak- bir hukuki çare sunduğunu kabul etmiştir.[1240] Öte yandan başvurucu, mahkemelerin web sayfası-web sitesi ayrımını yapamadığı, web sitesinin tamamının veya bir sayfasının engellenmesi arasında bir değerlendirme gerçekleştiremediğinden bahisle şikâyetlerine yönelik etkin bir hak arama yolunun olmadığını ileri sürmüştür.[1241]

Müdahil üçüncü taraflardan Avrupa Bilgi Toplumu Enstitüsü, etkilenen taraflar için hem *ex-ante* hem de *ex-post* hak arama yollarının

[1235] *Bulgakov v. Rusya*, para. 39.
[1236] *Bulgakov v. Rusya*, para. 40.
[1237] *Bulgakov v. Rusya*, para. 41.
[1238] *Bulgakov v. Rusya*, para. 42.
[1239] *Bulgakov v. Rusya*, para. 43.
[1240] *Bulgakov v. Rusya*, para. 44.
[1241] *Bulgakov v. Rusya*, para. 44.

sunulması gerektiğini belirtmiştir.[1242] *Ex-ante* yollar, engellemeye konu olan web sitelerinin sahiplerine ön bildirim yapılmasını içerir. *Ex-post* yollar ise bir engelleme kararı uygulandıktan sonra kararın kapsamını kısıtlamak veya yeni koşullar dikkate alınarak karara itiraz etmek için etkin mekanizmaların varlığını ifade eder.

AİHM, AİHS'nin 10. maddesi ile 13. maddesindeki menfaatlerin niteliğine ilişkin bir karşılaştırma yapmıştır.[1243] AİHM'ye göre 13. madde usuli bir koruma sağlarken, diğer bir deyişle etkin bir başvuru hakkını gerekli kılarken, 10. maddenin bünyesindeki usuli koruma ifade özgürlüğünün özüne saygıyı temin etme gibi daha geniş bir amacın yan unsuru niteliğindedir. Mahkemeye göre, başvurucunun, ifade özgürlüğünün kısıtlandığına dair bir iddiası vardır.[1244] Mahkeme, 13. maddenin, iddia edilen ihlalleri veya devamını önleyen veya vuku bulmuş ihlallere ilişkin uygun tazmin imkânları sağlayan, hem hukuken hem de uygulamada etkili bir yerel hak arama mekanizmasını gerektirdiğini hatırlatmıştır.

Tüm bu tespitler ışığında AİHM, başvurucuya engelleme kararına itiraz etme ve itiraz yargılamalarına katılma imkânı sağlanmış olsa da temyiz mahkemesinin şikâyetin özüne ilişkin bir değerlendirme yapmadığı görüşündedir.[1245] Keza, temyiz mahkemesi web sayfası ve web sitesi arasındaki ayrımı, engelleme tedbirinin gerekliliği ve ölçülülüğü ile tercih edilen bu yöntemi uygulamanın aşırı etkilerini ele almamış; başvurucunun delillerini değerlendirmemiş ve bu delillerin kabul veya reddedilmesine ilişkin herhangi bir muhakeme gerçekleştirmemiştir. AİHM bu sebeplerle başvurucunun davasının koşulları çerçevesinde ulusal hukukun etkin bir hak arama yolu sunmadığına hükmetmiş ve AİHS'nin 10. maddesiyle beraber 13. maddesinin de ihlal edildiğine karar vermiştir.[1246]

Sonuçta AİHM, başvuruyu kabul edilebilir görmüş, AİHS'nin 10. maddesinin ihlal edildiğine karar vermiş, 10. maddenin yanı sıra 13.

[1242] *Bulgakov v. Rusya*, para. 45.

[1243] *Bulgakov v. Rusya*, para. 46.

[1244] *Bulgakov v. Rusya*, para. 47.

[1245] *Bulgakov v. Rusya*, para. 48.

[1246] *Bulgakov v. Rusya*, para. 48.

maddenin de ihlal edildiğine kanaat getirmiş ve başvurucuya tazminat ödenmesine hükmetmiştir.

VIII. Yargıçlar Lemmens, Dedov ve Poláčková'nın mutabık görüşü

Mahkemenin kararına Yargıçlar Lemmens, Dedov ve Poláčková müşterek bir mutabık görüş yazmışlardır.[1247] AİHS'nin 10 ve 13. maddelerinin ihlal edildiği görüşünde olan Yargıçlar, 10. maddenin ihlaline yönelik gerekçeye ilave görüşlerini paylaşmışlardır. Engelleme sürecine atıf yapan Yargıçlar, sitede yer alan bir web sayfasındaki içeriği engellemek için tercih edilen teknik sebebiyle sitenin tamamen engellendiğini hatırlatmıştır.[1248] Yargıçlar, başvuranın engellemeye sebep olan e-kitabın hukukiliğini tartışmadığını, şikâyetinin temelinin söz konusu içerik kaldırılmasına rağmen web sitesine erişimin engellenmeye devam etmesi olduğunu belirtmişlerdir.

Yargıçlar, engelleme kararının, hedeflenen hukuka aykırı içeriği aşan şekilde uygulanmasının kanuni dayanaktan yoksun olduğu ve hukuka aykırı içerik (e-kitap) kaldırılmış olmasına rağmen engellemenin devam etmesinin yasal dayanağı olmadığı yönündeki Mahkeme tespitine katılmışlardır. Yargıçlara göre yerel hukukta bir dayanak olmaması, müdahalenin kanunla öngörülme şartını yerine getirmemesi için tek başına yeterlidir.[1249]

Yargıçların, yerel mahkemelerin yaklaşımlarının ele alınmasına ilişkin ilave yorumları vardır.[1250] Kararda, yerel kanunun web sitesi sahibine -olayda başvurucuya- erişimi engelleme süreçlerine müdahale imkânı vermemesi eleştirilmiştir. Müdahale, AİHS'yi iki sebeple ihlal etmiştir: Öncelikle, engelleme kararı başvurucunun haklarını savunmasına imkân

[1247] *Bulgakov v. Rusya*, Yargıçlar Lemmens, Dedov ve Poláčková'nın Mutabık Görüşü.
[1248] *Bulgakov v. Rusya*, Yargıçlar Lemmens, Dedov ve Poláčková'nın Mutabık Görüşü, para. 2.
[1249] *Bulgakov v. Rusya*, Yargıçlar Lemmens, Dedov ve Poláčková'nın Mutabık Görüşü, para. 3.
[1250] *Bulgakov v. Rusya*, Yargıçlar Lemmens, Dedov ve Poláčková'nın Mutabık Görüşü, para. 4.

vermeyecek şekilde alınmıştır; ikinci olarak, engelleme kararı yerel hukukta izin verilen müdahalenin sınırlarını aşmıştır.

Yargıçlara göre mevcut kararın gereğince uygulanabilmesi için Rus kanun koyucusu, kanunu, web sitesi sahiplerine haklarını gereğince savunma ve hukuka aykırı içeriği kaldırmaları durumunda web sitelerinin (veya ilgili sayfasının) engellenmesini önleme imkânı tanıyacak şekilde değiştirmelidir. Aynı doğrultuda hem savcılar hem de hâkimler bir web sayfasına erişimi engellemek için kullandıkları formülü gözden geçirmelidir. Yargıçlar Lemmens, Dedov ve Poláčková, şayet hâkimlerin bu konuda teknik uzmanlık eksiklikleri varsa kendilerine bu tür davalara ilişkin uygun bir eğitim sağlanması gerektiğini vurgulamışlardır.

IX. Değerlendirme

Bulgakov v. Rusya kararında AİHM, erişimi engelleme tekniklerinin ifade özgürlüğüne etkileri konusunu tekrar ele almıştır. Önceki içtihatlarıyla paralel şekilde AİHM, hukuka aykırı bir içerik sebebiyle tüm web sitesine erişimin engellenmesini AİHS'nin 10. maddesinde güvence altına alınan ifade özgürlüğüne ölçüsüz bir müdahale olarak nitelendirmiştir. Mahkeme analoji yaparak hukuka aykırı bir içerik sebebiyle web sitesinin tamamen engellenmesinin, bir gazetenin veya televizyon istasyonunun tamamen yasaklanmasına eş değer olduğunu belirtmiştir.

AİHM, internet içeriğinin engellenmesini tamamen reddetmemektedir. Ancak, bir engelleme gerçekleştirilecekse bunu düzenleyen mevzuatın belirli koşulları sağlaması gerektiğinin altını çizmektedir. Bu koşullar şu şekilde sıralanabilir: Engellemeye yönelik yasal bir dayanak olmalı, somut olayda daha az müdahaleci bir tedbirle aynı sonuca ulaşılıp ulaşılamayacağı değerlendirilmeli, mevzuat tedbirlerin aşırı ve keyfî olarak uygulanmasını önlemek için gerekli koruma mekanizmalarını içermelidir. Keza, etkin bir hak arama yolu mevcut olmalı ve bu yol kullanılarak hem *ex-ante* hem de *ex-post* ihlallere yönelik şikâyetler giderilebilmelidir. Tekrar etmek gerekirse *ex-ante* yollar, engellemeye konu olan web sitelerinin sahiplerine ön bildirim yapılmasını içerir. *Ex-post* yollar ise bir engelleme kararı uygulandıktan sonra kararın kapsamını kısıtlamak veya

yeni koşullar dikkate alınarak karara itiraz etmek için etkin mekanizmaların varlığını ifade eder.

Mevcut davada, yerel mahkemelerin erişimin engellenmesi amacıyla kullanılan IP engelleme tekniğine ilişkin teknik bilgi eksiklikleri göze çarpmaktadır. IP engellemesi, Dördüncü Bölümde ele alındığı üzere, en müdahaleci engelleme tekniğidir.[1251] Bu teknik, sadece bir web sitesini değil, alakasız binlerce web sitesini ve internet hizmetini işlevsiz kılabilmektedir.

Bulgakov v. Rusya kararında göze çarpan bir diğer husus ise engelleme tedbirinin niteliğine ilişkin yasal mevzuattaki hukuki belirsizliktir. Engelleme tedbiri, geçici bir koruma tedbiridir. Nihai amaç, hukuka aykırı içeriğin internet ortamından kaldırılmasını sağlamaktır. Mevcut uyuşmazlıkta ise engelleme tedbirleri nihai bir hüküm hâline dönüşmüş ve içerik kaldırılsa bile uygulanmaya devam etmiştir. Bu bağlamda, engelleme tedbirlerinin geçiciliği tekrar hatırlatılmaktadır.

Kararın önemli bir çıktısı, erişimin engellenmesi tedbirinin uygulandığı durumlarda, engellemeden etkilenen kişilerin bu tedbirden haberdar olmasının sağlanmasıdır. Bu şekilde kişilerin itiraz sürecini işletmeleri ve kendilerini savunmaları mümkün olabilecektir.

Avrupa Konseyinin İnternet Özgürlüğüne İlişkin Tavsiye Kararı'nda aslında bu şeffaflık ve de şikâyet mekanizmaları gayet yerinde bir şekilde ele alınmıştır. Tavsiye Kararı'nda isabetle belirtildiği üzere:[1252]

"*Devlet, faaliyetleri kapsamında tüm özel sektör aktörlerinin internet bağlamında insan haklarına saygı göstermesi için politikalar ve tedbirler uygular. Bilhassa internet ortamında insan hakları ve temel özgürlükleri olumsuz etkilenebilecek bireylerin, şikâyetlerini erkenden ve doğrudan iletebilecekleri etkin şikâyet mekanizmaları kurar. Mekanizmalar meşru (şikâyet süreçlerinin adil bir şekilde yürütülmesini temin eden güveni sağlar), erişilebilir (ilgililer tarafından bilinir, erişimin önünde engel yoktur), öngörülebilir (her bir adım için belirtici zaman dilimi, süreç türlerine ilişkin netlik ve muhtemel*

[1251] Bkz. **§4(X)(A)**[IP engellemesi].

[1252] İnternet Özgürlüğüne İlişkin Tavsiye Kararı için bkz. **§6(XXIV)**.

sonuç içeren açık ve bilinen bir usul ve uygulamayı takip etme imkânı veren araçlar sağlar), adil (bilgi kaynaklarına makul erişim, bir şikâyet sürecine dâhil olmak için gerekli tavsiye ve uzmanlık), şeffaf (bir şikâyetin sürecine ilişkin tarafları sürekli bilgilendirir) ve AİHS'nin 13. maddesiyle uyumludur."

Benzer şekilde Avrupa Konseyinin İnternet Filtreleri Bağlamında İfade ve Bilgi Özgürlüğüne Saygının Teşvik Edilmesine Yönelik Tedbirleri İçeren Tavsiye Kararı'nda belirtildiği üzere devletler; kullanıcıları ve/veya sahipleri içeriğin haklı olmayan bir gerekçeyle engellendiğini iddia ederlerse filtrelemenin askıya alınması dâhil etkili ve hemen erişilebilir denetim ve çözüm imkânları sağlamalıdır.[1253]

[1253] İnternet Filtreleri Bağlamında İfade ve Bilgi Özgürlüğüne Saygının Teşvik Edilmesine Yönelik Tedbirleri İçeren Tavsiye Kararı için bkz. **§6(IX)**.

§22. ENGELS V. RUSYA

AİHM'nin, 23 Haziran 2020 tarihinde Rusya'ya ilişkin verdiği bir diğer karar *Engels v. Rusya* kararıdır.[1254] Başvuru temelde, bir web sitesinde yer alan ve internette filtresiz gezinti teknolojilerine ilişkin bilgiler ihtiva eden içeriğin Rus mahkemelerinin kararıyla yasaklı içerik olarak nitelendirilmesine ilişkindir.

I. Davanın gelişimi

Başvurucu Bay Grégory Engels, Rusya doğumlu Alman bir siyasetçi ve internette ifade özgürlüğünü desteklemeye çalışan bir aktivisttir.[1255]

Başvurucu, 2012 yılında, yerel Rus aktivistlerle birlikte RosKomSvoboda isimli (rublacklist.net) web sitesini kurmuştur.[1256] Web sitesinde internet ortamında ifade özgürlüğü, online mahremiyet konuları, telif hakları ve dijital haberleşmeye ilişkin haber, bilgi, analiz ve araştırmalar yer almaktadır. Web sitesinin ismi, yasaklanmış online içeriklere ilişkin bir liste tutan Rus telekomünikasyon otoritesi Roskomnadzor'a (Rus Gözetim Komitesi) benzetilerek RosKomSvoboda (Rus Özgürlük Komitesi) konulmuştur.

RosKomSvoboda web sitesindeki rublacklist.net/bypass URL adresinde yer alan bir sayfada VPN, Tor tarayıcısı, I2P teknolojisi, web tarayıcılarındaki turbo modu ve içeriğe ulaşmak için online tercüme araçlarının kullanılması gibi internette özel haberleşmeler ve içerik filtreleri üzerindeki kısıtlamaları aşmak için kullanılan araçların ve yazılımların bir listesine ve kısa tanıtımlarına yer verilmiştir.[1257]

[1254] **AİHM**, *Engels v. Rusya*, Başvuru No: 61919/16, 23.6.2020.

[1255] *Engels v. Rusya*, para. 3.

[1256] *Engels v. Rusya*, para. 4.

[1257] *Engels v. Rusya*, para. 5.

2015 yılında Krasnodar Bölgesi'nde bir bölge savcısı, rublacklist.net/bypass sayfasındaki içeriğe Rusya'dan erişimin yasaklanması talebiyle Anapa İlçe Mahkemesine başvuruda bulunmuştur.[1258] Savcıya göre sayfada yer alan anonimleştirme araçları, kullanıcıların ilgisiz başka bir web sitesinde yer alan aşırılıkçı içeriklere erişmesine imkân tanımaktadır. 13 Nisan 2015 tarihinde Anapa İlçe Mahkemesi, başvurucuya söz konusu taleple ilgili herhangi bir bilgi vermeksizin savcının talebini kabul etmiş ve rublacklist.net/bypass sayfasının hukuka aykırı bir içerik olduğuna hükmetmiştir. Akabinde söz konusu sayfaya erişimi engellemesi için kararı Roskomnadzor'a göndermiştir.

Erişimi engelleme kararını uygulama aşamasında Roskomnadzor, başvurucuya rublacklist.net/bypass sayfasında yer alan içeriği kaldırmasını ihtar etmiş, aksi hâlde söz konusu içeriğe erişimi engelleyeceğini belirtmiştir.[1259] Başvurucu, talebi yerine getirmiş ve hukuka aykırı olduğu iddia edilen bilgiyi silmiştir.

Başvurucu, içeriği kaldırmasından sonra erişimi engelleme kararına karşı itirazda bulunmuştur.[1260] Başvurucu, tüm iletişim bilgileri web sitesinde yer almasına rağmen başsavcının talebinin kendisinin yokluğunda değerlendirilmiş ve kararın gıyabında alınmış olmasının hakkaniyete aykırı olduğunu ileri sürmüştür. Ayrıca, internet ortamında gezinti sırasında mahremiyetin korunması için kullanılan araçlar ve yazılımlar hakkında bilgi verilmesinin Rus hukukuna aykırı olmadığını belirtmiştir. 29 Eylül 2015 tarihinde Krasnodar Bölge Mahkemesi, başvurucunun iddialarını gereğince ele almaksızın itirazı reddetmiştir.[1261]

II. Hukuki arka plan

Konunun esasına girmeden önce AİHM, Rus hukukunun internet ortamını düzenleyen en temel yasası olan Bilgi Kanunu'nu (Federal Yasa

[1258] *Engels v. Rusya*, para. 6.

[1259] *Engels v. Rusya*, para. 7.

[1260] *Engels v. Rusya*, para. 8.

[1261] *Engels v. Rusya*, para. 9.

no. 149-FZ, 27 Temmuz 2006) incelemiştir.[1262] Bilgi Kanunu'nun 3. bölümü, bilgiye erişimi ve bilgi teknolojilerini düzenlemektedir. Burada yer alan 1. İlke, her türlü hukuki yolla bilgiyi arama, alma, yayma, oluşturma ve dağıtma özgürlüğünü güvence altına almaktadır. 2. İlke, bilgiye erişime ilişkin her türlü kısıtlamanın federal bir yasada düzenlenmesini zorunlu tutarken, 8. İlke yasal düzenlemelerin belirli bir bilgi teknolojisinin kullanımını öncelemesini yasaklamaktadır.

Bilgi Kanunu'nun 15.1'inci maddesi telekomünikasyon otoritesi Roskomnadzor'a Rusya Federasyonu'nda yasaklanan içeriklere ilişkin alan adlarının, web sayfa referanslarının (URL adresleri) ve ağ adreslerinin Bütüncül Sicil'ini tutma yükümlülüğü getirmektedir.[1263] Aynı hükmün beşinci fıkrası ise hangi içeriklerin hukuka aykırı sayılacağı ve Bütüncül Sicil'e ekleneceğini düzenlemektedir: (1) yetkili bir idari makamın bir içeriğin, yedi hukuka aykırı içerik kategorisinden (çocuk pornografisi, uyuşturucu üretimi veya kullanımı, intihar yöntemleri gibi) birine girdiğini tespit etmesi durumunda; (2) yargı makamları tarafından belirli bir internet içeriğinin Rusya'da dağıtımının yasaklanması gerektiğine yönelik karar alınması durumunda; (3) bir yetkili makam tarafından bir içeriğin hakaret niteliğinde olduğunun tespit edilmesi durumunda. Hükmün yedinci fıkrası uyarınca, bir barındırma hizmet sağlayıcısı hukuka aykırı içeriğin Bütüncül Sicil'e eklendiği konusunda Roskomnadzor tarafından haberdar edildiğinde web sitesi sahibini bilgilendirmek ve hukuka aykırı içeriği kaldırmasını talep etmekle yükümlüdür.

Bilgi Kanunu'na yaptığı atıflardan sonra AİHM, muhtelif uluslararası belgelere değinmiştir. Bunlardan ilki, Avrupa Konseyinin 28 Mayıs 2003 tarihli İnternette İletişim Özgürlüğüne İlişkin Deklarasyon'udur.[1264] Deklarasyon'un "Devletin ön kontrolünün bulunmaması" başlıklı 3. maddesine atıf yapan AİHM, kamu otoritelerinin her türlü sınırdan bağımsız olarak genel engelleme veya filtreleme tedbiri uygulayarak kamunun bil-

[1262] *Engels v. Rusya*, para. 10.

[1263] *Engels v. Rusya*, para. 11.

[1264] İnternette İletişim Özgürlüğüne İlişkin Deklarasyon için bkz. **§6(IV)**.

giye erişimini veya internet ortamında başka tür iletişimi engellememesi gerektiğini tekrarlamıştır.[1265]

Düşünce ve ifade özgürlüğü hakkının korunması ve desteklenmesine ilişkin BM Özel Raportörü'nün 2011 tarihli Rapor'una (A/HRC/17/27), Birleşmiş Milletler Fikir ve İfade Özgürlüğü Özel Raportörü, Avrupa Güvenlik ve İşbirliği Teşkilatı Medya Özgürlüğü Temsilcisi, Amerikan Devletleri Örgütü İfade Özgürlüğü Özel Raportörü, Afrika İnsan ve Halkların Hakları Komisyonu İfade Özgürlüğü ve Bilgiye Erişim Özel Raportörü'nün 1 Haziran 2011 tarihli Ortak Deklarasyonu'na ve Birleşmiş Milletler İnsan Hakları Komitesinin 11-29 Temmuz 2011 tarihleri arasında gerçekleşen 102. oturumunda Medeni ve Siyasi Haklara İlişkin Uluslararası Sözleşme'nin 19. maddesiyle ilgili olarak kabul ettiği 34 sayılı Genel Yorum'una vurgu yapmıştır.[1266]

Son olarak ise Avrupa Konseyinin CM/Rec(2016)5 sayılı İnternet Özgürlüğüne İlişkin Tavsiye Kararı'ndan alıntılar yapmıştır.[1267] Söz konusu Tavsiye Kararı'nın ilgili kısımlarını tekrar etmek gerekirse:

2.2.1. Devlet makamları veya özel sektör aktörleri tarafından bir internet platformunu (sosyal medya, sosyal ağlar, bloglar veya başka diğer web siteleri) veya bilgi ve haberleşme teknolojileri (BT) araçlarını (anlık mesajlaşma ve diğer uygulamalar) engelleyen veya bunlara erişimi başka şekilde kısıtlayan her türlü tedbir veya devlet makamlarının bu tür eylemlere yönelik talepleri, kısıtlamaların kanunla öngörülmesini, meşruluk ve ölçülülük koşullarına uygun olmasını öngören AİHS'nin 10. maddesiyle uyumlu olmalıdır.

2.2.2. Devlet makamları veya özel sektör tarafından alınan internet içeriğini engelleme, filtreleme veya kaldırmaya yönelik her türlü tedbir veya bu tür bir işlem için devlet makamları tarafından gerçekleştirilen her türlü talep, kısıtlamaların kanunla öngörülmesini, meşruluk ve ölçülülük koşullarına uygun olmasını öngören AİHS'nin 10. maddesiyle uyumlu olmalıdır.

[1265] *Engels v. Rusya*, para. 12.

[1266] *Engels v. Rusya*, para. 13-15.

[1267]

2.2.3. İnternet hizmet sağlayıcıları, genel bir ilke olarak, internet trafiğine eşit ve gönderen, alıcı, içerik, uygulama, hizmet veya cihaz temelli ayrımcılık yapmayacak şekilde muamele eder. İnternet trafik yönetim tedbirleri, AİHS'nin 10. maddesine uygun şekilde üstün kamusal yarara ulaşmak için şeffaf, gerekli ve ölçülü olmalıdır.

2.2.4. İnternet kullanıcılarının veya ilgili diğer tarafların, internete erişim, içerik veya bilgiyi alma ve yayma imkânlarını sınırlamaya yönelik işlemlere karşı AİHS'nin 6. maddesine uygun şekilde mahkemelere erişim hakkı vardır.

2.2.5. Devlet, bilgi alma ve yayma özgürlüğüne uyguladığı engellenen veya içerdiği bilgiler kaldırılan web sitelerini göstermek gibi kısıtlamalar hakkında bunların hukuki dayanağı, gerekliliği ve gerekçesi, bu işleme izin veren mahkeme kararı ve bu karara itiraz hakkını içerecek şekilde kamuoyunu zamanında ve uygun şekilde bilgilendirmelidir.

Yukarıda belirtilen Tavsiye Kararı'na Rusya Federasyonu tarafından özel çekince koyulduğunu belirtmek gerekir.

III. Tarafların iddiaları

Başvurucu, kendisini web sitesinden bir içeriği kaldırmak zorunda bırakan kararın AİHS'nin 10. maddesinde güvence altına alınan haklarını ihlal ettiğini ileri sürmüştür.[1268] AİHM, bu iddianın açıkça dayanaktan yoksun olmadığına ve kabul edilebilir olduğuna karar vermiştir.[1269]

IV. Rus Hükûmetinin savunması

Rus Hükûmeti, rublacklist.net/bypass sayfasında tanıtılan web araçlarının kullanıcılara Federal Aşırılıkçı İçerik Listesi'nde yer alan materyaller de dâhil yasaklı aşırılıkçı içeriklere sınırsız erişim imkânı tanıdığını iddia etmiştir.[1270] Hükûmete göre Anapa İlçe Mahkemesi,

[1268] *Engels v. Rusya*, para. 17.

[1269] *Engels v. Rusya*, para. 18.

[1270] *Engels v. Rusya*, para. 19.

savcının içeriğe erişimin engellenmesi başvurusunu isabetli bir şekilde onaylamıştır. Yine Hükûmete göre Bütüncül Sicil'in güncellenmesine ilişkin yasal düzenleme uygulamada yeterince açık ve öngörülebilirdir. Keza, Hükûmet, Roskomnadzor'un hukuka aykırı içeriği Bütüncül Sicil'e ekleme kararının da yasal, gerekçeli ve gerekli bir tedbir olduğunu ileri sürmüştür. Son olarak, başvurucunun hukuka aykırı içeriği kaldırması neticesinde web sitesi engellenmediği için AİHS'nin 10. maddesinin ihlal edilmediği görüşündedir.

V. Başvurucunun iddiaları

Başvurucu, web sitesinin engellenmesini önlemek adına hukuka uygun içeriği kaldırmaya zorlandığından bahisle bilgi yayma hakkının ihlal edildiğini ileri sürmüştür.[1271] Başvurucunun iddiaları şu şekildedir: Rus makamları, filtresiz gezinti araçlarına ilişkin bilgiyi kısıtlamak için herhangi bir yasal gerekçe belirtmemiş; web sayfasında aşırılıkçı veya terörizmle alakalı bir materyal bulunduğunu ispat edememiştir. Bu şartlarda içeriği kaldırmakla yükümlü tutulmak, Bilgi Kanunu'nun 3. bölümündeki 8. İlke'de yer alan belirli bir bilgi teknolojisini tercih etme yasağının ihlali niteliğindedir. Müdahalenin dayandırıldığı kural öngörülebilir değildir. Bu şekilde mahkemeler, herhangi bir tür veya kategori belirtmeye gerek duymaksızın dilediği içeriği hukuka aykırı olarak nitelendirebilecektir. Kendisi gibi web sitesi sahipleri, bir içeriğin kaldırılabileceği veya web sitelerinin engellenebileceğini önceden bilemeyecektir. Engellemeyi düzenleyen mevzuat belirlilik taşımamakta, bazı hukuka aykırı içerikler barındırdığı için tüm web sitesine erişimi engellemeye izin vermektedir.[1272] Bu bağlamda başvurucu, Rus mevzuatının, kötüye kullanımı önlemek için web sitesi sahiplerine herhangi bir güvence sağlamadığını belirtmiştir.

[1271] *Engels v. Rusya*, para. 20.

[1272] *Engels v. Rusya*, para. 20.

VI. Müdahil tarafların görüşleri

Davaya farklı taraflar ve sivil toplum örgütleri müdahil olmuş, görüşlerini paylaşmıştır. Bunlardan ilki Birleşmiş Milletler Fikir ve İfade Özgürlüğü Özel Raportörü'dür.[1273] Raportör, bireylerin çevrim içi ortamda tıpkı çevrim dışı ortamda olduğu gibi ifade özgürlüğünden faydalanmasına izin verilmesi gerektiğini vurgulamıştır. Web sitelerinin tamamen engellenmesi konusuna da değinen Raportör; bu tür engellemelerin, ifade özgürlüğünün izin verilen sınırlarına ilişkin kriterleri sağlaması, içeriğe özgü olması ve web sitelerinin salt hükûmeti veya siyasal sistemi eleştiriyor diye hedef alınmaması durumunda istisnai olarak uygulanabileceği görüşündedir.Davaya müdahil olarak görüş veren bir diğer taraf ise Article 19, EFF, Access Now ve Reporters without Borders isimli sivil toplum örgütleridir.[1274]

Söz konusu kuruluşlara göre, bir web sitesinin tamamına erişimi engelleme, hukuka uygun-hukuka aykırı içerik arasında ayrım yapma imkânı tanımadığı ve bu sebeple hukuken asla gerekli olamayacağı için aşırı ve ölçüsüz bir tedbirdir. Şayet erişimi engelleme tedbirine izin veriliyorsa kanun şu minimum standartları sağlamalıdır: (i) Bir mahkeme veya bağımsız bir yargısal organ tarafından engellemeye karar verilmelidir; (ii) ilgili taraflara engelleme kararının arandığı yargılamalara müdahale hakkı tanınmalıdır; (iii) engelleme kararlarının tüm mağdurlarına engelleme kararlarına itiraz hakkı tanınmalıdır; (iv) engellenen web sitelerine erişmeye çalışan herkes, engelleme kararının hukuki dayanağı ve gerekçeleri ile bu karara itiraz yollarına ilişkin bilgiyi görebilmelidir.

Son müdahil, Avrupa Bilgi Toplumu Enstitüsü isimli sivil toplum örgütüdür.[1275] Söz konusu kuruluş, hedefini aşan ve meşru içeriği aşırı şekilde engelleyen bir tedbirin demokratik toplumda kabul edilebilir olmadığını belirtmiş ve yetkili makamların aynı sonuca daha az müdahaleci bir tedbirle ulaşılıp ulaşılamayacağına dair bireyselleştirilmiş bir değerlendirme yapması gerektiğini vurgulamıştır. Bu doğrultuda, hedef

[1273] *Engels v. Rusya*, para. 21

[1274] *Engels v. Rusya*, para. 22.

[1275] *Engels v. Rusya*, para. 23.

alınan web sitesinin bilgilendirilmesi gerektiğini, hukuka aykırı içeriği kaldırması ve bu karara ilişkin beyanlarda bulunması için kendisine makul bir süre verilmesi lazım geldiğini beyan etmiştir.

VII. AİHM'nin tespit ve değerlendirmeleri

Konunun esasına giren AİHM, öncelikle *Ahmet Yıldırım v. Türkiye* kararındaki internetin niteliğine ilişkin tespitlerine atıf yapmıştır.[1276] Tekrar etmek gerekirse, AİHM söz konusu kararında erişilebilirliğin yanı sıra büyük miktarda veriyi muhafaza etme ve dağıtma imkânları sayesinde internet sitelerinin kamunun güncele erişiminin iyileştirilmesine ve bilginin iletilmesinin kolaylaştırılmasına önemli derecede katkıda bulunduğunu; internetin politik veya kamu menfaatine ilişkin tartışma ve eylemlere katılım konusunda asli vasıtaları barındırdığını ve AİHS'nin 10. maddesinin yalnızca bilgilerin iletilmesi hakkını değil, aynı zamanda toplumun bilgi alma hakkını da güvence altına aldığını belirtmiştir.

Başvurucu, online ortamda ifade özgürlüğü ve dijital mahremiyetin korunmasına hizmet eden bir web sitesinin sahibi ve yöneticisidir. Bir Rus mahkemesi Nisan 2015'te kendisinden habersiz şekilde, web sitesinin bir bölümünün yasaklı bilgi içerdiği tespitinde bulunmuş ve telekomünikasyon otoritesinden söz konusu web sitesinin tamamına erişimi derhâl engellemesini talep etmiştir.[1277] Yukarıda belirtildiği üzere, başvurucu bahsi geçen içeriği kaldırdığı için sitesine engelleme tedbiri uygulanmamıştır. AİHM, başvurucunun hukuka aykırı olduğu iddia edilen içeriği kaldırmak ya da web sitesinin tamamına erişimin engellenmesine katlanmak şeklinde bir tercihte bulunmak zorunda bırakıldığını belirtmiştir.[1278] Rus yerel mahkemesinin kararına uyularak içeriğin kaldırılması, web sitesinin ziyaretçilerinin söz konusu içeriğe erişememesine yol açmıştır.

Bu tespitten sonra Mahkeme, *Ahmet Yıldırım v. Türkiye* kararına tekrar atıf yaparak AİHS'nin 10. maddesinin yalnızca bilgilerin iletilme-

[1276] *Engels v. Rusya*, para. 24.

[1277] *OOO Flavus ve Diğerleri v. Rusya*, para. 25.

[1278] *OOO Flavus ve Diğerleri v. Rusya*, para. 25.

si hakkını değil, aynı zamanda toplum açısından bilgi alma hakkını da güvence altına aldığını hatırlatmıştır.[1279] AİHM'ye göre, bir müdahale, kanunla öngörülme, AİHS'nin 10. maddesinin ikinci fıkrasında belirtilen meşru amaçlardan bir veya birden fazlasını gütme ve bu amaçlara ulaşmak için demokratik bir toplumda gerekli olma şartlarını taşımadıkça 10. maddeyi ihlal etmiş olacaktır.

AİHM'ye göre "kanunla öngörülen" ifadesi öncelikle tedbirin iç hukukta bir dayanağı olmasını gerektirir. Ayrıca söz konusu yasanın, kendisi açısından ortaya çıkabilecek sonuçları ve hukukun üstünlüğü ilkesiyle uyumunu önceden değerlendirebilmesi için ilgili kişi açısından erişilebilir olması gerektiğini ifade eder.[1280] Yasanın yürütme organına temel haklara ilişkin konularda sınırsız bir takdir yetkisi vermesi hâlinde AİHS'nin benimsediği demokratik bir toplumu oluşturan ana ilkelerden hukukun üstünlüğü ilkesine aykırılık söz konusu olacaktır. Bu sebeple yasa, bu gücün kullanılmasının yöntemini ve kapsamını yeterli netlikte düzenlemelidir.

Müdahalenin yasal dayanağı, Bilgi Kanunu'nun 15.1. maddesidir. Yukarıda belirtildiği üzere, bu hükmün 5. fıkrasında Rus makamlarının kararlarıyla hukuka aykırı içerik olarak sınıflandırabileceği üç tüp içerik kategorisi yer almaktadır. Mevcut uyuşmazlık, bir mahkeme kararıyla hukuka aykırılık tespit edilerek bilginin Rusya'da yayılmasını önlemeye imkân tanıyan kategoriye girmektedir.

AİHM, bu hükmün kapsamının istisnai ve emsalsiz olduğu görüşündedir.[1281] Mahkemeye göre, bu hüküm, mahkemelere veya web sitesi sahiplerine, yasaklanması muhtemel online içerik kategorilerinin niteliğine ilişkin hiçbir bilgi vermemektedir. Keza, uygulanma kapsamına ilişkin bir ikincil düzenleme, yönetmelik veya regülasyona atıf yapmamaktadır. AİHM, bu tür müphem ve aşırı geniş bir yasal düzenlemenin öngörülebilirlik kriterini karşılamadığına karar vermiştir.[1282] Mahkemeye

[1279] *Engels v. Rusya*, para. 26.
[1280] *Engels v. Rusya*, para. 26.
[1281] *Engels v. Rusya*, para. 27.
[1282] *Engels v. Rusya*, para. 27.

göre bu hüküm, başvurucu gibi web sitesi sahiplerine, hangi tür içeriğin engellenmesinin muhtemel olduğu ve tüm web sitesinin erişiminin engellenmesi tedbirine yol açacağına dair davranışlarını düzenleme imkânı tanımamaktadır.

AİHM, mevcut davanın bu hukuki düzenlemenin uygulamada keyfî etki doğurmasına örnek teşkil eden nitelikte olduğunu vurgulamıştır.[1283] Olayda, savcı tarafından yapılan bir başvuru üzerine, bir Rus yerel mahkemesi başvurucunun sitesinde yer alan filtrelemeleri aşma araçları ve yazılımlarını "*Rusya'da dağıtımı yasaklanması gereken bilgi*" olarak nitelendirmiştir. AİHM, yerel mahkemenin, bu kararı verirken filtreleme aşma teknolojilerinin Rusya'da hukuka aykırı olduğuna veya bu tür bilgilerin herhangi bir Rus hukuku düzenlemesini ihlal ettiğine dair bir değerlendirme yapmadığının altını çizmiştir. Aynı doğrultuda, yerel mahkemenin başvurucunun web sitesinde aşırılıkçı ifadeler, şiddete veya hukuka aykırı eylemlere teşvik, çocuk pornografisi veya başkaca yasaklı içerik olup olmadığına dair bir tespit de yapmadıklarını belirtmiştir. Yerel mahkemenin kararının tek dayanağı, filtrelemeleri aşma teknolojilerinin internet kullanıcılarına başvurucuyla bağlantılı veya ilişkili olmayan ve üzerinde başvurucunun herhangi bir kontrolü bulunmayan başka internet sitelerindeki aşırılıkçı içeriklere erişime imkânı sağlamasıdır.

AİHM, filtreleme aşma teknolojilerinin salt aşırılıkçı içeriklere kötü niyetle ulaşmak için kullanılan bir araca indirgenemeyeceği görüşündedir.[1284] Mahkeme, herhangi bir bilgi teknolojisinin demokratik bir toplumun temel ilkeleriyle bağdaşmayan bir amaç için kullanılma riskinin her zaman mevcut olduğunu belirttikten sonra, filtreleme aşma teknolojilerinin uzaktaki sunuculara güvenli bağlantı sağlamak, yavaş bağlantılarda sayfa yükleme zamanını azaltmak için veri aktarım kanalı sunma, hızlı ve ücretsiz çeviri sağlama gibi meşru bir çok amaçla da kullanılabileceğini hatırlatmıştır.

AİHM, matbaadan internete tüm bilgi teknolojilerinin bilgiyi saklamak, işlemek ve bilgiye erişmek amacıyla geliştirildiğini belirtmiş ve

[1283] *Engels v. Rusya*, para. 28.

[1284] *Engels v. Rusya*, para. 29.

davaya müdahil BM İnsan Hakları Komitesinin bilgi teknolojilerinin içerikten bağımsız olduğuna dair tespitine atıf yapmıştır.[1285] Diğer bir deyişle, bu tür teknolojiler içeriği saklamak ve içeriğe erişmek için araçlar olup içeriğin kendisiyle özdeşleştirilmemelidir.

AİHM'ye göre matbaa nasıl okul kitaplarından aşırılıkçı ideolojiye ait broşürlerin basımına kadar farklı amaçlarla kullanılabilirse internet de benzer bir amaçla kullanılabilir.[1286] Mahkeme, bazı teknolojilerin bir şekilde aşırılıkçı içeriğe erişimi kolaylaştırmak için kullanılmasının engellenmesini, bir yazıcı veya fotokopi makinesinin bu tür bir içeriği basmak için kullanılmasının yasaklanmasına benzetmektedir. Tüm bu tespitler ışığında AİHM, bu tür teknolojilere ait bilgilerin engellenmesinin bu teknolojiler kullanılarak erişilebilecek tüm içeriğe erişimi engellemekle eş değer olduğunu belirlemiş, yerel hukukta bu konuda açık bir yasal düzenleme olmamasını dikkate alarak böylesine geniş bir tedbirin keyfî nitelikte olduğuna hükmetmiştir.[1287]

Tedbirin keyfî bir uygulamaya yol açtığına dair tespitinden sonra AİHM, aşırı ve keyfî uygulamaya karşı bireylere herhangi bir koruma mekanizması sağlanıp sağlanmadığı sorunsalını ele almıştır. AİHM, Bilgi Kanunu'nun 15.1 maddesinin (5)(2) bendiyle tanınan takdir yetkisinin genişliğinin, temyiz aşamasında mahkemenin kararına karşı çıkmayı -imkânsız kılmasa da- güçleştirdiği kanaatindedir.[1288] AİHM, bu kanaate varırken *Kablis v. Rusya* kararındaki tespitlerine de yer vermiştir.

AİHM, Rus hukukunun, başvurucu gibi web sitesi sahiplerine kendilerini keyfî müdahalelere karşı koruyacak usuli güvenceler içermediğini tespit etmiştir.[1289] Düzenleme, web sitesi sahiplerinin engellemeye ilişkin süreçlere bir şekilde dâhil olmasına imkân tanımamaktadır. Savcının engelleme kararı başvurusu, menfaatleri etkilenmesi muhtemel taraflara ön bir bildirim yapılmaksızın hazırlanmıştır. İletişim bilgileri web sitesinde

[1285] *Engels v. Rusya*, para. 30.
[1286] *Engels v. Rusya*, para. 30.
[1287] *Engels v. Rusya*, para. 30.
[1288] *Engels v. Rusya*, para. 31.
[1289] *Engels v. Rusya*, para. 31.

açıkça yer almasına rağmen filtresiz tarayıcı teknolojilerinin amacına ilişkin olarak başvurucunun bilgisine başvurulmamıştır. Aynı doğrultuda, İlçe Mahkemesi yargılamalara müdahil olması veya beyanda bulunması için başvurucuya çağrıda bulunmamış ve meseleyi savcı ile yerel internet hizmet sağlayıcısı arasındaki bir mesele olarak ele almıştır.

Peki, yerel İSS'nin sürece davalı olarak katılması yeterli bir koruma sağlar mı? AİHM'ye göre yerel İSS'nin davalı olarak belirlenmiş olması, süreç İSS aleyhine sonuç doğuracak nitelikte olmadığından yeterli değildir. Mahkemeye göre İSS, içeriği hakkında bilgi sahibi olmadığı milyonlarca web sitesine erişim kullanıcılara gerekli teknolojiyi sağlamaktadır. İSS, içerikler hakkında içeriklerin sahipleri kadar detaylı bilgiye sahip değildir ve engellemeye konu her web sitesini savunabilecek hukuki kaynaklardan da mahrumdur. Keza, İSS'nin yargılamaların neticelerine ilişkin hukuki bir menfaati yoktur. Engelleme kararlarının, bağlantı sağlama ticari hizmeti üzerinde bir yansıması yoktur ve bu kararlar kesinleştiği zaman tüm Rus İSS'lerinin aynı engelleme kararını uygulamasını gerektirmektedir. Tüm bu tespiteler ışığında AİHM, başvurucunun yokluğunda gerçekleştirilen yargılamaların ilgili tarafların kendilerini ifade edebilmeleri için gerekli ortamı sağlamadığına karar vermiştir.[1290] Mahkeme ayrıca savcının ve İlçe Mahkemesinin, tedbiri uygulamadan evvel engellemenin etkisine dair bir değerlendirme yapmadığını ve bu kararı ilgili taraflara bir itiraz hakkı tanımadan acilen uygulamanın gerekliliğini ortaya koymadığını belirtmiştir.[1291]

AİHM, mevcut uyuşmazlıkta Rus iç hukukunun itirazlara ilişkin mekanizmalarının da gereğince işletilmediğine işaret etmiştir.[1292] Aynı doğrultuda, Bölge Mahkemesinin mevzubahis olan muhtelif menfaatleri ele almaya yönelik bir girişimde bulunmadığını, incelemesini mevzuatın lafzıyla sınırlı tuttuğunu belirtmiştir.[1293] *Ahmet Yıldırım v. Türkiye* kararına tekrar atıf yapan AİHM'ye göre, AİHS ile uyumlu bir denetimde, özellikle internette bulunan meşru bilgilerin büyük çoğunluğuna erişimi

[1290] *Engels v. Rusya*, para. 32.

[1291] *Engels v. Rusya*, para. 32.

[1292] *Engels v. Rusya*, para. 33.

[1293] *Engels v. Rusya*, para. 33.

engelleyen bir tedbir kararının web sitesi sahiplerinin ve internet kullanıcılarının haklarını esaslı şekilde kısıtladığının ve önemli dolaylı etkiler oluşturabileceğinin dikkate alınması gerekir.

AİHM, bireyleri mevcut davada olduğu gibi toptan engelleme tedbirlerinin aşırı ve keyfî etkilerinden koruyabilecek güvenceler içermeyen yasal düzenlemelerin hukukun üstünlüğü ilkesiyle bağdaşmadığının altına çizmiştir.[1294] Davada uygulanan Rus mevzuatına ilişkin incelemesinin ışığında AİHM; Bilgi Kanunu'nun 15.1. maddesinin (5)(2) kısmında yer alan prosedürün, AİHS bağlamında öngörülebilirlik kriterini yerine getirmediğine ve kötüye kullanıma karşı demokratik bir toplumda hukukun üstünlüğünün emrettiği ölçüde güvence içermediğine hükmetmiştir.[1295] Mahkeme, müdahale "kanunla öngörülme" şartını yerine getirmediği için AİHS'nin 10. maddesinin ikinci fıkrasındaki diğer gereklilikler bağlamında inceleme yapılmasına gerek olmadığına karar vermiştir. Sonuç olarak, AİHS'nin 10. maddesinin ihlal edildiğine hükmetmiştir.[1296]

10. madde ihlaline ilişkin tespitinden sonra Mahkeme, 13. maddenin ihlal edilip edilmediğini ele almıştır. Başvurucu, Rus mahkemelerinin AİHS'nin 13. maddesinde güvence altına alınan etkili başvuru hakkını ihlal ettiğini ileri sürmüştür.[1297] 13. madde şu şekildedir: "*Bu Sözleşme'de tanınmış olan hak ve özgürlükleri ihlal edilen herkes, ihlal fiili resmî görev yapan kimseler tarafından bu sıfatlarına dayanılarak gerçekleştirilmiş olsa dahi ulusal bir makama etkili bir başvuru yapabilme hakkına sahiptir.*" AİHM, açıkça dayanaktan yoksun olmadığına kanaat getirerek bu iddiayı kabul edilebilir görmüştür.[1298]

Rus Hükûmeti, başvurucunun tüm etkili iç hukuk yollarını kendi inisiyatifiyle sonuna kadar tükettiğini ve uygulanabilir hukuk kuralları çerçevesinde taleplerinin mahkemelerce dikkate alındığını iddia etmiş-

[1294] *Engels v. Rusya*, para. 34.
[1295] *Engels v. Rusya*, para. 34.
[1296] *Engels v. Rusya*, para. 35.
[1297] *Engels v. Rusya*, para. 36.
[1298] *Engels v. Rusya*, para. 37.

tir.[1299] Ayrıca, web sitesi fiilen engellenmediğinden başvurucunun herhangi bir hakkının ihlal edilmediğini ileri sürmüştür.[1300]

Başvurucu, yerel hak arama yollarının etkin olmadığını vurgulamıştır.[1301] Başvurucu, içeriği yasaklayan yargılamalara dâhil edilmediğini ve bu yargılamalardan haberdar edilmediğini ileri sürmüştür.[1302] Ayrıca, temyiz mahkemesinin web sitesinin içeriğinin niteliğine veya ilk derece mahkemesinin kararının, haklarını nasıl etkilediğine dair bir değerlendirme yapmadığını belirtmiştir.

Müdahil üçüncü taraflardan Avrupa Bilgi Toplumu Enstitüsü, etkilenen taraflar için hem *ex-ante* hem de *ex-post* hak arama yollarının sunulması gerektiğini belirtmiştir.[1303] *Ex-ante* yollar, engellemeye konu olan web sitelerinin sahiplerine ön bildirim yapılmasını içerir. *Ex-post* yollar ise bir engelleme kararı uygulandıktan sonra kararın kapsamını kısıtlamak veya yeni koşullar dikkate alınarak karara itiraz etmek için etkin mekanizmaların varlığını ifade eder.

AİHM, AİHS'nin 10. maddesi ile 13. maddesindeki menfaatlerin niteliğine ilişkin bir karşılaştırma yapmıştır.[1304] AİHM'ye göre 13. madde usuli bir koruma sağlarken, diğer bir deyişle etkin bir başvuru hakkını gerekli kılarken, 10. maddenin bünyesindeki usuli koruma ifade özgürlüğünün özüne saygıyı temin etme gibi daha geniş bir amacın yan unsuru niteliğindedir.

Mahkemeye göre, başvurucunun, ifade özgürlüğünün kısıtlandığına dair bir iddiası vardır.[1305] Mahkeme, 13. maddenin, iddia edilen ihlalleri veya devamını önleyen veya vuku bulmuş ihlallere ilişkin uygun tazmin imkânları sağlayan, hem hukuken hem de uygulamada etkili bir yerel hak arama mekanizmasını gerektirdiğini hatırlatmıştır.

[1299] *Engels v. Rusya*, para. 38.
[1300] *Engels v. Rusya*, para. 38.
[1301] *Engels v. Rusya*, para. 39.
[1302] *Engels v. Rusya*, para. 39.
[1303] *Engels v. Rusya*, para. 40.
[1304] *Engels v. Rusya*, para. 41.
[1305] *Engels v. Rusya*, para. 42.

AİHM, başvurucuya engelleme kararına itiraz etme ve itiraz yargılamalarına katılma imkânı sağlanmış olsa da temyiz mahkemesinin şikâyetin özüne ilişkin bir değerlendirme yapmadığı görüşündedir.[1306] Keza, temyiz mahkemesinin belirli teknolojilere ilişkin bilginin özel niteliğini ele almadığı veya engelleme tedbirinin gerekliliği ve ölçülülüğünü incelemediği kanaatindedir. Tüm bu tespitler ışığında Mahkeme, ulusal hukukta sağlanan telafi imkânının mevcut davanın koşulları bağlamında etkili olmadığına karar vermiş ve AİHS'nin 10. maddesiyle bağlantılı olarak 13. maddenin de ihlal edildiğine hükmetmiştir.[1307]

Sonuçta AİHM, başvuruyu kabul edilebilir görmüş, AİHS'nin 10. maddesinin ihlal edildiğine karar vermiş; 10. maddenin yanı sıra 13. maddenin de ihlal edildiğine kanaat getirmiş ve başvurucuya tazminat ödenmesine hükmetmiştir.

VIII. Değerlendirme

Engels. v. Rusya kararını diğer kararlardan ayıran en temel özellik, bu kararın erişimin engellenmesi değil içeriğin yayından kaldırılmasına ilişkin olmasıdır. Başvurucu, kararın gereğini yerine getirip içeriği kaldırdıktan sonra hak arama yollarını tüketmiş ve konuyu AİHM'ye taşımıştır. AİHM, *Engels v. Rusya* kararı ile aynı gün vermiş olduğu diğer üç kararda da aslında *Ahmet Yıldırım v. Türkiye* kararındaki ilkeleri tekrar etmiştir. Bu ilkelerin, yerleşik içtihada dönüştüğü aşikârdır.

Bu kararda ilk defa, erişimin engellenmesi tedbirlerini aşmak için kullanılan yöntemlere ilişkin bir değerlendirme yapılmıştır. AİHM, bazı teknolojilerin bir şekilde hukuka aykırı içeriğe erişimi kolaylaştırmak için kullanılmasının engellenmesini, bir yazıcı veya fotokopi makinesinin bu tür bir içeriği basmak için kullanılmasının yasaklanmasına benzetmiştir. Mahkeme; bu tür teknolojilere ait bilgilerin engellenmesinin bu teknolojiler kullanılarak erişilebilecek tüm içeriğe erişimi engellemekle eş değer olduğunu belirlemiş, yerel hukukta bu konuda açık bir yasal düzenleme

[1306] *Engels v. Rusya*, para. 43.

[1307] *Engels v. Rusya*, para. 44.

olmamasını dikkate alarak böylesine geniş bir tedbirin keyfî nitelikte olduğuna hükmetmiştir. Diğer bir deyişle Mahkeme, erişimin engellenmesi tedbiri söz konusu olduğunda varsayımlarla hareket edilmemesi gerektiğini ve somut hukuka aykırılığın gerekliliğini ortaya koymuştur.

AİHM'ye göre, AİHS ile uyumlu bir denetimde, özellikle internette bulunan meşru bilgilerin büyük çoğunluğuna erişimi engelleyen bir tedbir kararının web sitesi sahiplerinin ve internet kullanıcılarının haklarını esaslı şekilde kısıtladığının ve önemli dolaylı etkiler oluşturabileceğinin dikkate alınması gerekir.

Somut olayda, *Ahmet Yıldırım v. Türkiye* veya *Bulgakov v. Rusya* olaylarında olduğu gibi genel bir engelleme uygulanmamıştır. Roskomnadzor'un web sitesinin sahibiyle iletişime geçmesi ve başvurucunun bu kararın gereğini yerine getirmesi neticesinde toptan bir engelleme önlenmiştir.

Engelleme kararının idari bir makam tarafından değil mahkemeler tarafından verilmesi, engelleme tedbirinin ortaya çıkardığı müdahaleye hukuka uygunluk karinesi sağlamamaktadır. Bu konuda idari makamlar yerine mahkemelerin son karar verici olması önemliyse de asıl belirleyici olan unsur kararların niteliğidir. Engelleme tedbirlerinin etkisini ele almayan ve ilgili tarafları dışlayan bir yargılama süreci, mevcut uyuşmazlıkta olduğu gibi AİHS'nin 10 ile 13. maddelerinde güvence altına alınan hakları zedeleyici nitelikte olacaktır.

Engels v. Rusya kararı, bir web sitesinin tamamında değil sitenin sadece bir sayfasındaki spesifik URL adresinde yer alan bir içeriğin hangi durumlarda kaldırılabileceği konusunda yol göstermesi bakımından önemlidir. Kararda, erişimi engelleme tedbirlerinin açık kanuni dayanağa sahip olması gerektiği vurgulanmış ve kanuni dayanağın ne olması, mevzuatın ne kadar detay içermesi gerektiği izah edilmiştir.

Aslında AİHM'nin bu çerçevedeki kararlarında AİHS'ye üye devletlerin, internet ortamını düzenleyen yasaları kaleme alırken nasıl bir çerçeve çizmeleri gerektiğine ilişkin önemli dersler yer almaktadır. Her şeyden evvel, erişimin engellenmesi tedbiri genel değil, özel nitelikte içe-

rikler için söz konusu olmalı; her zaman daha az müdahaleci bir tedbirin varlığı sorgulanmalı; menfaatleri etkilenen kişiler sürece dâhil edilmeli; bu kişilere bildirimde bulunulmayacaksa kararın neden derhâl uygulanması gerektiği somut olarak ortaya koyulmalı; hangi içeriğin engelleneceği (maddi hukuk) ve nasıl engelleneceği (usul hukuku) belirlenmeli; engelleme kararları somut hukuka aykırılığı mutlaka nitelendirmeli ve tanımlamalı; engelleme kararlarına karşı etkili bir itiraz mekanizması var olmalıdır.

AİHM, aslında hukuki belirliliği erişimin engellenmesi özelinde somutlaştırmaktadır. İnternet ortamını düzenleyecek mevzuatın bu bağlamda çerçeve değil, kazuistik olması kaçınılmazdır ve ideal olan da budur. Bu tür mevzuat, konunun teknik ve hukuki boyutuna uygun olarak kaleme alınmalı ve tüm paydaşların, internet ortamındaki davranışlarını önceden düzenleyebilmesini temin etmelidir.

§23. OOO FLAVUS VE DİĞERLERİ V. RUSYA

AİHM'nin 23 Haziran 2020 tarihinde Rusya'ya ilişkin verdiği üçüncü karar, *OOO Flavus ve Diğerleri v. Rusya* kararıdır.[1308] Karar, erişimin engellenmesi tedbirinin AİHS'ye uygunluğuna ilişkindir. Başvurunun konusunu, üç online medya sitesinin bazı sayfalarında hukuka aykırı içerikler bulunduğu iddiasıyla sitelere erişimin tamamen engellenmesi oluşturmaktadır.

I. Davanın gelişimi

AİHM'ye başvuru, OOO Flavus ve OOO Mediafokus isimli iki Rus limitet şirketi ile Rus vatandaşı Bay Garri Kimovich Kasparov tarafından 2015 yılında muhtelif tarihlerde Rusya Federasyonu aleyhine yapılmıştır.

Başvurucular, online medya sitelerinin sahibidir. İlk başvurucu, OOO Flavus, 2000 yılından beri var olan ve 2003 yılında elektronik süreli yayın olarak tescil edilmiş bulunan grani.ru web sitesinin sahibidir. İkinci başvurucu, Bay Kasparov, sosyal ve politik konulara ilişkin bir web yayını olan ve aynı zamanda bağımsız blog sahiplerine altyapı sağlayan www.kasparov.ru web sitesini işletmektedir. Üçüncü başvurucu, OOO Mediafokus, online günlük gazete olan ve ej.ru web sitesinden yayın yapan Ezhednevnyy Zhurnal (*Daily Newspaper*) sitesinin sahibidir. Bu web sitesi, 2004 yılından beri çoğu Rus Hükûmetine muhalif olan siyaset bilimci, ekonomist ve gazetecilerin araştırma ve analizlerini yayımlamaktadır.

Aralık 2013'te, Bilgi Kanunu'nda yapılan değişiklikle Rus Başsavcılığına kamu düzenini bozmaya, aşırılıkçı faaliyetlere veya izinsiz toplu gösterilere katılmaya çağıran web sitelerini tespit etmeye yönelik özel bir yetki tanınmıştır. Herhangi bir mahkeme kararı gerektirmeyen bu uygu-

[1308] **AİHM**, *OOO Flavus ve diğerleri v. Rusya*, Başvuru No: 12468/15, 23489/15, 19074/16, 23.6.2020.

lamada, Başsavcı erişimi engelleme talebini doğrudan telekomünikasyon düzenleyici otoritesi olan Roskomnadzor'a iletmekte ve bu kanalla web sitesinin yer sağlayıcısına bildirim yapılmaktadır. Yer sağlayıcının web sayfasına erişimi derhâl engelleme ve web sayfasının sahibine yirmi dört saat içinde bildirim yapma yükümlülüğü vardır.[1309]

Başsavcı, 13 Mart 2014 tarihinde Roskomnadzor'a bir talep göndererek başvuruculların online medya sitelerine erişimin engellenmesini talep etmiştir.[1310] Başsavcı talebinde, söz konusu web sitelerinin Rusya'da hukuka aykırı olarak nitelendirilen toplumsal olaylara yer verdiğini, özellikle ej.ru web sitesinin Moskova'daki Bolotnaya Meydanı'nda gerçekleşen kitlesel olaylara ve yasa dışı gösterilere ilişkin bilgiler içerdiğini ve kişileri bu tür eylemlere katılmaya davet ettiğini; grani.ru web sitesinin izinsiz yürüyüşte tutuklananlar lehine yayınlar yaptığını ve benzer eylemlere katılım çağrısı içerdiğini; kasparov.ru web sitesinin ise Kırım'a ilişkin haberler yayımlayıp Kırım sakinlerini hukuka aykırı eylemlerde bulunmaya çağırdığını ifade etmiştir.[1311]

Başsavcının talebi üzerine 14 Mart 2014 tarihinde Roskomnadzor, başvuruculların web sitelerine erişimi engellemiş ve yer sağlayıcıdan "aşırılıkçı faaliyetlere çağrı" ihtiva ettiği gerekçesiyle hukuka aykırı içeriği kaldırmasını talep etmiştir.[1312] Talepte, sayfa URL alanında, hedeflenen web sitesinin alan adı belirtilmiş ve savcının kararı yer almamıştır.

Başvurucular, engelleme tedbirine karşı yargısal itiraz sürecini başlatmıştır.[1313] Başvurucular, web sitelerine erişimin herhangi bir ayrım yapılmaksızın toplu olarak engellenmesinin ve spesifik olarak hukuka aykırı materyale ilişkin bildirimde bulunulmamasının mevcut usullere aykırı olduğunu; bu yöntemin, başvuruculları hukuka aykırı materyali kaldırarak web sitelerine erişimin tekrar açılmasını sağlamaktan alıkoyduğunu

[1309] *OOO Flavus ve Diğerleri v. Rusya*, para. 5.
[1310] *OOO Flavus ve Diğerleri v. Rusya*, para. 6.
[1311] *OOO Flavus ve Diğerleri v. Rusya*, para. 6.
[1312] *OOO Flavus ve Diğerleri v. Rusya*, para. 7.
[1313] *OOO Flavus ve Diğerleri v. Rusya*, para. 8.

iddia etmiştir.[1314] Ayrıca, ayrım gözetmeyen engelleme tedbirinin, hukuka aykırı olarak nitelendirilmemiş bilgiyi yayma haklarını esaslı ölçüde kısıtladığını ileri sürmüşlerdir.

6 Mayıs ve 20 Ağustos 2014 tarihlerinde Taganskiy Bölge Mahkemesi ve 6 Ağustos 2014 tarihinde Moskova'daki Khamovnicheskiy Bölge Mahkemesi, başvurucuların taleplerini reddetmiştir.[1315] Mahkemeler, web sitelerinin yetkili bir makam olan Başsavcılık tarafından değerlendirilip hukuka aykırı olduklarının tespit edildiğini; Roskomnadzor'un Başsavcının engelleme talebini yerine getirdiğini ve bu engellemeyi yaparken hukuka aykırı web sayfalarına ilişkin yeterli bilgiyi verdiğini; tüm bu gerekçelerle engelleme tedbirinin başvurucuların hak veya özgürlükleri üzerinde etkisinin olmadığını belirtmiştir. Bu kararlara yapılan itiraz da 2 Eylül, 28 Ekim 2014 ve 25 Nisan 2015 tarihlerinde Moskova Şehir Mahkemesi tarafından reddedilmiş, ilk derece mahkemelerinin kararlarının doğru olduğu belirtilmiştir.[1316]

Bay Kasporov'un web sitesi, hukuka aykırı olduğu iddia edilen resmi nötr bir görselle değiştirmiş ve Roskomnadzor'dan web sitesine erişimi açmasını tekrar talep etmiştir.[1317] Bu talebe bir yanıt verilmemiştir.

II. Hukuki arka plan

Konunun esasına girmeden evvel AİHM, Rus iç hukukunun konuyla ilgili düzenlemelerini ve muhtelif insan hakları belgesini alıntılamıştır. Mahkemenin alıntıladığı ilk düzenleme, Rus Bilgi Kanunu'nun (Kanun no. 149-FZ, 27 Temmuz 2006) 15.3. maddesi olmuştur. Söz konusu hükümde, hukuka aykırı içeriğe erişimi engellemeye ilişkin bir usul getirilmiştir.

AİHM, Bilgi Teknolojileri ve Bilginin Korunması Kanunu'nun 15(3) maddesine atıf yapmıştır. Söz konusu düzenleme şöyledir:

[1314] *OOO Flavus ve Diğerleri v. Rusya*, para. 8.

[1315] *OOO Flavus ve Diğerleri v. Rusya*, para. 9.

[1316] *OOO Flavus ve Diğerleri v. Rusya*, para. 10.

[1317] *OOO Flavus ve Diğerleri v. Rusya*, para. 11.

"İnternet dâhil telekomünikasyon ağlarında kitlesel düzensizliğe, aşırılıkçı faaliyetlere veya mevcut usullere aykırı bir şekilde kitlesel (kamusal) etkinliklere katılmaya çağıran bir bilgi tespit edilirse -federal Devlet makamları, bölgesel Devlet otoriteleri, belediyeler, teşkilatlar veya vatandaşlar tarafından tespit dâhil- Rusya Federasyonu Başsavcısı veya vekilleri bilgiyi yayan bilgi ortamına erişimin engellemesine yönelik tedbirlerin alınması için kitlesel medya, kitlesel haberleşme ve bilgi teknolojileri konusunda yetkili kolluk kuvvetine (Roskomnadzor'a) talimat verir.

Roskomnadzor; kitlesel düzensizliğe, aşırılık yanlısı faaliyetlere veya mevcut usullere aykırı bir şekilde kitlesel (kamusal) etkinliklere katılmaya çağıran bilgi içeren web sitesine veya web sitesinde yer alan bilgi ortamına erişimin kısıtlanmasına yönelik tedbirleri alması için hizmet sağlayıcıya talimat verir. Talimat web sitesinin alan adını, ağ adresini ve bilginin tespit edilmesini sağlayacak web sayfasının yeknesak kaynak belirleyici (URL) adresini içermelidir.

Yer sağlayıcı, bildirimi almasından itibaren yirmi dört saat içerisinde, bilgi kaynağının sahibine bildirimle ilgili ve kitlesel düzensizliğe, aşırılık yanlısı faaliyetlere veya mevcut usullere aykırı bir şekilde kitlesel (kamusal) etkinliklere katılmaya çağıran bilgiyi gecikmeksizin silmesinin gerekli olduğuna dair bilgi vermelidir. Bildirimi aldıktan ve doğruluğunu teyit ettikten sonra, Roskomnadzor, internet telekomünikasyon ağına erişim izni veren haberleşme hizmet sağlayıcısına web sitesi gibi bilgi ortamına erişimi tekrar açabileceğine dair derhâl bir bildirim göndermelidir."

AİHM, Avrupa Konseyinin 28 Mayıs 2003 tarihli İnternette İletişim Özgürlüğüne İlişkin Deklarasyon'unu zikrederek Deklarasyon'un internet ortamındaki içeriğe devletlerin ön kontrol uygulamaması gerektiğine ilişkin maddesini alıntılamıştır.[1318] Aynı şekilde, Birleşmiş Milletler (BM) düşünce ve ifade özgürlüğü hakkının korunması ve desteklenmesine ilişkin Özel Raportörü'nün aşırı engelleme tedbirlerine değinen 16 Mayıs 2011 tarihli Rapor'una (A/HRC/17/27), Birleşmiş Milletler Fikir ve İfade Özgürlüğü Özel Raportörü, Avrupa Güvenlik ve İşbirliği Teşkilatı Medya Özgürlüğü Temsilcisi, Amerikan Devletleri İfade Özgürlüğü Özel

[1318] İnternette İletişim Özgürlüğüne İlişkin Deklarasyon için bkz. **§6(IV)**.

Raportörü, Afrika İnsan ve Halkların Hakları Komisyonu İfade Özgürlüğü ve Bilgiye Erişim Özel Raportörü'nün 1 Haziran 2011 tarihli Ortak Deklarasyonu'na, Birleşmiş Milletler İnsan Hakları Komitesinin 11-29 Temmuz 2011 tarihleri arasında gerçekleşen 102. oturumunda Medeni ve Siyasi Haklara İlişkin Uluslararası Sözleşme'nin 19. maddesiyle ilgili kabul ettiği edilen ve internet içeriğinin kısıtlanmasında dikkat edilecek hususlara yönelik tavsiyeler içeren 34 sayılı Genel Yorum'una atıf yapmıştır. Ayrıca Avrupa Konseyinin 13 Nisan 2016 tarihli İnternet Özgürlüğüne İlişkin Tavsiye Kararı'ndan alıntılar yapmıştır.[1319] Söz konusu Tavsiye Kararı'nın ilgili kısımlarını tekrar etmek gerekirse:

2.2.1. Devlet makamları veya özel sektör aktörleri tarafından bir internet platformunu (sosyal medya, sosyal ağlar, bloglar veya başka diğer web siteleri) veya bilgi ve haberleşme teknolojileri (BT) araçlarını (anlık mesajlaşma ve diğer uygulamalar) engelleyen veya bunlara erişimi başkaca şekilde kısıtlayan her türlü tedbir veya devlet makamlarının bu tür eylemlere yönelik talepleri, kısıtlamaların kanunla öngörülme, meşruluk ve ölçülülük koşullarına uygun olmasını öngören AİHS'nin 10. maddesiyle uyumlu olmalıdır.

2.2.2. Devlet makamları veya özel sektör tarafından alınan internet içeriğini engelleme, filtreleme veya kaldırmaya yönelik her türlü tedbir veya bu tür bir işlem için devlet makamları tarafından gerçekleştirilen her türlü talep, kısıtlamaların kanunla öngörülme, meşruluk ve ölçülülük koşullarına uygun olmasını öngören AİHS'nin 10. maddesiyle uyumlu olmalıdır.

2.2.3. İnternet hizmet sağlayıcıları, genel bir ilke olarak, internet trafiğine eşit ve gönderen, alıcı, içerik, uygulama, hizmet veya cihaz temelli ayrımcılık yapmayacak şekilde muamele eder. İnternet trafik yönetim tedbirleri, AİHS'nin 10. maddesine uygun şekilde üstün kamusal yarara ulaşmak için şeffaf, gerekli ve ölçülü olmalıdır.

2.2.4. İnternet kullanıcılarının veya ilgili diğer tarafların, internete erişim, içerik veya bilgiyi alma ve yayma imkânlarını sınırlamaya yönelik işlemlere karşı AİHS'nin 6. maddesine uygun şekilde mahkemelere erişim hakkı vardır.

[1319] İnternet Özgürlüğüne İlişkin Tavsiye Kararı için bkz. **§6(XXIV)**.

2.2.5. Devlet, bilgi alma ve yayma özgürlüğüne uyguladığı engellenen veya içerdiği bilgiler kaldırılan web sitelerini göstermek gibi kısıtlamalar hakkında bunların hukuki dayanağı, gerekliliği ve gerekçesi, bu işleme izin veren mahkeme kararı ve bu karara itiraz hakkını içerecek şekilde kamuoyunu zamanında ve uygun şekilde bilgilendirmelidir.

Yukarıda belirtilen Tavsiye Kararı'na Rusya Federasyonu tarafından özel çekince koyulduğunu belirtmek gerekir.

III. Tarafların iddiaları

AİHM, yapılan başvuruların aynı konuya ilişkin olması sebebiyle bunların tek dosyada birleştirilmesine karar vermiştir. Ayrıca, söz konusu şikâyetin AİHS'nin 35. maddesinin üçüncü fıkrası anlamında açıkça dayanaktan yoksun olmadığını tespit etmiş ve başka hiçbir kabul edilemezlik engeli bulunmayan işbu şikâyetin kabul edilebilir olduğuna karar vermiştir.[1320]

IV. Rus Hükûmetinin savunması

Rus Hükûmeti, kamusal düzeni bozmaya yönelik çağrıların, aşırılıkçı faaliyetlerin ve izinsiz toplanmaların hukuka aykırı içerik niteliğinde olduğunu ve bunların internette yayılmasının yasaklanması gerektiğini belirtmiştir.[1321] Rus Hükûmetine göre, Rus mahkemeleri başvurucuların web sitelerinin bu tür çağrılar içeren materyaller ihtiva ettiğini tespit etmiş ve Başsavcılığın içeriğin engellenmesi kararını onamıştır. Rus Hükûmeti, Roskomnadzor'dan bildirim gelmesi üzerine başvurucuların web sitelerinin sahipleri olarak hukuka aykırı içeriği kaldırmakla yükümlü olmalarına rağmen bunu yerine getirmediklerini ileri sürmüştür.

Kasparov.ru web sitesine sahip ikinci başvurucu, hukuka aykırı içeriği kaldırdığı hususunda Roskomnadzor'u bilgilendirmiştir. Rus Hükûmeti, doğrulama üzerine, hukuka aykırı olduğu tespit edilen içeri-

[1320] *OOO Flavus ve Diğerleri v. Rusya*, para. 20.

[1321] *OOO Flavus ve Diğerleri v. Rusya*, para. 21.

ğin kaldırılmadığının görüldüğünü ileri sürmüştür. Bu doğrultuda Rus Hükûmeti, başvurucuların web sitelerine erişimin engellenmesinin gerekli ve ölçülü olduğunu beyan etmiştir.

V. Başvurucuların iddiaları

Başvurucular, kendilerine ait online medya sitelerinin öncelikle Rusya'daki kitleyi hedeflediğini ve web sitelerine Rusya'dan erişimin engellenmiş olmasının medya faaliyetleri üzerinde *de facto* bir yasaklamaya yol açtığını ileri sürmüştür.[1322] Başvurucular, grani.ru web sitesi için verilen basın tescil sertifikasının iptal edilmemiş olduğunun altını çizmişlerdir.

Başvurucular, Rus makamların taleplerinin öngörülemez ve tutarsız olduğunu iddia etmiştir.[1323] Başvuruculara göre, izinsiz gösterilere katılım çağrısı içerdiği iddiasıyla Başsavcılık web sitelerinin tamamının engellenmesini talep etmiştir. Fakat Başsavcılığın talebi kendilerine iletilmediği gibi Roskomnadzor'un bildiriminde de hangi içeriğin sorunlu olduğu belirtilmemiştir.[1324] Belirtilmediği için de o içeriği tespit edip kaldıramamışlar ve engellemeden kaçınamamışlardır. Başvurucular, kamu otoritelerinin çelişkili ve sürekli değişen talepleri sebebiyle, web sitesi sahipleri olarak bir içeriği yayımlamanın bir engelleme tedbirine yol açıp açmayacağını veya kamu otoritelerinin, web sitesinin tamamını mı ilgili makaleyi mi engelleyeceğini öngöremediklerini ileri sürmüşlerdir.

Başvurucuların ikinci iddiası, Rus hukukunun, online medya sitesi sahiplerini keyfî müdahalelerden koruyacak usuli güvenceler içermediğidir.[1325] Engelleme kararı bir hâkim veya başka bağımsız bir karar alma organı tarafından denetlenmemiştir. Başsavcılık ofisinin görevlileri kararı herhangi bir medya uzmanının görüşüne başvurmadan almıştır. İlgili yasa, söz konusu tedbir uygulanmadan önce bir yargısal denetim veya gereklilik ve ölçülülük değerlendirmesi öngörmemektedir. Tüm bunlar,

[1322] *OOO Flavus ve Diğerleri v. Rusya*, para. 22.

[1323] *OOO Flavus ve Diğerleri v. Rusya*, para. 22.

[1324] *OOO Flavus ve Diğerleri v. Rusya*, para. 22.

[1325] *OOO Flavus ve Diğerleri v. Rusya*, para. 23.

engelleme konularında Başsavcıyı demokratik bir toplumda hukukun üstünlüğü ilkesine aykırı şekilde sınırsız bir takdir yetkisiyle donatmaktadır.

Başvurucular, Rus makamlarının web sitelerini engellemesinin asıl amacının, önemli sosyal ve politik olaylara ve muhalefet ile sivil toplum faaliyetlerine ilişkin tarafsız görüşlerin yayılmasını önlemek olduğu görüşündedir.[1326] Rus makamlarının kamusal düzeni korumak gibi meşru bir amaç güttükleri varsayılsa bile başvurucuların bilgiyi yayma hakkı ile kamu düzeninin sağlanması ihtiyacı arasında denge kurmaya yönelik herhangi bir girişim söz konusu olmamıştır. Başvurucular, birkaç makaleyi veya kasparov.ru sitesi özelinde bir resmi engellemek için tüm web sitesine erişimin engellenmesinin ölçüsüz olduğunu tekrarlamışlardır. Ayrıca, bu durumun, Rusya'nın gidişatı hakkındaki kamusal tartışmalarda online medyayı kullanarak eleştirel görüşlerini dillendiren gazeteciler ve sivil aktivistler üzerinde esaslı bir caydırıcı etki doğurduğunu belirtmişlerdir.

VI. Müdahil tarafların görüşleri

Davaya farklı taraflar ve sivil toplum örgütleri müdahil olmuş, görüşlerini paylaşmıştır. Bunlardan ilki, Birleşmiş Milletler Fikir ve İfade Özgürlüğü Özel Raportörü'dür.[1327] Raportör, bireylerin çevrim içi ortamda tıpkı çevrim dışı ortamda olduğu gibi ifade özgürlüğünden faydalanmasına izin verilmesi gerektiğini vurgulamıştır. Web sitelerinin tamamen engellenmesi konusuna da değinen Raportör; bu tür engellemelerin, ifade özgürlüğünün izin verilen sınırlarına ilişkin kriterleri sağlaması, içeriğe özgü olması ve web sitelerinin salt hükûmeti veya siyasal sistemi eleştiriyor diye hedef alınmaması durumunda istisnai olarak uygulanabileceği görüşündedir. Davaya müdahil olarak görüş veren bir diğer taraf ise Article 19, EFF, Access Now ve Reporters without Borders isimli sivil toplum örgütleridir.[1328]

[1326] *OOO Flavus ve Diğerleri v. Rusya*, para. 24.

[1327] *OOO Flavus ve Diğerleri v. Rusya*, para. 25.

[1328] *OOO Flavus ve Diğerleri v. Rusya*, para. 26.

Söz konusu kuruluşlara göre, bir web sitesinin tamamına erişimi engelleme, hukuka uygun-hukuka aykırı içerik arasında ayrım yapma imkânı tanımadığı ve bu sebeple hukuken asla gerekli olamayacağı için aşırı ve ölçüsüz bir tedbirdir. Şayet erişimi engelleme tedbirine izin veriliyorsa kanun şu minimum standartları sağlamalıdır: (i) Bir mahkeme veya bağımsız bir yargısal organ tarafından engellemeye karar verilmelidir; (ii) ilgili taraflara engelleme kararının arandığı yargılamalara müdahale hakkı tanınmalıdır; (iii) engelleme kararlarının tüm mağdurlarına engelleme kararlarına itiraz hakkı tanınmalıdır; (iv) engellenen web sitelerine erişmeye çalışan herkes, engelleme kararının hukuki dayanağı ve gerekçeleri ile bu karara itiraz yollarına ilişkin bilgiyi görebilmelidir.

Son müdahil, Avrupa Bilgi Toplumu Enstitüsü isimli sivil toplum örgütüdür.[1329] Söz konusu kuruluş, hedefini aşan ve meşru içeriği aşırı şekilde engelleyen bir tedbirin demokratik toplumda kabul edilebilir olmadığını belirtmiş ve yetkili makamların aynı sonuca daha az müdahaleci bir tedbirle ulaşılıp ulaşılamayacağına dair bireyselleştirilmiş bir değerlendirme yapması gerektiğini vurgulamıştır. Bu doğrultuda, hedef alınan web sitesinin bilgilendirilmesi gerektiğini, hukuka aykırı içeriği kaldırması ve bu karara ilişkin beyanlarda bulunması için kendisine makul bir süre verilmesi lazım geldiğini beyan etmiştir.

VII. AİHM'nin tespit ve değerlendirmeleri

Konunun esasına giren AİHM öncelikle *Ahmet Yıldırım v. Türkiye* kararındaki internetin niteliğine ilişkin tespitlerine atıf yapmıştır.[1330] Tekrar etmek gerekirse, AİHM söz konusu kararında erişilebilirliğin yanı sıra büyük miktarda veriyi muhafaza etme ve dağıtma imkânları sayesinde internet sitelerinin kamunun güncele erişiminin iyileştirilmesine ve bilginin iletilmesinin kolaylaştırılmasına önemli derecede katkıda bulunduğunu; internetin politik veya kamu menfaatine ilişkin tartışma ve eylemlere katılım konusunda asli vasıtaları barındırdığını ve AİHS'nin

[1329] *OOO Flavus ve Diğerleri v. Rusya*, para. 27.

[1330] *OOO Flavus ve Diğerleri v. Rusya*, para. 28.

10. maddesinin yalnızca bilgilerin iletilmesi hakkını değil, aynı zamanda toplumun bilgi alma hakkını da güvence altına aldığını belirtmiştir.

Başvurucular, çoğunluğu Rus Hükûmetine muhalif olan siyasiler, gazeteciler ve uzmanların görüşlerini ve araştırmalarını yayımlayan online medya sitelerinin sahipleridir.[1331] AİHM, Başsavcının bazı içerikleri hukuka aykırı olarak nitelendirmesi üzerine Roskomnadzor'un 14 Mart 2014 tarihinde başvurucuların web sitelerini engellediğinin altını çizmiştir. Bu tespitten sonra Mahkeme, *Ahmet Yıldırım v. Türkiye* kararına tekrar atıf yaparak, yasal temeli ne olursa olsun, böyle bir tedbirin internete erişimi etkileme potansiyeli olduğundan davalı devletin 10. madde kapsamında sorumluluğunu doğuracağını ifade etmiştir. AİHS'nin 10. maddesinin yalnızca bilgilerin iletilmesi hakkını değil, aynı zamanda toplum açısından bilgi alma hakkını da güvence altına aldığını hatırlatmıştır.[1332] AİHM'ye göre, bir müdahale kanunla öngörülme, AİHS'nin 10. maddesinin ikinci fıkrasında belirtilen meşru amaçlardan bir veya birden fazlasını gütme ve bu amaçlara ulaşmak için demokratik bir toplumda gerekli olma şartlarını taşımadıkça 10. maddeyi ihlal etmiş olacaktır.

Mevcut uyuşmazlığa değinen AİHM, meşru amacın varlığının müdahalenin demokratik bir toplumda gerekli olup olmadığına ilişkin tespitten bağımsız ele alınamayacağını belirtmiştir. Bu sebeple, bu kriterleri beraber değerlendirmiştir.

AİHM'nin müdahaleyi ilk değerlendirdiği kriter "kanunla öngörülme" olmuştur. AİHM'ye göre "*kanunla öngörülen*" ifadesi öncelikle tedbirin iç hukukta bir dayanağı olmasını gerektirir. Ayrıca söz konusu yasanın, kendisi açısından ortaya çıkabilecek sonuçları ve hukukun üstünlüğü ilkesiyle uyumunu önceden değerlendirebilmesi için ilgili kişi açısından erişilebilir olması gerektiğini ifade eder.[1333] Yasanın yürütme organına temel haklara ilişkin konularda sınırsız bir takdir yetkisi vermesi hâlinde AİHS'nin benimsediği demokratik bir toplumu oluşturan ana ilkelerden hukukun üstünlüğü ilkesine aykırılık söz konusu olacaktır. Bu

[1331] *OOO Flavus ve Diğerleri v. Rusya*, para. 28.

[1332] *OOO Flavus ve Diğerleri v. Rusya*, para. 29.

[1333] *OOO Flavus ve Diğerleri v. Rusya*, para. 30.

sebeple yasa, bu gücün kullanılmasının yöntemini ve kapsamını yeterli netlikte düzenlemelidir.

Hatırlanacağı üzere başvuruculaların online medya sitelerine erişim, Bilgi Kanunu'nun 15.3. maddesine göre engellenmiştir.[1334] Bu hüküm, Başsavcının veya vekillerinin, kamusal kargaşaya veya kanuna aykırı kamusal etkinliklere katılıma davet dâhil üç farklı kategorideki içeriğe erişimi engelleme konusunda yetkili olduğunu belirtmektedir. AİHM, kanunilik kriterini incelerken yetkisinin ilgili kamu makamlarının iç hukukun yalnızca lafzına uyduğunu denetlemekten ibaret olmadığını belirtmiştir. Mahkemeye göre asıl incelenmesi gereken, mevzubahis yasanın kalitesinin başvuruculaların kendi davranışlarını düzenleyebilmesine ve keyfî müdahalelere karşı korunmalarına imkân verip vermediği olduğunu vurgulamıştır.[1335]

Mevcut uyuşmazlıkta, Başsavcılığın erişimi engelleme talebi, Roskomnadzor tarafından web sayfasının URL adresi olarak değil web sitesinin tam alan adı belirtilerek uygulanmıştır.[1336] Mahkemeye göre bu uygulama hem kaldırılacak içeriğin tespit edilmesine imkân vermemiş hem de başvuruculaların ilgili içeriği kaldırarak bir hukuki çare bulması imkânını ortadan kaldırmıştır.[1337] Bu bağlamda AİHM, Rus makamlarının sorunlu görülen web sayfalarının URL adreslerini belirlemeyerek keyfî davrandığını ve bu nedenle başvuruculaların sorunlu içeriği kaldırmak veya değiştirmek arasında bilinçli bir tercih yapma ve belirli web sayfalarına referansla Başsavcının kararına itiraz etme olanağından mahrum kaldığını belirtmiştir.

AİHM, ej.ru ile grani.ru web sitelerinin, Blotnaya davasının sanıklarına destek veren protestoları ve kamusal etkinlikleri onaylayan yazılar sebebiyle sorumlu tutulduğunu ve Başsavcılık kararıyla engellendiğini belirtmiştir.[1338] AİHM, Bilgi Kanunu'nun 15.3. maddesinde yer alan

[1334] *OOO Flavus ve Diğerleri v. Rusya*, para. 31.
[1335] *OOO Flavus ve Diğerleri v. Rusya*, para. 31.
[1336] *OOO Flavus ve Diğerleri v. Rusya*, para. 32.
[1337] *OOO Flavus ve Diğerleri v. Rusya*, para. 32.
[1338] *OOO Flavus ve Diğerleri v. Rusya*, para. 33.

"*kanuna aykırı şekilde gerçekleştirilen kamusal etkinlikler*" kavramının aşırı geniş olduğunu daha önce tespit ettiğini hatırlatmıştır.[1339] Bu hüküm, küçük veya zararsız olduğuna bakmaksızın ve kamusal düzene veya başkalarının haklarına herhangi bir tehdit oluşturup oluşturmadığına ilişkin bir değerlendirme yapmaksızın Başsavcıya erişimi engelleme konusunda yetki vermektedir. Nitekim Başsavcı bu yetkiyi bu tür bir çağrı içermeyen içerikleri de hedef almak için kullanmıştır. AİHM'ye göre her iki durum bu davada mevcuttur.[1340]

AİHM, 2012 yılında gerçekleştirilen Bolotnaya Meydanı protestolarını tekrar ele alarak, bu protestolarda meydana gelen olaylarla ilgili yürümekte olan davalar hakkında bilgi edinmenin Rusya'da yoğun bir kamusal menfaat konusu olduğunu, başvuruculların medya siteleri olan ej.ru ile grani.ru sitelerinin bu konudaki gelişmeleri ve polisler tarafından yapılan gözaltıları konu aldığını ve tüm bunların kamuyu bilgilendirmeye yönelik gazetecilik faaliyeti niteliğinde olduğunu tespit etmiştir.[1341] Mahkemeye göre, Başsavcının engelleme talebi, izin verilmiş veya kanuna aykırı protestolara katılım şeklinde bir ayrım gözetmemiştir. Kaldı ki Mahkemeye göre, Bolotnaya olaylarından yargılanan kişilere destek olmak ve sanıklarla dayanışma sergilemek izin verilmeyen bir kamusal etkinliğe katılım olarak nitelendirilemez.[1342] Tüm bu tartışmaların ışığında AİHM, kamusal menfaatleri ilgilendiren konulardaki ifadelerin güçlü bir koruma gerektirdiğini hatırlatarak Başsavcının yorumunun bir temeli olmadığına, keyfî olduğuna ve açıkça makul olmadığına kanaat getirmiştir.[1343]

AİHM, kasparov.ru web sitesine yönelik erişimi engelleme kararını da ele almıştır. Hatırlanacağı üzere, söz konusu sitede yer alan içerikte Kırımlıların sessiz kalmamaları ve teslim olmamalarına yönelik ifadeler yer almaktadır. AİHM'ye göre Başsavcının bu siteye yönelik kararı, iddia edilen hukuka aykırı eylemlere ilişkin veya içeriğin hangi bileşenlerinin hukuka aykırılığa yol açtığına dair bir değerlendirme içermemektedir.

[1339] *OOO Flavus ve Diğerleri v. Rusya*, para. 33.
[1340] *OOO Flavus ve Diğerleri v. Rusya*, para. 33.
[1341] *OOO Flavus ve Diğerleri v. Rusya*, para. 34.
[1342] *OOO Flavus ve Diğerleri v. Rusya*, para. 34.
[1343] *OOO Flavus ve Diğerleri v. Rusya*, para. 34.

Yine karar, bir Rus savcısının Rus olmayan ve Rusya'nın yargı yetkisi dışında kalan kişiler tarafından gerçekleştirilen eylemlerin hukuka aykırılığına karar vermeye ilişkin yetkisine dair bir bilgi içermemektedir.[1344] Mahkemeye göre "hukuka aykırı eylemler" kavramı, Bilgi Kanunu'nun 15.3. maddesindeki yasaklı içerikler kategorilerinden hiçbirinin altına girmemektedir. Bu bağlamda AİHM, Başsavcının kasparov.ru web sitesinin içeriğine ilişkin kararının hukuki dayanaktan yoksun olduğuna karar vermiştir.[1345]

Kanunla öngörülme şartını değerlendirdikten sonra AİHM, müdahaleyi meşru amaç ve demokratik toplumda gereklilik kriterlerine göre ele almıştır.[1346] AİHM, bir web sitesinin tamamının engellenmesinin bir gazetenin veya televizyon istasyonunun engellenmesiyle kıyaslanacak aşırı bir tedbir olduğunu vurgulamıştır. Zira, bu tür bir tedbir, Mahkemeye göre hukuka uygun-hukuka aykırı bilgi arasında bir ayrım yapmamakta ve hukuka aykırı kabul edilmeyen birçok içeriği de erişilmez kılmaktadır. *Ahmet Yıldırım v. Türkiye* kararını tekrar hatırlatan AİHM, bir web sitesinin tamamına erişimin engellenmesinin, hedef alınan hukuka aykırı içeriği engellemeyi aşan bir tedbir olduğunu belirtmiştir.[1347]

AİHM, hukuka aykırı nitelikte görülen web sitesi içeriklerine yönelik kararların temelsiz veya bütünüyle keyfî alındığı görüşündedir.[1348] Mahkemeye göre, istisnai durumlarda hukuka aykırı içeriği engellemek mümkünse de bir web sitesinin tamamına erişimi engelleme, hukuka aykırı içeriğe yönelen ilk kararın gerekçesinden ayrı olarak ve AİHS'nin 10. maddesi bağlamında geliştirilen ve uygulanan kritere göre gerekçelendirilmelidir. AİHM, sınırlı bir engelleme talebinin tüm web sitesine uygulanacak şekilde genişletilmesi suretiyle meşru içeriğin otomatik olarak engellenemeyeceğinin altını çizmiştir.[1349] Ayrıca, hukuka aykırı içerik veya web sitelerine yönelen bir tedbirin yan etkisi olarak hukuka uygun

[1344] *OOO Flavus ve Diğerleri v. Rusya*, para. 35.
[1345] *OOO Flavus ve Diğerleri v. Rusya*, para. 35.
[1346] *OOO Flavus ve Diğerleri v. Rusya*, para. 37.
[1347] *OOO Flavus ve Diğerleri v. Rusya*, para. 37.
[1348] *OOO Flavus ve Diğerleri v. Rusya*, para. 38.
[1349] *OOO Flavus ve Diğerleri v. Rusya*, para. 38.

içeriğe müdahale eden, ayrım gözetmeyen engelleme tedbiri bu tür web sitelerinin sahiplerinin haklarına keyfî müdahale oluşturacaktır.

AİHM'ye göre Rus Hükûmeti tüm web sitesinin engellenmesi için herhangi bir gerekçe ortaya koyamamıştır.[1350] Rus otoriteleri, başvuruculların online medya web sitelerine erişimi engelleyerek hangi meşru amacı güttüklerini veya baskın sosyal ihtiyacı yerine getirdiklerini açıklayamamışlardır. Nihayetinde, başvuruculların temel iddiasına göre, Rus makamlarının gerçek amacı muhalif medya sitelerine erişimi kısıtlamaktır.

AİHM, BM İnsan Hakları Komitesi ve Özel Raportörü'nün online medya veya web sitelerini sadece hükûmete veya politik sisteme muhalif olmaları sebebiyle erişimi engelleme tedbirine tabi tutmanın hiçbir zaman ifade özgürlüğüne gerekli bir müdahale olarak nitelendirilemeyeceğine ilişkin görüşünü hatırlatmıştır.[1351] Tüm bu tartışmaların neticesinde AİHM, başvuruculların web sitelerini hedefleyen toplu engelleme kararlarının, herhangi bir gerekçesinin olmaması sebebiyle meşru bir amaç gütmediğine kanaat getirmiştir.[1352]

AİHM'nin incelediği son husus ise tedbirlerin aşırı ve keyfî şekilde kötüye kullanılmasını önleyecek koruma mekanizmalarının varlığı meselesidir.[1353] AİHM, özellikle yayınlara ön kısıtlamanın ancak istisnai bir durumda getirileceğinin altını çizerek, nihayetinde haberin anlamını çabuk yitirebilir bir emtia olduğunu ve çok kısa bir gecikmenin bile değerini ve ona yönelik ilgiyi ortadan kaldırabileceğini belirtmiştir.[1354] Mevcut başvurudaki gibi medya sitelerinin faaliyetlerine ön kısıtlama getirilmesi durumunda, engellemenin kapsamına ilişkin sıkı bir kontrol ve etkili bir AİHS uyumlu yargısal denetim var olmalıdır.[1355]

AİHM, Rus hukukunun, Bilgi Kanunu'nun 15.3. maddesinde yer alan müdahalelerin keyfîliğine karşı başvurucular gibi online medya sa-

[1350] *OOO Flavus ve Diğerleri v. Rusya*, para. 38.
[1351] *OOO Flavus ve Diğerleri v. Rusya*, para. 38.
[1352] *OOO Flavus ve Diğerleri v. Rusya*, para. 38.
[1353] *OOO Flavus ve Diğerleri v. Rusya*, para. 39.
[1354] *OOO Flavus ve Diğerleri v. Rusya*, para. 39.
[1355] *OOO Flavus ve Diğerleri v. Rusya*, para. 39.

hiplerini koruyacak usuli güvenceleri içermediğine kanaat getirmiştir.[1356] Mahkemenin bu tespitinin gerekçesi şunlardır:

(i) Düzenleme, web sitesi sahiplerinin engellemeye ilişkin süreçlere bir şekilde dâhil olmasını gerektirecek bir düzenleme içermemektedir.

(ii) Hem Başsavcının orijinal kararı hem de Roskomnadzor'un uygulama kararı, hakları ve menfaatleri etkilenmesi muhtemel taraflara bir ön bildirim yapılmaksızın alınmıştır.

(iii) Bilgi Kanunu, yetkili makamların engelleme tedbirlerine ilişkin bu tür tedbirler uygulanmadan önce etki değerlendirmesi yapmasını veya bu tür tedbirlerin ilgili taraflara hukuka aykırı içeriği kaldırmak veya yargısal denetimi gerçekleştirmek için imkân tanımadan neden derhâl uygulandığına dair bir gerekçe belirtmelerini zorunlu tutmamaktadır.

(iv) Engelleme tedbirleri, ilgili tarafların dinlenmesine imkân tanıyacak bir mahkeme veya başka bir bağımsız organ tarafından karara bağlanmamaktadır.

AİHM, ayrıca Bilgi Kanunu'nun yetkili makamların, müdahalenin gerekliliğini ve ölçülülüğünü online ortamda ifade özgürlüğü bağlamında değerlendirmesini veya aynı sonuca daha az müdahaleci bir yöntemle erişilmesini sağlayacak şekilde gerçekleştirilmesini öngören bir kural içermediğini de belirlemiştir.[1357] Keza, söz konusu mevzuat, yetkili makamların uygulanan engelleme tedbirinin hukuka aykırı içeriği hedeflediği ve keyfî veya web sitesinin tamamının engellenmesinden kaynaklanan aşırı etkisi olmadığına dair bir denetim yapmalarını da gerektirecek bir kural içermemektedir.

Konuyu şeffaflık kriteri açısından da ele alan AİHM, Bilgi Kanunu'nun 15.3. maddesinin, engelleme kararının engellemenin hedeflediği web sitesi sahiplerine bildirimine ilişkin de bir hüküm içermediği tespitini yapmıştır.[1358] Mevcut uyuşmazlıkta başvurucular, söz konusu engelle-

[1356] *OOO Flavus ve Diğerleri v. Rusya*, para. 40.

[1357] *OOO Flavus ve Diğerleri v. Rusya*, para. 41.

[1358] *OOO Flavus ve Diğerleri v. Rusya*, para. 42.

me kararı uygulanana ve yargısal itiraz yapana kadar engelleme kararının gerekçesinden haberdar olmamıştır.

Kablis v. Rusya[1359] kararına atıf yapan AİHM, önceki içtihatlarında Bilgi Kanunu'nun 15.3. maddesinin yürütme organına verdiği takdir yetkisinin genişliğinin temyiz aşamasında engelleme tedbirinin yargısal denetimini -imkânsız kılmasa da- güçleştirdiğini belirtmiştir.[1360] AİHM'ye göre, AİHS ile uyumlu bir denetimde, büyük miktarda bilgiyi erişilmez kılan bir tedbirin internet kullanıcılarının haklarını esaslı şekilde kısıtladığının ve önemli dolaylı etkiler oluşturabileceğinin dikkate alınması gerekir.

Nihayetinde AİHM'ye göre, Bilgi Kanunu'nun 15.3. maddesindeki usulün uygulanması neticesinde gerçekleştirilen müdahale aşırı ve keyfî niteliktedir. Rus hukuku, başvuruculara demokratik bir toplumda hukukun üstünlüğü ilkesinin gerektirdiği ölçüde bir güvence sağlamamıştır. Hukuka aykırı içeriği aşan ve tüm online medya sitesinin engellenmesine yol açan müdahale AİHS'nin 10. maddesinin ikinci fıkrasındaki meşru hiçbir amaçla bağdaşmamaktadır.[1361] Mahkemeye göre müdahale, meşru bir amaç gütmemiştir ve demokratik bir toplumda gerekli değildir. Bu sebeple AİHS'nin 10. maddesi ihlal edilmiştir.

AİHS'nin 10. maddesine yönelik ihlali tespit ettikten sonra AİHM, başvuruculara web sitelerine yönelik şikâyetleri için etkili bir hak arama yolu olup olmadığı meselesini, diğer bir deyişle 13. maddeye yönelik ihlal iddiasını ele almıştır.[1362] Rus Hükûmeti, iç hukukta hak arama yolları bulunsa da (temyiz imkânı) başvuruculara bunları kullanmadığı iddiasındadır.[1363] Başvurucular, Rus mevzuatının, Başsavcıya engelleme talebinin ilgili taraflar üzerindeki etkisini ölçme yükümlülüğü getirmediğini ileri sürmüştür. Engelleme sürecinin herhangi bir aşamasına ne bir mahkeme ne de web sitesi sahipleri dâhil edilmiştir. Engelleme kararından sonraki denetim aşamasında ise Rus mahkemeleri çok dar bir çerçevede inceleme yaparak sadece Roskomnadzor'un kararın gereğini usulüne uygun olarak

[1359] Kablis v. Rusya kararı için bkz. **§20**.

[1360] *OOO Flavus ve Diğerleri v. Rusya*, para. 43.

[1361] *OOO Flavus ve Diğerleri v. Rusya*, para. 44.

[1362] *OOO Flavus ve Diğerleri v. Rusya*, para. 46.

[1363] *OOO Flavus ve Diğerleri v. Rusya*, para. 48.

yerine getirip getirmediğini incelemiştir. Mahkemeler engellemelerin ölçülülüğüne dair bir değerlendirme de yapmamıştır.[1364]

Müdahil üçüncü taraflardan Avrupa Bilgi Toplumu Enstitüsü, etkilenen taraflar için hem *ex-ante* hem de *ex-post* hak arama yollarının sunulması gerektiğini belirtmiştir.[1365] *Ex-ante* yollar, engellemeye konu olan web sitelerinin sahiplerine ön bildirim yapılmasını içerir. *Ex-post* yollar ise bir engelleme kararı uygulandıktan sonra kararın kapsamını kısıtlamak veya yeni koşullar dikkate alınarak karara itiraz etmek için etkin mekanizmaların varlığını ifade eder.

AİHM, daha önceki içtihatlarına atıf yaparak Rus hukuku bağlamında temyiz olanağının etkili bir hak arama yolu olmadığını hatırlatmıştır.[1366] AİHM, AİHS'nin 10. maddesi ile 13. maddesindeki menfaatlerin niteliğine ilişkin bir karşılaştırma yapmıştır.[1367] AİHM'ye göre 13. madde usuli bir koruma sağlarken, diğer bir deyişle etkin bir başvuru hakkını gerekli kılarken, 10. maddenin bünyesindeki usuli koruma ifade özgürlüğünün özüne saygıyı temin etme gibi daha geniş bir amacın yan unsuru niteliğindedir. Mahkemeye göre, başvurucunun, ifade özgürlüğünün kısıtlandığına dair bir iddiası vardır. Mahkeme, 13. maddenin, iddia edilen ihlalleri veya devamını önleyen veya vuku bulmuş ihlallere ilişkin uygun tazmin imkânları sağlayan, hem hukuken hem de uygulamada etkili bir yerel hak arama mekanizmasını gerektirdiğini hatırlatmıştır.

AİHM, başvurucuların, ifade özgürlüğü haklarının ihlal edildiğine ilişkin, temeli olan bir iddiası olduğu görüşündedir.[1368] Bu bağlamda, 13. maddenin bir gereği olarak, iddia edilen ihlali önlemek veya başlamış olan ihlali durdurmak yahut vuku bulmuş ihlaller için uygun tazmin yollarına sahip olmak, etkin bir hak arama yolunun olmazsa olmazlarıdır.

AİHM'ye göre, başvurucular engelleme kararlarına karşı itiraz imkânına sahip olsalar da Rus mahkemeleri şikâyetlerin esasını dikkate al-

[1364] *OOO Flavus ve Diğerleri v. Rusya*, para. 49.
[1365] *OOO Flavus ve Diğerleri v. Rusya*, para. 50.
[1366] *OOO Flavus ve Diğerleri v. Rusya*, para. 51.
[1367] *OOO Flavus ve Diğerleri v. Rusya*, para. 52.
[1368] *OOO Flavus ve Diğerleri v. Rusya*, para. 53.

mamıştır.[1369] Aynı doğrultuda AİHM, mahkemelerin, yetkili makamların sorunlu web sayfalarını tespit etmeye, engelleme tedbirlerinin gerekliliği, ölçülülüğü ve aşırı kapsamını incelemeye ilişkin hukuki yükümlülüklere uymaması hususunu değerlendirmediğini düşünmektedir. Bu bağlamda AİHM, mevcut uyuşmazlığın koşullarını dikkate alarak yerel hukukun sunmuş olduğu hak arama yolunun etkin olmadığı kanaatine varmıştır.[1370] Mahkeme, AİHS'nin 10. maddesiyle bağlantılı olarak 13. maddenin de ihlal edildiğine hükmetmiştir.[1371]

Sonuç olarak AİHM, başvuruları birleştirmiş, kabul edilebilir olduklarını açıklamış, AİHS'nin 10 ve 13. maddelerinin ihlal edildiğine karar vermiştir.

VIII. Değerlendirme

AİHM'nin *OOO Flavus ve Diğerleri v. Rusya* kararı, temeli *Ahmet Yıldırım v. Türkiye* kararı ile atılan içtihatlarıyla uyumlu bir karardır. AİHM, yetkili idari makamların veya mahkemelerin hukuka aykırı bir internet içeriğine tedbir uygulamasını ilkesel olarak reddetmemektedir. AİHM'ye göre istisnai durumlarda hukuka aykırı içeriği engellemek mümkünse de bir web sitesinin tamamına erişimi engelleme, hukuka aykırı içeriğe yönelen ilk karardan bağımsız olarak ve AİHS'nin 10. maddesi bağlamında geliştirilen ve uygulanan kritere göre gerekçelendirilmelidir.

İnternete ilişkin bir engelleme tedbirinin çok büyük miktarda veriyi erişilmez kılması sebebiyle AİHM'nin ölçülülük ilkesinin bu gerçeklik dikkate alınarak uygulanması gerekmektedir. Mahkeme, engelleme tedbirinin açık bir yasal dayanağı olmasını hem *ex ante* hem de *ex post* denetlenebilir olmasını, hakları etkilenen kişilerin mutlaka süreçlerden haberdar edilmesini, tüm sürecin şeffaf olmasını etkin bir hak arama mekanizmasının varlığına yönelik denge testinin temel bileşenleri olarak nitelendirmektedir.

[1369] *OOO Flavus ve Diğerleri v. Rusya*, para. 54.

[1370] *OOO Flavus ve Diğerleri v. Rusya*, para. 54.

[1371] *OOO Flavus ve Diğerleri v. Rusya*, para. 55.

§24. VLADİMİR KHARİTONOV V. RUSYA

AİHM'nin, 23 Haziran 2020 tarihinde Rusya'ya ilişkin verdiği son karar *Vladimir Kharitonov v. Rusya* kararıdır.[1372] Karar, erişimin engellenmesi tedbirinin AİHS'ye uygunluğuna ilişkindir. Başvurunun temelini, başka bir web sitesine uygulanan erişimi engelleme tedbiri sebebiyle aynı IP adresinde barınan diğer bir web sitesinin engellenmesi oluşturmaktadır.

I. Davanın gelişimi

Başvuru, Rus vatandaşı Bay Vladimir Vladimirovich Kharitonov tarafından 27 Aralık 2013 tarihinde Rusya Federasyonu'na karşı yapılmıştır. Başvurucu, Association of Electronic Publishers isimli ticari olmayan bir kuruluşun yöneticisi ve Association of Internet Users isimli sivil toplum örgütünün kurucularındandır.[1373] Başvurucu, www.digitalbooks.ru alan adıyla yayın yapan ve elektronik yayıncılıkla ilgili haber, makale ve yorumları derleyen bir web sitesinin sahibi ve yöneticisidir. Web sitesi 2008 tarihinde kurulmuş olup ABD'de bulunan ve paylaşımlı barınma hizmeti sunan DreamHost şirketi tarafından barındırılmaktadır. Bu hizmet kapsamında birden fazla web sitesi aynı IP adresi fakat farklı alan adı ile yayın yapmaktadır. Bir kullanıcı, bu sunucuda yer alan bir web sitesine erişmeye çalıştığında sunucu, gelen kullanıcı talebine göre hangi web sitesinin gösterileceğini belirlemektedir.

Aralık 2012'de, Rusya'nın farklı bölgelerinden kullanıcılar başvurucuya, web sitesinin "yetkili bir Rus makamının kararıyla" engellendiğine dair bildirim yapmıştır.[1374] Başvurucu, Rus telekomünikasyon otorotesi Roskomnadzor tarafından oluşturulan "kara listeye alınmış web siteleri sicili"ni incelediğinde kendi web sitesinin IP adresinin Federal Uyuştu-

---

[1372] **AİHM**, *Vladimir Kharitonov v. Rusya*, Başvuru No: 10795/14, 23.6.2020.

[1373] *Vladimir Kharitonov v. Rusya*, para. 5.

[1374] *Vladimir Kharitonov v. Rusya*, para. 6.

rucu Kontrol Dairesinin 19 Aralık 2012 tarihli kararına istinaden kara listeye eklendiğini tespit etmiştir.

Engelleme kararı; rastaman.tales.ru isimli, kenevir temalı muhtelif halk hikâyelerinin yer aldığı web sitesine yöneliktir. Bu web sitesi de DreamHost tarafından barındırılmakta ve başvurucunun web sitesi ile aynı IP adresini kullanmaktadır. Rus Hükûmeti, IP adresine yönelik engele 22 Mart 2013 tarihinde sona verildiği ancak engelleme ve engeli kaldırma kararlarının başvurucuya ve mahkemeye sunulmadığı bilgisini AİHM ile paylaşmıştır.[1375]

Başvurucu, Rusya'daki Takanskiy Bölge Mahkemesine başvurarak IP adresinin tamamının engellenmesinin, hukuka aykırı herhangi bir içerik barındırmayan kendi web sitesine erişimi de engellediğini belirtmiştir.[1376] Bölge Mahkemesi, 19 Haziran 2013 tarihinde başvurucunun şikâyetini reddetmiştir.[1377] Mahkemeye göre Roskomnadzor kendi yetkisi kapsamında, ilgili kanunlara uygun şekilde ve çocukları uyuşturucu kullanımına ilişkin zararlı bilgilerden korumak amacıyla hareket etmiştir. Ancak, Bölge Mahkemesi, tartışmalı tedbirin başvurucunun web sitesi üzerindeki etkisine ilişkin bir değerlendirme yapmamıştır.

Başvurucu, Takanskiy Bölge Mahkemesinin kararına itiraz etmiş ve bir barınma hizmetinin fark gözetilmeksizin engellenmesine ilişkin *Ahmet Yıldırım v. Turkey* kararını emsal göstermiştir.[1378] İtirazı ele alan Moskova Şehir Mahkemesi, 12 Aralık 2013 tarihinde itirazı reddetmiştir.[1379] Moskova Şehir Mahkemesi de Roskomnadzor'un hukuka aykırı içeriğe erişimi yasal bir şekilde engellediği ve ölçülülük ilkesini gözettiğini belirtmiş ancak tıpkı Bölge Mahkemesi gibi engelleme tedbirinin başvurucunun web sitesi üzerindeki etkisine değinmemiştir.

Başvurucu, engelleme tedbirinin dayanağını oluşturan Bilgi Kanunu'nun 15.1. maddesini somut norm denetimi yoluyla Anayasa Mahke-

[1375] *Vladimir Kharitonov v. Rusya*, para. 6.
[1376] *Vladimir Kharitonov v. Rusya*, para. 7.
[1377] *Vladimir Kharitonov v. Rusya*, para. 8.
[1378] *Vladimir Kharitonov v. Rusya*, para. 9.
[1379] *Vladimir Kharitonov v. Rusya*, para. 10.

mesinin önüne taşımıştır. 17 Temmuz 2014 tarihli kararında Anayasa Mahkemesi, başvuruyu şu gerekçeyle reddetmiştir: [1380]

"Herhangi bir yasaklı bilgi içermediği hâlde ağ adreslerinin sicile eklenmesi neticesinde web sitelerine erişim engellenen web sitesi sahiplerinin bilgiyi yayma hakkını etkileyen şey, ağ adreslerinin Bütüncül Sicil'e eklenmesi değil, barındırma hizmet sağlayıcısının özenli hareket etmemesidir. Bu nedenle, bilgiyi yayma hakları, ilk ve öncelikli olarak barındırma hizmet sağlayıcısıyla aralarındaki hukuki ilişki bağlamında savunulmalıdır."

II. Hukuki arka plan

Konunun esasına girmeden önce AİHM, Rus iç hukukunun konuyla ilgili düzenlemelerini ve muhtelif insan hakları belgesini alıntılamıştır. Mahkemenin ilk alıntıladığı düzenleme, Rus Bilgi Kanunu'nun (Kanun no. 149-FZ, 27 Temmuz 2006) 15.1 maddesi olmuştur.[1381]

28 Temmuz 2012 tarihinde, Bilgi Kanunu'na 15.1. madde eklenmiştir. Bu hüküm, Rusya Federasyonu'nda yasaklanmış alan adları, web sayfaları referansları (URL) ve web sitelerinin ağ adresleri için Bütüncül Sicil oluşturulmasını öngörmüştür (1. fıkra). Telekomünikasyon otoritesi Roskomnadzor, Bütüncül Sicil'i güncellemekle yükümlüdür (3. fıkra). Yetkili bir idari makamın kararıyla, yedi farklı hukuka aykırı içerik kategorisinden en az birine giren içeriği barındıran web siteleri listelenmektedir ki bu kategoriler arasında uyuşturucu üretimi ve kullanımı da yer almaktadır [5(1)(b). fıkra].

Bir web sitesin bu Sicil'e alınmasına ilişkin kararın; web sitesinin sahibi, barındırma hizmet sağlayıcısı veya internet hizmet sağlayıcısı tarafından bir mahkeme önünde itiraza konu edinilmesi mümkündür (6. fıkra). Bir web sitesinin bu listeye eklendiğine ilişkin bildirimi alan barındırma hizmet sağlayıcısı derhâl web sitesi sahibini bilgilendirmek ve hukuka aykırı içeriği kaldırmasını talep etmekle yükümlüdür (7. fıkra). Eğer sitenin sahibi bu konuda harekete geçmekten imtina ederse barın-

[1380] *Vladimir Kharitonov v. Rusya*, para. 11.

[1381] *Vladimir Kharitonov v. Rusya*, para. 12.

dırma hizmet sağlayıcısı bu web sitesine erişimi kısıtlamakla yükümlüdür (8. fıkra). Barındırma hizmet sağlayıcısı ve web sitesi sahibinin bu konuda herhangi bir işlem yapmaması durumunda web sitesinin IP adresi Bütüncül Sicil'e eklenmekte (9. fıkra) ve internet hizmet sağlayıcılar bu IP adresine erişimi engellemekle yükümlü kılınmaktadır (10. fıkra).

Rus Hükûmeti, 26 Ekim 2012 tarihinde, yasaklı içerik barındıran alan adlarının, web sayfası referansları (URL) ve ağ adreslerinin Bütüncül Sicili'e kaydına ilişkin ikincil bir düzenleme yapmıştır (Karar no. 1101). Bu ikincil düzenlemelerle Bilgi Kanunu'nun 15.1. maddesinin nasıl uygulanacağı belirlenmeye çalışılmıştır.[1382]

AİHM, Bilgi Kanunu'na yaptığı atıflardan sonra muhtelif uluslararası belgelere değinmiştir. Bunlardan ilki, Avrupa Konseyinin 28 Mayıs 2003 tarihli İnternette İletişim Özgürlüğüne İlişkin Deklarasyon'udur.[1383] Deklarasyon'un "Devletin ön kontrolünün bulunmaması" başlıklı 3. maddesine atıf yapan AİHM, kamu otoritelerinin her türlü sınırdan bağımsız olarak genel engelleme veya filtreleme tedbiri uygulayarak kamunun bilgiye erişimini veya internet ortamında başka tür iletişimi engellememesi gerektiğini tekrarlamıştır.[1384]

AİHM; düşünce ve ifade özgürlüğü hakkının korunması ve desteklenmesine ilişkin BM Özel Raportörü'nün 2011 tarihli Rapor'una (A/HRC/17/27), Birleşmiş Milletler Fikir ve İfade Özgürlüğü Özel Raportörü, Avrupa Güvenlik ve İşbirliği Teşkilatı Medya Özgürlüğü Temsilcisi, Amerikan Devletleri Örgütü İfade Özgürlüğü Özel Raportörü, Afrika İnsan ve Halkların Hakları Komisyonu İfade Özgürlüğü ve Bilgiye Erişim Özel Raportörü'nün 1 Haziran 2011 tarihli Ortak Deklarasyonu'na ve Birleşmiş Milletler İnsan Hakları Komitesinin 11-29 Temmuz 2011 tarihleri arasında gerçekleşen 102. oturumunda Medeni ve Siyasi Haklara İlişkin Uluslararası Sözleşmesi'nin 19. maddesiyle ilgili olarak kabul ettiği 34 sayılı Genel Yorum'una vurgu yapmıştır.[1385]

[1382] *Vladimir Kharitonov v. Rusya*, para. 13.

[1383] İnternette İletişim Özgürlüğüne İlişkin Deklarasyon için bkz. **§6(IV)**.

[1384] *Vladimir Kharitonov v. Rusya*, para. 12.

[1385] *Vladimir Kharitonov v. Rusya*, para. 14-17.

AİHM ayrıca, Avrupa Konseyi İnsan Hakları Komiseri'nin 2014 yılında hazırlamış olduğu "İnternet ortamında ve daha geniş dijital dünyada hukukun üstünlüğü" çalışmasına atıf yapmıştır.[1386] Söz konusu raporda, engelleme sistemlerinin eksiklikleri olarak şunlar gösterilmiştir: (i) Engellemenin, özellikle haberleşmeleri inceleyen bir yazılım veya donanım aracılığıyla gerçekleştirildiği durumlarda, yapısal olarak (kasti olmayan şekilde) yanlış pozitif (yasaklı içerik barındırmayan sitelerin engellenmesi) ve yanlış negatif (yasaklı içeriklerin fitrelerde yakalanmaması) sonuçlar üretmesi muhtemeldir; (ii) sadece belirli web sitelerini engelleme kriterleri ve engellenen sitelerin listeleri çoğunlukla en iyi ihtimalle şeffaf değildir en kötü ihtimalle gizlidir; (iii) itiraz mekanizmaları, özellikle neyin engellenip neyin engellenmeyeceği -bilerek- özel teşebbüslere bırakıldıysa külfetli olabilir, az bilinebilir veya hiç var olmayabilir.

Son olarak Avrupa Konseynin CM/Rec(2016)5 sayılı İnternet Özgürlüğüne İlişkin Tavsiye Kararı'ndan alıntılar yapmıştır.[1387] Söz konusu Tavsiye Kararı'nın ilgili kısımlarını tekrar etmek gerekirse:

2.2.1. Devlet makamları veya özel sektör aktörleri tarafından bir internet platformunu (sosyal medya, sosyal ağlar, bloglar veya başka diğer web siteleri) veya bilgi ve haberleşme teknolojileri (BT) araçlarını (anlık mesajlaşma ve diğer uygulamalar) engelleyen veya bunlara erişimi başka şekilde kısıtlayan her türlü tedbir veya devlet makamlarının bu tür eylemlere yönelik talepleri, kısıtlamaların kanunla öngörülmesini, meşruluk ve ölçülülük koşullarına uygun olmasını öngören AİHS'nin 10. maddesiyle uyumlu olmalıdır.

2.2.2. Devlet makamları veya özel sektör tarafından alınan internet içeriğini engelleme, filtreleme veya kaldırmaya yönelik her türlü tedbir veya bu tür bir işlem için devlet makamları tarafından gerçekleştirilen her türlü talep, kısıtlamaların kanunla öngörülmesini, meşruluk ve ölçülülük koşullarına uygun olmasını öngören AİHS'nin 10. maddesiyle uyumlu olmalıdır.

2.2.3. İnternet hizmet sağlayıcıları, genel bir ilke olarak, internet trafiğine eşit ve gönderen, alıcı, içerik, uygulama, hizmet veya cihaz temelli ay-

[1386] *Vladimir Kharitonov v. Rusya*, para. 18.

[1387] İnternet Özgürlüğüne İlişkin Tavsiye Kararı için bkz. **§6(XXV)**.

rımcılık yapmayacak şekilde muamele eder. İnternet trafik yönetim tedbirleri, AİHS'nin 10. maddesine uygun şekilde üstün kamusal yarara ulaşmak için şeffaf, gerekli ve ölçülü olmalıdır.

2.2.4. İnternet kullanıcılarının veya ilgili diğer tarafların, internete erişim, içerik veya bilgiyi alma ve yayma imkânlarını sınırlamaya yönelik işlemlere karşı AİHS'nin 6. maddesine uygun şekilde mahkemelere erişim hakkı vardır.

2.2.5. Devlet, bilgi alma ve yayma özgürlüğüne uyguladığı engellenen veya içerdiği bilgiler kaldırılan web sitelerini göstermek gibi kısıtlamalar hakkında bunların hukuki dayanağı, gerekliliği ve gerekçesi, bu işleme izin veren mahkeme kararı ve bu karara itiraz hakkını içerecek şekilde kamuoyunu zamanında ve uygun şekilde bilgilendirmelidir.

Yukarıda belirtilen Tavsiye Kararı'na Rusya Federasyonu tarafından özel çekince koyulduğunu belirtmek gerekir.

III. Tarafların iddiaları

Başvurucu, Rus makamlarının, IP adresini kara listeye almak suretiyle hukuka aykırı bir web sitesini engellemesinin kendi web sitesinin de engellenmesi şeklinde ölçüsüz bir yan yetki doğurduğu ve bu sebeple de AİHS'nin 10. maddesinde güvence altına alınan ifade özgürlüğünün ihlal edildiği iddiasındadır.[1388] Başvuruyu inceleyen AİHM, başvuruyu açıkça dayanaktan yoksun olarak nitelendirmeyerek kabul edilebilir görmüştür.[1389]

IV. Başvurucunun iddiaları

Başvurucu, uyuşturucu üretimi ve kullanımına ilişkin bilgiye erişimin engellenmesinin meşru bir amaca hizmet ettiğinin kabul edilebileceği görüşündedir.[1390] Başvurucunun itirazı, müdahalenin niteliğine

[1388] *Vladimir Kharitonov v. Rusya*, para. 20

[1389] *Vladimir Kharitonov v. Rusya*, para. 21.

[1390] *Vladimir Kharitonov v. Rusya*, para. 22.

ilişkindir. Başvurucu, müdahalenin kapsam ve yönteminin, hedeflenen amaç için ölçüsüz olduğu görüşündedir.

Başvurucu, "The Rastaman Tales" isimli sitenin, kenevir ile ilgili karikatür ve halk hikâyelerinin kitle kaynağı şeklinde toplanmasından oluştuğunu; bu sitenin yetişkinleri hedeflediğini ve uyuşturucu üretimi veya kullanımı için pratik bir rehberle mukayese edilemeyeceğini belirtmiştir. Ayrıca, bu hikâyelerin kitap formatında da yayımlandığı ve hatta prestijli bir Rus edebiyat ödülü aldığını, kâğıt formatında yıllarca yasal olarak satıldığını ve internet üzerinde birden çok kaynaktan erişilebilir olduğunu eklemiştir. Başvurucuya göre, otoritelerin söz konusu koleksiyonun birçok kopyasına erişimi engellemeye ilişkin kararları hedeflenen amaca ulaşmamış ve kendisinin bilgiyi yayma hakkına esaslı ve haksız bir zarar vermiştir.

Başvurucu, web sitesini haber yayımlamak için kullandığını belirtmiş ve AİHM'nin haberleri "*bozulabilir bir meta*" olarak nitelendirdiği ve geç yayımlamanın haberin değerini ve habere olan ilgiyi kaybettireceğine ilişkin içtihatlarına atıf yapmıştır.[1391] Başvurucu, engelleme gerçekleştiği sırada web sitesinin dört yıldır yayında olduğunu, arama motorları tarafından indekslendiğini ve düzenli bir okuyucu kitlesinin bulunduğunu belirtmiştir. Engelleme sebebiyle web sitesini taşımak durumunda kalırsa buna ciddi bir vakit ve kaynak ayırması gerektiğini, dört yıllık arşivine erişimi kesmek durumunda kalacağını ve en önemlisi Rus internet hukukundaki yapısal sorunlar sebebiyle alternatif bir platformda dahi bu sorunla karşılaşmasının pek muhtemel olduğunu ileri sürmüştür. Başvurucu, bu iddiasını Rus makamlarının Facebook ve Google sitelerine erişimi engellemeye hazırlandığına dair beyanlarına ve herhangi bir hukuka aykırı içerik barındırmasa da paylaşımlı IP adresleri sebebiyle Ekim 2017 itibarıyla 3.900.000'den fazla web sitesinin engellenmesine dayandırmıştır.

Başvurucu, engelleme kararının kendisiyle paylaşılmadığını, hukuka aykırı web sitesi veya İSS ile iletişime geçme imkânı bulunmadığını ve haklarını koruyabilmek için yapılması gerekenlerin farkında olmadığını

[1391] *Vladimir Kharitonov v. Rusya*, para. 23.

iddia etmiştir. Başvurucu, iyi niyetli bir web sitesi sahibi olarak üzerlerinde hiçbir gücü veya etkisi olmadığı üç aktörün insafına kaldığını ileri sürmüştür: Rus makamları, hukuka aykırı web sitesinin sahibi ve barındırma hizmet sağlayıcısı.[1392] Hem web sitesi sahibi hem de barındırma hizmet sağlayıcısı Rus olmayıp bunların Rus makamlarının taleplerini yerine getirmesi beklenmemektedir. Başvurucu, mevcut Rus hukukunun, hukuka aykırı içerik barındıran web sitesiyle aynı IP adresini paylaşan hukuka uygun web sitelerine haklarını aramak için hukuki bir koruma sağlamadığını belirtmiştir. Zira, Roskomnadzor bu tür web sitelerine ilişkin engelleme kararının etkilerini değerlendirmekle yükümlü tutulmamıştır.

V. Rus Hükûmetinin savunması

Rus Hükûmeti, hukuka aykırı web sitesi rastaman.tales.ru sitesinin engellenmesinin, uyuşturucu üretme ve kullanmayı kısıtlamaya yönelik önemli bir politik hedefe hizmet ettiğini belirtmiştir.[1393] Rus Hükûmetine göre, Roskomnadzor hukuka aykırı web sitesinin IP adresini yasaklı web siteleri siciline hemen eklememiş; öncelikle yer sağlayıcıyı söz konusu web sitesinin hukuka aykırı bilgi içerdiği konusunda hem Rusça hem de İngilizce bilgilendirmiştir. Yer sağlayıcı içeriği kaldırmadığı için Roskomnadzor beş gün sonra web sitesinin IP adresini Bütüncül Sicil'e eklemiştir.

Rus Hükûmeti, Roskomnadzor'un, Bilgi Kanunu'nun 15.1. maddesinin gerekliliklerini bire bir yerine getirerek hukuka uygun, gerekçeli ve gerekli bir tedbir aldığı görüşündedir.[1394] Kaldı ki ilgili mevzuatta Roskomnadzor'un, engellenen web sitesinin paylaşımlı IP adresindeki tüm web sitesi sahiplerini bilgilendirmeye ilişkin bir yükümlülüğü bulunmamaktadır. Rus Hükûmetine göre, bu tür kişilerin, Bütüncül Sicil'in web sitesindeki formu doldurarak bir kısıtlama olup olmadığını kontrol etmeleri mümkündür.

[1392] *Vladimir Kharitonov v. Rusya*, para. 24.

[1393] *Vladimir Kharitonov v. Rusya*, para. 25.

[1394] *Vladimir Kharitonov v. Rusya*, para. 25.

Rus Hükûmeti, mevcut davada yer sağlayıcıya önceden bir ihtar verildiğini ve engellemenin özel İSS'ler tarafından uygulandığını, bu sebeple mevcut davanın *Ahmet Yıldırım v. Türkiye* kararından farklı olduğunu ileri sürmüştür.[1395] *Ahmet Yıldırım v. Türkiye* kararına atıf yapan Rus Hükûmeti, Türk ceza mahkemesinin engelleme kararını uygulamadan önce Google sitesine bir ihtarda bulunmadığını ve engelleme kararının doğrudan Devlet telekomünikasyon idaresi tarafından uygulandığını belirtmiştir. Rus Hükûmeti mevcut uyuşmazlıkta başvurucunun İSS'ler aleyhine başvuruda bulunmadığını, mahkemelerden hukuka aykırı web sitesini engellemenin IP adresini engelleme dışında bir yöntemi olup olmadığını sorgulamadığını beyan etmiştir. Ayrıca, Türkiye ile bir kıyaslama yaparak, Rusya'nın aksine Türkiye'nin YouTube, GeoCities ve Dailymotion dâhil binlerce web sitesini engellediğini hatırlatmıştır.

Rus Hükûmeti, başvurucunun iddia edilen ihlalin mağduru olmadığını ileri sürmüştür.[1396] *Akdeniz v. Türkiye* kararına atıf yapan Rus Hükûmeti, mevcut durumun, bir Türk kullanıcısının müzik yayını yapan web sitesinin engellenmesi sebebiyle dolaylı olarak engellenmesi durumuna benzer olduğunu ileri sürmüştür. Rus Hükûmetine göre, başvurucu başka web siteleri, platformlar, online mecralar (LiveJournal, YouTube veya Facebook gibi) üzerinden elektronik kitap endüstrisiyle ilgili bilgi yayımlamaya devam edebilirdi.

Rus Hükûmetinin bir diğer iddiası ise engellemenin sadece üç ay gibi çok kısa bir süre uygulanmış olmasıdır.[1397] Hukuka aykırı web sitesinin sahibinin veya İSS'nin engelleme kararına itiraz ettiğini başvurucunun ortaya koymadığını belirten Rus Hükûmeti, Rus mahkemelerinin Roskomnadzor tarafından alınan kararı hukuka aykırı içeriğin yayılmasını önlemek amacıyla onayladığını ve yerel hukukun, keyfî müdahaleye karşı başvurucuya yeterli derecede koruma sağladığını iddia etmiştir.[1398] Rus Hükûmeti tüm bu iddialarını İngiliz, Fransız, Alman, Çin ve Amerikan hukukunun çocuk pornografisiyle mücadele için kullandığı benzer filtre-

[1395] *Vladimir Kharitonov v. Rusya*, para. 26.

[1396] *Vladimir Kharitonov v. Rusya*, para. 27.

[1397] *Vladimir Kharitonov v. Rusya*, para. 27

[1398] *Vladimir Kharitonov v. Rusya*, para. 27.

leme tekniklerini örnek vererek desteklemeye çalışmış, davaya müdahil olan üçüncü tarafların görüşlerinin mevcut davanın konusuyla ilgisiz olduğunu ileri sürmüştür.[1399]

VI. Müdahil tarafların görüşleri

Davaya farklı taraflar ve sivil toplum örgütleri müdahil olmuş ve görüş paylaşmışlardır. Bu taraflardan ilki Access Now isimli sivil toplum örgütüdür.[1400] Access Now, web sitelerinin engellenmesi dâhil ifade özgürlüğüne yönelik kısıtlamaların ölçülülüğünü değerlendirirken hem maddi (ne engelleniyor) hem de usuli (nasıl engelleniyor) unsurların dikkate alınması gerektiğini belirtmiştir. Bu doğrultuda, hukuka aykırı olduğu iddia edilen içeriğin tabiatına uygun seviyede koruma mekanizmalarının var olması gerektiğini hatırlatarak web sitesi engellemelerinin ifade özgürlüğünün özüne müdahale ettiğini ve bu sebeple, etkilenen bireylerin engelleme tedbirleri hakkında bilgilendirilmesi ve kendilerine uygun hak arama yollarının sağlanması gerektiğini vurgulamıştır.

Görüş veren diğer sivil toplum örgütleri, Article19 ve Electronic Frontier Foundation isimli kuruluşlardır. Bu kuruluşlara göre, web sitesinin tamamına erişimin engellenmesi, aşırı ve ölçüsüz bir tedbirdir.[1401] Hukuka uygun ve hukuka aykırı içerik arasında ayrım yapmadığı için bu tür bir tedbir gazete veya televizyonun engellenmesine benzetilmiştir.

Article 19 ve Electronic Frontier Foundation kuruluşlarına göre, engelleme kararları mümkün olduğunca dar şekilde kaleme alınmalı ve hukuka aykırı faaliyetleri önlemek için en az müdahaleci yöntemi tercih etmelidir.[1402] Bu tür kararlar, aşırı engelleme riskini dikkate alarak karara uyulması için kullanılacak teknolojiye de atıf içermelidir. Bu konuyu düzenleyen yasa şu standartları sağlamalıdır: (i) Engelleme kararları bir mahkeme veya bağımsız bir organ tarafından verilmelidir; (ii) İSS'ler ve diğer ilgili taraflara engelleme kararının alındığı yargılamalara müdahil

[1399] *Vladimir Kharitonov v. Rusya*, para. 28.

[1400] *Vladimir Kharitonov v. Rusya*, para. 29.

[1401] *Vladimir Kharitonov v. Rusya*, para. 30.

[1402] *Vladimir Kharitonov v. Rusya*, para. 30.

olma imkânı verilmelidir; (iii) kullanıcıların ve engellemenin yan etkilerinden mağdur olanların engelleme kararlarına itiraz etme imkânı olmalıdır; (iv) engellenen web sitesine ulaşmaya çalışan herkes, engellemenin yasal dayanağı ve engelleme kararının gerekçeleri ile karara itiraza ilişkin bilgileri görebilmelidir.

Bir diğer görüş veren sivil toplum örgütü Avrupa Bilgi Toplumu Enstitüsü isimli kuruluştur.[1403] Bu kuruluşa göre, 28 Haziran 2017 itibarıyla Rusya'da 6.522.629 internet kaynağı engellenmiş ve bunların 6.333.850 tanesi yani %97'si engellemenin yan etkileri sebebiyle dolaylı olarak gerçekleşmiştir.[1404] Kuruluş, Rus engelleme sisteminin açıkları bulunduğunu, aşırı engellemeye ve kötüye kullanıma uygun olduğunu, tek taraflı IP adresi yöntemleriyle binlerce web sitesinin erişilmez kılındığını ileri sürmüştür. Avrupa Bilgi Toplumu Enstitüsüne göre, web sitesi engellemeleri bağlamında ölçülülük ilkesi, her bir müstakil olayda engelleme kararının pozitif ve negatif etkileri ile uygulanacak engelleme tekniğinin ele alınmasını gerektirmektedir. Şayet ucuz bir engelleme tekniği olduğu için İSS'ler IP adresi engelleme tekniğini tercih edecekse devlet bu konudaki maddi külfete katlanarak insan haklarına uyumlu bir içerik engelleme şekli oluşturmalıdır.

Davaya müdahil olarak görüş veren son kuruluş ise RosKomSvoboda isimli Rus sivil toplum örgütüdür.[1405] Bu kuruluşa göre, engellemeye ilişkin yasal mevzuatın tahmin edilemeyen sonuçları olmuş ve mevzuat özel olarak hedef gösterilmemiş web sitelerinin engellenmesine sebebiyet vermiştir. Keza, bu mevzuatın, engelleme kararlarına itiraz için etkin bir mekanizma sunmadığı, iyi niyetli web sitesi sahiplerinin bu tür kararlardan ancak uygulandıktan sonra haberdar oldukları ileri sürülmüştür.

[1403] *Vladimir Kharitonov v. Rusya*, para. 31.

[1404] *Vladimir Kharitonov v. Rusya*, para. 31.

[1405] *Vladimir Kharitonov v. Rusya*, para. 32.

VII. AİHM'nin tespit ve değerlendirmeleri

Konunun esasına giren AİHM öncelikle *Ahmet Yıldırım v. Türkiye* kararındaki internetin niteliğine ilişkin tespitlerine atıf yapmıştır.[1406] Tekrar etmek gerekirse, AİHM söz konusu kararında erişilebilirliğin yanı sıra büyük miktarda veriyi muhafaza etme ve dağıtma imkânları sayesinde internet sitelerinin kamunun güncele erişiminin iyileştirilmesine ve bilginin iletilmesinin kolaylaştırılmasına önemli derecede katkıda bulunduğunu; internetin politik veya kamu menfaatine ilişkin tartışma ve eylemlere katılım konusunda asli vasıtaları barındırdığını ve AİHS'nin 10. maddesinin yalnızca bilgilerin iletilmesi hakkını değil, aynı zamanda toplumun bilgi alma hakkını da güvence altına aldığını belirtmiştir.

Başvurucu, elektronik kitapların üretimi ve dağıtımına ilişkin haberler, analitik raporlar ve uygulama rehberleri sunan bir web sitesinin sahibi ve yöneticisidir.[1407] Web sitesi 2008 yılından beri aktiftir, haftada birkaç defa güncellenmektedir, www.digital-books.ru isimli alan adında yayın yapmaktadır; bir Amerikan yer sağlayıcı şirketin sunucularında barındırılmaktadır fakat paylaşımlı IP adresi kullanmaktadır.

Süreci kronolojik olarak özetleyen AİHM, Aralık 2012 tarihinde başvurucunun, web sitesine erişimin engellendiğini tespit ettiğini ve durumun, bir devlet kurumunun aynı sunucuda bulunan ve aynı IP adresini kullanan başka web sitesine yönelik erişimi engelleme kararından kaynaklandığını belirtmiştir.[1408] AİHM, *Ahmet Yıldırım v. Türkiye* kararına tekrar atıf yaparak yasal temeli ne olursa olsun, internete erişimi etkileyebilme potansiyeli olan böyle bir tedbirin, davalı devletin AİHS'nin 10. maddesi kapsamında sorumluluğunu doğurduğunu vurgulamıştır.[1409]

AİHM, başvurucunun üçüncü taraf web sitesine yönelik süreçten, engelleme tedbirinin gerekçelerinden veya süresinden haberdar olmadığını belirtmiştir.[1410] Başvurucu, engellemenin kaldırılıp kaldırılmayacağı

[1406] *Vladimir Kharitonov v. Rusya*, para. 33.
[1407] *Vladimir Kharitonov v. Rusya*, para. 34.
[1408] *Vladimir Kharitonov v. Rusya*, para. 35.
[1409] *Vladimir Kharitonov v. Rusya*, para. 35.
[1410] *Vladimir Kharitonov v. Rusya*, para. 36.

ve web sitesine erişimin tekrar sağlanıp sağlanmayacağı hakkında ne bilgi sahibidir ne de sürece ilişkin bir kontrolü vardır. Başvurucu, engelleme sürecinde elektronik haberleşme konusundaki son gelişmeleri ve haberleri paylaşamamış, kullanıcılar da web sitesinin hiçbir içeriğine erişememiştir. AİHM'ye göre bu müdahale sadece bilgiyi yayma değil ayrıca kamunun bilgiyi alma hakkına "bir kamu otoritesi tarafından müdahale" niteliğindedir.[1411]

Bu tespitten sonra Mahkeme *Ahmet Yıldırım v. Türkiye* kararına tekrar atıf yaparak AİHS'nin 10. maddesinin yalnızca bilgilerin iletilmesi hakkını değil aynı zamanda toplum açısından bilgi alma hakkını da güvence altına aldığını hatırlatmıştır.[1412] AİHM'ye göre, bir müdahale, kanunla öngörülme ve AİHS'nin 10. maddesinin ikinci fıkrasında belirtilen meşru amaçlardan bir veya birden fazlasını gütme ve bu amaçlara ulaşmak için demokratik bir toplumda gerekli olma şartlarını taşımadıkça 10. maddeyi ihlal etmiş olacaktır.

AİHM'ye göre "kanunla öngörülen" ifadesi, öncelikle tedbirin iç hukukta bir dayanağı olmasını gerektirir. Ayrıca söz konusu yasanın, kendisi açısından ortaya çıkabilecek sonuçları ve hukukun üstünlüğü ilkesiyle uyumunu önceden değerlendirebilmesi için ilgili kişi açısından erişilebilir olması gerektiğini ifade eder.[1413] Yasanın yürütme organına temel haklara ilişkin konularda sınırsız bir takdir yetkisi vermesi hâlinde AİHS'nin benimsediği demokratik bir toplumu oluşturan ana ilkelerden hukukun üstünlüğü ilkesine aykırılık söz konusu olacaktır. Bu sebeple yasa, bu gücün kullanılmasının yöntemini ve kapsamını yeterli netlikte düzenlemelidir.

AİHM, mevcut uyuşmazlıktaki müdahalenin yasal temelinin Bilgi Kanunu'nun 15.1. maddesi olduğunu belirtmiş ve bu yasanın içeriğini detaylı bir analize tabi tutmuştur. Kanun, hukuka aykırı içerik kategorileri tanımlamakta ve engelleme kararlarının uygulanması için adım adım bir usul getirmektedir. Bu hükme dayalı olarak Rus makamları, "The Ras-

[1411] *Vladimir Kharitonov v. Rusya*, para. 36.

[1412] *Vladimir Kharitonov v. Rusya*, para. 36.

[1413] *Vladimir Kharitonov v. Rusya*, para. 37.

taman Tales" isimli kenevir temalı hikâyelere ilişkin online koleksiyona erişimi engellemiştir. AİHM, Bilgi Kanunu'nun 15.1 maddesinin yetkili makamlara hukuka aykırı ve hukuka uygun içerik ayrımı yapmaksızın tüm web sitesini engelleme imkân tanıdığını belirtmiştir.[1414] AİHM, bir web sitesinin tamamının engellenmesinin bir gazete veya televizyon istasyonunun engellenmesiyle kıyaslanacak düzeyde aşırı ve keyfî bir tedbir olduğunu vurgulamıştır.

AİHM, engellemeye konu olan web sitesinin hukuka aykırı içerik ihtiva ettiği ileri sürülebilirse de başvurucunun web sitesinde Bilgi Kanunu'nun 15.1. maddesi kapsamına girebilecek bir içerik bulunmadığını belirtmiş ve bu durumu *Ahmet Yıldırım* kararına benzetmiştir.[1415] Başvurucunun, hukuka aykırı olduğu belirtilen web sitesinin sahibiyle bir bağlantısı olmadığı gibi başvurucu hukuka aykırı içerikten de sorumlu değildir. AİHM, bu sebeple, müdahalenin söz konusu hükme dayandırılamayacağı görüşündedir.[1416]

Başvurucunun web sitesinin engellenmesi, Roskomnadzor'un hukuka aykırı web sitesinin IP adresini yasaklı materyaller siciline eklemesiyle oluşmuştur. Bu karar, DreamHost tarafından barındırılan ve engellenen web sitesi ile aynı IP adresini paylaşan tüm web siteleri üzerinde derhâl etki göstermiştir. Bu durum, Roskomnadzor'un, Bilgi Kanunu'nun 15.1. maddesinin 9. fıkrasına istinaden IP adresini Bütüncül Sicil'e eklemesiyle gerçekleşmiştir. AİHM, inceleme yetkisinin, ilgili devlet kuruluşunun iç hukuktaki mevzuata lafzi uyumuyla sınırlı olmadığının altını çizmiştir.[1417] Mahkeme, ilgili yasanın, başvurucunun davranışlarını düzenleyebilmesine ve keyfî müdahalelere karşı korunmasına imkân verip vermediği yönünden incelenmesi gerektiğini belirtmiştir. Bu doğrultuda, Bilgi Kanunu'nun 15.1. maddesini yasa kalitesi kriteri bağlamında irdelemeye devam etmiştir.

[1414] *Vladimir Kharitonov v. Rusya*, para. 38.

[1415] *Vladimir Kharitonov v. Rusya*, para. 39.

[1416] *Vladimir Kharitonov v. Rusya*, para. 39.

[1417] *Vladimir Kharitonov v. Rusya*, para. 40.

Bilgi Kanunu'nun 15.1. maddesi, erişimin engellenmesi kararları uygulanırken Roskomnadzor'a geniş bir yetki vermektedir. Roskomnadzor, bir web sitesini Bütüncül Sicil'e koyabilir, web sitesi sahibinden ve yer sağlayıcısından hukuka aykırı içeriği kaldırmasını talep edebilir, talep yerine getirilmezse web sitesinin IP adresini Bütüncül Sicil'e ekleyebilir. AİHM, Roskomnadzor'un, IP adresinin birden fazla web sitesi tarafından kullanılıp kullanılmadığını araştırma yükümlülüğünün olmadığının altını çizmiştir.[1418] Bu durum, mevcut davada olduğu gibi engelleme kararlarının hedeflenen içeriği aşmasına sebep olmaktadır. AİHM hem başvurucu hem de müdahiller tarafından işaret edildiği üzere, hukuka aykırı içerik barındıran diğer web siteleriyle aynı IP adresini paylaşmaları sebebiyle milyonlarca web sitesinin engellendiğini vurgulamıştır.[1419]

Paylaşımlı yer sağlama hizmeti, küçük ve orta ölçekli web siteleri için yaygın ve erişilebilir bir yöntemdir. Ancak, bu tür bireysel web sitelerinin sahipleri, beraber hizmet aldıkları web sitelerinin içeriğinden haberdar olamamaktadır. Bu olayda olduğu gibi Rusya'nın yetki alanı dışında bir yerde olan yer sağlayıcı, Rus makamlarının hukuka aykırılık tespitiyle bağlı değildir. Hangi paylaşımlı yer sağlama hizmeti kullanılırsa kullanılsın, Rus makamları barındırılan diğer web sitelerindeki içeriği hukuka aykırı olarak tespit eder ve web sitesi sahipleri ile yer sağlayıcıları içeriği kaldırma taleplerini yerine getirmezse başvurucunun benzer bir durumla karşılaşması kaçınılmaz olacaktır. AİHM, Rus hukukunun başvurucuya, beraber barındırılan diğer web sitelerinin içeriğini kontrol etme veya yer sağlayıcının içerik kaldırma taleplerine uyumunu gözetmekle ilgili bir yükümlülük getirmediğini belirtmiştir.[1420]

AİHM, Roskomondazor'a engelleme konusunda kanunla verilen yetkinin genişliği sebebiyle, başvurucunun kendi web sitesi ile başkasının hukuka aykırı içeriği arasındaki rastlantısal bir altyapı bağlantısının sonucu olarak Rus makamları tarafından alınan engelleme kararının neticesine katlanmak durumunda kaldığını belirtmiştir. Mahkeme, Bilgi Kanunu'nun, etkisi bakımından yeterince öngörülebilir olmadığına ve

[1418] *Vladimir Kharitonov v. Rusya*, para. 41.

[1419] *Vladimir Kharitonov v. Rusya*, para. 41.

[1420] *Vladimir Kharitonov v. Rusya*, para. 42.

başvurucuya davranışlarını düzenleme imkânı tanımadığına karar vermiştir.[1421]

AİHM'nin yasanın niteliğinden sonra incelediği ikinci boyut, kötüye kullanıma karşı koruyucu mekanizmaların varlığıdır. AİHM, bilgiyi yayma hakkına müdahaleye ilişkin yetkilerin kullanılması durumunda bu tür tedbirlerin internetin erişilebilirliğine olan etkilerinin açıkça minimize edilerek çerçevelendirilmesi gerektiğini tekrarlamıştır.[1422]

Mevcut uyuşmazlığa dönen AİHM, uyuşturucu ile mücadele biriminin, hukuka aykırı bir web sitesinin içeriğinin illegal olduğuna ilişkin kararının Roskomnadzor tarafından uygulandığını; hem ilk değerlendirmenin hem de Roskomnadzor'un uygulama kararının, hakları ve menfaatleri etkilenmesi muhtemel kişilerle önceden paylaşılmadığını belirtmiştir.[1423] Keza, engelleme kararı herhangi bir mahkeme veya başka bir bağımsız organca ilgili tarafların müdahil olabileceği şekilde karara bağlanmamıştır. Rus hukuku da engelleme kararları uygulanmadan önce bunların olası etkilerinin değerlendirilmesine ilişkin bir yükümlülük içermemektedir. AİHM, Rus Hükûmetinin Roskomnadzor'un bir IP adresini engellerken bunun muhtemel yan etkilerini araştırmakla yasal olarak yükümlü olmadığına ilişkin savunmasına atıf yapmıştır ki yaygın olarak kullanılan "ters IP adresi inceleme" tekniği gibi internet araçlarıyla aynı sunucuda barındırılan diğer web sitelerinin listelenmesi de mümkündür.[1424]

AİHM, engelleme tedbirinin şeffaflığı meselesini de incelemiştir. Rus Hükûmeti, başvurucunun Roskomnadzor'un web sitesi üzerinden engellemeyi tespit edebileceğini ileri sürmüştür.[1425] Esasında Roskomnadzor tarafından sağlanan ve http://blocklist.rkn.gov.ru adresinde yer alan hizmet aracılığıyla bu tür engelleme kararları detaylı olarak sorgulanabilmektedir. Ancak bu sitede, erişim engelleme kararının tam

[1421] *Vladimir Kharitonov v. Rusya*, para. 42.
[1422] *Vladimir Kharitonov v. Rusya*, para. 43.
[1423] *Vladimir Kharitonov v. Rusya*, para. 43.
[1424] *Vladimir Kharitonov v. Rusya*, para. 43.
[1425] *Vladimir Kharitonov v. Rusya*, para. 44.

metni, engelleme sebebi veya itiraz yollarına ilişkin bilgi yer almamaktadır. Ayrıca, Rus hukuku, engellemenin yan etkileri olması durumunda üçüncü taraflara bildirimde bulunulmasını öngören bir yasal hüküm içermemektedir. AİHM, başvurucunun hiçbir aşamada engelleme kararına erişemediğinin altını çizmiştir.[1426]

AİHM, mevcut uyuşmazlıkta Rus iç hukukunun itirazlara ilişkin mekanizmalarının da gereğince işletilmediğine işaret etmiştir.[1427] Aynı doğrultuda, yerel mahkeme hâkimlerinin başvurucunun şikâyetini ele alırken farklı menfaatleri dikkate almadığını, aynı IP adresini paylaşan tüm web sitelerine erişimin engellenmesinin gerekliliğini değerlendirmediğini belirtmiştir.[1428] *Ahmet Yıldırım v. Türkiye* kararına tekrar atıf yapan AİHM, AİHS ile uyumlu bir denetim mekanizmasında özellikle internette bulunan bilgilerin büyük çoğunluğuna erişimi engelleyen benzer tedbir kararları nedeniyle internet kullanıcılarının haklarına büyük ölçüde zarar verildiğini ve hâkimlerin önemli dolaylı etkiler oluşabileceğini dikkate almaları gerektiğini hatırlatmıştır.

AİHM, bir düzenlemenin, mevcut davadaki gibi, bireyleri aşırı ve keyfî engellemelerin etkisinden koruyacak tedbirleri içermemesi durumunda bu yasal düzenlemenin hukuk devleti ilkesiyle bağdaşmasının mümkün olmadığının altını çizmiştir.[1429] AİHM, hukuka aykırı içeriği engellemenin gerekçelendirilebildiği istisnai durumlarda, engelleme kararını alan devlet kuruluşunun, almış olduğu kararın sadece hukuka aykırı içeriğe yöneldiği ve uygulama yönteminden bağımsız olarak aşırı ve keyfî bir etkisi olmadığını temin etmekle yükümlü olduğunu tekrarlamıştır.[1430] Hukuka uygun içeriğe veya web sitelerine engellemenin bir yan etkisi olarak müdahale eden engelleme tedbiri, bu tür web sitelerinin sahiplerinin haklarına bir müdahale niteliğindedir.

[1426] *Vladimir Kharitonov v. Rusya*, para. 44.

[1427] *Vladimir Kharitonov v. Rusya*, para. 45.

[1428] *Vladimir Kharitonov v. Rusya*, para. 45.

[1429] *Vladimir Kharitonov v. Rusya*, para. 46.

[1430] *Vladimir Kharitonov v. Rusya*, para. 46.

Tüm bu tespitler ışığında AİHM, başvurucunun haklarına müdahalenin Bilgi Kanunu'nun 15.1. maddesindeki engelleme prosedürü sebebiyle gerçekleştiğine; söz konusu hükmün AİHS bağlamında öngörülebilirlik kriterini yerine getirmediğine ve kötüye kullanıma karşı demokratik bir toplumda hukukun üstünlüğünün emrettiği ölçüde güvence içermediğine hükmetmiştir.[1431] Mahkeme, müdahale "kanunla öngörülme" şartını yerine getirmediği için AİHS'nin 10. maddesinin ikinci fıkrasındaki diğer gereklilikler bağlamında inceleme yapılmasına gerek olmadığına karar vermiştir. Sonuç olarak, AİHS'nin 10. maddesinin ihlal edildiğine hükmetmiştir.

10. madde ihlaline ilişkin tespitinden sonra Mahkeme, 13. maddenin ihlal edilip edilmediğini ele almıştır. Başvurucu, Rus mahkemelerinin AİHS'nin 13. maddesinde güvence altına alınan etkili başvuru hakkını ihlal ettiğini ileri sürmüştür.[1432] 13. madde şu şekildedir: *"Bu Sözleşme'de tanınmış olan hak ve özgürlükleri ihlal edilen herkes, ihlal fiili resmî görev yapan kimseler tarafından bu sıfatlarına dayanılarak gerçekleştirilmiş olsa dahi ulusal bir makama etkili bir başvuru yapabilme hakkına sahiptir."* AİHM, açıkça dayanaktan yoksun olmadığına kanaat getirerek bu iddiayı kabul edilebilir görmüştür.[1433]

Rus Hükûmeti, başvurucunun Roskomnadzor'un uyarısına rağmen hareketsiz kalarak hakkının kısıtlanmasına sebep olan İSS veya yer sağlayıcı aleyhine dava açabilecekken bunu yapmadığını ileri sürmüştür.[1434] Başvurucu ise Rusya'da seksen üç bölgede 3.500'den fazla İSS bulunduğunu ve her biri aleyhine bir talepte bulunmanın etkin bir hak arama yolu olmadığını belirtmiştir.[1435] Başvurucu ayrıca İSS'lerin, bir web sitesini alan adı ya da IP adresi üzerinden engelleme seçeneklerine kanunen sahip olduğunu, tercih ettikleri engelleme yönteminin yasaya aykırılık oluşturmayacağını ifade etmiştir. Başvurucu son olarak Rus mahkemele-

[1431] *Vladimir Kharitonov v. Rusya*, para. 46.
[1432] *Vladimir Kharitonov v. Rusya*, para. 48.
[1433] *Vladimir Kharitonov v. Rusya*, para. 49.
[1434] *Vladimir Kharitonov v. Rusya*, para. 50.
[1435] *Vladimir Kharitonov v. Rusya*, para. 51.

rinin engelleme kararlarının ölçülülüğünü değerlendirmeyi reddettiğini iddia etmiştir.

Davaya müdahil olarak görüş beyan eden Article 19 ve Electronic Frontier Foundation, çoğu Avrupa ülkesinde İSS'lerin kendilerine yöneltilen engelleme kararlarına itiraz imkânı olduğunu ve bazı devletlerin bir engelleme kararının yan etkisi sebebiyle mağdur olanlara başvuru yolu tanıdığını beyan etmiştir.[1436] Fransa ve Birleşik Krallık, engellenen web sitelerinin kullanıcılarının bu engelleme kararına itiraz için bilgilendirici bir sayfaya yönlendirilmesine ilişkin düzenlemeler yapmıştır.

Müdahil üçüncü taraflardan Avrupa Bilgi Toplumu Enstitüsü, etkilenen taraflar için hem *ex-ante* hem de *ex-post* hak arama yollarının sunulması gerektiğini belirtmiştir.[1437] *Ex-ante* yollar, yan etki olarak engellemeye konu olan web sitelerinin sahiplerine -ki "ters IP adresi sorgusu" ile tespit edilebilirler- ön bildirim yapılmasını ve bir engelleme kararı uygulanmadan önce itiraz imkânı sağlanmasını içerir. *Ex-post* yollar ise yan etki olarak engellenen web sitesinin sahibine engelleme kararına itiraz imkânı sağlamak, engelleme kararlarını süre ile sınırlandırmak ve aşırı engelleme örneklerini izlemeyi sürdürmektir.

AİHM, AİHS'nin 10. maddesi ile 13. maddesindeki menfaatlerin niteliğine ilişkin bir karşılaştırma yapmıştır.[1438] AİHM'ye göre 13. madde usuli bir koruma sağlarken, diğer bir deyişle etkin bir başvuru hakkını gerekli kılarken, 10. maddenin bünyesindeki usuli koruma ifade özgürlüğünün özüne saygıyı temin etme gibi daha geniş bir amacın yan unsuru niteliğindedir.

Mahkemeye göre, başvurucunun, ifade özgürlüğünün kısıtlandığına dair bir iddiası vardır.[1439] Mahkeme, 13. maddenin, iddia edilen ihlalleri veya devamını önleyen veya vuku bulmuş ihlallere ilişkin uygun tazmin imkânları sağlayan, hem hukuken hem de uygulamada etkili bir yerel bir hak arama mekanizmasını gerektirdiğini hatırlatmıştır.

[1436] *Vladimir Kharitonov v. Rusya*, para. 52.

[1437] *Vladimir Kharitonov v. Rusya*, para. 53.

[1438] *Vladimir Kharitonov v. Rusya*, para. 54.

[1439] *Vladimir Kharitonov v. Rusya*, para. 55.

AİHM'ye göre başvurucunun Roskomnadzor'un engelleme kararına ve bu kararın web sitesine etkisine karşı itiraz imkânı olsa da Rus mahkemeleri şikâyetin esasını incelemeyi reddetmiştir.[1440] Keza, mahkemeler engelleme kararının başvurucunun web sitesi üzerindeki etkilerinin hukukiliğine ve ölçülülüğüne dair bir inceleme yapmamıştır. Tüm bunları dikkate alan AHİM, ulusal hukuk tarafından sağlanan tazmin imkânının başvurucunun davasının koşulları kapsamında etkili olmadığına karar vermiştir.[1441] Bu doğrultuda, AİHS'nin 10. maddesiyle bağlantılı olarak 13. maddesinin de ihlal edildiğine hükmetmiştir.[1442]

VIII. Yargıçlar Lemmens, Dedov ve Poláčková'nın mutabık görüşü

Yargıçlar Lemmens, Dedov ve Poláčková, heyetin AİHS'nin 10 ve 13. maddelerinin ihlaline ilişkin nihai kararına katılmakla birlikte *Vladimir Kharitonov v. Rusya* kararına mutabık görüş yazmışlardır.[1443] Yargıçların, 10. madde ihlaline ilişkin farklı gerekçeleri vardır. Yargıçlar, başvurucunun ifade özgürlüğüne müdahalenin "kanunla öngörülmediği" konusunda heyetle hemfikirdirler. Heyetten farklı olarak, kanunun öngörülebilirlik ilkesini karşılamadığı değil, müdahalenin yerel hukukta dayanağı olmadığı iddiasındadırlar. Yargıçlar, bu görüşlerinin salt teorik bir tartışma olmadığını belirterek görüşlerini izah etmişlerdir.

Bu davaya konu müdahale, Rastaman Tales isimli web sitesine yönelik engelleme kararı sebebiyle gerçekleşmiştir. Başvurucunun web sitesi, www.digital-books.ru, aynı sunucuda barındırılmakta ve aynı IP adresini kullanmaktadır. Roskomnadzor, Federal Uyuşturucuyla Mücadele Dairesi tarafından Rastaman sitesine erişimin engellenmesi talep edilince sitenin IP adresini, engellenen web siteleri siciline eklemiştir. Sonuçta

[1440] *Vladimir Kharitonov v. Rusya*, para. 56.

[1441] *Vladimir Kharitonov v. Rusya*, para. 56.

[1442] *Vladimir Kharitonov v. Rusya*, para. 57.

[1443] *Vladimir Kharitonov v. Rusya*, Yargıçlar Lemmens, Dedov ve Poláčková'nın Mutabık Görüşü.

sadece Rastaman Tales web sitesine değil, başvurucununki dâhil aynı IP adresini kullanan tüm web sitelerine erişim engellenmiştir.

Yargıçlar, uygulanan bu tedbirin Bilgi Kanunu'nun 15.1. maddesinin 5(1) fıkrasına dayandığını belirterek, bu hükme göre maddede sayılan hukuka aykırı içeriklerin (mevcut davada uyuşturucu üretimi ve kullanımına ilişkin bilginin) bir web sitesinde yer alması durumunda, federal bir birim (bu davada Federal Uyuşturucuyla Mücadele Dairesi) engelleme kararı almakta ve bu karar, kararları uygulamaktan sorumlu birim olan Roskomnadzor tarafından uygulanmaktadır.

Yargıçlara Roskomnadzor'un, Rastaman Tales web sitesini engellemek için tamamıyla uygunsuz bir metot kullandığı kanaatindedirler. Yargıçlara göre bu bağlamda sorulması gereken soru şudur: Bu, Bilgi Kanunu'nun 15.1 maddesinin 5(1) fıkrasının etkileri bakımından yeterince öngörülebilir olmamasından mı yoksa Roskomnadzor'un kendisine yasayla tanınan yetkilerini aşmasından mı kaynaklanmaktadır? İlk durum, yasanın gereken kalitede olmadığına işaret eder. İkinci durum ise müdahalenin kanuni dayanağı olmadığını imler.

Yargıçlar, heyetin diğer üyelerinin Bilgi Kanunu'nun Roskomnadzor'u IP adresinin birden fazla web sitesi tarafından kullanılıp kullanılmadığı, IP adresi tekniğiyle engellemeye ihtiyaç duyulup duyulmadığı konusunda bir kontrol yapma yükümlülüğü altına sokmadığı görüşüne atıf yapmışlardır. Diğer üyelere göre, Bilgi Kanunu'nun engelleme konusunda Roskomnadzor'a sağladığı "geniş serbesti", bir web sitesinin başka bir web sitesiyle rastlantısal altyapı bağlantısı sebebiyle engellenmesine imkân tanımaktadır. Yasa, etkileri sebebiyle yeterince öngörülebilir değildir ve başvurucunun kendi davranışlarını düzenlemesine imkân tanımamaktadır.

Yargıçlar Lemmens, Dedov ve Poláčková, yerel mevzuatın bu şekilde yorumlanmasına katılmadıklarını beyan etmişlerdir. Yargıçlara göre, Bilgi Kanunu, bilhassa 15.1. maddesinin 5(1) fıkrası, yasaklı içeriklerin kategorisini ve bu doğrultuda erişimi engellenecek içerikleri açıkça düzenlemiştir. Yargıçlar, bu hükmün yetkili federal makamlara sınırsız bir yetki vermediği düşüncesindedirler.

Yargıçlara göre, Bilgi Kanunu, bir engelleme kararı alındığı zaman Roskomnadzor'un nasıl ilerlemesi gerektiğini düzenlemektedir. Ancak, Yargıçlara göre AİHS, bir idari makamın kararlarının uygulanma şeklinin detaylı olarak bir kanunda düzenlenmesi gerektiğini öngörmemektedir. Bu durum bilhassa teknik nitelikte tedbirler alırken geçerlidir. Yargıçlar, bunun aksini iddia etmenin, istenmeyen aşırı bir düzenlemeye yol açacağı kanaatindedir.

Federal Uyuşturucuyla Mücadele Dairesinin talebini uygulamak için seçilecek metot Roskomnadzor'un takdirindedir. Hukukun üstünlüğü ilkesinin bir neticesi olarak Roskomnadzor seçilen metodun, yetkili idari makamın talebinin sınırları içerisinde kaldığından emin olmalıdır.

Yargıçlara göre, bir kanun idari bir makama takdir yetkisi tanıdığı zaman, bu idari makamın, kendisine tanınan yetkileri kanunu ihlal eder şekilde kullanmaması gerektiği açıktır. Yargıçlar, başvurucunun web sitesinin hukuka aykırı herhangi bir içerik ihtiva etmediği ve Federal Uyuşturucuyla Mücadele Dairesinin talebine de konu olmadığı ortadayken başvurucunun web sitesini engellemeyi netice veren bir metodu kullanan Roskomnadzor'un Bilgi Kanunu'nun 15.1 maddesinin 5(1) fıkrasında tanınan yetkiyi aştığı görüşündedirler. Bu durumun, Roskomnadzor'un uyguladığı engelleme tedbirinin yerel hukukta dayanağı olmadığı anlamına geldiğini beyan etmişlerdir.

Bilindiği üzere, yerel mahkemeler Roskomnadzor'un yetkisi dairesinde hareket ettiğini ve Bilgi Kanunu'yla uyumlu bir kararı uyguladığını belirtmiştir. Yargıçlara göre, söz konusu mahkemeler engelleme tedbirinin başvurucunun web sitesine etkisini ele almamıştır. Bu da karar açısından önemli nitelikte bir ayrıntıdır.

Yargıçlara göre, uygulanan tedbirin yerel hukukta bir dayanağı olmadığını belirlemek tedbirin "kanunla öngörülmediğini" söylemek için yeterlidir. Bu sebeple, Bilgi Kanunu'nun sınırları içerisinde kalmayan Roskomnadzor, başvurucunun haklarının ihlalinden birinci derecede sorumludur. Yargıçlar ayrıca Roskomnadzor'un eylemlerinin hukuka aykırılığına ilişkin belirleme yapmadıkları, AİHS'de belirlenen kriterleri dikkate almada eksiklik gösterdikleri ve hukuka aykırılığı gidermedeki

kusurları sebebiyle yerel mahkemelerin de sorumlu olduğu kanaatindedirler.

Yargıçlar Lemmens, Dedov ve Poláčková, diğer meslektaşlarının suçu başka birisine yükledikleri görüşündedir. Yargıçlar, diğer meslektaşlarının AİHS'nin ihlal edilmesinin kaynağı olarak Bilgi Kanunu'nu gösterdiklerini belirtmiştir. Diğer bir deyişle, Bilgi Kanunu'nun uygulamada yeterince öngörülebilir olmadığından hareketle müdahalenin "kanunla öngörülmediği" görüşündedirler ki Yargıçlar Lemmens, Dedov ve Poláčková buna itiraz etmektedir.

Yargıçlar Lemmens, Dedov ve Poláčková, Bilgi Kanunu'nun bu hâliyle AİHS'ye aykırı olmadığı görüşündedirler. Engelleme ve filtreleme alanında Avrupa Konseyi tarafından gerçekleştirilen mukayeseli çalışmaya atıf yapan Yargıçlar, Bilgi Kanunu'nun diğer Avrupa Konseyi üye devletlerinin aynı konudaki yasalarına çok benzer olduğu görüşündedirler.[1444] Bu bağlamda mevcut davada, asıl sorunun Bilgi Kanunu'nun uygulaması olduğu fikrindedirler.

Peki, bu karar nasıl uygulanmalıdır? Yargıçlara göre ortaya çıkan sorun, başvurucuya has değildir. Bu kararda belirtildiği üzere, milyonlarca web sitesi sadece hukuka aykırı içerik barındıran başka web siteleriyle aynı IP adresini paylaştıkları için engellenmiştir. Sorun sistemsel değilse de yaygın bir sorundur. Yargıçlara göre, idari uygulamayı (Roskomnadzor'un) ve yargısal uygulamayı (yerel mahkemelerin) değiştirmek yeterlidir. Yargıçlar, AİHS bağlamında bir telafiye yasa koyucunun müdahalesi olmaksızın erişilebileceği görüşündedirler. Oysaki Bilgi Kanunu'nun 15.1. maddesinin 5(1) fıkrasının AİHS'nin 10. maddesi bağlamında öngörülebilirlik şartını sağlamadığına ilişkin bir hüküm neticesinde hükmün uygulanabilmesi için Bilgi Kanunu'nun değiştirilmesi gerekecektir. Yargıçlar, bu tür bir değişikliğin makul bir süre içerisinde gerçekleştirileceğini ancak ümit edebileceklerini belirtmişlerdir.

[1444] Söz konusu çalışma için bkz. **Avrupa Konseyi**, "*Filtering, blocking and take-down of illegal content on the Internet*" <https://www.coe.int/en/web/freedom-expression/study-filtering-blocking-and-take-down-of-illegal-content-on-the-internet>

Yargıçlar, Roskomnadzor'un ve mahkemelerin kendi uygulamalarını değiştirmek için bir kanun değişikliği yapılmasını beklememesi gerektiğinin altını bir kez daha çizmişlerdir. Nihayetinde, AİHM'nin kararlarının icra edilmesi ilgili tüm yerel makamların meselesidir. Yargıçlar bu noktada *Fabris v. Fransa* kararından alıntı yaparak yerel mahkemelerin görevinin "*kendi anayasal düzenleriyle uyum içinde, Sözleşme standartlarının Mahkeme tarafından yorumlandığı şekliyle tam etki göstermesini sağlamak*" olduğunu hatırlatmışlardır. Yargıçlar, Roskomnadzor ve mahkemelerin bu suretle Bilgi Kanunu'nun değiştirilmesine giden yolu açabileceklerini belirterek görüşlerini tamamlamışlardır.

IX. Değerlendirme

Vladimir Kharitonov v. Rusya kararı, erişimi engelleme tedbirlerinin yan etkilerinin ele alındığı ve genel hatlarıyla *Ahmet Yıldırım v. Türkiye* kararına benzeyen bir karardır. Kararda, erişimi engelleme amacıyla kullanılan IP engelleme tekniğinin oluşturduğu yan etki, diğer bir deyişle aşırı engelleme ele alınmıştır.

Bu kararın en önemli çıktısı; engelleme kararlarının ölçülü, şeffaf ve hukuken etkili bir şekilde itiraz edilebilir olmasının gerekliliğinin vurgulanmış olmasıdır. Erişimi engelleme amacıyla kullanılan IP tekniği, Dördüncü Bölümde[1445] ele alındığı üzere, İSS'ler için maliyeti en düşük engelleme tekniğidir. Fakat pratikliğinin aksine en ölçüsüz engelleme tekniğidir. Zira, aynı IP adresinde yayın yapan tüm web sitelerini ve diğer internet hizmetlerini erişilmez kılmaktadır.

Bilgi Kanunu'nun 15.1. maddesi katalog bazı içerikler için idari makamlara erişimin engellenmesi kararı alma yetkisi tanımaktadır. Bakıldığı zaman engelleme tedbirinin uygulanmasının dayanağı yasayla öngörülmektedir. Ancak, sorun, kararın Roskomnadzor tarafından uygulandığı aşamada ortaya çıkmaktadır. Roskomnadzor, uyar-kaldır yoluna başvurmakta, bildirime uyulmadığı takdirde IP adresine erişimi engellemek-

[1445] **§4(X)(A)**[IP engellemesi].

tedir. Böyle müdahaleler, Bilgi Kanunu'nu uygulamada öngörülemez kılmaktadır.

Peki, Roskomnadzor'un teknik olarak başka alternatifi var mıdır? Kararın uygulandığı dönemde Rusya'daki internet ağında DPI uygulanıp uygulanmadığı yönünde bir bilgi yer almamaktadır. Dolayısıyla, URL engellemesi için bir yorum yapmak mümkün değildir. Karardan ve engellemeye konu web sitesi incelendiği zaman, web sitesinin tüm içeriğinin hukuka aykırı olarak nitelendirilebileceği anlaşılmaktadır. Bu durumda Roskomnadzor'un IP engellemesi gibi İSS'ler tarafından uygulanması kapsamlı bir teknik altyapı gerektirmeyen DNS engelleme tekniğini kullanması mümkündür. Ancak, Roskomnadzor, IP engellemeyi tercih etmiştir.

Peki, Roskomnadzor'un bu tercihi neticesinde ortaya çıkan müdahale, Bilgi Kanunu'nun öngörülebilirlik kriterini sağlayamamasından mı yoksa Roskomnadzor'un kanundaki yetkiyi açıkça ihlal etmesinden mi kaynaklanmaktadır? Önceki bölümde ele alındığı üzere Yargıçlar Lemmens, Dedov ve Poláčková ikinci görüştedir.

Ahmet Yıldırım v. Türkiye kararından bugüne kadarki tüm içtihatlarda AİHM belirli teknik varsayımlar üzerinden AİHS'nin 10. maddesinin ihlal edildiğine yönelik bir çıkarıma varmaktadır. *Vladimir Kharitonov v. Rusya* kararı da aynı metodolojinin bir ürünüdür. Aslında, Roskomnadzor'un teknik olarak neler yapabileceği tartışılmış olsaydı o noktada Yargıçlar Lemmens, Dedov ve Poláčková'nın görüşlerinin isabetli olacağı daha net oraya çıkacaktı.

Roskomnadzor, telekomünikasyon alanındaki yetkili otorite olarak DNS ve IP engelleme arasında yapılan tercihin etkilerini bilecek konumdadır. Burada IP engelleme tekniğinin bir sosyal tekniğe dönüştürüldüğü, yer sağlama hizmetleri üzerinde bir baskı unsuru hâline geldiği görülmektedir. Sorun Bilgi Kanunu değil, Kanun'un Roskomnadzor tarafından uygulanmasıdır. Yargıçlar Lemmens, Dedov ve Poláčková'nın tespitleri yerindedir.

ALTINCI KISIM

DEĞERLENDİRMELER

§25. AİHM KARARLARI IŞIĞINDA İNTERNET ORTAMININ DÜZENLENMESİ

İnternetin kendine özgü ve dinamik yapısı sebebiyle bu alana ilişkin tüm hususların tek bir kararla veya tek bir içtihatla tespit edilerek sonuca bağlanması mümkün değildir. Her bir karar veya içtihat, internetin bir parçasına veya fonksiyonuna ilişkin çıkarımlar yapılmasına olanak tanımaktadır.

I. Avrupa Konseyi ve internet

Avrupa Konseyinin tavsiye kararları, deklarasyonları, AİHM içtihatları, BM kararları bu alanda günün birinde varılması muhtemel uluslararası konsensüsün, bu alanda akdedilecek bir uluslararası antlaşmanın temelini oluşturacaktır. Yumuşak hukuk kurallarının zamanla bağlayıcı kurallara dönüşmesinin çok fazla örneği bulunmaktadır.

Avrupa Konseyinin tüm tavsiye kararları ve deklarasyonlar kronolojik sıra içinde şu şekilde özetlenebilir:

1999

Avrupa Konseyi, 23 Şubat 1999 tarihinde kabul ettiği İnternette Özel Hayatın Korunmasına İlişkin Tavsiye Kararı'nda, internet kullanıcıları ve internet hizmet sağlayıcıları için ayrı ayrı teknik ve hukuki tavsiyelerde bulunmuştur. Tavsiyeler her türlü bilgi otobanını kapsayacak şekilde hazırlanmış ve genel olarak hizmet sağlayıcıların şeffaflığına vurgu yapmıştır. Avrupa Konseyi, bu tavsiye kararında bilgi otobanlarındaki en temel sorunların anonimlik, veri güvenliği ve mahremiyet olduğunu belirtmiştir.

2000

Avrupa Konseyi, 13 Temmuz 2000 tarihli Arşiv Erişimine Yönelik Bir Avrupa Politikası Hakkında Tavsiye Kararı'nda arşivlere erişim konu-

sunu ele almıştır. Tavsiye kararında arşive erişimin bir hak olarak kabul edilmesi, bu hakkın herkese aynı şekilde kullandırılması, kısıtlamaların sadece kamusal menfaatleri ve kişileri korumak için gerekli olduğu durumlarda uygulanması, tüm kısıtlamaların süreyle sınırlı olması, kısıtlı erişimli belgelere erişim koşullarının herkes için aynı olması gerektiği belirtilmiştir.

2001

Avrupa Konseyinin 5 Eylül 2001 tarihli Siber İçeriğin Öz Düzenlemesine İlişkin Tavsiye Kararı, internet ortamındaki içeriğin sınıflandırılması konusunu ele almıştır. Bu tavsiye kararında zararlı içerik-hukuka aykırı içerik ayrımına değinilmiştir. Karar, hukuka aykırı içeriğin nitelendirilmesinde ulusal ceza mevzuatlarının belirleyici olacağını belirtmiştir. Zararlı içeriğin tanımının ise farklılık gösterebileceğini vurgulamıştır. Zira çocukların fiziksel, ruhsal ve ahlaki gelişimleri için neyin potansiyel anlamda zararlı olarak nitelendirileceği değişkenlik gösterebilen bir husustur. Karar ayrıca etkin şikâyet sistemlerinin sahip olması gereken asgari nitelikleri tanımlamıştır.

2003

2003 yılına gelindiğinde Avrupa Konseyinin gündemine internete erişim konusu girmiştir. 28 Mayıs 2003 tarihli İnternette İletişim Özgürlüğüne İlişkin Deklarasyon'da Konsey, internet ortamındaki iletişime yönelik sınırsız bir ön denetimin istisnai bir durum olarak kalması ve bireylerin internete erişiminin önündeki engellerin kaldırılması gerektiğinin altını çizmiştir. Deklarasyon'a göre kamu otoriteleri, engelleme veya filtreleme gibi genel önlemler vasıtasıyla, sınır tanımayan bir şekilde toplumun bilgiye veya internet ortamındaki diğer iletişim olanaklarına erişiminin önüne geçmemelidir. Bu durum, küçüklerin bulunabileceği okul veya kütüphane gibi yerlerde onların korunması amacıyla filtreleme yapılmasını engellemeyecektir.

2005

Avrupa Konseyi, 13 Mayıs 2005 tarihinde Bilgi Toplumunda İnsan Hakları ve Hukukun Üstünlüğü Deklarasyonu'nu kabul etmiştir. Bu Deklarasyon, Dünya Bilgi Toplumu Zirvesi'nin Tunus Aşamasına Avrupa Konseyinin görüşü olarak sunulmuştur. Deklarasyon'da Avrupa Konseyine üye devletler, bilgi ve iletişim teknolojilerinin, mevcut insan hakları enstrümanlarının aslen geliştiği sosyal, teknolojik ve hukuki ortamı değiştirme potansiyeli taşıdığının farkında olduklarını belirtmiştir. Üye devletler bu tür teknolojilerin, demokratik süreçlerin ayrılmaz parçası olduğunun ve insan haklarının kullanılmasında geniş imkânlar sunabildiğinin, Avrupa İnsan Hakları Sözleşmesi'nde (AİHS) güvence altına alınan tüm hakların bilgi çağında da tamamen geçerli olduğunun ve yeni teknolojik gelişmelerden bağımsız şekilde korunması gerektiğinin altını çizmiştir.

2006

2006 yılında Avrupa Konseyi, çocukların eğitimi konusuna odaklanmıştır. Konsey, 27 Eylül 2006 tarihinde kabul ettiği Yeni Bilgi ve İletişim Ortamında Çocukların Güçlendirilmesi Tavsiye Kararı'nda çocukların bilişim okuryazarlığının artırılmasını, çocukların bilinçlendirilmesini ve bunun üye devletlerin eğitim müfredatlarının bir parçası hâline getirilmesini önermiştir. Tavsiye kararı üye devletleri, çocukların bilgi ve iletişim teknolojileri karşısında güçlendirilmesi için pedagojik içerikler üretmeye, öğrenme araçları oluşturmaya ve araştırma programları geliştirmeye davet etmektedir.

2007

26 Eylül 2007 tarihinde kabul ettiği Yeni Bilgi ve İletişim Ortamında İfade ve Bilgi Özgürlüğünün Geliştirilmesine İlişkin Tavsiye Kararı'nda Avrupa Konseyi, yeni bilgi ve iletişim ortamında ifade ve bilgi özgürlüğünün geliştirilmesi için bireysel kullanıcıların güçlendirilmesi, güvenilir bilgi, esnek içerik oluşturma ve bilgi sürecinde şeffaflığın sağlanması için ortak standartlar ve stratejiler geliştirilmesi; bilgi teknolojileri (BT) altyapılarına makul şekilde erişim, bir kamu hizmeti olarak bilgiye erişim ve

paydaşlar arasında iş birliği konularında üye devletleri eyleme geçmeye çağırmaktadır.

Benzer doğrultuda 7 Kasım 2007 tarihinde kabul edilen İnternetin Kamu Hizmeti Boyutunun Geliştirilmesine Yönelik Önlemlere İlişkin Tavsiye Kararı, hayatın farklı alanlarında farklı amaçlarla kullanılması sebebiyle internetin erişilebilir, makul ücretli, güvenli, güvenilir ve işler olmasına yönelik meşru bir beklentinin oluştuğunu vurgulamış; insan hakları ve demokrasi, erişim, açıklık, çeşitlilik ve güvenlik bağlamında Avrupa Konseyinin paydaş katılımını önceleyen politikalar geliştirmesine yönelik çağrı yapmıştır.

2008

Avrupa Konseyi, 26 Mart 2008 tarihinde kabul ettiği İnternet Filtreleri Bağlamında İfade ve Bilgi Özgürlüğüne Saygının Teşvik Edilmesine Yönelik Tedbirleri İçeren Tavsiye Kararı'nda internet filtrelerine, bunların nasıl kullanıldıklarına ve kapsamlarının ne olduğuna değinmektedir. Tavsiye kararı, üye devletlere, filtreleme alanında minimum standartları geliştirme, kullanım amaçlarına göre filtrelerin etkinlik ve ölçülülüklerini düzenli olarak gözden geçirme ve güncelleme çağrısında bulunmaktadır.

Aynı yıl kabul edilen 20 Şubat 2008 tarihli İnternet Ortamında Çocukların İtibar, Güvenlik ve Mahremiyetlerinin Korunmasına İlişkin Deklarasyon ise ifade özgürlüğünün ve bilgiye erişim hakkının herhangi bir kamusal kısıtlamaya veya sınıra tabi olmaksızın kullanılması gerektiğinin altını çizmiştir. Deklarasyon, Avrupa Konseyine üye tüm devletlerin çocukların haklarının korunmasına yönelik sorumluluğu olduğunu hatırlatarak internette iletişim özgürlüğünün özellikle çocukların haklarına halel getirmemesi gerektiğini tekrarlamıştır.

2009

Avrupa Konseyi, eğitim meselesini 2009 yılında tekrar gündemine almıştır. 8 Temmuz 2009 tarihli Çocukları Zararlı İçeriğe ve Davranışlara Karşı Koruma ve Çocukların Yeni Bilgi ve İletişim Ortamına Aktif Katılımlarını Yaygınlaştırmaya İlişkin Tavsiye Kararı'nda, bilgi ve haber-

leşme ortamlarında küçükleri zararlı içeriklerden korumak ve çocukların medya okuryazarlık becerilerini artırmak suretiyle ifade özgürlüğünü ve insan onurunu korumanın Avrupa Konseyinin bir önceliği olduğu vurgulanmıştır. Kararın ekinde yer alan Rehber'e göre online içeriğin etiketlenmesi çocuklar için güvenli ve güvenlikli alanlar geliştirilmesine katkı sunmaktadır. Ancak bu tür etiketleme inisiyatiflerinin etkinliği ve güvenilirliği bu sistemlerden sorumlu olanların hesap verebilirliklerine ve sistemlerin birlikte çalışabilmesine bağlıdır.

2010

Avrupa Konseyi, internet ağında verilerin dolaşımına ilişkin temel bir ilke olan ağ tarafsızlığını ilk defa 2010 yılında kapsamlı olarak gündemine almıştır. Konseyin 29 Eylül 2010 tarihli Ağ Tarafsızlığı Deklarasyonu'na göre kullanıcılar; internet temelli içeriğe, uygulamaya veya tercih edecekleri hizmetlere bunların ücretli veya ücretsiz olmasından bağımsız olarak istedikleri cihazlarla mümkün olan en geniş kapsamda erişim hakkına sahip olmalıdır. Altyapı veya internete bağlanmak için kullanılan ağdan bağımsız şekilde bu ilke, ağ tarafsızlığı olarak ifade edilmektedir. Avrupa Konseyine göre altyapıya erişim, bu hedefin gerçekleştirilmesi için ön koşuldur.

Avrupa Konseyi, 29 Eylül 2010 tarihinde ayrıca İnternet Protokol Adres Kaynaklarının Kamu Yararına Uygun Yönetimine İlişkin Deklarasyon'u kabul etmiştir. Deklarasyona göre İnternet Protokolü Versiyon 4 (IPv4) adresleri kısıtlı kaynaktır ve tükenme aşamasındadır. Bu durum, internetin genişlemesine ve mevcut çalışabilirliğine risk oluşturmaktadır. Bu sebeple dağıtılmayan veya kullanılmayan IPv4 adreslerinin kamu yararına uygun şekilde yönetilmesi arzu edilmektedir. Deklarasyona göre Avrupa Konseyinin nihai hedefi, herkes tarafından internet kaynaklarına stabil ve sürekli erişiminin sağlanmasıdır.

2011

Avrupa Konseyinde internete ilişkin en yoğun tartışmaların yaşandığı yıl, 2011 yılı olmuştur. Bu yıl internetin farklı bir boyutuna ilişkin muhtelif tavsiye kararları alınmış ve deklarasyonlar yayımlanmıştır.

Avrupa Konseyinin 21 Eylül 2011 tarihinde kabul ettiği Alan Adları ve İsim Dizeleri Bağlamında İfade ve Bilgi Özgürlüğü ile Toplantı ve Örgütlenme Özgürlüğünün Korunmasına İlişkin Deklarasyon'a göre alan adları ve isim dizelerinde yer alan ifadelerin önsel şekilde (*apriori*) ifade özgürlüğü ile bilgi alma ve verme hakkının dışında değerlendirilmemesi gerekmektedir. Nihayetinde bir alan adı veya isim dizesi ve bunların oluşturdukları ifade türleri, barındırılan içerikle ayrılmaz şekilde iç içe geçmiştir. Deklarasyon'a göre internet özgürlüklerine halel gelmemesi için bu konudaki hassasiyetlerin hem Avrupa Konseyine üye devletler nezdinde hem de ICANN ("*The Internet Corporation for Assigned Names and Numbers*") tarafından geliştirilen yeni üst düzey alan adlarında gözetilmesi gerekmektedir.

2005 yılında Tunus'ta gerçekleştirilen Birleşmiş Milletler Dünya Bilgi Toplumu Zirvesi ile alevlenen internet yönetişimi konusu, 2011 yılında tekrar Avrupa Konseyinin gündemine gelmiştir. Konsey, 21 Eylül 2011 tarihinde güncel politik pozisyonunu ortaya koymak amacıyla İnternet Yönetişimi İlkeleri Deklarasyonu'nu kabul etmiştir. Deklarasyon, internette sürdürülebilir, insan merkezli ve hak temelli bir yaklaşımı mümkün kılmak için internet yönetişimi ilkelerini hâkim kılmak gerektiğini belirtmiştir. Deklarasyon bu doğrultuda insan hakları, demokrasi ve hukukun üstünlüğü, çoklu paydaş yönetişimi, devletlerin sorumlulukları, internet kullanıcılarının güçlendirilmesi, internetin evrenselliği, internetin bütünlüğü, merkezî olmayan yönetim, mimari ilkeler, açık ağ, kültürel ve dilsel çeşitlilik konularında temel ilkeler ortaya koymuştur.

Benzer şekilde 21 Eylül 2011 tarihinde kabul edilen Yeni Bir Medya Nosyonuna İlişkin Tavsiye Kararı, internet aracılığıyla yürütülen faaliyetlerin medya faaliyetleriyle kesiştiği noktalarda onları da kapsama alarak medyanın tanımını yeni medya nosyonu altında alabildiğine genişletmiştir. Medyanın teknolojiyle etkileşimi yeni medya nosyonu olarak kavramsallaştırılmıştır.

Aynı doğrultuda 21 Eylül 2011 tarihinde kabul edilen İnternetin Evrenselliğini, Bütünlüğünü ve Açıklığını Koruma ve Geliştirmeye İlişkin Tavsiye Kararı'na göre internet günlük faaliyetler için çok farklı amaçlarla

kullanılmaktadır. İnternet hizmetlerinin erişilebilir, makul fiyatlı, güvenli, güvenilir ve işler olmasında bireylerin haklı beklentileri vardır. Bu beklentiler, devletlere internete ilişkin politikalar geliştirirken genel kamusal yararı dikkatlice gözetme sorumluluğu yüklemektedir. Keza devletlerin de internetin kamu hizmeti değerini korumak ve geliştirmek için en iyi çabanın gösterilmesine yönelik karşılıklı beklentileri vardır.

Son olarak 7 Aralık 2011 tarihinde kabul edilen Özel Olarak İşletilen İnternet Platformları ve Online Hizmet Sağlayıcıları Bağlamında İfade Özgürlüğü ile Toplantı ve Örgütlenme Özgürlüğünün Korunması Deklarasyonu'na göre kamuya sunulan içeriğe müdahale edilmesi veya tüm web sitelerini erişilmez kılmaya yönelik girişimler, ifade özgürlüğü ile bilgi alma ve verme hakkını güvence altına almaya çalışan başta AİHS'nin 10. maddesi ile AİHM'nin ilgili içtihatları olmak üzere uluslararası standartlara göre değerlendirilmelidir. Aynı değerlendirme, belirli menfaat gruplarının etkileşimine yönelik engeller bakımından da yapılmalıdır.

2012

Arama motorları, bilgi toplumundaki artan önemleri sebebiyle Avrupa Konseyinin de gündemine gelmiştir. Konseyin 4 Nisan 2012 tarihli Arama Motorları Bağlamında İnsan Haklarının Korunmasına İlişkin Tavsiye Kararı, arama motorlarının dünya genelinde bilgi almak, tartışmalara katkı sunmak ve demokratik süreçlere katılmak için bilginin, fikirlerin ve diğer içeriklerin araştırılması, alınması ve dağıtımına imkân tanıdığını belirtmiştir. İnternetin kamu hizmeti niteliğine ilişkin 2007 yılındaki kararı hatırlatan Tavsiye Kararı, internete erişimdeki önemlerine binaen arama motorlarının internet ortamında yer alan, kamuya açık ve dış erişimi amaçlanan içeriği serbestçe tarayıp indekslemesine izin verilmesinin önemli olduğunu vurgulamıştır.

Arama motorlarıyla birlikte sosyal medyanın insan hakları bağlamında düzenlenmesi de Avrupa Konseyinin politik radarına girmiştir. Avrupa Konseyi 4 Nisan 2012 tarihinde Sosyal Ağ Hizmetleri Bağlamında İnsan Haklarının Korunmasına İlişkin Tavsiye Kararı'nı kabul etmiştir. Tavsiye kararına göre sosyal ağ veya yaygın adıyla sosyal medya, insan haklarından faydalanmayı mümkün kılmanın yanında demokrasi için

katalizör görevindedir. Öyle ki bireyler arasında ifade ve haberleşmenin ve ayrıca kitle iletişimi veya genel olarak kitle haberleşmesinin de aracı konumundadır.

Tavsiye kararına göre sosyal ağlar, daha geniş halk kitlelerinin bilgiyi alma ve yaymasına yardımcı olmakta; bireylerin politik, sosyal ve kültürel hayata katılımını geliştirmektedir. Aynı doğrultuda, sosyal ağ, internetin kamu hizmeti değerinin bir uzantısı olması sebebiyle demokrasiyi ve sosyal katılımı kolaylaştırmaktadır.

Tavsiye kararı, sosyal ağların sadece sunduğu fırsatlara değil ayrıca oluşturduğu tehdit ve risklere de işaret etmiştir. Tavsiye kararına göre sosyal ağlarda ifade ve bilgi özgürlüğü, özel yaşam hakkı ve insan onuru ihlal edilebilir ve sosyal medya, ayrımcı uygulamalara ev sahipliği yapabilir. Tavsiye kararına göre bu tür tehditler, bireylerin dışlanmasına yol açan süreçleri kapsayan uygun hukuki ve usule ilişkin korumaların yokluğundan kaynaklanmaktadır. Tavsiye kararı, sosyal ağ hizmetlerinin kişilerin hak ve özgürlüklerine saygı göstermesi gerektiğine ilişkin çağrıda bulunmuştur.

2014

Avrupa Konseyinin internete ilişkin en kapsamlı politik metni, 16 Nisan 2014 tarihli İnternet Kullanıcıları İçin İnsan Hakları Rehberi'dir. Avrupa Konseyi bu rehberde, üye devletlerin insan haklarına saygı gösterme, insan haklarını koruma ve yaygınlaştırma yükümlülüklerinin özel şirketlerin denetlenmesini de kapsadığını belirtmiştir. Rehbere göre evrensel ve bölünemez olan insan hakları ve bununla ilgili standartlar, herhangi bir özel sektör oyuncusunun internet kullanıcıları üzerine yükleyeceği genel şart ve kuralların üzerindedir.

Keza rehbere göre, internete ilişkin tüm süreçlerde AİHS ve AİHM'nin ilgili içtihatlarının dikkate alınması gerekmektedir. Ayrıca, internete uygulanacak tür türlü kısıtlama yasa ile öngörülmeli, demokratik bir toplumda geçerli bir amaca ulaşılması için gerekli ve orantılı olmadır. Rehber, hak ve özgürlüklerinin kısıtlandığını veya haklarının ihlal edildiğini düşündüklerinde internet kullanıcılarının etkili yasal çözümlere

erişimlerinin temin edilmesini, devlet ve devletler dışındaki aktörlerle koordinasyonun yaygınlaştırılmasını, devlet yetkilileri ve sivil toplumla etkin bir diyaloğun teşvik edilmesini, ayrıca tavsiye etmektedir.

2015

Avrupa Konseyi, erişimin engellenmesi uygulamalarının artışının oluşturduğu riskleri dikkate alarak 1 Nisan 2015 tarihinde Bilginin İnternet Ortamında Sınır Ötesine Serbestçe Akışına İlişkin Tavsiye Kararı'nı kabul etmiştir. Tavsiye kararına göre internet trafiğine kasıtlı veya kasıtsız müdahale eden veya internet içeriğine yahut hizmetlerine ülke içinde sınırlamalar getiren ulusal politikalar, önlemler, ticari faaliyetler, teknolojik uygulamalar o devletin sınırları dışında ifade özgürlüğü ile toplantı ve örgütlenme haklarının kullanımı üzerinde de sonuçlar doğurabilir. Tavsiye kararı, bu durumda başka bir devletin egemenlik hakkının etkilenebileceğinin altını çizmiştir.

Tavsiye kararı, uluslararası ortak bir anlayış geliştirilmesi gerektiğini, internet ortamında bilginin sınır ötesine serbest akışına ilişkin kuralların konsolide hâle getirilmesinin zorunlu olduğunu, tüm bunlar yapılırken çocukların online ortamlarda korunmasına, siber suçlarla mücadeleye ve kişisel verilerin korunmasına ilişkin uluslararası sözleşmelerle uyumun temin edilmesi gerektiğini belirtmiştir.

2016

Ağ tarafsızlığı, önemi sebebiyle 2010 yılından sonra 2016 yılında da Avrupa Konseyinin gündemine tekrar gelmiştir. 13 Ocak 2016 tarihinde kabul edilen Ağ Tarafsızlığı Bağlamında İfade Özgürlüğü Hakkı ile Özel Hayat Hakkının Korunması ve Geliştirilmesine İlişkin Tavsiye Kararı, Avrupa Konseyinin ağ tarafsızlığına ilişkin güncel yaklaşımını ortaya koymuştur. Ağ tarafsızlığı ilkesi, internet trafiğinin ayrımcılık yapılmaksızın işlerliği, kullanıcıların bilgi alma ve yayma hakkı ile dilediği hizmeti kullanma hakkı üzerine kuruludur. AİHS'nin 10. maddesinin, bilginin sadece içeriğini değil mecrasını da güvence altına aldığını belirten tavsiye kararı, ağ tarafsızlığının, teknik yenilikçiliği ve ekonomik gelişmeyi desteklediğini belirtmiştir.

Aynı yıl kabul edilen 13 Nisan 2016 tarihli İnternet Özgürlüğüne İlişkin Tavsiye Kararı ise internet özgürlüğünü tanımlamış ve bu bağlamda kullanılabilecek göstergeleri ortaya koymuştur. Tavsiye kararında internet özgürlüğü; insan hakları ve temel özgürlüklerin internet ortamında AİHS'ye ve Kişisel ve Siyasal Haklar Uluslararası Sözleşmesi'ne uygun şekilde icrası, kullanılması ve korunması olarak tanımlanmıştır. Tavsiye kararı ulusal, bölgesel veya küresel tüm internet yönetişimi düzenlemelerinin internet özgürlüğü anlayışının üzerine inşa edilmesi gerektiğini belirtmektedir. Keza devletlerin internet özgürlüğü için uygun ortamı hazırlamakla yükümlü olduğu ifade edilmektedir.

2018

Avrupa Konseyinin internete ilişkin son metni ise 7 Mart 2018 tarihli İnternet Aracı Platformlarının Rolleri ve Sorumluluklarına İlişkin Tavsiye Kararı'dır. Tavsiye kararına göre yaygın, çeşitli ve hızla değişen nitelikte "internet aracıları" olarak adlandırılan oyuncular, çeşitli işlev ve hizmetler sunmak ve sağlamak suretiyle internette gerçek ve tüzel kişiler arasındaki etkileşimi kolaylaştırmaktadır. Aracı platformları tanımladıktan sonra tavsiye kararı, hukukun üstünlüğünün hem insan haklarının korunması ve geliştirilmesi hem de çoğulcu ve katılımcı demokrasi için bir ön koşul olduğunu belirtmiştir.

Sonuç olarak, tüm bu metinler birlikte değerlendirildiğinde Avrupa Konseyinin internete ilişkin dengeli bir yaklaşım ortaya koyduğu söylenebilir. Konseyin temel regülasyon paradigması, klasik düzenleme değil öz düzenleme (*self-regulation*) ve ortak düzenleme (*co-regulation*) yöntemleridir. Konsey, hizmet sağlayıcılara, platformlara veya arama motorlarına belirli konularda sorumsuzluklar ve muafiyetler tanırken bunun karşılığında kullanıcılar için etkin bir hak arama mekanizması kurmalarını zorunlu tutmaktadır. Bu suretle internet ortamında sınır içi ve sınır dışı veri akışının devamını ve hizmetlerin kesintisiz sürdürülmesini teminat altına almaya çalışmaktadır.

II. AİHM ve internet

AİHM, farklı tarihlerde, internet ortamının düzenlenmesi ve sorumluluk konusuna ilişkin kararlar vermiştir. Aşağıda tüm kararlar kısaca özetlenmeye çalışılacaktır.

Ahmet Yıldırım v. Türkiye

Ahmet Yıldırım v. Türkiye kararı, üçüncü kişiye uygulanan içeriğe erişimi engelleme tedbiri neticesinde başvurucunun web sayfasının engellenmesinin AİHS'nin 10. maddesine aykırılığı iddiasıyla yapılan bir başvuruyu konu almaktadır. Google Sites sitesinde yer alan ve Atatürk'e hakaret içeren bir blog sayfasını engellemek için tüm Google Sites hizmeti engellemiş, yerel mahkemeler daha az müdahaleci bir tedbirin uygulanabilirliğini araştırmamıştır.

AİHM, tüm web sitesine yönelik engelleme tedbirini demokratik toplum gerekliliklerine uygun bulmamış, müdahaleyi keyfî müdahale olarak nitelendirmiş ve yargısal denetimin etkin olmamasını AİHS'ye aykırı bulmuştur. Mahkemeye göre "*[b]elirli bir siteye erişimin engellenmesine ilişkin tedbir kararının genel bir engelleme aracı olarak kullanılmasını önlemek için iç hukukta herhangi bir güvence sunulmamaktadır.*" Mahkeme, AİHS'nin 10. maddesinin ihlal edildiğine hükmetmiştir.

Akdeniz v. Türkiye

Akdeniz v. Türkiye kararının konusunu, telif haklarının korunması sebebiyle içeriğe uygulanan tedbirin yan etkisi olarak hukuka uygun içeriğe erişimin de engellenmesinin AİHS'nin 10. maddesini ihlali ettiği iddiası oluşturmaktadır. Telif haklarını ihlal eden içerikler sebebiyle myspace.com ve last.fm siteleri engellenmiştir. Söz konusu sitelere erişememenin bilgi alma özgürlüğünün ölçüsüzce kısıtlanması anlamına geldiği iddiasıyla yapılan başvuruda AİHM, "bilgi alma özgürlüğü" ve "telif hakkının korunması" gibi çatışan menfaatlerin dengelenmesi konusunda yerel mahkemelerin geniş bir takdir yetkisine sahip olduğu, platformun ikame edilebilirliği, salt internet kullanıcısı olmanın AİHS'nin 34. maddesi bağlamında mağdur sıfatı vermeyeceği gerekçeleriyle başvuruyu kabul

edilmez (kişi bakımından/*ratione personae*) bulmuştur. Diğer bir deyişle AİHM, AİHS'nin 34. maddesi bağlamında mağdur sıfatını dar yorumlamıştır.

Cengiz ve Diğerleri v. Türkiye

Cengiz ve Diğerleri v. Türkiye kararı, hem erişimin engellenmesi hem de internete müdahale durumlarında mağdur sıfatının AİHM gündemine tekrar geldiği bir karardır. Mahkeme, öncelikle aktif kullanıcı-pasif kullanıcı ayrımı ve bununla bağlantılı olarak platformun ikame edilip edilemeyeceği değerlendirmesi yapmıştır. Mağdur sıfatını bu kararda daha geniş yorumlayan AİHM, başvuruyu kabul edilebilir görmüştür. YouTube sitesinde yer alan hukuka aykırı bir video sebebiyle YouTube sitesinin tamamına erişimin engellenmesine ilişkindir. AİHM, yerel düzenlemenin battaniye bir engellemeye ilişkin açık hüküm içermemesi ve yerel makamların engellemenin yan etkilerini (hukuka uygun bilginin de erişilmez kılınması) değerlendirmemiş olması sebebiyle AİHS'nin 10. maddesinin ihlal edildiğine hükmetmiştir.

Delfi AS v. Estonya

Delfi AS v. Estonya kararı platformların sorumluluğu açısından önemli bir kırılma noktasıdır. Başvurunun konusunu, anonim üçüncü taraflarca yazılan hukuka aykırı yorumlar sebebiyle internet haber sitesinin zararlardan hukuken sorumlu tutulması oluşturmaktadır. AİHM, ekonomik amaçlı internet haber portalının, kullanıcı yorumlarındaki nefret söylemi ve şiddete teşvik niteliğindeki içeriği proaktif şekilde filtreleme yükümlülüğü olduğunu, nefret söylemi ve şiddete teşvik içeriğinin kaldırılmasının "özel sansür" (*private censorship*) olarak nitelendirilemeyeceğini, kullanıcı yorumlarından dolayı internet haber portalının tazminat ödemesinin ifade özgürlüğüne ölçüsüz bir müdahale niteliğinde olmadığını belirterek AİHS'nin 10. maddesinin ihlal edilmediğine hükmetmiştir. Bu kararla, AİHM internet platformlarının veya genel ifadeyle hizmet sağlayıcılarının güvenli liman ve sorumsuzluk rejimine ilişkin kurallardan radikal sapma niteliğinde bir içtihat geliştirmiştir. Kararın artçı şokları sürmektedir.

Kalda v. Estonya

Kalda v. Estonya kararı, hapishanelerde sunulan internet hizmetinde belirli web sitelerine (mahkeme kararı veri tabanı) erişimin engellenmesinin AİHS'nin 10. maddesine aykırılığı iddiasına ilişkindir. AİHM, internete erişimi temel bir hak olarak nitelendirmiş, bazı bilgilerin sadece internette yer alıyor olmasına dikkat çekmiştir. Mahkeme, başkalarının hak ve menfaatleri ile kamu düzeninin korunmasını ve suç işlenmesinin önlenmesini meşru amaçlar olarak görmekle birlikte belirli sitelere erişimi açmanın oluşturacağı güvenlik riskleri ve maliyet değerlendirilmeden talebin doğrudan reddedilmesini AİHS'nin 10. maddesinin ihlali niteliğinde görmüştür.

MTE ve Index.hu Zrt v. Macaristan

MTE ve Index.hu Zrt v. Macaristan kararı, *Delfi AS v. Estonya* kararı ile oluşturulan platform sorumluluğu içtihadının tekrar test edildiği bir karardır. Başvurunun konusu, bir internet haber sitesinde yer alan yorumlar sebebiyle bir şirketin ticari itibarının zedelendiği gerekçesiyle haber sitesinin üçüncü taraflara ait yorumlardan dolayı objektif olarak sorumlu tutulmasının AİHS'nin 10. maddesini ihlal ettiği iddiasıdır. *Delfi AS v. Estonya* kararından farklı olarak nefret söylemi ve şiddete teşvik içeriğinin söz konusu olmaması, genel kaba ifadelerin yer alması sebebiyle bu kez AİHM farklı bir karara hükmetmiştir. AİHM, (1) yorumların bağlamı, (2) başvurucu şirket tarafından hakaret içeren yorumların önlenmesi için uygulanan tedbirler, (3) aracı platforma alternatif olarak gerçek yazarların sorumluluğu, (4) başvurucu şirket aleyhine sürdürülen yerel yargılamaların neticeleri gibi kriterleri somut olaya uygulamıştır. Neticede somut uyuşmazlıktaki uyar-kaldır mekanizmalarının ve hukuka aykırılığın giderilmesine yönelik diğer mekanizmaların etkinliği platformun kullanıcı yorumlarından sorumluluğu hususunda belirleyici olmuştur. AİHM, bu doğrultuda AİHS'nin 10. maddesinin ihlal edildiğine hükmetmiştir.

Jankovskis v. Litvanya

Jankovskis v. Litvanya kararı, *Kalda v. Estonya* içtihadının tekrar test edildiği bir karardır. Kararın konusunu hapishanelerde sunulan internet erişiminde belirli web sitelerine (eğitim sitesi) erişimin engellenmesinin AİHS'nin 10. maddesine aykırılığı iddiası oluşturmaktadır. AİHM, mahkûmiyetin genel olarak belirli haklardan yoksunluğa yol açtığını kabul etmektedir. Ancak Mahkeme, başkalarının hak ve menfaatlerinin korunması ile kamu düzeninin korunması ve suç işlenmesinin önlenmesini meşru amaçlar olarak görmesine rağmen, belirli sitelere erişimi açmanın oluşturacağı maliyet değerlendirilmeden erişim talebinin yetkili makamlar tarafından doğrudan reddedilmesini bir hukuka aykırılık hâli olarak görmüştür. Sorun, engellemeden ziyade engelleme kararının alınış şekli, takdir yetkisinin kullanılma yöntemi, alternatif erişim ihtimallerinin değerlendirilmemesi, müdahalenin bu bağlamda demokratik toplumda gerekli görülmemesidir. AİHM, bu doğrultuda AİHS'nin 10. maddesinin ihlal edildiğine hükmetmiştir.

Rolf Anders Daniel Pihl v. İsveç

Rolf Anders Daniel Pihl v. İsveç kararının konusunu, bir blog sayfasındaki kişilik haklarını ihlal eden bir kullanıcı yorumundan blog sayfasının sahibinin sorumlu tutulmamasının AİHS'nin 8. maddesine aykırılık teşkil ettiği iddiası oluşturmaktadır. Temel sorun, başvuranın özel hayatının korunması bakımından yerel mahkemelerin sundukları korumanın yetersizliği iddiasıdır. Hem *Delfi AS v. Estonya* hem de *MTE ve Index.hu Zrt v. Macaristan* içtihadına çapraz atıf yapan AİHM, filtrelenmemiş yorumların hukuka aykırı nitelikte olabileceğini, bunlar nedeniyle platformu sorumluluk altına sokmanın, pratik olmayan, aşırı bir öngörü/tedbir gerektiren ve hâliyle internet ortamında bilgiye erişim hakkına halel getiren bir yaklaşım olduğunu belirtmiştir. Mahkeme, çatışan hakların dengelenmesinde blog sayfasının yöneticisinin AİHS'nin 10. maddesinde güvence altına alınan ifade özgürlüğü hakkının ağır bastığına karar vermiştir. Bu karara varılırken uyar-kaldır mekanizmalarının etkinliği önemli rol oynamıştır. Diğer bir deyişle, platformlar, portallar veya haber siteleri ne kadar etkin hak arama mekanizması sunuyorsa o kadar az hu-

kuki sorumluluk söz konusu olacaktır. AİHM, sonuç olarak AİHS'nin 8. maddesinin ihlal edilmediğine hükmetmiştir.

Tamiz v. Birleşik Krallık

Tamiz v. Birleşik Krallık başvurusunun konusu *Rolf Anders Daniel Pihl v. İsveç* kararının konusuna benzemektedir. Başvurunun konusu, blogger.com sitesinde yer alan içerik sebebiyle Google Inc. şirketine yöneltilen tazminat talebinin kabul edilmemesinin AİHS'nin 8. maddesini ihlal ettiği iddiasıdır. AİHM, haklar arasında gerekli dengelemeyi yapan yerel mahkemelerin "gerçek ve esaslı" bir haksız fiil olmadığı tespitinin yerindeliğine işaret etmiştir. Mahkeme, bilgi toplumunda hizmet sağlayıcıların bilgiye erişimi kolaylaştırmadaki önemli rolü karşısında, AİHS'nin 10. maddesindeki ifade özgürlüğü hakkının somut olaydaki koşullar bağlamında AİHS'nin 8. maddesine nazaran daha üstün bir hak olması sebebiyle 8. maddenin ihlal edilmediğine hükmetmiştir.

M.L. ve W.W. v. Almanya

M.L. ve W.W. v. Almanya kararı, AİHM'nin unutulma hakkıyla ilgili vermiş olduğu ilk karardır. Başvurunun konusunu, basının online arşiv içeriklerinde suç faillerinin isimlerini anonimleştirmeyi reddetmesinin AİHS'nin 8. maddesini ihlal ettiği iddiası oluşturmaktadır. Konu, içeriğin silinmesi değil anonimleştirilmesi talebidir. AİHM, yerel makamların çatışan menfaatleri dengelemede sahip olduğu takdir yetkisine işaret etmiş; yayımlandığı tarihte hukukiliği tartışma konusu olmayan haber raporlarına erişimin muhafaza edilmesinin önemini ve başvuranların basına yönelik hareketlerini dikkate alarak taleplerinin Alman Federal Mahkemesi tarafından yerine getirilmemesi sonucunda Alman Devletinin başvuranların özel hayatlarına saygı haklarını korumaya yönelik pozitif yükümlülüğünü ihlal etmediğine hükmetmiştir. Bu doğrultuda AİHS'nin 8. maddesinin ihlal edilmediğine karar verilmiştir.

Magyar Jeti Zert v. Macaristan

Magyar Jeti Zert v. Macaristan kararının konusunu, hakaret ihtiva eden içeriğe bağlantı sağlamasından dolayı online haber sitesinin sorumlu

tutulmasının AİHS'nin 10. maddesini ihlal ettiği iddiası oluşturmaktadır. Bu karar, bağlantı verilen içerikten dolayı sorumluluğun ve genel olarak internet hukukunun temel ilkelerinin en kapsamlı tartışıldığı karardır. AİHM, bağlantılardan sorumlu tutulmayı bütünüyle reddetmemektedir. Bilakis, belirli koşullarda üçüncü taraflara ait bağlantılardan dolayı sorumluluğun doğabileceğini kabul etmektedir. AİHM, *Magyar Jeti Zrt v. Macaristan* kararında bir sorumluluk kriteri geliştirmiştir. Buna göre bağlantıdan sorumlu tutulabilmek için şu soruların yanıtlanması gerekmektedir: (i) Gazeteci, ihtilaflı içeriği benimsemekte midir? (ii) Gazeteci, benimsemeden ihtilaflı içeriği tekrarlamış mıdır? (iii) Gazeteci, ihtilaflı içeriği benimsemeden veya tekrarlamadan sadece içeriğe bağlantı mı sağlamıştır? (iv) Gazeteci, içeriğin hakaret içerdiğini veya hukuka aykırı olduğunu bilmekte midir veya biliyor olması kendisinden beklenebilir mi? (v) Gazeteci, gazeteciliğin etik kuralları bağlamında iyi niyetle hareket etmiş ve sorumlu bir gazeteciden beklenen özeni göstermiş midir? AİHM, yerel mahkemelerin başvuran şirketler üzerine objektif sorumluluk yüklemesinin makul ve yeterli sebeplere dayanmadığına, bu tür objektif bir sorumluluğun internet ortamında bilginin akışı üzerinde öngörülebilir olumsuz etkileri olacağına, haber yazarlarının ve yayıncıların, üzerinde kontrolleri olmayan değişebilir içerikli materyallere bağlantı sağlamaktan çekineceğine, doğrudan veya dolaylı olarak internet ortamında ifade özgürlüğü üzerinde caydırıcı etki doğuracağına işaret etmiş ve ifade özgürlüğü üzerinde ölçüsüz bir müdahale teşkil ettiğine hükmetmiştir. AİHM, bu doğrultuda AİHS'nin 10. maddesinin ihlal edildiğine karar vermiştir.

Høiness v. Norveç

Høiness v. Norveç kararının konusunu, internet haber sitesinin anonim üçüncü taraflarca yayımlanan cinsiyetçi yorumlardan hukuken sorumlu tutulmamasının AİHS'nin 8. maddesine aykırılık teşkil ettiği iddiası oluşturmaktadır. Başvurucu, bir online tartışma platformunda yayımlanan yorumları gereğince önlemedikleri veya hızlıca kaldırmadıkları gerekçesiyle açtığı bir tazminat davasında yerel mahkemelerin bazı basın kuruluşları ve editörlerini tazminata mahkûm etmemesi sebebiyle AİHS'nin 8. maddesinde güvence altına alınan özel hayata saygı hakkının ihlal edildiğini iddia etmiştir. AİHM, yerel mahkemelerin ihtilafın tüm

boyutlarını takdir yetkileri kapsamında gereğince değerlendirdiklerini, başvuranın hakları ile haber portalı ve tartışma forumlarının sağlayıcısının hakları arasında gerekli dengeyi gözettiklerini belirtmiş ve *Rolf Anders Daniel Pihl v. İsveç*, *Tamiz v. Birleşik Krallık* içtihatlarıyla uyumlu şekilde, AİHS'nin 8. maddesinin ihlal edilmediğine hükmetmiştir.

Kablis v. Rusya

Kablis v. Rusya kararının konusunu, toplantı ve gösteri hakkına ilişkin içeriklere ve sosyal medya hesabına erişimin savcılık kararıyla engellenmesi sebebiyle AİHS'nin 10. maddesinin ihlal edildiği iddiası oluşturmaktadır. AİHM, internet içeriğine müdahalede en az kısıtlayıcı yöntemin tercih edilmesi gerekliliğine işaret ederek iç hukuktaki düzenlemenin, önleyici tedbirlerin istismar edilmesini önlemek için gerekli teminatlardan uzak olduğunu tespit etmiştir. AİHM, yerel mahkemeler tarafından uygulanan standartların AİHS'nin 10. maddesinde vücut bulan ilkelerle uyumlu olmadığına ve başvuranın ifade özgürlüğüne müdahale için "ilgili ve yeterli" gerekçeler sunmadığına karar vermiştir. Mahkeme, AİHS'nin 10. maddesinin ihlal edildiğine hükmetmiştir. Bu karar, *Ahmet Yıldırım v. Türkiye* kararından beri geliştirilmiş olan içtihatlarla uyumlu bir karardır.

Bulgakov v. Rusya

Bulgakov v. Rusya kararının konusunu, hukuka aykırı bir web sayfası sebebiyle tüm web sitesine erişimin engellenmesi ve içerik kaldırılmasına rağmen engellemenin devam etmesinin AİHS'nin 10. maddesine aykırılık teşkil ettiği iddiası oluşturmaktadır. Uyuşmazlığın temelinde, aşırılıkçı bir içeriğe uygulanan engelleme kararı sebebiyle tüm web sitesine erişimin, IP engelleme tekniğiyle tamamen engellenmesi yatmaktadır. AİHM, "web sitesi" ile "web sayfası" ayrımı yapılmaması, daha az müdahaleci nitelikte bir tedbire yönelik araştırma gerçekleştirilmemesi, engellemeye konu web sitesinin sahibine şeffaf bir bilgilendirme yapılmaması, başvurucunun engelleme gerçekleşene kadar web sitesi aleyhine alınan karardan haberdar olmaması, hukuka aykırı içerik yayından kaldırıldıktan sonra dahi tüm web sitesine erişimin engellenmesi tedbirinin devam etmesi, yerel düzenlemenin aşırı ve keyfî etkileri, yerel düzenlemenin

kötüye kullanımı önleyecek bir mekanizma içermemesi sebepleriyle ve müdahalenin kanunla öngörülme şartını yerine getirmediği gerekçesiyle AİHS'nin 10. maddesinin ihlal edildiğine hükmetmiştir. AİHM'nin bu kararı, *Ahmet Yıldırım v. Türkiye* kararından beri geliştirmiş olduğu içtihatlarla uyumlu bir karardır.

Engels v. Rusya

Engels v. Rusya kararının konusunu, web sitesine erişimin engellenmesini aşma yöntemi olarak kullanılan araçlara ilişkin bilgi veren içeriğin kaldırılmasına mecbur edilen başvurucunun, AİHS'nin 10. maddesinin ihlal edildiği iddiası oluşturmaktadır. Başvurucunun web sitesinde yer alan internette filtresiz gezinti teknolojilerine ilişkin bilgiler, bir mahkeme kararıyla yasaklı içerik olarak nitelendirilmiş ve başvurucudan içeriği kaldırması talep edilmiştir. Başvurucu, bu talebi yerine getirmiş ve akabinde ilgili hak arama mekanizmalarını işletmiştir. AİHM, herhangi bir bilgi teknolojisinin demokratik bir toplumun temel ilkeleriyle bağdaşmayan bir amaç için kullanılmak üzere dönüştürülmesinin her zaman mümkün olduğu, yerel düzenlemenin bireyleri engelleme kararlarının aşırı ve keyfî etkilerinden koruyacak mekanizmalar içermediği, AİHS bağlamında kanuni öngörülebilirlik şartını taşımadığı, kötüye kullanıma karşı başvurucuya demokratik bir toplumda beklenen şekilde bir güvence sağlanmadığı sebepleriyle ve müdahalenin kanunla öngörülme şartını yerine getirmemesi gerekçesiyle AİHS'nin 10. maddesinin ihlal edildiğine hükmetmiştir.

OOO Flavus ve Diğerleri v. Rusya

OOO Flavus ve Diğerleri v. Rusya kararının konusunu, muhalif bir online haber sitesine erişimin gerekçesiz şekilde engellenmesinin AİHS'nin 10. maddesinin ihlali olduğu iddiası oluşturmaktadır. İhtilafın odak noktasında, engellemenin, hukuka aykırı olduğu iddia edilen web sayfasının URL adresi yerine web sitesinin tam alan adı belirtilerek uygulanması yatmaktadır. Başvurucular hangi içeriğin hukuka aykırı olduğu kendilerine bildirilmediği için o içeriği tespit edip kaldıramamış ve engellemeden kaçınamamışlardır. Keza, içerik kaldırıldıktan sonra da erişimin engellenmesi tedbiri devam etmiştir. AİHM, yerel düzenlemenin, bireyleri, en-

gelleme kararlarının aşırı ve keyfî etkilerinden koruyacak mekanizmalar içermemesi ve müdahalenin demokratik bir toplumda gerekli olan meşru bir amacı gütmemesi gerekçesiyle AİHS'nin 10. maddesinin ihlal edildiğine hükmetmiştir. AİHM'nin bu kararı da *Ahmet Yıldırım v. Türkiye* kararından beri geliştirmiş olduğu içtihatlarla uyumlu bir karardır.

Vladimir Kharitonov v. Rusya

Vladimir Kharitonov v. Rusya kararının konusu, bir web sitesine uygulanan erişimi engelleme kararı sebebiyle bu siteyle aynı IP adresini kullanan bir başka web sitesinin de otomatik olarak engellenmesinin AİHS'nin 10. maddesine aykırılık teşkil ettiği iddiasıdır. AİHM, yerel düzenlemenin, bireyleri engelleme kararlarının aşırı ve keyfî etkilerinden koruyacak mekanizmalar içermemesi, AİHS bağlamında kanuni öngörülebilirlik şartını taşımaması, başvurucuya kötüye kullanıma karşı demokratik bir toplumda beklenen şekilde bir güvence sağlamaması sebebiyle ve müdahalenin kanunla öngörülme şartını yerine getirmediği gerekçesiyle AİHS'nin 10. maddesinin ihlal edildiğine hükmetmiştir. AİHM'nin bu kararı, *Ahmet Yıldırım v. Türkiye* kararından beri geliştirmiş olduğu içtihatlarla uyumlu bir karardır.

III. İdeal bir internet yasası nasıl olmalıdır?

AİHM, internet içeriğine erişimin engellenmesi, içeriğin kaldırılması veya içerikten platformun yahut kullanıcıların sorumlu tutulmasını temelde reddetmemektedir. Bilakis Mahkeme, içtihatlarıyla belirli kriterler geliştirerek internetin dinamik yapısına uygun bir metodoloji oluşturmaya çalışmaktadır.

AİHM'nin *Węgrzynowski ve Smolczewski v. Polonya* kararında vurgulandığı üzere "*Mahkeme, internetin bilhassa bilgiyi barındırma ve iletme kapasitesi bakımından basılı medyadan farklı nitelikte bir bilgi ve iletişim aracı olduğunu belirtmiştir. Dünya genelinde milyarlarca kişiye hizmet sunan bu elektronik ağ, -basılı medya ile- aynı tür düzenleme ve kontrole muhtemelen hiçbir zaman tabi olmayacaktır. İnternet üzerindeki içerik ve iletilerin, başta özel hayata saygı hakkı olmak üzere insan hak ve özgürlüklerinin kullanımı-*

na ve bunlardan faydalanılmasına yönelik oluşturduğu zarar riski, geleneksel basının oluşturduğu riskten kesinlikle daha fazladır. Bu sebeple, basılı medyadan ve internetten materyal çoğaltılmasını düzenleyen politikalar birbirinden farklılık gösterecektir." [1446]

Devlet makamları tarafından gerçekleştirilen her türlü müdahale şüphesiz AİHS'nin 10. maddesinde düzenlenen kanunla öngörülme, meşruluk ve ölçülülük koşullarına uygun olmalıdır. Tüm tedbirler şeffaf, gerekli ve ölçülü olmalıdır. İnternet kullanıcılarına veya ilgili diğer taraflara internete erişim, içerik veya bilgiyi alma ve yayma imkânlarına yönelik işlemlere karşı AİHS'nin 6. maddesine uygun şekilde hak arama yolları sunulmalıdır.

AİHM, hukuki belirliliğin sağlanabilmesi için AİHS'de güvence altına alınan haklara kamu gücünün keyfî müdahalelerini önleyecek birtakım korumaların olması ve yasanın bu gücün kullanılmasının yöntemini ve kapsamını yeterli netlikte düzenlemesi gerektiğini vurgulamıştır.

Yine AİHM içtihatlarına göre önleyici kısıtlamalar (*prior restraints*) *a priori* AİHS'ye uyumsuz değildir. Yeter ki muhtemel kötüye kullanma durumlarına karşı sunulan hukuki güvenceler etkili olsun ve yasağın sınırlandırılması hususunda katı bir yasal çerçeve mevcut bulunsun.

Peki, AİHM'nin internete ilişkin tüm içtihatlarının ışığında ideal bir internet yasası nasıl olmalı ve ne tür nitelikleri haiz bulunmalıdır? Kanunla öngörülme, meşruluk ve ölçülülük kriterleri yasal düzenleme için nasıl somutlaştırılmalıdır?

Öncelikle internet ortamının düzenlenmesine ilişkin açık bir yasal dayanak olmalıdır. Bu alanda genel değil, özel bir düzenleme bulunmalıdır. Yasal düzenlemede, internet içeriğine hangi tekniklerle müdahale edileceği açıkça belirlenmelidir. İnternet ortamını düzenleyecek yasanın bu bağlamda çerçeve değil, kazuistik olması kaçınılmazdır ve ideal olan da budur. Bu tür mevzuat, konunun teknik ve hukuki boyutuna uygun olarak kaleme alınmalı ve tüm paydaşların, internet ortamındaki davranışlarını önceden düzenleyebilmesini temin etmelidir. IP adreslerinin,

[1446] **AİHM**, *Węgrzynowski and Smolczewski v. Polonya*, B. No:33846/07, 16.7.2013, para. 58.

portların, ağ protokollerinin veya sosyal ağ gibi kullanım tiplerinin engellenmesine yönelik tedbirler açıkça tanımlanmalıdır.

İnternet ortamına ancak açık ve meşru amaçlarla müdahale edilmelidir. Bu amaçların öncelikle AİHS'nin 10. maddesinin ikinci fıkrasında kabul edilen meşru menfaatleri karşılaması temin edilmelidir. Genel nitelikli, hukuki belirliliği sağlamayan, müphem gerekçelerle internet ortamına müdahale edilmemelidir. Erişimin engellenmesi tedbiri genel nitelikte değil, özel nitelikte içerikler için söz konusu olmalıdır. Bir içeriği hedefleyen erişim engeli tedbirinin genel bir erişim engeli olarak kullanılmasından kaçınılması için gerekli önlemler alınmalıdır.

İnternetin aynı anda birden çok temel hak ve hürriyetin icrası için temel bir araç hâline dönüşmüş olması sebebiyle her bir hakka ilişkin müdahale koşulları ayrı ayrı değerlendirilmelidir. Bu süreçte ifade özgürlüğünün esasına (çekirdek özüne) saygı gösterilmesi sağlanırken ifade özgürlüğü ile yarışan diğer menfaatlerin de dengesi gözetilmelidir. İfade özgürlüğüne yapılan müdahalenin, güdülen menfaati uygun bir şekilde geliştirip geliştirmediğinin ve söz konusu "sosyal ihtiyacı" gerçekleştirmek için gerekli olandan daha ileri gidilip gidilmediğinin tespitini mümkün kılan gereklilik ilkesine riayet edilmelidir.

AİHM içtihatlarından yapılabilecek bir diğer çıkarım ise müdahalenin geçici nitelikte olmasıdır. İnternet sitelerine veya platformlara uygulanan, süresiz veya uzun süre geçerli olan engellemeler sansür olarak nitelendirilecektir. Bu sebeple, koruma tedbiri veya ihtiyati tedbir olarak alınan engelleme tedbirlerinin süre sınırının olması yasada açıkça belirtilmelidir. Benzer şekilde, istisnai durumların yasa dışı bir içeriğin engellenmesini meşru kılması hâlinde *de jure* veya *de facto* olarak yasa dışı yayından sorumlu olmayan veya onun içeriğine abone olmayan kişi ve kurumların hedef alınmasından kaçınılmalıdır. Yasa dışı içeriğe yönelen tedbirlerin bu çerçevede düzenlenmesi gerekir. Özellikle de kararların tüm etkileriyle ortadan kaldırılması, engellenen yayınların devamının hızlıca sağlanması önem arz eder.

AİHM'ye göre internet ortamına müdahalede ölçülülük ilkesi her daim gözetilmeli ve en az müdahaleci tekniğin kullanılması zorunlu

tutulmalıdır. Diğer bir deyişle, tedbirler statik değil dinamik olmalıdır ve somut olayın özelliklerine göre gözden geçirilebilmelidir. Örneğin, erişimin engellenmesi kararı verecek mahkeme veya idari makam, somut olayda amaca ulaşmak için en elverişli engelleme tekniğini tespit etmeli ve neden bu tekniği kullandığını gerekçesiyle ortaya koymalıdır. Engellemenin teknik sebeplerle (örneğin IP değişikliği veya altyapıdaki güncellemeler) amacı aşan bir hâle dönüşmesi durumunda ise söz konusu karar hızlıca gözden geçirilmelidir. Kısacası, her zaman daha az müdahaleci tedbirin varlığının sorgulanması yasada açık bir yükümlülük olarak tanımlanmalıdır.

AİHM kararlarından çıkarılan bir diğer not ise internet ortamına kural olarak bir hâkim kararıyla müdahale edilmesi gerektiğidir. İdari makamlara istisnai durumlarda ve kararlarının bağımsız mahkemelerce etkin şekilde denetlenmesini temin edecek mekanizmaların kurulması kaydıyla yetki verilmelidir. Engelleme kararını vermeye yetkili makamlar yasal düzenlemede açıkça belirtilmelidir. Ayrıca yasal düzenlemede bölgesel, ulusal veya küresel düzeyde etkisi olabilecek engelleme talimatlarının yer bakımından uygulanmasına ilişkin hükümler de yer almalıdır. Uluslararası hukukun temel ilkeleri gözetilmelidir.

Bir hâkim kararıyla internete müdahale edilecekse hangi engelleme tekniğinin uygulanacağına ilişkin nihai karar hâkim tarafından verilmeli, genel engelleme kararı verilerek uygulama idari makamların keyfine bırakılmamalıdır. Bu sebeple, karar vericilerin, hangi engelleme tekniğini uygulayacaklarını gerekçelendirmeleri zorunludur.

AİHM kararları ışığında önemle vurgulamak gerekir ki internet ortamına müdahaleye ilişkin tüm adli ve idari süreçlerde en üst düzey şeffaflık sağlanmalıdır. Bu doğrultuda, menfaatleri etkilenen kişiler sürece dâhil edilmeli, bir bildirim söz konusu olmayacaksa kararın neden derhâl uygulanması gerektiği somut olarak ortaya koyulmalı, hangi içeriğin engelleneceği (maddi hukuk) ve nasıl engelleneceği (usûl hukuku) belirlenmeli, engelleme kararları somut hukuka aykırılığı mutlaka nitelendirmeli, tanımlamalı ve engelleme kararlarına karşı etkin bir itiraz mekanizması var olmalıdır.

Menfaatleri etkilenenler dışında söz konusu içeriğe erişmek isteyenler de bilgilendirilmelidir. Bu tür tedbirlerin hukuki dayanağı, gerekliliği ve gerekçesi, bu işlemi emreden mahkeme kararı ve bu karara itiraz gibi bilgiler dahil, bu konularda kamuya bilgi verilmelidir. Engelleme talebine dayanak teşkil eden içeriğin yetkili makam tarafından incelenmesi ve zarar gören kişi veya kurumun dinlenmesi sağlanmalıdır. Dinleme fiilen mümkün değilse veya güdülen menfaate zarar verecekse bundan vazgeçilebilmesi mümkündür.

İnternet ortamındaki içeriğin değeri hızlıca ortadan kalkabilmektedir. Çok kısa süreli bir engelleme veya içeriğin yayından kaldırılması tedbiri, verilen mesajı veya ulaşılmak istenen amacı anlamsız kılabilmektedir. Bu sebeple, müdahalelerin bu dinamizme uygun hak arama yöntemlerini barındırması gerekmektedir. Müdahale kararlarına karşı pratik itiraz imkânı ve etkin hak arama mekanizmaları tesis edilmelidir. Ayrıca, keyfî müdahalelere ilişkin özel koruma mekanizmaları ve tazmin imkânları var olmalıdır. Kısaca, içerikler çok hızlı bir şekilde değerini yitirebileceği için itiraz mekanizmaları da aynı hızda işlemelidir.

Şeffaflığın ve etkin itiraz mekanizmalarının hem *ex-ante* hem de *ex-post* aşamalarda sağlanması gerekir. *Ex-ante* yollar, engellemeye konu olan web sitelerinin sahiplerine ön bildirim; *ex-post* yollar ise bir engelleme kararı uygulandıktan sonra kapsamını kısıtlamak veya yeni koşullar dikkate alınarak itiraz etmek için etkin mekanizmalar sunmaktır. Dijital yollarla bildirim dahi bu bağlamda yeterli olabilmektedir.

İtiraz imkânı web sitesinin sahibi veya platformun işleteni gibi salt hak sahiplerine değil, her türlü menfaati doğrudan veya dolaylı olarak etkilenen tüm internet kullanıcılarına verilmelidir. Nihayetinde AİHM'nin, internet kısıtlamaları bağlamında mağdur sıfatını artık geniş yorumladığı dikkate alınırsa itiraz hakkına sahip kişilerin mümkün olduğunca geniş yorumlanması gerekir. Hukuka aykırı içeriklerin, internet sitelerinin ve platformlarının yerli veya yabancı sahibi, bu internet sitelerinin veya platformlarının kullanıcıları veya bu site ve platformları link olarak verenler ve bu içeriklere abone olanlar, bu engellemelerin yan etkisi sebebiyle hiz-

metlerine halel gelen kişiler ve engellenen web sitelerinin kullanıcılarının tamamının sürece dâhil olması değerlendirilmelidir.

AİHM içtihatlarında çerçevesi çizilmiş ve yerel hukukta mutlaka dikkate alınması gereken son konu ise platformların hukuki sorumluluğudur. Bu platform bir haber sitesi de olabilir bir sosyal medya ağı da. AİHM'ye göre platformlar içeriği saklamak ve erişmek için birer araç olup içeriğin kendisiyle özdeşleştirilmemelidir. Erişimin engellenmesi tedbiri söz konusu olduğunda varsayımlarla hareket edilmemeli ve somut bir hukuka aykırılık var olmalıdır.

Keza platform sorumluluğuna ilişkin muafiyet kuralları gözetilmelidir. *Delfi v. Estonya* kararında ilk kez karara bağlandığı ve *MTE ve Index.hu Zrt v. Macaristan* kararı ile teyit edildiği üzere her türlü hukuki zarardan platformun veya hizmet sağlayıcının müteselsil veya müşterek sorumluluğuna gidilmemelidir. Böyle bir sorumluluk ancak özel koşullarda ve sadece nefret söylemi ve şiddete teşvik gibi sebeplerden dolayı söz konusu olmalıdır.

İnternet Aracı Platformlarının Rolleri ve Sorumluluklarına İlişkin Tavsiye Kararı'nda da vurgulandığı üzere kullanıcılara, içerik sağlayıcılara ve internet platformlarına karşı, ifade özgürlüğünü zedeleme niyetiyle kamunun katılımını önleme amaçlı stratejik davalar (SLAPP - *strategic lawsuits against public participation*) veya kötü niyetli ve bezdirme amaçlı davalar açılabilir. Bunları önlemeye dönük özel bir düzenleme yapılmaması sosyal teknik olarak nitelendirilebilmektedir. Bu durum ise ifade özgürlüğüne demokratik bir toplum düzeninde kabul edilmeyecek nitelikte ölçüsüz bir müdahale teşkil edebilecektir.

Devletlere yüklenen bu yükümlülük karşısında hizmet sağlayıcıların da buna denk gelen temel yükümlülükleri vardır. İnternet Aracı Platformlarının Rolleri ve Sorumluluklarına İlişkin Tavsiye Kararı'nda da belirtildiği üzere, platformlar, aracı hizmet sağlayıcılar veya geniş ifadeyle hizmet sağlayıcılar "Birleşmiş Milletler İş Dünyası ve İnsan Haklarına Dair Rehber İlkeler: Birleşmiş Milletler 'Koruma, Saygı Gösterme ve Telafi Edici Çözüm Üretme' Çerçevesi"ne uygun şekilde, tüm eylemlerinde kullanıcılarının ve etkilenen tarafların insan haklarına saygı göster-

mekle yükümlüdür. Bu yükümlülük, uygulanabilir hukuk kurallarına ve düzenleyici çerçevelere uyumlu şekilde hareket etme sorumluluğunu da içermektedir. Diğer bir deyişle, hizmet sağlayıcılar tamamen kontrolsüz ve hukukun dışında değildir.

AİHM bir denge kurarak hizmet sağlayıcılara belirli hukuki muafiyetleri koşullu olarak tanımaktadır. Hizmet sağlayıcıların en temel yükümlülüğü, hukuka aykırı içerik hakkında bilgilendirildiklerinde içeriği kaldırmak veya bu içeriğe erişimi engellemektir. Sistemlerini proaktif şekilde tarayarak nefret söylemi ve şiddete teşvik içeriğini filtrelemekle yükümlüdürler. Daha genel bir ifadeyle, kullanıcıların temel hak ve hürriyetlerine yönelik talepleri etkin şekilde çözümlemek durumundadırlar. Bu tür bir mekanizmayı kurmamış ve mekanizmanın etkinliğini sağlamamış bir platform veya hizmet sağlayıcısı, kendisine özel olarak tanınmış hukuki muafiyetlerden faydalanamayacaktır. Kısaca, ne kadar etkin uyar-kaldır mekanizması varsa o kadar az hukuki sorumluluk söz konusu olacaktır.

AİHM'nin içtihatları ışığında ideal bir internet yasası özetle şu kriterleri sağlamalıdır:

(1) İnternet ortamının düzenlenmesine ilişkin açık bir yasal düzenleme olmalıdır.

(2) İnternete açık ve meşru amaçlarla müdahale edilmelidir.

(3) Müdahale geçici nitelikte olmalıdır.

(4) Müdahale belirli bir hedefe yönelmeli ve spesifik olmalıdır.

(5) Ölçülülük ilkesi her daim gözetilmeli ve en az müdahaleci tekniğin kullanılması zorunlu tutulmalıdır. Müdahale gerekçeleri demokratik bir toplumda gerekli olmalı ve müdahale için baskın bir sosyal ihtiyaç bulunmalıdır. Bir içeriğe yönelik tedbirin genel bir engellemeye dönüşmesini önleyecek teknik önlemler alınmalıdır.

(6) İnternet ortamına ancak bir mahkeme kararıyla müdahale edilmelidir. İdari makamlara istisnai durumlarda ve kararlarının bağımsız mahkemelerce etkin şekilde denetlenmesini temin edecek mekanizmaların kurulması kaydıyla yetki verilmelidir.

(7) İnternete müdahale kararları gerekçeli olmalıdır. Karar, kısıtlamanın etkinliği ve aşırı engelleme risklerine göre yapılacak bir değerlendirmeye dayanmalıdır. Bu değerlendirme, kısıtlamanın internet içeriğine veya belirli tip içeriğe erişimi ölçüsüz engelleyip engellemeyeceğini ve ayrıca belirtilen meşru amaca ulaşmak için en az kısıtlayıcı araç olup olmadığını içermelidir.

(8) Tüm süreçte en üst düzeyde şeffaflık sağlanmalıdır.

(9) Müdahale kararlarına ilişkin pratik itiraz imkânı ve etkin hak arama mekanizmaları tesis edilmelidir.

(10) Keyfî müdahalelere ilişkin özel koruma mekanizmaları ve tazmin imkânları var olmalıdır.

(11) Platform sorumluluğuna ilişkin muafiyet kuralları gözetilmelidir. Her türlü hukuki zarardan değil, sadece nefret söylemi ve şiddete teşvik içeriklerinden dolayı bunların sorumluluklarına gidilebilmelidir.

(12) Platformların, uyar-kaldır mekanizmalarının etkinliğini sağlaması temin edilmelidir.

AİHM'nin internet ve insan hakları konusundaki yaklaşımının özeti AİHS'nin 8. ve 10. maddesi arasında denge sağlanması; ayrıca, internete ilişkin tüm süreçlerde hukuki dinlenilme ve adil yargılanma haklarının temin edilmesidir.

İnternet ortamını düzenleyecek yasanın bu bağlamda çerçeve değil, kazuistik olması kaçınılmazdır ve ideal olan da budur. Bu tür mevzuat, konunun teknik ve hukuki boyutuna uygun olarak kaleme almalı ve tüm paydaşların, internet ortamındaki davranışlarını önceden düzenleyebilmesini temin etmelidir.

AİHM'nin içtihatları ışığında ideal bir internet düzenlemesi, hukuk ve teknoloji arasındaki uyumun en üst düzeyde gözetildiği bir düzenlemedir. İnternetin etkilediği hakların çokluğu ve çeşitliliği sebebiyle bu tür bir yasanın *sui generis* nitelikte olması ve hem kamu hukuku hem de özel hukuka ilişkin hükümler içermesi kaçınılmazdır.

§26. SONUÇ

İnternete erişim temel bir insan hakkıdır. İnternet hem bireylerin hem de devletlerin temel iletişim ve bilgi paylaşım mecrası hâline gelmiştir. İnternetin sosyal, ekonomik, kültürel, siyasi veya ticari amaçlarla kullanım alanları her geçen gün artmakta; bir yandan da altyapı, esaslı bir dönüşüm geçirmektedir. İnternet, neredeyse birçok hakkın kullanılmasının tek yöntemi haline gelmektedir. Bireysel kullanımın yanı sıra kamu hizmetlerinin sunumunda da artık varsayılan mecra internettir. Keza devletler arasındaki çatışmalar da internet ağına taşınmıştır.[1447]

İnternetin bireylerin davranışlarını etkileyen önlenemez bir özgürleştirme gücü vardır. Bireylerin sosyal ve kültürel olarak kişiliklerinin gelişmesine yardımcı olan internet, ekonomik kalkınmanın hızlanmasında da önemli bir etkendir. İnternet, toplumları dönüştürmekte, yönetimleri şeffaflaştırmaktadır. Kamusal yönetimde üretkenliği ve saydamlığı sağlarken elektronik ticareti artırmakta ve bilişim alanında yeni iş kolları oluşturmak suretiyle istihdam yaratmaktadır. İnternetin tüm bu faydaları göz önüne alındığında internete ilişkin düzenlemelerin sınırlayıcı değil teşvik edici olması gerekmektedir.

İnternetin ilk mimarları interneti şu an olduğu gibi küresel bir ağ olarak tasarlamamışlardır. Tam aksine, internet askerî bir proje olarak geliştirilmiştir ve belirli noktalarda hâlâ bu izleri muhafaza etmektedir. İnternetin nasıl yönetileceği sorusunun kesin bir yanıtı yoktur. Bu *soru*nun kökeninde meşruiyet sorunu kadar, bu denli büyük, dağıtık ve kendine özgü teknik yapısı olan, çok farklı egemenlik alanlarını, kurumları ve kişileri ilgilendiren bir alanın regülasyonuyla ilk kez karşı karşıya kalınmış olması yatmaktadır.

[1447] "Netwar" olarak da adlandırılan bu tür çatışmalara ilişkin temel bir inceleme için bkz. **Arquilla, John/Ronfeldt, David F** (2001). *Networks and Netwars: The Future of Terror, Crime, and Militancy*, Santa Monica, Rand.

İnternet klasik bir iletişim aracı olarak görülmemelidir. Nihayetinde internet bir iletişim ağı olduğu kadar bilgiye erişim ağıdır. İnternetin kullanım alanlarının çok hızlı bir şekilde artması sebebiyle olası bir engelleme veya kısıtlamadan etkilenecek hakların sayısı da artmıştır. Somut olayda engellenen veya kısıtlanan içeriğin özelliklerine göre bu hakların ayrı ayrı tespit edilmesi ve bu hakların teknolojik gelişmelere uygun bir şekilde yeniden yorumlanması gerekmektedir.

Örneğin, elektronik ticaret hizmeti sunan bir web sitesi engellendiğinde iletişim ve ifade hürriyeti dışında web sitesi sahibinin mülkiyet hakkı da bundan etkilenmiş olacaktır. Benzer şekilde, bir sosyal ağ sitesi veya bir forum engellendiğinde iletişim ve ifade hürriyetleri dışında bireylerin toplantı hak ve hürriyeti de etkilenmektedir. Tüm bu sebeplerle, internetin kontrolü ve internet ortamındaki içerikten dolayı sorumluluğun, etkilenen her bir hak için müstakil olarak değerlendirilmesi zorunludur.

Teknolojinin gelişmesiyle yeni engelleme ve filtreleme teknikleri ortaya çıktığı gibi bu engelleme veya filtrelemeleri aşacak özgün teknikler de aynı hızla ortaya çıkmıştır. Hangi yöntem ve tekniğin kullanılması gerektiği sorusunun yanıtı, nasıl bir içerikle mücadele edileceği ve bu içerikle mücadelenin ne kadar önemli olduğuyla yakından ilintilidir. Aynı doğrultuda, bu alana yapılan para, emek ve zaman yatırımı da tercih edilecek yöntem ve kullanılacak tekniği belirleyen ana faktörlerdendir. Eğer ki kamu düzenini tehdit eden bir içerik varsa tüm yöntem ve tekniklerin karma şekilde kullanılması bile söz konusu olacaktır. Devletler, bu tür durumlarda pire için yorgan yakmaktan çekinmemektedir!

İnternetin teknik kontrolü, bünyesinde muhtelif yapısal sorunlar barındıran bir meseledir. Şifreleme teknolojilerinin yaygınlaşması, yerelleşme, ağların fragmantasyonu, içeriğin kontrolü için çok büyük ölçekte verinin işlenmesinin gerekli olması ağ izleme ve kontrol teknolojilerinin yetersiz kalmasına sebep olmaktadır. Aşırı engelleme veya hiç engellememenin, diğer bir deyişle hatalı pozitif (*false positive*) ve hatalı negatif (*false negative*) durumların ortaya çıkması kaçınılmaz olmaktadır.

Önemle belirtmek gerekir ki bir ülkede uygulanan engelleme yöntem ve teknikleri, içerik sağlayıcılar ve sosyal medya platformları ile o

ülke arasındaki iş birliğiyle yakından ilgilidir. Platform temelli engelleme yöntemi uygulanıyorsa diğer engelleme yöntem ve tekniklerini kullanmaya zaten gerek yoktur. Dolayısıyla, erişimi engelleme tedbirlerinin sayısıyla platform temelli engelleme arasında ters orantı vardır.

İnternete erişimin engellenmesinin veya kısıtlanmasının yan etkileri çok fazladır. Bu sebeple, internete yönelik bir kısıtlamaya üstün bir kamusal yararın varlığı durumunda ve son çare olarak başvurulması gerekmektedir. Diğer bir deyişle, internete ilişkin bir müdahale kararı verilirken etkilenmesi muhtemel tüm temel hak ve hürriyetlere ilişkin müdahale sebepleri ve usullerinin göz önünde bulundurulması gerekir.

İnternet içeriğine müdahale eden bir düzenlemenin bireyleri hareketsizliğe itmemesi, aksine internetin kullanımını teşvik etmesi gerekmektedir. Hakkın özü bilhassa internet içeriğine doğrudan değil ama dolaylı teknikler kullanarak müdahale edildiğinde önem taşımaktadır. Üçüncü bölümde açıklandığı üzere, bazı sebeplerden dolayı doğrudan engelleme kararı almak yerine, başkaca yöntemler kullanılarak sitelere erişim fiilen zorlaştırılmakta veya kullanıcıların otosansür uygulamaları sağlanmaktadır. Örneğin, internet ortamında yapılan tüm işlemlerin takip edilmesi veya fiilen bu takip yapılmasa bile bu şekilde bir takibin yapıldığı izlenimi verilmesi yahut internete bağlanmak için vatandaşlık numarası gibi bazı bilgilerin girilmesinin istenmesi yaygın kullanılan sosyal tekniklerdir. Böyle durumlarda bireyler, takip edildikleri düşüncesiyle, devletçe sakıncalı görülebilecek web sitelerine girmekten kendileri vazgeçmektedir. Erişim engelleme gibi somut bir teknik kullanmadığı için de fiilî engelleme devlete atfedilememektedir. Bir yasaklamanın sansür olarak kabul edilmesi için, etkilenen hakların sayısı ve yasaklama gerekçelerinin keyfî uygulamaya yol açıp açmadığının tespiti gerekmektedir.

Şunu da belirtmek gerekir ki bilişim ve teknoloji hukuku alanındaki çalışmalar bir nevi hukuk tarihi çalışmalarıdır. Zira, hukukun yorumladığı teknoloji o kadar hızlı değişmektedir ki içtihatlar, yorumlar, kurallar çok kısa sürede anlamsız hâle gelebilmektedir.

Bu kitaptaki incelemeler IPv4 dünyasının internetine uygulanan hukuku içermektedir. IPv6 dönüşümünün gerçekleştiği bir dünyada mev-

cut sorunlara yeni pratik çözümler üretilecek ve fakat yeni problemler de ortaya çıkacaktır. Her bir cihazın ağda özgün adresiyle konumlandırılmasının mümkün olması, sadece internet hukukunu değil bilişim suçlarını ve adli bilişimi de köklü olarak değiştirecektir.

Tıpkı bulut bilişimin yaygınlaşması ve standart hatta varsayılan bir bilişim yöntemine dönüşmesindeki gibi internete erişimde 5G ağının yaygınlaşması ve uydu internetinin makul şekilde erişilebilir olması ile internetin kontrolü ve erişimin kısıtlanması alanında yeni tartışmalar ortaya çıkacaktır.

İnternet, bir dönüm noktasındadır. Kişisel verilerin korunması bağlamında veri lokalizasyonunun artması, yerelleşmenin öne çıkması, özel erişim sağlanan alanların artması, çok yaygın kullanılan internet hizmetlerinin belirli şirketler etrafında toplanması, ağ tarafsızlığından sapmaların çoğalması ve en önemlisi de ulusal güvenliğin sağlanması amacıyla müstakil ağların oluşturulması gibi sebeplerle internet parçalanmakta, adacıklara bölünmektedir. Fiziki serbest dolaşımdaki sınırlara benzer şekilde internet ortamında sanal sınırlar kurularak belirli kullanıcıların daha kaliteli ve nitelikli içeriğe erişmesi ve altyapıyı kullanması söz konusu olmaktadır.

İnternetin küresel bir ağ niteliğini yitirmesi uzak bir ihtimal değildir. Kırılma belki yumuşak belki de sert olacaktır. Tüm bu gelişmeler, güneyden kuzeye, batıdan doğuya küresel bir regülasyon dalgasına yol açacaktır. Nasıl gerçekleşirse gerçekleşsin, bu kırılmanın insan haklarının küresel ölçekte korunması üzerinde ciddi bir etkisi olacaktır.

KAYNAKÇA

Açıkgöz, Emre İkbal (2020) *Bilişim Sistemi Aracılığıyla Haksız Yarar Sağlama Suçu (TCK m. 244/4)*, Ankara, Adalet Yayınevi.

Akdeniz, Yaman/Altıparmak, Kerem (2008) *İnternet: Girilmesi Tehlikeli ve Yasaktır - Türkiye'de İnternet İçerik Düzenlemesi ve Sansüre İlişkin Eleştirel Bir Değerlendirme*, Ankara: İmaj.

Arquilla, John/Ronfeldt, David F (2001). *Networks and Netwars: The Future of Terror, Crime, and Militancy*, Santa Monica, Rand.

Arx, Kim G. (2003) "*ICANN - Now and Then: ICANN's Reform and Its Problems*", Duke Law & Technology Review, Cilt: 2, s. 1-22.

Aykaç, Alper Can (2009) "*Resmî Belgelere Erişime İlişkin Avrupa Konseyi Sözleşmesi*" TBB Dergisi, Sayı: 83, s. 402-411.

Bayamlıoğlu, İbrahim Emre (2008) *Fikir ve Sanat Eserleri Hukukunda Teknolojik Koruma*, İstanbul, On İki Levha Yayıncılık.

Belli, Luca (2016) "*End-to-End, Net Neutrality and Human Rights*": Belli, Luca; De Filippi, Primavera (Editörler) *Net Neutrality Compendium*, Cham, Springer.

Berners-Lee, Tim/Fischetti, Mark (1999) *Weaving the web : the original design and ultimative destiny of the World Wide Web by its inventor*, New York, HarperCollins.

Cerf, Vinton G/Kahn, Robert E (1974) "*A Protocol for Packet Network Intercommunication*" IEE Transactions on Communications, Cilt: 22, s. 637-648.

DeNardis, Laura (2009) *Protocol politics: the globalization of Internet governance*, Cambridge, MIT Press.

Dinwoodie, Graeme B (2017). *A Comparative Analysis of the Secondary Liability of Online Service Providers*, Cham, Springer.

Dodd, Annabel Z. (2012) *The Essential Guide to Telecommunications*, Upper Saddle River, Prentice Hall.

Drake, William J (2005) *Reforming Internet governance: perspectives from the Working Group on Internet Governance (WGIG)*, New York, United Nations Information and Communication Technologies Task Force.

Dülger, Murat Volkan (2007) "*İnternet Erişiminin Engellenmesinin Hukuksal Açıdan Değerlendirilmesi ve 5651 Sayılı Yasayla Getirilen Düzenleme*" İstanbul Barosu Dergisi, Cilt: 81, Sayı: 4, s. 1477-1545.

Falcıoğlu, Mete Özgür (2004) *Karşılaştırmalı Hukuk ve (Amerikan Hukuku ve Viyana Antlaşması) Türk Hukukunda Elektronik Satım Sözleşmesi ve Kurulması*, Ankara, Yetkin.

Faris, Robert/Villeneuve, Nart (2008) "*Measuring Global Internet Filtering*": Deibert, Ronald/Palfrey, John/Rohozinski, Rafal/Zittrain, Jonathan (Editörler) *Access denied: the practice and policy of global Internet filtering*, Cambridge, MIT Press.

Fuller, Kathleen E (2001) "*ICANN: The Debate Over Governing the Internet*", Duke Law & Technology Review, Cilt: Rev 1, s. 1-9.

Furht, Borko (2010) "*Cloud Computing Fundamentals*": Borivoje, Furht/Escalante, Armando (Editör) *Handbook of cloud computing*, New York, Springer.

Geiger, Christophe /Izyumenko, Elena (2020) "*Blocking Orders: Assessing Tensions with Human Rights*": Frosio, G (Editör) *Oxford Handbook of Online Intermediary Liability*, Oxford, Oxford University Press.

Gök, Mehmet Salih (2012) *5651 sayılı Kanun ve Bilgi Güvenliği İlişkisi*, İstanbul, On İki Levha Yayıncılık, s.17-20.

Goldsmith, Jack L/Wu, Tim (2006) *Who controls the Internet? Illusions of a borderless world*, New York, Oxford University Press.

Gupta, Juhi (2013) "*John Doe Copyright Injunctions in India*" Journal of Intellectual Property Rights, Sayı: 18, s. 351-359.

Haber, Eldar (2011) "*The French Revolution 2.0: Copyright and the Three Strikes Policy*", Harvard Journal of Sports and Entertainment Law, Sayı: 2, s. 297-339.

Hall, Eric A. (2000) *Internet core protocols: the definitive guide*, Cambridge, O'Reilly.

Hofstetter, Fred Thomas (2006) *Internet literacy*, Boston, McGraw-Hill/Irwin.

Jandarma Genel Komutanlığı Kriminal Dairesi Başkanlığı (2016) *Kriminal Terimleri Sözlüğü*, Ankara, TDK Yayınları.

Kayany, Joseph M (2004) "*Internet Etiquette (Netiquette)*": Bidgoli, Hossein (Editör) *The Internet encyclopedia - Volume 2*, Hoboken New Jersey, John Wiley & Sons.

Kecskeméti, Charles/Székely, Iván (2005) *Access to Archives: A Handbook of Guidelines for Implementation of Recommendation No R (2000)13 on a European Policy on Access to Archives*, Belgium, Council of Europe Publishing.

Keser Berber, Leyla/Sert, Elif/Atabey, Ayça (2020) *Net Neutrality, Turkey, and Beyond - A Road Map for Net Neutrality Regulation in Turkey*, İstanbul, On İki Levha Yayıncılık.

Kieso, Douglas W. (2005) *Unjust Sentencing and the California Three Strikes law*, New York, LFB Scholarly Pub.

Köksal, Tuğçe Duygu (2018) *"İnternet sağlayıcılarının üçüncü kişiler tarafından yapılan yorumlar bakımından hukuki sorumluluğu üzerine: Avrupa İnsan Hakları Mahkemesi'nin Delfi AS Kararı"* Suç ve Ceza, Sayı: 1, s. 95-114.

Kozierok, Charles M. (2005) *The TCP/IP guide : a comprehensive, illustrated Internet protocols reference*, San Francisco, No Starch Press.

Kulesza, Joanna (2012) *International Internet law*, Milton Park, Routledge.

Kunter, Nurullah/Yenisey, Feridun/Nuhoğlu, Ayşe (2006) *Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku*, İstanbul, Beta Yayınları.

Kurbalija, Jovan (2010) *An introduction to Internet Governance*, Msida, Malta, Diplo Foundation.

Kuru, Baki/Arslan, Ramazan/Yılmaz, Ejder (2005) *Medeni Usul Hukuku*, Ankara, Seçkin Yayıncılık, s. 694.

Lambert, Paul (2018) *Gringras: The Laws of the Internet*, Haywards Heath, Bloomsbury Professional.

Lukasik, Stephen (2011) *"Why the Arpanet Was Built"*, IEEE Annals of the History of Computing, Cilt:33, Sayı:3, s. 4-21.

Mathiason, John (2009) *Internet governance: the new frontier of global institutions*, London, Routledge

McGonagle, Tarlach (2020). *"Free Expression and Internet Intermediaries: The Changing Geometry of European Regulation"*: Frosio, Giancarlo (Editör) *Oxford Handbook of Online Intermediary Liability*, Oxford, Oxford University Press.

McQuade, Samuel C (2009) *Encyclopedia of cybercrime*, Westport, Greenwood Press.

Mueller, Milton (2002) *Ruling the root Internet governance and the taming of cyberspace*, Cambridge, MIT Press.

Mueller, Milton/Mathiason, John/Klein, Hans (2007) "*The Internet and Global Governance: Principles and Norms for a New Regime*" Global Governance, C:13, Sayı: 2, 237-254.

Muldoon, James P (2012) "*New types of organizations and global governance in the twenty-first century - The case of ICANN*": Oestreich, Joel E (Editör) *International Organizations as Self-directed Actors : A Framework for Analysis*, Abingdon, Routledge.

Nunziato, Dawn C (2009) *Virtual freedom: Net Neutrality and Free Speech in the Internet age*, Stanford, Stanford Law Books.

Pazarcı, Hüseyin (2015) *Uluslararası Hukuk*, Ankara, Turhan Kitabevi.

Ryan, Johnny (2010) *A history of the Internet and the digital future*, London, Reaktion Books.

Schultz, E Eugene (2004) "*Denial of Service Attacks*": Bidgoli, Hossein (Editör) *The Internet encyclopedia - Volume 1*, Hoboken New Jersey, John Wiley & Sons.

Schulze, Reiner/Staudenmayer, Dirk (2020) *EU Digital Law Article-by-Article Commentary*, Baden, Nomos Verlagsgesellschaft.

Sherry, John/Brown, Colleen (2004) "*History of the Internet*": Bidgoli, Hossein (Editör) *The Internet Encyclopedia - Volume 2*, Hoboken New Jersey, John Wiley & Sons.

Smith, Graham (2017) "*Cyberborders and the Right to Travel in Cyberspace*": Kohl, Uta (Editör) *The Net and the Nation State - Multidisciplinary Perspectives on Internet Governance*, Cambridge, Cambridge University Press.

Son, Sooel/Shmatikov, Vitaly (2010) "*The Hitchhiker's Guide to DNS Cache Poisoning*": Jajodia, Sushil/Zhou, Jianying (Editörler) *Security and Privacy in Communication Networks*, Berlin, Springer, s. 466-483.

Soysal, Tamer (2014) *İnternet Alan Adları Hukuku (Domain Name Law)*, Ankara, Adalet.

Sözüer, Eren (2017) *Unutulma Hakkı - İnsan Hakları Hukuku Perspektifinden Bir İnceleme*, İstanbul, On İki Levha Yayıncılık.

Susi, Mart (2014) "*Delfi AS AS v. Estonia*" The American Journal of International Law, Cilt: 108, Sayı: 2, s. 295-302.

Taşkın, Cankat (2016) *İnternete Erişim Yasakları*, Ankara, Seçkin.

Taştan, Furkan Güven (2017) *Türk Sözleşme Hukukunda Kişisel Verilerin Korunması*, İstanbul, On İki Levha.

Toluner, Sevin (1996) *Milletlerarası Hukuk Dersleri: Devletin Yetkisi*, İstanbul, Beta.

Van der Hof, Simone/Van den Berg, Bibi/Schermer, Bart (2014) *Minding Minors Wandering the Web: Regulating Online Child Safety*, The Hague, T.M.C. Asser Press, s. 131.

Zittrain, Jonathan (1999) "*ICANN: Between the Public and the Private Comments before Congress*", Berkeley Technology Law Journal, Cilt: 14, Sayı: 3, s. 1071-1094.

Zittrain, Jonathan/Palfrey, John "*Internet Filtering: The Politics and Mechanisms of Control*": Deibert, Ronald/Palfrey, John/Rohozinski, Rafal/Zittrain, Jonathan (Editörler) *Access denied: the practice and policy of global Internet filtering*, Cambridge, MIT Press.

AİHM KARARLARI

Ahmet Yıldırım v. Türkiye, Başvuru No: 3111/10, 18.12.2012.

Akdeniz v. Türkiye, Başvuru No: 20877/10, 11.3.2014.

Ashby Donald ve Diğerleri v. Fransa, Başvuru No: 36769/08, 10.1.2013.

Axel Springer AG v. Germany, Başvuru No: 39954/08, 7.02. 2012.

Bulgakov v. Rusya, Başvuru No: 20159/15, 23.6.2020.

Cengiz ve diğerleri v. Türkiye, Başvuru No: 48226/10 ve 14027/11, 1.12.2015.

Delfi AS v. Estonya, Başvuru No: 64569/09, 16.6.2015.

Engels v. Rusya, Başvuru No: 61919/16, 23.6.2020.

Høiness v. Norveç, Başvuru No: 43624/14, 19.6.2019.

Jankovskis v. Litvanya, B. No. 21575/08, 17.4.2017.

K.U. v. Finlandiya, Başvuru No:2872/02, 2.12.2008.

Kablis v. Rusya, Başvuru No: 48310/16 ve 59663/17, 30.4.2019.

Kalda v. Estonia, Başvuru No: 17429/10, 19.1.2016.

Khurshid Mustafa ve Tarzibachi v. İsveç, Başvuru No: 23883/06, 16.12.2008.

Krone Verlags GmbH & Co. KG v. Avusturya (No. 4), Başvuru No: 72331/01, 9.11. 2006.

M.L. ve W.W. v. Almanya, Başvuru No: 60798/10 ve 65599/10, 28.6.2018.

Magyar Jeti Zrt v. Macaristan, Başvuru No: 11257/16, 4.12.2018.

Magyar Tartalomszolgáltatók Egyesülete (MTE) ve Index.hu Zrt v. Macaristan, Başvuru No: 22947/13, 2.5.2016.

Monnat v İsviçre, Başvuru No: 73604/01, 21.9.2006.

OOO Flavus ve diğerleri v. Rusya, Başvuru No: 12468/15, 23489/15, 19074/16, 23.6.2020.

Österreichischer Rundfunk v. Avusturya, Başvuru No: 35841/02, 7.12. 2006.

Print Zeitungsverlag GmbH / Avusturya, Başvuru No: 26547/07, 10.10.2013.

Rolf Anders Daniel PIHL v. İsveç, Başvuru No: 74742/14, 7.2.2017.

Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland, Başvuru No: 931/13, 27.06. 2017.

Sdružení Jihočeské Matky v. Czech Republic, Başvuru No: 19101/03, 10.07.2006.

Tamiz v. Birleşik Krallık, Başvuru No: 3877/14, 19.9.2017.

Tanrıkulu ve Diğerleri v. Türkiye, Başvuru No: 40150/98, 40153/98 ve 40160/98, 6.11. 2001.

Times Newspapers v. Birleşik Krallık (1 ve 2 sayılı), Başvuru No: 3002/03 ve 23676/03, 10.3.2009.

Uj v. Hungary, Başvuru No: 23954/10, 19.07. 2011.

Vladimir Kharitonov v. Rusya, Başvuru No: 10795/14, 23.6.2020.

Węgrzynowski and Smolczewski v. Polonya, Başvuru No:33846/07, 16.7.2013.

AVRUPA KONSEYİ BELGELERİ

Avrupa Konseyi, "*Committee of Ministeres Declaration on freedom of communication on the Internet*", <https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805dfbd5>

Avrupa Konseyi, "*Committee of Ministers' Recommendation Rec(2004)11 on legal, operational and technical standards for e-voting*", <https://www.coe.int/t/dgap/goodgovernance/Activities/Key-Texts/Recommendations/Rec(2004)11_Eng_Evoting_and_Expl_Memo_en.pdf>

Avrupa Konseyi, "*Contribution by the Council of Europe to the 2nd Preparatory Committee for the World Summit on the Information Society (Geneva, 17-28 February 2003)*" <https://www.itu.int/dms_pub/itu-s/md/03/wsispc2/c/S03-WSISPC2-C-0032!!PDF-E.pdf>

Avrupa Konseyi, "*Convention on Access to Official Documents CETS No.205*" <https://rm.coe.int/1680084826>

Avrupa Konseyi, "*Declaration by the Committee of Ministers on Internet governance principles*", <https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cc2f6>

Avrupa Konseyi, "*Declaration by the Committee of Ministers on the protection of freedom of expression and information and freedom of assembly and association with regard to Internet domain names and name strings*", <https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805b1059>

Avrupa Konseyi, "*Declaration of the Committee of Ministers on human rights and the rule of law in the Information Society CM(2005)56*", <https://www.coe.int/t/dgap/goodgovernance/Activities/Public_participation_internet_governance/Declaration-Information-Society/011_DeclarationFinal%20text_en.asp>

Avrupa Konseyi, "*Declaration of the Committee of Ministers on network neutrality 29 September 2010*" <https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805ce58f>

Avrupa Konseyi, "*Declaration of the Committee of Ministers on protecting the dignity, security and privacy of children on the Internet*", <https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805d3d2d>

Avrupa Konseyi, "*Declaration of the Committee of Ministers on the management of the Internet protocol address resources in the public interest*", <https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805ce5bd>

Avrupa Konseyi, "*Declaration of the Committee of Ministers on the protection of freedom of expression and freedom of assembly and association with regard to privately operated Internet platforms and online service providers*", <https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805cb844>

Avrupa Konseyi, "*Recommendation (91)10 of the Committee of Ministers to member states on the communication to third parties of personal data held by public bodies*", <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804c1486>

Avrupa Konseyi, "*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*", <https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805d4d0e>

Avrupa Konseyi, "*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*", <https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805d3bc4>

Avrupa Konseyi, "*Recommendation CM/Rec(2009)5 of the Committee of Ministers to member states on measures to protect children against harmful content and behaviour and to promote their active participation in the new information and communications environment*", <https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805d0b0f>

Avrupa Konseyi, "*Recommendation CM/Rec(2011)7 of the Committee of Ministers to member states on a new notion of media*", <https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cc2c0>

Avrupa Konseyi, "*Recommendation CM/Rec(2011)8 of the Committee of Ministers to member states on the protection and promotion of the universality, integrity and openness of the Internet*", <https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cc2f8>

Avrupa Konseyi, "*Recommendation CM/Rec(2012)3 of the Committee of Ministers to member States on the protection of human rights with regard to search engines*", <https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805caa87>

Avrupa Konseyi, "*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*", <https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805caa9b>

Avrupa Konseyi, "*Recommendation CM/Rec(2015)6 of the Committee of Ministers to member States on the free, transboundary flow of information on the Internet*", <https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c3f20>

Avrupa Konseyi, "*Recommendation CM/Rec(2016)1 of the Committee of Ministers to member States on protecting and promoting the right to freedom of expression and the right to private life with regard to network neutrality*", <https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c1e59>

Avrupa Konseyi, "*Recommendation CM/Rec(2016)5 of the Committee of Ministers to member States on Internet freedom*", <https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016806415fa>

Avrupa Konseyi, "*Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries*", <https://rm.coe.int/1680790e14>

Avrupa Konseyi, "*Recommendation No. R (2000) 13 of the Committee of Ministers to member states on a European policy on access to archives*", <https://rm.coe.int/16804cea4f>

Avrupa Konseyi, "*Recommendation No. R (81) 19 of the Committee of Ministers to Member States on the access to information held by public authorities*", <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804f7a6e>

Avrupa Konseyi, "*Recommendation No. R (89) 7 concerning principles on the distribution of videograms having a violent, brutal or pornographic content*", <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804e8fe8>

Avrupa Konseyi, "*Recommendation No. R (92) 19 on video games with a racist content*", <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804d74f7>

Avrupa Konseyi, "*Recommendation No. R (97) 19 on the portrayal of violence in the electronic media*", <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680509212>

Avrupa Konseyi, "*Recommendation No. R (97) 20 on "hate speech"*", <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680505d5b>

Avrupa Konseyi, "*Recommendation No. R (99) 14 Of the Committee of Ministers to Member States on universal community service concerning new communication and information services*", <https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680502333>

Avrupa Konseyi, "*Recommendation No. R (99) 5 of the Committee of Ministers to member states for the protection of privacy on the Internet - Guidelines for the protection of individuals with regard to the collection and processing of personal data on information highways*", <https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016804f4429>

Avrupa Konseyi, "*Recommendation of the Committee of Ministers to member States on a Guide to human rights for Internet users*", <https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016804d5b31>

Avrupa Konseyi, "*Recommendation Rec (2001) 8 of the Committee of Ministers to member states on self-regulation concerning cyber content (self-regulation and user protection against illegal or harmful content on new communications and information services)*", <https://www.osce.org/files/f/documents/0/7/31584.pdf>

Avrupa Konseyi, "*Recommendation Rec(2006)12 of the Committee of Ministers to member states on empowering children in the new information and communications environment*", <https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805af669>

Avrupa Konseyi, "*Resolution No. 1 of the 5th European Ministerial Conference on Mass Media Policy (Thessaloniki, 11-12 December 1997)*", <https://rm.coe.int/16804f49ed>

ELEKTRONİK KAYNAKLAR

Bu çalışma kapsamında atıf yapılan tüm internet içeriklerinin güncelliği, **1 Aralık 2020** tarihinde tekrar erişilmek suretiyle teyit edilmiştir. Bu sebeple, dipnotlarda müstakil erişim tarihleri belirtilmemiştir. Tüm kaynaklar için son erişim tarihi **1 Aralık 2020** tarihidir.

Access Now (2017) "*Net Neutrality Matters For Human Rights Across The Globe*" <https://www.accessnow.org/net-neutrality-matters-human-rights-across-globe/>

AİHM, "*Case Law of the European Court of Human Rights Concerning the Protection of Personal Data*" <https://www.echr.coe.int/Documents/FS_Data_ENG.pdf>

APNIC, "*Explained: IANA Transition*", <https://www.apnic.net/wp-content/uploads/2017/01/IANA-Factsheet.pdf>

Article 29 - Data Protection Working Party, "Third Annual Report on the Situation Regarding the Protection of Individuals with Regard to the Processing of Personal Data and Privacy in the Community and in Third Countries - Covering the Year 1998, Adopted on 22nd December, 1999" <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2000/wp35_en.pdf>

Avrupa Konseyi, "*Filtering, blocking and take-down of illegal content on the Internet*" <https://www.coe.int/en/web/freedom-expression/study-filtering-blocking-and-take-down-of-illegal-content-on-the-internet>

Baran, Paul (1964) "*On Distributed Communications: I. Introduction To Distributed Communications Networks*", <http://www.rand.org/content/dam/rand/pubs/research_memoranda/2006/RM3420.pdf>;

BBC, "*GDPR: US news sites unavailable to EU users under new rules*", <https://www.bbc.com/news/world-europe-44248448>

Belli, Luca (2016) "*Net Neutrality Reloaded: Zero Rating, Specialised Service, Ad Blocking and Traffic Management Annual report of the UN IGF Dynamic Coalition on Net Neutrality*", <http://www.ict-21.ch/com-ict/IMG/pdf/Net-Neutrality.pdf>

BEREC (2016) "*About BEREC's Net Neutrality Guidelines*", <https://berec.europa.eu/files/document_register_store/2016/8/NN%20Factsheet.pdf>

BEREC (2016) "*Guidelines on the Implementation by National Regulators of European Net Neutrality Rules*", <https://berec.europa.eu/eng/document_register/subject_matter/berec/download/0/6160-berec-guidelines-on-the-implementation-b_0.pdf>

Berners-Lee, Tim (1997) "*Links and Law: Myths*" <https://www.w3.org/DesignIssues/LinkMyths.html>

Berners-Lee, Tim, "*Information Management: A Proposal*", <https://www.w3.org/History/1989/proposal.html>

Berners-Lee, Tim, "*Links and Law: Myths*" <https://www.w3.org/DesignIssues/LinkMyths.html>

Berners-Lee, Tim, "*Long Live the Web: A Call for Continued Open Standards and Neutrality*" <https://www.scientificamerican.com/article/long-live-the-web/>

Berners-Lee, Tim, "*Long Live the Web: A Call for Continued Open Standards and Neutrality*", <https://www.scientificamerican.com/article/long-live-the-web/>

Birleşmiş Milletler, "*The UN Human Rights Council's Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression of 16 May 2011 to the Human Rights Council (A/HRC/17/27)*" <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G11/132/01/PDF/G1113201.pdf?OpenElement>

Bradner S/Mankin A, "*The Recommendation for the IP Next Generation Protocol*", <https://tools.ietf.org/html/rfc1752>

Bradner, S, "Intellectual Property Rights in IETF Technology" <https://tools.ietf.org/html/rfc3979>

BTK, "*Şebeke Tarafsızlığı*", <https://www.btk.gov.tr/uploads/pages/slug/sebeke-tarafsizligi.pdf≥

Carpenter, B, "Charter of the Internet Architecture Board (IAB)" <https://tools.ietf.org/html/rfc2850>

CERRE (Centre on Regulation in Europe) (2018), "*A Fresh Look at Zero-Rating*" <https://cerre.eu/sites/cerre/files/CERRE_ZeroRating_FinalReport_0.pdf>

Cimpanu, Catalin, "*Germany and the Netherlands to build the first ever joint military internet*", <https://www.zdnet.com/article/germany-and-the-netherlands-to-build-the-first-ever-joint-military-internet/>

Cimpanu, Catalin, "*Russia to disconnect from the internet as part of a planned test*", <https://www.zdnet.com/article/russia-to-disconnect-from-the-internet-as-part-of-a-planned-test/>

Citizen Lab (University of Toronto) (2007) "*Everyone's guide to by-passing Internet censorship for citizens worldwide*" <http://citizenlab.org/guides/everyones-guide-english.pdf>

Der Sar, Ernesto Van, "*Hollywood Studios Flag Their IMDb Listings as "Pirate" Links*", <https://torrentfreak.com/hollywood-studios-flag-their-imdb-listings-as-pirate-links-180818/>

Dünya Bilgi Toplumu Zirvesi <http://www.bilgitoplumu.gov.tr/uluslararasi-calismalar/dunya-bilgi-toplumu-zirvesi/ikinci-asama-tunus/>

European Commission, "*Open Internet*" <https://ec.europa.eu/digital-single-market/en/open-internet-net-neutrality>

FBI, "*Federal Courts Order Seizure of 150 Website Domains Involved in Selling Counterfeit Goods as Part of DOJ, ICE-HSI, and FBI Cyber Monday Crackdown*" <https://archives.fbi.gov/archives/washingtondc/press-releases/2011/federal-courts-order-seizure-of-150-website-domains-involved-in-selling-counterfeit-goods-as-part-of-doj-ice-hsi-and-fbi-cyber-monday-crackdown>

Fei, Zongming (2001), "*A Novel Approach to Managing Consistency in Content Distribution Networks*", <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.19.4192&rep=rep1&type=pdf>

Ferguson, Paul/Huston, Geoff, "*What is a VPN?*" <https://www.potaroo.net/papers/1998-3-vpn/vpn.pdf>

Galvin, J, "*IAB and IESG Selection, Confirmation, and Recall Process: Operation of the Nominating and Recall Committees*" <https://www.ietf.org/rfc/rfc2727.txt>

Google Blocks Privacy Push at the Group That Sets Web Standards <https://www.bloomberg.com/news/articles/2019-09-24/google-blocks-privacy-push-at-the-group-that-sets-web-standards>

Google, "*Filter explicit results using SafeSearch*", <https://support.google.com/websearch/answer/510?source=gsearch&hl=en>

Haberleşme Komisyonu, "*Bulut Bilişim*", <https://www.btk.gov.tr/File/?path=ROOT/1/Documents/Sayfalar/Arastirma_Raporlari/Bulut_Bilisim.pdf>

Hern, Alex, "*Anti-porn filters stop Dominic Cummings trending on Twitter*", <https://www.theguardian.com/politics/2020/may/27/anti-porn-filters-stop-dominic-cummings-trending-on-twitter>

Hill, Jonah Force (2012), "*Internet Fragmentation - Highlighting the Major Technical, Governance and Diplomatic Challenges for U.S. Policy Makers*", <http://www.belfercenter.org/sites/default/files/legacy/files/internet_fragmentation_jonah_hill.pdf>

History of the Internet and Web <http://www.anderbergfamily.net/ant/history/>

Hoffman, Paul, "*The Tao of IETF: A Novice's Guide to the Internet Engineering Task Force*", <https://www.ietf.org/tao.html>

Huitema, C/Postel, J/S. Crocker, "*Not All RFCs are Standards*" <https://tools.ietf.org/html/rfc1796>

IANA, "*About the Internet Assigned Numbers Authority*" <http://www.iana.org/about/>

IANA, "*Port Numbers*", <http://www.iana.org/assignments/port-numbers>

ICANN, "*5G Technology*", <https://www.icann.org/en/system/files/files/octo-004-23jan20-en.pdf>

ICANN, "*Articles of Incorporation of Internet Corporation for Assigned Names And Numbers*" <https://www.icann.org/resources/pages/articles-2012-02-25-en>

ICANN, "Brief Overview of the Root Server System", <https://www.icann.org/en/system/files/files/octo-010-06may20-en.pdf>

ICANN, "*ICANN and the International Organization for Standardization (ISO)*", <https://www.icann.org/resources/pages/icann-iso-3166-2012-05-09-en>

ICANN, "*ICANN Board Transmits IANA Stewardship Transition Proposal and Enhancing ICANN Accountability Recommendations to NTIA*", < https://www.icann.org/stewardship>

ICANN, "*Internationalized Domain Names*", <https://www.icann.org/resources/pages/idn-2012-02-25-en>

ICANN, "*Scoping the relation between ICANN and Human Rights*" <https://community.icann.org/download/attachments/53772653/ICANN%20and%20Human%20Rights%20Jan2018.pdf>

IDC, "Worldwide Cloud 2019 Predictions" <https://www.idc.com/research/viewtoc.jsp?containerId=US43001718>

IETF, "*DNS Queries over HTTPS (DoH) - Request for Comments: 8484*", <https://tools.ietf.org/html/rfc8484>

IETF, "*Domain Administrators Guide*", <https://tools.ietf.org/html/rfc1032>

IETF, "*Domain Name System Structure and Delegation*", <https://www.rfc-editor.org/rfc/rfc1591.txt>

IETF, "*Guidelines for creation, selection, and registration of an Autonomous System (AS)*" <https://tools.ietf.org/html/rfc1930>

IETF, "*IPv6 is an Internet Standard*", <https://www.ietf.org/blog/ipv6-internet-standard/>

IETF, "*Netiquette Guidelines*", <http://www.ietf.org/rfc/rfc1855.txt>

IETF, "*The TLS Protocol*" <https://www.ietf.org/rfc/rfc2246.txt>

IETF, "*Working Group Guidelines and Procedures*" <https://tools.ietf.org/html/rfc2418>

IGF, "*About IGF FAQs*" <http://www.intgovforum.org/multilingual/content/about-igf-faqs>

International Telecommunication Union (2005), "*Report of the Tunis phase of the World Summit on the Information Society, Tunis, Kram Palexpo, 16-18 November 2005 WSIS-05/TUNIS/DOC/9(Rev.1)-E*", <http://www.itu.int/net/wsis/docs2/tunis/off/9rev1.pdf>,

Internet Architecture Board, "*Description*" <https://www.iab.org/about/description/>

Internet Archive: Wayback Machine <http://www.archive.org/web/web.php>

Internet Exchange Map <https://www.internetexchangemap.com>

Internet Network Operations' Groups <http://www.senki.org/network-operations-groups-meeting/>

Internet Research Task Force <https://irtf.org>

Internet Society (1997), "*Brief History of the Internet*", <https://www.internetsociety.org/wp-content/uploads/2017/09/ISOC-History-of-the-Internet_1997.pdf>

Internet Society (2012) "*Internet Society Perspectives on Domain Name System (DNS) Filtering*", <https://www.internetsociety.org/sites/default/files/Perspectives%20on%20Domain%20Name%20System%20Filtering-en.pdf>

Internet Society, "*Internet Society Perspectives on Internet Content Blocking: An Overview*", <https://www.internetsociety.org/sites/default/files/ContentBlockingOverview_20170326_FINAL_0.pdf>

Internet Society, "Net Neutrality Experts' Roundtable Series", <https://www.internetsociety.org/tag/netneutrality/>

IRTF, "*Current Research Groups*" <https://irtf.org/groups>

ISO, "*About ISO*" <http://www.iso.org/iso/home/about.htm>

ISO, "*ISO 3166-1:2013 Codes for the representation of names of countries and their subdivisions*" <http://www.iso.org/iso/home/standards/country_codes.htm>

ISO, "*ISO Country codes*" <https://www.iso.org/obp/ui/>

ISOC, "*Brief History of the Internet*" <http://www.internetsociety.org/sites/default/files/Brief_History_of_the_Internet.pdf>, s

ISOC, "*Internet Society Founding - An Oral History of the Internet Society's Founding*" <https://www.internetsociety.org/internet-society-founding>

İnternet Tarihi <http://www.internetarsivi.metu.edu.tr/tarihce.php>

İTÜ, "*NAT (Network Address Translation - Ağ Adresi Çeviricisi)*" <http://bidb.itu.edu.tr/seyirdefteri/blog/2013/09/07/nat-(network-address-translation---a%C4%9F-adresi-%C3%A7eviricisi)>

Lawis, Peter H, "*U.S. Begins Privatizing Internet's Operations*" <http://www.nytimes.com/1994/10/24/business/us-begins-privatizing-internet-s-operations.html>

Leyden, John, "*French gov used fake Google certificate to read its workers' traffic*" <https://www.theregister.co.uk/2013/12/10/french_gov_dodgy_ssl_cert_reprimand/>

Maxwell, Andy, "MPAA Granted 'Dynamic' Pirate Site Blocking Order in Singapore" <https://torrentfreak.com/mpaa-granted-dynamic-pirate-site-blocking-order-in-singapore-181006/>

Maxwell, Andy, "*US Embassy Threatens to Close Domain Registry Over 'Pirate Bay' Domain*" <https://torrentfreak.com/us-embassy-threatens-to-close-domain-registry-over-pirate-bay-domain-170620/>

Maxwell, Winston/Bourreau, Marc (2014) "*Technology Neutrality in Internet, Telecoms and Data Protection Regulation*", <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2529680>

Mozilla, "*451 Unavailable For Legal Reasons*" <https://developer.mozilla.org/en-US/docs/Web/HTTP/Status/451>

National Science Foundation, "*NSFNET Acceptable Use Policy*", <http://old.cni.org/docs/infopols/NSF.html>

NIST (2011) "*The NIST Definition of Cloud Computing*", <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>

Nichols, Shaun, "*Seven 'no log' VPN providers accused of leaking – yup, you guessed it – 1.2TB of user logs onto the internet*" <https://www.theregister.com/2020/07/17/ufo_vpn_database/>

NTIA (National Telecommunications and Information Administration) "*Memorandum of Understanding Between the U.S. Department of Commerce and the Internet Corporation for Assigned Names and Numbers*", <http://www.ntia.doc.gov/ntiahome/domainname/icann-memorandum.htm>

NTIA, "*Statement of Policy, Management of Internet Names and Addresses 63 Fed. Reg. 31741(1998)*", <https://www.ntia.doc.gov/federal-register-notice/1998/statement-policy-management-internet-names-and-addresses>

OECD, "*Governance*" <https://stats.oecd.org/glossary/detail.asp?ID=7236>

O'Reilly, Tim, "*Web 2.0 Nedir*", <http://www.turk-internet.com/portal/yazigoster.php?yaziid=14394>

Post, David G/Kehl, Danielle (2015), "*Controlling Internet Infrastructure The "IANA Transition" and Why It Matters for the Future of the Internet Part I*", <https://static.newamerica.org/attachments/2964-controlling-internet-infrastructure/IANA_Paper_No_1_Final.32d31198a3da4e0d859f989306f6d480.pdf>

Postel J/Reynolds J, "*Domain Requirements*" <https://tools.ietf.org/rfc/rfc920.txt>

Resnick, Pete "*On Consensus and Humming in the IETF*", <https://tools.ietf.org/html/rfc7282>

Reverse IP Lookup <https://hackertarget.com/reverse-ip-lookup/>

Root Server Technical Operations Association <http://www.root-servers.org>

Roy, Eleanor Ainge, "*Papua New Guinea bans Facebook for a month to root out 'fake users'*" <https://www.theguardian.com/world/2018/may/29/papua-new-guinea-facebook-ban-study-fake-users>

Samuels, Julie, "Rojadirecta: The Government Reverses Course and Returns Domains Without Explanation. Again" <https://www.eff.org/deeplinks/2012/08/rojadirecta-government-reverses-course-and-returns-domains-without-explanation>

Simon, Maarten/Müller, Moritz, "*Does the arrival of DoH mean browsers should be regulated?*" <https://www.sidn.nl/en/news-and-blogs/does-the-arrival-of-doh-mean-browsers-should-be-regulated>

Simonite, Tom, "*AI Has Started Cleaning Up Facebook, but Can It Finish?*" <https://www.wired.com/story/ai-has-started-cleaning-facebook-can-it-finish/>

Stone, Jeff, "*FBI enlists internet domain registries in fight against coronavirus scams*" <https://www.cyberscoop.com/fbi-coronavirus-scams-internet-domains/>

TechSpot, "*Wi-Fi 6 Explained: The Next Generation of Wi-Fi*" <https://www.techspot.com/article/1769-wi-fi-6-explained/>

The Institute for Information Security & Privacy at Georgia Tech (2016) "*Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others*", <http://www.iisp.gatech.edu/sites/default/files/images/online_privacy_and_isps.pdf>

Trendacosta, Katherine, "*This Disastrous Copyright Proposal Goes Straight to Our Naughty List*", <https://www.eff.org/deeplinks/2020/12/disastrous-copyright-proposal-goes-straight-our-naughty-list>

TSE (2013) "*Bulut Bilişim Güvenlik ve Kullanım Standardı (Taslak)*", <https://www.tse.org.tr/upload/tr/dosya/duyuruyonetimi/1082/12122014170015-2.pdf>

Twitter, "*About Twitter's link service (http://t.co)*" <https://support.twitter.com/articles/109623>

Vynck, Gerrit, "*Google Blocks Privacy Push at the Group That Sets Web Standards*" <https://www.bloomberg.com/news/articles/2019-09-24/google-blocks-privacy-push-at-the-group-that-sets-web-standards>

W3C, "*Facts About W3c*", <https://www.w3.org/Consortium/facts>

WGIG (2005) "*Report of the working group on Internet governance*", <http://www.wgig.org/docs/WGIGREPORT.pdf>

Yandex, "*Filter adult content*" <https://yandex.com/support/search/additional-features/adult-filter.html>

Zittrain, Jonathan/Edelman, Benjamin, "*Localized Google search result exclusions*", <https://cyber.harvard.edu/filtering/google/>

Zittrain, Jonathan/Faris, Robert/Noman, Helmi/Clark, Justin/Tilton, Casey/Morrison-Westphal, Ryan (2017) "*The Shifting Landscape of Global Internet Censorship*" Berkman Klein Center Research Publication No. 2017-4, Harvard Public Law Working Paper No. 17-38, <https://ssrn.com/abstract=2993485>

KAVRAM DİZİNİ

1

108 sayılı Sözleşme 109, 111, 112, 143, 158, 161, 162, 182, 185, 193, 346

5

5G 15, 62, 63, 517

A

açık ağ mimarisi 11, 149
actio popularis bkz. *halk davası*
adblocker 66, 75
AFRINIC 40
ağ tarafsızlığı 11, 25, 57, 85, 141, 182, 492, 496, 517
akran sansürü 74
aktif kullanıcı 236, 241, 499
anonimlik 111, 121, 126, 194, 339, 347, 488
APNIC 40, 54
arabuluculuk 70, 118
arama motorları 66, 70, 99, 157, 158, 166, 167, 174, 206, 215, 216, 259, 277, 315, 318, 347, 351, 356, 357, 358, 467, 494
ARIN 40
ARPANET 8
arşivlere erişim 112, 488

B

bilgisayar okuryazarlığı 129, 306
bilgiye erişim hakkı 31, 115, 120, 134, 136, 150, 164, 175, 195, 274, 277, 318, 359, 491, 501
bulut bilişim 22, 89, 199, 517

C

caydırıcı etki 91, 290, 301, 319, 330, 347, 353, 370, 379, 450, 503
CERN 9, 49
chilling effect bkz. *caydırıcı etki*
co-regulation bkz. *ortak düzenleme*

Ç

çocuk pornografisi 2, 128, 131, 315, 321, 428, 435, 469

D

DDOS 87
deep packet inspection bkz. *derin paket analizi*
de-listing 301
demonitezation 89
derin paket analizi 82, 86, 90, 222, 284, 485
digital rights management bkz. *dijital hak yönetimi*
dijital arşivler 339, 348, 353, 358, 359
dijital hak yönetimi 85
dijital medya 249, 253
dinamik IP 16, 18
DNS 18, 36, 39, 54, 55, 58, 89, 95, 97, 103, 210, 217, 485

DNS engelleme 80, 210, 222
domain de-registration 88
DPI bkz. *Deep Packet Inspection*
DRM bkz. *dijital hak yönetimi*

E

erişim engelleme 64, 69, 70, 72, 78, 79, 90, 96, 100, 224, 238, 402
eşyaların interneti 15, 18, 31, 33, 43
ex-ante 390, 420, 423, 439, 459, 479, 510
ex-post 390, 420, 423, 439, 459, 479, 510

F

false negative bkz. yanlış negatif
false positive bkz. yanlış pozitif
filtreleme 2, 57, 61, 67, 69, 73, 75, 78, 84, 101, 104, 116, 118, 119, 121, 122, 124, 133, 134, 141, 163, 182, 189, 214, 233, 239, 260, 268, 271, 284, 330, 413, 425, 428, 435, 447, 464, 483, 491, 499, 512, 515
filtresiz tarayıcı 437
fragmantasyon 61, 62

G

gizli sansür 131
gözetim 194

H

hakaret 209, 232, 245, 259, 287, 295, 296, 297, 315, 320, 322, 323, 327, 333, 362, 365, 373, 375, 387, 391, 394, 428, 498, 500, 502, 503,
haksız fiil 324, 326, 333, 388, 502
halk davası 226, 235, 241
hesap verebilirlik 139, 170, 180, 185, 492

I

IAB 43, 44
IANA 17, 39, 40, 41, 44, 52, 54, 80
ICANN 30, 36, 39, 40, 47, 48, 52, 56, 146, 493
IETF bkz. *Internet Engineering Task Force*
IGF 44, 47
Internet Architecture Board 43, 49
Internet Engineering Task Force 17, 40, 43, 44, 49
Internet Exchange Point 14, 50, 56
Internet Society 48, 49
IOT bkz. *eşyaların interneti*
IP adresi 15, 50, 79, 80, 94, 231, 318, 410, 414, 461, 464, 466, 472, 474, 475, 484, 506
IPv4 16, 17, 39, 144, 492, 516
IPv6 17, 18, 39, 50, 144, 516
ırkçılık 128, 131, 321, 372
ISO bkz. *Uluslararası Standartlar Teşkilatı*
ISOC bkz. *Internet Society*
IXP bkz. *Internet Exchange Point*

İ

içerik dağıtım ağı 25
içerik engelleme 84, 86, 100, 105, 134, 312, 471
içerik sağlayıcısı 25, 75, 95, 255, 334, 336, 357, 366
içerik şikâyet mekanizmaları 119
ihtiyati tedbir 71, 72, 508
indeksten çıkarma 163, 164, 165
İnternet Ağ İşletmecileri Grupları 50,
internet aracıları 198, 199, 200, 497
internet değişim noktası bkz. *Internet Exchange Point*
internet içeriğinin filtrelenmesi 61, 133
internet özgürlüğü göstergeleri 186
internet servis sağlayıcısı 11, 27, 102
internetin bütünlüğü 149, 153, 154, 493
internetin evrenselliği 149, 151, 179, 493

İSS bkz. *internet servis sağlayıcısı*

K

kamu düzeni 2, 63, 113, 173, 191, 276, 405, 443, 450, 500, 515
kişisel verilerin korunması 38, 57, 74, 83, 109, 112, 113, 128, 152, 157, 161, 179, 182, 185, 193, 206, 342, 357, 359, 496, 517
koruma tedbirleri 71, 72, 79, 81

L

LACNIC 40

M

MAC bkz. *Media Access Control*
Madde 29 Çalışma Grubu 111, 166, 346
mahremiyet 38, 45, 49, 50, 57, 74, 96, 109, 110, 119, 127, 128, 130, 133, 136, 137, 143, 157, 162, 166, 169, 172, 174, 175, 185, 197, 199, 206, 223, 273, 324, 339, 350, 426, 433, 491
Media Access Control 21, 22, 65, 69

N

NAT IP 16, 17
nefret söylemi 2, 3, 67, 116, 131, 191, 243, 255, 273, 294, 296, 300, 301, 316, 319, 320, 321, 372, 394, 395, 499, 500, 511, 512, 513,
netiquette 36
netizen 15
NSF 8

O

obiter dictum 240
OECD 45, 333
online taciz 176
ortak düzenleme 116, 121, 124, 135, 159, 165, 203, 497
otosansür 85, 91, 190, 265, 271, 303, 372, 516

Ö

önleyici kısıtlamalar 406, 409, 507
öz düzenleme 111, 115, 117, 120, 124, 128, 135, 159, 165, 181, 489, 497
özen yükümlülüğü 153, 154, 382

P

pasif kullanıcı 236, 499
peering 14
PEGI 139
phising 65
platformların sorumluluğu 267, 271, 318, 335, 499
POP noktası 14
pornografi 2, 86, 101, 116, 131, 138
port 17, 19, 80, 220
prior restraints bkz. *önleyici kısıtlamalar*
privacy by design 169
privacy enhancing technologies 128
private censorship 243, 303, 499
proaktif 272, 343, 395, 499, 512
proxy 58, 82, 84, 99,

R

ratione materiae 234
request for comments 41, 42, 44, 48,
reverse IP address lookup 79
RFC bkz. *Request for Comments*
RIPE 40
router 12, 16, 22, 69, 82, 85

S

sanal gerçeklik
secure sockets layer
SLAPP 92, 203, 511
SMTP 17, 80
sosyal medya 2, 15, 57, 66, 78, 90, 93, 155, 167, 189, 192, 254, 256, 266, 272, 277, 334, 336, 397, 404, 407, 413, 429, 447, 465, 494, 495, 504,

511, 515
Starlink 13
statik IP 16, 66
subdomain 19, 20
super-flagging 74

Ş

şeffaflık 26, 27, 29, 54, 110, 112, 160, 170, 180, 185, 199, 201, 203, 424, 457, 509, 513
şiddete teşvik 2, 255, 261, 262, 294, 301, 302, 316, 319, 394, 499, 511, 512, 513

T

tamamlayıcı sansür 92, 265
TCP/IP 8, 10, 84
telif hakları 70, 172, 224, 228, 234, 236, 426, 498
TİB 209
tor tarayıcısı 98, 426
trafik yönetimi 2, 27, 61, 141, 142, 184, 185

U

üç ihlal kuralı 68
Uluslararası Standartlar Teşkilatı 41, 48
unutulma hakkı 4, 67, 115, 206, 259, 318, 337, 346, 355, 357, 360
URL 20, 49, 75, 82, 85, 94, 97, 101, 209, 222, 384, 399, 426, 428, 441, 446, 453,
üst düzey alan adları 19, 48, 81, 88, 146, 493
uyar-kaldır 70, 94, 233, 245, 252, 260, 261, 266, 271, 286, 290, 297, 299, 329, 330, 484, 500, 501, 512, 513

V

VPN 58, 66, 95, 98, 99, 102, 103, 426

W

W3C bkz. *World Wide Web Consortium*
Web 2.0 24, 100, 209, 221, 244, 254, 272, 302, 320, 385, 395
WHOIS 38
World Wide Web Consortium 49

Y

yanlış negatif 465
yanlış pozitif 465
yer sağlayıcı 3, 66, 70, 78, 90, 95, 212, 218, 272, 288, 331, 336, 400, 444, 446, 468, 469, 472, 475, 478
yönetişim 4, 26, 36, 44, 117, 130, 137, 146, 147, 148, 149, 186, 301, 302, 493

Z

zero rating 28, 29